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

MINISTERO DELLO SVILUPPO ECONOMICO

Ricerca di Sistema elettrico

Analisi dei requisiti per infrastruttura Blockchain in ottica di scalabilità e decentralizzazione

G.Iovane, A.Rapuano

Report RdS/PTR(2020)/029

Analisi dei requisiti per infrastruttura Blockchain in ottica di scalabilità e decentralizzazione

G.Iovane, A.Rapuano - Università degli Studi di Salerno, Dip. Informatica

Aprile 2021

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dello Sviluppo Economico - ENEA
Piano Triennale di Realizzazione 2019-2021 - II annualità
Obiettivo: Tecnologie
Progetto: Tecnologie per la penetrazione efficiente del vettore elettrico negli usi finali
Work package: WP1 "Local Energy District"
Linea di attività: LA 1.54
Responsabile del Progetto: Claudia Meloni, ENEA
Responsabile del Work package: Claudia Meloni, ENEA

Il presente documento descrive le attività di ricerca svolte all'interno dell'Accordo di collaborazione "Analisi dei requisiti per infrastruttura Blockchain in ottica di scalabilità e decentralizzazione"

Responsabile scientifico ENEA: Marta Chinnici
Responsabile scientifico Università degli Studi di Salerno: Gerardo Iovane

Indice

Sommario

Nella presente attività è stata effettuata l' analisi delle idee alla base delle migliori criptovalute, le chiavi del loro successo e i relativi algoritmi con un focus particolare all'ASIC (Application specific integrated circuit) resistance. Nel dettaglio, è stata valutata la compatibilità delle piattaforme esistenti di blockchain con l'infrastruttura ENEA e gli Smart Contract. Infine sono stati valutati i vari meccanismi di custodia delle chiavi private. In particolare le attività hanno riguardato:

- panoramica sui progetti delle migliori criptovalute per capitalizzazione, nella panoramica sono stati analizzati i meccanismi di mining utilizzati, le caratteristiche tecniche, i motivi del loro successo e gli eventuali svantaggi rispetto ad altri progetti;
- tipi di hardware per il mining Proof of Work ed evoluzione degli stessi, algoritmi in utilizzo, i vantaggi della decentralizzazione del mining e architetture per la decentralizzazione;
- valutazione delle piattaforme blockchain che implementano Smart Contracts e compatibilità sull'infrastruttura ENEA in ottica di scalabilità e decentralizzazione;
- valutazione dei meccanismi di custodia chiavi private per miglioramento usabilità e sicurezza.

Dal report sono emersi i requisiti per lo sviluppo di un buon progetto blockchain che garantiscano una buona adozione di eventuali token. Inoltre è risultato che al momento tra le migliori piattaforme per il deploy degli Smart Contracts compatibili con l'infrastruttura ENEA, si annovera la Binance Smart Chain, perché garantisce ottima maturità sia dal punto di vista della tecnologia blockchain che dagli strumenti di sviluppo attraverso l'Ethereum Virtual Machine. Essa garantisce un'ottima sicurezza, scalabilità a discapito di una discreta decentralizzazione. Sono da tenere in considerazione gli ecosistemi Cardano di cui, però, il sistema di Smart Contracts è ancora in via di sviluppo e Energy Web, piattaforma EVM orientata alle aziende per le tecnologie energetiche sostenibili, che ha un ottimo potenziale, ma che è ancora poco matura. Per tale motivo sono state considerate insieme ad ENEA, oltre alle piattaforme proposte nel presente documento, altre soluzioni con le stesse caratteristiche ma più mature da un punto di vista della gestione delle contrattazioni soprattutto in ambito Smart City.

Infine, è emerso che al fine di mantenere al sicuro i fondi dedicati allo sviluppo dei nuovi token, sarà importante e possibile destinare i fondi ad un cold wallet di tipo paper multifirma per i fondi su cui non si ha bisogno di effettuare operazioni frequenti ed un hot wallet di tipo hardware wallet per le operazioni frequenti.

1. Introduzione

In una società che evolve in modo esponenziale e caotico, uno dei settori che resiste alle attuali difficoltà economiche, ma anzi, si sviluppa e rispecchia questa rapida e continua evoluzione è quello della tecnologia e in particolare dell'Information Technology e Internet che ormai fa sempre più parte delle nostre vite quotidiane. Ogni giorno milioni di dati vengono inviati e trasmessi sulla rete: sono semplici messaggi, dati sensibili o risorse finanziarie. La necessità di utilizzare o creare meccanismi affidabili che consentano transazioni sicure è sempre stata oggetto di ricerche nel campo della sicurezza delle informazioni e della crittografia. Infatti, nel corso degli anni sono stati sviluppati diversi metodi per garantire l'autenticità dei dati; basti pensare che siamo passati dalle firme elettroniche a quelle digitali, che hanno portato un enorme balzo in avanti, soprattutto nel campo della pubblica amministrazione.

Negli ultimi anni sta facendo discutere molto di sé una nuova tecnologia che sembra garantire un importante punto di svolta per il futuro della convalida e del trasferimento dei dati e, potenzialmente, per il coordinamento di tutte le attività umane su scala globale come non è mai stato possibile finora: la tecnologia blockchain; di cui parliamo spesso di un'innovazione destinata a cambiare per sempre i meccanismi transazionali. C'è chi la descrive come una rivoluzione che avrà un impatto simile a quello che ha fatto il World Wide Web. Questo è possibile, dal momento che tutti gli eventuali scenari sono ancora in fase di definizione.

L'infrastruttura ENEA sta progettando di utilizzare questa tecnologia al fine di renderla scalabile e energicamente competitiva, permettendo inoltre di trasferire token tramite blockchain in modo da registrare, certificare e tracciare tutte le operazioni effettuate dagli Smart Contract impiegati. Il punto focale della linea di attività è l'infrastruttura che ospiterà la piattaforma blockchain dedicata alla coniazione e alla circolazione dei token, i metodi di sviluppo e di custodia dei fondi.
Siccome l'ecosistema blockchain è in continuo sviluppo, è importante analizzare le piattaforme presenti sul mercato e definire, tenendo conto delle prestazioni, dei costi e della probabilità di successo dell'ecosistema scelto, quale piattaforma permette di minimizzare i rischi dell'infrastruttura che andrà a nascere.

In particolare, nel presente documento, verranno analizzati gli ecosistemi al momento più capitalizzati, con un focus particolare e approfondito su Bitcoin ed Ethereum, inquadrando poi i fattori di successo o insuccesso (al fine di minimizzare il rischio) delle principali piattaforme presenti attualmente sul mercato.

Verranno, dopodichè, analizzati i metodi di incentivi per la messa in sicurezza della rete, come si è evoluto il sistema di incentivi di Bitcoin ed i principali algoritmi di mining per il meccanismo di consenso Proof of Work, l'algoritmo attualmente più utilizzato e sicuro.

È altresì importante, una volta costruita l'infrastruttura, mantenere al sicuro i fondi utilizzati dagli Smart Contracts. A tal fine, verranno analizzati i meccanismi di custodia delle chiavi private individuando le migliori strategie per la custodia dei fondi da utilizzare nