Agenzia nazionale per le nuove tecnologie,
l'energia e lo sviluppo economico sostenibile

MINISTERO DELLO SVILUPPO ECONOMICO

Ricerca di Sistema elettrico

Local Energy Communities: definizione visione, modelli, tecnologie

O. Gregori, M. Annunziato, S. Bossi, M. Chinnici,
P. Clerici Maestosi, G. D'Agosta, G. D'Agostino,
P. De Sabbata, N. Gessa, G. Massa, C. Meloni,
F. Moretti, S. Pizzuti, S. Sylos Labini,
A. Tofani

RdS/PTR(2019)/010

LOCAL ENERGY COMMUNITIES: DEFINIZIONE VISIONE, MODELLI, TECNOLOGIE

O. Gregori, M. Annunziato, S. Bossi, M. Chinnici, P. Clerici Maestosi, G. D'Agosta, G. D'Agostino, P. De Sabbata, N. Gessa, G. Massa, C. Meloni, F. Moretti, S. Pizzuti, S. Sylos Labini, A. Tofani (ENEA)

Dicembre 2019

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dello Sviluppo Economico - ENEA
Piano Triennale di Realizzazione 2019-2021 - I annualità
Obiettivo: Tecnologie
Progetto: Tecnologie per la penetrazione efficiente del vettore elettrico negli usi finali
Work package 1: Local Energy District
Linea di attività 46: Local Energy Communities: definizione visione, modelli, tecnologie.
Responsabile del Progetto: Claudia Meloni, ENEA
Responsabile del Work package: Claudia Meloni, ENEA

Indice

Sommario

Nella Linea di Attività 46 sono state svolte le attività preliminari allo studio di un nuovo filone di ricerca sulle Energy Communities, che prende avvio con il presente Piano triennale della RdS, nell'ambito del WP1, Progetto 1.7.
L'attività, che è stata svolta dal mese 1 al mese 12, ha visto le seguenti azioni:

- analisi dello stato dell'arte e progetto del modello di riferimento per local energy communities che sarà utilizzato per la progettazione e l'implementazione della piattaforma a servizio della energy community; tale modello è basato su convertibilità tra flessibilità energetica, virtuosismo energetico da una parte e servizi di comunità dall'altra;
- la definizione dello stato dell'arte nelle tecnologie blockchain con l'identificazione della piattaforma disponibile che meglio risponde alle esigenze identificate per la energy community;
- identificazione di strategie di coinvolgimento degli utenti attraverso l'utilizzo di reti sociali;
- identificazione dei ruoli e delle capacità dei partecipanti.

I risultati di questa attività, integrati con lo studio realizzato dal Politecnico di Milano sul quadro regolatorio del sistema elettrico (LA 51) e l'analisi prodotta da ENEA sull'integrazione della Energy Community con la rete elettrica (LA 69) costituiscono un esaustivo stato dell'arte delle tecnologie abilitanti per la Energy Community.
L'output di questa attività sarà la base di lavoro di tutto il lavoro implementativo per le successive linee di attività sulla Local Energy Community.

1. INTRODUZIONE

Questa Linea di Attività si propone la creazione di modelli e strumenti per la nascita di Energy Community a supporto dei differenti profili energetici che caratterizzano il tessuto urbano (abitazioni, terziario, piccole imprese). L'obiettivo è quello di fornire un ampio spettro di servizi e tool, destinato ai vari attori che partecipano alla Energy Community, a partire da un'analisi dettagliata degli scenari di interazione tra essi e, contemporaneamente, tra la comunità e i gestori energetici. L'utilizzo di moderne tecnologie, come le blockchain, gli strumenti di ottimizzazione degli hub energetici e la collaborazione con gli altri task del progetto permetteranno la creazione di un ecosistema energetico intelligente ed interattivo con la rete di distribuzione dell'energia.

L'obiettivo è lo sviluppo di metodologie, infrastrutture tecnologiche, modelli gestionali ed economici per sostenere e sviluppare la aggregazione e l'iniziativa dei prosumers e la messa a punto di un processo auto-organizzativo (codificato) di una comunità di cittadini che sviluppa la capacità di auto-gestire una serie funzionalità connesse alla rete energetica; tra le funzionalità citiamo la relazione con le utilities e le ESCO, la riqualificazione della propria abitazione nella direzione smart home con funzioni di aggregazione e di assisted living, la formazione dei cittadini ed il supporto alla consapevolezza energetica ed infine la partecipazione alla governance del distretto.

Nel task sono incluse una serie di tecnologie abilitanti per la implementazione della energy community e lo sviluppo dei modelli abilitanti di servizi aggregati per i cittadini basata su blockchain e di metodologie per la remunerazione della flessibilità e del comportamento virtuoso della comunità attraverso l'utilizzo di cripto valute locali.

L'attività si focalizza sulla definizione del modello di riferimento di una piattaforma per le Energy Communities in grado di fornire i seguenti servizi:

- valorizzazione energetica dei comportamenti dei membri della Community (tra cui abitazioni, piccole aziende ecc.);
- valorizzazione della flessibilità elettrica verso il distributore e/o tra utenti della comunità;
- valorizzazione del virtuosismo energetico con servizi di comunità;
- co-design dei servizi di comunità.

L'attività sulla *energy community* comprende:

- definizione del concept per le Energy Communities e analisi degli attuali scenari tecnologi e normativi (1 annualità);
- progettazione e implementazione della piattaforma per lo scambio di beni e servizi (flessibilità energetica e di comunità) per le LEC, studio di un modello di economia locale di sharing (2 annualità).
- applicazione prototipale su un distretto urbano del modello implementato per la Energy Community con ingaggio degli utenti (3 annualità).

L'attività mira a mitigare il decongestionamento della rete elettrica attraverso la promozione di comportamenti virtuosi da parte di chi consuma e chi produce elettricità da fonti rinnovabili; inoltre contribuisce alla creazione di potere d'acquisto addizionale per attivare le risorse inutilizzate all'interno di una Comunità e al soddisfacimento di bisogni sociali e economici inespressi. In particolare attraverso l'analisi e lo sviluppo di Energy Community basate sul paradigma della blockchain si intendono valutare i costi ed i benefici economici, ambientali, sociali derivanti, tra cui:

- l'ottimizzazione dell'autoconsumo e il contributo alla produzione/consumo di fonti rinnovabili;
- la partecipazione attiva alla gestione del sistema elettrico (riduzione degli sbilanciamenti);
- la riduzione delle emissioni inquinanti;
- la riduzione della dipendenza energetica dall'estero;
- la coesione sociale.

In sostanza, con questa ricerca vengono messi in relazione il vettore elettrico con le monete virtuali e la blockchain ed entrano in gioco questioni sociali, economiche ed energetiche. Nell'ambito dell'evoluzione del sistema elettrico verso la smart grid, le Energy Community rappresentano uno dei principali elementi costitutivi della sua architettura. La blockchain è una tecnologia che può accelerare e favorire l'evoluzione del mercato elettrico in tal senso, permettendo la gestione di transazioni condivise tra più nodi di una rete, senza il bisogno di intermediari.

2. DESCRIZIONE DELLE ATTIVITÀ SVOLTE E RISULTATI

I capitoli successivi (da cap. 3 a cap 9) descrivono le attività svolte e i risultati ottenuti nell'ambito della presente Linea di Attività.

Il capitolo 3 si concentra sulla realtà innovativa del Positive Energy District, uno dei risultati delle 10 linee d'azione del SET-PLAN nella sua versione aggiornata. Viene chiarito il ruolo che, nel SET-PLAN e nella recente normativa comunitaria, viene dato al consumatore ed alla comunità in cui esso è integrato. Si conclude con il presentare l'azione innovativa dei Positive Energy Districts che saranno oggetto di analisi nelle successive annualità in linea con l'azione attualmente in corso in ambito comunitario nel PED Programme.

Nel capitolo 4 si analizzano i potenziali drivers di cambiamento del sistema energetico attuale, quali la tecnologia blockchain, i modelli di economia collaborativa, il paradigma delle Energy Community (EC) ed i sistemi di crowdsourcing. In questa prima parte del rapporto è delineato il concept ENEA di Energy Community, espressione della convergenza in un unico framework delle tre dimensioni dell'innovazione - tecnologica, sociale e collaborativa - necessarie alla transizione energetica.

Nel capitolo 5 si esaminano le possibili applicazioni della tecnologia blockchain al settore energetico, dal lato della domanda, evidenziandone sia i vantaggi che le attuali barriere normative, tecnologiche ed economiche.

Il capitolo 6 descrive le tipologie e categorie di Energy Community ponendo l'accento sull'aspetto organizzativo e sulla dimensione sociale delle collettività di riferimento. Il capitolo contiene inoltre una rassegna di casi d'uso per categoria di EC a livello internazionale ed una SWOT analysis di comparazione tra l'attuale regime energetico e le EC Centralizzate, Distribuite e Decentralizzate.

Nel capitolo 7 si analizzano le tipologie, gli obiettivi ed il funzionamento delle community inclusive currency. In particolare l'attenzione è rivolta ai Local Exchange Trading Systems, un sistema di valuta comunitaria considerato, dalla letteratura, tra i più evoluti e particolarmente idonei a sviluppare una struttura di reciprocità, ricostruendo lo spirito comunitario attraverso la valorizzazione delle forze sociali.

Il capitolo 8 esamina i fondamenti della tecnologia blockchain in termini di crittografia, teoria dei giochi e linguaggi di programmazione nonchè i requisiti prestazionali della facility computazionale ENEA. L'analisi è propedeutica e funzionale alla selezione della piattaforma blockchain da impiegare per la gestione del modello di Energy Community proposto.

Infine il capitolo 9 riporta le conclusioni che sono state raggiunte nel lavoro presentato e che rappresentano la base per la costruzione delle attività future.

3. IL RUOLO DEL CONSUMATORE E DELLE ENERGY COMMUNITY NEL QUADRO DI RIFERIMENTO EUROPEO

3.1 Strategia dell'Unione Europea sull'Energia

La strategia dell'Unione Europea sull'Energia è stata pubblicata nel febbraio 2015 (COM/2015/080) come priorità chiave del governo Juncker (2014-2019) con l'obiettivo chiaro di offrire ai consumatori della UE un'energia sicura, sostenibile, competitiva e conveniente promuovendo una strategia quadro per un'Unione dell'energia resiliente, corredata da una politica lungimirante in materia di cambiamenti climatici.

Per il raggiungimento di questo obiettivo occorre operare una drastica trasformazione del sistema energetico europeo, disegnando un sistema energetico integrato a livello continentale che consenta ai flussi di energia di transitare liberamente attraverso le frontiere e che si fondi sulla concorrenza e sull'uso ottimale delle risorse. Bisogna altresì prendere le distanze da un'economia basata sui combustibili fossili, con una gestione centralizzata dell'energia incentrata su un'offerta che si avvale di tecnologie obsolete e si fonda su modelli economici superati. Occorre consentire ai consumatori di assumere un ruolo attivo mettendo nelle loro mani le informazioni e la possibilità di operare delle scelte, garantendo la flessibilità per gestire non solo l'offerta ma anche la domanda.

Secondo i dati riportati nella COM/2015/080 l'Unione Europea importa il 53% del proprio bisogno energetico, con un costo di circa 400 miliardi di euro, collocandosi così al primo posto per l'importazione di energia. Sei Stati Membri dipendono da un unico fornitore esterno per la totalità delle importazioni di gas e rimangono quindi troppo vulnerabili alle crisi di approvvigionamento. Inoltre il 75% del parco immobiliare è a bassa efficienza energetica, mentre il 94% dei trasporti dipende dai prodotti petroliferi, di cui il 90% importati da aree extraeuropee.

SE poi si considerano i prezzi all'ingrosso dell'elettricità questi rimangono superiori del 30% rispetto a quelli praticati negli Stati Uniti, così come i prezzi del gas che sono più che doppi. Il differenziale dei prezzi rispetto ad altre economie incide sulla competitività della nostra industria, in particolare in tutti quei settori ad alta intensità energetica.

Un mercato dell'energia integrato è necessario per rafforzare la concorrenza, incrementare l'efficienza del mercato migliorando l'uso degli impianti di generazione di energia e garantire prezzi accessibili ai consumatori.

3.2 Le cinque dimensioni della Energy Union

L'Energy Union [1] è un misto di misure legislative e proposte politiche che sono state poste in essere negli anni passati e che in futuro verranno rafforzate. L'iniziativa evidenzia l'interesse crescente delle autorità Europee per i temi energetici e per un approccio "allargato" alla sicurezza energetica, enfatizzando il ruolo di ogni governo in questo campo.

L'Unione dell'energia è l'approdo di una evoluzione iniziata con il Libro verde della Commissione Europea sulla politica di efficienza energetica del 2005 (COM/2005/265) che rappresentava una ripresa dei temi dell'efficienza energetica dopo i primi passi degli anni 90 (Direttiva 93/76/CEE). L'evoluzione successiva passa attraverso la direttiva del 2006 e trova un assetto stabile con la direttiva 27/2012 che è solo parzialmente modificata con il Winter Package pubblicato nel novembre 2016, senza tuttavia dimenticare la strategia 2020 in cui la Commissione collocava l'efficienza energetica al centro della strategia energetica dell'Unione.

La strategia dell'Energy Union si articola in cinque dimensioni, strettamente interconnesse e che si rafforzano a vicenda tese a migliorare:

a) la sicurezza energetica, solidarietà e fiducia;

b) piena integrazione del mercato europeo dell'energia;
c) efficienza energetica per contenere la domanda;
d) decarbonizzazione dell'economia;
e) ricerca, innovazione e competitività.

È in questo quadro di riferimento che và calato il "New Deal" per i consumatori. In una Unione dell'energia i consumatori di un determinato Stato Membro dovrebbero poter fare scelte informate ed essere liberi di acquistare energia agevolmente anche da società ubicate in altri Stati Membri. Infatti in alcuni Stati Membri i consumatori godono di una scelta limitata di fornitori e le procedure per cambiare fornitore sono relativamente complesse. Per rafforzare la posizione dei consumatori gli Stati Membri e le autorità nazionali devono attuare ed applicare pienamente la normativa europea vigente, comprese le norme di tutela dei consumatori in modo da offrire ai consumatori informazioni comprensibili e facilmente accessibili, strumenti di agevole uso e incentivi finanziari per risparmiare energia. Grazie alle tecnologie intelligenti i consumatori e le imprese di servizi energetici potranno avvantaggiarsi delle opportunità esistenti sul mercato dell'energia controllando il proprio consumo energetico, ed eventualmente producendo essi stessi energia. Il ruolo del consumatore verrà ridisegnato grazie ad una maggiore flessibilità del mercato con conseguente riduzione dei costi per i consumatori.

3.3 Il ruolo del consumatore: consumer, prosumer e Energy Community

Il nuovo approccio richiesto dalla Energy Union Strategy tende a spostare il baricentro dal lato dell'offerta a quello della domanda in quanto riconosce una necessaria valorizzazione del consumatore finale. A tale soggetto infatti viene riconosciuto un ruolo centrale anche grazie alla introduzione ed alla installazione degli smart metering che consentono non solo fatturazione su misure reali ed informazione giornaliera dei consumi ma anche un miglioramento delle performance relative alle attività commerciali ed alle offerte dei venditori. Inoltre introducono una nuova funzionalità utilizzabile per la diffusione dell'informazione, per servizi di efficienza energetica come per offerte di servizi innovativi da parte dei venditori. Questo nuovo ruolo del consumatore può essere ulteriormente esteso anche attraverso l'attivazione di contratti di Demand Side Response con possibilità di distacco in tempi brevi (da remoto), quindi di supporto alla rete con remunerazione nei momenti di criticità.

Il nuovo ruolo del consumatore si concentra sulla capacità/possibilità dell'utilizzatore finale da un lato di scegliere consapevolmente quanto consumare e quanto risparmiare (consumer), dall'altro attribuisce al cittadino la capacità di diventare prosumer ossia consumatore attivo di energia rinnovabile. E poiché i prosumer possono rappresentare sia nuclei familiari, sia istituzioni che piccole aziende che partecipano al marcato dell'energia producendola su base individuale o collettiva si diversifica ulteriormente il ruolo del consumatore fino alla nascita delle Energy Community intese quali comunità di utenze (private, pubbliche, o miste) localizzate in una determinata area di riferimento in cui gli utilizzatori finali (cittadini, imprese, Pubblica Amministrazione, ecc.), gli attori di mercato (utility, ecc.), i progettisti, gli addetti alla pianificazione e i politici cooperano attivamente per sviluppare livelli elevati di fornitura "intelligente" (smart) di energia, favorendo l'ottimizzazione dell'utilizzo delle fonti rinnovabili e dell'innovazione tecnologica nella generazione distribuita e abilitando l'applicazione di misure di efficienza, al fine di ottenere benefici sulla economicità, sostenibilità e sicurezza energetica [2].

Il ruolo chiave delle Community è delineato molto chiaramente nella Direttiva UE del giugno 2019 [3] dove viene ribadito che i consumatori possono svolgere un ruolo strategico attraverso le "comunità energetiche dei cittadini", le "citizen energy communities". "Le comunità energetiche dei cittadini", si legge nel testo "non dovrebbero essere soggette a restrizioni normative quando

applicano tecnologie dell'informazione e della comunicazione esistenti o future per condividere tra i loro membri o soci, sulla base di principi di mercato, l'energia elettrica prodotta utilizzando impianti di generazione all'interno della comunità energetica dei cittadini, per esempio compensando la componente energetica dei membri o soci con la produzione disponibile all'interno della comunità, anche se la condivisione avviene sulla rete pubblica, purché entrambi i punti di misura appartengano alla comunità. La condivisione consente ai membri o soci di essere riforniti di energia elettrica proveniente da impianti di generazione all'interno delle comunità senza trovarsi in prossimità fisica diretta dell'impianto di generazione o sottesi a un punto di misura unico. Qualora l'energia elettrica sia condivisa, la condivisione non dovrebbe incidere sulla riscossione degli oneri di rete, delle tariffe e dei tributi connessi ai flussi di energia elettrica. La condivisione dovrebbe essere agevolata nel rispetto degli obblighi e delle tempistiche stabiliti per il bilanciamento, la misurazione e il conguaglio. Le disposizioni della presente direttiva relative alle comunità energetiche dei cittadini non interferiscono con le competenze degli Stati membri in materia di elaborazione e attuazione delle politiche per il settore energetico relative agli oneri di rete e alle tariffe o di elaborazione e attuazione di sistemi di finanziamento della politica energetica e di ripartizione dei costi, purché tali politiche siano non discriminatorie e legittime".

Si punta dunque l'accento sullo sharing energetico.

Inoltre si dice che gli Stati membri dovrebbero adottare le misure necessarie per proteggere i clienti vulnerabili e in condizioni di povertà energetica nel contesto del mercato interno dell'energia elettrica. Tali misure possono variare a seconda delle circostanze particolari nello Stato membro in questione e possono includere misure sociali o di politica energetica. E dunque tale scenario apre ad una visione del consumatore che non è solo attore in quanto prosumer energetico ma quale soggetto in grado in interagire nella comunità energetica attraverso anche in termini di soggetto in "povertà energetica", verso il quale occorre identificare idonei strumenti e modelli di sostegno in seno alle "citizen energy communities".

Viene rimarcato anche l'aspetto legato al benessere dei cittadini. I servizi energetici sono fondamentali per salvaguardare il benessere dei cittadini dell'Unione. Un'erogazione adeguata di calore, raffrescamento, illuminazione ed energia per alimentare gli apparecchi è essenziale per garantire un tenore di vita dignitoso e la salute dei cittadini. Inoltre, l'accesso a tali servizi energetici consente ai cittadini dell'Unione di sfruttarne appieno le potenzialità e migliora l'inclusione sociale. Basso reddito, spesa elevata per l'energia e scarsa efficienza energetica delle abitazioni sono concause che impediscono ai nuclei famigliari in condizioni di povertà energetica di usufruire di questi servizi. Gli Stati membri dovrebbero raccogliere le informazioni necessarie a monitorare il numero di nuclei famigliari che versano in condizioni di povertà energetica. In questo compito di individuazione, teso a fornire sostegno mirato, gli Stati membri dovrebbero avvalersi di misurazioni accurate.

L'Unione Europea promuove quindi approcci integrati, ad esempio nel quadro della politica sociale ed energetica, e relative misure sia in termini di politiche sociali che di miglioramenti dell'efficienza energetica per le abitazioni. La recente direttiva dovrebbe migliorare le politiche nazionali a favore dei clienti vulnerabili e in condizioni di povertà energetica

3.4 SET Plan ed Energy Union: ricerca, innovazione e competitività versus i Positive Energy District

Il SET Plan [4] è uno degli strumenti messi a punto a livello comunitario in grado di promuovere la transizione verso un sistema energetico neutro dal punto di vista climatico. Il SET Plan promuove azioni coordinate tra le Stati Membri sulle nuove tecnologie riducendo così i costi grazie alla

collaborazione ed all'allineamento della ricerca internazionale sugli obiettivi chiave dell'Unione dell'Energia.
Il SET Plan ha adattato nel 2015 la sua struttura e i suoi processi per accelerare efficacemente la trasformazione del sistema energetico dell'UE in linea con questo nuovo obiettivo proponendo un focus più mirato in dieci azioni strutturate attorno alle priorità di ricerca e innovazione dell'Unione dell'Energia con approccio integrato, allontanandosi da un focus specifico sulle tecnologie per guardare invece al sistema energetico nel suo insieme Sono così state identificate 10 key actions con l'obiettivo di sviluppare tecnologie rinnovabili performanti integrate nel sistema energetico; ridurre il costo delle principali tecnologie rinnovabili; creare nuove tecnologie e servizi per i consumatori; aumentare la resilienza e la sicurezza del sistema energetico; sviluppare materiali e tecnologie ad alta efficienza energetica per gli edifici; migliorare l'efficienza energetica per l'industria; far diventare l'Europa competitiva nel settore globale delle batterie (e-mobility); rafforzare la diffusione sul mercato dei carburanti rinnovabili; guidare l'ambizione nella cattura del carbonio e nello stoccaggio /utilizzo; aumentare la sicurezza nell'uso dell'energia nucleare.
A seguito del processo consultivo avviato nel 2016, che identificava le priorità chiave e fissava gli obiettivi per ciascuna delle dieci azioni chiave, a gennaio 2018 sono stati adottati undici piani di attuazione (SET-Plan action Implementation Plan) in diversi settori.
Sono quindi stati istituiti dallo Steering Group del SET-Plan gli Implementation Working Group (IWG) al fine di affrontare e promuovere 10 azioni per la ricerca e l'innovazione in grado di trasformare il sistema energetico europeo ed aumentare il potenziale di crescita ed occupazione dell'Unione Europea nel campo dell'energia. I paesi del SET-Plan, rappresentati negli IWG da funzionari pubblici o persone nominate dai rispettivi governi, si sono impegnati a utilizzare i loro programmi e politiche nazionali di R&I nel settore dell'energia per attuare alcune delle attività di R&I selezionate dall'IWG, sviluppando e perseguendo la ricerca congiunta con altri paesi.
Gli IWG hanno identificato specifiche iniziative di R&I definite come "iniziative faro", in grado di evidenziare come progetti di R&I coordinata, a livello nazionale e dell'UE, possano contribuire al raggiungimento degli obiettivi e comportare attività di interesse visibili al grande pubblico. Sulle iniziative faro che riguardano anche il "new Deal" dei consumatori, inteso come ***smart consumer-center energy system***, lavorano l'IWG Implementation Working Group 3.1 "Energy Consumers" e IWG Implementation Working Group 3.2 "Smart Cities and Communities".
IWG 3.1 Energy Consumers - ha prodotto un Implementation Plan [5] il cui focus sono gli standard per gli apparecchi intelligenti che potrebbero facilitare l'accessibilità dei dispositivi per i consumatori concentrandosi essenzialmente su 2 pilastri l'interoperabilità delle soluzioni energetiche intelligenti da un lato e i vantaggi per i consumatori dall'altro. Sono così state identificate 7 azioni prioritarie (rispettivamente 5 sull'interoperabilità e 2 sui benefici per i consumatori), per raggiungere l'obiettivo generale ossia quello di sviluppare ulteriormente soluzioni plug-and-play per la gestione dell'energia che porteranno a un ambiente di vita più confortevole, conveniente e più sano a costi energetici inferiori per i consumatori. Le soluzioni plug-and-play saranno basate su tecnologie ICT e energetiche e i servizi che ne deriveranno potranno essere implementati nelle case utilizzando modelli di business e servizi innovativi. Gli stessi dispositivi aumenteranno inoltre l'efficienza energetica, creeranno nuove opportunità di risposta alla domanda, ottimizzeranno il funzionamento degli edifici e garantiranno l'integrazione delle RES nelle case.
Gli interventi in R&I contribuiranno a sviluppare le tecnologie abilitanti per la casa intelligente attraverso la dimostrazione di nuovi servizi e modelli organizzativi basati sull'**interoperabilità e sulla condivisione dei dati** tra diversi dispositivi migliorare le prestazioni degli strumenti per la previsione del consumo di elettricità della casa intelligente (range 80% del consumo reale con 1 ora di anticipo); sviluppare interfacce user-friendly (comprese le app) che trasformano le tecnologie di gestione

dell'energia in servizi di facile utilizzo accompagnati dallo sviluppo di KPI (Key Performance Indicator) rigorosi per misurare i benefici per i consumatori; implementazione di sensori e controllori avanzati e interoperabili collegati o integrati nei dispositivi di energia domestica che possono essere facilmente integrati nei sistemi di gestione domestica intelligente e sono facili da mantenere e aggiornare.

IWG 3.2 "Smart Cities and Communities" - Il focus dell'Implementation Plan è sui **Positive Energy District** quali soluzioni per aumentare la qualità della vita nelle città europee, contribuire al raggiungimento degli obiettivi COP21 e migliorare le capacità e le conoscenze europee per diventare un modello globale. L'Implementation Plan ha sviluppato un approccio integrato che include prospettive tecnologiche, spaziali, normative, legali, finanziarie, ambientali, sociali ed economiche per supportare la pianificazione, la diffusione e la replica di PED per l'urbanizzazione sostenibile.

L'Europa potrà così diventare un modello globale per le soluzioni integrate e innovative per la pianificazione, la diffusione e la replica dei distretti energetici positivi con l'obiettivo di avere almeno 100 distretti energetici positivi entro il 2025, che siano sinergicamente collegati al sistema energetico in Europa. I PED richiedono l'interazione e l'integrazione tra gli edifici, gli utenti e il sistema energetico, di mobilità, nonché un approccio integrato comprendente prospettive tecnologiche, spaziali, normative, finanziarie, legali, sociali ed economiche. Idealmente, i PED saranno sviluppati in un quadro di innovazione aperto, guidato dalle città in cooperazione con l'industria e gli investitori, la ricerca e le organizzazioni di cittadini. In questo contesto, un PED è visto come un distretto con un'importazione netta annua di energia pari a zero e un'emissione netta pari a zero di CO2 che lavora verso una produzione locale in eccesso di energia rinnovabile.

I "mattoni" dei PED [6] sono:

- essere incorporato in un sistema energetico urbano e regionale, preferibilmente guidato da energia rinnovabile, al fine di fornire sicurezza e flessibilità di approvvigionamento ottimizzate;
- l'elettricità generata da sistemi dedicati di energia rinnovabile nella regione e la biomassa fornita alla PED non sono necessariamente considerate importazione nella PED;
- un PED si basa su un elevato livello di efficienza energetica, al fine di mantenere il consumo annuo di energia locale inferiore alla quantità di energia rinnovabile prodotta localmente;
- all'interno del sistema energetico regionale, un PED consente l'uso di energia rinnovabile offrendo flessibilità ottimizzata e nella gestione dei consumi e delle capacità di stoccaggio su richiesta;
- un PED unisce ambiente, produzione e consumo sostenibili e mobilità per ridurre il consumo di energia e le emissioni di gas serra e creare valore aggiunto e incentivi per il consumatore;
- un PED fa un uso ottimale di elementi come materiali avanzati, RES locale e altre fonti di energia a basse emissioni di carbonio, stoccaggio locale, reti energetiche intelligenti, demand/response, gestione energetica innovativa;
- un PED dovrebbe offrire una vita accessibile per gli abitanti;
- i PED saranno potranno comprendere sia distretti di recente costruzione che di retrofit, con un mix di entrambi.

Appare dunque evidente che anche nel caso dei PED le Energy Communities potrebbero diventare strategiche per il perseguimento degli obiettivi propri.

Al fine di un posizionamento internazionale del tema delle Energy Communities occorre monitorare lo sviluppo che gli IWGs individuati proporranno nel corso dei prossimi mesi.

Per esempio l'IWG 3.2 ha avviato un lavoro di ricognizione sul tema dei PED (PED Booklet), lavoro a cui ENEA-DTE-SEN partecipa attivamente, con l'idea di mappare le caratteristiche dei PED già realizzati (essenzialmente un paio nei paesi scandinavi), in fase di implementazione (15) o in fase di pianificazione (7 tra cui 2 italiani: Parma e Trento) oppure che hanno avviato il processo di transizione verso il modello del PED trovandosi così o nella in operation phase (11 di cui 1 in Italia: Milano) in implementation phase (14 di cui 2 italiane: Bolzano e Firenze), in planning stage (6 di cui 1 italiana: Lecce).
L'IWG 3.1 invece definendo ad esempio i criteri per l'interoperabilità e la condivisione dei dati andrà puntualmente verificata per allineare le caratteristiche dei nostri prodotti al contesto europeo.
Per il prossimo report probabilmente vi sarà una maturità di contenti tale che potremo strutturare un report esaustivo sul tema.

4. TRANSIZIONE VERSO IL NUOVO SISTEMA ENERGETICO. PRINCIPALI DRIVERS.

4.1 Digitalization, Blockchain, Internet of value

La digitalizzazione è tra i protagonisti del cambiamento in atto sulla filiera dell'energia elettrica e con la blockchain, costituisce uno tra i fattori abilitanti al raggiungimento degli obiettivi proposti dal recente Piano Nazionale Integrato Energia e Clima (PNIEC). Infatti, la diffusione della generazione distribuita con le Fonti Energetiche Rinnovabili (FER) ed il proliferare di valide soluzioni di storage sono le promotrici della transizione in atto nel sistema elettrico e la blockchain ha un ruolo propulsivo nell'ambito di questo cambiamento.

I dati forniti da Terna registrano che il fabbisogno di energia elettrica nazionale nel 2018 è stato di 321,4 TWh (+0,3% sul 2017) coperto per l'86,3% dalla produzione nazionale (277,5 TWh: -1,9% sul 2017) e per la restante quota da importazioni nette dall'estero (43,9 TWh: +16,3% sul 2017). La produzione nazionale lorda, pari a 289,7 TWh, è stata coperta per il 33,5% dalle rinnovabili (+25,7% sul 2017) [7]. La potenza attualmente disponibile delle rinnovabili risulta pari a 54,1 GW lordi e circa 53 GW netti. L'evoluzione tecnologica inevitabilmente determina cambiamenti nella società offrendo migliori condizioni di vita che si traducono in un continuo aumento della domanda di energia che a livello globale si stima avrà un aumento del 18% al 2030. Perché questa vocazione energivora del progresso non continui a generare processi irreversibili e deleteri per l'ambiente e per l'uomo occorre che si rivedano, in termini di sostenibilità, le soluzioni atte a produrre energia da destinare al fabbisogno energetico della società. La digitalizzazione dell'energia elettrica coinvolgendo tutti gli attori operanti lungo la filiera, rappresenta un abilitatore di nuovi prodotti e servizi caratterizzanti le reti, i sistemi di produzione e di consumo dell'energia. L'evoluzione tecnologica e normativa (in termini anche di comunità energetiche) accelereranno l'attuale ridisegno del mercato elettrico favorendo: il raggiungimento dell'**obiettivo FER del PNIEC di arrivare per le rinnovabili ad un incremento complessivo della generazione al 2030 di 73TWh** e più in generale la gestione sempre più smart dei flussi energetici (con il passaggio della produzione elettrica da un modello centralizzato ad un modello distribuito; cambiando il flusso della rete elettrica da unidirezionale a bidirezionale; trasformando il concetto stesso di consumatore di energia in quello di *prosumer*). La **blockchain**, parte integrante dell'evoluzione tecnologica e digitale in corso, è un data base distribuito fatto di blocchi di dati che memorizzano transazioni. Un registro delle transazioni dove i dati non sono memorizzati su un solo computer, ma su più nodi collegati tra loro via Internet, attraverso un'applicazione dedicata che permette di interfacciarsi con la "catena". Per essere consolidato all'interno di un blocco, ogni dato, e successivamente ogni blocco viene sottoposto a un processo di validazione basato su algoritmi di consenso. I sistemi blockchain consentono quindi di effettuare delle transazioni di asset univoci che possono essere criptovalute o token, tali asset possono essere nativamente digitali o fisici con un corrispettivo digitale (per ulteriori dettagli nelle definizioni si veda il capitolo 8 del presente rapporto). Questa tecnologia riesce a realizzare, quello che Ripple ha definito per primo, ***l'internet of value***. Il termine descrive Internet come uno spazio di trasferimento e di memorizzazione di qualsiasi valore immaginabile (denaro, diritti, titoli). La tecnologia Blockchain, basata su protocolli di consenso che eliminano il problema della fiducia, può rendere l'Internet dei valori una realtà, perché garantisce che i valori possano essere memorizzati e condivisi in modo sicuro, decentralizzato, efficiente e trasparente. Questa tecnologia per le sue caratteristiche intrinseche di disintermediazione, decentralizzazione, trasparenza, immutabilità, tracciabilità, programmabilità e digitalizzazione [8]può avere molteplici applicazioni al settore energy (si veda capitolo 5) con un ruolo propulsivo nel processo di transizione

del sistema energetico in un sistema decentralizzato, decarbonizzato e digitalizzato. Qui ci limiteremo ad un rapido excursus delle possibili applicazioni, lasciando l'analisi di maggior dettaglio al capitolo 5. La blockchain può essere utilizzata come soluzione IT per elaborare transazioni energetiche in modo efficiente e ad un costo ridotto senza necessità di un tradizionale organo di controllo centrale, come una ESCO, per garantire l'affidabilità del processo. Ogni transazione energetica viene registrata e memorizzata dalla blockchain su tutti i nodi che formano la sua rete (ad esempio una microgrid). Tutti i partecipanti sono informati di ogni transazione in tempo reale e dai loro computer controllano gli altri. L'elaborazione delle transazioni può anche essere automatizzata e resa ancora più efficiente e meno costosa grazie all'implementazione di un sistema di smart contract e, in una fase futura, utilizzando applicazioni autonome decentrate (Dapps) che non richiedono nessun intervento umano. La tecnologia permette di registrare e memorizzare tutte i flussi di energia e transazioni in modo distribuito e sicuro. Il registro distribuito può essere utilizzato per documentare in qualsiasi momento quali utenti hanno energia, quanta energia hanno prodotto, venduto o acquistato e l'evoluzione del loro portafoglio energetico. Tutto ciò avviene in modo trasparente e ogni stakeholder - ESCO, gestori del sistema di distribuzione, gestori di reti di trasmissione, organizzazioni comunitarie, autorità locali – hanno accesso in qualsiasi momento al registro indelebile di dati a prova di falsificazione. Si può quindi creare una registrazione di tutte le transazioni (prova dell'esistenza), essenziale dal punto di vista giuridico e giudiziario in caso di controversie. Questa capacità di documentazione delle catene a blocchi potrebbe cambiare le pratiche di certificazione energetica e di verifica, soprattutto quando applicata alle garanzie di origine delle fonti rinnovabili ed ai sistemi di scambio delle quote di emissioni. La blockchain può essere utilizzata per il pagamento della bolletta energetica con criptovaluta (come Bitcoin o Ether). I contratti intelligenti potrebbero facilitare l'attuazione di un meccanismo automatizzato e flessibile in grado di remunerare i *prosumer* in tempo reale ed adeguare la domanda di energia, quando necessario, all'offerta. Questo meccanismo renderebbe anche possibile i micro-pagamenti dell'energia, a costi generali praticamente nulli e a intervalli di tempo molto brevi (ad esempio ogni 15 minuti). In un contesto locale, nell'ambito di una partnership tra una comunità energetica ed enti locali: l'energia fornita agli enti locali dalla comunità energetica potrebbe essere pagata con una criptovaluta comunitaria minata dalla stessa autorità locale e fatta circolare nel contesto locale per accrescere gli scambi e favorire l'inclusione sociale. Un'altra possibile applicazione sarebbe quella di utilizzare la tecnologia per realizzare in un mercato locale o regionale dell'energia on-line. Una piattaforma blockchain on-line gestita da un ente locale elencherebbe i vari produttori locali di energia e le loro offerte, quindi aiuterebbe i cittadini a scegliere un mix energetico conveniente e pulito. Questa applicazione contribuirebbe a mantenere il valore economico dell'energia all'interno del territorio locale, dato che tutte le transazioni avrebbero avuto luogo a livello locale o regionale. La blockchain può essere utilizzata anche per le transazioni peer-to-peer e l'autoconsumo collettivo in un sistema decentralizzato. Altre applicazioni prevedono il trading automatizzato e disintermediato di certificati di energia rinnovabile e l'impiego dei veicoli elettrici per la stabilizzazione della rete. Da questi esempi emerge chiaramente il potenziale della tecnologia nel processo di trasformazione del sistema energetico promettendone di risolvere nel complesso delle sue applicazioni il noto trilemma di [9]: ridurre i costi ottimizzando i processi energetici, migliorare la sicurezza energetica in termini di sicurezza informatica, agire come una tecnologia di supporto che potrebbe migliorare la sicurezza dell'approvvigionamento e infine promuovere la sostenibilità facilitando la generazione rinnovabile e soluzioni a basse emissioni di carbonio.

4.2 Il paradigma delle Energy Community

Le recenti definizioni comunitarie di "Renewable Energy Community"(REC) e di "Citizen Energy Community"(CEC) introdotte rispettivamente dalle direttive UE 2018/2001 sulla promozione delle energie rinnovabili (REDII) e la UE 2019/944 sulle norme che regolano il funzionamento del mercato elettrico (EMD II) richiamano una forma partecipativa collettiva ad un progetto di sviluppo di produzione ed uso di energia da fonti rinnovabili o da altre fonti secondo principi di efficienza utilizzando forme di autoconsumo e gestione smart delle reti di distribuzione. Le definizioni di comunità di energia rinnovabile contengono in sé molti elementi che consentono di configurare tali soggetti. Tra le varie cose, rappresentano elementi importanti da indagare sia il **principio della prossimità fisica dei membri**, che quelli della **definizione e misura dei benefici ambientali, economici, sociali e finanziari** che possono derivare dalle azioni di risparmio ed efficientamento energetico. L'introduzione della definizione di comunità energetica di cittadini (CEC), in particolare, poggia sul fatto che, grazie alle tecnologie dell'energia distribuita e alla responsabilizzazione dei consumatori, le iniziative collettive sono divenute un modo efficace ed economicamente efficiente di rispondere ai bisogni e alle aspettative dei cittadini riguardo alle fonti energetiche, ai servizi e alla partecipazione locale (si veda a tale proposito il RdS/PTR(2019)/011 prodotto dal Politecnico di Milano).

Una **Energy Community (EC)** può essere costituita da un piccolo numero di famiglie nelle immediate vicinanze, ma può anche comprendere fino ad un centinaio di migliaia di famiglie ed imprese, coprendo un'ampia area geografica. I singoli membri di questa struttura possono essere liberamente o fortemente correlati tra loro, e possono provenire da una vasta gamma di gruppi socio-economici con interessi ed obiettivi diversi in ambito economico, sociale e ambientale. Tuttavia, essi condivideranno obiettivi comuni specifici come membri della comunità energetica, che possono includere la promozione di una produzione energetica più pulita e sostenibile, l'autosufficienza, il risparmio nella produzione e consumo di energia, la partecipazione al mercato dell'energia, la rivitalizzazione dell'economia locale. I membri delle EC possono svolgere ruoli diversi, come produttori, consumatori, *prosumer*, investitori, proprietari di beni o una combinazione di questi. Possono contribuire alle EC sotto forma di investimenti finanziari, offerta di energia elettrica, riduzione della domanda, attrezzature fisiche quali impianti di generazione e stoccaggio delle batterie, o semplicemente consumare energia elettrica. I residenti e le imprese di una comunità possono avere i propri impianti fotovoltaici, impianti di cogenerazione, stoccaggio batterie, strutture per la gestione della domanda o, agire come investitori in parchi eolici, e parchi solari che possono essere in comproprietà e gestiti da terzi o dai network di distribuzione locale.

Le questioni tecnologiche rappresentano solo una parte della discussione sulle comunità energetiche. Il progressivo coinvolgimento delle comunità locali nella proprietà, nel processo decisionale e nell'organizzazione degli impianti di produzione di energia rappresenta un'innovazione sociale che congiuntamente alle innovazioni tecnologiche del settore fa intravedere la nascita di un nuovo sistema socio-energetico basato sulla generazione distribuita da rinnovabili [10]. L'energia è dunque un ambito che pone sempre più spesso questioni di carattere sociale. Le nuove tecnologie per la produzione distribuita di energia stanno raggiungendo un livello di maturità che lascia presagire un ampio sviluppo di iniziative dal basso nella costituzione di "sistemi energetici locali", formule che giocano un ruolo cruciale nella ridiscussione dell'intero sistema infrastrutturale e del mercato dell'energia. Se questo tema è ampiamente trattato dal punto di vista tecnologico e ingegneristico, il dibattito sulle caratteristiche delle organizzazioni che dovranno guidare le iniziative locali necessità di approfondimenti.

In tutto il mondo sono emerse varie forme di EC, queste includono progetti energetici su scala comunitaria, centrali elettriche virtuali, piattaforme di trading peer-to-peer (P2P), microgrid comunitarie e sistemi comunitari integrati di energia (ICEM).
Nel capitolo 5 si passeranno in rassegna le tipologie e categorie di comunità energetiche individuate in letteratura, saranno forniti esempi di casi concreti al fine di evidenziarne in particolar modo gli aspetti di natura sociale: la proprietà degli *asset*, *governance*, livello di coesione, la prossimità fisica dei membri, livello di innovazione tecnologica e sociale.

4.3 La sharing economy nell'era della blockchain

La transizione del sistema energetico passa anche attraverso il paradigma della sharing economy. Le comunità energetiche, come già evidenziato, oltre ad essere un insieme di utenze che decidono di effettuare scelte condivise per soddisfare il proprio fabbisogno energetico costituiscono un nucleo di famiglie ed imprese di cui è necessario considerare anche l'aspetto sociale. Rafforzare la dimensione sociale di una comunità energetica vuol dire accrescere il senso di appartenenza dei suoi membri mediante la reciprocità ed il legame emozionale e questo passa attraverso la condivisione di obiettivi più ampi di natura sociale, ambientale, economica oltreché energetica che possono essere perseguiti attraverso modelli di economia collaborativa o sharing economy. I principi cardine della sharing economy sono ravvisabile nella reciprocità, nella fiducia e nel consenso. La reciprocità diretta è tipica delle reti amicali e di buon vicinato: tra due amici o due buoni vicini si fanno dei trasferimenti, nel senso che a volte si dà e a volte si riceve, ma mai si pretende di dare e ricevere simultaneamente. Lo statuto dei servigi, saperi, oggetti trasferiti è quello del 'dono', che secondo Marcel Mauss [11] è regolato da un ciclo di tre vincoli: di 'dare', di 'ricevere' e di 'rendere'. Regolarmente avviene che chi ha dato desideri 'ricevere' e chi ha ricevuto voglia 'dare', ma non si completa mai il ciclo, perché le caratteristiche del 'rendere ' sono volutamente imprecisate. Di conseguenza non esiste nessuna garanzia sul rendere, pertanto il trasferimento si poggia sulla nozione di **fiducia** [12].Tra donante e ricevente si instaura una 'simmetria bilaterale'. L'azione di trasferire, sia quella del dare che quella del ricevere, suscita un tipo d'emozione, che lega il donante e il ricevente in una relazione d'amicizia o di buon vicinato. La sorgente del legame emozionale è nell'individuo stesso, perciò ogni trasferimento per compiersi necessita del **consenso** dei due protagonisti, l'uno volendo dare, l'altro volendo ricevere.
Una comunità energetica forte di questi principi ha una maggiore potenzialità nell'innescare i cambiamenti necessari nel ruolo degli attori tradizionali, nei modelli di business che caratterizzano il settore energetico e nel quadro normativo ed istituzionale che lo governa.
Secondo Botsman e Rogers [13]un modello economico basato sulla collaborazione e sulla condivisione di asset, spazi, competenze si può articolare su tre dimensioni:

- il **consumo collaborativo**: in cui la gente scambia, condivide, redistribuisce prodotti di cui non ha bisogno e che non utilizza con continuità, o paga per avervi accesso piuttosto che acquisirne la proprietà (es: il car sharing);

- la **produzione collaborativa**: per cui reti di individui collaborano per la progettazione/design, la produzione e la distribuzione di beni e servizi;

- **l'apprendimento collaborativo**: corsi aperti o forme di condivisione e agglomerazione di conoscenze in un'ottica crowd (Wikipedia o Future Learn);

- la **finanza collaborativa**: raccolte fondi in cui la gente può supportare la creazione di progetti, imprese, iniziative benefiche (crowdfunding) gratuitamente o ricevendo una forma di ricompensa simbolica o tangibile, ma troviamo anche altre forme come i prestiti tra pari o le monete comunitarie.

La sharing economy si propone come modello di economia innovativo perché:

- sostituisce un modello di produzione lineare di beni e servizi attraverso un modello circolare di produzione, distribuzione e fruizione basato sull'accesso all'*over-capacity* di un bene/servizio, che tradizionalmente è stata considerata come priva di valore, o semplice rifiuto, nello scambio tradizionale [14]è un modello basato sulla disintermediazione abilitata perlopiù da piattaforme digitali [15];

- si tratta di un paradigma che mira alla *re-embeddedness* dello scambio economico rilanciando il valore della reciprocità a lungo soccombente al modello dello scambio del mercato e alle sue logiche, sempre più centrate sul mero profitto e o su processi di estrazione di valore [16];

- si basa su un sistema ibrido tra produzione e consumo, abilitando la capacità creative e generative dei cosiddetti *prosumer* [17].

Gli attuali modelli di sharing economy pur sembrando innovativi possono essere tuttavia considerati come una rivisitazione di vecchie idee necessarie per stare al passo con la complessità e la velocità di cambiamento che caratterizza la società attuale.
Nel corso dell'esistenza si acquisisce presto la consapevolezza che la cooperazione migliora la qualità della nostra vita e spesso prolunga la nostra sopravvivenza. La **cooperazione** è stata apprezzata nella storia dalle civiltà che hanno intuito per prime il potenziale della naturale inclinazione degli individui a lavorare insieme per il reciproco vantaggio ed il benessere comune fino alla sua graduale trasformazione nel sistema del baratto. Attraverso semplici baratti, le persone potevano scambiare oggetti di valore per ottenere le cose di cui avevano bisogno. Finché le richieste rimanevano relativamente semplici da soddisfare, era facile generare una "coincidenza di bisogni".
Nell'era di internet la sharing economy si realizza attraverso transazioni peer to peer abilitate da una piattaforma digitale che disciplina la contrattazione tra le parti, appropriandosi di una parte del valore generato. Le relazioni sono perlopiù transitorie e strumentali, mediate da sistemi fiduciari basati su rating reputazionali on line [18]. Il problema di questo modello di business è che il valore prodotto dai *prosumer* non si ridistribuisce equamente verso tutti quelli che hanno contribuito a crearlo; la maggior parte dei profitti, infatti, è catturata dai grandi intermediari che gestiscono le piattaforme.
La sharing economy grazie alla diffusione della **tecnologia blockchain**, in diversi settori tra cui quello energetico, può raggiungere il suo massimo potenziale. **La tecnologia essendo *trustless*** -il sistema di incentivi su cui sono costruiti i protocolli di consenso della blockchain eliminano il problema della fiducia garantendo l'onestà e l'integrità tra i nodi del network e scoraggiando comportamenti malevoli-**elimina di fatto la necessità di una piattaforma gestita da un'entità centrale per la condivisione degli assets tangibili e intangibili con una riduzione dei costi delle transazioni ed un controllo da parte degli utenti dei propri dati.**
Nell'ambito di una comunità energetica l'adozione di modelli di economia collaborativa basati sulla tecnologia blockchain possono riguardare sia il vettore energetico che la dimensione sociale della comunità nonché una loro possibile intersezione.

Vedremo nel dettaglio come le piattaforme di trading peer to peer sono un ottimo esempio di applicazione del modello di sharing economy al vettore energetico nell'ambito di una microgrid consentendo in maniera disintermediata al prosumer di vendere l'energia autoprodotta e non consumata al proprio vicino in cambio di token. Per quanto riguarda la dimensione sociale della community uno strumento di economia e finanza collaborativa che ha ripreso a diffondersi a livello internazionale a seguito della più recente crisi finanziaria è quello della valuta comunitaria, o valuta complementare che si propone come obiettivo quello di combattere la penuria di liquidità in aree depresse favorendo l'incontro tra i bisogni insoddisfatti e le risorse inutilizzate a livello locale favorendo così la crescita degli scambi commerciali e l'inclusione sociale tra i membri. Tra i vari sistemi di valuta complementare presenti saranno di seguito esaminati i sistemi Local Exchange Systems (LETS) che per le loro caratteristiche meglio si adattano alla possibilità di essere gestiti tramite una piattaforma blockchain.

4.4 Il ruolo del crowdsourcing in ambito energy

Il termine crowdsourcing si riferisce ad un insieme di attività in cui gli esseri umani (prevalentemente i cittadini) vengono utilizzati per contribuire alla realizzazione di un obiettivo o migliorare l'efficienza di una attività senza che detengano una competenza specifica o strumenti particolari. La gestione dei servizi essenziali, tra cui quelli energivori e la fornitura stessa dell'energia, per la loro natura, possono beneficiare intensamente dell'apporto umano, che in questa ottica, può contribuire inconsapevolmente o spontaneamente al processo di trasformazione del sistema energetico ovvero senza un beneficio specifico diretto o comunque senza incidere significativamente sulla vita stessa del cittadino.

Il miglioramento dei servizi essenziali e conseguentemente la gestione delle infrastrutture, necessita una costante e continua valutazione della qualità dei servizi erogati. Gli operatori dispongono di strumenti specifici che consentono di quantificare indicatori oggettivi per la definizione della Qualità del Servizio (Quality of Service, QoS). Accanto a questi indicatori oggettivi (come ad esempio l'energia erogata o la differenza tra l'energia richiesta e quella erogata) è molto importante disporre di altri indicatori sulla qualità dei servizi percepita dagli utenti (perceived Quality of Service, pQoS). Inoltre, la rete di misurazione di parametri oggettivi può essere incompleta o non essere in grado di misurare tutti gli aspetti percepiti dagli utenti. Infine disporre di riscontri continui da parte dei cittadini per valutare la qualità percepita del servizio può orientare i futuri investimenti e migliorare l'allocazione delle risorse fisiche ed umane.

Il recente sviluppo delle tecnologie di comunicazione e dei modelli comportamentali della società ha portato ad una intensificazione delle comunicazioni tra i cittadini in generale ed in particolare tra gli utenti dei servizi energivori e non. Alla tradizionale comunicazione di diffusione in cui tramite i network ufficiali i responsabili delle infrastrutture comunicavano agli utenti le informazioni pertinenti nel tempo si sono aggiunte altre forme di comunicazione in verso opposto. Le comunicazioni dei disservizi da parte degli utenti sono ricevute sia da soggetti umani che automatizzati in grado di recepirle in modalità anche interattive. In generale gli utenti non amano questo tipo di comunicazione in cui non si riceve una risposta immediata e concreta in tempi brevi e pertanto le opinioni degli utenti vengono espresse raramente tramite i canali dedicati dai gestori delle infrastrutture. Negli ultimi anni lo sviluppo intensivo dei social network ha condotto gli utenti ad esternare le proprie considerazioni sui social network in cui la risposta degli altri utenti è molto rapida e spesso estesa. L'intensità della risposta dei sistemi sociali è una delle principali motivazioni per il coinvolgimento degli utenti nella valutazione della percezione dei servizi.

La valutazione della percezione della qualità di servizio da parte degli gli utenti può avvenire anche in maniera stimolata attuando delle campagne specifiche di indagine conoscitiva; tipicamente

condotte tramite telefono, che vengono maldigerite dagli utenti e contribuiscono esse stesse ad una valutazione negativa della gestione del servizio erogato. Invece l'acquisizione delle esternazioni spontanee degli utenti consente una maggiore genuinità delle stesse senza gli effetti negativi delle campagne conoscitive.
Essenzialmente sulla rete sono disponibili due grandi fonti di informazione legata all'erogazione dei servizi essenziali: i media qualificati e i social network. Nel primo caso l'analisi di un evento indesiderato, di una contingenza o di un malfunzionamento è mediata dalla valutazione di un giornalista; nel secondo caso invece il campione è selezionato solo in base alla tendenza all'attività sui social dei diversi soggetti. Entrambe le sorgenti sono pregiudizievoli (tecnicamente si dice che rappresentano campioni con "bias") per molteplici ragioni. I giornalisti spesso detengono una competenza specifica, ma possono subire l'influenza dei loro editori e possono perdere l'obiettività per altri fattori legati alle sensibilità specifiche o al desiderio di colpire l'immaginario collettivo catturando l'attenzione del pubblico. Viceversa, gli utenti dei social network sono in genere poco competenti e (con significative eccezioni) rappresentano un campione abbastanza variegato e casuale. Anche in questo caso vi sono dei pregiudizi dovuti alla diversa propensione degli utenti alle esternazioni e all'attuazione di vere e proprie campagne di manipolazione di soggetti portatori di interessi politici o economici. Purtroppo le regole per l'accesso ad alcuni social network (anche in conseguenza del regolamento europeo GDPR Data Privacy Regulation) non consentono di acquisire in forma massiva le informazioni e quindi non tutti i social network si prestano ad essere analizzati.

L'attività denominata ECListener si innesta in questa cornice ed ha per finalità l'acquisizione delle informazioni fornite spontaneamente da semplici utenti e giornalisti professionisti sui social network e nelle testate giornalistiche più accreditate. ECListener (Energy Community Listener) si inserisce nell'ambito di un progetto più ampio denominato "Obserbot" (dalla crasi di Observe e Robot) che mira ad osservare in maniera automatizzata ciò che i cittadini spontaneamente collocano sulla rete discutendo su tutti i servizi essenziali. Nella versione specifica ECListener si focalizza sulle notizie giornalistiche dei principali media e le esternazioni su Twitter che per sua natura è una piattaforma Social sistema aperta. Il monitoraggio di questi sistemi associato all'acquisizione delle informazioni sulla piattaforma social della Energy Community consentirà una valutazione dell'apprezzamento degli utenti dei servizi forniti dalla Energy Community e più in generale sul gradimento dei servizi essenziali (illuminazione, fornitura domestica, semafori etc) legati all'uso dell'energia elettrica.
ECListener è un lavoro in continua evoluzione che si basa sugli algoritmi già sviluppati per la piattaforma Obserbot che, nella sua forma più ampia, si occupa di reperire le informazioni fornite da utenti e giornalisti sui malfunzionamenti di tutte le infrastrutture, non solo quelle energetiche. Per questa ragione non è possibile utilizzare automaticamente le informazioni già disponibili dalle campagne precedenti, ma occorre adattare gli algoritmi utilizzati alle esternazioni spontanee e agli articoli relativi alla "Comunità Energetica". In altre parole è necessario epurare l'insieme dei dati acquisiti da tutte le informazioni non pertinenti. Invece, le informazioni reperite direttamente sul bus della piattaforma Social della Energy Community nascono già in formato "Urban Data Format" che, usando le sintassi json o xml, consente di specificare gli scambi previsti dai negoziati tra i vari utenti della Energy Community. Il collettore (collector) di ECListener acquisirà tutti i dati trasmessi sul bus e ne valuterà le statistiche di successo per monitorare l'intensità dell'uso della piattaforma e il gradimento della stessa.

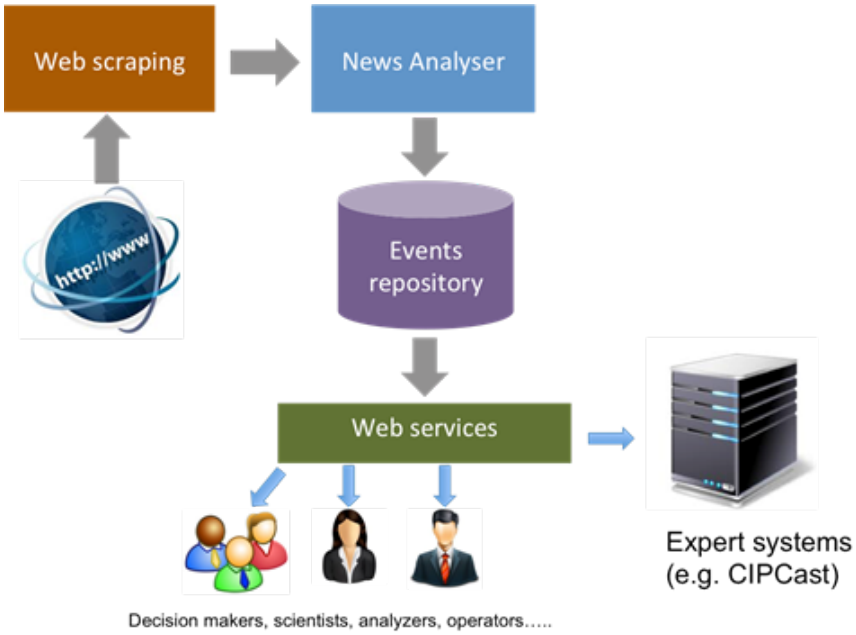

Figura 1. La struttura a blocchi di mediabot

ECListener si comporrà di un "web crawler" cioè un programma che spazia un insieme predefinito di nodi della rete e scarica gli articoli pertinenti e un secondo agente che riceve i twitter specifici utilizzando gli applicativi (API) forniti dal gestore di Twitter.
Il materiale acquisito tramite questi due distinti canali viene elaborato in maniera diversa data la diversa natura dei testi. In entrambi i casi l'elaborazione dell'informazione acquisita avviene in maniera totalmente automatizzata tramite un insieme di codici interoperabili attualmente eseguiti su una stessa piattaforma. Per semplicità espositiva chiameremo "mediabot" l'insieme dei codici che elabora le notizie e "tweetbot" l'insieme dei codici che elabora i tweets.
Allo stato attuale entrambi i sistemi sono eseguiti su una piattaforma Debian fisicamente collocata nella sala calcolo C59 del CR ENEA Casaccia, ma è pianificata una più ampia allocazione di risorse di calcolo. In particolare è in fase di sperimentazione una piattaforma ibrida basata su kubernetes che garantirà una maggiore resilienza del servizio.
Le notizie provenienti dalle testate giornalistiche vengono scaricate dal crawler in formato html indicizzato con la data e il sito di provenienza e vengono memorizzate su un database relazionale attualmente gestito tramite postgreSQL. I dati vengono sottoposti ad un primo "filtro di pertinenza" che tramite un'analisi semantica automatizzata del testo individua quali sezioni della sorgente html trattano la tematica di interesse. Gli articoli che passano il vaglio di pertinenza vengono ulteriormente classificati per individuare quali infrastrutture sono coinvolte, quali tipi di malfunzionamenti sono osservati (se ci sono), la localizzazione degli eventi e la loro collocazione temporale. Queste informazioni vengono aggiunte al database relazionale. Infine una interfaccia web consente agli utenti autorizzati di acquisire le statistiche relative agli eventi indesiderati. La Figura 1 rappresenta lo schema a blocchi dell'architettura di mediabot.
L'analisi del flusso di dati di Twitter (Figura 2) avviene in modalità simili, ma l'acquisizione è mediata dalle API di Twitter e dai loro protocolli di ricerca basati sull'occorrenza di alcune parole chiave fornite da chi esegue l'acquisizione. L'affinamento dell'insieme delle parole chiave scelte per la ricerca dei tweets svolge un ruolo cruciale; infatti, un insieme troppo ampia porta ad un eccessivo numero di "falsi postivi" (tweets che parlano d'altro) mentre un insieme troppo ristretto porta ad una drastica riduzione del numero dei tweets pertinenti raccolti. I tweets raccolti rappresentano un

flusso continuo di dati in formato json (JavaScript Object Notation) che vengono gestiti dal software Apache-Kafka. Anche su questo flusso di dati vengono eseguiti il filtro di pertinenza e gli analizzatori tassonomici per conservare solo i tweets significativi ed indicizzarli tramite le categorie legate ai servizi ed il tipo di malfunzionamento. Anche in questo caso viene creato un data-base ed il flusso di dati può essere direttamente osservato tramite una interfaccia web (distinta dalla precedente). La stessa interfaccia consente anche la visualizzazione degli istogrammi di frequenza del numero di tweet sulle diverse tematiche e le statistiche sui servizi coinvolti nei diversi malfunzionamenti.
Allo stato attuale la classificazione dei tweet e delle notizie avviene tramite delle euristiche (i cui algoritmi sono al momento coperti dal vincolo di riservatezza) che consentono elevati livelli di efficienza di raccolta e potere di reiezione. Le prestazioni (di media-bot) sono molto buone per le notizie giornalistiche in cui i falsi positivi sono solo qualche percento; ma insufficienti per i tweet che, essendo scritti in una forma meno strutturata, sono più ostici da classificare.

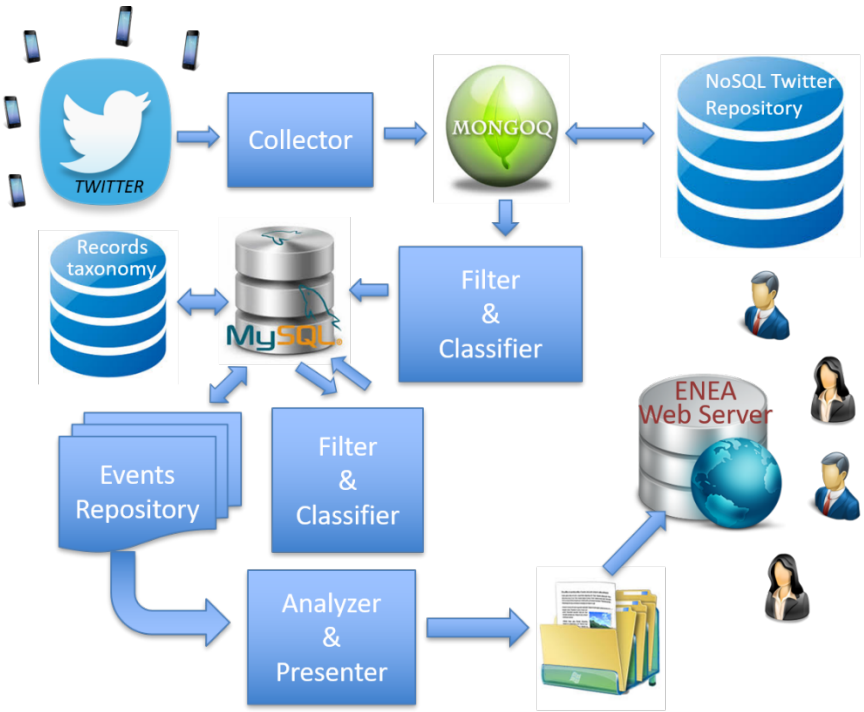

Figura 2. La struttura a blocchi di tweetbot

Obserbot sarà utilizzato per selezionare le notizie pertinenti alla comunità demo del progetto e verrà valutato il gradimento degli utenti ed eventuali malfunzionamenti.

4.5 Concept Enea: Energy Community basata sullo sharing di servizi energetico-sociali

Il nuovo modello di Energy Community che l'ENEA vuole sviluppare, tiene conto dell'impatto potenziale della digitalizzazione e dei modelli di economia collaborativa sul processo di transizione energetica e prende spunto dall'analisi congiunta di casi di studio di comunità energetiche e di esperienze di valute comunitarie digitali, a livello internazionale. In particolare, si vuole proporre un modello di microgrid virtuale peer to peer, basata sull'impiego della tecnologia blockchain, che dovrà abilitare la reciprocità degli scambi tra prosumer e consumatori locali in ambito sociale oltreché energetico.
La Figura 3 vuole rappresentare la centralità della dimensione sociale nella Energy Community proposta e contrapporre il nuovo modello di economia circolare di generazione da fonte rinnovabile distribuita a quello tradizionale, lineare e centralizzato di generazione da fonte non rinnovabile. La

tecnologia considerata abilitante per attivare gli scambi sociali ed energetici è la blockchain, indicata nella figura dal simbolo di Ethereum posizionato in alto nell'immagine.

Figura 3. Il nuovo concetto di Energy Community

La Energy Community, coerentemente con la direttiva EMD II, attribuisce un ruolo chiave al consumatore/cittadino nel processo di transizione energetica sia come prosumer, a cui garantire adeguati strumenti tecnologici per la partecipazione diretta al mercato elettrico, sia come consumatore vulnerabile, in condizioni di povertà energetica, verso il quale identificare strumenti idonei di sostegno (si veda capitolo 3). L'idea di base è quella di fare riferimento al quadro normativo della Citizen Energy Community, il che vuol dire:

- focalizzarsi sul vettore elettrico;
- ammettere la partecipazione di cittadini, piccole imprese ed autorità locali al progetto;
- avere come finalità principale il raggiungimento di obiettivi sociali economici ed ambientali.

In merito a questo ultimo aspetto si evidenzia la necessità di costruire una comunità energetica con un perimetro territoriale definito e circoscritto anche se questo requisito non è stringente nella definizione delle CEC. Infatti, la prossimità fisica dei membri risulta, a nostro avviso, un elemento fondamentale per sviluppare in maniera adeguata la dimensione sociale della comunità, funzionale alla corretta implementazione di un modello di business collaborativo. La crescita territoriale potrà essere garantita dalla creazione di comunità di comunità, facendo uso di un modello aperto ed integrante delle differenti entità. Si potrà quindi valutare l'applicazione del modello proposto a comunità energetiche che rientrano nel perimetro più ampio delle Renewable Energy Community, come ad esempio le Microgrid fisiche e gli Integrated Community Energy System (ICES).

In questo processo di transizione la principale tecnologia abilitante a gestire scambi di servizi energetici e sociali è la blockchain.

Da un punto di vista sociale la piattaforma blockchain deve gestire l'emissione e la circolazione di una Community Inclusive Currency (CIC) ovvero una valuta comunitaria digitale appartenente al sistema valutario complementare, attualmente più evoluto, noto come **Local Exchange Trade System (LETS)** (si veda il capitolo 7 per una descrizione di dettaglio). La CIC avrà la funzione di premiare la messa a disposizione da parte dei partecipanti alla comunità di competenze e tempo per erogare servizi di assistenza sanitaria, babysitting, co-learning e servizi di natura ecologica,

riscattabili sotto forma di sconti presso gli operatori commerciali aderenti all'iniziativa o trasferibili come "titoli di credito" per ottenere altre prestazioni. La registrazione su blockchain delle prestazioni erogate nel tempo permetterà di costruire un database certificato di CV sociali dei membri della community a disposizione di aziende e centri per l'impiego. Questo sistema valutario complementare, che meglio di altri si presta ad essere gestito mediante la tecnologia blockchain, favorisce l'incontro tra i bisogni insoddisfatti (assistenza di anziani, disabili e bambini, riciclo e riuso di materiali, servizi di pulizia di spazi pubblici, ripetizioni, car sharing) e le risorse inutilizzate della community (disoccupati, pensionati, persone affette da disabilità ma anche ad esempio posti vuoti al ristorante, cinema o teatro) risolvendo il problema della penuria di liquidità in aree depresse ad alto tasso di disoccupazione.

Per sviluppare un progetto di valuta comunitaria è necessario creare un **gruppo di supporto** che dovrebbe comprendere: il gestore della piattaforma, la cooperativa energetica, le associazioni di volontariato, centri di assistenza per anziani e disabili, centri per l'impiego, circoli culturali, operatori commerciali ed imprese.

In una prima fase, da un punto di vista energetico la piattaforma abiliterà, utilizzando la tecnologia blockchain, lo scambio di energia elettrica prodotta mediante impianti di energia da fonte rinnovabile tra le utenze comunitarie interconnesse fornendo un servizio di intermediazione tra domanda ed offerta; in una seconda fase gestirà il demand/response, consentendo ai membri della community di accettare che alcuni dei loro apparecchi siano accesi o spenti dal gestore di rete o da soggetti aggregatori per un migliore equilibrio tra domanda ed offerta di energia. In questo caso la criptovaluta comunitaria servirà a remunerare l'energia pulita autoprodotta e non consumata, messa a disposizione dal prosumer e la flessibilità energetica delle utenze. La piattaforma blockchain dovrà svolgere anche la funzione di registro dei dati relativi alla produzione, al consumo e al trading di energia al fine di una loro successiva analisi.

Ogni utenza dovrà essere dotata di smart meter 2G e sistema di monitoraggio del consumo (consumer) ed eventualmente produzione (prosumer), e storage (constormer) o entrambi (prostormer). Tramite gli smart meter i partecipanti possono eseguire transazioni ed avere il controllo su dispositivi e sullo storage.

Un ruolo importante è svolto dall'aggregatore che partecipa al mercato elettrico vendendo e comprando energia in caso di avanzo o disavanzo da parte della comunità.

Dalla intersezione delle due dimensioni – sociale ed energetica- scaturiscono due opportunità:

- impiegare la criptovaluta comunitaria come mezzo di scambio di servizi di natura diversa ed intracomunitaria;
- valorizzare al massimo l'impegno sociale e di comunità dei partecipanti attraverso il riconoscimento del tempo messo a disposizione degli altri;

con potenziali sinergie ottenibili in termini di aumento del potere di acquisto, volume degli scambi, riduzione della disoccupazione, risparmio energetico, coesione sociale, riduzione delle emissioni inquinanti.

In un bazar, differenti lingue e monete permettono comunque di effettuare scambi e accordi sugli oggetti o i servizi più differenti: la possibilità di utilizzare differenti monete digitali all'interno della stessa comunità e la creazione di metodi per lo scambio di queste monete tra di loro, permette di immaginare scenari di micro-economia locale molto differenti tra loro ma comunque coerenti con l'essenza della comunità energetica.

Inoltre, la criptovaluta comunitaria potrebbe essere lo strumento per interfacciare la comunità con attori esterni (es. aggregatori, investitori, …) qualora fosse possibile identificare un modello di scambio in moneta fiat.

Figura 4. Il funzionamento del nuovo modello di Energy Community

Dall'unione delle tematiche sociali ed energetiche nasce la visione di "comunità locali flessibili" in cui il cittadino è attore principale di un ampio ecosistema di servizi: in particolare il cittadino diventa un 'prosumer' di servizi, ovvero una entità in grado di produrre e consumare servizi per una comunità che sono gestiti in un portale dedicato (portale CEC) che di fatto rappresenta un 'market place digitale' in cui si incontrano domanda ed offerta di servizi energetico/sociali.
Nella figura 4 si schematizza il funzionamento della EC che prevede la presenza di tre entità:

- Un gestore della piattaforma blockchain;
- Il gruppo di supporto del progetto;
- Una Utility.

Da un punto di vista tecnologico, oltre alla blockchain, risulterà un fattore chiave per la integrazione dei servizi la realizzazione di un bus-dati comune per lo scambio delle informazioni sia all'interno della comunità che verso l'esterno. Infine, il portale CEC, per gestire adeguatamente ed efficientemente le grandi quantità di dati eterogenei della comunità, si appoggerà su una infrastruttura Big-Data dedicata.
La Figura 5 sintetizza i concetti fin qui espressi.

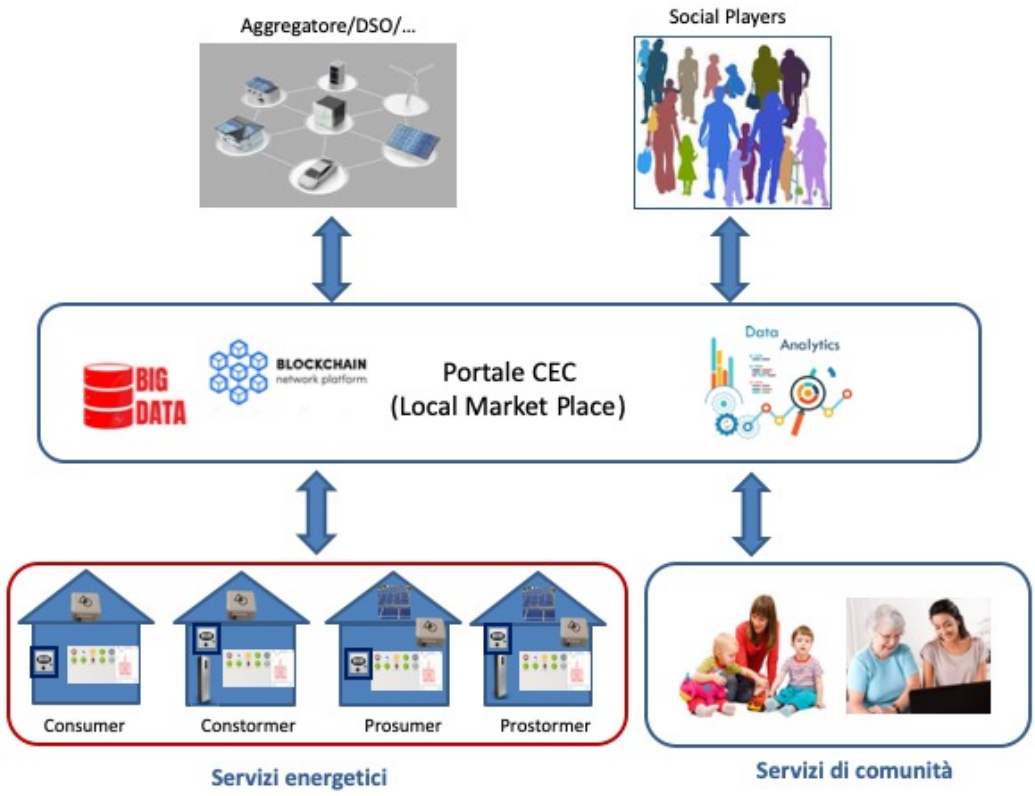

Figura 5: Schema a blocchi funzionale del modello CEC

In questo scenario il gestore della piattaforma blockchain, tipicamente un'organizzazione no-profit, sviluppa e gestisce la piattaforma occupandosi del mining della criptovaluta e della sua distribuzione presso il gruppo di supporto. La cooperativa energetica, le associazioni e le aziende del gruppo di supporto, che formano nel loro insieme la Energy Community in senso ampio, potranno acquistare con valuta fiat la valuta comunitaria oppure riceverla gratuitamente dal gestore. La valuta comunitaria sarà emessa dai soggetti partecipanti al gruppo di supporto come corrispettivo di azioni energetiche e sociali considerate virtuose sulla base delle linee guida fornite dal gestore della piattaforma peer to peer. La valuta potrà essere guadagnata in cambio di energia messa a disposizione della comunità e di servizi sociali erogati dai prosumer, e potrà essere spesa per ottenere sconti sull'acquisto di beni e servizi presso i punti vendita aderenti al progetto, per erogare bonus ai dipendenti delle aziende coinvolte, per opere di beneficienza, per l'acquisto di energia.
In Figura 6 viene rappresentata l'idea che la valuta principale della blockchain, facendo uso anche di valute secondarie, può essere utilizzata per convertire quello che viene fornito dalla comunità, come energia, flessibilità, virtuosismo energetico o tempo sociale in moneta fiat (€/$) oppure in energia o tempo sociale. Di particolare interesse per la i cittadini partecipanti alla comunità sono gli scambi Energia <=> tempo sociale, mentre le aziende potrebbero essere interessate maggiormente allo scambio Energia ⇔ €/$ più renumerativo di quello attuale.

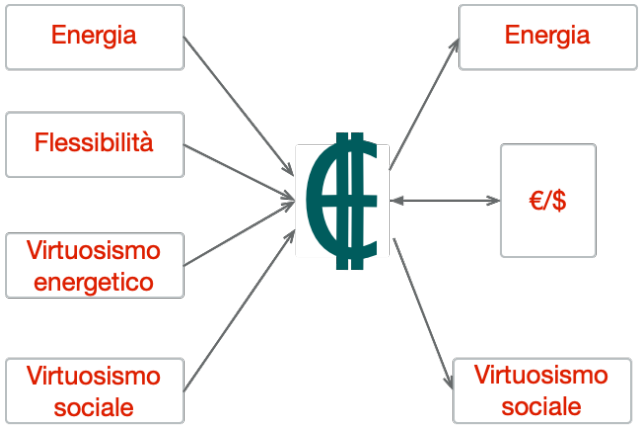

Figura 6. La valuta principale è usata per convertire differenti elementi in altri

Qui di seguito si vuole applicare il Business Model Canvas al concetto di Energy Community proposto, facendo riferimento al modello aggregato su 3 sezioni adottato dal Politecnico di Milano nel Rapporto RdS/PTR(2019)/011 e generalizzato ai nostri fini. Le 9 dimensioni del Canvas sono aggregate nel seguente modo:

- **Value proposition & customer interface**: che comprende la proposizione di valore (il pacchetto di prodotti e servizi che rappresenta un valore per uno specifico segmento di clienti); i segmenti di cliente (il target di clienti a cui ci si vuole rivolgere); le relazioni con i clienti, (tipo di relazione che l'azienda stabilisce con i diversi segmenti di clienti) e i canali (che definiscono le modalità di contatto con i clienti);
- **Value network** che racchiude i partner (la rete di soggetti esterni all'impresa necessari per il corretto funzionamento del modello di business); risorse chiave (asset strategici di cui l'impresa deve disporre per dare vita e sostenere il modello di business); attività chiave (attività "core" che devono essere svolte per creare e sostenere le value proposition);
- **Economic model** composta da flussi di ricavi (connessi all'implementazione del business model; struttura dei costi (che dovranno essere sostenuti).

Tabella 1. Business model - New Energy Community

Value proposition & customer Interface	**Value network**	**Economic model**
▪ Aumento della domanda di beni e servizi ▪ Diminuzione del tasso di disoccupazione ▪ Minore emarginazione sociale ▪ Riduzione dei costi sociali e sanitari ▪ Disponibilità di nuovi servizi ▪ Creazione di un market place locale per il trading di energia ▪ Incremento delle installazioni FER nella comunità ▪ Riduzione della bolletta energetica della comunità ▪ Consapevolezza energetica ▪ Partecipazione attiva dell'utente.	▪ Organizzazione no- profit che regola l'emissione e circolazione della valuta comunitaria ▪ Gruppo di supporto del progetto: ○ Associazioni di volontariato ○ Uffici per l'impiego ○ Circoli culturali e ricreativi ○ Commercianti ○ Aziende ○ Consumatori ○ Prosumer energetico-sociali ○ Università ○ Utility ○ Cooperativa Energetica	▪ **Costi**: ○ piattaforma blockchain per il trading peer to peer di servizi socio-energetici ○ impianto fotovoltaico e storage ▪ **Ricavi**: ▪ **prosumer sociale**: coin spendibili nel circuito commerciale della community sotto forma di sconti su beni e servizi ▪ **punti vendita**: maggiori vendite ▪ **consumatore di energia**: risparmio energetico ▪ **prosumer energetico**: dalla vendita del surplus alla community o alla rete.

Come vedremo nel capitolo 7, gran parte delle monete complementari esistenti hanno un ancoraggio fisso alla moneta ufficiale, di norma secondo una parità di 1 a 1. I circuiti che hanno per oggetto lo scambio di servizi adottano spesso, come unità di riferimento, l'ora di lavoro. Nel WAT giapponese, ad esempio, l'unità di conto è 1KWh della corrente elettrica generata dalle comunità energetiche da fonti rinnovabili, equivalente a 6 minuti di lavoro e a circa 75-100 yen. Alcune valute sono convertibili in valuta fiat altre no, generalmente alla convertibilità è applicato una penalità per scoraggiare la fuoriuscita dal circuito della valuta.

5. LE APPLICAZIONI BLOCKCHAIN AL SETTORE ENERGETICO

5.1 Monitoraggio, billing e pagamento energia

I processi del settore energetico, come la fatturazione e la distribuzione degli oneri, richiedono lo scambio di dati tra i vari attori del mercato. I dati di consumo di un cliente vengono scritti nella blockchain tramite un sistema di smart metering (smart meter gateway). Il fornitore redige la fattura, mentre il gestore del sistema di distribuzione determina le tariffe e la riallocazione degli oneri. Dopo la verifica ed il trasferimento, i valori convalidati vengono scritti nel registro distribuito [19].

La Blockchain integrata all'infrastruttura di smart metering garantisce la tracciabilità dell'energia prodotta e consumata, informando i consumatori sulle origini ed i costi del loro approvvigionamento, rendendo le tariffe più trasparenti con il risultato di incentivare la flessibilità energetica. La sicurezza della transazione e la garanzia che la piattaforma su cui poggia una microgrid non possa venir manomessa ha spinto diverse società di servizi ad avviare progetti basati su blockchain per consentire il billing in tempo reale il cui pagamento (in cryptovalute o in valute fiat), da parte dell'utente, diventa contestuale all'erogazione di energia stessa. Si distinguono a tale riguardo due possibili casi di implementazione della tecnologia [20]:

- Utilizzo di criptovalute per effettuare il pagamento dell'energia consumata.;
- Forme alternative di billing dell'energia prodotta e consumata.

Per quanto riguarda la prima applicazione **BAS Netherlands** è stata pioniera nell'accettare Bitcoin come nuova forma di pagamento per le bollette elettriche. Hanno fatto seguito il provider tedesco **Enercity** i cui clienti residenziali possono effettuare i pagamenti via Internet e utilizzare automaticamente lo scambio di Bitcoins in Euro, ed **Elegant Energy**, provider di energia rinnovabile delle Fiandre, che invece ha introdotto la crittografia dei pagamenti in valuta per la fornitura di servizi energetici, compresi i pagamenti di gas ed elettricità. Più di 1 milione di clienti **Marubeni** possono beneficiare di una riduzione dal 4% al 6% delle bollette, se sono disposti a pagare le loro bollette elettriche con Bitcoin invece che con le valute fiat. Marubeni sta espandendo i pagamenti in valuta criptata anche per altri servizi ed asset. I risparmi così conseguiti possono essere raccolti in valute crittografiche a scelta del cliente e conservati in portafogli digitali. In **Italia Sorgenia** con **Chainside** si sta muovendo in questa direzione, per ora i clienti Sorgenia possono pagare in bitcoin soluzioni smarthome e prodotti dedicati alla mobilità. Per quanto riguarda il secondo tipo di applicazione, **LO3 Energy** sta utilizzando la blockchain progettata da Consensys per il regolamento finanziario real-time del trasferimento di energia tra i partecipanti al TransActive Grid Project di Brooklyn. **Bankymoon**, una start up sudafricana, in collaborazione con Sarb, Banca di Riserva Sud Africana, consente pagamenti in criptovaluta grazie all'utilizzo di contatori intelligenti situati in aree remote del paese compatibili con bitcoin. La soluzione mira a superare i problemi sperimentati nei paesi in via di sviluppo con i ritardi nei pagamenti, i mancati pagamenti dovuti all'elevato tasso di popolazione non" bancarizzata". Sempre in questa ottica, **SunChain**, una startup di TECSOL che collabora con Enedis, utilizza la tecnologia blockchain per certificare, convalidare ed eseguire automaticamente le transazioni tra consumatori e produttori di energia. I dati degli smart meter sono trasferiti in registri distribuiti, che possono essere condivisi con i gestori delle reti di distribuzione ed i fornitori di energia assicurando una generazione di energia verde tracciabile ed una fatturazione accurata. Nel contesto italiano **E-Prosume**, nata dalla joint venture tra le società Prosume ed Evolvere ha integrato la tecnologia blockchain su Eugenio, lo smart hub domestico

usato dai membri della community energetica di Evolvere. Attraverso la blockchain Eugenio oltre ad occuparsi dell'ottimizzazione dei consumi degli elettrodomestici permetterà ad Evolvere di gestire il tracciamento dell'energia prodotta e consumata dal singolo utente abilitando al billing in tempo reale dell'energia attraverso smart contract.

Pros & Cons "Monitoring, billing, payment"
Se da un lato, l'impiego della blockchain nel monitoraggio, billing e pagamento dell'energia promette una gestione decentralizzata dei dati dei contatori, eliminando la necessità di un'autorità centrale dedicata ed il rischio di un unico *point of failure*, dall'altro la disponibilità di un'adeguata infrastruttura di smart metering di nuova generazione e la necessità di sviluppare nuovi standard che ne garantiscano l'interoperabilità costituisce al momento una delle barriere principali alla diffusione su larga scala di questa applicazione.
Il circolante in criptovaluta rappresenta un asset importante che può portare valore all'economia reale e all'economia "domestica". La partnership Sorgenia-Chainside, e gli altri use case che prevedono il pagamento dei consumi energetici con criptovaluta, permettono di intercettare questa disponibilità di risorse ed agevolare lo sviluppo di una economia collegata alle *criptocurrency*. I rischi principali associati all'ambito applicativo in questione sono essenzialmente imputabili alla volatilità delle criptovalute, che determina incertezza sui costi associati ad ogni transazione, ed ai tempi di esecuzione dei pagamenti superiori rispetto ai quelli supportati da sistemi di pagamento tradizionali [20].

5.2 E-mobility

La gestione della ricarica dei veicoli elettrici e la fatturazione della mobilità elettrica per la loro natura decentralizzata si prestano in modo particolare alle applicazioni blockchain. Una delle problematiche ancora irrisolte nell'ambito della mobilità elettrica è rappresentato dalla **mancanza di interoperabilità software** dovuta alla presenza di infrastrutture di ricarica appartenenti a reti distinte e che utilizzano piattaforme e protocolli di comunicazione differenti non condivise tra i vari gestori [20]. Il problema potrebbe essere superato tramite l'impiego della blockchain come protocollo standard di comunicazione tra gestori e possessori di vicoli e tra i differenti gestori. Questo permetterebbe di estendere la rete di ricarica disponibile dando la possibilità all'utilizzatore di accedere a tutte le colonnine di ricarica munite di smart contract, comprese le colonnine di privati, abilitando alla cosiddetta ricarica P2P. Sono numerose le aziende che stanno sperimentando queste applicazioni. **MotionWerk** ha introdotto in Germania l'applicazione **Share&Charge**, che superando il problema dell'interoperabilità software, abilita gli utenti registrati a visualizzare le stazioni di ricarica presenti nell'area, autenticarsi e pagare l'energia consumata tramite smart contract senza alcun costo aggiuntivo. I gestori delle colonnine di ricarica possono realizzare smart contract basati su differenti sistemi di tariffazione, l'app Share&Charge si occuperà della fatturazione. Nel 2018 Share& Charge ha aderito all'iniziativa di **Energy Web Foundation (EWF),** una piattaforma open-source per applicazioni blockchain dedicate al settore energetico. L'obiettivo di questa sinergia è garantire una ricarica con soluzione di continuità, sicura e smart integrando i poli di ricarica ed i veicoli elettrici a livello globale, con la promessa di migliorare l'esperienza del cliente finale, i processi aziendali e la sicurezza informatica. Con sede in Germania, **Car&Wallet** ha sviluppato una piattaforma blockchain di transazione P2P che integra diversi servizi di mobilità, come la ricarica delle auto da diversi fornitori di energia e stazioni di ricarica private, parcheggi, car sharing e

noleggio auto. Car&Wallet elimina la necessità di piattaforma centralizzata per la gestione delle transizioni utilizzando un registro condiviso sviluppato con la tecnologia Hyperledger. I pagamenti possono essere elaborati automaticamente o manualmente a seconda delle esigenze del cliente. **Bosch** in collaborazione con il fornitore austriaco di energia EnBW sta lavorando su un prototipo che utilizza la tecnologia blockchain per migliorare il processo di ricarica delle auto elettriche**.** L'idea è quella di semplificare e adattare l'intero processo alle esigenze dei clienti in modo che possano selezionare, prenotare e pagare i servizi di rifornimento come preferiscono. L'operatore potrebbe combinare il software sviluppato da Bosch per le automobili con la gestione di una stazione di **ricarica smart** e offrire ai clienti modelli di prezzo trasparenti, con opzioni variabili in tempo reale a seconda della disponibilità di stazioni di ricarica ed energia pulita proveniente da fonti rinnovabili. L'intera transazione, dalla prenotazione al pagamento, è un'operazione completamente automatizzata sulla blockchain. Questo servizio può tener conto anche di altre preferenze del cliente e venire incontro alle diverse esigenze di ciascuno, in termini di tempi di sosta, livello di ricarica desiderato, vicinanza a determinati servizi. La tecnologia blockchain può infatti abilitare una modalità di **ricarica personalizzata** per l'utente finale attraverso l'impiego di smart contract sviluppati sulla base delle preferenze degli utenti finali questo oltre a migliore l'esperienza dell'utente permetterebbe al gestore dell'infrastruttura di modulare la ricarica del veicolo in base all'esigenze di bilanciamento della rete (Vehicle to Grid, V2G). **Honda** e **General Motors** (GM) stanno conducendo delle ricerche sull'interoperabilità di veicoli elettrici e smart grid utilizzando la tecnologia blockchain. Come parte del progetto, Honda e GM esamineranno se i veicoli elettrici possono essere utilizzati per stabilizzare la fornitura di energia nelle smart grid. Nello specifico, le società intendono sviluppare dei metodi di recupero dei dati tra veicoli elettrici e reti intelligenti, che consentiranno ai possessori di tali auto di guadagnare commissioni dallo stoccaggio dell'energia nelle batterie e dallo scambio con la rete. Le due aziende lavoreranno all'interno del consorzio tecnologico internazionale **Mobility Open Blockchain Initiative** (MOBI), che ha come obiettivo proprio quello di rendere più efficienti i servizi di mobilità. La piattaforma è stata lanciata nel 2019 ed è frutto dell'ingegno di oltre trenta partecipanti tra cui Bosch, Hyperledger, IBM e IOTA. GM ha depositato un brevetto che descrive una soluzione blockchain per la gestione dei dati provenienti dai veicoli autonomi. Il sistema mira a fornire una distribuzione dei dati "sicura" e "robusta" e uno scambio interoperabile tra più veicoli automatizzati e altre entità, come comuni, autorità regionali e strutture pubbliche. Il colosso automobilistico americano sta inoltre collaborando ad un progetto della startup **Spring Labs**, che mira a migliorare la sicurezza dei dati.

Pros &Cons "E-Mobility"

I vantaggi delle applicazioni blockchain alla mobilità elettrica sono numerosi: eliminazione della necessità di un'infrastruttura di ricarica dei veicoli elettrici gestita centralmente, ampliamento della rete di ricarica disponibile, una maggiore tolleranza ai guasti delle colonnine di ricarica, eliminazione della collusione tra i gestori delle stazioni di ricarica nella fissazione dei prezzi e possibilità di contribuire alla stabilizzazione della rete utilizzando le batterie dei vicoli in base alle preferenze di ricarica espresse dai proprietari. Mentre la sfida principale che in questa applicazione la blockchain deve ancora superare riguarda principalmente la tutela della privacy in merito alla localizzazione e agli spostamenti dei veicoli elettrici connessi.

5.3 Incentivazione alla produzione di energia rinnovabile

Uno degli incentivi adottati dagli stati per promuovere l'installazione di capacità produttiva da fonti rinnovabili è stata l'emissione di **Certificati Verdi** o **Renewable Energy Certificates** [20].Tuttavia le attuali strutture di mercato per i certificati verdi sono frammentate e complesse ed i piccoli produttori di energia rinnovabile sono di fatto esclusi dall'attribuzione dei relativi certificati a causa degli alti costi associati alla procedura. Inoltre i processi di audit condotti manualmente da un ente centrale sono error-prone e soggetti a possibili frodi. L'utilizzo della blockchain permette di automatizzare l'emissione dei certificati verdi anche per piccoli volumi di energia prodotta, rimuovendo la necessità di un ente centrale per la emissione ed il ritiro dei certificati sul mercato con l'effetto di ridurrebbe i costi di transazione ed aumentare la trasparenza del mercato. Mediante l'installazione di smart meter integrati con la blockchain agli impianti di produzione a fonte rinnovabile si può tracciare l'effettiva produzione di energia ed automatizzare l'emissione dei certificati al raggiungimento di una determinata soglia fissata in uno smart contract. Anche il trading può essere automatizzato permettendo una monetizzazione in tempo reale del certificato venduto a chi deve soddisfare gli obblighi di riduzione delle emissioni. Anche in questo caso gli esempi non mancano. La principale utility di Singapore, la **SP Group**, ha lanciato uno dei primi mercati mondiali di Renewable Energy Certificates, basato sulla tecnologia blockchain. Questo mercato consente alle imprese ed ai consumatori di commerciare in certificati di energia rinnovabile a livello globale. Le particolari caratteristiche della tecnologia blockchain, su cui si basa la piattaforma, consentono agli acquirenti di essere abbinati automaticamente ai venditori di tali certificati, in base alle loro preferenze. Il mercato SP REC permette, infatti, di commercializzare certificati di origine locale, regionale e internazionale e supporta anche diverse opzioni di scelta, compresi i tipi di venditori e le diverse fonti di energia rinnovabile. La statunitense **Volts Markets** utilizza contratti intelligenti per emettere automaticamente e tracciare certificati relativi alla produzione di energia rinnovabile attraverso una piattaforma di exchange di asset energetici. **Verdium** ha lanciato una piattaforma basata su ethereum per lo scambio di crediti di carbonio attraverso il token TRG. L'austrica **Grid Singularity**, membro fondatore della Energy Web Foundation, mira a fornire diverse soluzioni blockchain per il settore energetico, incluso il commercio di Renewable Energy Certificates.
Altre applicazioni in ambito environment della blockchain riguardano l'emissione di criptvalute legata alla produzione di energia rinnovabile con l'obiettivo di incentivare comportamenti consapevoli e facilitare gli investimenti in energia pulita. La strat up **SolarChange** ha creato SolarCoin per incentivare la produzione di energia solare. I proprietari di pannelli fotovoltaici ricevono un SolarCoin per ogni megawattora di elettricità prodotta. I SolarCoin possono essere scambiati con altre criptovalute o monete fiat. Attualmente attiva in 32 paesi, SolarCoin mira ad incentivare 97.500 TWhs di produzione globale di energia solare nel corso dei prossimi 40 anni. SolarCoin funziona su una blockchain pubblica simile a Bitcoin, il protocollo di consenso usato in questo caso è il proof of stake.

Pros &Cons "Incentivazione produzione energia rinnovabile"

I vantaggi delle applicazioni blockchain finalizzate ad incentivare la produzione di energia verde sono riconducibili: alla trasparenza sui dati di produzione; all'abbattimento dei costi burocratici nei casi di emissione in tempo reale dei certificati di energia rinnovabile; all'eliminazione delle barriere all'ingresso dei piccoli produttori di energia verde al mercato dei certificati, alla possibilità di ammortizzare più velocemente l'impianto di generazione. Ciò che ancora è inesplorato è il potenziale di manomissione degli smart meter connessi al registro distribuito, che hanno il compito fondamentale di tracciare costantemente l'energia prodotta ed automatizzare l'emissione dei certificati, sulla cui attendibilità poggia l'intera soluzione. Si parla a tale riguardo di **oracle problem**. Nel codice del sensore è presente una chiave privata e chiunque la possiede può impersonare il sensore e manomettere i dati trasmessi. Tra le possibili soluzioni attualmente disponibili: le chiavi possono essere generate al momento della produzione in memorie sicure non volatili (NVM), oppure possono essere derivate da *physically unclonable functions* (PUF). Le PUF sono uniche per ciascun dispositivo, e non possono essere clonate. L'output può essere utilizzato per generare chiavi uniche per ogni sensore.

5.4 Piattaforme di trading Peer to Peer

La blockchain può abilitare i *prosumer* a vendere direttamente ai consumatori l'energia prodotta e non consumata. Soprattutto garantisce una tracciabilità dello scambio energetico che i soggetti non possono negare o falsificare. L'energia prodotta da un Prosumer con un sistema di fonti rinnovabili verrà registrata in un token e assegnata ad un wallet [21]. Il wallet sarà decurtato della parte dell'energia autoconsumata dal prosumer, la parte restante potrà essere accumulata o venduta ad altri utenti del network. Il consumer che necessita di energia, fissa con una app il prezzo massimo per l'approvvigionamento della stessa, lo smart contract di riferimento collegherà tutte le offerte che soddisfano le condizioni richieste. Una volta che la domanda ha incontrato l'offerta desiderata viene generata e notarizzata una transazione su blockchain. Il billing ed il pagamento sono automatizzati ed avvengono in real-time tramite il trasferimento dal wallet del consumatore a quello del prosumer di token pari al valore dell'energia scambiata. In questo modo, utilizzando uno schema di incentivazione ad hoc, che induca il prosumer a fornire energia ai consumatori localizzati nella stessa area, si favoriscono i consumi locali e la creazione di microgrid. Nel caso di transazioni all'interno di microgrid basate su infrastrutture di distribuzione private, i prezzi relativi al trading di energia effettuati dai privati, comprenderebbero solamente la "componente energia" e sarebbero inferiori a quelli ottenibili sulla rete elettrica grazie al mancato pagamento degli oneri di sistemi relativi alla trasmissione e distribuzione dell'energia.

Piclo è una piattaforma di trading energetico P2P sviluppata nel Regno Unito grazie ad una collaborazione tra Open Utility (provider tecnologico innovativo) e Good Energy (fornitore di energia rinnovabile) dove i consumatori possono acquistare direttamene energia elettrica dai produttori locali. I dati dei contatori, le preferenze di prezzo sono usati per il *matching* tra la domanda e l'offerta di energia ogni mezz'ora. Similmente **Vandebron** è una piattaforma online sviluppata in Olanda dove i consumatori possono acquistare direttamente energia da produttori indipendenti. **PeerEnergyCloud** è un'altra piattaforma di trading di energia elettrica sviluppata in Germania per

gestire l'eccesso di produzione locale, usata anche per studiare procedure innovative di registrazione e previsione dei consumi elettrici di specifici dispositivi e per sviluppare servizi a valore aggiunto all'interno di una microgrid. Enyway, è nata in Germania e consente ai consumatori di comprare l'elettricità da piccolissimi fornitori, proprietari di una singola pala eolica o di un tetto solare sopra la fattoria. Sul portale di Enyway si raccontano le loro storie, arricchite da foto. La transazione avviene su di una piattaforma basata su protocollo blockchain che consente di registrare in automatico gli scambi, collegando l'elettricità in uscita dal fornitore con quella in entrata nelle case dei consumatori. In Australia sta prendendo piede **Power Ledger**, che ha lanciato una serie di scambi peer-to-peer fra piccoli produttori e clienti interessati a comprare energia verde in varie parti del Paese, massimizzando così l'utilizzo dei pannelli. L'ultimo progetto, sempre basato su piattaforma blockchain, è appena entrato in funzione nel porto di Fremantle, vicino a Perth, ma l'idea è allargarsi in tutto il Sud dell'Australia, dove c'è molta generazione distribuita.

Pros &Cons "Trading Peer to Peer"

I vantaggi rispetto alle forniture tradizionali di energia, dove il privato compra da un operatore di grandi dimensioni, sono riconducibili alla tipologia del rapporto "alla pari" con gli altri nodi della rete, che consente di abbassare i costi delle transazioni nonché alla sicurezza della transazione e garanzia che la piattaforma su cui gira la microgrid non possa venir manomessa. L'utente finale inoltre potrà visualizzare con la massima trasparenza sia i consumi energetici, che in caso di prosumer, la quantità di energia prodotta dal proprio impianto. I limiti attuali sono principalmente normativi dato che in diversi paesi, tra cui l'Italia, i prosumers presenti sul territorio non possono vendere direttamente il surplus energetico ai consumatori finali presenti sulla rete.

5.5 Grid Management & Active Demand Response

L'aumento di impianti di produzione rinnovabile non programmabile pone delle sfide inerenti il bilanciamento della domanda e dell'offerta all'interno dell'infrastruttura elettrica, creando una maggiore richiesta di servizi legati alla "**flessibilità**". In Italia il servizio è fornito da Terna che emette all'interno del mercato di dispacciamento le richieste di approvvigionamento di risorse necessarie alla gestione e al controllo del sistema elettrico. Gli operatori abilitati all'erogazione di servizi di rete rispondono alla chiamata di Terna per offrendo la propria capacità di fornire elettricità oppure di ridurre la produzione. Le offerte sono attivate da Terna in base al merito economico e sono valorizzate al prezzo offerto [19]. I gestori dei mercati di dispacciamento potrebbero semplificare l'attuale sistema attraverso l'impiego di smart contracts da parte di tutti i soggetti abilitati a partecipare. In questo modo le utenze potrebbero definire istante per istante, all'interno dello smart contract stesso, sulla base di coefficienti di equivalenza tra differenti fasce orarie, la quantità di capacità messa a disposizione del mercato e il prezzo richiesto per l'effettiva attivazione della stessa. I gestori potrebbero visualizzare in real-time le offerte da parte di ciascun soggetto abilitato e attivare direttamente gli smart contract fino alla risoluzione della congestione di rete [20].Di seguito sono presentate alcune delle iniziative più significative in questo ambito. **PONTON** ha sviluppato **Gridchain**, un innovativo software basato sulla tecnologia blockchain per la creazione di processo integrato che coordina in pochi secondi le richieste di bilanciamento di potenza tra TSO e DSO, aggregatori ed unità di generazione. **Grid Singularity**, membro fondatore dell'associazione

Energy Web Foundation, offre soluzioni per la gestione della rete. In Germania le congestioni di rete hanno determinato un aumento dei costi per il sistema elettrico e per i consumatori finali pari a 800 milioni di €, derivanti dal taglio della produzione da impianti eolici localizzati nel nord della Germania e dall'attivazione dei più costosi impianti a carbone e gas localizzati nel sud della stessa. Per cercare di risolvere questo problema **TenneT** in partnership con **Sonnen** e **IBM**, ha avviato nel 2017 un progetto pilota volto a identificare le capacità dei protocolli blockchain di integrare i sistemi di storage residenziale della **Sonnen Community** all'interno di un **Virtual power plant** da utilizzare per la stabilizzazione delle stesse infrastrutture di trasmissione-distribuzione energetica controllate dal TSO TenneT. All'interno di questo progetto l'utilizzo della blockchain permette di abilitare un dialogo costante tra i sistemi di storage e la rete, permettendo ai singoli accumulatori di rispondere autonomamente alle richieste di bilanciamento provenienti dall'infrastruttura elettrica, caricando o scaricando energia, in base alle necessità del momento. Una piattaforma blockchain sviluppata da **PROSUME** mira a ridurre i costi di rete migliorando il bilanciamento del carico con i dispositivi di accumulo dell'energia e gli scambi di trasmissione. **EvolvePower** ha sviluppato soluzioni blockchain per le società di servizi energetici e gli operatori di rete, consentendo loro di ottenere una migliore visibilità, accesso e controllo su dati di rete, consentendo un controllo più rapido sui servizi di *demand response.*

Pros &Cons "Grid Mangement & Active Demand Response"

Queste applicazioni mirano a sviluppare una collaborazione più diretta tra gestore dei mercati dei servizi di dispacciamento e soggetti abilitati grazie all'utilizzo della tecnologia blockchain, la quale permette di aumentare il numero di soggetti abilitati a fornire servizi legati alla flessibilità e ridurre i costi sostenuti dalla collettività per il bilanciamento della rete [20]. L'implementazione di queste tipologie di progetti permette di gestire la sempre maggiore introduzione di capacità di generazione non programmabile, ma anche di migliorare i tempi di ritorno relativi all'adozione di sistemi di storage residenziale in quanto gli utenti otterranno vantaggi non solo dalla massimizzazione dell'autoconsumo, ma saranno remunerati per aver messo a disposizione i propri sistemi di storage per fornire servizi di rete. Essendo la rete di distribuzione di energia elettrica un'infrastruttura critica le blockchain pubbliche *permissionless* mal si adattano a questo ambito applicativo a causa di quelli sono considerati gli attuali limiti di questo particolare tipo di registro distribuito: problemi di privacy; alti costi di transazione e performance limitata.

6. TIPOLOGIE E CATEGORIE DI ENERGY COMMUNITY

6.1 Tipologie di EC

6.1.1 Centralizzate

Ci riferiamo ad una comunità energetica centralizzata come ad una rete coesa di famiglie ed imprese che collettivamente possiedono o partecipano a progetti connessi all'energia, come il solare, l'eolico e altri progetti di generazione di energia rinnovabile, di efficienza energetica, e di gestione della domanda. La caratteristica principale di una EC centralizzata è che può essere relativamente facile la sua integrazione nell'infrastruttura elettrica esistente, nell'ambito dell'attuale regime [21]. Gran parte dei progetti energetici comunitari esaminati in letteratura sono riconducibili a questa tipologia. Le EC centralizzate perseguono progetti di energia rinnovabile su scala comunitaria sotto forma di cooperative energetiche, o imprese di comunità caratterizzate da un livello relativamente alto di coesione è strettamente orientate al raggiungimento di obiettivi comuni. Naturalmente ciò non implica necessariamente la prossimità geografica dei membri della comunità, ma piuttosto un'elevata interazione tra gli stessi. Le iniziative spesso provengono dal basso, le decisioni sono prese a livello comunitario. Le regole e le attività sono controllate e gestite da un organo di governo rappresentativo della comunità. L'organo di governo centrale agisce come portavoce, pianificatore strategico e decisionale per l'intera comunità, gioca anche un ruolo centrale nella comunicazione con gli stakeholder esterni, assegna risorse, e mantiene la coesione e la stabilità tra i membri [22]. L'alto livello di coesione e coordinamento all'interno di queste comunità paradossalmente rende più difficile l'innovazione ed il cambiamento. La coesione ostacola la capacità delle CE centralizzate di raggiungere una cerchia più ampia di utenti e di generare soluzioni non convenzionali che comportano esperimenti innovativi e l'assunzione di rischi [23]. L'equità sociale può essere rafforzata grazie ad organizzazioni che svolgendo il ruolo di facilitatori contribuiscono allo scambio di idee e conoscenza e forniscono consulenza tecnica e finanziaria [24]. La scarsità di risorse finanziarie che caratterizza queste comunità che si basano solo sulle risorse dei propri membri e su finanziamenti esterni spesso limita il loro raggio di azione ad un numero ridotto di piccoli progetti locali con il conseguente rischio di non raggiungere economie di scala sufficienti a destare l'interesse di provider tecnologici ed operatori di rete. La connessione e l'accesso alla rete sono un altro limite delle EC centralizzate che per mancanza di esperienza tecnica e commerciale restano dipendenti dall'operatore di rete.

Di conseguenza, anche se le EC centralizzate hanno un ruolo importante nel processo di transizione energetica attualmente non hanno le dimensioni, la portata, l'influenza economica e il potenziale richiesto per smantellare o trasformare il regime esistente.

6.1.2 Distribuite

Una comunità energetica distribuita è definita come un network di famiglie ed imprese che possiedono individualmente gli impianti di generazione distribuita, connesse virtualmente o fisicamente tra di loro attraverso una unità di controllo che condividono le stesse regole nella domanda ed offerta di elettricità. Le EC distribuite comprendono un certo numero di nodi senza richiederne la prossimità geografica o normativa [21]. Se confrontate con le EC centralizzate e decentralizzate i confini delle EC distribuite possono essere definiti come parziali, permeabili e transitori. Le tecnologie smart e le moderne reti di comunicazione hanno consentito alle organizzazioni ed alle comunità di estendere i propri confini permettendo il facile collegamento tra

individui anche in assenza di una connessione diretta favorendo lo sviluppo delle comunità non locali [25]. I membri di una comunità distribuita decidono individualmente i propri investimenti sulla base delle proprie preferenze e capacità finanziarie. I membri o nodi della comunità virtuale sono uniti da un'entità di controllo che può essere rappresentata o da un provider tecnologico che fornisce una piattaforma blockchain abilitando le transazioni energetiche tra i membri oppure da una utility che agisce da broker per la comunicazione e l'accesso al network. I legami relazionali tra provider/utility e comunità devono essere plasmati e rafforzati stabilendo regole comuni e sistemi di incentivi trasparenti e fruibili. Il comportamento collaborativo è incoraggiato dalle passate interazioni ed il costo della futura collaborazione è probabile che diminuisca con il passare del tempo essendo inversamente proporzionale alla distanza relazionale tra le parti. Le EC distribuite si basano principalmente sull'infrastruttura tecnologica e sull'hub organizzativo che fornisce il servizio per la creazione di una Virtual Power plant (VPP) o di una piattaforma di trading P2P e di conseguenza sui provider tecnologici e sulle utility che forniscono questi servizi. Sia le VPP che le piattaforme di trading P2P rappresentano nuovi modelli di business che creano valore garantendo un migliore impiego degli asset ed il trading di servizi, distribuendo benefici economici ai membri della collettività e rappresentando una opportunità di business per imprenditori ed utility lungimiranti. Alcuni piccoli distributori, vedendo in questi modelli l'opportunità di espandere l'offerta dei propri prodotti e quindi la propria clientela, esercitano una pressione sui grandi players affinché percorrano queste alternative, influenzando indirettamente anche l'evoluzione normativa.

6.1.3 Decentralizzate

Una EC decentralizzata è definita come un insieme di famiglie ed imprese che genera e consuma energia a livello locale per l'autosufficienza energetica che può essere connessa o meno alla rete principale. Si distingue dalla EC centralizzate e distribuite proprio per la sua autonomia ed indipendenza rispetto al sistema energetico centralizzato. Un EC decentralizzata poggia sulla forte coesione esistente tra i sui membri che hanno una visione condivisa su tematiche energetiche ed ambientali [21].

I membri di un EC decentralizzata appartengono ad una area delimitata, come un quartiere, un villaggio/città o un comune, possono detenere gli impianti di generazione individualmente o collettivamente in molti casi sono proprietari anche delle infrastrutture di distribuzione, costituendo parte di una microgrid comunitaria, e/o di un sistema energetico comunitario integrato. Per le microgrid connesse alla rete una sfida risiede nel raggiungere la conformità ai rigorosi standard di affidabilità. I processi di connessione della generazione integrata e la funzionalità islanding/re-joining rappresentano infatti una prospettiva relativamente nuova per gli operatori di rete [26].

Una EC decentralizzata richiede l'implementazione di nuove l'infrastruttura e/o la riconfigurazione dell'infrastruttura esistente, il che implica una strategia di lungo termine e una struttura di governance in grado di coinvolgere i principali stakeholders, i rappresentati della comunità, i fornitori di servizi, creando una coalizione in grado di mobilizzare ingenti risorse [27].

Date le caratteristiche a lungo termine degli asset delle infrastrutture elettriche, un'attenta e graduale attuazione delle soluzioni può aiutare a gestire l'implementazione e i rischi finanziari, consentire scenari di "trial-and-error" e scoprire soluzioni e alternative e migliori durante il processo.

Alcuni studi evidenziano come il coinvolgimento di agenzie governative ed associazioni professionali nelle EC decentralizzate rappresentino un fattore determinante nelle decisioni di investimento legate a questi progetti [28].

Una struttura di governance direzionale con una interazione non fitta tra una varietà di gruppi di attori con motivazioni differenti può essere vantaggiosa in termini di apprendimento e networking

stabilendo collegamenti ed ottenendo il supporto di stakeholder chiave per la creazione di un nuovo sistema di approvvigionamento e per innescare il processo di trasformazione [29].

6.2 Categorie di EC

6.2.1 Community-scale energy project

I progetti energetici su scala comunitaria rientrano nella tipologia di EC centralizzata e sono finalizzati ad accrescere l'approvvigionamento locale da fonti rinnovabili e l'efficienza dei servizi energetici comunitari. Questi progetti sono realizzati seguendo un approccio bottom up: i membri si organizzano in una forma societaria idonea per poter finanziare collettivamente e realizzare in autonomia il progetto. L'energia autoprodotta viene venduta alle utility locali ed i profitti sono ripartiti tra i membri della comunità [21].

I community-scale energy project oltre ad avere un ruolo importante nel processo di transizione verso un'energia a basse emissioni di carbonio, offrono anche altri benefici collaterali: consentono ai partecipanti di sfruttare le risorse naturali locali, costruire capitale sociale, contrastare la fuel poverty ed aumentare le opportunità occupazionali a livello locale. In Europa alcuni paesi più di altri hanno saputo cogliere queste opportunità. In particolare la Germania e la Danimarca sono pioniere a livello mondiale nello sviluppo di questi modelli di comunità energetiche. Dagli anni '70 le comunità energetiche danesi hanno investito collettivamente in parchi eolici. Circa l'80% delle turbine eoliche esistenti sono di proprietà delle comunità energetiche ed anche il tasso di produzione di energia rinnovabile di proprietà delle comunità è diventato uno dei più alti al mondo. In Danimarca, il governo federale è responsabile della maggior parte delle questioni energetiche. Sebbene il sostegno sia diminuito negli ultimi anni, il governo danese ha da sempre promosso lo sviluppo di progetti energetici di proprietà delle comunità, ed in particolare delle centrali eoliche. I proprietari delle turbine devono pagare solo per il collegamento al punto tecnicamente più vicino della rete mentre le utility sono tenute a pagare gli eventuali ampliamenti della rete. Inoltre dal 2009, la legge danese sulle energie rinnovabili impone che tutti i nuovi progetti eolici siano di proprietà di almeno il 20% della popolazione locale. In Danimarca, pertanto, la produzione comunitaria di energia avviene prevalentemente in partenariato con le società di servizi energetici (progetti energetici comunitari in comproprietà).

Il parco eolico di **Middelgrundens** in **Danimarca** è un buon esempio di questo modello di comunità energetica. Il 50% del parco eolico di Middelgrundens (20 turbine da 2 MW ciascuna) è di proprietà del comune di Copenhagen, mentre il restante 50% è di proprietà dei membri della cooperativa Middelgundens Vindmollelaug I/S. All'inizio del progetto, solo i residenti del comune di Copenhagen potevano essere membri della partnership, ora è aperta a tutti. I privati sono attratti dall'investimento a basso rischio (poiché la partnership non può contrarre debiti) e dalla possibilità di partecipare alle decisioni importanti, godendo di un diritto di voto indipendente dalla quantità di azioni possedute [30].

Un parco eolico a **Hvide Sande** è un altro esempio di best practice in **Danimarca**. Qui la produzione di energia va a beneficio non solo degli individui che detengono quote del progetto, ma della comunità nel suo complesso. All'interno del piccolo villaggio di pescatori danese Hvide Sande, nel 2010 sono state create tre turbine eoliche offshore sotto la direzione di diversi attori (sindacati, industrie ed utility) che hanno dato luogo ad una fondazione per la comunità locale. L'80% del parco eolico è detenuto dalla fondazione comunitaria, il restante 20% dalla società in nome collettivo Hvide Sande Norde Nordhavn Mollelaug I/S1 [31]

La **Germania** è uno dei paesi europei leader nella realizzazione di progetti energetici comunitari sia nell'eolico che nel solare. Dall'inizio degli anni '90 diverse politiche federali hanno sostenuto la

produzione di energia rinnovabile (di proprietà comunitaria). l **Windpark Druiberg** a Dardesheim, in Germania, è un esempio eccellente di progetto energetico comunitario. Fuori dal piccolo villaggio rurale, dall'inizio degli anni '90 sono state installate 31 turbine eoliche (66 MW). La proprietà delle quote del parco eolico è limitata ai soli residenti locali, circa il 90% dei residenti di Dardesheim è coinvolto nel progetto. Gli obiettivi di progetto condivisi dai membri della comunità riguardano il rilancio dell'economia locale e l'autosufficienza energetica locale. L'utile realizzato è impiegato nell'ulteriore espansione delle energie rinnovabili nella regione e per sostenere lo sviluppo di infrastrutture locali e altri progetti regionali. Il finanziamento complessivo si è basato sugli investimenti di capitale degli azionisti e sul cofinanziamento mediante crediti commerciali [32].
La città di Friburgo sostiene fortemente l'installazione di impianti solari fotovoltaici (PV) e termici su edifici pubblici (in particolare scuole). Attraverso procedure amministrative trasparenti, i cittadini sono motivati ad investire in tali progetti. Con lo sviluppo di uno strumento online chiamato "FREE-SUN", i cittadini sono in grado di identificare facilmente gli spazi sul tetto disponibili per impianti solari fotovoltaici e termici. Questo facilita il processo di pianificazione di progetti fotovoltaici comunitari per i cittadini. Tramite "FREE-SUN" i cittadini possono accedere alle informazioni sull'idoneità di alcune strutture edilizie per impianti fotovoltaici e termici e su come i progetti potrebbero essere realizzati [33].

6.2.2 Virtual Power Plants e Community-based Virtual Power Plant

Appartenente alla tipologia di EC distribuite la centrale elettrica virtuale altrimenti nota come Virtual Power Plant (VPP) permette di aggregare tramite un sistema in cloud unità di generazione, accumulo e consumo decentralizzate nella rete elettrica e coordinate tramite un sistema di controllo. Le unità possono essere produttrici di energia elettrica quali impianti a biogas, centrali eoliche, impianti fotovoltaici, impianti di cogenerazione o centrali idroelettriche, consumatori di energia elettrica, accumulatori e impianti di conversione dell'energia (energia in gas, elettrolizzazione), veicoli elettrici. Lo scopo della Centrale Elettrica Virtuale consiste nella rivendita nei mercati dell'energia elettrica e della flessibilità dell'aggregato di impianti. Ogni attore, produttore o consumatore, può costituire parte di una Centrale Elettrica Virtuale.
La VPP impiega tecnologie quali l'ICT, gli smart meter, il data processing per incorporare varie fonti energetiche distribuite, come le energie rinnovabili, su larga scala in un'unica fonte di potenza che contribuisce al funzionamento del sistema. La gestione dell'aggregato è eseguita da un sistema di controllo centrale che mediante uno speciale algoritmo non solo coordina i singoli impianti, ma al pari di un'unica grande centrale elettrica, supporta il Gestore di rete per la fornitura di servizi per il bilanciamento e la regolazione, necessari per il funzionamento in sicurezza della rete.
La flessibilità di un impianto consiste nella capacità di modulare rapidamente e compensare le variazioni di potenza richiesta; è una caratteristica preziosa per il sistema energetico ed è il punto forte numero uno delle Centrali Elettriche Virtuali. Un unico sistema di controllo permette di ottimizzare il fabbisogno dei singoli consumatori che fanno parte della stessa VPP. In questo modo, l'energia può essere condivisa per gestire efficacemente la domanda: se un impianto sta consumando molta più energia di quella che produce, può sfruttare quella proveniente dagli altri sistemi collegati alla VPP. I sistemi di controllo delle centrali elettriche virtuali, sulla base di elementi quali le condizioni metereologiche, i cambiamenti dei prezzi e la domanda di energia, riescono a gestire la produzione, l'immagazzinamento ed i fabbisogni in modo efficace. La Centrale Elettrica Virtuale è inoltre in grado di reagire in modo veloce ed efficiente ai segnali di prezzo provenienti dai mercati dell'energia e di modulare di conseguenza il proprio funzionamento.
Negli ultimi anni si sono verificati due eventi che hanno favorito notevolmente lo sviluppo delle Centrali Elettriche Virtuali: da una parte la velocizzazione del processo di digitalizzazione che ha

permesso la creazione di un sistema di controllo potente, affidabile e performante nelle comunicazioni in tempo reale; dall' altra, la diffusione degli impianti di generazione da fonte rinnovabile e il progressivo smantellamento delle centrali termoelettriche tradizionali. Dato che le VPP sono composte da impianti (spesso rinnovabili) interconnessi, l'immissione è soggetta ad oscillazioni. Accanto a una varietà teoricamente illimitata di produttori di energia, anche i consumatori di energia, le centrali di accumulo e gli impianti di conversione di energia, quali quelli da elettricità a gas (power-to-gas, P2G) o da elettricità a calore (power-to-heat, PtH), possono essere integrati nell' aggregato di impianti. Tutte queste unità sono in grado di modulare la potenza e compensare le fluttuazioni di energia a seguito di oscillazioni della generazione.
Lo scambio di dati e l'invio di comandi è essenziale nella Centrale Elettrica Virtuale. Gli impianti che la compongono sono connessi al sistema centrale tramite sistemi a configurazione ridondata per avere il massimo dell'affidabilità. La connessione dati avviene tramite con corsie preferenziali virtuali (tunneling) criptate ad hoc. Questi collegamenti preferenziali sfruttano l'infrastruttura di comunicazione pubblica ma sono schermati dal restante traffico dati dal punto di vista dei loro protocolli di comunicazione. Questi collegamenti di dati bidirezionali dei singoli impianti alla Centrale Elettrica Virtuale non consentono soltanto l'invio di comandi, ma forniscono continuamente e in tempo reale dati sullo stato degli impianti connessi e pertanto anche della Centrale Elettrica Virtuale. Si possono così ad esempio generare previsioni precise riguardo l'immissione o il prelievo di energia elettrica ed ottimizzare la programmazione degli impianti regolabili conoscendo l'immissione degli impianti eolici e fotovoltaici, il consumo dei carichi elettrici e lo stato degli accumulatori si energia. L'acquisizione e l'elaborazione dei dati è effettuato dalla piattaforma della Centrale Elettrica Virtuale che provvede anche ad inviare comandi agli impianti.
Le Centrali Elettriche Virtuali si presentano al mercato alla stregua di una grande centrale elettrica e possono raggiungere le dimensioni di una o più centrali nucleari dal punto di vista della loro potenza installata.
Gli impianti di generazione controllabili da fonte rinnovabile quali impianti a biogas o centrali idroelettriche, ma anche impianti di cogenerazione e generatori di emergenza possono fornire dei servizi ancillari al Gestore di rete per contribuire a bilanciare l'energia in rete. Possono sia ridurre o interrompere la loro produzione in presenza di un'offerta eccessiva di energia elettrica (offrendo servizi "a scendere"), sia di immettere di più in caso di scarsità di energia (offrendo servizi "a salire"). Per poter fornire questi servizi, un impianto di produzione deve poter garantire la disponibilità di una banda di potenza. Al fine di raggiungere la soglia minima richiesta l'impianto può aggregarsi con altri impianti in una Centrale Elettrica Virtuale: lavorando congiuntamente la Centrale può fornire più risorse e far fronte anche a richieste superiori di potenza da parte del gestore di rete. Eseguendo questi comandi si è remunerati e i ricavi ottenuti dalla commercializzazione di tali servizi vengono suddivisi proporzionalmente al contributo fornito.
Anche i consumatori di energia elettrica possono offrire servizi ancillari: ad esempio, un'industria collegata alla Centrale Elettrica Virtuale può fornire riserva a salire modificando il prelievo in rete a seguito della ricezione del comando da parte della Centrale Elettrica Virtuale.
Attraverso i dati acquisiti in tempo reale nella Centrale Elettrica Virtuale anche i consumatori di energia elettrica, quali clienti industriali e commerciali, possono beneficiare direttamente dell'ottimizzazione economica legata ai prezzi di mercato. Operando in questo modo si può concentrare il consumo nei periodi in cui in borsa il prezzo dell'energia è più conveniente.
Tale ottimizzazione può essere eseguita dalla Centrale Elettrica Virtuale anche in modo del tutto automatico: il sistema di controllo della Centrale Elettrica Virtuale invia impulsi al quadro di controllo dell'azienda, intervenendo naturalmente nei processi soltanto quando è necessario. Infine i nuclei familiari possono essere integrati nelle Centrali Elettriche Virtuali in qualità di consumatori

flessibili, in grado di modulare i propri consumi in funzione dell'andamento dei prezzi dell'energia elettrica.
Le Centrali Elettriche Virtuali assicurano una democratizzazione dell'approvvigionamento energetico che restituisce la centralità alla società: l'operatore di una Centrale Elettrica Virtuale non possiede infatti gli impianti, ma ottimizza soltanto l'esercizio degli impianti di proprietà altrui.
Secondo Navigant Research le VPP invaderanno il mercato nei prossimi anni, tanto che negli Stati Uniti si stima che 28.000 MW verranno gestiti come VPP nel 2023 [34].
La loro diffusione al momento è frenata dalle normative, da problemi di interfacciamento e dai costi dell'elettronica di controllo non ancora standardizzata, ma è ragionevole aspettarsi che nei prossimi anni queste difficoltà verranno superate. Sul mercato esistono già diversi progetti di VPP sviluppati da grandi player caratterizzate da un focus top-down sui parametri tecnici. Negli Usa la Con Edison di New York ha lanciato un programma che coinvolge centinaia di sistemi fotovoltaici abbinati a sistemi di accumulo da gestire in funzione delle esigenze della rete, mentre la Southern California Edison ha fatto un accordo con Nest, che produce termostati wireless intelligenti, per installare 50.000 dispositivi in altrettanti appartamenti, creando una centrale elettrica virtuale con una capacità complessiva di 50 MW.
In Germania, la norvegese Statkraft controlla dai suoi uffici di Düsseldorf un insieme virtuale di ben 9.000 MW, che raggruppa 4.800 aerogeneratori, 100 centrali solari e 12 impianti a biomassa. In Olanda è stata creata una rete di batterie Tesla Powerwall attraverso il programma pilota CrowdNett con l'obiettivo di sviluppare modelli di controllo della domanda elettrica, aggregando diversi dispositivi di energy storage in una sola VPP, in grado di fornire servizi di vario tipo. Sonnen in Germania ha realizzato una vera e propria comunità energetica virtuale, basata sull'energy sharing tra proprietari di batterie Sonnen, che scambiano tra loro l'energia prodotta in eccesso usando la tecnologia blockchain.
Diversamente le iniziative bottom-up o comunitarie di VPP (community-based VPP, c-VPP) sono solo in fase di sviluppo prototipale [35]. Una c-VPP è definita come *"a community owned distributed energy resources aggregated and coordinated by an ICT-based control system, adopted by a (place-based, interest-based, virtual or sectoral) network of people and organizations, who collectively perform a certain role in the energy system. What makes it community-based is not only the involvement of a community, but also the community-logic under which it operates*". A tale riguardo il **progetto europeo Interegg North-West Europe** prevede sviluppi di modelli di c-VPP in Irlanda, Belgio ed Olanda. Una c-VPP può abilitare la comunità di riferimento a generare energia ed immetterla nella rete, gestire e distribuire energia autoprodotta tra i membri della comunità, a scambiare energia sul mercato, vendere flessibilità al mercato supportando il TSO nel bilanciamento della rete, e quindi ad assumere contemporaneamente differenti ruoli, tra cui quello di facilitatore, fornitore, ESCo, aggregatore e DSO (si veda Figura 7).

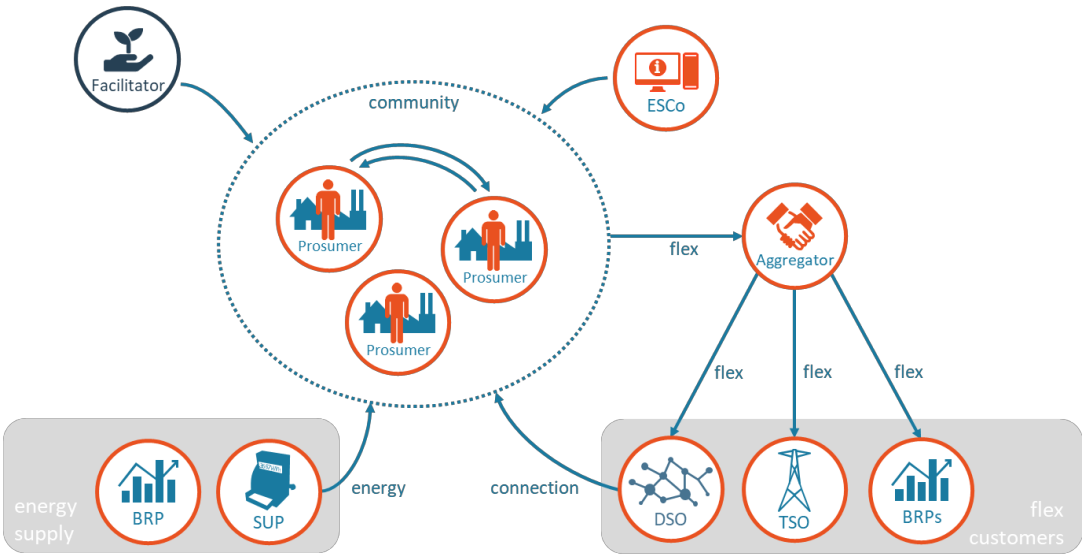

Figura 7. Ruolo della Comunità nel sistema energetico.
Fonte: USEF white paper: Energy and Flexibility Services – February 2019

Community as Facilitator si occupa delle attività che contribuiscono allo sviluppo, all'implementazione e/o all'espansione del c-VPP. Questo ruolo può comprendere un'ampia gamma di attività relative alla diffusione delle informazioni, al finanziamento, alla consulenza, all'organizzazione di acquisti collettivi. Potenzialmente una comunità può facilitare la partecipazione ad un c-VPP gestita da una terza parte, un Aggregatore o una Energy Service Company (ESCo).
Community as Supplier partecipa al trading di energia. Ciò potrebbe includere la fornitura di energia autoprodotta ai membri della comunità, lo scambio di energia autoprodotta sul mercato all'ingrosso e/o facilitare lo scambio di energia all'interno della comunità attraverso una piattaforma dedicata.
Community as Energy Service Company ottimizza i profili energetici individuali e/o comunitari in relazione alla dinamica dei prezzi (demand response) o alla disponibilità di energia prodotta localmente. Gli obiettivi di ottimizzazione sono strettamente correlati agli obiettivi delle comunità, quali ad esempio la riduzione della bolletta energetica, l'autosufficienza e/o la riduzione delle emissioni di carbonio.
Community as Aggregator vende flessibilità aggregata al DSO, TSO o al BRP. Questa flessibilità è impiegata per la stabilizzazione della rete e può essere fornita partecipando al mercato di dispacciamento, con il demand response ed attraverso lo storage.
Community as Distribution System Operator si occupa del bilanciamento e del trasporto di energia elettrica sulla rete locale. La comunità diventa (in parte) responsabile della gestione e della manutenzione della propria (micro) rete.
Nell'ambito del progetto Interreg cVPP, l'implementazione di c-VPP in diversi paesi europei necessita la sperimentazione di nuovi modelli di business. Qui di seguito si riporta l'analisi condotta da Murik, Breukers et al. [35] in cui sono messe a confronto le dimensioni del modello di business ideale, basato su di una logica comunitaria, della c-VPP con le dimensioni di un modello realistico sostenibile nell'attuale contesto istituzionale e normativo (vedi tabella 2).

Tabella 2. Business Model Dimensions Community logic v. Reality Check

Business Model Dimensions	Community Logic	Reality Check
Activities	**Produzione ed offerta locale di energia, storage, vendita della flessibilità al mercato**. **Un sistema di controllo ed una infrastruttura ICT che permetta il *demand response***. La complessità di queste tecnologie dovrebbe riflettere le esigenze, competenze ed ambizioni locali.	**La generazione locale, l'autoconsumo e il trading p2p non è consentito in molti paesi**. I progetti pilota finanziati da Interreg per poter svolgere queste attività si avvalgono di una esenzione temporanea dalla normativa nazionale *Experimental Arrangement*.
Value Proposition	Sviluppo locale, creazione di posti di lavoro, minor costo dell'energia, inclusione sociale, resilienza sociale, democratizzazione del controllo, della proprietà, del processo decisionale; bolletta energetica più bassa, riduzione delle emissioni inquinanti.	Fornitura affidabile; servizi di rete; differimento degli investimenti di rete; capacità di riserva primaria e secondaria; *demand response flexibility*; riduzione delle congestioni di rete; migliore previsione dei carichi; semplificazione della comunicazione
Resources	Contributi volontari basati sulle competenze e risorse finanziarie dei membri della comunità che agiscono in qualità di gestori. L'esternalizzazione non dovrebbe rappresentare una prima opzione.	Coerentemente con lo **shift della *value proposition* le risorse e competenze locali non sono più sufficienti**. La maggiore complessità e dimensione del progetto implica il ricorso alle **esternalizzazioni e a finanziamenti esterni.**
Customer Segment	Un modello di business basato su una logica comunitaria mira in *primis* a servire la comunità. I **clienti di Una c-VPP dovrebbero esserne anche i proprietari**. In caso di **surplus energetico il modello prevede che l'energia sia venduta esternamente ad una società cliente**.	Per vendere energia sul mercato la cVPP dovrebbe avere una dimensione rilevante in termini di fonti rinnovabili collegate o vendere il proprio surplus ad un fornitore autorizzato che diventerebbe un cliente della c-VPP. Analogamente la c-VPP dovrebbe vendere la flessibilità ad un cliente aggregatore. Nella stessa misura in cui la proposizione di valore si sposta dalla comunità agli stakeholder istituzionali questi stessi, **DSO e TSO rischiano di diventare i clienti target del modello**.
Relations	**Coinvolgimento della comunità locale** nel processo decisionale relativo alle **scelte di *make or buy* e alla selezione delle tecnologie da impiegare.**	Tra i clienti della comunità rientrano fornitori di elettricità ed aggregatori, le relazioni complesse richiedono l'esternalizzazione di alcune attività con un capovolgimento del modello: **i membri della comunità diventano azionisti e risorse per stakeholder istituzionali anziché essere i proprietari delle idee** e degli asset perdendo la capacità di influenzare la gestione dell'energia all'interno della comunità.
Channels	**Canali di interazione diretti,** si attiverebbero attraverso l'amministrazione e la gestione quotidiana del cVPP e attraverso le assemblee degli azionisti.	**I canali diretti di interazione personale diventano meno importanti** (in quanto i membri fondatori della cVPP devono interfacciarsi con una varietà di stakeholder esterni da cui dipende la realizzazione del progetto) e più simili alle interazioni commerciali tra i fornitori di energia e i loro clienti.
Partners	Membri della comunità, provider tecnologici locali, partner di filiera, finanziatori.	**Una cVPP per sopravvivere deve collaborare con il DSO** (che supporta l'integrazione delle fonti energetiche rinnovabili e dispone di informazioni sullo stato della rete) e con i **grandi fornitori autorizzati** ad operare sul mercato. Questo tipo di partnership è l'unico modo per evitare costi e conseguenze organizzative derivanti dal dover rispettare la normativa sui meccanismi di bilanciamento. **La creazione di una relazione di dipendenza con questi partner rischia di minare il ruolo**

		(influenza, autonomia) della comunità e dei suoi membri.
Costs	Costi per lo studio di fattibilità e di progettazione, costi per l'approvazione del piano regolatore, costi di capitale per la costruzione e l'installazione del cVPP, i costi di partecipazione al mercato, i costi di gestione e manutenzione, di investimento per migliorare o ampliare la cVPP.	Dovendo diventare fornitore a livello nazionale o comunque partecipando in altro modo al mercato dell'elettricità, **la c-PVV**, al fine di coprire i costi per soddisfare i requisiti necessari, **deve aumentare significativamente la propria clientela o trovare nuovi investitori**.
Revenues	Contributi dei membri della comunità in cambio di quote societarie; contratti con fornitori ai quali la cPVV dovrebbe vendere il proprio surplus energetico, sussidi.	Le modifiche al BM comporteranno un altro tipo di entrate legate alla vendita di energia e di flessibilità agli operatori istituzionali che difficilmente potranno anche essere destinate al soddisfacimento dei bisogni comunitari.

6.2.3 Energy Community basate su Piattaforme di trading Peer to Peer

Una EC distribuita può essere basata su una piattaforma software di trading che grazie ad un'infrastruttura elettrica intelligente abbina gli acquirenti di energia rinnovabile con i fornitori locali. In questo caso l'obiettivo principale della EC è lo sharing energetico. La piattaforma fornisce il servizio di intermediazione tra domanda ed offerta di energia e può pertanto coinvolgere sia prosumer che consumatori. Questo richiede un alto grado di coordinamento tra la piattaforma tecnologica, le utility ed i clienti per consentire le transazioni fisiche e finanziarie (metering e billing) questo spinge verso un potenziale cambiamento dei ruoli degli attori all'interno del mercato elettrico.

Diversamente dalle VPP che possono essere coordinate per fornire un'offerta elettrica extra alla rete le piattaforme di trading P2P offrono prevalentemente benefici transazionali ai consumatori finali quando sottostanno ad una struttura inefficiente delle tariffe e possono creare incentivi all'istallazione di energia distribuita. Le piattaforme di trading P2P devono affrontare sfide simili ad altre piattaforme aperte tipo Uber o Linux, dovute alla forte resistenza delle coalizioni politiche ed economiche ben insediate, dato che potrebbero erodere i margini di profitto delle utility dominanti, soprattutto in considerazione del fatto che la rete potrebbe moltiplicare rapidamente raggiungendo altre comunità attraverso una piattaforma open.

Il **Basselton lifestyle village** [21]. australiano è stato avviato da una start up di Pert per testare il trading peer to peer sulla rete elettrica occidentale. La piattaforma di prova sarà implementata attraverso la tecnologia blockchain che permetterà di identificare la proprietà dell'energia prodotta e quindi di gestire molteplici accordi commerciali tra le parti. La piattaforma consentirà ai clienti con generazioni solari di vendere l'energia in eccesso ad altri utenti del programma ad una velocità superiore a quella di esportazione in rete, senza l'aggiunta di oneri di reti e di margini commerciali. Il trading P2P rappresenta un nuovo modello di business che non solo consente la creazione di valore comune aumentando il tasso di impiego degli asset e lo scambio di servizi, ma apporta benefici economici alle comunità locali, rappresentando un'opportunità di business per imprenditori tecnologici ed utility lungimiranti. Questi modelli potrebbero essere implementati in comunità dove è presente una generazione distribuita sottoutilizzata per fornire energia rinnovabile in maniera affidabile conveniente ai consumatori favorendo la transizione verso un sistema energetico più distribuito dinamico e partecipativo. La piattaforma di trading P2P può abilitare gli scambi all'interno di una microgrid virtuale o tra differenti microgrid.

6.2.4 Community Microgrid

Con il termine di microgrid ci riferiamo ad una molteplicità di utenze elettriche attive e passive, riunite sotto un unico punto di connessione (Point of Common Coupling o PCC) con la rete elettrica

di distribuzione, le varie unità di produzione e consumo devono essere collegate non solo dal punto di vista elettrico, ma anche attraverso un sistema di comunicazione su cui opera il Microgrid Energy Manager [36].

Un "raggruppamento localizzato di fonti e carichi elettrici" che può o meno essere collegato a una rete elettrica più grande. Le microgrid possono essere completamente autonome o "incorporate" all'interno di infrastrutture esistenti, consentendo loro di attingere alla rete elettrica in caso di deficit energetico di vendere energia elettrica alla rete di maggiori dimensioni in caso surplus energetico. Sono viste come una strategia per ridurre il decentramento introdotto dalle fonti di energia rinnovabile attraverso nuovi concetti di controllo.

Le microgrid comunitarie sono progettate per servire una determinata comunità rappresentano un nuovo approccio per la progettazione e la gestione della rete elettrica, basandosi fortemente sulle fonti rinnovabili per ottenere un sistema energetico più sostenibile, sicuro ed economico, fornendo al contempo energia di backup a tempo indeterminato, guidata da fonti rinnovabili per i carichi prioritari. L'obiettivo quello di mettere a fattore comune le risorse locali (principalmente energie rinnovabili su piccola scala) per massimizzare l'autosufficienza energetica. Possono anche essere costruite per ragioni finanziarie, come i prezzi elevati dell'elettricità sulla rete principale.

La **Goleta Load Pocket Community Microgrid** (GLPCM) rappresenta un sistema di alimentazione all'avanguardia. La Goleta Load Pocket, un tratto di 70 miglia di costa della California meridionale, soggetto a disastri e alla trasmissione di vulnerabilità, offre l'opportunità perfetta per una microgrid comunitaria che garantisce all'area vantaggi economici, ambientali e di resilienza. Una Community Microgrid può isolarsi dalla macrogrid durante un'interruzione di corrente - che sia causata da un disastro naturale, o da qualsiasi altro evento - fornendo energia di backup a tempo indeterminato basata sulle energie rinnovabili per le strutture critiche della comunità, come le stazioni dei vigili del fuoco e i rifugi di emergenza. Durante le normali operazioni di rete, il GLPCM continua a fornire alla comunità i benefici dell'energia locale pulita [37]

Mentre le microgrid fisiche sono ancora rare si osserva uno sviluppo di microgrid virtuali attraverso l'impiego del trading peer to peer abilitato dalla tecnologia blockchain che fornisce una piattaforma affidabile a basso costo per effettuare, convalidare, registrare, regolare le transazioni energetiche in tempo reale attraverso un sistema energetico localizzato e decentralizzato.

In seguito all'uragano Sandy la municipalità di NY ha incentivato lo sviluppo delle community microgrid in grado di rendersi indipendenti in caso di emergenza. Da questo stimolo è nato a **Brooklyn il progetto** di **LO3 Energy** la start up che ha attivato nel 2016 la prima grid peer to peer basata su blockchain che permette di condividere l'energia elettrica, prodotta mediante pannelli fotovoltaici, tra gli edifici di quartiere interconnessi (**BMG**). La piattaforma fornisce il servizio di intermediazione tra domanda ed offerta di energia e può pertanto coinvolgere sia prosumer che consumatori. Ciò richiede un elevato livello di coordinamento tra la piattaforma tecnologica, le utility ed i clienti per garantire le transazioni fisiche e finanziarie. Gli obiettivi sono quelli di una migliore utilizzazione degli assets e di una diminuzione delle bollette energetiche.

All'interno della BMG l'utilizzo di smart metering abilitati alla blockchain permette di gestire in modo automatizzato gli scambi di energia tra gli utenti senza l'intervento di un ente centrale. I membri della community mediante un'applicazione gestiscono le proprie preferenze di prezzo, saranno poi gli smart meter a gestire i flussi energetici all'interno della rete avviando la vendita/acquisto di energia sulla base delle preferenze presenti all'interno degli smart contract. La microgrid di Brookling basandosi su una rete di distribuzione già esistente permette ai partecipanti della community di rimanere collegati alla rete per gestire surplus/deficit della microgrid stessa.

Data la crescente domanda di una maggiore flessibilità dell'energia offerta ci si attende una continua crescita delle microgrid virtuali ed una graduale evoluzione delle microgrid fisiche lungo i seguenti fasi [38]:
La prima fase di sviluppo, è quella attualmente in corso di realizzazione, a titolo esemplificativo, nell'ambito della Brooklyn Microgrid (BMG), che presenta alcuni tratti di una vera e propria microgrid in termini di località, ma è ancora completamente collegata alla rete elettrica.
Una seconda fase inizierebbe con l'introduzione del demand response, il che significa che i partecipanti possono accettare che alcuni dei loro apparecchi siano accesi e spenti dal gestore di rete per consentire un migliore equilibrio tra domanda e offerta.
Una terza ed ultima fase comporterebbe la disconnessione della microgrid dalla rete elettrica nazionale e l'obbligatorietà del demand response con un meccanismo di tariffazione integrato per determinare quali apparecchi possono essere spenti con priorità e delle eccezioni, in cui i prosumer pagano una tariffa extra per non rispettare le regole di demand response (ad esempio, prendere una decisione a breve termine per mantenere un apparecchio acceso).
Oltre alla tecnologia dell'internet degli oggetti (IoT) e della tecnologia Machine to Machine (M2M), un fattore chiave per consentire questa evoluzione sono gli smart contract, ovvero contratti a prova di manomissione che vengono attivati automaticamente attraverso il monitoraggio in tempo reale delle transazioni. Quando una serie di requisiti predefiniti si verifica, come il bilanciamento dell'energia in una rete peer-to-peer, uno smart contract viene creato ed eseguito ad un prezzo determinato automaticamente.
Per i paesi con un approvvigionamento energetico affidabile si prevede che un passaggio alle microgrid possa portare a i benefici in termini di riduzione dei costi energetici, offrendo due opportunità chiave:

- **Eliminazione dei costi di distribuzione**: in sostanza, l'attuale ruolo del distributore di energia elettrica diventerebbe ridondante;
- **Riduzione dei costi di capacità**: la capacità della microgrid di rispondere rapidamente ai cambiamenti dell'offerta attraverso una demand/response intensiva ridurrà la quantità e quindi i costi della produzione di riserva energetica. L'entità di questo risparmio sui costi crescerà man mano che si passerà ad una maggiore proporzione di produzione intermittente di energia rinnovabile.

6.2.5 Integrated Community Energy Systems

Un sistema integrato di gestione delle risorse urbane, che non solo fornisce l'approvvigionamento energetico, ma può riguardare anche la gestione di edifici efficienti, la cogenerazione, la produzione di acqua, la gestione dei servizi igienici, dei trasporti e dei rifiuti per aumentare l'efficienza energetica e ridurre le emissioni di gas ad effetto serra a livello locale. Un ICES cattura tutti gli attributi delle diverse opzioni di integrazione dei sistemi energetici applicandoli a livello comunitario. Mendes et al [39]. definiscono un IECS un approccio multiforme per soddisfare il fabbisogno energetico di una comunità locale attraverso la cogenerazione o la trigenerazione ad alta efficienza, nonché attraverso tecnologie energetiche rinnovabili combinate a soluzioni di storage innovative come l'impiego della batteria a dei veicoli elettrici per i servizi di rete e misure di demand-side management. I sistemi integrati di comunità energetiche contribuiscono ad accrescere l'autoconsumo e favoriscono la combinazione tra domanda ed offerta energetica a livello locale avendo come obiettivo l'autosufficienza. Koirala et al. [40] nel valutare un ICESs individuano i seguenti criteri: prossimità, modularità, flessibilità, intelligenza, sinergia, coinvolgimento del cliente ed efficienza.

- ***Locality****: the system should have a larger proportion of local investment and ownership. It should be operated locally. Local generation should be used for self-provision through local energy exchange;*
- ***Modularity****: the system should be able to cope with entry and exit of its members. House hold and community level technologies could be added later to adapt with rising demand;*
- ***Flexibility****: one of the important criteria for ICES is flexibility, which can be achieved through local demand response, local balancing, flexible load and supply. This flexibility can be utilized to provide energy and system services;*
- ***Intelligence****: for the co-ordination of energy and information flow to match supply and demand locally, ICESs should be intelligent;*
- ***Synergy****: the system should allow synergies between different sectors such as electricity, heat and transport as well as between different technologies;*
- ***Customer*** *engagement: the system should engage customers through different means such as investment, ownership, local energy exchange and economic incentives;*
- ***Efficiency****: the system should be both technically as well as economically efficient.*

Le attività di un sistema energetico integrato di comunità possono riguardare la generazione locale, lo storage, il demand response, gli acquisti collettivi di energia ed il trading di energia. Un ICES può essere maggiormente focalizzato sulle attività dal lato dell'offerta (gli acquisti in comproprietà degli impianti di generazione) e/o sulle attività dal lato della domanda (come il risparmio energetico, l'ammodernamento delle abitazioni, le iniziative di sensibilizzazione energetica). Gli ICES posso avere diversa ampiezza ed essere o meno collegati alla macrogrid.

Il coinvolgimento della comunità locale anche in questo caso ha un ruolo critico nella riuscita del progetto. Costituisce infatti un prerequisito di un sistema energetico integrato di comunità un elevato coinvolgimento dei membri a livello locale nella pianificazione, nello sviluppo e nell'amministrazione del progetto energetico così come nella distribuzione dei benefici da esse derivanti.

Gli **incentivi economici**, in termini di risparmi energetici e di distribuzione degli utili derivanti dalla partecipazione alle cooperative energetiche, accrescono l'interesse delle persone in questa tipologia di investimento. Nei paesi sviluppati i consumatori sono disposti a pagare un prezzo più alto per l'energia autoprodotta da fonte rinnovabile tuttavia è importante garantire, attraverso un'adeguata mappatura di tutti gli interessi in gioco, che i costi e benefici del progetto siano condivisi equamente tra i partecipanti facendo in modo che chi non è coinvolto non si appropri di parte di essi [41].

L'autonomia energetica e la **riduzione della povertà energetica** sono dei drivers chiave per i sistemi energetici locali. Gli ICESs possono utilizzare le risorse disponibili localmente in modo sostenibile riducendo la dipendenza dall'importazione da fonti fossili attraverso un consumo locale intelligente, sistemi comunitari di storage ed unità flessibili di cogenerazione. Una **delle principali barriere per i sistemi integrati comunitari sono gli elevati costi di** investimento per gli adeguamenti dell'infrastruttura di rete. Maggiori studi finalizzati a dimostrarne la convenienza economica potrebbero contribuire ad aumentare la bancabilità di questi progetti. Oltre ad aumentare l'efficienza e l'affidabilità nell'approvvigionamento energetico locale gli ICESs sono considerati un'alternativa sostenibile rispetto ai sistemi di generazione centralizzati. Webster et al. [42] stimano che in Canada i sistemi energetici integrati possano ridurre entro il 2050 le emissioni di CO2 dal 5% al 12% annuo.

Feldheim è un villaggio a 60 km da **Berlino** di 37 case che rappresenta un esempio di successo di un ICESs, decentralizzato ed autosufficiente in un paese sviluppato. Feldheim è organizzato in una cooperativa energetica locale gestita dalla compagnia energetica Energiequelle. Le prime istallazioni

di turbine a vento nel villaggio risalgono al 1995. Il sistema energetico è cresciuto rapidamente raggiungendo la capacità istallata di 81.1 MW di turbine a vento, 2.25 MW di fotovoltaico e 500 kWe/500kWt di biomassa per il riscaldamento e la conservazione di energia nel distretto. Il tentativo fallito di acquistare o di prendere in leasing la rete di distribuzione posseduta da E.ON ha spinto Feldheim ha costruire la propria rete finanziata da Energiequelle, con sovvenzioni europee, capitale di prestito e contributi individuali. Questo sistema energetico alternativo nella forma di ICESs ha avuto come risultato una riduzione del costo dell'energia fissato dalla cooperativa indipendentemente dai prezzi che si formano sul mercato all'ingrosso. Feldheim è autosufficiente in termini energetici e dipende dalla macrogrid solo per l'esportazione di energia e per l'erogazione dei servizi di rete [43].

La **cooperativa Urja Upatayka** in **Nepal** è un esempio rappresentativo di ICESs in un paese in via di sviluppo. Sei micro-impianti idroelettrici sono stati integrati nel 2011 con finanziamenti esterni. La cooperativa funziona come operatore di rete e distributore mentre le sei unità lavorano come un unico impianto di produzione. Urja Upatayka acquista elettricità dalle 6 unità di generazione a 5 centesimi di euro al KW h e la rivende ai consumatori ad 8 centesimi, usando la differenza per mantenere e gestire il sistema. Con una rete di distribuzione lunga 8km il sistema fornisce elettricità a 1200 famiglie. Grazie all'integrazione la qualità, affidabilità e la disponibilità di elettricità è migliorata mentre la rete nazionale del Nepal soffre di una riduzione del carico fino a 16 ore al giorno [41].

Nonostante i sistemi energetici integrati di comunità si prestino, per la loro natura, ad applicazioni blockchain nei diversi pillar esaminati, ad oggi non sono stati individuati progetti pilota di blockchain-based ICESs.

6.3 Analisi SWOT per le tipologie di EC

Avendo esaminato le tre tipologie di comunità energetiche ed i modelli in cui si possono concretizzare: Centralizzate (Community–based Project), Distribuite (VPP e c-VPP) e Decentralizzate (Community Microgrid, che ICESs) è possibile confrontarle con il paradigma attuale ed evidenziarne punti di forza e di debolezza nonché le minacce ed opportunità legate all'attuale contesto di riferimento [21].

Tabella 3. Analisi SWOT per Tipologie di Energy Community

Fonte: rielaborazione "Typology of future clean energy communities: An exploratory structure, opportunities, and challenges", Energy Research & Social Science, Gui et al (2017)

	Current Utility Model	**Comunità Energetiche Centralizzate**	**Comunità Energetiche Distribuite**	**Comunità energetiche Decentralizzate**
Strengths	**Economie di scala**; modello consolidato e collaudato; gode del supporto/accettazione da parte di players istituzionali, utility e mondo accademico.	**Facilmente integrabile** nel regime esistente centralizzato; utilizzo di tecnologie mature e a basso rischio; investimenti collettivi, comproprietà degli asset. Tipologia più conosciuta meglio compresa dall'industria e dal mondo accademico.	**Investimenti distribuiti** da parte degli utenti in base a preferenze e disponibilità individuali. Comunità virtuali coordinate dall'organizzazione di hub in VPP o tramite piattaforme di trading P2P che non richiedono la prossimità fisica dei membri.	**Infrastrutture energetiche locali**/regionali funzionali agli obiettivi locali economici e sociali e all' efficienza energetica nel lungo periodo; la gestione locale crea occupazione; responsabilità ben definite degli stakeholder nel processo decisionale.
Weaknesses	Il **processo decisionale centralizzato** fornisce soluzioni top-down che non sono necessariamente in grado di massimizzare il benessere sociale.	Richiesto un **elevato livello di coesione** comunitaria; potrebbe non essere considerato prioritario dalle utility nell'organizzare la connessione e l'accesso alla rete dei membri.	**Nuova piattaforma** che si basa su infrastrutture tecnologiche specializzate, organizzazione di hub da parte di utility, broker e aggregatori.	**Grandi investimenti in CAPEX** in nuove infrastrutture, o nella riconfigurazione di infrastrutture esistenti; assenza di economie di scala nella gestione dell'infrastruttura di

				rete; necessaria una nuova piattaforma tecnologica gestita da provider tecnologici per fornire energia e servizi integrati
Opportunities	**Spinta** da parte di utenti, comunità e governi **per una maggiore efficienza**, ad esempio sperimentando nuove tecnologie, nuovi modelli di business in grado di influenzare il processo decisionale e normativo.	La **forma più comune** e meglio conosciuta di integrazione di risorse energetiche rinnovabili; i nuovi progetti possono essere migliorati sulla base delle **lezioni apprese nel corso delle passate esperienz**e.	Migliore **utilizzo degli asset e sharing di servizi energetici**; opportunità di business per imprenditori ed utility lungimiranti.	Pianificazione della infrastruttura locale in accordo con la pianificazione nazionale per una **maggiore efficienza, autosufficienza energetica e per il benessere sociale locale**; opportunità di business per imprenditori ed utility.
Threats to change/ up-scaling	**Inerzia del modello**; nuove tecnologie/e modelli di business emergenti che minacciano la posizione ed i profitti degli operatori tradizionali.	**Limitata capacità di innovare** e di influenzare il processo di cambiamento; non è adatta a comunità remote/isolate con accesso limitato alle infrastrutture di rete.	**Complessità tecnica; problemi di regolamentazione** dovuti agli effetti derivanti dalla ridondanza delle imprese di rete e dei distributori.	**Requisiti patrimoniali elevati, complessità tecnica**, coordinamento di una varietà di soggetti interessati con interessi diversi.

Il passaggio al nuovo paradigma energetico, decentralizzato, decarbonizzato e digitalizzato di produzione e distribuzione dell'energia, richiede una pianificazione ed un coordinamento prudente, sostenuto da obiettivi sociali e governativi incrementali, che tengano in considerazione la varietà delle tecnologie disponibili, gli aspetti culturali delle comunità e che prevedano lo sviluppo di nuovi modelli di business.

Il successo della transizione richiede una comprensione più chiara della dimensione sociale oltreché infrastrutturale dei diversi percorsi possibili. I fattori chiave da considerare nel valutare il potenziale delle diverse tipologie di comunità nell'accelerare il passaggio al nuovo paradigma energetico possono essere rintracciati nella **capacità della comunità di realizzare un'innovazione sociale e collaborativa e di promuovere un'interazione sinergica tra attori e le istituzioni**. Le EC distribuite e decentralizzate, per le caratteristiche sopra descritte, sembrano essere la tipologia di comunità energetica più adatta ad innescare il processo di trasformazione auspicato. Le EC distribuite rappresentano di per sé nuovi modelli di business che creano valore garantendo un migliore impiego degli asset ed il trading di servizi, distribuendo benefici economici ai membri della collettività. Le EC decentralizzate nonostante siano caratterizzate da un'elevata complessità tecnica e da ingenti investimenti in capex, rispetto alle EC distribuite, sono tuttavia localizzate in un'area geografica ben definita e come è noto la prossimità fisica facilità l'innovazione collaborativa (come lo sharing di servizi energetico-sociale). Differentemente dalle EC centralizzate, per la necessità di mobilizzare ingenti risorse finanziarie, le EC decentralizzate richiedono una struttura di governance in grado di coinvolgere i principali stakeholders tra cui le istituzioni, i rappresentati della comunità, i fornitori di servizi. Il coinvolgimento di gruppi di attori diversi con differenti motivazioni favorisce l'apprendimento, il networking e la propensione al cambiamento.

7. COMMUNITY INCLUSIVE CURRENCY (CIC)

7.1 Definizioni e tipologie

L'innovazione sociale collaborativa e tecnologica combinate insieme con la pressione socio-politica per un approvvigionamento energetico più pulito possono generare un cambiamento strutturale ed istituzionale nell'attuale regime centralizzato di fornitura di energia elettrica verso un futuro regime energetico distribuito e decentralizzato. **Le comunità energetiche rappresentano il terreno fertile per lo sviluppo di tutte le tre dimensioni dell'innovazione necessarie al cambiamento auspicato**.
Le valute comunitarie possono essere considerate un'innovazione sociale e collaborativa, uno strumento per il rafforzamento economico e sociale delle comunità in cui viviamo che attiva una rete di solidarietà fondata sullo 'scambio alla pari di prestazioni e servizi' capaci di soddisfare bisogni legati alla vita quotidiana e al lavoro di assistenza come nessun servizio pubblico può fare. Un modo per potenziare la rete di reciproco aiuto tipica dei rapporti di buon vicinato [12].
Pur avendo un'origine antica hanno ripreso a diffondersi a livello globale in seguito alla crisi finanziaria del 2008 assumendo sempre più frequentemente la forma di valute digitali e negli anni più recenti di criptovalute.
Il termine moneta complementare si riferisce a tutte quelle monete che non godono del regime di corso forzoso, e che svolgono quindi un ruolo supplementare rispetto alla valuta ufficiale. Le valute locali invece possono essere definite come un tipo particolare di moneta complementare, la cui circolazione è delimitata ad una zona geografica ben definita. Nella lingua italiana come in quella inglese si è soliti utilizzare i due termini come sinonimi.
Secondo M. Amato e L. Fantacci [44] la moneta non è sempre in grado di svolgere adeguatamente tutte le sue funzioni (unità di conto, mezzo di scambio e riserva di valore). Il fenomeno del credit crunch ne è una dimostrazione: la moneta tende ad essere tesaurizzata e sottratta alla circolazione, perché appare come la forma più sicura di detenzione della ricchezza, tanto per gli individui quanto per le banche, che saranno disposte a separarsene solo in cambio di un tasso di interesse molto elevato. Così, da mezzo di scambio la moneta diventa una riserva di valore, creando quindi una "divergenza tra l'interesse individuale a tesaurizzare e l'interesse collettivo alla sua circolazione". Le monete complementari nascono con l'obiettivo di uscire dalla cosiddetta trappola della liquidità - concetto ipotizzato da J.M. Keynes, negli anni trenta nel definire la sopravvenuta incapacità della politica monetaria di determinare una crescita della domanda e quindi di influenzare lo sviluppo economico – e sono concepite come mezzi di scambio, utili soprattutto a rilanciare la crescita produttiva o il pieno impiego di tutte le risorse disponibili, sebbene ciò avvenga in genere su una scala molto ridotta.
Blanc [45] individua tre **modelli di moneta complementare**:

- **Local currency**: implementata in uno spazio geopolitico ben definito che si propone come supplementare alla moneta nazionale con l'obiettivo di risollevare il tessuto economico-sociale in cui viene creata. Sono di solito emesse da un'autorità centrale che si incarica di immettere e ritirare la liquidità dal sistema. Tramite questa attività l'autorità locale può avviare un processo redistributivo;
- **Community currency**: introdotte all'interno di singole comunità per favorirne il benessere, lo scambio sociale e la tutela ambientale;
- **Complementary currency**: perseguono finalità esclusivamente economiche. Il principale obiettivo è quello di aumentare gli scambi seguendo le regole del mercato.

Focalizzandosi sulle valute complementari nate dopo gli anni ottanta Blanc propone una diversa classificazione individuando **4 generazioni di valute complementari**:

- Mutual Credit: è un sistema a **compensazione multilaterale** creato per la prima volta in Canada nel 1982 con il **LETS (Local Exchange and Trading System)** finalizzato a risolvere il problema della penuria di liquidità nelle zone con alta disoccupazione. La compensazione multilaterale si avvale di una moneta scritturale e inconvertibile che dovrà essere riutilizzata all'interno del circuito in cui è stata creata. Il sistema consente agli aderenti di scambiarsi e compensare le reciproche ragioni di debito e di credito provvedendo al regolamento dei soli saldi finali a chiusura del ciclo operativo. I saldi possono essere calcolati su base bilaterale o su base multilaterale (nei confronti del sistema nel suo complesso). Si tratta in genere di monete comunitarie emesse da organizzazioni no-profit;
- Sistemi di valute complementari che impiegano il **tempo** come mezzo di scambio inconvertibili in valuta ufficiale. In Giappone, i Fureai Kippu elettronici sono versati in un conto di risparmio automatizzato agli individui che aiutano anziani o disabili, riguardo ad ogni aspetto della loro cura che il sistema sanitario nazionale giapponese non copre. L'unità di conto del Fureai Kippu è l'ora di servizio. Ci sono tassi differenti applicati a servizi differenti. Questi Fureai Kippu possono essere conservati o trasferiti a chi ha bisogno di assistenza;
- Il terzo tipo di valuta prende piede negli anni novanta con le Ithaca hours, create con **finalità economiche in uno spazio geopolitico definito**. Queste valute sono ancorate alla moneta ufficiale tramite un rapporto di cambio fisso e sono convertibili dietro il pagamento di una commissione. L'impiego avviene in concomitanza con la moneta ufficiale al fine di incrementare la produzione e gli scambi locali per mitigare la delocalizzazione industriale. Richiedono una forte partnership con le imprese del territorio e le autorità governative. Un altro valido esempio è rappresentato dal Bristol Pound;
- La quarta generazione prende vita a Rotterdam nel 2002 con le NU il cui scopo è quello di incentivare la **sostenibilità ambientale**. Usando il trasporto pubblico, acquistando dispositivi ad efficienza energetica, praticando il car-sharing, vengono caricati su una smartcard dei "greenpoints". Questi punti possono essere usati poi per ottenere sconti nello stesso tipo di attività, incentivando comportamenti ecologicamente responsabili.

Diversi fattori ricorrenti differenziano questi strumenti di pagamento dalla moneta ufficiale nazionale:

- Il **corso su base volontaria**, che si distingue dal corso legale della valuta nazionale riconosciuta dall'autorità statale come mezzo di pagamento;
- La presenza di **incentivi alla circolazione**, che possono assumere la forma di un interesse passivo per chi tiene ferma per troppo tempo la valuta (***demurrage***), una data di scadenza, limitandone così la funzione a mezzo di pagamento ed evitando la stagnazione dell'economia;
- Il **profilo spiccatamente locale** affinché la ricchezza prodotta rimanga in loco anziché uscire dal contesto comunitario.

Come è evidenziato nello studio di Amato e Fantacci [44] lo stato attuale delle conoscenze non consente di stabilire in termini esatti il numero dei sistemi di moneta complementare oggi attivi, ma ci fornisce l'indicazione di una certa varietà di schemi, che poggia su uno spirito spontaneo d'innovazione istituzionale. Una spontaneità che spesso è stata sacrificata in nome di istanze di accentramento, e che invece andrebbe salvaguardata, incoraggiata e opportunamente indirizzata,

per evitare che risulti inadeguata rispetto alle stesse esigenze di sostegno dell'economia a cui vorrebbe rispondere.
Il ruolo della valuta comunitaria è quello di mettere in relazione dei bisogni insoddisfatti con risorse che altrimenti rimarrebbero improduttive. Possono esistere diversi tipi di bisogni insoddisfatti: sociali, economici e commerciali, ecologici, culturali educativi. Le risorse inutilizzate sono le più svariate: i tavoli non prenotati di un ristorante, gli edifici non ancora occupati, i disoccupati, i pensionati. L'idea alla base delle valute comunitarie e di mettere in relazione risorse e bisogni in modo tale ad esempio che i posti rimasti liberi in uno stadio possano essere occupati da chi si è reso disponibile per un servizio di baby-sitting.
Nella maggior parte dei casi, le valute complementari appartenenti alle ultime generazioni, hanno come obiettivo lo sharing di competenze, abilità, la promozione di rapporti solidali e comportamenti virtuosi da un punto di vista ambientale e sociale per la valorizzazione delle risorse disponibili ed inutilizzate assumendo sempre di più la connotazione di monete ad inclusione sociale. Nell'ambito di una comunità energetica la diffusione di una valuta complementare con obiettivi di inclusione sociale, oltreché di sharing energetico può innescare un circolo virtuoso di reciprocità in grado non solo di garantire il coinvolgimento e la partecipazione necessaria di tutti i membri al successo del progetto energetico ma anche di mobilitare beni e risorse che altrimenti resterebbero inutilizzati per soddisfare i bisogni comunitari di altra natura.
La più recente evoluzione delle valute complementari è rappresentata dalla possibilità di usare soluzioni basate su piattaforme web e cripto valute impiegando la **tecnologia blockchain.**
Esistono già diversi progetti in cui la tecnologia blockchain è impiegata per lo sviluppo di community currency. Uno di questi esempi è noto come **Hull Coin**, sviluppato nella città portuale di Hull nello Yorkshire grazie ad un finanziamento governativo di 240.000, 00 sterline. Hull Coin è il risultato di una ricerca condotta dal consiglio comunale di Hull che ha indagato su come la tecnologia potesse essere impiegata per sviluppare una valuta locale in grado di sostenere la comunità colpita dalla povertà. La tecnologia blockchain ha permesso di incorporare nella stessa moneta le prove del risultato sociale di qualsiasi attività intrapresa nella comunità creando un registro distribuito di tutte le attività socialmente rilevanti intraprese dai membri ed offrendo alle persone un CV sociale utile nella ricerca di un nuovo impiego. InvolveMINT è un'altra valuta locale, operativa a Pittsburg basata su blockchain che viene utilizzata per scopi sociali. **InvolveMINT** consente ai membri della comunità di trovare opportunità di volontariato a cui dedicare il proprio tempo guadagnando una criptovaluta per ogni ora di lavoro dedicata. La blockchain è impiegata per tracciare le competenze ed i servizi resi nel tempo dai membri della community. Bancor, l'exchange decentralizzato di criptovalute in partnership con Grassroots Economics sta lanciando una blockchain-based community currency per combattere la povertà in Kenia. Il nuovo progetto dell'azienda ha l'obbiettivo di stimolare il commercio locale e regionale e le attività peer-to-peer, consentendo così alle comunità del Kenya di creare e gestire i propri token digitali.

7.2 Gli obiettivi

Le valute complementari o locali possono avere una molteplicità di obiettivi.
Quelle con uno scopo commerciale sono principalmente di quattro categorie:

- Business to Business (B2B): generalmente create dalle aziende per facilitare gli scambi con fornitori e clienti all'ingrosso;
- Business to Consumer (B2C): monete di fidelizzazione emesse da un'azienda o da un gruppo di aziende (frequent flyer);

- Consumer to Business (C2B): basate su circuiti di commercio e consumo. I consumatori acquistano la valuta complementare con valuta convenzionale ricevendo un premio. La valuta è impiegata per pagare beni e servizi forniti dalle aziende aderenti;
- Consumer to Consumer (C2C): Si tratta di monete volte a permettere scambi tra singoli individui, come accade in molte comunità virtuali – fenomeno cresciuto a dismisura con la sempre più elevata penetrazione di internet nei paesi industrializzati. Una moneta virtuale si caratterizza in base al suo rapporto con la moneta ufficiale: può essere una moneta virtuale chiusa (ottenuta e spesa solo all'interno della comunità virtuale di riferimento, come nel caso del popolare World of Warcraft), una moneta virtuale a flusso unidirezionale (come i Wii Points della Nintendo, che possono essere acquistati con moneta ufficiale ma non possono essere riconvertiti), o una moneta virtuale a flusso bidirezionale (come i Linden Dollars, la valuta del social network Second Life, che possono essere scambiati nuovamente in moneta ufficiale una volta acquistati). Un esempio famoso in questo particolare ambito è il Bitcoin. I Bitcoin sono creati attraverso un algoritmo informatico, possono essere acquistati con moneta ufficiale e possono essere spesi per comprare servizi online o beni tangibili. Tuttavia, il loro utilizzo prevalente sembra essere per scopi speculativi, vista l'elevata oscillazione del loro controvalore in dollari;
- Circuiti commerciali misti misti: come il WIR in Svizzera ed i Sardex in Italia. Il Sardex è un circuito di credito commerciale nato nel gennaio 2010, cui aderiscono oggi oltre 1300 imprese sarde. Quando un'azienda entra a far parte del circuito mette a garanzia un plafond di beni e servizi ricevendo in cambio un massimale di spesa (simile a un fido di cassa). Utilizzando tale linea di credito (a interesse zero), l'impresa può acquistare beni e servizi dalle altre aziende aderenti senza aver ancora accumulato il credito derivante dalle vendite. Nei dodici mesi successivi, l'impresa deve riuscire a rientrare del proprio debito vendendo nel circuito i propri beni o servizi, pena il pagamento in euro della parte non compensata. Per Sardex il cambio è 1:1 con l'euro e più della metà delle transazioni tra aderenti al sistema è regolata in moneta complementare. Sardex ha iniziato recentemente ad ampliare il sistema dei pagamenti in modo tale da poter corrispondere parte dei salari in moneta locale e, allo stesso tempo, estendere ai consumatori la possibilità di utilizzare Sardex, dando vita a un sistema integrato tra cittadini e imprese.

Le valute con **obiettivi sociali** sono principalmente focalizzate su problemi specifici che vanno dall'assistenza alla disoccupazione.

Assistenza anziani e disabili: La "Banca Del Lavoro Volontario" creata in Giappone nel 1978, un prototipo che successivamente è stato reinventato in occidente come Banca del tempo, in particolare, negli Stati Uniti e nel Regno Unito. Nel Giappone, il sistema di Fureai Kippu è oggi il discendente diretto di quei sistemi pionieristici di allora.

Disoccupazione: all'inizio degli anni 80, la piccola città di Courtenay, British Columbia dipendeva dalla locale base aerea della Air Force USA e da un laminatoio di legname. Quando la base fu riassegnata ed il laminatoio chiuso, l'economia locale crollò. La disoccupazione divenne alta e le difficoltà finanziarie significative. Il programma LETS venne implementato intorno al 1983, introducendo il "dollaro verde" (la valuta LETS). Questo sistema ha permesso ai cittadini di scambiare beni e servizi tra loro anche in assenza di dollari canadesi ufficiali.

Educazione: Il sistema MUSE (Mutua Unità per l'educazione sostenibile) è una valuta complementare progettata per stimolare l'apprendimento e l'insegnamento reciproco tra ragazzi/e.

Rafforzamento della comunità: uno dei motivi principali per sviluppare una valuta locale in un'area depressa è la ricostruzione stessa della comunità dopo una crisi economica o un evento catastrofico.

Rafforzamento dell'identità: il logo sulle banconote di Ithaca Hours sostiene "In Ithaca we trust", (in contrapposizione con "In God we trust" scritto sui dollari Usa), cosi come la maggior parte delle valute complementari cartacee in circolazione raffigurano personaggi noti della storia locale per rafforzare l'identità locale (Bristol Pound).
Sostenibilità ambientale: si veda l'esempio delle NU di Rotterdam al paragrafo 5.1.
Obietti sociali di diversa natura: come il Samen Doen Olandese che incentiva comportamenti socialmente utili di diversa natura dall'assistenza agli anziani all'insegnamento reciproco al riuso di materiali usati.
Identificato l'obiettivo o gli obiettivi che si vogliono perseguire con la creazione di una valuta locale è necessario identificare un **gruppo locale di supporto** che implementi il progetto.
Il fattore determinante che decreta il successo o il fallimento di ogni progetto di moneta complementare è la presenza di un gruppo di supporto efficacemente coordinato. Sia che l'obiettivo consista nell'avere un effetto reale sulla dimensione sociale della comunità o sugli scambi commerciali al suo interno, è necessario in ogni caso che gli stakeholders del settore siano coinvolti attivamente nel disegno e nell'implementazione della valuta [46].

7.3 Caratteristiche distintive

Un'ulteriore analisi delle valute complementari riguarda le dimensioni fondamentali che le contraddistinguono. Amato e Fantacci mettono in evidenza le seguenti caratteristiche distintive di una valuta comunitaria:

- **Spazio**. Perché vi sia propriamente una moneta, occorre che sia chiaramente definito il suo ambito di circolazione. Le monete complementari sono generalmente caratterizzate da un ambito di circolazione diverso, e quasi sempre più circoscritto, rispetto alle monete ufficiali. La restrizione è spesso di carattere territoriale. Tuttavia, lo spazio di riferimento di una moneta non è da intendersi necessariamente in termini geografici. Per esempio, numerosi esperimenti recenti hanno come ambito di circolazione internet o qualche suo nodo (i già citati Bitcoin o il Ripple Monetary System). Si parla, anche in questo caso, di community currencies, con riferimento però a una comunità virtuale;
- **Scopo/Obiettivo**. Esistono monete complementari a servizio del marketing (punti fragola Esselunga), del welfare (buoni scuola, voucher sociali), dello sviluppo locale (Brixton Pound, Sol-Violette), dell'ambiente (come l'Edogawatt, basato nella città giapponese di Edogawa, o il Maia Maia Emissions Reduction Currency System, i cui partecipanti guadagnano moneta piantando alberi per ridurre il diossido di carbonio nell'atmosfera) ecc;
- **Supporto materiale**. Lo sviluppo di nuove tecnologie offre l'occasione per cambiamenti istituzionali. Oggi, molte monete complementari nascono come monete virtuali, in uno spazio, come quello della rete, poco permeabile alle regolamentazioni. La maggior parte delle monete locali, invece, utilizza banconote cartacee, solo recentemente affiancate da supporti telematici;
- **Modalità di emissione**. L'emissione può avvenire in tre modalità. Esistono monete dotate di copertura (backed currencies); monete senza copertura emesse da autorità centrali (fiat currencies); monete scritturali di tipo bancario emesse contestualmente allo scambio con cui simultaneamente sono registrati un debito in capo all'acquirente ed un credito in capo al venditore. Il debito e credito pur essendo relativi a scambi bilaterali sono registrati in un sistema centralizzato come crediti e debiti nei confronti del sistema (mutual credit currencies);
- **Unità di conto**. Si ha propriamente emissione di moneta solo quando sia definito il rapporto fra un mezzo di scambio (comunque sia fatto) e un'unità di conto. La peculiare unità di conto

adottata costituisce, dunque, un ulteriore criterio di differenziazione. Gran parte delle monete complementari esistenti, hanno un ancoraggio fisso alla moneta ufficiale, di norma secondo una parità di 1 a 1. I circuiti che hanno per oggetto lo scambio di servizi adottano spesso, come unità di riferimento, l'ora di lavoro: è il caso, già visto, delle Banche del Tempo e dei Time Dollars. Gli Ithaca Hours, invece, hanno un controvalore di 10 dollari, idealmente corrispondente al salario orario, ma che resta fisso. Esistono valute denominate in una certa unità fisica nelle Frequent Flyers Miles l'unità di conto è un volo della distanza di un miglio. Nel WAT giapponese l'unità di conto è 1KWH della corrente elettrica generata dalle comunità energetiche da fonti rinnovabili, equivalente a 6 minuti di lavoro semplice e a circa 75-100 yen;

- **Convertibilità**. Nei sistemi concepiti come circuiti chiusi, le monete complementari non hanno alcun valore esterno: o perché è esplicitamente previsto che, uscendo dal circuito, un partecipante rinunci a ogni credito maturato, o perché non è prevista la possibilità di trasferire una posta attiva all'esterno del circuito, convertendo la moneta complementare in moneta ufficiale. Il Sardex, per esempio, è una valuta inconvertibile. All'estremo opposto, si hanno sistemi strutturalmente aperti, in cui la comunicazione con il circuito della moneta ufficiale avviene alla fine di ogni ciclo della moneta complementare: è il caso, per esempio, dei buoni pasto. In tutti gli altri casi, in cui la conversione non è né esclusa né imposta a priori dalle logiche di funzionamento del sistema, essa appare semplicemente come possibilità, accordata ai detentori di moneta complementare, a determinate condizioni. Di norma, la riconversione in valuta ufficiale avviene ad un tasso scontato, ovvero con una perdita, in maniera da scoraggiare l'uscita dal circuito rispetto all'entrata (come per il Chiemgauer);
- **Accumulabilità**. Alcune monete complementari possono essere accumulate indefinitamente, senza alcun limite di tempo o di importo. Si può creare, in tal modo, un'ingente, e a pericolosa, riserva di liquidità. Alcuni sistemi di moneta complementare sono già andati incontro alla bancarotta a causa di un'eccessiva esposizione (si vedano, per esempio, i due casi di monete elettroniche circolanti su internet, beenz e netcentives). Per scongiurare problemi simili, la maggioranza dei sistemi di scambio complementari prevede una limitazione alla possibilità di accumulare la moneta, ovvero alla possibilità di detenerla come riserva di valore. La limitazione più ovvia consiste nell'imposizione di una data di scadenza. I sistemi di scambio locali, adottano sempre più di frequente una forma più raffinata di limitazione dell'accumulabilità della moneta, indicata come demurrage che, come già visto, può essere assimilato a un tasso di interesse negativo sugli accumuli. Esistono diverse forme di decumulo, secondo la destinazione dell'importo stornato, il quale può essere: cancellato o trasferito ad altri enti, come contributo per il finanziamento di spese d'interesse collettivo. Il decumulo reimmette la moneta nella circolazione, contribuendo a chiudere il circuito.

I costi dell'infrastruttura necessaria al funzionamento del sistema di pagamento complementare possono essere recuperati con diverse modalità. Nei sistemi di mutual credit anche noti come Local Exchange Systems (LETS) si provvede ad aprire un conto per le spese generali dove chi ha lavorato per la messa a punto del sistema viene iscritto a credito nei confronti dei futuri partecipanti al circuito.
Altre opzioni prevedono l'applicazione di una tariffa fissa di entrata o periodica, o l'applicazione di tariffe di transazione (in % alle quantità scambiate).

7.4 Sistemi Local Exchange Systems (LETS). Alcune esperienze a livello internazionale di valute comunitarie digitali

Tra i vari esempi di valute locali esamineremo in maggior dettaglio i sistemi di credito reciproco come il **LETS** ed il **TIME DOLLARS** (in cui i partecipanti si accordano su una transazione e creano la valuta necessaria rispettivamente come debito e credito) perché presentano caratteristiche ideali per una gestione su **piattaforme blockchain**: sono **autoregolamentati**, non hanno bisogno di una banca centrale per monitorare l'offerta di moneta; la maggior parte di essi sono già completamente **informatizzati**; promuovono attivamente la **cooperazione** piuttosto che la concorrenza tra i partecipanti favorendo lo sviluppo delle comunità di riferimento [47].

Un sistema di muto credito è un sistema contabile di scambio, in cui non vi è nessuna riserva iniziale di liquidità. Quando un membro aderisce, il saldo iniziale del suo conto è impostato a zero. Il sistema consente un saldo negativo in una certa misura predefinita, ed i valori vengono trasferiti tra i conti delle parti convolte nella transazione.

Amato e Fantacci inoltre nel disegnare il loro modello ideale di valuta locale ideale chiamano in gioco proprio questi sistemi basati su una valuta digitale complementare e non inflazionistica. Per evitare che il circuito produca inflazione secondo gli autori devono essere fissati precisi massimali sugli squilibri di conto corrente (in proporzione al valore degli scambi di ciascun individuo nell'economia locale) e devono essere applicati tassi d'interesse non solo sui saldi di debito ma anche, simmetricamente, sui saldi di credito (tassi di decumulo o demurrage).

I sistemi di credito reciproco si basano sul principio della "**co-produzione**" e della **reciprocità**: **il miglior modo per costruire una comunità sana è quello di considerare ogni persona come portatrice di competenze, idee e risorse convertendo il contributo del singolo allo sviluppo e al rafforzamento della comunità in potere di acquisto.**

Gli obiettivi di un sistema di credito reciproco locale sono soprattutto di carattere economico e solidale. Le motivazioni che stanno alla base della loro costituzione sono infatti: la mancanza di denaro, la lotta contro la solitudine, l'integrazione all'interno della comunità locale, la costituzione di buon vicinato, la possibilità di acquisire servizi a costi più bassi, la possibilità di utilizzare lavoratori disoccupati, il sostegno a beni e servizi locali scarsamente valorizzati, lo sviluppo di una economia locale rispettosa delle risorse naturali.

Il desiderio è quello di correggere le logiche distorte del l'economia, passando così da un commercio impersonale a «rapporti più personali e umani», introducendo trasferimenti tra persone che possiedono conoscenze, abilità, tempo e beni non utilizzati. Si ottiene cosi il riconoscimento di quelle competenze che il mercato tradizionale non valorizza, rinforzando il senso di autenticità nelle relazioni con gli altri. L'unità locale, denominata in modo vario e fantasioso nei diversi sistemi (Oliver, Bright, Storie, Acorn, Beacon, Pigs, Onny), è frequentemente allineata alla valuta nazionale. Secondo alcuni economisti il sistema è potenzialmente interessante per le regioni ad alto tasso di disoccupazione perché permette alle persone di ottenere beni e servizi che non possono pagare con la moneta tradizionale. I problemi legati al tasso di inflazione e alla disoccupazione che ne consegue, vengono così aggirati creando una moneta locale, da usare solo all'interno della comunità della quale si è parte, che assicura scambi di beni, servizi e abilità tra gli utenti del sistema stesso. Le valute locali sono state utilizzate anche nel passato ogni volta che una comunità voleva proteggere l'economia interna da fattori esterni quali la guerra o la depressione. Attualmente il sistema dei LETS costituisce la più avanzata forma di valuta locale in circolazione.

Un sistema LETS è basato su di un gruppo di persone che accettano di condividere reciprocamente le loro competenze con l'ausilio di una moneta su base locale. Il LETS è stato ideato da Michael Linton sull'isola di Vancouver, in Canada, negli anni '80. Il circuito, composto inizialmente da 500 membri, ha visto negli anni successivi una rapida diffusione anche in Australia, Nuova Zelanda e

Regno Unito, mentre in Europa si diffondevano sistemi ispirati ad esso e pressoché analoghi nel funzionamento.
Il LETS funziona in maniera molto semplice: un gruppo di persone interessate a partecipare redige un elenco di competenze (ma anche di beni e servizi) che può offrire agli altri, stilando al contempo una lista di cosa invece vorrebbe ricevere come corrispettivo di tale servizio. Tali liste vengono messe poi a disposizione degli altri aderenti tramite un app ed i partecipanti vengono iscritti in un conto che registra con una moneta comunitaria le entrate e le uscite del sistema. Per ogni prestazione offerta il conto registrerà un credito (che potrà essere usato per "acquistare" un altro servizio), mentre nel caso opposto verrà registrato sul conto un obbligo di prestazione futura che dovrà essere rispettato se si vuole continuare a usufruire del sistema. La contabilizzazione degli scambi avviene attraverso l'emissione di assegni (nella versione cartacea); l'unità di misura è una moneta interna chiamata con un nome di fantasia, oppure nelle realtà dove si scambiano servizi è il tempo. In questo modo tutti soddisfano le proprie necessità senza l'ausilio del denaro convenzionale. Se si sommano insieme tutti i crediti e i debiti registrati sulla piattaforma da parte di tutti i partecipanti, questi si compensano. La moneta locale utilizzata negli scambi all'interno del sistema viene creata in quantità che rispettino gli scambi realmente effettuati nel sistema, evitando problemi di sovrabbondanza o insufficienza.
Nella valutazione dei beni e dei servizi ogni LETS ha un diverso modo di agire, fondamentalmente esistono tre tipi di schema:

- i servizi vengono conteggiati in base al tempo di produzione (un'ora di baby-sitting equivale ad un'ora di idraulico);
- i beni e i servizi vengono valutati in base al valore d'uso, anche se spesso è vicino al prezzo corrente del mercato locale;
- ogni aderente può fissare il valore del proprio tempo, ma entro vincoli predefiniti dal LETS per evitare sperequazioni eccessive.

Molti LETS condividono anche le seguenti proprietà volte ad aumentare la stabilità del sistema. Per facilitare il monitoraggio reciproco e consentire ai membri di verificare la fattibilità del sistema in generale non vi è alcun segreto bancario quindi, l'amministrazione centrale regolarmente pubblica i dettagli dei saldi
e il fatturato dei membri. Inoltre, prima di una transazione il fornitore ha la possibilità di verificare l'equilibrio finanziario ed il fatturato dell'acquirente per valutarne il merito creditizio. In generale, nessun interesse viene addebitato su saldi negativi o positivi. Introdurre un limite di fiducia al saldo negativo per evitare uno squilibrio eccessivo nei saldi degli aderenti. I LETS non svolgono solo una funzione bancaria ma anche di market-matcher di domanda ed offerta pubblicizzando regolarmente i servizi e prodotti offerti e/o richiesti dai membri e realizzando eventi con scopi di networking. Le tre funzioni principali svolte sono di: gestione di una transazione, erogazione di credito e market-matching.
Il **Time Dollar** è un sistema di credito reciproco basato sul mutuo aiuto tra i membri di una comunità attraverso lo sviluppo del trasferimento paritario del tempo. I partecipanti acquisiscono un credito per il tempo utilizzato ad aiutare un altro membro. Tale credito espresso in TIME DOLLAR da la possibilità di ottenere un particolare servizio di cui si abbia necessità (lavori domestici, assistenza anziani, trasporti, ripetizioni, attività amministrative di supporto al programma). Obiettivo principale è quello di sviluppare una struttura di reciprocità, ricostruendo il buon vicinato e lo spirito comunitario, attraverso la valorizzazione delle forze sociali ed economiche locali. Ideatore del sistema Time dollar è stato Edgar Cahn. Il sistema TIME DOLLAR negli Stati Uniti non è tassabile in quanto la sua attività è assimilata a quella delle organizzazioni di volontariato. Il Time Dollar non è

un modo per pagare i volontari, serve per costruire la solidarietà di mutuo aiuto e le comunità, insomma il buon vicinato. Non è pensato per ottenere servizi a costo più basso, ma per valorizzare le risorse di pensionati e disoccupati. Con gli stessi obiettivi e modalità strutturali, il Time Dollar è stato sperimentato in Giappone, in Sekizen, con un progetto fortemente orientato alla solidarietà intergenerazionale.

Un sistema di muto credito può essere un'alternativa praticabile solo se può garantire una valuta stabile. In definitiva, la stabilità di un sistema valutario comunitario, come il sistema di mutuo credito, dipende dalla sua credibilità. La credibilità può essere influenzata da fattori endogeni ed esogeni. Per un dato livello del prezzo, la capacità produttiva effettiva e potenziale del sistema rispetto alle unità di moneta circolante è un fattore endogeno che determina la credibilità del sistema. Le condizioni commerciali interregionali in termini di prezzi di beni scambiati, l'offerta di moneta nazionale e l'inflazione sono fattori esogeni che possono influenzare la credibilità della valuta comunitaria tra i sui membri su cui però l'amministrazione del sistema di mutuo credito non ha alcun controllo.

L'offerta di moneta per un sistema di mutuo credito è rappresentata dalla somma di tutti i debiti in essere che equivale alla somma di tutti crediti in sospeso. Tuttavia la moneta non è emessa centralmente per l'intero sistema ma a livello micro dai singoli individui che sono in grado di emettere unità di valuta per facilitare gli scambi. Come abbiamo visto la credibilità e stabilità della moneta dipende dal livello ottimale di moneta offerta. Per il cosiddetto *"**Common Problem**"* il livello ottimale di offerta di moneta differisce a seconda che sia valutato per l'intero sistema o per il singolo individuo. Supponiamo che ci sia un livello ottimale di credibilità, in cui il vantaggio collettivo di emettere un'altra unità di valuta per facilitare le transazioni sia esattamente compensato dal costo collettivo in termini di riduzione della credibilità. A questo punto, il costo di un'ulteriore riduzione della credibilità (maggiore probabilità di collasso del sistema) è inferiore per un individuo che per il sistema nel suo insieme. Quindi, **l'individuo tenderà a "sovra-emettere" crediti fintanto che i benefici individuali di esecuzione della transazione superano il costo individuale della riduzione associata della credibilità del sistema. Nel caso limite questo comportamento individualistico e ottimizzante potrebbe causare inadempienze individuali ed infine collettive facendo collassare il sistema.**

Nonostante le possibilità di monitoraggio reciproco, i sistemi di mutuo credito sembrano essere **vulnerabili a comportamenti opportunistici dei membri, che potrebbe accumulare debiti e successivamente rifiutarsi (o essere incapace) di rimborsare**. Il crollo dell'Australiano Baytown LETS può essere attribuito a questo problema esacerbato da cattive pratiche amministrative.

Un sistema LETS si basa sulla fiducia tra i partecipanti e, con l'adesione di un maggior numero di persone, il livello medio di fiducia tra i partecipanti diminuisce. Un calo di fiducia riduce la disponibilità ad accettare il credito emesso e mette a repentaglio la stabilità del sistema [48].

Il comportamento sleale viene visto come una sorta di tradimento nei confronti degli altri membri; non sono previste sanzioni ma chi esce dal circuito deve saldare il proprio debito. E' prevista la presenza di un organo "controllore" è l'Advisory Group che ha il compito di segnalare chi disattende alle regole e favorirne l'espulsione.

Adeguati principi di progettazione istituzionale dei sistemi di mutuo credito accanto al corretto funzionamento di norme sociali possono attenuare il "Common problem" ed i comportamenti opportunistici [49]. Le procedure di iscrizione, la registrazione e lo svolgimento degli scambi, devono essere regolamentati. Si punta all'efficienza per avere una struttura snella che possa venire incontro con facilità alle esigenze degli associati; a tal proposito è stata predisposta una serie di figure cardine (record coordinator, steward, advisory group) ognuna con compiti precisi, che crea una sorta di modello funzionale in cui ognuno si occupa della gestione di una determinata fase

organizzativa, senza però che ci sia alcun potere gerarchico-sanzionatorio poiché si tende ad una totale orizzontalità dei rapporti, i quali si basano sulla completa fiducia reciproca.
Se da un lato l'aumento della dimensione della comunità di riferimento riduce la fiducia nel sistema dall'altro lato una dimensione limitata di partecipanti in un sistema di mutuo credito bilaterale o multilaterale pone dei limiti intrinseci all'utilizzo della valuta come mezzo di scambio. In altre parole, ci sarà un bisogno insoddisfatto di una varietà di servizi e beni che non sono offerti all'interno della comunità. Per questo motivo, potrebbe essere vantaggioso per i partecipanti poter scambiare con partecipanti di altre comunità che sono in grado di soddisfare tali bisogni insoddisfatti [50] oppure coinvolgere anche i lavoratori nel circuito. In questo modo anche le imprese che vendono ma non riescono ad acquistare da altre imprese avrebbero un uso certo per i loro saldi attivi in moneta locale che per di più tornerebbe a loro vantaggio: un salario in moneta locale si traduce integralmente in domanda per prodotti locali, consentendo l'ingresso anche alle imprese che acquistano da altre imprese ma che vendono ai privati beni di consumo. In tal modo, il circuito creditizio locale fra imprese si estenderebbe fino a diventare un circuito monetario a sostegno dell'economia locale nel suo insieme. Piattaforme web centralizzate per la gestione dei sistemi di mutuo credito esistono dal 2004, e sono tipicamente basate su stanze di compensazione centralizzate o Sub Hub regionali interconnessi [50]. Tuttavia l'impiego di **piattaforme web** centralizzate presenta due implicazioni cruciali. In primo luogo, i partecipanti alla comunità devono fare **affidamento sull'onestà degli operatori** della piattaforma per l'elaborazione di pagamenti elettronici in modo corretto secondo le regole predefinite. Poiché le transazioni vengono elaborate dagli operatori della piattaforma sono reversibili e modificabili, il che a sua volta rende non trasparente per i partecipanti della community la valutazione della loro legittimità. In secondo luogo, le piattaforme centralizzate hanno un'architettura ***single point of failure***, che le rende vulnerabili agli attacchi dolosi.
Come soluzione al problema intrinseco dello scambio di valore virtuale su piattaforme centralizzate, l'anonimo noto come **Satoshi Nakamoto** [51] ha pubblicato il whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System" nel 2008. Il whitepaper di Bitcoin conclude: "Abbiamo proposto un sistema per le transazioni elettroniche senza fare affidamento sulla fiducia". Al fine di risolvere il problema della fiducia, e della doppia spesa il whitepaper propone una rete di transazioni completamente trasparente e peer-to-peer utilizzando un algoritmo di consenso bizantino tollerante agli errori.
La tecnologia Blockchain per le sue caratteristiche può fornire effettivamente una soluzione ai problemi di sicurezza e trasparenza sopra descritti, a cui sono soggette le valute comunitarie digitali basate su piattaforme centralizzate, anche se attualmente il potenziale della tecnologia nella gestione delle valute comunitarie non è stato ancora sufficientemente indagato e sfruttato [52]. Nei paragrafi successivi saranno prese in esame alcune esperienze a livello internazionale di LETS con particolare riferimento a monete digitali o sistemi abilitati dalla tecnologia blockchain.

7.4.1 WAT

Il sistema WAT, utilizzato in Giappone, permette di emettere note di debito IOU (I Owe You) che possono circolare come valuta complementare all'interno di una comunità. Il sistema WAT si caratterizza per la sua natura policentrica. Mentre quasi tutti gli altri sistemi credito reciproco richiedono un'amministrazione centrale, il sistema WAT può essere gestito senza alcuna autorità centralizzata [53].
Questa valuta è considerata d'interesse ai fini del presente rapporto oltre per il fatto di essere basata su di un approccio P2P anche per l'unità di conto utilizzata. Il valore di 1 WAT equivale ad 1 kWh di corrente elettrica generata da fonte rinnovabile da una comunità energetica. Si suppone che i costi per la generazione di corrente elettrica da fonti naturali diminuiranno nel tempo. Poiché i costi momentanei per 1 kWh sono pari a circa 6 minuti di forza lavoro, questo è stato fissato come

valore di base per il sistema WAT (corrispondenti a circa a circa 75-100 ¥). Il sistema è stato implementato nell'agosto del 2000 ed ha avuto inizio con la distribuzione dei moduli WAT e la creazione di una associazione.
Ottenere un modulo WAT da compilare è molto facile. Possono essere ordinati presso la fondazione, essere scaricati dalla WAT-homepage, attualmente con il sistema I WAT la valuta sarà digitalizzata. Non esiste un ufficio o un coordinatore per il sistema WAT, quindi non verrà addebitata alcuna quota associativa. L'associazione esiste solo per la fornitura e la distribuzione di moduli e la pubblicazione di un periodico informativo. Chiunque voglia utilizzare ed emettere biglietti WAT diventa automaticamente membro dell'associazione.
Lo scambio tra acquirenti e venditori si basa su un accordo reciproco e si svolge con responsabilità personale. Chiunque può emettere un WAT-ticket in qualsiasi momento, se vuole realizzare una transazione. Naturalmente il WAT-ticket non può essere usato se il destinatario non lo riconosce come mezzo di pagamento. Poiché il WAT-ticket è una sorta di promessa di pagamento (promessa di lavoro in cambio di beni e servizi), assomiglia ad una cambiale. Tuttavia, non esiste una data fissa per il riscatto. La persona che accetta un WAT-ticket può utilizzarlo per un accordo con una terza persona mostrando a colui da cui desidera acquistare bene o servizi che ha già concesso un credito a un'altra persona che ritiene affidabile. In questo modo il biglietto circola all'interno della cerchia dei soci mentre ogni cambio di mano sarà registrato sul retro del biglietto. Non appena il biglietto ritorna da chi lo ha emesso cessa la sua funzione e viene liquidato. Nel funzionamento della valuta cartacea esistono tre moneti (si veda Figura 8):

- **Emissione**: una persona che ha bisogno di alcuni beni o servizi diventa un debitore ed emette una nota di debito WAT. Il debitore scrive sulla nota il nome del fornitore dei beni o del servizio, l'importo del debito e appone la sua firma. Il debitore consegna la nota a colui che diventa creditore e in cambio ottiene la merce o il servizio;
- **Circolazione**: Il creditore può utilizzarlo per un'altra negoziazione. Per fare ciò, è scritto il nome del beneficiario sul retro della nota. Il beneficiario diventa il nuovo creditore. La lunghezza della catena di creditori mostra la fiducia riposta nella valuta;
- **Liquidazione**: la nota di debito viene liquidata quando ritorna, a seguito di una transazione, alla persona che l'ha emessa.

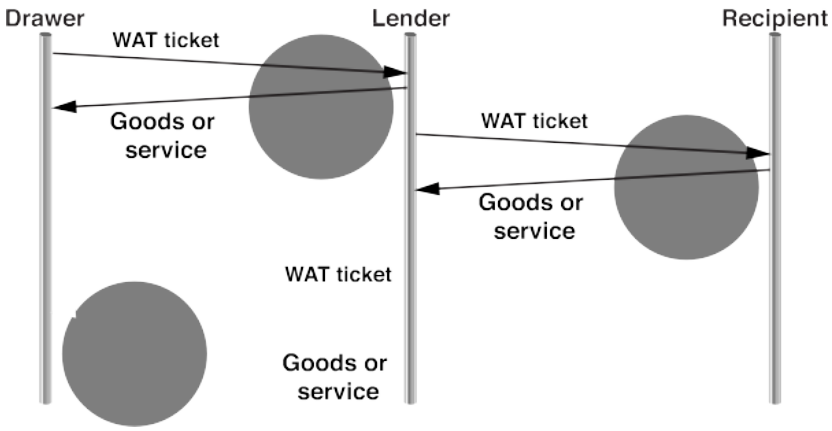

Figura 8. Schema di funzionamento WAT

Se chi ha emesso per primo il WAT-ticket, al termine del ciclo, non riesce a liquidare il suo debito. La responsabilità segue la catena degli avvalli fino all'ultimo destinatario del ticket.

Se una transazione viene fatta con un WAT-ticket ci sono diverse modalità di pagamento che il contraente può aspettarsi. Queste dipendono dal rapporto di fiducia tra i due e dai vari livelli di fiducia del WAT-ticket stesso. In realtà ci sono tre modalità:

- trattare con un biglietto di nuova emissione (new ticket deal);
- trattare con un biglietto che è già in circolazione (circulating ticket deal);
- offerta con l'utilizzo di nuovi biglietti e di biglietti già in circolazione allo stesso tempo (mixed tickets deal).

L'accettazione di un biglietto di nuova emissione dimostra la fiducia del contraente nell'affare. Un biglietto già emesso, che era stato utilizzato in precedenti accordi, indica una cerchia di partecipanti già esistente. Anche con lo stesso valore nominale un biglietto con un numero di ingressi sul retro ha accumulato la fiducia di molte queste persone e guadagna un valore aggiuntivo oltre a quello nominale.
Questo sistema di pagamento si è diffuso rapidamente in Giappone ed è considerato come uno dei sistemi di valuta complementare esistenti più efficienti in termini di costi di gestione in grado di creare spontaneamente circuiti di fiducia tra sottogruppi di partecipanti.

7.4.2 Hull Coin

Hull Coin è il risultato di una ricerca condotta dall'organizzazione no-profit Kaini Industries, finanziata dal consiglio comunale di Hull con il compito di indagare su come la tecnologia blockchain possa essere impiegata per sviluppare una valuta locale in grado di sostenere la comunità colpita dalla povertà. Dopo alcuni anni di sviluppo e di sensibilizzazione della comunità, è stata lanciata nel marzo del 2019 nella città di Kingston Upon Hull la criptovaluta Hullcoin, che permette alle persone di guadagnare valuta facendo volontariato e svolgendo attività che vanno a beneficio della comunità. Kingston Upon Hull è una delle tante città del Regno Unito che ha sofferto a causa della recessione nazionale e delle riforme del welfare adottate dal governo di coalizione. Questo a sua volta ha portato a un forte aumento del numero di persone che vivono in condizioni di povertà finanziaria. I progetti di valuta comunitaria avviati in passato in molti paesi, e che stanno ancora proliferando a livello internazionale, in molti casi sono stati utilizzati per proteggere le imprese locali: creando un circuito commerciale in cui il denaro rimane all'interno di un'economia locale e non viene speso con le aziende della grande distribuzione che non restituiscono i capitali sotto forma di investimenti alla comunità. Nel Regno Unito esistono diversi esempi quali il Brixton Pound, Bristol, Stroud, Lewes e Totnes, e molti altri. Tuttavia, nessuna di queste valute è digitale, ne mira direttamente alla giustizia sociale o alla povertà. Nel caso del Consiglio comunale di Hull, Dave Shepherdson, il Financial Inclusion Support Officer, ha spiegato che le altre valute comunitarie inglesi sono state considerate come risorse sacrificabili. Nel caso di HullCoin, l'estrazione di una criptovaluta governativa funziona come mezzo per aggiungere valore all'economia locale. L'idea di usare la criptovaluta nasce quando è stato chiesto a Shepherdson dal responsabile dei diritti sociali del Consiglio comunale di Hull, Lisa Bovill, di indagare sulla possibilità di usare una valuta alternativa (nel senso della Sterlina di Brixton delle valute locali) come mezzo per fornire un framework anti-povertà alla città di Hull. Questo doveva far parte dello schema "Hull People Premium", volto ad aiutare la gente di Hull a risparmiare denaro e ad avere accesso ad aiuti per il cibo, il carburante e il credito. Dopo uno studio approfondito si è giunti alla conclusione che la valuta digitale potesse avere un grande potenziale ai fini della redistribuzione del reddito, grazie al suo processo di emissione tramite il mining, se ancorata alla valuta digitale stabile. Mentre il progetto è agli inizi, il consiglio comunale di Hull sta attivamente estraendo criptovaluta. Il suo impianto GPU di estrazione è basato su due schede grafiche Sapphire R9 290X che funzionano a 1,6 MH/sec. Hullcoin utilizza gli script di mining di Ven (ha una sua blockchain ed impiega il Proof of Authority) e Feathercoin (usa il Proof of

work ed è nato da unfork con litecoin). Il mix dei due aggiunge maggiore stabilità alla volatilità della valuta. In particolare il valore di Ven è ancorato ad un paniere di materie prime tra cui l'oro che la rende molto stabile. Il denaro per questa attrezzatura non proviene dai fondi dei contribuenti ma da una donazione da parte di un benefattore anonimo. Gli obiettivi finali sono quelli di poter installare una piattaforma KnC per il mining e generare una maggiore quantità di valuta che possa consentirne l'utilizzo per il pagamento degli affitti delle bollette e del cibo fino alla creazione di una Banca di Hull, mentre al momento è possibile un impiego solo su piccola scala [54].
Kaini Industries mina hullcoin e le distribuisce ad organizzazioni locali di volontariato, centri per l'impiego e di assistenza sanitaria, banche del tempo che stabiliscono le proprie regole su come emetterla in base di alcune linee guida stabilite dall'organizzazione stessa. Hullcoin per ragioni legali non ha un valore monetario può essere riscattata sotto forma di sconti (dal 15 al 50%) su ogni sorta di bene e servizio presso gli oltre 140 rivenditori partecipanti all'iniziativa in tutta la città. I rivenditori possono scegliere di usare le monete come ricompensa per i dipendenti, donandole ai clienti più fedeli come sconti su acquisti futuri, donarle ad un gruppo della comunità o ad un ente di beneficenza per stimolare ulteriormente l'economia locale (si veda Figura 9). La tecnologia blockchain usata come stanza di compensazione decentralizzata ha permesso di incorporare nella stessa moneta le prove del risultato sociale di qualsiasi attività intrapresa nella comunità creando un registro distribuito di tutte le attività socialmente rilevanti intraprese dai membri ed offrendo alle persone un CV sociale utile anche nella ricerca di un nuovo impiego.

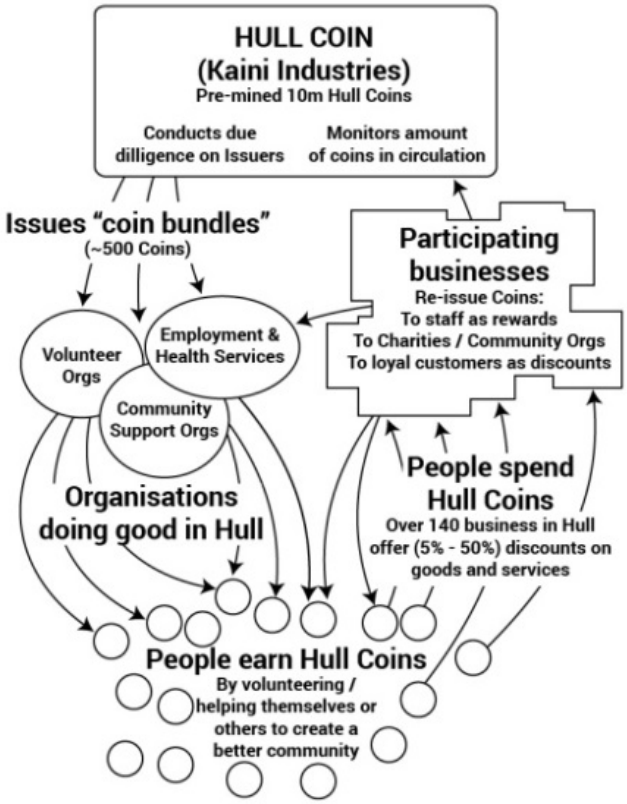

Figura 9. Schema di funzionamento Hull Coin

Il concetto di Hullcoin ha molte analogie con "Covestment", termine coniato da Jordan Bober e Michael Linton, l'inventore di LETS, per descrivere un mezzo per "finanziare il futuro e creare resilienza economica tessendo innovazioni nelle valute della rete, crowdfunding e microprestiti comunitari". In Covestment, come evidenziato nella figura 10 le aziende depositano valuta (o buoni

sconto) in un Fondo di Covestment della Comunità da cui i membri della comunità possono acquistare la valuta locale con denaro regolare. Il fondo Covestment utilizza il contante per fornire prestiti agli imprenditori e alle imprese locali, e le persone usano la loro valuta locale per ottenere sconti quando fanno acquisti presso le imprese che hanno sostenuto la valuta all'inizio. Esattamente come per Hullcoin, il risultato è uno stimolo per l'offerta di denaro e quindi per l'economia locale.

Figura 10. Covestment

7.4.3 Time Credit

Basandosi sulle potenzialità della blockchain, InvolveMINT è un'organizzazione che gestisce un'altra valuta comunitaria, chiamata TIME CREDIT, utilizzata con obiettivi sociali. Questa valuta è operativa a Pittsburgh. Analogamente a HullCoin, InvolveMINT permette ai suoi utenti di trovare opportunità di volontariato e progetti su cui lavorare e a cui dedicare il loro tempo, guadagnando valuta criptata riscattabile con l'acquisto di beni e servizi presso i partner aderenti. La tecnologia blockchain permette di tenere traccia delle competenze di ogni utente e delle prestazioni erogate nel tempo creando un CV sociale per ogni membro attivo della cummunity. Robert Kauffman [55] sostiene che questi tipi di progetti possano funzionare bene con la tecnologia blockchain perché finalizzati allo sviluppo di un sistema economico sano nelle comunità locali. I principi delle criptovalute applicabili ai progetti di valute comunitarie possono essere riassunti nel seguente modo: permettere lo scambio di beni e servizi tramite un mezzo di pagamento il cui valore, che deve essere chiaramente compreso tra gli utilizzatori, sia trasmissibile e impiegabile come titolo di credito. InvolveMINT sta cambiando la cultura del volontariato creando un'ampia rete di organizzazioni e di imprese a sostegno di coloro che cercano di dare un impulso al rafforzamento delle nostre comunità. Questa rete promuove un servizio regolare ed una collaborazione ponderata alla (ri)costruzione di comunità in un contesto sociale, come quello attuale, di vite sempre più stratificate ed impegnate. La valuta comunitaria è usata come strumento per cambiare la cultura del volontariato e l'impatto sociale. L'obiettivo e di coinvolgere le comunità per creare capacità economiche laddove attualmente non esistono - facendo leva sulle risorse della comunità (come le imprese e le istituzioni di base) permettendo alle persone di affrontare in modo collaborativo i problemi locali attraverso una nuova forma di valuta "intenzionale" che si guadagna partecipando da un progetto o ad un'iniziativa comunitaria. Questa valuta di mutuo credito può poi essere scambiata con altri membri della comunità per servizi, o riscattata presso aziende e istituzioni locali attraverso un'applicazione smartphone. L'app è nata dalla partecipazione di involveMINT al Codefest l'annuale competizione

di hackathon che riunisce giovani professionisti della tecnologia provenienti da tutta la regione. Organizzazioni come Pittsburgh Parks Conservancy, Allegheny CleanWays e Light of Life Rescue Mission sono salite a bordo per fornire opportunità di volontariato. I crediti guadagnati potranno essere riscattati acquistando beni o servizi offerti da una serie di partner aderenti: Venture Outdoors, Photo Antiquities Museum, James Street Gastropub e DECO Resources. Per questo caso di studio sono state trovate minori informazioni sulla piattaforma blockchain impiegata e sui protocolli di consenso usati.

7.4.4 Sarafu

Una missione fondamentale della Bprotocol Foundation (Bancor) è quella di ridurre gli ostacoli tecnici alla progettazione e distribuzione delle valute comunitarie. Le valute comunitarie, che esistono a sostegno delle valute nazionali, hanno dimostrato di migliorare il flusso di cassa ed aumentare la collaborazione nelle comunità locali di tutto il mondo.
Bernard Lietaer, il noto economista teorico della moneta complementare, membro della banca nazionale del Belgio e della Banca dei Regolamenti Internazionali è stato anche presidente del Consiglio della Fondazione Bprotocol dal 2017-2019, fino alla sua scomparsa nel febbraio 2019. Lietaer in una sua famosa dichiarazione ha incoraggiato il mondo a "far fiorire mille valute". Credeva che la diversità valutaria fosse cruciale per la salute delle economie locali come la diversità naturale per la salute degli ecosistemi [56].
Dopo l'ingresso di Bernard in Bancor nel 2017 numerosi imprenditori si sono avvicinati alla Fondazione Bprotocol per essere supportati nel lancio delle proprie valute comunitarie basate su blockchain. Tra queste, l'organizzazione no-profit keniota, Grassroots Economics Foundation, che ha manifestato interesse per la piattaforma Bancor per la creazione, distribuzione e gestione del proprio sistema di valute comunitaria nelle zone rurali del Kenya.
La Fondazione Bprotocol a sua volta stupita dai progressi di Grassroots, da quando le sue valute di carta colorata hanno iniziato ad apparire a Mombasa, in Kenya nel 2010, ha erogato una sovvenzione all'organizzazione per implementare la rete di Sarafu sulla blockchain usando Bancor. La rete di Sarafu (o "valuta" in swahili) servirebbe da sistema di valuta locale trasparente e decentralizzato costituito da token interconnessi a livello di villaggio, creando circuiti chiusi di commercio locale all'interno dei villaggi collegati in rete. Questa nuova forma di trasferimento di denaro ha lo scopo di stimolare il commercio all'interno delle economie locali e mantenere il flusso di valore di fronte alla carenza di valuta nazionale.
La rete di Sarafu ha iniziato i test nell'agosto 2018. Circa sei mesi dopo, sono stati testati nove token a livello di villaggio e centinaia di aziende sono state coinvolte nel progetto. I wallet generati sono di proprietà dei membri della comunità che lavorano come agricoltori, insegnanti, rivenditori, operatori sanitari. Un agricoltore può ora ricevere pagamenti nella valuta locale del suo villaggio, che può quindi impiegare per pagare le tasse scolastiche di suo figlio, e per l'acquisto di altri beni e servizi, tramite smartphone.
LocalCoin, sviluppatore principale del Protocollo Bancor, ha creato una piattaforma che consente a Grassroots di creare token e distribuirli agli utenti, offrendo allo stesso tempo agli utenti la possibilità di scambiare e gestire i propri token ininterrottamente utilizzando wallet crittografici per smartphone.
Il protocollo Bancor garantisce la convertibilità e la liquidità dei token senza la necessità di una controparte o di un intermediario. Ciò significa che il commercio può essere elaborato in modo autonomo e sicuro sulla blockchain senza dover fare affidamento su un'autorità centrale come una

banca. Prezzi e transazioni avvengono attraverso una architettura di smart contracts verificabili integrati con il protocollo Bancor sulla side-chain POA network Ethereum, consentendo transazioni istantanee e riducendo al minimo i costi fino a una frazione di centesimo per transazione.
I ricercatori di Grassroots, LocalCoin e le università di tutto il mondo sono ora in grado di analizzare, in tempo reale, il flusso di valute comunitarie all'interno e attraverso i villaggi, che creano canali diversi e resilienti di collegamenti monetari tra i locali. In questa fase molto precoce del progetto pilota si stanno approfondendo questioni relative al demurrage (interessi negativi o denaro in scadenza), alle stable coin, e alla velocità di circolazione del denaro. Tutti questi aspetti indagati potranno essere utilizzati per migliorare la rete di Sarafu e il protocollo Bancor, affinché le comunità di tutto il mondo possono implementare più facilmente i sistemi di valuta comunitaria.
La costante crescita della rete di Sarafu ci ricorda che molti dei beni e servizi in questi villaggi sono presenti in natura - hanno solo bisogno di nuove forme di denaro per diventare praticamente trasferibili. In definitiva la vision di Bancor e Grassroots è quella di creare n'infrastruttura comune per il commercio locale - un bene pubblico decentralizzato che non richiede commissioni, nessuna autorità centrale e che può essere gestito senza soluzione di continuità, conveniente e accessibile per qualsiasi comunità così da trasformare la scarsità in prosperità.

8 DISTRIBUTED LEDGER TECHNOLOGY E BLOCKCHAIN: INTRODUZIONE AD UNA NUOVA FORMA DI CONSENSO E TRASPARENZA DISTRIBUITA

8.1 Background concettuale

La blockchain e le Distributed Ledger Technology (DLT) sono, a livello generale, delle strutture dati digitali, dei database distribuiti e condivisi che contengono storici continuamente crescenti di transazioni in ordine cronologico.

In altre parole, la struttura dei dati è un ledger, ovvero un libro mastro, che può contenere informazioni digitali, che siano transazioni, record di dati od eseguibili. Le transazioni sono aggregate in insiemi più grandi, chiamati blocchi, codificati crittograficamente e marcati con un timestamp. Tali blocchi sono collegati ai precedenti formando una catena di record che determina l'ordine di sequenza degli eventi o la "blockchain". Il termine blockchain è anche ampiamente usato in letteratura per rappresentare architetture di consenso, algoritmi o domini di applicazioni costruite su tali architetture [57].

Come confermato da un'analisi del 2019 dell'Osservatorio sulle Blockchain e Distributed Ledger del Politecnico di Milano, le tecnologie Blockchain e Distributed Ledger nel 2019 [58]sono entrate in una fase di consolidamento e sono ormai riconosciute come le infrastrutture distribuite che abiliteranno l'Internet of Value. Se nel passato il valore delle tecnologie Blockchain e Distributed Ledger è stato messo in discussione, nel 2019 qualcosa sembra essere cambiato. Tutti ora guardano con grande interesse a queste tecnologie: sviluppatori, startup, aziende, big tech, governi, istituzioni e pubbliche amministrazioni. L'utilizzo delle tecnologie Blockchain e Distributed Ledger, è partito dal settore finanziario, per poi diffondersi in molti altri ambiti. Colossi come Walmart (grande distribuzione), Maersk (logistica) e LVMH (moda e lusso) hanno intrapreso importanti progetti di innovazione basati su queste tecnologie. Le big tech si sono attivate: Facebook con Libra; Telegram con TON; Amazon, Microsoft e Alibaba con soluzioni "Blockchain as a Service" per le aziende. Anche le istituzioni pubbliche ed i governi hanno iniziato ad investire in maniera decisa sulla Blockchain: la Cina ha annunciato l'imminente lancio di una sua moneta digitale, il Regno Unito sta lavorando ad un catasto nazionale, gli Stati Uniti e la Russia stanno testando diverse applicazioni dal voto al pagamento delle imposte, la Commissione Europea ha lanciato l'European Blockchain Service Infrastructure (EBSI), per promuovere servizi pubblici basati su queste tecnologie.

8.2 Definizione e caratteristiche

Le blockchain funzionano su reti digitali. La trasmissione dei dati in tali reti equivale alla copia dei dati da un luogo all'altro, ad es. nel dominio delle criptovalute questo equivale a spostare monete digitali dal digital wallet di un utente a un altro. La sfida principale risiede nel fatto che il sistema deve garantire che le monete vengano spese una sola volta e che non vi siano spese doppie. Una soluzione tradizionale consiste nell'utilizzare un'autorità centrale, come una banca centrale, che funge da intermediario di fiducia tra le parti ed il cui compito è archiviare, salvaguardare lo stato valido del libro mastro e tenere aggiornati i registri. Se più parti devono scrivere nel ledger contemporaneamente, un'autorità centrale implementa anche il controllo della concorrenza e consolida le modifiche nel ledger. In alcune occasioni, la gestione centrale potrebbe non essere fattibile o auspicabile, poiché introduce costi di intermediazione e richiede agli utenti della rete di affidarsi a terzi per il funzionamento del sistema. I sistemi centralizzati presentano anche svantaggi significativi a causa del single point of failure, che li rende più vulnerabili sia ai guasti tecnici che agli attacchi dannosi.

8.2.1 Reti peer to peer

Lo scopo principale delle tecnologie blockchain è rimuovere la necessità di tali intermediari e sostituirli con una rete distribuita di utenti che lavorano in partnership per verificare le transazioni e salvaguardare l'integrità del ledger.
La struttura decentralizzata per eccellenza è un grafo non orientato connesso, rappresentato da una rete peer-to-peer (p2p), come mostrato in Figura 11. Per rete p2p si intende un insieme di nodi interconnessi che si scambiano informazioni senza una struttura centralizzata, in cui ogni componente della rete è paritario.

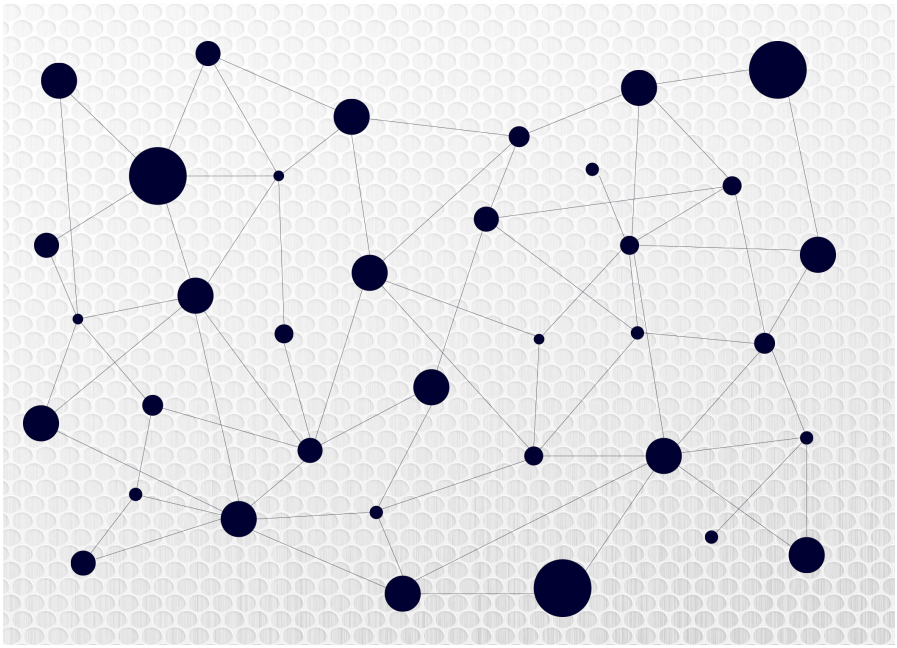

Figura 11. Rete peer-to-peer

Le caratteristiche di una rete peer-to-peer applicata alla blockchain sono:

- Uguaglianza. Ogni nodo può potenzialmente avere gli stessi ruoli degli altri, non esistono nodi master e nodi slave, non c'è alcun tipo di sistema di deleghe dei ruoli.
- Ridondanza. Ogni nodo della rete essendo potenzialmente tutti uguali, ha una copia esatta dello stato del ledger, per cui la struttura della rete è ad alto livello di ridondanza.
- Resilienza. La ridondanza della rete consente di avere, di conseguenza, un'elevata resilienza ai guasti
- Trasparenza. Chiunque nella rete può avere accesso al registro storico delle transazioni del sistema e verificarne la validità.

Se la gestione centrale viene rimossa, la sfida sta nel trovare un modo efficiente per consolidare e sincronizzare più copie del ledger. Il processo di convalida e consolidamento del ledger varia a seconda dei diversi tipi di blockchain, tuttavia in linea di principio i membri della rete confrontano le loro versioni del ledger attraverso un processo assimilabile al voto distribuito, attraverso il quale il viene raggiunto il consenso sullo stato di validità del ledger. Questi meccanismi di validazione sono noti come algoritmi di consenso distribuito. La collaborazione e il comportamento onesto dei nodi distribuiti sono garantiti da ricompense o incentivi basati sulla teoria dei giochi [59], per un'analisi più approfondita vedi paragrafo 8.6.

8.2.2 Crittografia

Le blockchain possono essere molto difficili da manomettere, senza che una parte significativa della rete sia collusa e malevola. Di conseguenza, i sistemi blockchain possono essere sicuri e resistenti alle manomissioni.

Altri elementi che garantiscono una maggiore sicurezza sono le funzioni hash e la crittografia a chiave pubblica, per un'analisi più approfondita vedi paragrafo 8.5.1. Le funzioni hash crittografiche sono algoritmi matematici o funzioni unidirezionali che accettano un input e lo trasformano in un output di lunghezza specifica, ad es. una serie di 256 bit, chiamata output hash. Il loro funzionamento si basa sul fatto che è non è possibile ricreare i dati di input originali dal solo output di hash e che la lunghezza del valore dell'output è fissa ed indipendente dalla lunghezza del contenuto dell'input. La crittografia a chiave pubblica è un protocollo di crittografia asimmetrico. Ogni utente possiede due chiavi crittografiche costituite da caratteri numerici o alfanumerici, una chiave privata segreta e una chiave pubblica che può essere condivisa con altri nodi della rete. Le chiavi sono matematicamente correlate in modo tale che le informazioni crittografate da una parte possano essere decodificate solo dalla sua controparte. L'uso della crittografia a chiave pubblica-privata garantisce l'autenticazione, ovvero che una transazione viene eseguita dall'utente che sostiene di essere e l'autorizzazione, il che significa che le azioni sono eseguite dagli utenti che hanno il diritto di farlo. Ad esempio, la rete può verificare l'identità del mittente, poiché solo la chiave pubblica del mittente può decrittografare il messaggio originale (crittografato e firmato digitalmente dalla chiave privata del mittente). Un messaggio elaborato con la propria chiave pubblica può essere decrittografato solo dal destinatario previsto che detiene la chiave privata segreta. Queste e altre funzionalità di comunicazione standard come la validità e la sicurezza dei dati sono garantite nei sistemi blockchain utilizzando la comunicazione P2P e tecniche di crittografia avanzate.

8.2.3 Smart contracts e common knowledge

Secondo Dipartimento della scienza britannico [60], il vero potenziale delle tecnologie blockchain può essere pienamente raggiunto solo se combinato con gli **smart contracts**, ovvero programmi definiti dall'utente che determinano le regole di scrittura nel ledger ed altri tipi di interazione (es. oracoli). Gli smart contracts sono programmi di esecuzione che apportano modifiche nel ledger e possono essere attivati automaticamente se viene soddisfatta una determinata condizione, ad esempio se viene rispettato un accordo tra le parti contraenti. Il contenuto del contratto è registrato in linguaggio informatico che codifica i vincoli legali e i termini dell'accordo. Gli smart contracts sono auto-eseguiti e a prova di manomissione e comportano vantaggi significativi come la rimozione degli intermediari e la riduzione dei costi di transazione, contrattazione, esecuzione e conformità.

Tali caratteristiche abilitano alla **common knowledge**, un aspetto innovativo mai introdotto precedente. Infatti nella computazione classica il controllo dell'esecuzione di un determinato codice è completamente affidata a chi detiene, eventualmente, i diritti di tale codice e chidetiene il controllo delle macchine, fisiche o virtuali, che eseguono tale codice. In questo modo non c'è trasparenza su determinati aspetti:

- se il codice sia stato manomesso;
- se sia stato eseguito in maniera corretta;
- cosa fa esattamente.

Il fatto che il codice risieda invece sulla blockchain garantisce la common knowledge computing, ovvero che tale codice:

- non è modificabile;
- non è censurabile;

- è eseguibile da tutti i nodi della rete;
- non è interrompibile.

Da uno studio effettuato dall'osservatorio sulle Blockchain e Distributed Ledger [58] con gli smart contract è possibile effettuare varie operazioni sulle transazioni. Di seguito vengono elencati alcuni smart contract semplici che possono essere sviluppati sulle Blockchain:

- **split payment**, ovvero pagamenti che si dividono in due parti e che potrebbero ad esempio permettere un pagamento automatico dell'IVA o di qualsiasi altra percentuale dovuta ad enti terzi;
- **transazioni condizionate** dal realizzarsi di determinate condizioni, come ad esempio un'assicurazione che invia un pagamento automatico nel caso in cui venisse riscon- trato il ritardo di un particolare volo;
- **whitelist**, come ad esempio permettere solo a determinati operatori di poter effettuare transazioni (come ad esempio acquistare o scambiare azioni);
- **registrazione di dati** (ad esempio un'impronta digitale di un documento creata tramite una funzione di hash3) all'interno di una transazione che viene registrata su un registro immutabile. Tale smart contract rappresenta un processo cosiddetto di **notarizzazione** che permette di certificare documenti e garantirne l'incorrutibilità e immutabilità.

Allo stesso modo, anche gli eventi che abilitano uno smart contract o le condizioni per la sua esecuzione possono essere di diverso tipo:

- **tempo**: uno smart contract può discriminare il proprio funzionamento in base al momento in cui viene attivato. Ad esempio è possibile congelare la disponibilità dei fondi per un periodo di tempo predefinito;
- **proprietà**: uno smart contract può essere programmato in maniera tale che una transazione possa essere effettuata solo verso determinati account e in modo che l'autorizzazione debba essere vincolata ad alcune condizioni. Ad esempio è possibile suddividere il pagamento su più ac- count oppure limitare la disponibilità di una transazione solamente ad un destinatario prefissato oppure vincolare l'esecuzione di una transazione all'autorizzazione di uno o più attori attraverso sistemi multi-firma;
- **evento on-chain**: uno smart contract può attivarsi all'accadimento di eventi sulla rete, ad esempio alla ricezione di una transazione esso potrebbe dividerne l'importo in ulteriori parti verso altri destinatari prestabiliti;
- **evento off-chain**: ovvero un evento che non avviene all'interno della piattaforma, ma che è connesso al mondo esterno ad esso. All'interno di uno smart contract che gestisce una scommessa sportiva esso dovrebbe ad esempio attivarsi una volta acquisito il risultato finale della partita.

Questo elenco di possibili applicazioni degli smart contract costituisce solamente un esempio dei principali utilizzi che oggi vengono fatti di questi strumenti, non sarà però ovviamente comprensivo di tutte le possibilità offerte da un linguaggio di programmazione Turing completo, dato che esse sono per definizioni illimitate. Partendo da queste singole operazioni sulle transazioni infatti è possibile utilizzare più smart contract per costruire vere e proprie applicazioni decentralizzate, il cui codice rispetti le caratteristiche del common knowledge computing.

8.2.4 Blocchi e catene

I blocchi sono la componente delle blockchain che contiene effettivamente le informazioni per cui tale blockchain è destinata: per cui ad esempio transazioni nel caso di Bitcoin e codice macchina nel caso di Ethereum.

La Figura 16 mostra le informazioni principali di un blocco Bitcoin:

- **Prev_hash.** Valore che contiene l'hash code del blocco precedente, utilizzato per risalire allo storico di tutte le operazioni fatte sulla blockchain.
- **Timestamp**. Data e ora dell'immissione del blocco in blockchain.
- **Tx_root**. Codice hash della root delle transazioni contenute nel blocco. E' ottenuto applicando iterativamente l'hashing su ogni coppia di transazioni memorizzate. Ogni transazione è una foglia dell'albero, il merkle tree, ogni coppia di transazioni forma un livello superiore dell'albero, fino ad arrivare alla radice. Questo campo serve a verificare in maniera immediata che le transazioni contenute all'interno siano tutte valide e verificate, perché anche la modifica di una singola di quelle transazioni modificherebbe il valore del tx_root.
- **Nonce**. Unico campo che non contiene informazione, è un valore utilizzato dai miner, in combinazione con tutte le altre informazioni, per generare un valore di hash che rispetti i requisiti target imposti dall'algoritmo di consenso Proof of Work. I minatori generano quindi iterativamente un codice hash con le stesse informazioni ma variando solo il nonce, fino a quanto non trovano un hash ammissibile.

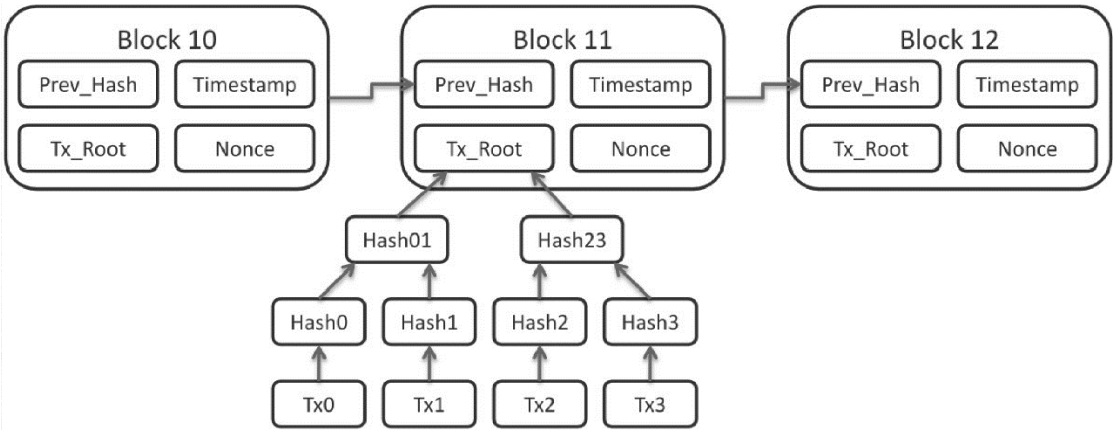

Figura 12. Dettaglio dei blocchi

La componente "chain" delle blockchain regola la logica con cui i blocchi si concatenano, e può essere una linked list come nel caso di Bitcoin, o delle varianti come tangle, usata da IOTA. Alcune rappresentazioni alternative sono mostrate in Figura 13.

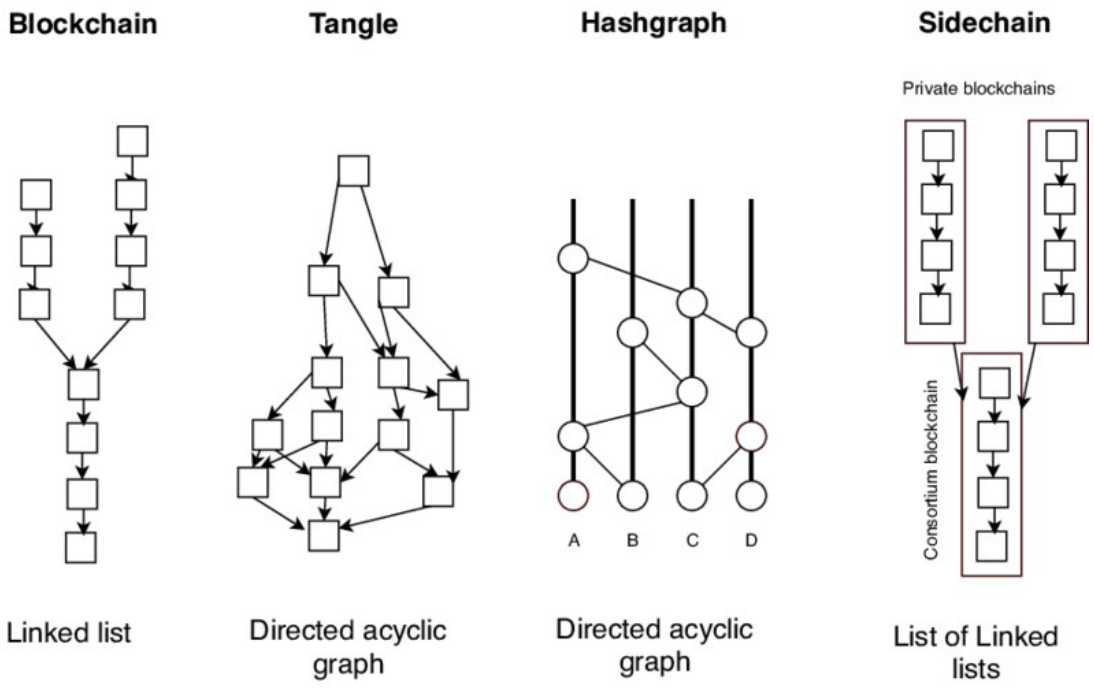

Figura 13. Tipologie di chains

8.2.5 Campi di applicazione

Le tecnologie blockchain e le strategie di consenso distribuito presentano potenzialmente vantaggi significativi, maggiore sicurezza, resistenza alla censura e trasparenza che potrebbero essere utili per una varietà di applicazioni e casi d'uso [61]. Quando si prende in considerazione l'uso della tecnologia blockchain in una nuova area di applicazione, ci si deve chiedere se la blockchain sia la tecnologia giusta per affrontare il problema specifico. La tecnologia blockchain è emergente, ancora in fase di sviluppo, quindi l'identificazione di casi d'uso adeguati e come applicare la tecnologia in maniera appropriata può risultare difficoltoso. In letteratura alcuni autori [62] [63] hanno tentato di affrontare questo tema analizzando i criteri che un caso d'uso deve soddisfare per essere considerato un buon candidato per l'applicazione di tecnologie basate su blockchain. È emerso dallo studio che le blockchain mirano principalmente a gestire transazioni per trasferimento di assets o servizi forniti. Quindi il primo criterio da soddisfare è che gli assets dello use case possono essere rappresentati nella forma di un distributed ledger o un database. In secondo luogo, poiché i nodi della rete sono sconosciuti o comunque non affidabili, il database dovrebbe essere condiviso tra utenti e le modifiche devono essere eseguite su più nodi contemporaneamente, il che significa che le transazioni risultanti sono interdipendenti dalle decisioni di altri nodi. Infine, una domanda cruciale da porsi è perché è richiesto il decentramento: le potenziali ragioni possono essere la riduzione dei costi introdotti dagli intermediari, il raggiungimento di transazioni più rapide e sicure, le procedure di liquidazione automatizzate, la resistenza alla censura, una maggiore resilienza ai guasti, la necessità di rispettare la trasparenza e la regolamentazione e l'eliminazione del necessità di affidarsi a un intermediario di fiducia (ad esempio, la visione dietro Bitcoin e altre criptovalute era quella di eliminare la necessità delle banche come intermediario di fiducia). Inoltre l'uso della blockchain consente di assicurare la tracciabilità delle transazioni, una caratteristica da prendere in considerazione nella valutazione dell'idoneità della tecnologia per lo use case specifico.

8.3 Architetture e Tassonomia

Una rete o un sistema blockchain può seguire regole e architetture di sistema diverse a seconda dell'operazione desiderata e del caso d'uso specifico. I sistemi blockchain sono in genere costituiti da nodi **utente** e **nodi validatori**. I nodi utente possono avviare o ricevere transazioni e conservare una copia del ledger. Oltre ai privilegi di accesso in lettura, i nodi validatori sono responsabili dell'approvazione delle modifiche del ledger e del raggiungimento del consenso in tutta la rete in merito alla validità dello stato del ledger. A seconda della configurazione del sistema, possono essere applicati diritti di accesso parziali o universali e diritti di validazione. Tutti gli utenti possono aderire a una blockchain pubblica. Al contrario, nelle blockchain private l'accesso è limitato ai soli partecipanti autorizzati. I **permissionless ledger** sono condivisi apertamente con tutti gli utenti del network, e sono affidabili e, teoricamente, immutabili poiché qualsiasi membro della rete può contribuire alla convalida delle transazioni. Al contrario, nei **permissioned ledger** solo alcuni nodi validatori possiedono i diritti di accesso in scrittura per modificare la blockchain. Nei ledger pubblici e permissionless, utenti e validatori sono completamente sconosciuti l'uno all'altro, quindi il lavoro di collaborazione e la fiducia richiesti per la gestione dei registri sono garantiti da incentivi e ricompense basate sulla teoria dei giochi. Gli incentivi si basano tipicamente su risorse consumabili come lavoro computazionale, elettricità oppure penalizzazioni che mirano a scoraggiare comportamenti egoistici. Nei registri permissioned e privati l'identità degli utenti è nota a priori. I nodi validatori sono noti e considerati affidabili, pertanto non sono richiesti incentivi per garantire il funzionamento del sistema. Di conseguenza, i registri permissioned e privati possono essere più veloci, più flessibili ed efficienti, tuttavia ciò comporta delle spese per la garanzia dell'immutabilità e la resilienza alla censura. Inoltre, alcune architetture possono essere classificate come **consortium blockchain**, ovvero ibridi che hanno alcune caratteristiche di entrambe le categorie, pubbliche e private.

Le blockchain possono anche essere classificate in base al loro scopo di sviluppo, ad esempio **general purpose** o **specific purpose**. Esempi tipici sono Ethereum, nel caso delle permissionless e Libra ed EBSI, nel caso delle permissioned, tutte progettate per consentire una vasta gamma di casi d'uso e applicazioni. Nello scenario degli specific purpose rientrano Bitcoin, progettata per transazioni di criptovaluta; we.trade [64] dedicata al trade finance; Foodchain [65] per la tracciabilità di filiera; Tradelens [66] per il trasporto logistico delle merci.

In termini di governance e regole di controllo del funzionamento del sistema, le blockchain possono essere classificate come **open-source** o **closed-source**. Le architetture open source sono aperte a tutti i membri della rete e possono beneficiare di contributi dai peer in maniera aperta e trasparente, possono verificarsi dibattiti pubblici e le decisioni sono prese a livello di comunità. Le blockchain a closed-source funzionano in modo simile alle imprese private, dove qualsiasi modifica viene decisa in privato. È importante sottolineare che un'architettura blockchain non si adatta a tutte le applicazioni e ai casi d'uso, quindi è possibile esplorare approcci ibridi che si trovano in qualsiasi punto dello spettro tra blockchain pubbliche e private e hanno vari gradi di centralizzazione. L'architettura scelta e l'algoritmo di consenso applicato sono congiuntamente responsabili delle prestazioni della blockchain, quali velocità, scalabilità ed efficienza delle risorse spese.

La natura decentralizzata delle blockchain ha consentito lo sviluppo di un innovativo concetto di computing su cui si basano le **Distributed Applications (DApp)** su blockchain. Rispetto alle DApp tradizionali basate su una rete p2p classica, le DApp devono rispettare i requisiti definiti nel white paper [67]):

- Applicazione completamente open-source;
- Dati e record delle operazioni storicizzati su una blockchain pubblica;

- Utilizzo di un token crittografico;
- Generazione di token da parte dell'applicazione.

Secondo il white paper le DApp si classificano

- Tipo1: Dapp con una propria blockchain, ad esempio Ethereum;
- Tipo2: Dapp che utilizza la blockchain di una Dapp di tipo 1, ma con token proprietario per il proprio funzionamento;
- Tipo3: Dapp che utilizza il protocollo di una Dapp di tipo 2.

8.4 Cryptovalute e Token

Le criptovalute ed i token sono entrambi degli asset digitali che rappresentano un valore in qualche modo associato alla blockchain, ma si differenziano per natura e scopi.

Le criptovalute sono asset associati esclusivamente alla blockchain di cui fanno parte e sono generalmente utilizzate come sistema di rewarding nelle blockchain basate su proof of work (PoW), come ad esempio Bitcoin ed Ethereum. La corretta verifica del PoW garantisce un certo numero di criptovalute al nodo minatore che è riuscito a completare correttamente il blocco. Tali valute sono utilizzate anche dagli utenti che vogliono usufruire dei servizi della blockchain come ad esempio operare una transazione di valuta sulla rete Bitcoin, oppure caricare uno smart contract su Ethereum. Il costo di ogni azione su BC in termini di criptovaluta è proporzionato alla quantità di risorse che richiede tale azione, in termini di calcolo computazionale e storage, ad esempio caricare uno smart contract è più costoso che richiederne l'esecuzione di una sua funzione. Le criptovalute hanno anche un loro corrispettivo in valuta FIAT e hanno anche assunto nel tempo un valore finanziario notevole, come mostrato in Figura 14.

Figura 14. Storico dell'andamento dei Bitcoin degli ultimi 5 anni ($)

L'andamento delle criptovalute nel tempo è molto fluttuante, per cui il loro valore è volatile. La volatilità è una delle maggiori criticità dell criptovalute. Se la volatilità di una criptovaluta può alimentare la speculazione, e dunque creare un certo interesse attorno a sé, a lungo andare ostacola l'adozione del mondo reale. Per questo motivo si sono affacciate sul mercato le **stable coins** delle valute nate per minimizzare la volatilità dei prezzi, ancorando il proprio valore alle valute fiat, come ad esempio USD Tether (USDT) e Gemini Dollar (GUSD), oppure alle materie prime, come l'oro. La Figura 15 mostra la differenza di fluttuazione tra l'oro ed il Bitcoin. La stabilità permette a una stable coin di essere adottata come mezzo di pagamento. Per qualsiasi valuta la stabilità è fondamentale per lo scambio di beni e servizi senza il rischio che il compratore o il venditore ci rimettano a causa della volatilità dei prezzi.

Inoltre, sono recentemente nate delle stable coin decentralizzate supportate da criptovalute, ovvero con un collaterale che, invece di essere una fiat o una materia prima, è una criptovaluta: in questo caso la collateralizzazione è fatta on-chain, ovvero su blockchain.

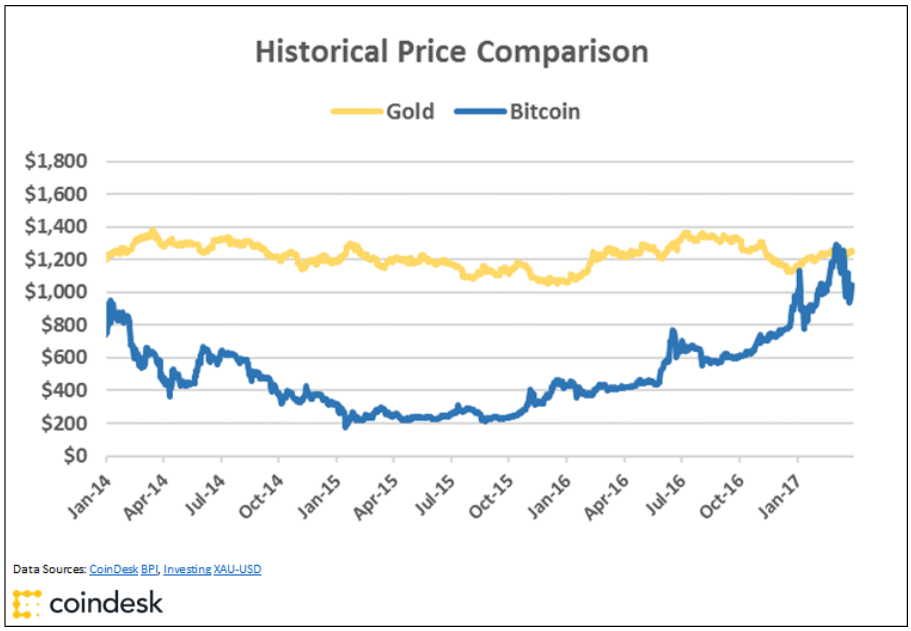

Figura 15. Comparazione andamento Bitcoin e Oro

Attraverso gli smart contract è possibile non solo automatizzare l'esecuzione di operazioni e transazioni, ma è anche possibile creare nuovi token, che possono essere posseduti e scambiati all'interno della stessa piattaforma.
I token sono una particolare tipologia di asset digitali che possono essere scambiati su una Blockchain e che sono spesso utilizzati come rappresentazioni di altri beni digitali o fisici o di un diritto, come la proprietà di un asset o l'accesso a un servizio.
Esistono diverse tipologie di token, che sono riconducibili a tre categorie principali, distinguibili in particolare per lo scopo che le caratterizza e per la tipologia di asset che rappresentano.

- **Utility Token:** rappresentano un asset che serve ad avere accesso a particolari prodotti o servizi, rispetto ad una moneta, tradizionale o digitale, hanno il vantaggio di astrarsi dall'associazione di un valore monetario corrispettivo e facilitano la diffusione e l'accessibilità a tale prodotto o servizio.
- **Security Token**: sono dei token che non sono generalmente associati ad un asset, non necessariamente fisico, che può essere scambiato. A differenza degli utility token non è associato ad un particolare bene o servizio, e il suo valore è esclusivamente legato all'asset o la porzione di asset cui è associato. Questo tipo di token può essere visto effettivamente come investimento finanziario.
- **Debt token:** rappresentano i debiti e quindi saranno valorizzati in base all'ammontare del capitale, del suo interesse e dell'affidabilità del debitore; quello che nella finanza tradizionale sono rappresentati dai bond o mutui.
- **Asset Token:** rappresentano diritti su asset e ne rappresentano il diritto di proprietà, come ad esempio di una società o di un immobile.
- **Equity token**: rappresenta sostanzialmente la proprietà della società sottostante, condividendone le fortune e gli eventuali fallimenti. E, come la proprietà delle azioni di Amazon o Google, i diritti e le varie sottocategorie di azionisti sono definiti dall'atto

costitutivo della società e sue modifiche. Al contrario del sistema tradizionale in cui la quota viene registrata in un database accompagnato da certificato cartaceo, l'equity token sarà invece registrato sulla blockchain riferito alla proprietà aziendale. In base alle necessità aziendali, ultimamente si è sentito molto parlare di ETO (offerte di equity token). Un esempio pratico è il caso dell'azienda tedesca Neufund [68], che si è rivelata una vera apripista per questo modello ibrido di fundraising.

Dal punto di vista tecnico sono emersi alcuni standard principali, che con il tempo sono stati sviluppati, così che essi possano avere caratteristiche ben precise e comuni che li rendano simili tra di essi e che ne semplifichino l'emissione, la conservazione, la transazione. Gli standard più diffusi all'interno di Ethereum e a cui si rifanno anche altre piattaforme che utilizzano i token sono ERC20 e ERC721.

I token ERC20, noti come "fungible", godono delle seguenti proprietà:

- è possibile vederne il bilancio di ciascun account;
- possono essere trasferiti;
- possono avere un valore ed essere utilizzati per i pagamenti di servizi;
- i token sono identici tra loro e possono essere divisibili in sotto parti.

I token ERC721, anche detti "non-fungible", per i quali invece:

- è possibile vederne il bilancio di ciascun account;
- possono essere trasferiti;
- possono avere un valore;
- ciascun token ha un unico identificativo e non è divisibile.

Per comprendere appieno ciò che rende speciali questi token, occorre spiegare correttamente la differenza tra "fungibile" e"non-fungibile".

Quando qualcosa è "fungibile", come ad esempio in questo caso un token ERC20, significa che può essere facilmente sostituito da qualcosa di identico ed è per questo intercambiabile con altre unità della stessa cosa.

Esempi del mondo reale di qualcosa di fungibile potrebbero essere le stesse banconote. Nel caso in cui si prestasse 5 euro a qualcuno, non importerebbe a nessuno se i 5 euro che verranno restituiti non saranno esattamente gli stessi. A questa categoria appartengono difatti tutti quei token che sono utilizzabili come criptovalute, come ad esempio anche lo stesso Ether o Bitcoin.

Tutto questo non è valido quando si ha che fare con un asset che è "non-fungible". Sebbene due elementi possano sembrare identici a colpo d'occhio, ognuno avrà informazioni o attributi unici che li rendono insostituibili o impossibili da scambiare.

Queste caratteristiche corrispondo appunto a quelle dei token ERC721 all'interno di ciascuno dei quali è possibile includere metadati dettagliati su un asset a cui corrispondono e includere informazioni sulla proprietà dello stesso. Questi asset del mondo reale potranno quindi essere adeguatamente digitalizzati e archiviati in un wallet Blockchain, mantenendoli al sicuro e garantendo che non possano essere alterati o contraffatti da terzi.

A differenza delle criptovalute, generalmente associate in rapporto 1:1 con la rispettiva blockchain, ci possono essere diversi tipi di token nella stessa blockchain che rappresentano diversi tipi di asset. Il ciclo di vita dei token inizia e finisce all'interno di una blockchain già esistente. Quindi è possibile creare nuovi token, senza istanziare una nuova blockchain: è sufficiente definire uno smart contract che regola la logica di creazione e distribuzione di tali token. Sia token che criptovalute sono immagazzinati all'interno del digital wallet. Sebbene alcune differenze tra token e criptovalute appiano sfumate, le comunità concordano sul fatto che il dominio delle prime sia strettamente legato al mondo dei pagamenti, fungendo anche come sistema di alimentazione del funzionamento

delle blockchain mantenute dai miners, mentre i secondi siano associato alla fruizione di altri tipi di servizi, asset virtuali reali, fruizione di Dapps ecc.
Le criptovalute ed i token sono uno dei più diffusi casi d'applicazione per la blockchain, nuove criptovalute e nuovi token stanno continuamente emergendo nei mercati, specialmente nel settore energetico. Emettere una criptovaluta nel campo di applicazione energetico può avere dei risvolti in termini di rewarding nei confronti degli stakeholders che offrono dei servizi utili o a minore impatto (ad esempio, nel caso di un'applicazione riguardante le energie rinnovabili, i produttori possono essere ricompensati con un quantitativo proporzionato di token se l'energia prodotta è low carbon o carbon free). Le criptovalute sono utilizzate come metodo di tokenizzazione degli asset in contesti di nuovi mercati o business innovativi in cui si mira alla creazione di co-ownership o condivisione di asset. Un numero sempre maggiore di imprese usano le criptovalute come strumento per attrarre nuovi investitori e come metodo di finanziamento (noto come ICO, Initial Coin Offering). Nel paragrafo sono stati analizzate diverse iniziative a livello internazionale che hanno sfruttato la tecnologia blockchain e le relative criptovalute e token per promuovere iniziative volte ad incrementare la sharing economy, aprire nuovi mercati e nuovi business.
Esempi specifici includono 4NEW [69], una startup britannica che offre un nuovo token di energia chiamato KWATT, attraverso un processo ICO (Initial Coin Offering). Una moneta da 1 KWATT rappresenta 1 kW di elettricità all'anno prodotta da un termovalorizzatore accoppiato ad una mining farm di criptovalute. I possessori dei token possono decidere di vendere l'energia alla elettrica rete nazionale del Regno Unito o utilizzarla per minare altre criptovalute, come Bitcoin ed Ethereum. In sostanza, i possessori di monete KWATT possono evitare di pagare il costo dell'elettricità necessaria per estrarre le criptovalute, che dipende dal sempre crescente consumo di energia e dalla crescente difficoltà degli algoritmi di hashing [70].Analogamente a 4New, una startup PRTI con sede negli Stati Uniti intende costruire un impianto di termovalorizzazione che estrarrà criptovalute [71].Envion, una startup tedesca, utilizza energia solare in eccesso per estrarre criptovalute, mentre HydroMiner utilizza idro generatori a basso costo nelle Alpi austriache [71].
Diverse aziende utilizzano DLT e criptovalute per facilitare gli investimenti nel settore dell'energia rinnovabile e la co-ownership degli asset. Sun Exchange ha sviluppato una piattaforma blockchain basata sulla sharing economy con l'obiettivo di attrarre potenziali investitori in progetti sul fotovoltaico [72]. Le DLT tengono traccia delle ownership e dei ricavi in registri immutabili e forniscono la trasparenza richiesta per la conformità normativa. I potenziali investitori possono acquistare i solar assets, sottoforma di token, che vengono successivamente affittati ai consumatori nei paesi in via di sviluppo, in genere scuole locali e piccole imprese. Gli smart contracts vengono utilizzati per eseguire automaticamente pagamenti dai produttori di energia solare agli investitori, poiché l'energia viene prodotta quasi in tempo reale. In questi casi, le soluzioni basate su blockchain possono ridurre i costi di trasferimento di denaro e aumentare la sicurezza in caso di furto di identità. I pagamenti possono essere eseguiti in criptovalute o FIAT, ovvero valute legali. Sun Exchange ha finanziato con successo 5 progetti nel settore dell'energie solare, per una capacità di 155 kWp, con un ulteriore progetto di 473 kWp in una pipeline vicino a Cape Town, in Sudafrica. Oltre ai pagamenti regolari da progetti supportati, gli investitori possono anche raccogliere 1 SolarCorin per ogni MWh di energia prodotta. WePower, una startup con sede a Gibilterra, sta sviluppando una piattaforma a disposizione dei generatori di FER e investitori interessati a sostenere progetti riguardanti la green energy. Le energie rinnovabili prodotte vengono tokenizzate e successivamente scambiate attraverso la piattaforma per acquistare elettricità o scambiate con valute legali o criptovalute. La piattaforma utilizza blockchain e smart contracts [73]. Seguendo un concetto simile, ImpactPPA [74] mira a sviluppare una piattaforma decentralizzata per il finanziamento di progetti FER, basata su Ethereum. Nel suo progetto ha lanciato due token

energetici, uno (MPAQ) venduto a potenziali investitori per raccogliere capitali per le comunità che hanno scarsa disponibilità di energia elettrica e l'altro (NRG) utilizzato dai consumatori per l'acquisto di elettricità per soddisfare la domanda di energia e tracciare i dati di produzione di energia verde e le relative transazioni. EverGreenCoin è una criptovaluta progettata per facilitare investimenti sostenibili e rinnovabili.

Un'altra piattaforma basata su Ethereum è stata sviluppata da Solar DAO [71].La piattaforma distribuita riunisce le parti interessate alla costruzione di impianti solari. I token DAO possono essere acquistati e scambiati tramite la piattaforma. Le transazioni di sistema sono archiviate in un libro mastro condiviso e possono essere completamente tracciabili e trasparenti.

Anche PROSUME ha introdotto criptovalute per la condivisione di asset di green energy, come ad esempio asset relativi a risorse rinnovabili e storage, in diversi progetti [75]. Green Energy Wallet, una startup tedesca, utilizza blockchain per facilitare il leasing di dispositivi di storage residenziali, come i sistemi di batterie domestiche o batterie EV, per valorizzare l'eccesso di offerta da fonti rinnovabili. Farad segue un nuovo approccio. La società con sede negli Emirati Arabi Uniti ha emesso una criptovaluta basata sulle attività economiche relative alla produzione di ultracapacitori per lo stoccaggio di energia. La criptovaluta si basa su Ethereum e smart contracts, e mira a commercializzare i diritti di proprietà intellettuale e incoraggiare lo sviluppo di soluzioni di accumulo di energia [76].MyBit, una società svizzera, mira a incentivare gli investimenti nei servizi IoT. Hanno sviluppato una soluzione blockchain per investire e gestire le entrate generate nel settore dell'automazione. Una piattaforma di investimento decentralizzata si basa su smart contracts e consente il crowdfunding degli asset e la distribuzione dei ricavi. Inoltre, MyBit ha anche sviluppato MYDAX, uno scambio decentralizzato di risorse IoT [77]. Local-e, una startup con sede negli Stati Uniti, ha lanciato una nuova criptovaluta Sun-e che mira a sostenere finanziariamente gli investimenti locali e nelle energie rinnovabili. Le monete Sun-e sono concesse ai produttori di energia solare ogni 100 kWh di energia verificata prodotta [78].

8.5 Crittografia

La crittografia è uno degli aspetti fondamentali che caratterizzano le blockchain e ne garantiscono la fruibilità e la diffusione. La crittografia infatti abilita una serie di metodologie che consentono di garantire ai nodi della blockchain l'anonimità, l'integrità e l'autenticità delle informazioni scambiate attraverso diverse componenti che saranno analizzate più in dettaglio:

- crittografia simmetrica/asimmetrica;
- firma digitale;
- hashing;
- zero-knowledge-proof.

8.5.1 Crittografia simmetrica e asimmetrica

In via generale la crittografia mira allo studio e l'implementazione di protocolli che evitano che terze parti abbiano accesso a contenuti privati, di qualsiasi forma. La branca della crittografia comprende una vasta gamma di domini, tra cui crittazione (un sotto-dominio della crittografia), matematica, fisica, informatica, scienze della comunicazione e l'elettronica. È inoltre una branca in continua evoluzione, poiché gli algoritmi sono progettati in funzione della difficoltà computativa di risoluzione, e le capacitò computazionali sono in continuo aumento. Sebbene esistano algoritmi che è stato dimostrato essere non risolvibili anche con infinita capacità computazionale, come il one-time-pad (OTP), efficace ma di scarsa applicabilità in quanto richiede una chiave di cifratura di grandezza almeno uguale al messaggio da inviare, l'obiettivo è quello di trovare il giusto compromesso tra usabilità ed efficacia.

Esistono tre macrocategorie di crittografia:

- simmetrica;
- asimmetrica;

La **crittografia simmetrica** è stata la prima storicamente ad essere utilizzata, e comprende tutti gli algoritmi in cui sia il mittente che il destinatario condividono la stessa chiave di cifratura. I cifratori simmetrici sono implementati con:

- Stream Cyphers (cifrari a flusso);
- Block Cyphers (cifrari a blocco).

Gli **stream cyphers** cifrano il contenuto del messaggio andando ad attuare uno XOR tra il contenuto del messaggio da cifrare ed una stringa, chiamata keystream, ottenuta utilizzando uno pseudo-random generator (PRG) che, a partire da un seed di lunghezza limitata, produce una keystream della stessa lunghezza del messaggio, consentendo quindi uno XOR bit-a-bit, per questo è conosciuto anche come cifratore di stato. I PRG generano una sequenza di lunghezza M a partire da una sequenza iniziale (il seed) di lunghezza N, dove M è molto maggiore di N. Il concetto è quello di avere quindi una keystream di lunghezza sufficientemente lunga per poter essere confrontata bit a bit con il messaggio senza dover condividere una chiave segreta della stessa lunghezza. Infatti l'OTP è un caso particolare dello stream cyphers in cui non si fa uso di PRG, ma la chiave stessa funge da keystream per il confronto bit-a-bit, la soluzione come detto è poco praticabile perché di fatto richiede una chiave segreta per ogni messaggio scambiato delle stesse dimensioni del messaggio stesso. Una caratteristica che devono avere gli PRG è l'imprevedibilità dell'algoritmo di generazione della stringa. Infatti la pseudorandomiticità deriva dal fatto che l'unica componente non deterministica degli PRG è il seed, la stringa risultante invece è sempre la stessa e data da un algoritmo che allo stesso seed in input produce lo stesso output (si veda Figura 20).

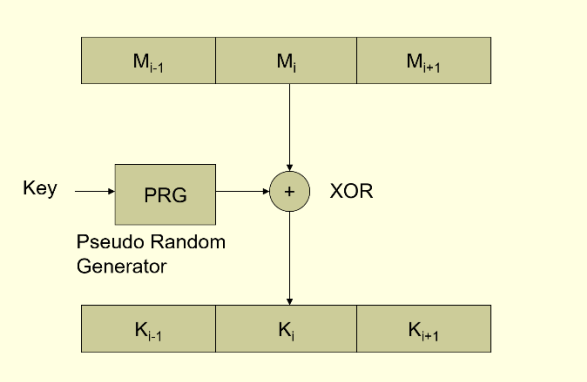

Figura 16. Esempio di cifratore a flusso

È quindi importante che la logica con cui la componente deterministica è generata sia di difficile risoluzione, in quanto altrimenti la conoscenza anche di un solo bit parte della stringa consentirebbe di risalire al contenuto dell'intero messaggio. Gli stream cyphers possono essere:

- sincroni, in cui il mittente ed il destinatario devono essere perfettamente allineati affinchè la comunicazione abbia successo;
- autosincronizzanti, in cui dopo N bit il cifratore si sincronizza automaticamente, riducendo il rischio di failure.

I block cyphers sono costituiti da due algoritmi, uno per la crittazione C ed uno per la decrittazione D. Entrambi come input prendono un blocco b di n bit ed una chiave k. La condizione affinché la cifratura a blocco sia ammissibile è che D sia la funzione inversa di C in modo tale che D(k,E(b,k))=b.

Inoltre il numero di bit di un blocco in input e in output delle funzioni di crittazione e decrittazione devono essere gli stessi.
Esistono diverse categorie di cifratori a blocco, ma i più famosi sono il Data Encryption Standard (DES) e l'Advanced Encryption Standard (AES), molto diffusi e riconosciuti a livello internazionale. Sono stati progettati dal governo americano.
Il DES è un algoritmo che nella sua prima versione lavorava a blocchi di 64 bit, di cui solo 56 effettivamente usati dall'algoritmo, per cui la chiave usata è di 56 bit. Il principio è quello di applicare iterativamente diverse espansioni, trasformazioni, permutazioni e sostituzioni ai sottoblocchi del blocco di input attraverso una funzione di Festel.

- La metà destra del blocco è soggetta ad espansione, quindi da 32 passa a 48 bit;
- Al blocco espanso viene applicato uno XOR con una porzione della chiave;
- I restanti 8 bit della chiave vengono utilizzati per applicare delle sostituzioni, al blocco suddiviso in 8 sottoblocchi da 6bit, chiamati S-boxes, substitution boxes. Attraverso una trasformazione non lineare i blocchi da 6 bit vengono convertiti in blocchi da 4;
- Nella ricomposizione dei sottoblocchi da 4 bit ad un blocco da 32 viene attuato uno shuffling;
- Viene applicato uno XOR con la metà sinistra del blocco di input.

Il processo, mostrato in Figura 17, viene ripetuto per 16 volte.

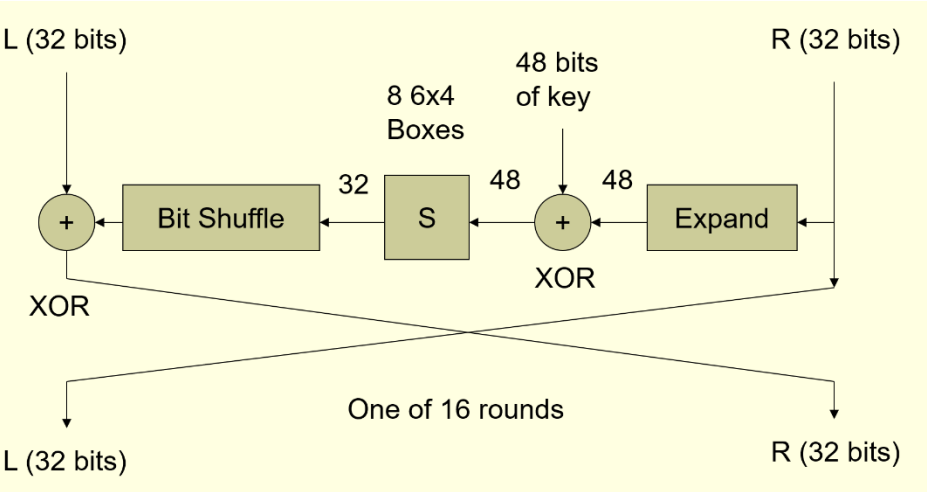

Figura 17. DES

AES ha sostituito il vecchio metodo DES, anche se le varianti più aggiornate di DES, come DES-3, portato a 112 bit, ancora trovano impiego.
AES opera utilizzando matrici di 4×4 byte chiamate stati (states). Quando l'algoritmo ha blocchi di 128 bit in input, la matrice State ha 4 righe e 4 colonne; se il numero di blocchi in input diventa di 32 bit più lungo, viene aggiunta una colonna allo State, e così via fino a 256 bit. In pratica, si divide il numero di bit del blocco in input per 32 e il quoziente specifica il numero di colonne.
I passaggi dell'algoritmo, mostrati anche in sono i seguenti:

- AddRoundKey. Ogni byte della tabella viene combinato con la chiave di sessione, la chiave di sessione viene calcolata dal gestore delle chiavi;
- SubBytes. Sostituzione non lineare di tutti i byte che vengono rimpiazzati secondo una specifica tabella;
- ShiftRows. Spostamento dei byte di un certo numero di posizioni dipendente dalla riga di appartenenza;

- MixColumns. Combinazione dei byte con un'operazione lineare, i byte vengono trattati una colonna per volta.

Il numero di round o cicli di processamento/elaborazione crittografica dei quattro passaggi precedenti è 10 con l'ultimo round che salta il passaggio MixColumns.

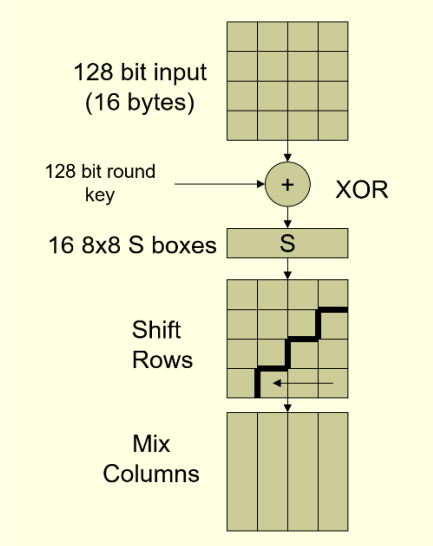

Figura 18. AES

L'introduzione di algoritmi basati su **chiave pubblica** o **asimmetrica** ha rivoluzionato il mondo della crittografia, ed è tuttora la branca più diffusa, su cui si basano molte delle blockchain sviluppate.
La crittografia simmetrica presentava infatti degli svantaggi non trascurabili, in quanto per ogni comunicazione mittente-destinatario era necessario lo scambio di una chiave privata condivisa, il che, con l'aumentare della dimensione del network avrebbe reso sempre più complicata la gestione delle chiavi, in quanto il loro numero cresce in maniera quadratica rispetto al numero di connessioni. Inoltre, in caso di attacco di tipo man-in-the-middle, la comunicazione della chiave segreta in fase di acknowledge tra i nodi comporta la compromissione della segretezza della comunicazione.
In un sistema a crittografia asimmetrica tutti i nodi sono dotati di due chiavi, una pubblica ed una privata.
La chiave pubblica è una funzione della chiave privata; tale funzione è basata su un possibile range di algoritmi (es. curva ellittica). Un messaggio un chiaro viene criptato con la chiave pubblica, e per essere decriptato occorre la chiave privata. Quindi quando il nodo A vuole comunicare con B, A per criptare il messaggio utilizza la chiave pubblica di B, che essendo pubblica viene distribuita a chiunque voglia comunicare con B; per decriptare il messaggio è necessaria la chiave privata di B in possesso solo di B. Questo sistema garantisce che anche in caso di man-in-the-middle il messaggio rimanga comunque secretato.

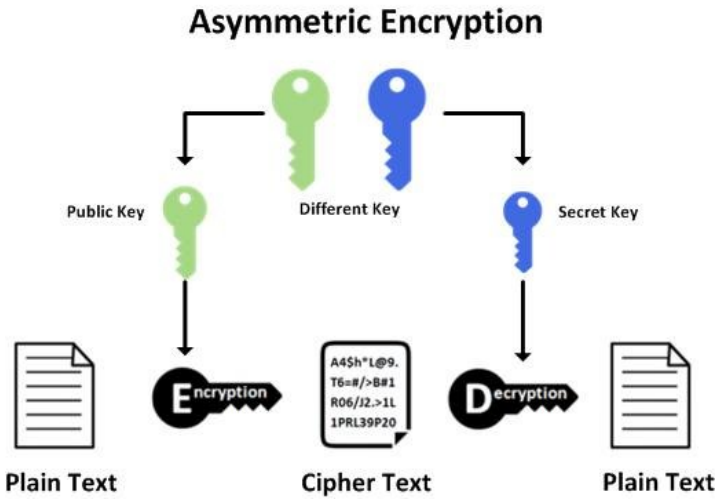

Figura 19. Crittografia asimmetrica

Uno dei più diffusi algoritmi basati su chiave pubblica è **Rivest-Shamir-Aldeman (RSA)**, e si basa sulla difficoltà di fattorizzazione di due numeri primi molto grandi: sebbene sia facile calcolare il prodotto tra due numeri primi, è molto difficile partendo dal risultato finale, capire quali sono i fattori che lo hanno determinato. L'efficacia dell'algoritmo risiede proprio nel fatto che il calcolo del prodotto è immediato, per cui non c'è overhead in fase di crittazione, mentre il calcolo della funzione inversa richiede un tempo computazionale molto elevato. Non è impossibile risalire ai fattori ma, per numeri sufficientemente grandi, molto improbabile.

8.5.2 Firma digitale

Lo stesso concetto di chiave pubblica e privata viene largamente utilizzato per la **firma digitale**, un processo che serve a tutelare l'autenticità del contenuto di un messaggio, di un documento o in generale qualsiasi contenuto digitale. Anche la firma digitale è una componente fondamentale del mondo blockchain, in quanto garantisce ai nodi della rete:

- l'autenticità della comunicazione: ovvero che sto veramente comunicando con il nodo con cui desideravo comunicare;
- l'integrità della transazione: ovvero che il contenuto del messaggio che mi è arrivato è veramente quello che il mittente mi ha inviato e che non sia stato compromesso nel tragitto;
- il non ripudio: ovvero che una volta firmato un contenuto digitale da un particolare nodo, tale nodo non potrà in un secondo momento negare la responsabilità di tale contenuto.

In maniera speculare al funzionamento della crittografia asimmetrica, come mostra la Figura 20:

1. un nodo che vuole trasmettere un documento digitale lo codifica con un algoritmo di hashing;
2. il documento viene criptato con la chiave privata del proprietario ed in questo modo viene firmato digitalmente;
3. una volta ricevuto il documento dal destinatario, per verificarne l'autenticità viene confrontato l'hash ottenuto applicando l'algoritmo al documento inviato con l'hash ottenuto decriptando la firma utilizzando la chiave pubblica del mittente. Se i due hash coincidono il documento è autentico.

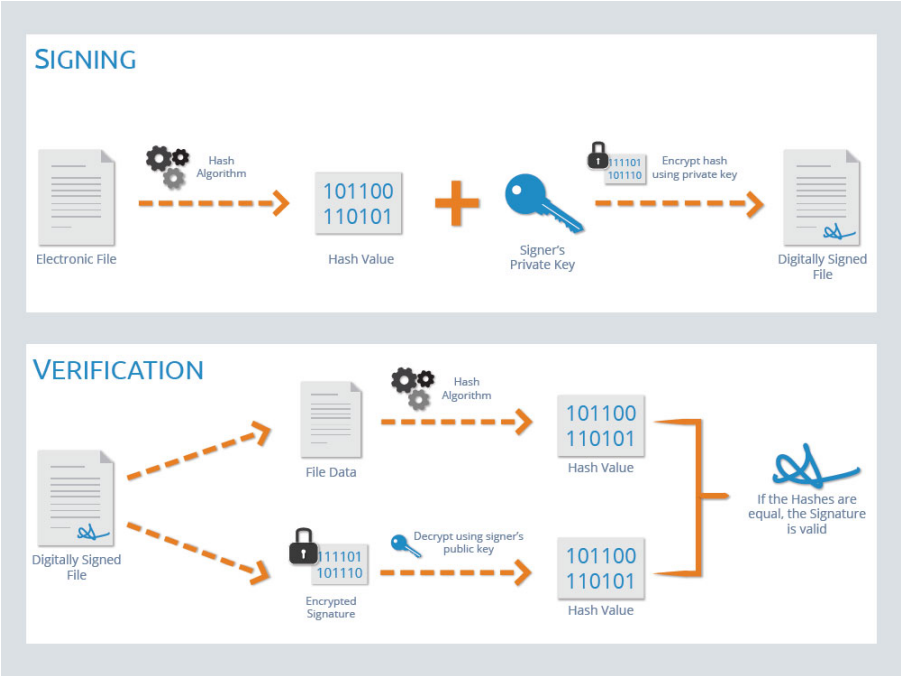

Figura 20. Esempio firma digitale e verifica

8.5.3 Hashing

Le funzioni di hash sono una branca importante della crittografia ed è una delle proprietà caratterizzanti delle blockchain. Le funzioni di hash trasformano un input di qualsiasi lunghezza in un output di una lunghezza prefissata e sono utilizzate come ulteriore mezzo di sicurezza e per la verifica dell'autenticità di una sorgente non verificata, vedi paragrafo 8.5.2.

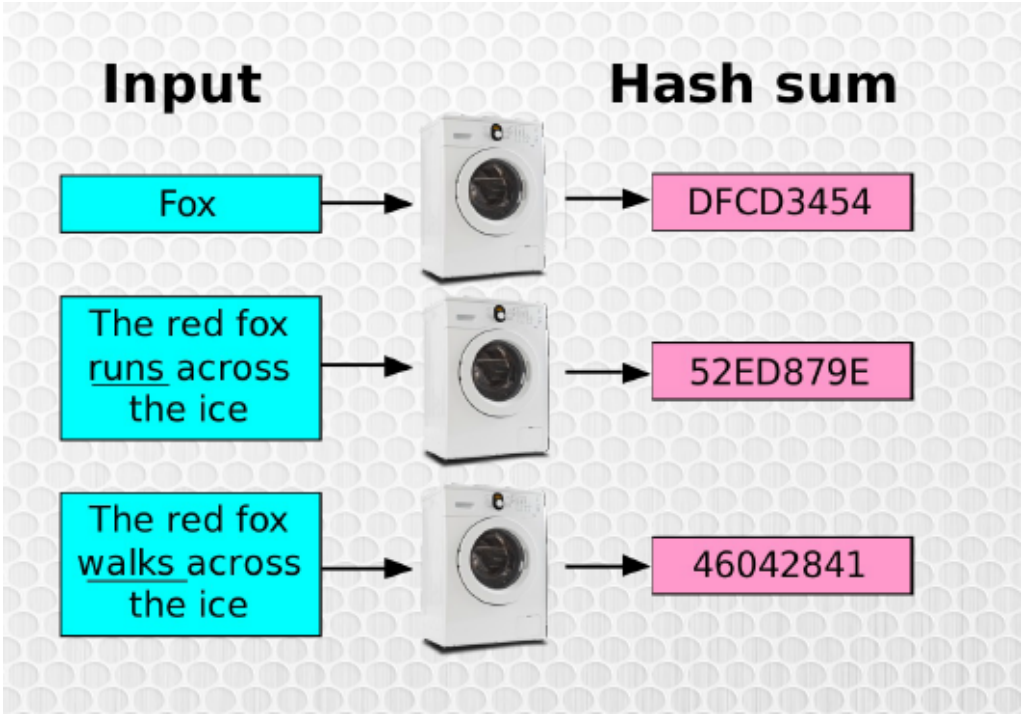

Figura 21. Esempio di hasing di stringhe di testo.

Affinché una funzione di hash soddisfi i requisiti di operatività, deve essere minimizzata la probabilità che due input diano lo stesso output in quanto genererebbe collisioni, ad esempio a livello di wallet, blocchi o transazioni. A differenza dei cifratori, a flusso o a blocchi, le funzioni di hash non sono invertibili, ovvero non è possibile tornare all'input originario una volta applicata la trasformazione.
Una funzione di hash molto diffusa è **MD5**, una versione migliorata del precedente md4, che produce un hash di 128 bit. A causa della suscettibilità ai collision attacks, ovvero il processo in cui vengono identificati gli input differenti che producono lo stesso output, viene oggigiorno utilizzato per scopi non critici, quali ad esempio il checksum di un file, ovvero la verifica dell'integrità del file.
La serie dei **Secure Hash Algoritms (SHA)**, **SHA1** produce un output di 160bit, mentre la sua evoluzione SHA2 ha differenti algoritmi che producono output di differenti lunghezze, dai 224 ai 512 bit. Entrambi però sono stati deprecati in quanto non immuni alle collisioni. SHA3 è la versione più recente della famiglia di funzioni di hash, rilasciato nel 2015, ed è tuttora considerato uno degli algoritmi più robusti e meno proni alle collisioni.

8.5.4 Zero-knowledge-proof

La **zero-knowledge-proof (ZKP)** è un concetto molto diffuso in ambito blockchain in quanto consente di dimostrare la veridicità di un fatto, un documento, in generale un contenuto digitale, senza rivelare altre informazioni, nemmeno il contenuto stesso.
Nella crittografia la ZKP è un metodo per cui un'entità (chi dimostra) riesce a dimostrare ad un'altra entità (chi verifica) che conosce il valore di un contenuto digitale basandosi si nessun'altra informazione a parte la conoscenza del valore di quel contenuto.
La ZKP deve soddisfare tre criteri:

- **Completezza**. Se l'affermazione è vera il dimostratore onesto che segue il protocollo sarà in grado di convincere un verificatore onesto.
- **Validità**. Se l'affermazione è falsa nessun dimostratore imbroglione sarà in grado di convincere un verificatore onesto che l'affermazione sia vera.
- **Conoscenza zero**. Se l'affermazione è vera, nessun verificatore viene a conoscenza di informazioni aggiuntive oltre al fatto che l'affermazione sia vera.

La completezza e la solidità sono proprietà generali che appartengono alla branca generale delle metodologie di dimostrazione, mentre la conoscenza zero è la proprietà principale che caratterizza la ZKP. Tali dimostrazioni non hanno una solida base matematica, in quando c'è una probabilità, seppur minima, che un dimostratore imbroglione convinca il verificatore della veridicità di una affermazione in realtà falsa. Quindi le ZKP sono dimostrazioni probabilistiche piuttosto che deterministiche, ma ci sono delle tecniche che riducono la probabilità di errore a valori sufficientemente piccoli da essere trascurabili.
La struttura generale di una ZKP consiste in tre azioni sequenziali tra due entità coinvolte, A (il dimostratore) e B (il verificatore) le azioni sono definite come:

- witness;
- challenge;
- answer.

La witness consiste nel definire un insieme di domande la cui risposta dimostra la conoscenza dell'informazione che A vuole provare di sapere e che B deve verificare. Successivamente A sceglie causalmente dall'insieme una delle domande ed invia la risposta a B.
Nel processo di challenge, o challenge, B sceglie una nuova domanda dall'insieme e ne richiede una verifica ad A. Infine, nel processo di answer, A manda la risposta a B, che ne verifica la correttezza. Questo processo viene iterano per un numero di volte ritenuto sufficiente a limitare la probabilità che A risponda correttamente perché tira ad indovinare piuttosto che sappia realmente la risposta.

8.6 Protocolli di Consenso e Teoria dei Giochi

La teoria dei giochi è una disciplina della matematica che studia I comportamenti di un soggetto razionale in situazioni di competizione o interazione strategica con altri soggetti o rivali. L'obiettivo di tutti I giocatori è massimizzare il proprio guadagno attraverso l'identificazione della migliore strategia.
Storicamente, la teoria dei giochi ha origine nel 1654 in un carteggio tra Blaise Pascal e Pierre de Fermat a proposito del calcolo delle probabilità applicato al gioco d'azzardo.
Più recentemente, l'introduzione ai problemi e l'identificazione di alcuni fondamentali concetti legati alla teoria dei giochi risale ad un libro del 1944 pubblicato da John von Neumann e Oskar Morgensten, un matematico e un economista, dal titolo "Theory of Games and Economic Behviour". L'obiettivo degli autori è quello di descrivere, attraverso alcuni concetti matematici, il comportamento umano nei casi in cui l'interazione implichi la vincita o la spartizione di una risorsa.
Una ulteriore e fondamentale spinta alla teoria dei giochi è stata data da John Forbes Nash Jr. che ha dimostrato l'esistenza di soluzioni ottimali per giochi competitive non collaborativi, la cui definizione verrà fornita più avanti.
Come accennato prima, l'obiettivo della teoria dei giochi è l'identificazione e lo studio della funzione guadagno per identificare quei comportamenti, o strategie, che massimizzano il risultato utile per i giocatori.
Un gioco è completamente definito una volta che siano state identificate la funzione guadagno e le possibili strategie che ogni giocatore può intraprendere.

8.6.1 Giochi cooperativi e non cooperativi

Una primissima classificazione dei giochi può essere data dalla distinzione tra giochi cooperativi e non cooperativi (o competitivi). Come suggerisce il termine, un gioco cooperativo a più giocatori e quello in cui l'accordo tra i giocatori garantisce a questi ultimi un risultato migliore di quello che avrebbero senza accordo. In particolare, il valore massimo della funzione di guadagno si ha quando il numero dei partecipanti all'accordo è uguale al numero di giocatori. Sia V la funzione guadagno, R l'insieme di n giocatori, allora, per ogni sottoinsieme Gi $\subseteq$ R, vale che:
V(G1) + V(G2) + … + V(Gk) < V(R)
dove K = 2n-1 è il numero massimo di sottoinsiemi di R. In questo caso, la funzione V non identifica come verranno spartiti i guadagni ma indica che il massimo ottenibili da una coalizione è quello che si raggiunge se tutti i partecipanti si accordano.
Nel caso di giochi non cooperativi, l'accordo tra i giocatori è espressamente vietato o impedito ed ogni giocatore punta ad ottenere il massimo per sé stesso.

8.6.2 Giochi simultanei o sequenziali

Una caratteristica dei giochi è data dall'ordine in cui le strategie vengono applicate: nel gioco della dama le mosse si susseguono una di seguito all'altra ed ogni giocatore conosce tutte le mosse precedenti, sia le proprie che quelle dell'avversario, e cerca di indovinare le successive. In questo caso, le azioni si susseguono in ordine sequenziale, sempre prima uno e poi l'altro giocatore, fino al termine della partita. È possibile, però, immaginare di giochi in cui l'ordine delle azioni non è rilevante ma, soprattutto, un giocatore non conosce la mossa dell'altro, che avviene contemporaneamente alla propria.
Un esempio di questo tipo di gioco è fornito dal Dilemma del prigioniero e da molte delle sue varianti. Il gioco è descritto come segue. I due giocatori hanno commesso un reato grave e dei reati minori per cui sono stati arrestati dalla polizia. Senza la confessione di almeno uno dei due, la polizia

non ha elementi sufficienti per accusare i prigionieri del reato grave ma solo per i reati minori. Se un giocatore collabora accusando l'altro, la polizia lo rilascerà e farà condannare l'altro a 3 anni, accusandolo di tutti i reati. Se nessuno dei due collabora, entrambi verranno condannati ad 1 anno di carcere per i soli reati minori, mentre se collaborano entrambi la condanna sarà di 2 anni.

Tabella 4. Schema rappresentativo del dilemma del prigioniero

		A	
		Non confessa	Confessa
B	Non confessa	(1,1)	(0,3)
	Confessa	(3,0)	(2,2)

In Tabella 4 sono riportate schematicamente i dati che illustrano il dilemma del prigioniero. Guardando lo schema, la soluzione sembra semplice: entrambi i giocatori non confessano e sconteranno 1 anno di pena ciascuno. Però questa soluzione non è corretta. Supponiamo che A decida di non confessare. La strategia migliore per B sarebbe di confessare perché, così, verrebbe rilasciato. Se A confessasse, allora ancora la strategia migliore per B è quella di confessare, riducendo il totale della pena di un anno. Quindi in ogni caso, la strategia migliore per B è confessare in ogni caso. Analogamente, cercando la migliore strategia per A, la soluzione sarebbe ancora confessare comunque. La scelta di A è B sarà di confessare qualsiasi sia quella dell'avversario: questo è un esempio di equilibrio di Nash. L'equilibrio di Nash è la soluzione di un gioco in cui ciascun giocatore decide la propria strategia ottimale indipendentemente da quella degli altri e in cui non c'è nessun ulteriore guadagno nel modificare la propria scelta.

Questo esempio permette di definire il concetto di strategia dominante per un giocatore. Sia ui(si, sj) la funzione guadagno dell'i-esimo giocatore in che dipende dalla sua strategia si e dalle altre sj allora si è dominante se vale ui(si, sj) $\geq$ ui(s'i, sj). Cioè la strategia dominante per un giocatore è quella che massimizza il proprio guadagno in funzione delle strategie degli altri giocatori. È facile vedere che confessare rappresenta la strategia dominante per il giocatore A (o B) nell'esempio riportato sopra.

Per giochi sequenziali, la tabella riportata sopra non è la migliore rappresentazione, perché non illustra la sequenza delle scelte operate dai giocatori. Un esempio di gioco sequenziale può essere immaginato come segue. Supponiamo che un'azienda (A) voglia entrare in un mercato che è monopolizzato dalla presenza di un singolo player (B) molto forte. La scelta di A è quella di entrare oppure no nel mercato. Dall'altra parte, l'azienda B può decidere se competere per mantenere il monopolio, ad esempio operando uno sconto sul prodotto oppure rinunciare, riducendo le proprie quote di mercato facendo entrare il competitor. Nel caso in cui A decida di entrare e B di competere, il costo della competizione si ripercuoterà sui guadagni di entrambe le aziende.
Una rappresentazione della situazione è la seguente:

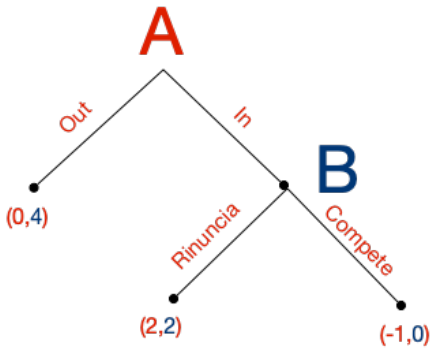

Figura 22. Esempio di gioco sequenziale

Nel grafo precedente, i guadagni di ciascun giocatore sono indicati nel fondo della riga conseguente. Anche in questo caso, si può dimostrare che la strategia scelta sarà, per A, quella di entrare nel mercato, mentre per B sarà quella di rinunciare alla competizione, mantenendo almeno in parte le proprie quote e, quindi, ridurre i propri guadagni. L'esempio delle due aziende introduce un concetto che verrà poi utilizzato nell'analizzare la teoria dei giochi applicata alle blockchain: il risultato in cui A decide di entrare e B di competere per mantenere il monopolio tiene conto del *costo* che entrambe le aziende pagheranno per i loro sforzi. In questo caso, il guadagno di A sarà negativo perché riuscirà a conquistare delle quote di mercato, supponiamo che il guadagno sia ancora 2, ma dovrà pagare 3 per ottenere questo risultato, con un guadagno pari a -1. Analogamente, B manterrà solo una parte del mercato, ma dovrà pagare 2 per lo sforzo fatto, con un guadagno 0.

8.6.3 Giochi ad equilibrio instabile e di coordinamento

Si consideri un gioco che abbia come tabella rappresentativa la Tabella 5 e che, per una qualche causa durante il gioco la situazione di equilibrio trovata dai giocatori non sia (4,4) ma (2,2). In questo caso, se si rimuove la causa che ha originato questa situazione, l'equilibrio si sposterà naturalmente verso la posizione (4,4), quella di maggior guadagno per entrambi i giocatori. In alcune situazioni, lo spostamento dall'equilibrio può avvenire per fattori perturbativi esterni e potrebbe non generare un'altra situazione di equilibrio se non dopo molto tempo. Applicando questi concetti a realtà socio-politiche mondiali, si può capire che azioni destabilizzanti anche moralmente corrette, come l'abbattimento di un dittatore, possano generare situazioni instabili per lungo tempo, dove il guadagno complessivo risente notevolmente delle energie spese per ottenerlo.

Tabella 5. Situazione Instabile

	A	
B	(2,2)	(0,0)
	(0,0)	(4,4)

La stessa Tabella 5 può essere utilizzata per affrontare un altro problema comune nel sistema delle blockchain, quello della coordinazione delle azioni. Se la posizione di equilibrio è ancora (2,2) ma, in questo caso, il numero di giocatori è particolarmente alto, centinaia o migliaia, lo spostamento verso l'equilibrio più vantaggioso richiede una qualche sorta di incentivo o di motivazione che convinca la maggior parte dei giocatori nello scegliere la nuova strategia, vincendo l'inerzia che un punto di equilibrio stabile di solito genera. In questo caso, il gioco fallisce se solo una parte minoritaria dei giocatori sceglie il nuovo punto di equilibrio.

8.6.4 Il problema dei generali bizantini

Il problema descrive la situazione in cui alcuni generali devono conquistare la città di Bisanzio ma tra le loro fila potrebbero esserci dei traditori. La situazione è tipica in reti complesse di computer in cui uno (o più) dei nodi potrebbe non funzionare correttamente sia per un guasto software: i messaggi che arrivano da questi nodi, che non sono identificati, sono incoerenti con quelli del resto della rete e possono generare dei danni fino alla distruzione della rete stessa o al fallimento del lavoro collaborativo.
Tornando ai generali bizantini, ogni generale ha la scelta se attaccare in collaborazione con gli altri o ritirarsi: solo un attacco coordinato da parte di tutte le truppe porta alla conquista della città mentre un attacco scoordinato porta alla disfatta completa degli assedianti.
Il problema, per semplicità, può essere ridotto a 3 soli generali, A, B e C ed ai loro messaggeri.
Il caso semplice è quello in cui tutti e 3 i generali sono d'accordo e decidono di attaccare o ritirarsi in maniera coordinata. In questo caso, il messaggio "Attacco!" o "Ritirata!" viene scambiato correttamente tra i partecipanti.
Se, invece, uno dei generali fosse un traditore, possono essere individuate due situazioni:

- A comunica a B e C che vuole attaccare, ma B comunica a C che si deve ritirare, cosa che, a detta di B, farà anche A. Ancora, il traditore in questo caso è B ma né A né C possono capirlo e smascherarlo. L'attacco sarà destinato a fallire.
- A comunica a C che vuole attaccare e, contemporaneamente, a B che vuole ritirarsi. C riceve da A il messaggio che deve attaccare e da B quello che deve ritirarsi, non sapendo assolutamente cosa fare. A è chiaramente il traditore ma né B né C possono scoprirlo. L'attacco fallirà miseramente.

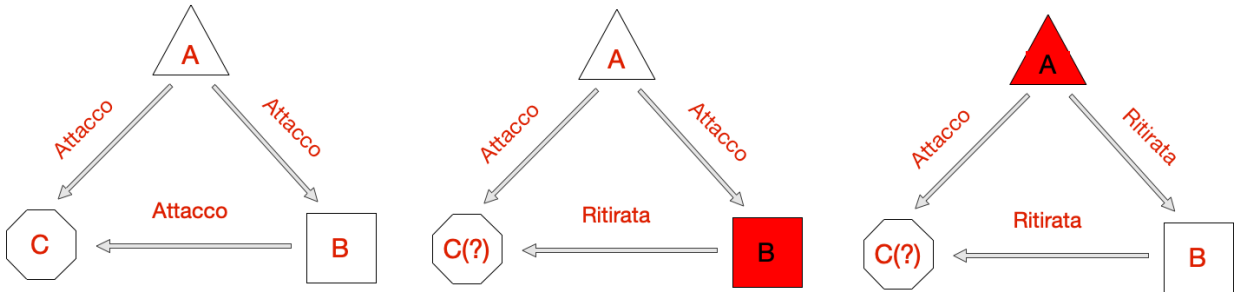

Figura 23. Rappresentazione grafica del problema dei Generali bizantini

Il problema venne proposto da Leslie Lamport [79] nel 1982 e, nello stesso articolo, l'autore propose una soluzione dimostrando che se il numero di generali è M, non esiste soluzione quando il numero di traditori T è tale che M<3T, ovvero quando il numero di traditori è maggiore ad un terzo del numero dei generali complessivi.
Nella blockchain, i metodi di consenso, insieme con alcuni elementi della teoria dei giochi presentati in precedenza, permettono di identificare i *traditori* all'interno della rete prima che il loro numero diventi critico.

8.6.5 Blockchain e teoria dei giochi

In una blockchain possono essere identificati due tipi di giocatori:

- I miner;
- I semplici user.

Come visto in precedenza, il ruolo del miner è fondamentale per garantire l'integrità della rete e permette la creazione di nuovi blocchi. D'altro canto, l'attività di mining può essere remunerativa abbastanza da garantire un vantaggio economico a chi riesce a creare nuovi blocchi.

Dal punto di vista del guadagno, il miner partecipa al gioco fino a quando il numero di successi è sufficiente a garantire un ritorno economico considerato ragionevole rispetto agli investimenti fatti. In questo caso, un ruolo fondamentale lo gioca il valore in fiat della criptovaluta utilizzata dalla specifica blockchain: questo è un parametro che viene determinato, nella maggior parte dei casi, dal mercato speculativo che non segue regole definite.
Dall'altra parte, però, un miner potrebbe avere un interesse, anche economico, nel momento in cui mette in atto comportamenti pericolosi per la rete tra cui:

- Creare blocchi falsi con informazioni modificate a suo vantaggio;
- Creare blocchi che non rispettino le richieste della procedura di consenso.

Nella analisi seguente, viene presa in considerazione una blockchain che utilizzi come protocollo di consenso il "proof-of-work" che risulta essere quello più aperto e, quindi, quello più soggetto ad attacchi malevoli.
La blockchain è una catena di blocchi legati uno all'altro tramite una chiave, in particolare, ogni nodo contiene l'hashcode del nodo che lo precede.
Nella catena possono essere identificati:

- Il primo nodo o nodo "genesis";
- Il nodo padre: il nodo che precede un blocco specifico. Ad esempio, il blocco 13 è il padre del blocco 14;
- Il costo computazionale che è stato richiesto per creare il blocco (proof-of-work).

Lo score del blocco che è una funzione definita come, in funzione del numero del blocco:

- Score(0) = 0 (lo score del blocco genesis è 0):
- Score(n) = Score(n-1) + proof-of-work;

Lo Score, quindi, è una funzione crescente nel tempo che non può essere determinata a priori in base alla conoscenza del suo valore nei blocchi inseriti nella catena. La Figura 24 mostra un esempio di catena a blocchi: la freccia indica la direzione di evoluzione della catena. Ogni blocco contiene il riferimento al blocco precedente e un proprio "Score" che aumenta con il crescere del numero di blocchi.

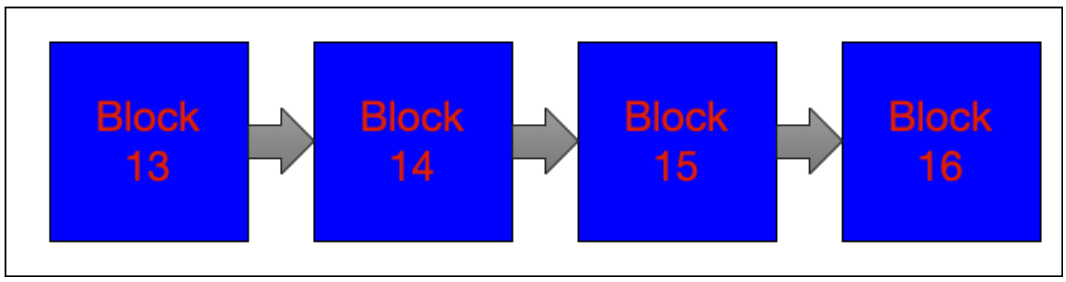

Figura 24. Esempio di catena di blocchi

Come visto in precedenza, l'aggiunta di un nuovo blocco avviene quando un miner risolve un determinato problema matematico e gli altri nodi verificano la soluzione. Come nel gioco della maggioranza, solo quando la maggioranza dei nodi verifica la soluzione proposta il nuovo blocco viene inserito all'interno della catena. In questo modo, è impossibile inserire nodi che non rispettino le regole del gioco: un eventuale attacco informatico dovrebbe essere coordinato su centinaia o migliaia di nodi contemporaneamente per poter permettere la validazione e l'inserimento di un nodo non valido. Sebbene possibile, la probabilità di successo di questo tipo di attacco decresce notevolmente con l'aumento del numero di nodi partecipanti alla rete. Già con soli 100 nodi, se si considera p la probabilità di successo di questo tipo di attacco su di un singolo nodo, il valore della probabilità di successo su 51 nodi è pari a (p)51. Anche considerando una probabilità di successo di

un attacco sul singolo nodo molto alta, ad esempio 80%, la probabilità complessiva di successo dell'attacco coordinato alla rete blockchain risulta pari a P=1x10-5.
Se V è il vantaggio massimo ottenibile da questa operazione, la probabilità di successo è così bassa che il vantaggio atteso v = V x P risulta essere comunque molto piccolo. D'altra parte, è molto alto il rischio che il truffatore venga scoperto e cacciato dalla rete.
Dal momento in cui un miner propone un nuovo blocco in forza della soluzione trovata a quando questo nodo entra effettivamente a far parte della catena passa un certo tempo: in questo periodo è possibile, come accade nella realtà, che un altro nodo trovi un'altra soluzione valida, proponendo un blocco differente dall'altro. In questo caso, la catena presenta un "fork" che deve essere gestito onde evitare incongruità all'interno della rete.

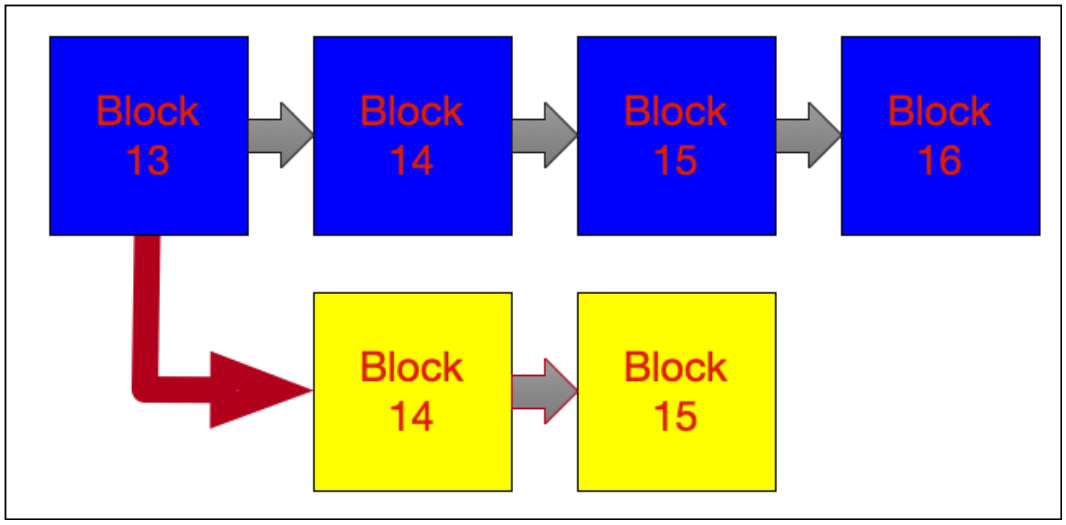

Figura 25. Catena con fork

Un fork può essere creato artificiosamente da miner disonesti che, per ottenere dei vantaggi economici, cercano di inserire blocchi non validi. Ad esempio, il proprietario del miner X effettua una transazione scambiando una certa quantità di bitcoin per ottenere un bene o un servizio. Questa transazione viene registrata nel blocco 14.
A questo punto, egli forza il suo miner alla creazione di un nuovo blocco 14, che non contiene la transazione effettuata. Questo è un esempio di "double spending" di una moneta elettronica: una volta che l'utente si è assicurato un bene o servizio, allora opera per far si che la transazione di pagamento venga cancellata e nel suo "wallet" risulti un ammontare di moneta maggiore del reale.
Guardando la Figura 25 è facile intuire che lo Score del blocco 16 (blu) è certamente più alto di quello del blocco 15 non valido (giallo): tutti gli altri miner, al momento di scegliere quale blocco utilizzare per proseguire la catena, scelgono quello con lo Score più alto. In questo modo, ogni eventuale fork diventa sterile dopo un numero piccolo di passaggi e viene abbandonato.
Sia nel caso in cui il fork sia generato casualmente che artificiosamente, nel momento in cui un qualsiasi miner verifica il nuovo blocco inserito aggiorna la propria catena e comincia a lavorare per produrre ulteriori blocchi, nell'ottica di una competizione in cui il fattore temporale è fondamentale. Man mano che il nuovo blocco viene approvato, sempre un maggior numero di miner fa questa operazione.
Sia N il numero di miner nella rete, p(Δt) la probabilità che dopo un certo periodo di tempo Δt un miner abbia verificato il nuovo blocco e iniziato il calcolo per proseguire nella competizione. Allora dopo un periodo Δt, che è il tempo che intercorre tra la proposta del blocco 14 blu e quello del blocco 14 giallo il numero di miner che avranno approvato il blocco e ricominciato a lavorare è

$n(T) = N \times P(\Delta t) \times \Delta t + [N \times (1- P(\Delta t)) \times P(\Delta t)] \times 2\Delta t \ldots$

Se N = 100 e P(1s) = 40% (probabilità dopo 1 secondo) dopo un secondo 40 nodi avranno approvato il blocco e 60 no, mentre dopo 2 secondi questo valore è pari a 64, mentre dopo 3 secondi è pari a 78. Se dopo 3 secondi appare il nuovo blocco 14 giallo, allora solo 22 nodi avranno il "dubbio" di quale nodo prendere in considerazione effettivamente. Anche se tutti e 22 lavorassero con il nuovo nodo, la probabilità che la catena gialla continui è estremamente bassa. Quindi, dopo un po', anche gli ultimi 22 miner smettono di lavorare sulla catena di minoranza perché non remunerativo.

Come visto in precedenza, l'algoritmo di consenso "proof-of-work" non è l'unico che viene implementato all'interno di una blockchain: altri metodi prevedono la possibilità che i miner non si comportino correttamente introducendo il concetto di "punizione". Nei giochi che fanno uso di questo concetto, il guadagno deve essere ridotto del rischio associato al fallimento ed al valore della punizione. Se il guadagno massimo di una rapina in banca fosse G con una probabilità di successo pari a $p(G) < 1$, mentre la punizione fosse C associata alla probabilità di un fallimento pari a $p(c) = 1 - p(G)$, allora il valore atteso per la rapina sarebbe:

$G_{att} = G \times p(G) - C \times (1-p(G))$

Se $p(G) = 1/2$ e $C = G$ (il ladro una volta preso deve restituire il maltolto) allora Gatt = 0 e il ladro non avrebbe nessun guadagno dal rapinare la banca. Se aggiungesse anche il rischio di essere condannato a diversi anni di galera, razionalmente il ladro non dovrebbe rubare.
Nel caso del protocollo di consenso "proof-of-stake" i proprietari dei miner versano un ammontare di denaro considerevole per partecipare al gioco come miner: questo denaro viene perso se il comportamento all'interno della rete non è quello corretto. In questo caso, il numero dei miner è notevolmente più basso, quindi la probabilità di successo di un eventuale attacco notevolmente più alta. D'altra parte, il costo di un eventuale insuccesso è notevolmente più alto rendendo ancora sconveniente un comportamento malevolo.

8.6.6 Algoritmi di consenso

In quanto sistema decentralizzato, la registrazione di un'informazione, transazione o in generale la scrittura di dati all'interno della catena di blocchi di una blockchain è regolata da un algoritmo di consenso, che gestisce tali operazioni. Tale algoritmo va ad identificare, fra i diversi nodi di una blockchain che si sono candidati alla gestione dei blocchi e quindi possono eseguire verifiche e scritture su di essi (e quindi non solo letture), il soggetto che è autorizzato a salvare in blockchain gli ultimi dati mandati in scrittura ma ancora in attesa di essere "congelati".
In altre parole, ogni volta che uno dei miner (i soggetti della blockchain che possono creare nuovi blocchi e quindi scrivere nella blockchain) ha accumulato sufficienti dati per un nuovo blocco, può crearlo seguendo quello che è il protocollo di consenso della blockchain.
La prima blockchain della storia è nata nel 2008 e nella sua formulazione, descritta da Satoshi Nakamoto, adottava come algoritmo di consenso il proof of Work. Successivamente, con lo svilupparsi della tecnologia e la nascita di altre piattaforme, sono comparsi altri algoritmi di consenso, sempre nel tentativo di conciliare sicurezza, decentralizzazione, prestazioni e scalabilità. In questo panorama alcuni di essi hanno avuto più o meno fortuna, altri sono tentativi più o meno originali o eccentrici di dare un contributo allo sviluppo del tema.
Di seguito una descrizione sommaria dei principali algoritmi di consenso.

Proof of Work (PoW)

Proof of Work (PoW) è il primo algoritmo adottato, quello descritto nell'articolo di Nakamoto [51] e quello in uso nella blockchain Bitcoin. In seguito è stato adottato da altre blockchain, come Ethereum, e da altre criptovalute. L'algoritmo va a scegliere il responsabile della creazione del blocco (miner) e quindi della conferma delle transazioni. La scelta del miner viene fatta andando a verificare che lo stesso miner, una volta raccolta dalla rete le transazioni dei vari utenti, abbia creato il blocco rispettando alcune caratteristiche per il blocco stesso, e quindi andando a fare il lavoro di elaborazione (work) necessario per il rispetto di queste caratteristiche. In altre parole, il miner, nel creare il blocco deve eseguire una elaborazione molto pesante in termini di sforzo computazionale, e questo sforzo può essere facilmente verificabile dalla rete alla fine della elaborazione. Il primo a creare un blocco secondo le caratteristiche richieste aggiunge il blocco stesso alla catena facendola crescere, ma ciò non impedisce che possano esserci altri miner che aggiungono dei blocchi, creando a tutti gli effetti dei fork nella catena. La blockchain però si riserva un periodo in cui il sistema "rimane a guardare", cioè aspetta di capire quale delle ramificazioni andrà a crescere più rapidamente, e quindi su quale di esse gli utenti della rete andranno a convergere. Questa versione diventerà la versione "finale" della blockchain, andando a scartare le altre. Questo sistema isola i comportamenti malevoli, che possono (benchè con gran impiego di risorse) inserire inizialmente dei blocchi artefatti, ma nel tempo vengono sostituiti da blocchi che ricevono maggior consenso dagli utenti.

Proof of Stake (PoS)

L'algoritmo Proof of Stake (PoS) è stato introdotto nel 2011, come prima alternativa a PoW ed è al momento l'alternativa ad esso più adottata. Il limite e svantaggio principale di PoW consiste nel suo crescente bisogno di risorse per poter soddisfare le richieste in fase di creazione di nuovi blocchi, con un consistente impiego di energia elettrica, e forti problemi di sostenibilità. Ad esempio, nel 2014 per la generazione di un singolo Bitcoin servivano circa 240kWh, circa 16 galloni di gas, e il consumo è stato sempre in crescita, proprio in basa all'originari definizione dell'algoritmo: benché si parli di stime approssimative, alcune valutazione riportano che nel 2018 la rete Bitcoin consumava quanto l'intera Svizzera. Per avere un algoritmo di consenso che utilizzasse meno energia, e fosse anche più ecologico, si è arrivati alla proposta di PoS, che impiega molta meno energia.

Nell'algoritmo PoS, la scelta del miner (validatore) viene fatta fra coloro che all'interno della blockchain hanno un deposito di moneta virtuale. Sono poi stati definiti diversi modi per fare tale scelta, sempre nel tentativo di evitare che dei soggetti possano prendere il controllo della rete e essere costantemente gli unici a generare i blocchi. Tra queste modalità, alcune si basano sulla casualità, o sulla quantità, altre sia sulla quantità di denaro posseduta che sull'anzianità del soggetto e del deposito, altre sulla quantità di scambi che vengono fatti da chi possiede la moneta, andando così proprio ad incentivare la movimentazione della moneta. L'idea alla base è che coloro che posseggono moneta nella blockchain sono quelli che più dovrebbero avere interesse a far funzionare correttamente la blockchain. Esiste un dibattito comunque sul fatto che PoS possa dare minori garanzie in termini di decentralizzazione e sicurezza rispetto ad PoW o altri algoritmi. Uno dei problemi di PoS è chiamato "Nothing-at-stake", che indica la possibilità di un validatore di creare due blocchi contemporaneamente per incassare le commissioni delle transazioni su entrambi i blocchi. Per risolvere tali problemi sono studiati meccanismi che vadano a bloccare temporaneamente il deposito del validatore, e "bruciarlo" in caso di comportamento scorretto.

Peercoin è stata la prima blockchain a usare PoS; Ethereum, nella versione Casper, passerà a PoS per cercare di aumentare la sua scalabilità

Delegated Proof of Stake (D-PoS)

L'algoritmo Delegated Proof of Stake (D-PoS) è un'ulteriore versione del PoS, nel quale l'onere di generare i blocchi e creare moneta ricade potenzialmente non su tutti i partecipanti alla blockchain che possiedono moneta, ma su un loro sottoinsieme chiuso e limitato, scelto attraverso una votazione fatta dall'intera rete. Tutti possono provare ad entrare nell'insieme dei delegati, ma devono raccogliere un numero di voti sufficiente. Il sistema di votazione e i voti disponibili ai soggetti della rete dipendono a loro volta dalla quantità di monete possedute. DPoS è stato implementato da Daniel Larimel, sulla rete Bitshares.

Proof of Authority (PoAu)

Proof of Authority (PoAu)è un algoritmo di consenso basata sul concetto di reputazione, ed è una delle soluzioni più ambita da imprese e reti che preferiscono partecipare a blockchain private e chiuse dove può essere mantenuto un livello alto di privacy. La PoAu non prevede alcun meccanismo di mining: i soggetti della rete che vogliono agire come validatori dei blocchi si devono registrare e identificare, e poi vengono selezionati attraverso una determinata procedura. Inoltre i validatori rimangono sotto osservzione, per verificare il loro comportamento e scoprire eventuali atteggiamenti scorretti. Come anche il nome suggerisce, questo algoritmo di discosta dall'idea originaria di decentralizzazione della rete, poiché per sua natura introduce dei soggetti che sono riconosciuti come i gestori della rete, centralizzando quindi il meccanismo di creazione dei blocchi. Mantenendo un numero di validatori limitato, questo algoritmo è altamente scalabile, veloce e inoltre non energivoro. D'alotra parte, si creano dei punti di vulnerabilità ben precisi, poiché essendo i validatori ben definiti e pubblici, possono essere attaccati da soggetti che vogliono compromettere il sistema.

Proof of Activity (PoA)

L'algoritmo di Proof of Activity cerca di unire caratteristi che vantaggi dei due algoritmi PoW e PoS. In pratica, in PoA vengono separate le due attività fatte dal miner: la creazione del blocco e la validazione. In pratica, in PoA viene adottato l'algoritimo di Pow per creare il blocco, che quindi è creato attraverso l'uso di
una capacità di calcolo per poter soddisfare la struttura del blocco stessa, e in seguito viene validato attraverso PoS, da un insieme di delegati scelti secondo l'algoritmo stesso.
Per proteggere una blockchain dalla possibilità di un attacco 51%, PoA potrebbe essere una buona scelta poiché offre i vantaggi di entrambi gli algoritmi di consenso ed è più sicuro di entrambi separatamente. D'altra parte però mantiene anche svantaggi di entrambi, come il consumo di risorse e problemi come la doppia firma sulle transazionoi ("Nothing-at-stake").
Questo algoritmo non è molto usato.

Proof of Importance (PoI)

L'algoritmo proof of Importance è quello che regola la piattaforma NEM, che è stata anche testata in Giappone coem meccanismo per gestire nuove forme di pagamento. Successivamente NEM è stata anche sperimentata da altri istituti di credito.
Tornando all'algoritmo, PoI si basa su un sistema simile a proof of Stake, nel quale l'importanza di un utente è stabilita in basa alla quantità di criptovaluta (XEM) posseduta, ma anche al numero di transazioni che effettua, e al volume stesso delle transazioni.

8.7 Linguaggi di programmazione per smart contract

Una delle caratteristiche che più destano interesse nella tecnologia blockchain è la possibilità di sviluppare e registrare all'interno della stessa blockchain dei programmi, detti smart contract. Tali programmi possono essere scritti con linguaggi di programmazione di alto livello (tipo Java), e, essendo registrati ed eseguiti dentro la blockchain, ne ereditano caratteristiche come immutabilità (quindi nessun può modificare il codice una volta che è stato caricato) e trasparenza (tutti possono vedere ciò che viene eseguito e come agisce il codice stesso).
Gli smart contract sono stati ipotizzati per la prima volta nel 1997 da Nick Szabo [80] , unendo principi legali, teorie economiche, protocolli e algoritmi per la sicurezza, con l'obiettivo di avere uno strumento sicuro e affidabile per formalizzare relazioni e scambio di informazioni attraverso una rete. Il primo modello di smart contract secondo la teorizzazione di Szabo è stato quello della vending machine, cioè di una macchina in grado di gestire una certa procedura (in questo caso la distribuzione di una bibita in seguito all'immissione di una moneta) in maniera sicura, affidabile e garantita (con buona pace di coloro che si sono visti mangiati i soldi inseriti nelle macchinette).
Successivamente con il termine smart contract si fa oggigiorno riferimento generalmente a programmi che sono in esecuzione su una blockchain e che ne modificano lo stato, andando a gestire e controllare transazioni all'interno della blockchain stessa (quindi ad esempio spostando cryptovaluta fra wallet elettronici), o modificando i valori delle variabili degli stessi smart contract. Come tutte le operazioni fatte in blockchain, anche l'esecuzione di uno smart contract, e il suo risultato, è registrato in blockchain attraverso l'applicazione di un algoritmo di consenso (tipo proof-of-work o proof-of-stake) fra i nodi della blockchain.
Successivamente alla loro ideazione nel 1996, e con l'avvento della tecnologia blockchain prima con Bitcoin e poi con lo svilupparsi di altre blockchain, il concetto di smart contract ha trovato terreno fertile su cui poter attecchire e svilupparsi. Una vera svolta è arrivata nel 2014, con l'avvento della blockchain Ethereum ad opera di Vitalik Buterin, allora solo diciannovenne. Buterin aveva definito una blockchain nella quale non solo poteva essere scambiato in maniera sicura del valore in cryptomoneta, ma potevano essere eseguiti, con le stesse garanzie di sicurezza, dei programmi. Nasceva così il primo e più importante riferimento a livello mondiale per la creazione di piattaforme che consentissero lo sviluppo e l'esecuzione di smart contract. Con Ethereum era possibile finalmente cristallizzare in un software non modificabile una di procedura, magari nata dall'accordo di più parti, e che potesse funzionare anche senza il controllo di una terza parte. Il principale punto di forza di Ethereum è il fatto che ha la maggior parte degli utenti, sviluppatori, documentazione e dApp sulla rete. D'altro canto, la principale forza di Ethereum è anche la sua debolezza. Poiché Ethereum ha il maggior numero di utenti, la sua rete è anche per lo più congestionata. Pertanto, qualsiasi interazione con le dApp costa molto più di quanto dovrebbe e molte volte c'è una lunga attesa per la conferma della transazione. Per questo motivo, i produttori di blocchi di Ethereum hanno recentemente aumentato il limite di gas di quasi il 25%, il che è paragonabile all'aumento del limite di dimensione del blocco per Bitcoin. Si è quindi alleviato la congestione della rete ma rimane il problema della scalabilità. Ethereum sta cercando di risolverlo nella nuova versione ETH 2.0, nel gennaio 2020.

Nel riassumere meglio le caratteristiche di uno smart contract si può dire (da [81]):

- "sono software "scritti" su un database condiviso (blockchain) sicuro, tracciabile ed immutabile, che verificano automaticamente, ad una certa data e/o evento, certe condizioni prestabilite a monte da una o più parti/enti/macchine;"

- “le suddette condizioni devono essere verificabili istantaneamente da un software. Spesso vi sono centinaia di condizioni in un singolo Smart Contract o esistono svariati Smart Contract tra di loro “collegati” da un nesso logico/sistemico”;

Con la nascita e la proliferazione delle varie blockchain, alcune nate da zero con progetti completamente nuovi, la maggior parte invece derivate da modifiche di blockchain esistenti, ogni iniziativa ha potuto valutare se adottare linguaggi di smart contract esistenti, o se definirne di nuovi, per poter aggiungere (o anche togliere) caratteristiche e proprietà dei linguaggi stessi. Nel dover sviluppare un’applicazione su blockchain quindi, la scelta della blockchain stessa determina il relativo linguaggio di programmazione per smart contract che può essere utilizzato nello sviluppo, non essendo certezza che questi tra loro siano interscambiabili.
Una prima lista di linguaggi di programmazione per smart contract viene quindi necessariamente fatta partendo dal tipo blockchain [82], come ad esempio nella seguente tabella:

Tabella 6. Linguaggi di programmazione

Piattaforma blockchain	Linguaggio
Ethereum, Rootstock	Solidity
EOS	C++, C
AION	Python, Groovy
NEM	?
Hyperledgefabric	Go, Javascript, Java
Libra	Move
Neo	C#, Python, Java, Javascript, Go
Cardano	Plutus (da Haskell)

Come si può vedere dalla tabella precedente, alcune blockchain condividono i linguaggi di programmazione per smart contract, molto spesso utilizzando linguaggi già esistenti (come Java e Python ad esempio, che sono usati anche in altri contesti e hanno una grande versatilità) favorendo il riuso e l’adattamento delle applicazione fra più piattaforme, mentre altre blockchain hanno soluzioni specifiche pensate esplicitamente per una determinata piattaforma, e quindi non riusabili (come ad esempio Solidity).
Per un programmatore, poter usare un linguaggio ampiamente noto, conosciuto e più ampiamente documentato (per non parlare delle risorse in temine di codice, librerie o esempi disponibili), con cui si è magari già sviluppato in passato, senza dover studiare le caratteristiche e le peculiarità di un nuovo linguaggio, rappresenta sicuramente un vantaggio. Lo sviluppatore potrà scegliere il linguaggio a lui più noto ed accelerare il processo di sviluppo di una applicazione, senza “perdere” tempo a imparare trucchi e insidie di un nuovo formalismo. Poter usare quindi linguaggio come Java o C++, ad esempio, o anche più moderni come Go, tende ad attirare su una piattaforma un numero più ampio di programmatori che vogliano lanciarsi un questo tipo di attività. Questa semplicità e immediatezza chiaramente va a vantaggio delle relative blockchain, che potrebbero vedere aumentata la loro adozione a scapito di altre piattaforme.
Ma allora, perché creare nuovi linguaggi di programmazione, come Solidity o Move? Quale vantaggio?
Proprio perché immutabili, e destinati a gestire transazioni delicate in maniera automatica, relative il più delle volte allo scambio e allo spostamento di valore sulla rete, gli smart contract, hanno un ruolo e criticità ben diverse rispetto al solito codice. Chiaramente anche nello sviluppo del codice classico si pone il problema di programmi ben strutturati, solidi e affidabili, ma in questo caso il tema

viene ulteriormente esasperato. I nuovi linguaggi di programmazione nascono quindi (anche con specifici costrutti) proprio allo scopo di supportare e rendere ancora più robusto e affidabile il codice degli smart contract, che deve esser anche compatto, cercando di minimizzare il più possibile errori di sviluppo ed evitare quindi problemi più gravi, o falle che possono, accidentalmente o in maniera malevola, portare a veri e propri disastri. L'uso di linguaggi non specializzati in altre parole potrebbe portare a codice non sicuro o con un comportamento non del tutto controllato, con gravi ripercussioni sulla gestione delle transazioni.
Un esempio famoso e storico in questo senso, che può dare l'idea della dimensione dei problemi e del rischio che si possono avere in questi contesti, è dato dal caso relativo all'organizzazione DAO.
DAO era una "decentralized autonomous organization", cioè una organizzazione autonoma decentralizzata, senza personale e governata da software.
L'obiettivo di DAO era di fornire un nuovo modello di business decentralizzato che fosse a supporto di imprese sia commerciali che non profit, quindi con lo scopo di investire i soldi raccolti in altre società.
Fu lanciata nell'aprile 2015 dopo una campagna di crowfounding e vendita di token, diventando la più grande campagna di crowfounding della storia e accumulando circa 150 milioni di dollari. Tali soldi erano il fondo stesso dell'organizzazione e gestiti dall'applicazione e dallo smart contract relativo, istanziato sulla blockchain Ethereum. Altra particolarità, DAO non era legata a nessun stato in particolare, e risultava apolide.
Nel maggio 2016, si iniziarono a notare e sollevare alcune obiezioni in merito ad alcune vulnerabilità del codice stesso che sottostava al funzionamento di DAO. Nel giugno 2016, sfruttando tali vulnerabilità, il fondo è stato sottoposto ad un attacco, riuscendo a trasferire un terzo del fondo stesso su un altro conto, agendo peraltro in maniera del tutto lecita, dato che si appoggiavano alle specifiche dello smart contract. La discussione che ne è sorta successivamente ha portato a "forzare" la mano, venendo meno al principio della intoccabilità della blockchain, recuperando i fondi e trasferendoli in un altro conto, attraverso un fork sulla rete Ethereum, facendo nascere così Ethereum Classic, ora esistente.
Questo episodio ha dimostrato che non è sufficiente dotare una blockchain di un linguaggio Turing-completo come Solidity per realizzare la gestione di smart contract [83]. Al contrario, è importante studiare se questi linguaggi sono adatti e abbastanza espressivi [84] per la formalizzazione di smart contract. Significa che un linguaggio deve comprende concetti e proprietà per consentire la formulazione di contratti del mondo reale secondo diverse prospettive e in modo leggibile da una macchina e che deve avere una chiarezza formale tale da garantire una esecuzione uniforme anche da parte di diversi elaboratori. Quest'ultimo aspetto è anche importante per consentire verifiche supportate da strumenti per prevenire un ripetuto caso DAO.
Per cercare di mediare tra le due visioni (linguaggi classici – Java, C++ vs linguaggi specifici - Solididy), alcune piattaforme come HLF traducono smart contract scritti in un linguaggio generale in linguaggio specifico per la piattaforma, cercando di ridurre i rischi.

SOLIDITY

Come detto precedentemente, nel 2014, con la nascita di Ethereum, si ebbe una svolta nello sviluppo e nelle possibilità offerte degli smart contract. Ethereum introduceva infatti il linguaggio Solidity, nato apposta per il loro sviluppo. Solidity rappresenta quindi al momento sicuramente uno dei linguaggi di riferimento per lo sviluppo di dApp, cioè di "decentralized applications", quelle applicazioni che vengono eseguite in maniera decentralizzata sui nodi di una rete blokchain.
La creazione di Solidity è stata fortemente influenzata da linguaggi esistenti, come Java, e C++, ma il linguaggio è stato da subito pensato per interagire con le reti blockchain. Rimane un linguaggio ad

alto livello, quindi un livello di astrazione importante rispetto alle logiche di funzionamento di base di un computer. Essendo stato il primo linguaggio per lo sviluppo di smart contract, ha avuto una grande diffusione. Secondo alcune stime dell'osservatorio del POLIMI su blockchain nel 2019 circa il 50% delle Proof of Concept e dei progetti su blockchain "permissionless" e il 9% dei progetti su blockchain permissioned si basano su Ethereum. Inoltre Ethereum secondo le ultime stime sta aumentando la sua rilevanza nel panorama mondiale.
Solidity è un linguaggio di programmazione Turing Complete orientato agli oggetti di tipo statico, proposto nell'agosto 2014 da Gavin Wood e sviluppato dal team per Solidity del progetto Ethereum, guidato da Christian Reitwiessner, Alex Beregszaszi, Yoichi Hirai. Il codice Solidity viene compilato e trasformato in bytecode che viene poi eseguito dalla Ethereum Virtual Machine. Supporta ereditarietà, librerie ed è tipizzato staticamente. Essendo forse la principale piattaforma per smart contract, molte blockchain alternative mantengono la compatibilità con il linguaggio Solidity per poter eseguire sulle loro reti smart contract scritti in Solidity. In questo modo gli smart contract implementati sulla rete Ethereum possono essere facilmente trasferiti su reti blockchain compatibili. Ad esempio, la piattaforma Rootstock, benchè abbia caratteristiche e peculiarità differenti da Ethereum (esecuzione su altra Virtual Machine, e maggiori garanzie di sicurezza rispetto a Ethereum).
Con il diffondersi della tecnologia blockchain e dello sviluppo di dAPP, è sorta la necessità di avere, visti anche i requisiti molto forti di robustezza degli stessi programmi, dei modelli di riferimento per lo sviluppo stesso degli smart contract. Esistono quindi degli standard (es ERC20 o ERC721) che indicano come implementare via smart contract dei token compatibili con i portafogli elettronici e le blockchain.

JAVASCRIPT
JavaScript è un linguaggio di programmazione orientato agli oggetti dinamico e leggero. Creato da Brendan Eich costituisce, insieme a HTML e CSS, i tre pilastri della progettazione Web, e ha reso più fruibile, intuitiva e dinamica la navigazione del web. JavaScript viene utilizzato per sviluppare smart contract sulla blockchain NEO.

JAVA
Java è un linguaggio di programmazione orientato agli oggetti creato da Sun Microsystems nel 1995; molto diffuso per creare applicazioni, può essere usato anche per sviluppare per smart contract su alcune piattaforme, come ad esempio NEO. Gran parte della sua sintassi e struttura è stata derivata dal C ++.
Java è stato progettato per offrire una grande flessibilità agli sviluppatori: consente infatti di scrivere codice che, essendo eseguito tramite un Virtual Machine, può essere eseguito su qualsiasi macchina, indipendentemente dalla piattaforma o dall'architettura di esecuzione.

GO (GOLANG)
Go, o Golang, è un linguaggio di programmazione open source sviluppato da Google. Supporta la programmazione concorrente, il che significa che consente l'esecuzione simultanea di più processi. Si basa in parte sulla sintassi del linguaggio di programmazione C ed è un linguaggio semplice per gli sviluppatori

C++
C ++ è un linguaggio di programmazione generico che comprende almeno oltre 4,4 milioni di sviluppatori. Il suo punto di forza è nello sviluppo e nel far scalare le applicazioni resource-intensive

(che richiedono cioè un uso intensivo e pesante di risorse), e per farle funzionare meglio e in maniera più efficiente. Gli smart contract sviluppati in C++ (ma anche C) posso essere compilati in WebAssembly. Poiché la blockchain di EOS supporta i contratti intelligenti tramite la sua macchina virtuale WebAssembly, qualsiasi linguaggio in grado di compilare in WebAssembly (WASM) potrà essere usato per programmare smart contract. C++ è comunque il linguaggio da utilizzare consigliato per gli sviluppatori sulla piattaforma EOS. In questo caso i vantaggi del linguaggio si legano ai vantaggi della piattaforma (ad esempio EOS garantisce migliori performance nel verificare le transazioni, non ha costi di transazione, e le applicazioni hanno temi di risposta molto rapidi, a discapito di un minore numero di applicazioni presenti).

MOVE
Secondo la documentazione ufficiale, il linguaggio Move è un nuovo linguaggio di programmazione per l'implementazione di logiche di transazione personalizzate e "smart contract " sulla Blockchain Libra. Con l'esigenza di servire miliardi di persone un giorno, il linguaggio è progettato per garantire alti standard di sicurezza. Come linguaggio, MOVE consente la gestione di cryptocurrency, token a digital asset, e la gestione delle transazioni su blockchain. La caratteristica chiave di Move è la capacità di definire tipi di risorse personalizzati con semantica ispirata alla logica lineare: una risorsa non può mai essere copiata o scartata implicitamente, ma solo spostata in diverse posizioni di un programma.

PLUTUS
Plutus è essenzialmente una versione di Haskell (un linguaggio di programmazione compilato particolarmente difficile da imparare) per lo sviluppo specifico di smart contract sulla blockchain Cardano [85]. Il problema principale con l'apprendimento di Haskell è che si tratta di un linguaggio funzionale piuttosto che di un linguaggio orientato agli oggetti come Javascript, C ++ e la maggior parte dei linguaggi di codifica moderni.
La forza di Cardano risiede nella sua rete e nella sicurezza degli smart contract, che deriva dal modo stessa in cui la sua rete è stata progettata. Lo svantaggio principale nell'adozione di Cardano è la mancanza di dApp utilizzabili sulla rete.

In generale, quello che si può vedere è che il mondo degli smart contract ha avuto una notevole evoluzione e sviluppo nel tempo, con la nascita di numerose proposte, con piattaforme e linguaggi che hanno seguito quella al momento più diffusa e che è stata la prima, la piattaforma Ethereum col suo linguaggio Solidity.
In alcuni casi le piattaforme adottano uno specifico linguaggio, altre invece consentono una scelta fra più linguaggi di sviluppo per implementare una dApp. In generare però, nella scelta della tecnologia, bisogna tenere conto che le caratteristiche risultanti di una applicazione sono strettamente legate e vincolate da una combinazione di linguaggio e piattaforma sui cui verrà fatto sviluppo e deployment.

8.8 Oracle Problem

Al momento della sua prima apparizione, la tecnologia blockchain appariva come un mondo "chiuso" e auto contenuto, il cui funzionamento era in qualche modo gestito solo attraverso logiche interne e in cui tutte le cose "capitavano" entro i suoi limiti.
La generazione di criptovaluta, lo spostamento di valore, le transazioni, le esecuzioni degli smart contract, tutto avveniva senza alcuno intervento dal mondo esterno e senza contatti con esso. Con il diffondersi della tecnologia, l'aumentare dei suoi campi di applicazione, le implicazioni connesse

a questo nuovo paradigma e le sue incredibili potenzialità, tanto da far dire a molti di essere di fronte ad una rivoluzione tecnologica dopo l'avvento di Internet, hanno però fatto nascere anche nuove esigenze e nuove prospettive, che richiedevano la necessità di forzare questo isolamento e di rompere con un mondo chiuso e autoreferenziale.
Per poter veramente far esplodere le potenzialità della nuova tecnologia, e poter applicare il nuovo approccio decentralizzato al più ampio insieme di settori produttivi, si rendeva necessario mettere in collegamento il sistema basato sulla blockchain con il mondo esterno, consentire cioè uno scambio di informazioni fra due entità prima disgiunte. Gli gli smart contract non sono infatti in grado di interagire con risorse esterne quali i sistemi bancari, le API e i feed di dati.
Nasceva quindi quello che viene comunemente dello il problema degli Oracoli – Oracle Problem: come portare dentro la blockchain informazioni provenienti dall'esterno? Con Oracoli ci si riferisce dunque ad un soggetto il cui scopo è registrare, all'interno di una blockchain, delle informazioni provenienti dal mondo reale e che sia chiaramente di interesse e necessario per il corretto funzionamento degli smart contract. Il termine stesso Oracolo indica la provenienza esterna di queste informazioni, poiché mentre tutto cioè che "accade" dentro la blockchain è registrato, verificato e garantito, questo non vale per le informazioni che arrivano dall'esterno, in forma appunto di "Oracolo" (L'oracolo - dal latino oraculum - è un essere o un ente – spesso soprannaturale - considerato fonte di saggi consigli o di profezie, un'autorità infallibile, solitamente di natura spirituale).
Un esempio per spiegare il concetto, è quello di immaginare una applicazione implementata attraverso degli smart contract su blockchain e che deve accedere ad un valore esterno, come la temperatura, per poter eseguire le sue elaborazioni. Come potere accedere a questo valore? Per fare questo è necessario una terza parte affidabile (trusted third party) che verifichi l'informazione e possa importarla nel sistema. Tale terza parte, oltre ad essere affidabile, deve essere identificata crittograficamente con un indirizzo, ma ci si espone anche a diversi problemi: chi garantisce che la terza parte non sbagli, o non venga sostituita da un soggetto malevolo? Il problema degli oracoli ripresenta quindi, in maniera diversa, il problema di avere una terza parte garantita che attesti certe informazioni. Crittografia e algoritmo di consenso sono strumenti che evitano il coinvolgimento di una terza parte per le transazioni interne alla blockchain, ma se servono informazioni dall'esterno il problema si ripresenta.

Nel tempo sono sorte diverse soluzioni, e diversi attori nel mercato per affrontare e risolvere il problema. Nel seguito una serie di esperienze o casi che delineano in parte lo scenario e le idee che ruotano intorno al contetto di Oracolo nelle blockchain.

PROVABLE (ex ORACLIZE)
Oraclize era una start-up di Arezzo, con l'intento di fornire servizi di attestazione e certificazione di dati. La società si è specializzata nel tempo sui sistemi decentralizzati, sulle piattaforme per smart contract e la gestione di transazioni, fornendo una infrastruttura per lo sviluppo di applicazioni in questo campo. Lo scopo della piattaforma è quella di fornire quello che può essere definito un "**attestation-as-a-service**", un sistema che fornisca garanzie , sfruttando anche i sistemi di crittografia, sull'autenticità dei dati. In altre parole, di consentire ad applicazioni basate su smart contract di accedere a informazioni direttamente da altri siti web.
Successivamente, Oraclize ha cambiato nome e proprietà, ed è diventata Provable Things [86], al momento con sede a Londra, ed è stata acquisita dal Poseidon Group. Mantenendo il focus sul tema degli oracoli blockchain, e agendo come fonte di informazioni per terze parti e quindi mettere il mondo blockchain in comunicazione con il mondo reale.

Nel sito web di Provable Things si possono vedere i punti principali della loro proposta:

- **SICUREZZA**: vhiaramente, un elevato grado di sicurezza e uso di ambienti di esecuzione affidabili, per garantire che tutti i dati che vengono elaborati non hanno subito manomissione
- **GENERALITA'**: un servizio agnostico rispetto alla blockchain che lo richiede, in maniera tale da poter essere usato da varie piattaforme
- **SEMPLICITA'**: fornitura di interfacce semplici per consentire un comodo e facile accesso al servizio.
- **OPEN**-SOURCE: la maggior parte del software prodotto è open-source e tutti i pezzi ad alta criticità sono pubblicati in questo modo. Sono disponibili su GitHub.
- **CERTIFICAZIONE**: audit e controlli esterni vengono fatti per verificare che il codice faccia quello che viene proclamato.
- **FLESSIBILITA' e EFFICIENZA:** per poter soddisfare esigenze diverse proveniente dal mondo reale.

CHAINLINK

Chainlink è una piattaforma open source per la gestione degli oracoli (progetto avviato nel settembre 2017) sviluppata dalla società SmartContract, fondata nel 2014.

La considerazione di partenza è che la connessione di smart contract a input di dati attraverso un singolo nodo crea lo stesso problema che gli stessi smart contract cercano di evitare, un singolo punto di errore, un una unica terza parte a cui affidarsi. Con un singolo oracolo, il tuo contratto intelligente è affidabile solo come quell'oracolo.

L'idea di Chain link è quella di promuovere una rete di oracoli completamente decentralizzata e sicura basata sulla tecnologia blockchain e per collegare gli smart contract con le risorse off-chain. Questa rete consente a diversi attori di fornire feed di dati o API direttamente a smart contract in cambio di token di collegamento (LINK). Queste persone sono chiamate Operatori di nodo.

La rete ChainLink è costituita da due componenti:

- una si occupa di filtrare gli oracoli attraverso accordi sul livello dei servizi offerti, a seconda delle metriche necessarie per uno smart contract.
- l'altra è costituita dagli Operatori di Nodo, collegati alla rete Ethereum, che recuperano le risposte alle richieste in tempo reale. Chainlink si propone di agire come un intermediario fornendo dati corretti, se necessario, assicurandosi che ciò che viene ricevuto dagli oracoli è preciso e indipendente.

Qualsiasi fornitore di dati può entrare a far parte della rete collegando un'API e diventando un Node Operator, responsabile di mantenere la propria API connessa alla rete, in cambio di token LINK per ogni richiesta che soddisfano. Finora la rete di oracoli è compatibile con Hyperledger, Bitcoin ed Ethereum.

IoT

Il problema degli oracoli è fortemente e naturalmente collegato a quel mondo di dispositivi e dei sensori che sta sempre più invadendo la nostra vita quotidiana. L'Internet Of Things può essere visto, infatti, come parte di quel mondo esterno alla blockchain che fornisce dati e consente agli smart contract di poter essere usati in applicazioni che fanno elaborazioni e vanno a gestire situazioni della vita reale. Progetti che vanno ad integrare tecnologia blockchain e IoT sono ormai ampiamente diffusi, ed è probabile che possano diffondersi sempre più, visto anche l'evidente crescita del mercato e delle applicazioni IoT. La tecnologia blockchain potrebbe diventare l'infrastruttura di riferimento per gestire l'operatività di questa rete di sensori, e la più adatta gestire tutte le problematiche di sicurezza, affidabilità e interoperabilità legate a questo inevitabile sviluppo di architetture IoT.

Ciò a cui si tende, e lo sviluppo di applicazioni che reagiscono in maniera automatica e dati forniti da sensori (come ad esempio sensori che rilevano la temperatura, o che indicano il consumo di una

risorsa, come un contatore elettrico). Questa simbiosi fra mondo IoT e blockchain potrebbe portare nuove soluzioni e servizi (aumentando sicurezza e affidabilità), ma contemporaneamente porta anche diversi problemi da risolvere, primo fra tutti quello della scalabilità.

Augur

Altro tema legato agli oracoli è quello delle previsioni. Può essere utile ad una applicazione chiedere delle delle informazioni su un possibile evento futuro. Augur [87] nasce per sfruttare la tecnologia blockchain e la teoria dei giochi per poter meglio sfruttare quella che è definita come la "saggezza dl popolo" o intelligenza collettiva e provare a ottenere le migliori previsioni. È quindi una piattaforma decentralizzata per Prediction Market, dove l'oggetto scambiato è proprio la previsione su un evento

KLEROS

Secondo la definizione che si può trovare sul suo whitepaper [88], Kleros è un'applicazione decentralizzata costruita su Ethereum che funziona come una terza parte decentralizzata per gestire e risolvere le controversie nella gestione di ogni tipo di smart contract, da quelle molto semplici a quelle molto complesse, e che possa supportare applicazioni in diversi settori: nel commercio, nella finanza, nelle assicurazioni, viaggi, ecc. Si basa sulla teoria dei giochi, col risultato di avere un sistema di risoluzione delle controversie che fornisce giudizi in modo rapido, economico, affidabile e decentralizzato.

Nato con l'obiettivo sopra descritto, la piattaforma Kleros può essere utilizzata in differenti contesti e casi d'uso. Il whitepaper ne indica 7, tra i quali quello relativo al tema degli oracoli: in questo caso (che è stato uno dei casi d'uso previsti in anticipo per Ethereum), uno smart contract fa una richiesta di informazione ad un "Oracolo". Chiunque può registrarsi e fornire all'oracolo l'informazione richiesta, lasciando anche un deposito all'oracolo stesso (che può adottare la piattaforma Kleros). Se tutti danno la stessa risposta, l'oracolo la riporta allo smart contract. Se ci sono più risposte, ne consegue una procedura di risoluzione delle controversie fra le diverse versioni della risposta. L'oracolo in seguito restituisce la risposta risultante dal processo di risoluzione delle controversie e le parti che hanno fornito risposte errate perdono i propri depositi, che vengono dati ai partecipanti che hanno risposto correttamente. Realitio [89] fornisce un servizio di oracoli basato su tali principi, offrendo la possibilità di utilizzare Kleros per gestire le eventuali controversie.

8.9 L'infrastruttura ENEA

L'infrastruttura ENEA sarà resa scalabile e energeticamente competitiva e permetterà di trasferire token per mezzo della blockchain e registrare, certificare e tracciare gli smart contract che verranno impiegati per eseguire automaticamente pagamenti e altre procedure. Nel corso della seconda annualità saranno valutate differenti piattaforme di supporto per lo scenario applicativo di interesse. Di fondamentale importanza per la costruzione delle applicazioni blockchain è considerare un database che sia decentralizzato ovvero con nessuna autorità centrale ma allo stesso tempo distribuito (replicabile su tutte le macchine computazionali che ne fanno parte, composto da blocchi immutabili e basato su crittografia e firma digitale per garantirne la riservatezza, l'immutabilità e la proprietà dei dati.

Il punto focale della linea di attività è l'infrastruttura che ospiterà la piattaforma blockchain dedicata alla produzione di questi token. L' ENEA possiede un'esperienza di alto livello nella gestione di una complessa infrastruttura distribuita di Calcolo ad Alte Prestazioni (HPC), grazie ad un insieme di attività da molti anni avviate per lo sviluppo della griglia computazionale ENEA e dell'inserimento di questa nei network nazionali ed europei. L'ENEA opera dal 1998 su questa tematica riuscendo a

pervenire a soluzioni tecnologiche originali per la condivisione in GRID di piattaforme di calcolo eterogenee e la remotizzazione di strumenti scientifici di grande complessità. Presso il Centro Ricerche Portici, nel maggio 2008, è stato inaugurato il supercalcolatore "CRESCO" (Centro di Ricerca Computazionale sui Sistemi Complessi), una delle più importanti infrastrutture di calcolo ad alte prestazioni a livello nazionale. La facility CRESCO è stata più volte rinnovata grazie a progetti a finanziamento nazionale e comunitario. Attualmente è stato messo in produzione la nuova macchina denominata CRESCO6+, frutto di una partnership fra ENEA e CINECA che ha vinto la gara per la fornitura dell'infrastruttura computazionale alla comunità internazionale per la ricerca sulla Fusione Nucleare. CRESCO 6+ ha una potenza di picco di circa 1,4 PetaFlops e si colloca al 420° posto nella graduatoria TOP500 [90], che fornisce il ranking delle infrastrutture di calcolo più performanti a livello mondiale. In Italia ENEA è l'unico Ente di ricerca presente in questa graduatoria, oltre a CINECA che mantiene la posizione di leader nazionale.
Nello specifico, per la linea di attività in essere, verrà utilizzata parte dell'infrastruttura distribuita ENEA portici sulla quale verrà installata la piattaforma blockchain dedicata ala produzione dei token.
L'infrastruttura CRESCO6+ è basata sui nuovi processor Intel SkyLake a 24 core e sulla nuova tecnologia di rete a bassa latenza OmniPath di Intel, capace di sostenere una banda di 100 Gbps. Il complesso dell'architettura computazionale ENEA comprende i seguenti elementi:

a. Infrastrutture di Calcolo ad alte prestazioni (HPC): l'ENEA gestisce un'infrastruttura per il calcolo scientifico e tecnico distribuita su 6 centri di ricerca. Portici, dove è ubicato CRESCO, è il sito principale seguito da Frascati e risorse più ridotte sono disponibili anche a Casaccia, Brindisi, Trisaia e Bologna. I cluster HPC sono basati principalmente su processori multicore convenzionali INTEL Xeon e processori accelerati dedicati basati sia su Intel Xeon/PHI che GPU/Nvidia;
b. Importanti risorse di storage: ca 2 PByte su disco, e una tape library da 2,5 PByte
c. Inoltre, l'infrastruttura ICT dell'ENEA include i seguenti servizi:
    - Generali: rete, SSO su Active Directory, E-Mail – dominio enea.it
    - Videoconferenze e Voip
    - Gestionale: servizi amministrativi (retribuzioni, time-sheets, missioni…)
    - Cloud Computing: VMware e OpenStack (500 Virtual Machines),
    - Cloud Storage: OwnCloud storage (eneabox e E3S)
    - Web site basati su architetture Plone/WordPress su piattaforme LAMP
    - Gestione Remota di laboratori ed esperimenti scientifici

Le facility computazionali vengono utilizzate per attività di Ricerca e Sviluppo in alcuni dei settori di punta dell'ENEA, quali ad esempio l'ingegneria, le tematiche energetiche, le biotecnologie, la bioinformatica, la struttura della materia, le infrastrutture critiche, la *computer science*, le applicazioni rivolte al settore dei beni culturali. Al fine di espandere le facility computazionali di ENEA per lo sviluppo di sistemi di acquisizione elaborazione di dati per applicazioni di intelligenza artificiale nel contesto smart cities e per ospitare una piattaforma blockchain, le attività di prossima implementazione comprendono:

- il potenziamento del servizio di calcolo scientifico per i ricercatori dell'Agenzia, attraverso il raddoppio del sistema di calcolo CRESCO6 (1,4 Pflops), realizzato tramite il rinnovo della commessa di EuroFusion ad ENEA-CINECA per la fornitura di un sistema di calcolo a supporto della comunità della Fusione;

- la prosecuzione dell'attività di ricerca nel campo del calcolo scientifico ad alto parallelismo, della gestione di Big Data e dell'analisi dei sistemi complessi, nell'ambito di progetti di ricerca nazionali ed europei, quali EoCoE-II (Energy Oriented Centre of Excellence) e Focus-CoE, recentemente acquisiti;
- lo sviluppo delle applicazioni connesse con l'acquisizione, il trattamento e la visualizzazione di dati scientifici e sperimentali, con particolare riguardo a quanto previsto dai nuovi progetti PON recentemente acquisiti e dai progetti inseriti nel piano del Distretto Tecnologico sui Beni Culturali del Lazio;
- la prosecuzione dell'adeguamento tecnologico, delle infrastrutture a (10-40 Gbit), dei servizi di rete, della sicurezza informatica e delle soluzioni tecnologiche per il rispetto della normativa GDPR.

Di particolare interesse per la presente linea di attività sarà il programma di realizzazione di test delle piattaforme blockchain attualmente sul mercato come ad esempio Ethereum che sono focalizzate su concetti chiavi quali:

- **Smart Contracts**
- **Exchange decentralizzati**
- **Decentralized Autonomous Organizations (DAO)**
- **Microtransazioni e maggiore velocità di mining**
- **Creazione e trasferimento di risorse virtuali: Smart Property.**

In particolare un output della linea di attività saranno gli Smart Contracts per lo scenario local community e che sono alla base della nuova idea di blockchain introdotta da Ethereum e successivi progetti:

- Entità appartenenti alla blockchain in grado di esprimere vincoli e obblighi contrattuali, senza bisogno di una terza parte;
- Capacità di utilizzare le transazioni per eseguire codice arbitrario (non solo movimenti economici);
- Definiti utilizzando linguaggi di programmazione specifici;
- Contratto: entità avente uno stato, funzioni ed un indirizzo;
- Ridefiniscono la transazione come esecuzione di una funzione, non più solo in termini economici;
- Per ottenere il consenso tutti i nodi eseguono le operazioni definite dal contratto, e confrontano il risultato.

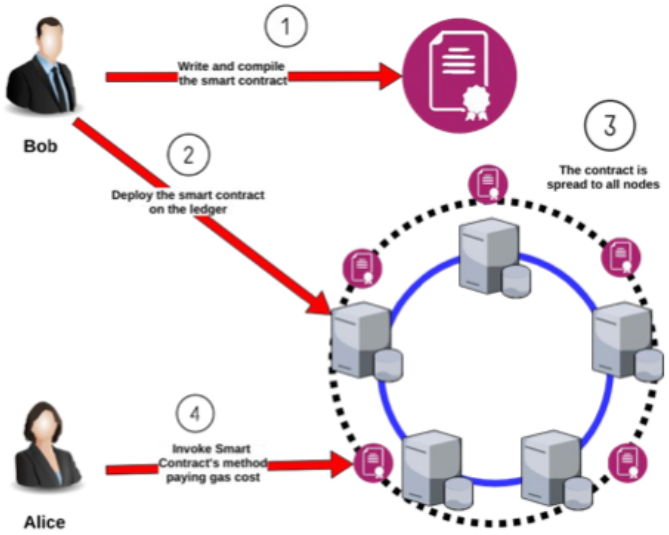

Figura 26. Ciclo di vita di uno smart contract

Considerando che gli smart contracts essendo dei software, come tali sono soggetti a bug con l'effetto collaterale che le versioni "errate" non possono essere cancellate, possono esserci problematiche notevoli legati al loro essere:

- Uno smart contract può contenere bug più o meno critici che possono essere sfruttati da altri sviluppatori tramite altri smart contracts;
- Un bug critico può portare al furto di risorse come criptovalute o altre risorse più o meno sensibili;
- Una correzione di un bug comporta il ri-deployment di uno smart contract (e di altri ad esso associati) con conseguente costo in termini di commissioni (gas nel gergo di Ethereum).

Al fine di far fronte a queste problematiche appositi studi verranno intrapresi in termini infrastrutturali per far si che il rischio delle problematiche su elencate sarà il minore possibile. Inoltre, l'infrastruttura sarà in grado di gestire ed ospitare i Dapps, ovvero Decentralized applications che vengono "eseguite" sulla blockchain:

- Con logica principale realizzata mediante smart contracts;
- Con Blockchain come backend decentralizzato e pubblicamente gestito;
- Intrinsecamente resistenti a censura e a controllo esterno;
- Che possono interagire con dati provenienti dal mondo esterno mediante sorgenti di dati dette oracoli.

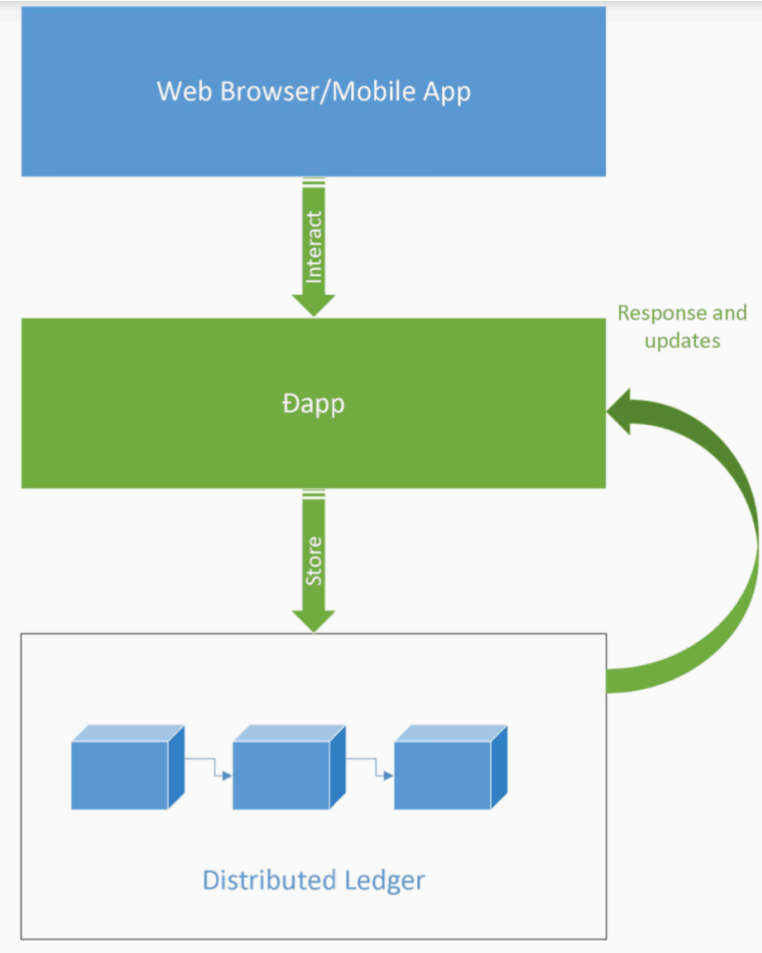

Figura 27. Schema infrastrutturale fruizione DAPP

8.10 Valutazione di alcune piattaforme BC e loro compatibilità sull'infrastruttura ENEA in ottica di scalabilità

Recenti studi [91] [92] identificano alcuni elementi che caratterizzano il comportamento di differenti blockchain rispetto alle problematiche intrinseche di uno specifico contesto di utilizzo. Infatti, essendo la tecnologia blockchain una tecnologia ad ampio campo di utilizzo, la definizione dei parametri di comparazione tra due differenti implementazioni deve essere legata all'utilizzo che si intende fare dello strumento, altrimenti è alto il rischio di scegliere una soluzione che si può rivelare inadatta ad affrontare il problema.

Analizzando la letteratura, gli elementi che posso distringure differenti soluzioni tecnologiche, almeno dal punto di vista qualitativo, nel contesto delle energy community sono:

- **Transaction time** o numero di transazioni al secondo in media;
- **Ease of integration** ovvero la facilità di utilizzo in soluzioni complesse;
- **Trasparenza**: la possibilità di accedere alle informazioni contenute nei blocchi;
- **Privacy**: il livello di sicurezza dei dati dell'utente e del suo anonimato;
- **Maturità**: il livello di maturità del codice e del suo sviluppo;
- **Criptovaluta principale:** la disponibilità di una criptovaluta intrinseca della blockchain;
- **Consumi energetici**.

Transaction time: Il tempo medio che passa dalla richiesta di registrazioe di una transazione al suo definitivo inserimento in un blocco valido della catena; a seconda delle tipologie di blockchain, questo tempo varia da pochi secondi o a minuti. Il valore medio si ottiene misurando il tempo medio

che passa tra la crezione di un blocco ed il successivo e il numero medio di transazioni registrate in n blocco. Nel caso della blockchain bitcoin, il tempo medo tra due blocchi è circa 10 minuti, quindi 300 secondi, mentre il numero di transazioni è circa 1000, quindi il transaction time è circa 3,5 trnsazioni al secondo. L'algoritmo di consenso implementato nella singola soluzione incide profondamente su questo parametro: algoritmi più "aperti" come PoW hanno un transaction time estremamente basso;

Ease of integration: la blockchain deve essere uno strumento che fornisce servizio alla piattaforma a supporto della comunità, deve essere quindi facilmente integrabile con gli altri componenti della piattaforma che verrà realizzata. Gli elementi che caratterizzano questo fattore sono:

- L'integrazione di un linguaggio "Turing-complete" all'interno della blockchain per la scrittura degli smart contract;
- La disponibilità di librerie aperte (API) di programmazione per l'accesso ai dati contenuti all'interno della blockchain.

Trasparenza: l'accesso alle informazioni contenute all'interno della blockchain può essere limitato attraverso tecniche specifiche o lasciato completamente libero a tutti, facendo leva sul fatto che tutte le informazioni personali sono criptate e, quindi, è impossibile ricondurre una determinata transazione alla persona fisica che l'ha generata o ne beneficia. Nella comunità energetica, la trasparenza permette di dare visibilità a tutti i partecipanti del comportamento degli altri e poterne verificare la correttezza.

Privacy: questo elemento è strettamente collegato al precedente ed identifica il livello di protezione dei dati, come il profilo energetico, dei partecipanti alla comunità. Molte blockchain pongono questo elemento alla base stessa dell'infrastruttura.

Maturità: anche se la maggior parte (se non tutte) le blockchain sono completamente open source, avere alle spalle un'ampia comunità di sviluppatori ed utilizzatori aiuta nel processo di implementazione del software riducendo il tempo necessario a risolvere eventuali malfunzionamenti del sistema. La maturità è strettamente legata anche al numero di tool presenti a supporto dell'uso, dello sviluppo e del test delle applicazioni e delle piattaforme basate su blockchain.

Criptovaluta principale: la criptovaluta principale regola il funzionamento della blockchain e permette di avere un elemento di riferimento per dare valore non solo a tutte le transazioni affettuate sulla blockchain, ma in generale a tutte le operazioni che vengono svolte, come ad esempio il valore del KWh consumato e dei token utilizzati nella comunità.

Consumi energetici: in una blockchain utilizzata da una comunità ampia, il fattore del costo energetico ed economico per il suo utilizzo diventa un parametro fondamentale. Anch'esso è strettamente collegato con la tipologia di algoritmo di consenso utilizzato nella blockchain: algoritmi più aperti (ad esempio Proof of Work) richiedono un maggior tempo di calcolo a garanzia del corretto comportamento dei participanti, aumentando notevolmente il costo in termini di consumo energetico; algoritmi più chiusi (ad esempio Proof of Stake) possono permettere una riduzione di questo costo.

Il presente lavoro ha identificato, in letteratura, alcune soluzioni di blockchain che possono essere valutate nei termini definiti sopra. La Tabella 7 fornisce un rapido colpo d'occhio delle differenze tra le varie blockchain. Un caso interessante è rappresentato da BitCoin ed Ethereum: da queste due soluzioni sono state derivate una moltiplicità di blockchain che migliorano determinati aspetti per essere applicati a speficici contesti. Nella tabella sono state accorpate soluzioni derivate da queste che mantengono la maggior parte delle caratteristiche identificate sopra e, che per il presente studio, non possono essere differenziate.

Infine, caso particolare è HyperLedger Fabric promosso dalla Linux Software Foundation: in questo caso non esiste una catena di blocchi comune a tutti i peer partecipanti alla rete ma c'è la condivisione di uno stato del sistema che viene replicato tra tutti i partecipanti. Ogni nuova transazione viene creata e validata da un partecipante che si occupa poi di scambiarla con tutti gli altri ottenendone in consenso in maniera immediata. In questo caso, il numero di transazioni al secondo dipende strettamente dal numero di nodi che partecipano alla rete perché ogni transazione, per essere registrata, deve ricevere il consenso dalla maggior parte dei nodi.

Tabella 7: Confronto qualitativo tra le differenti blockchain

	Transaction time (transazioni al secondo)	**Algoritmo di consenso**	**Ease of integration (Turing-Language/ API)**	**Trasparenza**	**Privacy**	**Maturità**	**Cripto / Token**	**Consumi energetici**
Bitconin	3,5	Proof of work	No/SI	Completa	SI	Alta	SI/No	Alti
Ethereum (PoW)	5,4	Proof of work	Si/Si	SI/Parziale	SI	Alta	SI/SI	Alti
Ethereum (PoS)	~1000	Proof of stake	Si/Si	SI/Parziale	SI	Alta	SI/SI	Medi
Stellar	~ 1000	Stellar Consensus protocol (SCP)	Si/Si	SI/Parziale	SI	Alta	SI/SI	Medi
Hyperledger	Variabile ~ 3500	Differenti	Si/Si	SI/Parziale	SI	Alta	No/No	Medi
Quadrans	~ 1000	Proof of Authority	Si/Si	Si/Parziale	SI	Bassa	SI/SI	Medi

8.10.1 Comparazione qualitativa tra le differenti blockchain

Transaction time: i valori riportati in tabella sono quelli ottenibili attraverso l'analisi di alcuni studi di benchmark pubblici o dei whitepaper delle singole applicazioni. Mentre per Bitcoin e Ethereum con Proof of Work sono valori assestati, gli altri rappresentano dei valori variabili che dipendono dalla configurazione della rete di nodi e che sono indicati dagli sviluppatori delle soluzioni specifiche. Hyperledger è la soluzione che risulta essere più performante da questo punto di vista, anche se l'ordine di grandezza di alcune altre soluzioni, come Stellar, Ethereum (PoS) e Quadrans è molto simile. Bitcoin e Ethereum (PoW) non sono invece comparabili.

Algoritmo di consenso: le performance delle differenti implementazioni di blockchain dipendono dall'algoritmo di consenso utilizzato per il funzionamento. Alcuni algoritmi, come lo SCP, rendono la piattaforma particolarmente performante dal punto di vista del numero di transazioni al secondo e, dall'altra parte, dal punto di vista energetico. L'algoritmo di consenso di Stellar richiede la creazione di nodi con un differente livello di affidabilità rispetto a tutta la rete. Da considerare anche che la scelta dell'algoritmo di consenso condiziona non solo le performance, ma anche la struttura stessa della blockchain, che nasceva in origine per eliminare del tutto le terze parti nella verifica delle transazioni: algoritmi più performanti possono richiedere l'introduzione di alcuni nodi speciali dedicati alla creazione dei blocchi, e quindi creado varie classi di nodi e venendo meno in una certa misura all'idea di una rete di peer completamente paritaria, ma introducendo soggetti con ruoli ben identificati.

Ease of integration: elemento fondamentale per l'implementazione della piattaforma a supporto della Energy Community è la possibilità di utilizzare la tecnologia degli smart contract per registrare le transazioni e regolare gli accessi ai dati salvati. Bitcoin e Stellar non supportano un linguaggio "Turing-Complete" che permetta la completa programmazione degli eventi, mentre tutte le altre implementazioni forniscono un linguaggio completo da questo punto di vista.
Trasparenza: a parte il caso della piattaforma Bitcoin, l'accesso ai dati inclusi nella blockchain in tutti le altre piattaforme è regolata attraverso l'uso di smart contract che controllano l'identità di chi chiede l'accesso. In questo modo si possono creare contesti differenti che convivono (ad esempio una stessa blockchain può ospitare più gruppi di utenti che non interagiscono tra di loro) al costo di ridurre la visibilità delle informazioni registrate nel ledger.
Privacy: in tutte le implementazioni analizzate, l'accesso ai propri dati può avvenire tramite soluzioni di anonimizzazione degli utenti che utilizzano coppie di chiavi crittografiche per accedere ai propri profili ed ai wallet.
Maturità: a parte Quadrans, tutte le piattaforme analizzate hanno un alto livello di maturità e di documentazione a supporto della tecnologia. Tutte le piattaforme sono più o meno attive dal punto di vista dello sviluppo del codice e della correzione di eventuali bug. Le comunità di utilizzatori e sviluppatori, a parte sempre Quadrans, sono ampie e attive.
Cryptovaluta/Token: a parte Bitcoin e HyperLedger, tutte le altre piattaforme permettono la creazione di token specifici per i contesti di utilizzo e validità degli stessi, fornendo uno strumento fondamentale per il supporto alla comunità energetica.
Consumi energetici: come visto in precedenza, un'implementazione blockchain richiede, come uno dei suoi punti di forza, un alto numero di nodi della rete che collaborano. Rispetto ad un normale database distribuito, il numero di nodi richiesto è piuttosto alto proprio per ridurre la probablità di successo di attacchi su un ampio numero di nodi. Questo porta ad una valutazione complessiva del consumo energetico a medio/alto per tutte le soluzioni analizzate.

8.10.2 Valutazione finale

Anche per una rete relativamente piccola come quella a supporto di una comunità energetica il numero di transazioni al secondo può essere un parametro critico. Avere soluzioni più performanti permette di trascurare soluzioni complesse per permettere l'immagazzinamento di un notevole numero di dati. Per questo motivo, Bitcoin e Ethereum (PoW) devono essere scartate o valutate con molta attenzione. Inoltre, Bitcoin non supporta nativamente lo sviluppo di smart contract e l'utilizzo di token, almeno per il momento, e quindi non è in grado di supportare la comunità energetica.
D'altra parte, anche se estremamente performante, Stellar non permette la creazione di smart contract complessi quali quelli che potrebbero essere necessari per la gestione di tutti gli aspetti della comunità energetica.
HyperLedger, infine, non supporta nativamente né una criptovaluta di riferimento né criptovalute secondarie (token) che sono alla base del modello economico della comunità.
Le due piattaforme chemeglio rispondono alle esigenze della comunità energetica sono Ethereum (PoS) e Quadrans, che hanno in comune moltissimi aspetti in quanto la piattaforma Quadrans è derivata direttamente dal codice di Ethereum.
Sfortunatamente, la piattaforma Quadrans ha un livello di adozione e di maturità molto più basso rispetto ad Ethereum e questo rappresenta un nodo cruciale per lo sviluppo e la diffusione della piattaforma per le comunità energetiche.
Per questi motivi, una prima scelta sulla piattaforma blockchain da utilizzare per il successivo sviluppo della piattaforma a supporto delle comunità energetiche ricade su Ethereum, con l'uso di PoS come algoritmo di consenso.

8.11 Sviluppo e test di un ambiente simulato per le transazioni energetiche nella Comunità

L'esperienza preliminare svolta in questa annualità è stata focalizzata sull'analisi degli strumenti che consentono di predisporre un ambiente simulato al fine di testare tutte le fasi del processo di sviluppo, deploy, migrazione on-chain e fruizione degli smart contracts.
L'obiettivo è stato quello di progettare e rendere attivo un sistema di registrazione dei comportamenti degli utenti basato sulla blockchain Ethereum che mette a disposizione differenti strumenti di sviluppo informatico.
Il framework di riferimento utilizzato è **Truffle Suite** [93], contenente gli strumenti necessari per la gestione del ciclo di vita degli smart contracts. Basato su NodeJS, un compilatore runtime di codice Javascript lato backend, Truffle offre una serie di tool dedicati molti utili per testare lo sviluppo, senza doversi appoggiare alla rete di test di ethereum che introduce overhead computazionale e latenza.
La suite è composta di tre elementi:

- Truffle;
- Ganache;
- Drizzle.

Truffle è uno strumento che presenta una serie di funzionalità utili per lo sviluppo:

- Sistema integrato di compilazione dello smart contract, gestione del binario generato, del deploy e ed il linking delle librerie;
- Testing automatico dei contratti attraverso gli strumenti Mocha e Chain;
- Pipeline di processo configurabile;
- Compilatore integrato di script esterni all'interno dell'ambiente Truffle.

L'installazione è stata eseguita utilizzando **npm** il package manager di NodeJS.

```
npm install -g truffle
```

Una volta installato il tool è possibile:

- Inizializzare un progetto:
  truffle init
- Compilare un progetto:
  truffle compile
- Testare il progetto:
  truffle test
- Migrare il progetto locale su blockchain:
  truffle migrate

Una volta compilato lo smart contract è possibile utilizzarlo tramite **remix:** una web application che consente di utilizzare le funzioni messe a disposizione da uno smart contract sia su una versione locale di Ethereum che remota, che sia di test o di produzione.

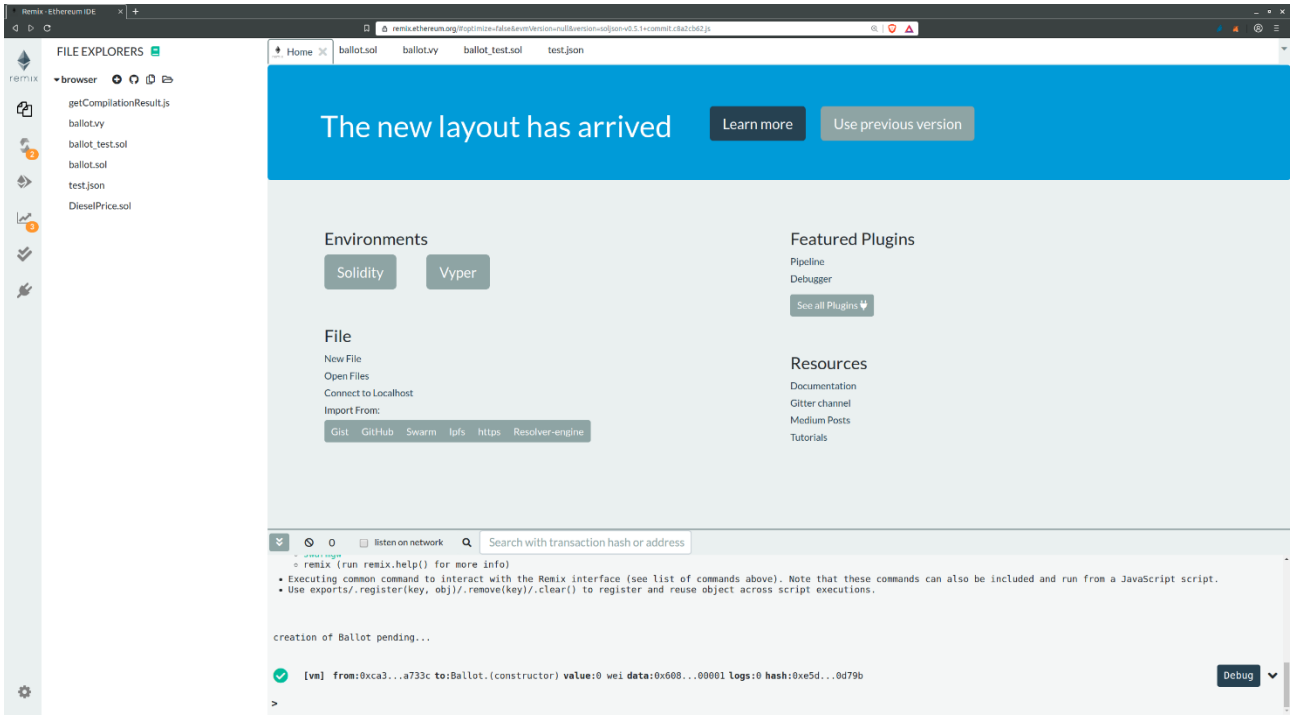

Figura 28. Remix IDE

Ganache è un software che consente di installare una blockchain Ethereum simulata in ambiente locale.

Al momento della creazione del workspace, crea 10 wallet, corrispondenti a dei nodi utente della rete. La Figura 29 mostra un esempio di istanza di Ganache.

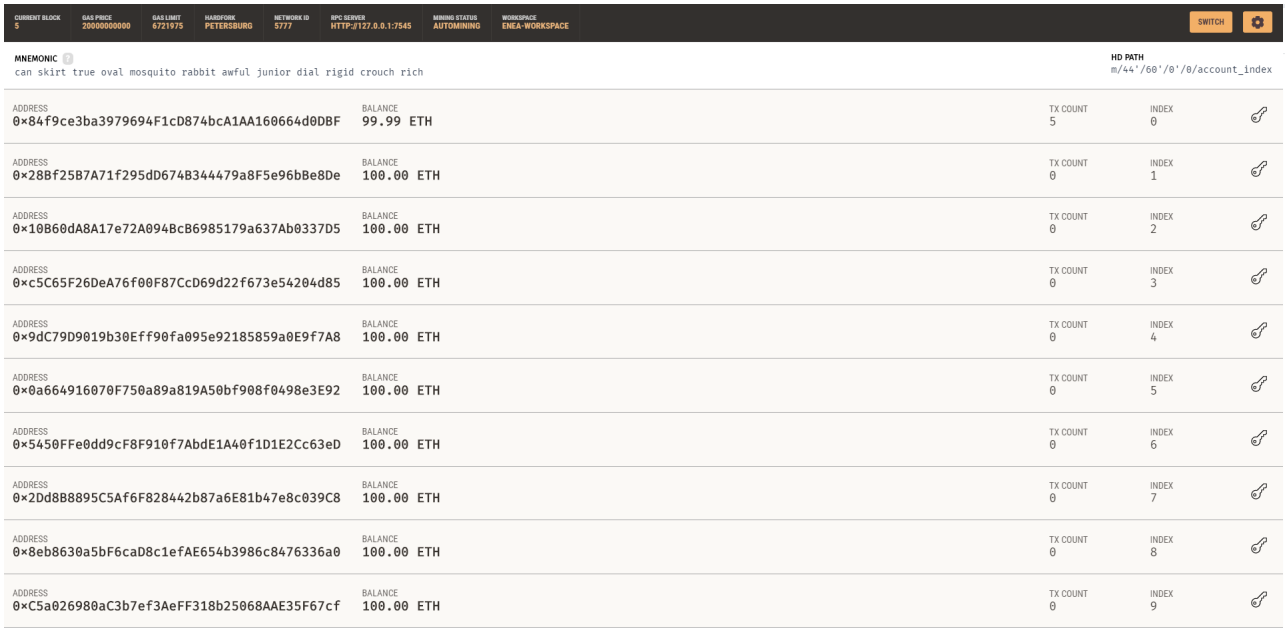

Figura 29. Interfaccia Ganache

Drizzle è un framework che consente di integrare frontend preesistenti off-chain con le informazioni contenute on-chain, sfruttando le librerie web3. Molto utile per costruire delle Dapp che

interrogano la blockchain. Contiene inoltre un pacchetto già built-in per l'integrazione con diffuse librerie frontend, quali ad esempio react.
Infine è stato analizzato il framework **go-ethereum**, contenente un pacchetto di servizi, tra cui geth, che consentono tra le altre cose di svolgere la funzione di full node al server in cui viene deployato tale servizio.

L'obiettivo quindi della prima sperimentazione è stato quindi quello di investigare i principali strumenti che consentono di sviluppare degli use case su Ethereum, quindi è stato necessario valutare le differenze tra l'uso di blockchain locali, simulate o sulla catena originale in test e produzione ed i relativi strumenti per la fruizione della blockchain al fine di valutare la soluzione tecnologica più adeguata.

La seconda sperimentazione ha avuto come obiettivo principale la realizzazione di un PoC (il cui concept era stato realizzato nel report RdS/PAR2018/022) per validare e testare un modello virtuale di aggregatore orientato al distributore.
Attraverso l'unione di Internet of Things, Blockchain, Smart Contract e Smart Meter è stato possible realizzare:

- Un modello innovativo per la gestione della flessibilità da parte del TSO/DSO;
- Un modello di incentivazione di atteggiamenti virtuosi per i *Prosumers*, attraverso dinamiche di premialità e penalità;
- La certificazione degli scambi tra i diversi soggetti che caratterizzano una Energy Communities.

L'approccio utilizzato garantisce trasparenza al processo di flessibilità, con svariati vantaggi per il soggetto aggregatore, i suoi clienti e l'operatore di rete.
Si è quindi provveduto a realizzare detto sistema all'interno del centro Enea della Casaccia nel quale è già funzionante un prototipo di rete in grado di simulare detta situazione (il cui schema è riportato sotto).

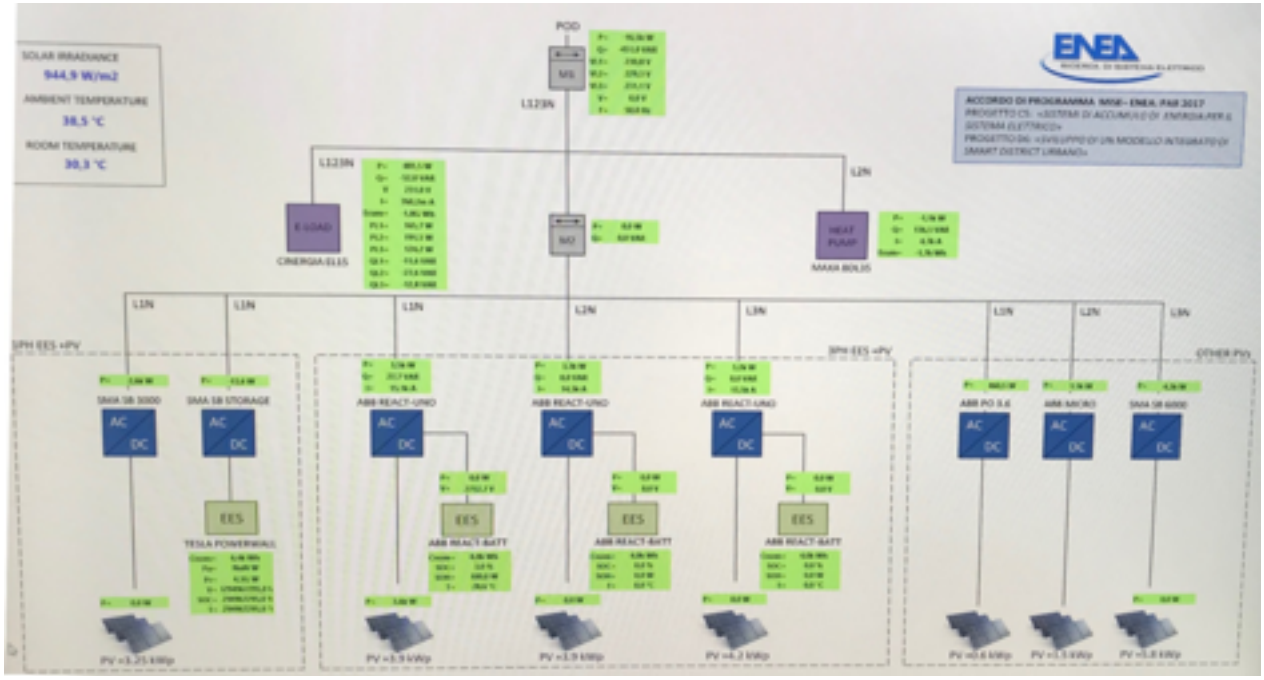

Figura 30: Schema della infrastrutura della rete

In questo scenario sono stati individuati i seguenti attori:

- Produttore non dotato di storage quindi configurato come “Produttore”;
- Produttore dotato di storage quindi configurato come “Produttore Flessibile 1”;
- Produttore dotato di storage quindi configurato come “Produttore Flessibile 2”;
- Un consumatore con capacità di load-shifting quindi configurato come “Consumatore Flessibile”;
- Un consumatore non dotato di capacità di load-shifting quindi configurato come “Consumatore”;
- Un misuratore a monte delle seguenti utenze configurato come “Gestore di rete”;

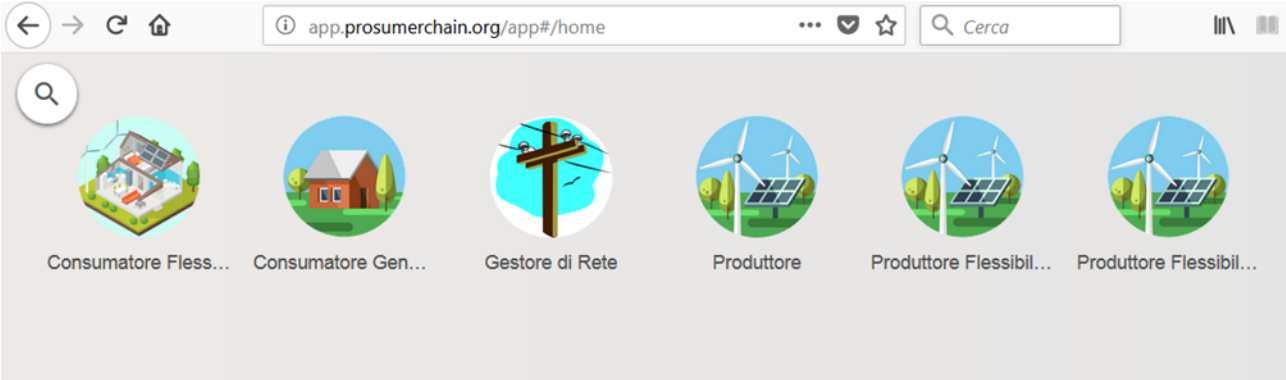

Figura 31. Esempio GUI di gestione

Sono quindi stati predisposti 6 nodi blockchain costituiti da Full Node Ethereum e implementati attraverso un client Geth (client sviluppato attraverso tecnologia GO). I seguenti nodi sono stati sincronizzati con un ulteriore nodo in Cloud in grado di eseguire l’algoritmo di consenso e con la potenza computazionale necessaria per eseguire l’algoritmo di Proof of Work (PoW): *Ethash*.
In un’architettura decentralizzata il nodo in *cloud* oltre ad eseguire il PoW e quindi permettere alla rete di chiudere i blocchi con le transazioni, espone anche un client RPC in grado di implementare le chiamate API utilizzate dalla piattaforma di monitoraggio ApioOS per visualizzare le informazioni e condividere le informazioni con piattaforme esterne come la Dashboard di visualizzazione dati della rete.
I nodi e la piattaforma blockchain sono quindi stati sviluppati in rete privata (*permissioned approach*) in questo modo è stato possibile fissare la difficolta dell’algoritmo di PoW permettendo ad un’infrastruttura leggera, dal punto di vista computazionale, di sostenere la rete e gli scambi di dati.

L’architettura del sistema per i produttori è la seguente:

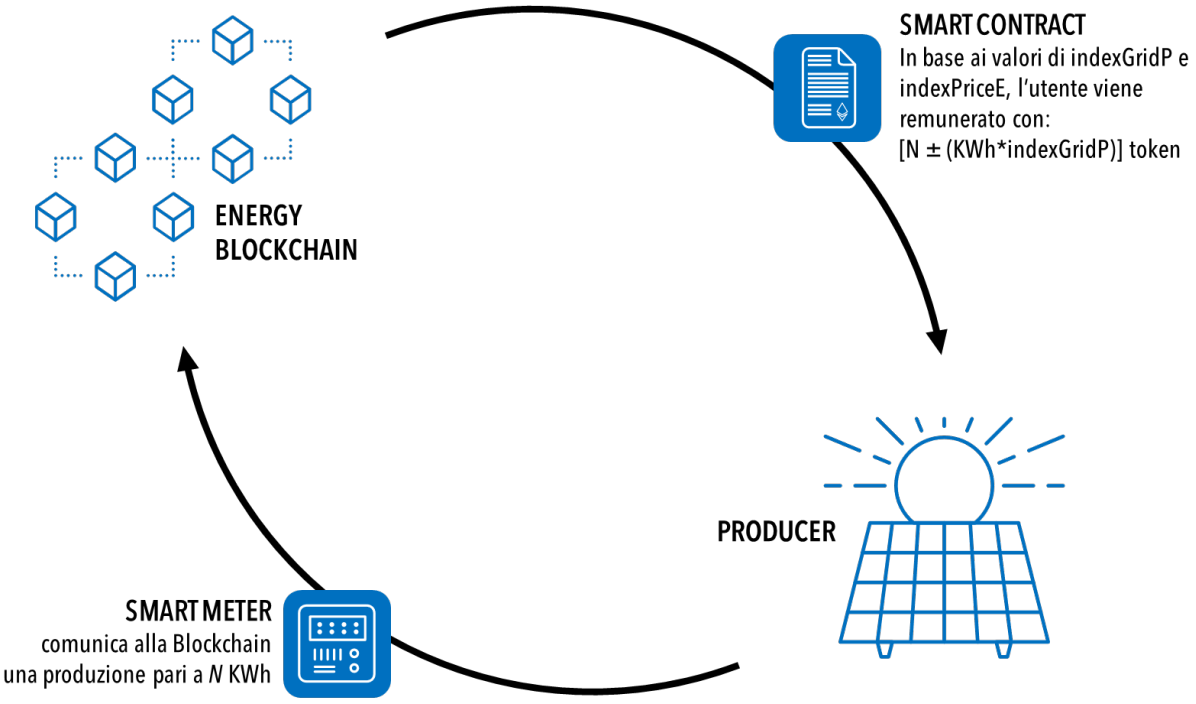

Figura 32. Architettura per i produttori

L'architettura del sistema per i consumatori è la seguente:

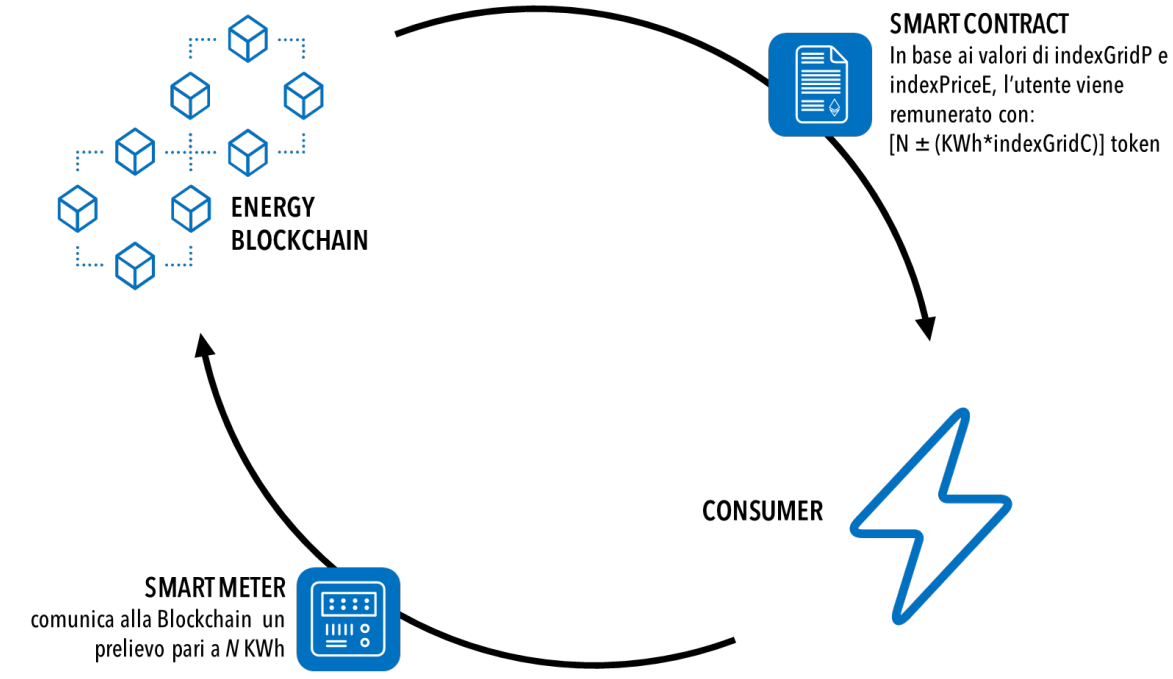

Figura 33. Architettura per i consumatori

Il meter di linea installato a monte di ogni impianto (produttori, consumatori e gestore di rete) invia i parametri di rete registrati ogni 5 secondi, attraverso uno smart contract che calcola in modo certificato gli indici di rete e invia i token ai vari attori.

L'EnergyToken rappresenta il *gettone* che permette di valorizzare economicamente premialità, penalità, energia prodotta o consumata, di seguito denominato semplicemente "token" rendendo attivo il prosumer in termini di:

a) **immissione in rete dell'energia**. Il produttore flessibile, sfruttando sia la produzione istantanea da fotovoltaico che lo storage, dovrà immettere determinati quantitativi di energia secondo un profilo giornaliero definito (con una granularità di 5 secondi) e con un cosϕ ed un livello di tensione almeno pari ad un determinato valore. Per ogni kWh di energia immessa in rete il produttore riceverà un equivalente in token, secondo fattori moltiplicativi discendenti da regole che saranno dettagliate in seguito, tanto maggiore di 1 quanto la produzione avverrà nelle ore richieste e/o se il rapporto tra attiva e reattiva sarà superiore al valore richiesto dal gestore di rete; diversamente l'equivalente in token del kWh immesso in rete sarà minore di 1. Altro fattore moltiplicativo dei kWh erogati ai fini dell'ottenimento di token sarà la contemporaneità della produzione di energia con l'utilizzo della stessa nella local community in determinate ore della giornata, dal momento che questo facilita il compito del gestore di rete che a seconda delle diverse condizioni di rete può necessitare di abbassare il carico sulla cabina MT/BT;

b) **flessibilità nell'utilizzo dell'energia nell'arco della giornata**. Il consumatore flessibile, che paga al gestore di rete un token per ogni kWh consumato, si vedrà addebitato un numero di token sul suo borsellino elettronico inferiore al numero effettivo di kWh consumati tanto più rispetterà le indicazioni del gestore sui quantitativi di energia da utilizzare in determinati periodi, tanto più il suo carico rispetterà il rapporto ottimo attiva / reattiva, tanto più utilizzerà l'energia prodotta localmente in determinati orari. Di contro si vedrà addebitati più token dei kWh consumati tanto più il suo comportamento sarà lontano da quello concordato;

c) i produttori (ed i consumatori) non flessibili (P3 e C2 rispettivamente) vedranno ridotto (aumentato) quanto ricavato (pagato) dalla vendita (consumo) di energia elettrica dalle penalità applicate in token agli effettivi kWh scambiati nel caso di non rispetto dei parametri di qualità dell'energia prodotta (utilizzata);

Per quanto concerne l'architettura del sistema a servizio della certificazione degli scambi, si è ipotizzato lo schema seguente:

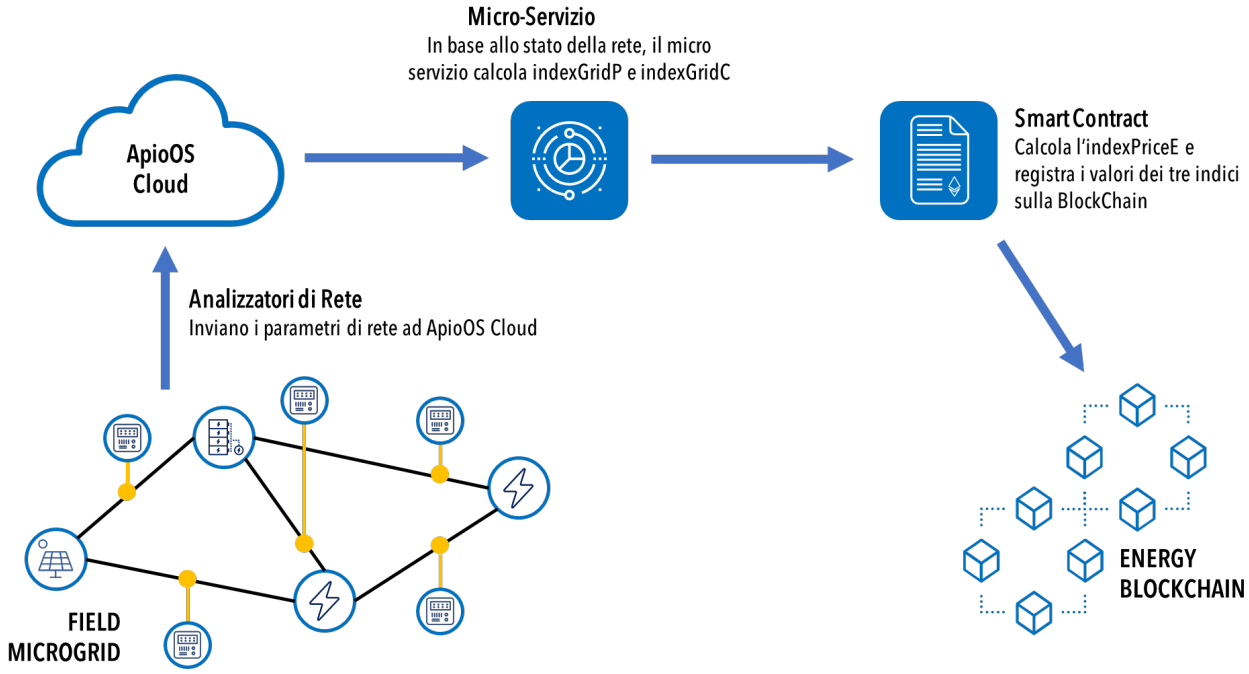

Figura 34. Architettura complessiva

All'interno dello *Smart Contract* sono state previste due funzioni per la scrittura certificata degli indici di rete su *Blockchain*:

- updateIndexGridC: È la funzione che permette di registrare il nuovo indice legato al prelievo dalla rete (consumo);
- updateIndexGridP: È la funzione che permette di registrare il nuovo indice legato all'immissione in rete (produzione);
- updateIndexGridCF: È la funzione che permette di registrare il nuovo indice legato al prelievo della rete flessibile (consumatore flessibile);
- updateIndexGridPF: È la funzione che permette di registrare il nuovo indice legato all'immissione in rete flessibile (produttore flessibile);

L'indice di prezzo può invece essere calcolato direttamente dallo Smart Contract in base allo stato della rete, all'energia disponibile e all'energia che si sta consumando. In una evoluzione futura del sistema, l'indice potrà essere guidato dalle indicazioni di prezzo provenienti dai mercati nazionali preposti.
Per la realizzazione del *PoC* il servizio di calcolo degli indici di rete può girare su un server esterno; in futuro dovrà invece essere anch'esso uno Smart Contract, garantendo una maggior sicurezza e affidabilità all'infrastruttura. Funzioni invocate dai Nodi nei momenti di prelievo o immissione in rete.

Le funzioni per la remunerazione e valorizzazione degli scambi degli utenti rispetto allo stato della rete sono principalmente due: **Produced** e **Consumed**, entrambi con due diverse declinazioni a seconda del fatto se il soggetto è di tipo flessibile o meno.

Funzione per l'immissione in rete (Produced)

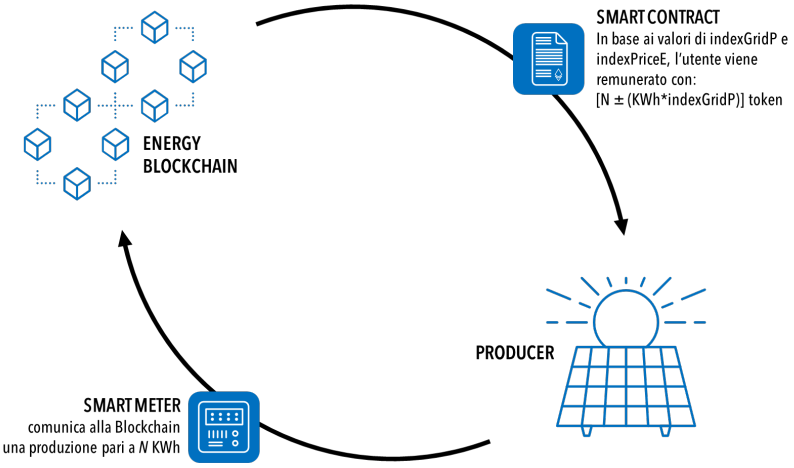

Figura 35. Ciclo del processo di immisisone

Produced: Funzione che permette di comunicare quanti KWh (o Wh) sono stati prodotti dall'utente; tale funzione viene chiamata dall'utente periodicamente (ogni x unità di tempo), a questa funzione vengono comunicati i KWh (o Wh) immessi in rete nel lasso di tempo.
La funzione calcola il numero di token in base all'indice di prezzo EnergyToken/KWh (posto per semplicità nel seguito pari ad 1) e a questo sottrae o aggiunge la premialità o penalità calcolata moltiplicando il numero di KWh (o Wh) per l'indice di qualità del prelievo o dell'immissione e, se il se il produttore è di tipo flessibile, ulteriori premialità se la produzione rispetta i criteri di contribuzione alla qualità generale degli indici di rete sottoscritti nello smart contract.
Se l'indice è negativo, allora significa che l'utente deve essere penalizzato. In questo caso, se ad esempio all'utente dovevano essere remunerati N token (in quanto aveva generato N kWh) verranno invece assegnati N – (KWh*IndexGridP) perché l'utente ha immesso energia in rete in un momento non opportuno per la Grid o con scarsa qualità o non contemporaneamente al consumo di energia da parte di soggetti appartenenti alla local community.
Se invece l'IndexGridP è positivo, allora l'utente deve essere premiato. In questo caso, se ad esempio all'utente dovevano essere remunerati N token verranno invece assegnati N + (KWh*IndexGridP).
La funzione registra inoltre su *Blockchain* il timestamp della transazione, il numero di KWh inviati al contratto, l'indice utilizzato per premiare/penalizzare, l'indice di prezzo e il numero di token assegnati o tolti all'utente.

Funzione per il prelievo dalla rete (Consumed)

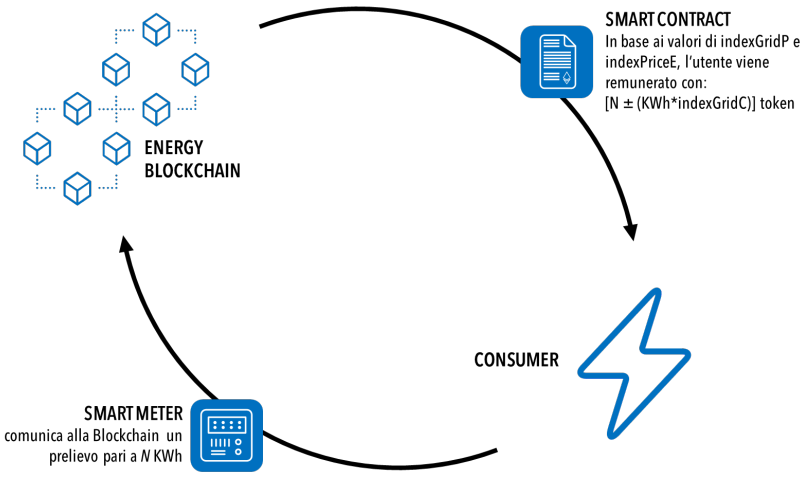

Figura 36. Ciclo del processo di prelievo

Consumed: Funzione che permette di comunicare quanti KWh sono stati consumati dall'utente; tale funzione viene chiamata dall'utente periodicamente (ogni 5 secondi), a questa funzione vengono comunicati i KWh prelevati dalla rete nel lasso di tempo.
La funzione calcola il numero di token di energia consumata e a questo sottrae o aggiunge la premialità o penalità calcolata moltiplicando il numero di KWh per l'indice della Grid associato al consumo e valido in quel momento e, se il consumatore è di tipo flessibile, assegna premialità in caso di rispetto dei criteri di consumo sottoscritto nello smart contract.
Se l'indice è negativo, allora significa che l'utente deve essere penalizzato. In questo caso, se ad esempio all'energia consumata corrispondevano N token verranno invece richiesti all'utente N + (KWh*IndexGridC) token perché l'utente ha consumato energia prelevandola dalla rete in un momento non opportuno per la Grid o non contemporaneamente alla produzione locale di energia da fonte rinnovabile.
Se invece l'IndexGridC è positivo, allora l'utente deve essere premiato. In questo, caso se ad esempio all'energia consumata corrispondevano N token verranno invece richiesti all'utente N - (KWh*IndexGridP) token.
La funzione registra inoltre su *Blockchain* il timestamp della transazione, il numero di KWh inviati al contratto, l'indice utilizzato per premiare/penalizzare, l'indice di prezzo e il numero di token assegnati o tolti all'utente.
Tutti gli indici vengono calcolati ed aggiornati nella più piccola frazione di tempo resa possibile dalla strumentazione installata (5 secondi) ed i token risultanti, differenti a seconda del tipo di soggetto in considerazione, saranno dati dalla sommatoria giornaliera dei prodotti calcolati nei micro-intervalli suddetti tra:
*(potenza istantanea) * (intervallo di tempo in ore –5 secondi-) * (indice specifico risultante)*

La chiamata alle funzioni produced o consumed potrà essere eseguita a soglie (ad esempio ogni N KWh) o, se di più semplice implementazione, ad evento (inizio e fine produzione, inizio e fine flessibilità consumatore, …).
Gli indici di produzione e di consumo per singolo intervallo di 5 secondi saranno stabiliti (al momento in maniera fissa in futuro variabile sulla base di funzioni rese da applicativi esterni) in maniera pesata degli elementi di:

- compliance con il profilo giornaliero di produzione / consumo;

- maggiore o minore rispetto del cosϕ e del livello di tensione di rete;
- indice di contemporaneità tra produzione e consumo locale;
- indice generale della rete, a cui tutti i soggetti rispondono (anche i non flessibili).

L'indice globale che ne risulterà sarà un fattore moltiplicativo (da 0,8 a 1,2) dei token che formalmente equivarranno ad 1 kWh: detti token saranno caricati / prelevati sui seguenti borsellini elettronici:

- del gestore di rete, che remunera la produzione, addebita i consumi e può partecipare al mercato della local community;
- del produttore, che li riceve dal gestore di rete e può spenderli sul mercato della local community;
- del consumatore, il quale dovrà ricaricarlo per pagare il gestore di rete anche con ricavi proveniente dalla vendita di servizi alla local community;
- del generico offerente di beni – servizi della local community.

Il concetto su cui si basa la formulazione degli indici qualitativi che generano premialità e penalità per i prosumer che sottoscrivono un contratto di flessibilità col gestore si basano sul contributo che il prosumer (o il semplice consumatore) dà alla rete in termini di:

a. Stabilizzazione temporale delle potenze fornite dalla rete;
b. Bilanciamento dei fenomeni meteorologici o endogeni a cui la rete è esposta;
c. Mantenimento di un adeguato valore del cosϕ e del livello di tensione;
d. Autoconsumo all'interno della local community (e quindi nell'ambito delle utenze sottese dalla stessa cabina MT/BT del gestore) dell'energia prodotta localmente;

In una futura evoluzione del modello lo Smart Contract sarà di tipo dinamico, ossia prenderà in input dati di congestione, metereologici, fisici di rete etc tali da richiedere in tempo reale ai prosumer di modulare il loro carico o la loro produzione. In questo POC, per semplicità di implementazione è stato definito un profilo giornaliero prefissato di richiesta di flessibilità a cui i prosumer sono chiamati a rispondere e a verificare se (e in quali quantità) questi atteggiamenti non solo saranno rispettati, ma anche di quanto andranno ad influenzare l'indice di qualità generale della rete.

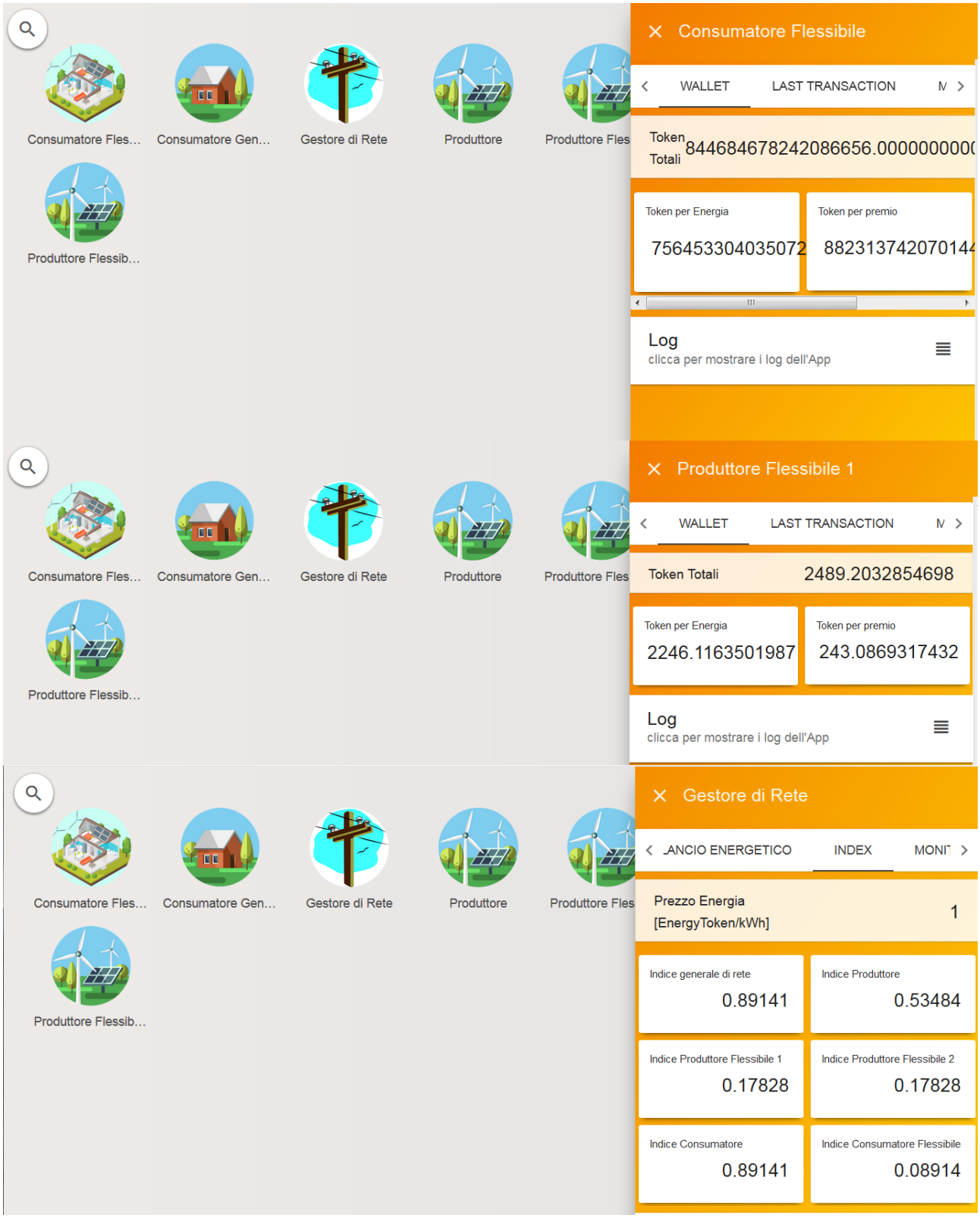

Figura 37. Esempio di GUI con wallet

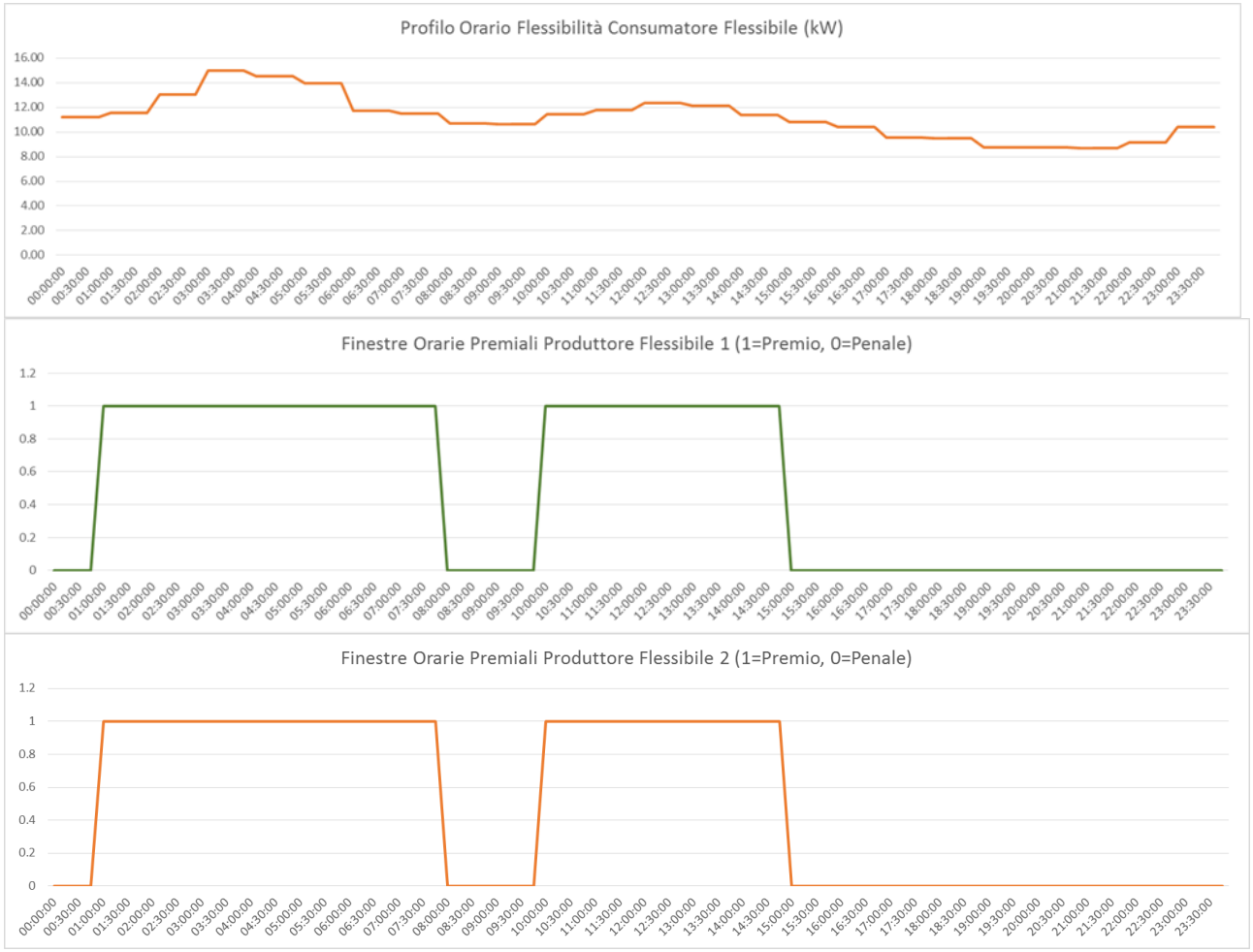

Figura 38. Esempi gestione flessibilità rispetto al consumo

Tabella 8. Riepilogo caratteristiche use case

	Versione Ethereum	Nodi	Visibilità	Accesso	Consenso	Engine Blockchain
Use case 1	Locale Simulata	1	Privata	Permissioned	PoW	Ganache
Use case 2	Ropsten	Nodi ropsten	Pubblica	Permissionless	PoW	-
Use case 3	Locale Reale	6	Privata	Permissioned	PoW	Geth

La Tabella 8 riassume i casi d'uso presi in considerazione nelle sperimentazioni effettuate. Per ognuno di essi sono state riepilogate alcune delle caratteristiche principali: sono state sperimentate la versione simulata locale con ganache, la versione di pubblica di test Ethereum, Ropsten [94] ed una versione reale di una blockchain Ethereum implementando 6 full node attraverso Geth. Lo use case 3, di cui è stato presentato il POC, risulta essere la strada potenzialmente più promettente, perché a fronte di un iniziale dispendio iniziale in termini di setup dell'ambiente, dell'installazione dei nodi e della manutenzione, consente di sganciarsi dai vincoli prestazionali ed economici relativi alla rete Ethereum ufficiale, di cui le prove fatte in ambiente di test negli use case precedenti ne hanno evidenziato i limiti.

9 CONCLUSIONI

Il rapporto di ricerca è partito da un'analisi preliminare, di ampio respiro, al fine di inquadrare il tema delle Energy Community nell'ambito della strategia energetica europea (capitolo 3) e per descrivere i principali drivers alla transizione che si stanno delineando a livello interazionale (capitolo 4). Nel capitolo 5 sono state analizzate delle soluzioni blockchain applicate al settore energetico, identificando quali iniziative possono essere prese come riferimento per una Energy Community. Nel capitolo 6 sono state analizzate le differenti tipologie di energy community al fine di identificare gli aspetti comuni e quelli spefici di ciascuna soluzione proposta. Successivamente nel capitolo 7 è stata proposta un'analisi dei modelli di criptovaluta inclusivi per comunità eterogenee. Infine, capitolo 8 viene introdotta la tecnologia delle blockchain nel suo complesso e viene identificata quella soluzione che, allo stato dell'arte, fornisce un supporto migliore all'implementazione della piattaforma a supporto delle energy community.

Il SET Plan, uno degli strumenti messi a punto a livello comunitario per promuovere la transizione verso un sistema energetico climaticamente neutro, posiziona l'Implementation Working group 3.2 focalizzato sulle "Smart Cities and Communities" nell'ambito delle cosiddette "iniziative faro" ed in particolare sui Positive Energy District. Ciò che emerge chiaramente, dal capitolo 3, è che i **PED** - quali soluzioni per aumentare la qualità della vita nelle città europee, contribuire al raggiungimento delle decarbonizzazione entro il 2050, migliorare le capacità e le conoscenze europee - insieme al paradigma delle comunità energetica, possono costituire, secondo la visione strategica comunitaria, l'idoneo volano per la transizione energetica internazionale. L'Italia baricentrando il proprio modello sulle Energy Community risulta perfettamente integrata in tale scenario.

Il Rapporto di ricerca identifica nel capitolo 4 i principali **drivers** al cambiamento del sistema energetico:

- **la tecnologia blockchain;**
- **i modelli di economia collaborativa;**
- **il paradigma delle Energy Community;**
- **i sistemi di crowdsourcing**.

In primo luogo la **tecnologia blockchain** per le sue caratteristiche intrinseche di disintermediazione, decentralizzazione, trasparenza, immutabilità, tracciabilità, programmabilità e digitalizzazione può avere molteplici applicazioni al settore energy promettendo di risolvere il noto trilemma energetico: ridurre i costi ottimizzando i processi, migliorare la sicurezza energetica in termini di sicurezza informatica, agire come una tecnologia di supporto che potrebbe migliorare la sicurezza dell'approvvigionamento ed infine promuovere la sostenibilità facilitando la generazione rinnovabile e soluzioni a basse emissioni di carbonio.

Inoltre le recenti direttive comunitarie, hanno posto l'accento sul ruolo strategico delle **Energy Community** nell'ambito del processo di transizione, introducendo il concetto di "Renewable Energy Community" e di "Citizen Energy Community". Entrambe le definizioni di REC e CEC richiamano una forma partecipativa collettiva ad un progetto di sviluppo di produzione ed uso di energia da fonti rinnovabili o da altre fonti secondo principi di efficienza utilizzando forme di autoconsumo e gestione smart delle reti di distribuzione.
Il progressivo coinvolgimento delle comunità locali nella proprietà, nel processo decisionale e nell'organizzazione degli impianti di produzione di energia rappresenta **un'innovazione sociale** che

congiuntamente alle **innovazioni tecnologiche** del settore fa intravedere la nascita di un sistema socio-energetico basato sulla generazione distribuita da fonti rinnovabili.

La transizione del sistema energetico passa anche attraverso il paradigma della **sharing economy**. Le comunità energetiche, oltre ad essere un insieme di utenze che decidono di effettuare scelte condivise per soddisfare il proprio fabbisogno energetico costituiscono un nucleo di famiglie ed imprese di cui è necessario considerare anche l'aspetto sociale. Rafforzare la dimensione sociale di una comunità energetica vuol dire accrescere il senso di appartenenza dei suoi membri mediante la reciprocità ed il legame emozionale e questo passa attraverso la condivisione di obiettivi più ampi di natura sociale, ambientale, economica oltreché energetica che possono essere perseguiti attraverso modelli di economia collaborativa o sharing economy. La sharing economy grazie alla diffusione della tecnologia blockchain, in diversi settori tra cui quello energetico, può raggiungere il suo massimo potenziale. La tecnologia essendo trustless elimina la necessità di una piattaforma gestita da un'entità centrale per la condivisione degli assets tangibili e intangibili con una riduzione dei costi delle transazioni ed un controllo da parte degli utenti dei propri dati.
Nell'ambito di una comunità energetica l'adozione di modelli di economia collaborativa basati sulla tecnologia blockchain possono riguardare sia il vettore energetico che la dimensione sociale della comunità nonché una loro possibile intersezione.
Infine i sistemi di **crowdsourcing,** grazie alla penetrazione dei social network, danno voce alle forze sociali della energy community, trasformando le informazioni raccolte spontaneamente in dati utili per la realizzazione di obiettivi collettivi. Il progetto ENEA **ECListener**, basato sul crowdsourcing, agirà da collector delle informazioni reperite sul bus della piattaforma Social della Energy Community e ne valuterà le statistiche di successo per monitorare l'intensità dell'uso della piattaforma e il gradimento della stesa.

Questa analisi preliminare termina con l'identificazione del Concept Enea di Energy Community.
L'idea di base è quella di fare riferimento al quadro normativo della Citizen Energy Community, il che vuol dire:

- focalizzarsi sul vettore elettrico;
- ammettere la partecipazione di cittadini, piccole imprese ed autorità locali al progetto;
- avere come finalità principale il raggiungimento di obiettivi sociali economici ed ambientali.

In merito a questo ultimo aspetto si evidenzia la necessità di costruire una comunità energetica con un perimetro territoriale definito funzionale alla corretta implementazione di un modello di business collaborativo.
In particolare, si vuole proporre un **modello di microgrid virtuale peer to peer**, **basata sull'impiego della tecnologia blockchain, che dovrà abilitare la reciprocità degli scambi tra prosumer e consumatori locali in ambito sociale oltreché energetico.**

Da un punto di vista sociale la piattaforma blockchain deve gestire l'emissione e la circolazione di una Community Inclusive Currency (CIC) appartenente al sistema valutario complementare, attualmente più evoluto, noto come **Local Exchange Trade System (LETS)**. La CIC avrà la funzione di premiare la messa a disposizione da parte dei partecipanti alla comunità di competenze e tempo per erogare servizi di assistenza e di natura ecologica, riscattabili sotto forma di sconti presso gli operatori commerciali aderenti all'iniziativa o trasferibili come "titoli di credito" per ottenere altre prestazioni.

Da un punto di vista energetico la piattaforma blockchain abiliterà, in una prima fase, lo scambio di energia elettrica, prodotta mediante impianti di energia da fonte rinnovabile, tra le utenze comunitarie interconnesse fornendo un servizio di intermediazione tra domanda ed offerta; in una seconda fase il demand response, consentendo ai membri della community di accettare che alcuni dei loro apparecchi siano accesi o spenti dal gestore di rete o da soggetti aggregatori per un migliore equilibrio tra domanda ed offerta di energia. In questo caso la criptovaluta comunitaria servirà a remunerare l'energia pulita autoprodotta e non consumata, messa a disposizione dal prosumer e la flessibilità energetica delle utenze.
Dalla intersezione delle due dimensioni – sociale ed energetica- scaturiscono due opportunità:

- impiegare la criptovaluta comunitaria come mezzo di scambio di servizi di natura diversa intracomunitaria;
- valorizzare al massimo l'impegno sociale e di comunità dei partecipanti attraverso il riconoscimento del tempo messo a disposizione degli altri;

con potenziali sinergie ottenibili in termini di aumento del potere di acquisto, volume degli scambi, riduzione della disoccupazione, risparmio energetico, coesione sociale, riduzione delle emissioni inquinanti.

Per sostenere con adeguate argomentazioni il modello di EC proposto, nei capitoli successivi, il Rapporto si articola in un'analisi di dettaglio riguardante: le possibili applicazioni della tecnologia blockchain al settore energy (capitolo 5); le tipologie e categorie di EC ricorrenti in letteratura (capitolo 6); le community inclusive currency (capitolo 7) quale strumento per rafforzare la dimensione sociale della community; i fondamenti della tecnologia blockchain, le piattaforme disponibili, la loro compatibilità con l'infrastruttura Enea e con il modello di EC proposto (capitolo 8).

La rassegna delle applicazioni blockchain al settore energy ha fatto emergere i potenziali benefici e le attuali barriere normative e tecnologiche nei seguenti ambiti:

- monitoring, billing e payment di energia;
- e-mobility;
- incentivazione alla produzione di energia da fonti rinnovabili;
- piattaforme di trading P2P;
- grid Managemnet e Active Demand Response.

In particolare per quanto riguarda la prima applicazione, se da un lato l'impiego della blockchain nel monitoraggio, billing e pagamento dell'energia promette una gestione decentralizzata dei dati dei contatori, eliminando la necessità di un'autorità centrale dedicata ed il rischio di un unico *point of failure*, dall'altro la disponibilità di un'adeguata infrastruttura di smart metering di nuova generazione e la necessità di sviluppare nuovi standard che ne garantiscano l'interoperabilità costituisce al momento una delle barriere principali alla diffusione su larga scala di questa applicazione.
Con riferimento alle applicazioni blockchain alla mobilità elettrica tra i vantaggi individuati vanno menzionati l'eliminazione sia della necessità di un'infrastruttura di ricarica dei veicoli elettrici gestita centralmente, che di un ampliamento della rete di ricarica disponibile, una maggiore tolleranza ai guasti delle colonnine di ricarica, l'eliminazione del problema della collusione tra i gestori delle stazioni di ricarica nella fissazione dei prezzi e la possibilità di contribuire alla stabilizzazione della rete utilizzando le batterie dei veicoli in base alle preferenze di ricarica espresse dai proprietari. Mentre la sfida principale, che in queste applicazioni, la blockchain deve ancora superare riguarda

principalmente la tutela della privacy in merito alla localizzazione e agli spostamenti dei veicoli elettrici connessi.

In merito all'incentivazione alla produzione di energia da fonti rinnovabili tra i vantaggi potenziali la trasparenza sui dati di produzione; l'abbattimento dei costi burocratici nei casi di emissione in tempo reale dei certificati di energia rinnovabile; l'eliminazione delle barriere all'ingresso dei piccoli produttori di energia verde al mercato dei certificati, la possibilità di ammortizzare più velocemente l'impianto di generazione. Ciò che ancora è inesplorato è il potenziale di manomissione degli smart meter connessi al registro distribuito, che hanno il compito fondamentale di tracciare costantemente l'energia prodotta ed automatizzare l'emissione dei certificati, sulla cui attendibilità poggia l'intera soluzione (oracle problem).

Per quanto riguarda le piattaforme di trading P2P, i vantaggi rispetto alle forniture tradizionali di energia, dove il privato compra da un operatore di grandi dimensioni, sono riconducibili alla tipologia del rapporto "alla pari" con gli altri nodi della rete, che consente di abbassare i costi delle transazioni nonché alla sicurezza della transazione e garanzia che la piattaforma su cui gira la microgrid non possa venir manomessa. L'utente finale inoltre potrà visualizzare con la massima trasparenza sia i consumi energetici, che in caso di prosumer, la quantità di energia prodotta dal proprio impianto. I limiti attuali sono principalmente normativi dato che in diversi paesi, tra cui l'Italia, i prosumers presenti sul territorio non possono vendere direttamente il surplus energetico ai consumatori finali presenti sulla rete.

Le applicazioni di Grid Managemnet e Active Demand Response mirano a sviluppare una collaborazione più diretta tra gestore dei mercati dei servizi di dispacciamento e soggetti abilitati grazie all'utilizzo della tecnologia blockchain, la quale permette di aumentare il numero di soggetti abilitati a fornire servizi legati alla flessibilità e ridurre i costi sostenuti dalla collettività per il bilanciamento della rete. L'implementazione di queste tipologie di progetti permette di gestire la sempre maggiore introduzione di capacità di generazione non programmabile, ma anche di migliorare i tempi di ritorno relativi all'adozione di sistemi di storage residenziale in quanto gli utenti otterranno vantaggi non solo dalla massimizzazione dell'autoconsumo, ma saranno remunerati per aver messo a disposizione i propri sistemi di storage per fornire servizi di rete. Essendo la rete di distribuzione di energia elettrica un'infrastruttura critica le blockchain pubbliche *permissionless* mal si adattano a questo ambito applicativo a causa di quelli sono considerati gli attuali limiti di questo particolare tipo di registro distribuito: problemi di privacy; alti costi di transazione e performance limitata.

Tra le applicazioni prese in considerazioni quelle che maggiormente si prestano nel breve termine ad essere implementate in una EC, tenendo conto delle barriere tecnologiche e normative menzionate, sono le piattaforme di trading P2P e la ricarica di EV P2P entrambe finalizzate ad abilitare lo sharing energetico tra i membri della collettività.

Nel rapporto è stata mutuata la categorizzazione di EC ricorrente in letteratura per far emergere il ruolo potenziale di ogni tipologia e categoria nel processo di transizione energetica ponendo l'accento sugli aspetti organizzativi e sociali della collettività di riferimento.
A tale riguardo è stato preso in esame anche il progetto europeo Interegg North-West Europe che prevede lo sviluppo di modelli di community-based VPP (c-VPP) in Irlanda, Belgio ed Olanda. Una c-VPP può abilitare la comunità di riferimento a generare energia ed immetterla nella rete, gestire e distribuire energia autoprodotta tra i membri della comunità, a scambiare energia sul mercato, vendere flessibilità al mercato supportando il TSO nel bilanciamento della rete, e quindi ad assumere contemporaneamente differenti ruoli, tra cui quello di facilitatore, fornitore, ESCo, aggregatore e

DSO. Questi modelli bottom-up di VPP, basati su una logica comunitaria di assunzione dei rischi e di ripartizione dei benefici richiedono la formazione delle competenze tecniche e manageriali necessarie all'interno della comunità di riferimento, ingenti capitali di investimento ed un adeguamento del quadro normativo nei paesi di riferimento, pertanto non rientrano tra le tipologie di EC destinate ad avere una diffusione su larga scala nel breve periodo.
Quello che risulta dall'analisi comparativa tra le tipologie di EC esistenti è che il passaggio al nuovo paradigma energetico richiede una pianificazione ed un coordinamento prudente, sostenuto da obiettivi sociali e governativi incrementali, che tengano in considerazione la varietà delle tecnologie disponibili, gli aspetti culturali delle comunità e che prevedano lo sviluppo di nuovi modelli di business. I fattori chiave da considerare nel valutare il potenziale delle diverse tipologie di comunità nell'accelerare il passaggio al nuovo paradigma energetico possono essere rintracciati nella capacità della comunità di realizzare un'innovazione sociale e collaborativa e di promuovere un'interazione sinergica tra attori e le istituzioni. Le EC distribuite e decentralizzate, per le caratteristiche sopra descritte, risultano essere le tipologie di comunità più adatte ad innescare il processo di trasformazione auspicato. Le EC distribuite (nelle categorie delle piattaforme di trading P2P (o microgrid virtuali) e delle VPP) rappresentano di per sé nuovi modelli di business che creano valore garantendo un migliore impiego degli asset ed il trading di servizi, distribuendo benefici economici ai membri della collettività. Le EC decentralizzate (nelle categorie delle Micogrid fisiche e ICES) nonostante siano caratterizzate da un'elevata complessità tecnica e da ingenti investimenti in capex, rispetto alle EC distribuite, sono localizzate in un'area geografica ben definita e come è noto la prossimità fisica facilità l'innovazione collaborativa (come lo sharing di servizi energetico-sociale). Differentemente dalle EC centralizzate, per la necessità di mobilizzare ingenti risorse finanziarie, le EC decentralizzate richiedono una struttura di governance in grado di coinvolgere i principali stakeholders tra cui le istituzioni, i rappresentati della comunità, i fornitori di servizi. Il coinvolgimento di gruppi di attori diversi con differenti motivazioni favorisce l'apprendimento, il networking e la propensione al cambiamento.

Lo strumento di economia collaborativa ritenuto più idoneo ad attivare la reciprocità degli scambi in abito sociale, necessaria al rafforzamento della community in tutte le sue dimensioni, anche quella energetica, è stato individuato nella valuta comunitaria (community inclusive currency).
Nella maggior parte dei casi, le valute comunitarie appartenenti alle ultime generazioni, hanno come obiettivo lo sharing di competenze, abilità, la promozione di rapporti solidali e comportamenti virtuosi da un punto di vista ambientale e sociale per la valorizzazione delle risorse disponibili ed inutilizzate assumendo sempre di più la connotazione di monete ad inclusione sociale. Nell'ambito di una comunità energetica la diffusione di una valuta complementare con obiettivi di inclusione sociale, oltreché di sharing energetico può innescare un circolo virtuoso di reciprocità in grado non solo di garantire il coinvolgimento e la partecipazione necessaria di tutti i membri al successo del progetto energetico ma anche di mobilitare beni e risorse che altrimenti resterebbero inutilizzati per soddisfare i bisogni comunitari di altra natura.
Tra i vari esempi di valute locali esistenti sono stati presi in considerazione i sistemi di credito reciproco come il **LETS** perché presentano caratteristiche ideali per una gestione su piattaforme blockchain: sono autoregolamentati, non hanno bisogno di una banca centrale per monitorare l'offerta di moneta; la maggior parte di essi sono già completamente informatizzati; promuovono attivamente la cooperazione piuttosto che la concorrenza tra i partecipanti favorendo lo sviluppo delle comunità di riferimento.
I sistemi di credito reciproco si basano sul principio della "co-produzione" e della reciprocità: il miglior modo per costruire una comunità sana è quello di considerare ogni persona come portatrice

di competenze, idee e risorse convertendo il contributo del singolo allo sviluppo e al rafforzamento della comunità in potere di acquisto.
Il desiderio è quello di correggere le logiche distorte dell'economia, passando così da un commercio impersonale a «rapporti più personali e umani», introducendo trasferimenti tra persone che possiedono conoscenze, abilità, tempo e beni non utilizzati. Si ottiene cosi il riconoscimento di quelle competenze che il mercato tradizionale non valorizza, rinforzando il senso di autenticità nelle relazioni con gli altri.
Tra gli esempi a livello internazionale, più significativi di valuta comunitaria gestita tramite una piattaforma blockchain, è stato individuato il caso di Hull Coin e InvolveMint. Entrambi i progetti sono stati sviluppati nel Regno Unito.

Nel caso di HullCoin, l'estrazione di una criptovaluta governativa funziona come mezzo per aggiungere valore all'economia locale. Hullcoin utilizza gli script di mining di Ven e Feathercoin. Il mix dei due aggiunge maggiore stabilità alla volatilità della valuta. In particolare il valore di Ven è ancorato ad un paniere di materie prime tra cui l'oro che la rende molto stabile. La tecnologia blockchain usata come stanza di compensazione decentralizzata ha permesso di incorporare nella stessa moneta le prove del risultato sociale di qualsiasi attività intrapresa nella comunità creando un registro distribuito di tutte le attività socialmente rilevanti intraprese dai membri ed offrendo alle persone un CV sociale utile anche nella ricerca di un nuovo impiego. InvolveMINT gestisce una valuta comunitaria chiamata TIME CREDIT che permette ai suoi utenti di trovare opportunità di volontariato e progetti su cui lavorare e a cui dedicare il loro tempo, guadagnando valuta criptata riscattabile con l'acquisto di beni e servizi presso i partner aderenti. InvolveMINT sta cambiando la cultura del volontariato creando un'ampia rete di organizzazioni e di imprese a sostegno di coloro che cercano di dare un impulso al rafforzamento delle comunità. Questa rete promuove un servizio regolare ed una collaborazione ponderata alla (ri)costruzione di comunità in un contesto sociale, come quello attuale, di vite sempre più stratificate ed impegnate.

La tecnologia Blockchain si è dimostrata essere dirompente ed estremamente innovativa nell'ambito economico/monetario, permettendo di immaginare e realizzare scenari di collaborazione ed interazione che non sono realizzabili con le classiche monete fiat.
Questa tecnologia armonizza un ampio insieme di soluzioni e conoscenze, come la teoria dei giochi, tecniche di crittografia avanzata, sistemi di protezione dei dati o applicazioni peer to peer, per mettere a disposizione una piattaforma affidabile che possa essere utilizzata in differenti contesti.
L'evoluzione e la diffusione delle blockchain hanno dimostrato che non esiste la soluzione unica ai problemi che possono essere affrontati con questa tecnologia: scenari differenti richiedono blockchain con differenti caratteristiche per poter essere affrontati correttamente e in modo proficuo per gli utenti. Questo fatto ha dato origine ad un ampio spettro di soluzioni già disponibili o in realizzazione che hanno caratteristiche e peculirità interessanti per una Energy Community.
Dall'altra parte, questa proliferazione di soluzioni richiede l'identificazione di alcuni parametri che permettano la differenziazione e la valutazione della singola soluzione e, infine, la comparazione con le altre soluzioni.
L'identificazione dei parametri di valutazione, attraverso un'analisi della letteratura, ha permesso di comprendere quali sono gli elementi quantitativi e qualitativi che la tecnologia blockchain deve garantire alla piattaforma per essere funzionale: in base a questi parametri è stata identificata la piattaforma Ethereum come quella più promettente per lo sviluppo di una piattaforma a supporto delle Energy Community.

L’analisi dei requisiti tecnici necessari per la messa in produzione della piattaforma ha permesso di individuare quali caratteristiche deve avere l’infrastruttura informatica a contorno della piattaforma ed ha permesso di individuare le risorse disponibili all’interno della struttura ENEA.
Una proof of concept sviluppata da ENEA in collaborazione con altri partner, dimostra come questa soluzione tecnologica possa essere integrata in un contesto di misurazione dei profili energetici e di monitoraggio dei comportamenti degli utenti della piattaforma. Anche se questa proof of concept non risolve tutti gli aspetti contingenti di una comunità energetica, perché ad esempio non tiene in considerazione gli aspetti sociali di collaborazione tra le persone, indica una strada che può essere percorsa per arrivare alla implementazione del prodotto finale del progetto.

10 Riferimenti bibliografici

[1] «Energy Union Package,» European Commission, 2015.

[2] L. Ammannati, Una nuova governance per la transizione energetica dell'unione Europea. Soluzioni ambigue in un contesto conflittuale, 2018.

[3] «UE 944/2019,» European Commission.

[4] S. Plan, «Declaration of Intent on Strategic Targets in the context of an Initiative for Smart Cities and Communities».

[5] S. Plan, «Plan n.3.2 Implementation Plan – TWG – June 2018,» 2018.

[6] [Online]. Available: 5. https://jpi-urbaneurope.eu/news/consultation-on-the-framework-definition-for-positive-energy-districts-and-neighbourhoods/.

[7] Terna SpA, «Pubblicazioni Statistiche,» 2018. [Online]. Available: https://www.terna.it/it/sistema-elettrico/statistiche/pubblicazioni-statistiche.

[8] School of Management, «L'universo dell'internet of value, tra le glassie della Blockchain,» Politecnico di Milano, 2019.

[9] Council World Energy, «Energy Trilemma Index,» 2019. [Online]. Available: https://trilemma.worldenergy.org/.

[10] L. Tricarico, «Community energy enterprises in the distributed energy geography: A review of issues and potential approaches,» *International Journal of Sustainable Energy Planning and Management,* pp. 81-93, 2018.

[11] M. Mauss, Essai sur le don' in Sociologie et anthropologie, 7° edizione, Parigi: Quadrige/PUF, 1997.

[12] R. Amorevole e P. Rizzo, in *Senza denaro*, Roma, Edizioni Lavoro, 2000.

[13] R. Botsman e R. Rogers , What's Mine Is Yours: The Rise of Collaborative Consumption, Harper Collins, 2010.

[14] Y. Benkler , «Sharing nicely: On shareable goods and the emergence of sharing as a modality of economic production,» *Yale Law Journal,* vol. 114, pp. 273-358, 2004.

[15] A. Bonomi, F. Della Puppa e R. Masiero, La società circolare. Fordismo, capitalismo molecolare, sharing economy, Roma: DeriveApprodi, 2016.

[16] I. Pais e G. Provasi, «Sharing economy: A step towards "re-embedding" the economy?,» *Stato e Mercato,* vol. 3, pp. 347-377, 2015.

[17] A. Arvidsson e A. Giordano, Society Reloaded. Pubblici produttivi e innovazione sociale, Milano: Egea, 2013.

[18] D. Arcidiacono, «Sharing economy and startup: alternative economic exchange or myth of a dis-intermediated market,» *Quaderni di Sociologia,* n. 73, pp. 29-47, 2017.

[19] D. Donnerer, «Blockchain and Energy Transition. What Challanges for cities?,» 18 April 2018. [Online]. Available: https://energy-cities.eu/blockchain-and-energy-transition-what-challenges-for-cities-find-out-in-our-newly-released-publication/. [Consultato il giorno October 2020].

[20] Energy & Strategy Group, «Energy Innovation Report,» Politecnico di Milano, Milano, 2019.

[21] E. Gui e I. MacGill, «Typology of future clean energy communities: An exploratory structure, opportunities, and challenges,» *Energy Research & Social Science,* vol. 35, pp. 94-107, January 2018.

[22] B. Carolan, Social Network Analysis and Education: Theory, Methods&Applications, SAGE Publications, 2014, p. 542–577..

[23] J. Watson e P. Devine-Wright, «Centralization, decentralization and the scales in between,» in *The Future of Electricity Demand: Customers, Citizens and Loads*, Cambridge, Cambridge University Press, 2011, pp. 542-577.

[24] P. Selman e A. Wragg, «Local sustainability planning: from interest-driven networks to vision-driven super-networks?,» *Plann. Pract. Res.,* vol. 14, n. 3, pp. 329-340, 1999.

[25] S. Tongsopit e B. Haddad, «Decentralised and centralised energy: a property rights analysis,» *Int. J. Global Energy Issues,* vol. 27, n. 3, pp. 323-338, 2007.

[26] D. Pitt e E. Bassett, «Innovation and the role of collaborative planning in local clean energy policy, Environ,» *Policy Gov.,* vol. 24, n. 1, pp. 377-390, 2014.

[27] M. Richter, «Business model innovation for sustainable energy how german municipality utilities invest in off-shore wind,» *Int. J. Technol. Manage.,* vol. 63, n. 1/2, pp. 24-50, 2013.

[28] R. Madriz-Vargas, A. Bruce e M. Watt, *A review of factors influencing the success of community renewable energy minigrids in developing countries,* Brisbane: 2015 Asia-Pacific Solar Research Conference, 2015.

[29] C. Hawkins e X. Wang, «Sustainable development governance: citizen participation and support networks in local sustainability initiatives,» *Public Works Manage. Policy,* vol. 17, n. 1, pp. 7-29, 2012.

[30] Middelgrundens Vindmollelaug, «Middelgrundens Vindmollelaug,» 2010. [Online]. Available: http://www.middelgrunden.dk/middelgrunden/?q=en/node/35.

[31] Community Power, «Denmark Inspiring Story,» [Online]. Available: https://www.communitypower.eu/en/9-join-community-power/963-denmark-inspiring-story.html.

[32] Energiepark Druiberg Gmbh, «Energiepark Druiberg,» [Online]. Available: http://www.energiepark-druiberg.de/.

[33] Freiburger, «Freiburger Sonnendacher FREESUN,» [Online]. Available: https://www.freiburg.de/pb/232537.html.

[34] NAVIGANT Research, «Microgrids or VPPs or Both?,» [Online]. Available: https://www.navigantresearch.com/news-and-views/microgrids-or-vpps-or-both.

[35] R. Mourik, S. Breukers, L. Summeren e A. Wieczorek, *Community-Based Virtual Power Plants: Against All Odds?,* Presented at the Sustainable Places 2019, 2019.

[36] Microgrid Knoledge, «Community Microgrids: Four Examples of Local Energy that Improves Lives,» [Online]. Available: https://microgridknowledge.com/community-microgrids-examples/.

[37] Clean Coalition, «Goleta Load Pocket Community Microgrid (GLPCM),» [Online]. Available: https://clean-coalition.org/community-microgrids/goleta-load-pocket/.

[38] Deloitte, «Will microgrids transform the market?,» [Online]. Available: https://www2.deloitte.com/ch/en/pages/energy-and-resources/articles/will-microgrids-transform-the-marke.html.

[39] Council of Energy Ministers, «Integrated Community. A Roadmap for Action,» Canada, 2009.

[40] B. PrasadKoirala, E. Koliou, J. Friege e R. Hakvoort, «Energetic communities for community energy: A review of key issues and trends shaping integrated community energy systems,» *Renewable and Sustainable Energy Reviews,* vol. 56, n. 1, pp. 722-744, 2016.

[41] D. Parra, M. Gillott, S. Norman e G. Walker, «Optimum community energy storage system for PV energy time-shift,» *Applied Energy,* vol. 137, n. 1, pp. 576-587, 2015.

[42] J. Webster, B. Korteling, B. Gilmour, K. Margerm e J. Beaton, *Integrated Community Energy Modelling: Developing Map-Based Models to Support Energy and Emissions Planning in Canadian Communities,* World Renewable Energy Congress - Sweden, 2011.

[43] Rinnovabili.it, «Feldheim, un'isola energetica 100% rinnovabile,» [Online]. Available: http://www.rinnovabili.it/storico/feldheim-unisola-energetica-100-rinnovabile/.

[44] L. Fantacci e M. Amato, Moneta Complemenatre. Sai cosè?, Milano: Bruno Mondatori, 2014.

[45] J. Blanc, «Classifying "CCs": Community, complementary and local currencies' types and generations,» *International Journal of Community Currency Research,* vol. 15, n. 1, pp. 4-10, 2011.

[46] Community Currencies in Action (CCIA), People powered money: Designing, developing & delivering community currencies, New Economics Foundation, 2015.

[47] G. Hallsmith e B. Lietaer, Creating Wealth: Growing Local Economies with Local Currencies, New Society Publishers, 2011.

[48] Resilience.org, «Bitcoin, Blockchain, and Local Currencies,» 2017. [Online]. Available: https://www.resilience.org/stories/2017-12-14/bitcoin-blockchain-and-local-currencies/.

[49] N. Kichiji e M. Nishibe, «A comparison in transaction efficiency between dispersive and concentrated money creation,» *International Journal of Community currency Research,* vol. 12, n. 1, pp. 49-47, 2012.

[50] L. Huber e J. Martignoni, «Improving Complementary Currency Interchange By a Regional Hub-Solution,» *International Journal of Community Currency Research,* vol. 17, n. A, pp. 1-7, 2013.

[51] S. Nakamoto, «Bitcoin: A Peer-to-Peer Electronic Cash System,» 2008.

[52] Cointelegraph, «The Saber Case: How Complementary Currencies Can Go Crypto And Change The World,» 2018. [Online]. Available: https://cointelegraph.com/news/the-saber-case-how-complementary-currencies-can-go-crypto-and-change-the-world.

[53] Gesell Research Society Japan, «The WAT-System,» [Online]. Available: https://www.watsystems.net/watsystems-translation/english.html.

[54] Shareable.net, «The English City With Its Own Cryptocurrency: Q&A With the Founders of HullCoin,» 2017. [Online]. Available: https://www.shareable.net/the-english-city-with-its-own-cryptocurrency-qa-with-the-founders-of-hullcoin/.

[55] Grounded, «Community EngageMINT: Fresh Connections with involveMINT,» 2017. [Online]. Available: https://groundedpgh.org/event/involvemint/.

[56] N. Hindman, «Bancor,» 3 Marzo 2019. [Online]. Available: https://blog.bancor.network/redesigning-community-currencies-from-one-tomato-to-1000-wallets-on-sarafu-network-80a629354ab1. [Consultato il giorno 2020].

[57] J. Mattila, T. Seppälä, C. Naucler, R. Stahl, M. Tikkanen e A. Bådenlid, «Industrial blockchain platforms: An exercise in use case development in the energy industry,» 2016.

[58] Osservatori.net. [Online]. Available: https://www.osservatori.net/it_it/osservatori/blockchain-distributed-ledger.

[59] A. Back, M. Corallo, L. Dashjr, M. Friedenbach, G. Maxwell e A. Miller, «Enabling blockchain innovations with pegged sidechains,» 2014.

[60] M. Walport, «Distributed ledger technology: beyond blockchain,» 2016.

[61] J. Mattila, «The blockchain phenomenon-the disruptive potential of distributed consensus architectures,» 2016.

[62] J. Seppälä, «The role of trust in understanding the effects of blockchain on business models,» 2016.

[63] G. Greenspan, «Ending the Bitcoin vs Blockchain debate,» 2015.

[64] we.trade, [Online]. Available: https://we-trade.com/.

[65] Foodchain. [Online]. Available: https://food-chain.it/.

[66] Tradelens, [Online]. Available: https://www.tradelens.com/.

[67] D. Johnston, «The General Theory of Decentralized Applications, Dapps.,» [Online]. Available: https://github.com/DavidJohnstonCEO/DecentralizedApplications.

[68] Cryptonomist. [Online]. Available: https://cryptonomist.ch/2018/11/27/neufund-equity-token-eto-su-blockchain/.

[69] 4New, «Clean Green Energy for Crypto Mining,» [Online]. Available: https://4new.io/.

[70] 4New, « Introducing the KWATT coin tokenized electricity,» [Online]. Available: https://4new.io/wp-content/themes/4new/images/whitepaper.pdf.

[71] SolarPlaza, «Comprehensive guide to companies involved in blockchain and energy,» 2017. [Online]. Available: https://www.solarplaza.com/channels/future-grid/11751/report-comprehensive-guide-companies-involved-blockchain-energy/.

[72] Sun Exchange, «Solar Exchange, The solar panel sharing economy.,» [Online]. Available: https://thesunexchange.com.

[73] WePower, «Wepower White paper,» 2019. [Online]. Available: https://wepower.network/media/WhitePaper-WePower_v_0.81-1.pdf.

[74] ImpactPPA, «The world's decentralized energy platform,» [Online]. Available: https://www.impactppa.com/wp-content/uploads/2018/03/ImpactPPA_WP_v1.2WEB.pdf.

[75] Prosume, «Decentralizing Power,» 2017. [Online]. Available: https://prosume.io/wp-content/uploads/PROSUME_Commercial-Deck_17012020.pdf.

[76] W. M. Hasni, M. H. Ismail e Y. Nong, *FARAD : Commoditising Forward Purchase Contract in Ultra-capacitor Intellectual Property Rights on Ethereum Blockchain,* 2017.

[77] MyBit, «MyBit White paper,» [Online]. Available: https://whitepaper.mybit.io/.

[78] Local-e, «Local-e FAQ,» [Online]. Available: https://www.local-e.us/faq/.

[79] L. Lamport, R. Shostak e M. Pease, «The Byzantine Generals Problem,» *ACM Transactions on Programming Languages and Systems,* vol. 4, n. 3, 1982.

[80] N. Szabo, «Formalizing and Securing Relationships on Public Networks,» *First Monday,* vol. 2, n. 9, Settembre 1997.

[81] EthereumItalia. [Online]. Available: https://www.ethereum-italia.it/community/322/.

[82] Criptorivista. [Online]. Available: https://www.cryptorivista.com/ch-it/articles/894ec6b6.

[83] Steemit. [Online]. Available: https://steemit.com/smart/@alexbafana/smart-contract-languages-comparison.

[84] A. Norta, L. Ma, D. Y, A. Rull, M. Kolvart e K. Taveter, «Econtractual choreography-language properties towards cross-organizational business collaboration.,» *Journal of Internet Services and Applications,* pp. 1-23, 2015.

[85] Cardano. [Online]. Available: https://www.cardano.org/en/home/.

[86] ProvableThings. [Online]. Available: https://provable.xyz/index.html.

[87] Augur. [Online]. Available: https://www.augur.net/.

[88] Kleros. [Online]. Available: https://kleros.io/whitepaper_en.pdf.

[89] Realitio. [Online]. Available: https://realit.io/.

[90] Top500. [Online]. Available: https://www.top500.org/.

[91] T. Kalmi, «Comparison of Blockchain-based Technologies for Implementing Community Currencies,» Aalto University, 2018.

[92] H. Z. R. a. L. O.-M. Tsung-Ting Kuo, «Comparison of blockchain platforms, a systematic review and healthcare examples,» pp. 462-478, 2019.

[93] T. Coulter. [Online]. Available: https://www.trufflesuite.com/.

[94] Ropsten. [Online]. Available: https://github.com/ethereum/ropsten.

[95] Tecnoandroid. [Online]. Available: https://www.tecnoandroid.it/2019/06/19/facebook-libra-11-cose-da-sapere-sulla-criptovaluta-542987.

[96] Irena. [Online]. Available: https://cms.irena.org/-/media/Files/IRENA/Agency/Publication/2019/Feb/IRENA_Innovation_Landscape_2019_report.ashx.

[97] Fintastico. [Online]. Available: https://www.fintastico.com/it/blog/smart-contract-e-linguaggi-di-programmazione/.

[98] Neo. [Online]. Available: https://neo.org/dev.

[99] Chainlink. [Online]. Available: https://link.smartcontract.com/whitepaper.

[100] N. Hindman, «Bancor,» 3 Marzo 2019. [Online]. Available: https://blog.bancor.network/redesigning-community-currencies-from-one-tomato-to-1000-wallets-on-sarafu-network-80a629354ab1. [Consultato il giorno 2020].

Abbreviazioni ed Acronimi

AES	Advanced Encryption Standard
B2B	Business to Business
B2C	Business to Consumer
BMG	Brooklyn Microgrid
C2B	Cosumer to Business
C2C	Consumer to Consumer
CEC	Citizen Energy Community
CIC	Community Inclusive Currency
c-VPP	Community-based Virtual Power Plant
DAO	Decentralized Autonomous Organizations
DApp	Distributed Applications
DES	Data Encryption Standard
DLT	Distributed Ledger Technolgy
D-PoS	Delegated Proof of Stake
EC	Energy Community
EMD II	Directive on common rules for the internal market for electricity
EoCoE-II	Energy Oriented Centre of Excellence
ETO	Equity Token Offering
EV	Electric Vehicle
EWF	Energy Web Foundation
FER	Fonti Energetiche Rinnovabili
GLPCM	Goleta Load Pocket Community Microgrid
ICO	Initial Coin Offering
IWG	Implementation Working Group
JPI	Joint Programme Initiative Urban Europe
LETS	Local Exchange Systems
MOBI	Mobility Open Blockchain Initiative
OTP	one-time-pad
P2P	Peer to Peer
Pcc	Point of Common Coupling
PED	Postive Energy District
PNIEC	Nazionale Integrato Energia e Clima
PoA	Proof of Activity
PoAu	Proof of Authority
PoI	Proof of Importance
PoS	Proof of Stake
PoW	Proof of Work
PQoS	Perceived Quality of Service
PRG	pseudo-random generator

PUF	Physical unclonable function
QoS	Quality of Service
KPI	Key Performance Indicator
REC	Renewable Energy Community
RED II	Renewable Energy Directive
RSA	Rivest-Shamir-Aldeman
SET- Plan	Strategic Energy and Technology Plan
SHA	Secure Hash Algoritms
V2G	Vehicle to Grid
VPP	Virtual Power Plant
XOR	exclusive or
ZKP	zero-knowledge-proof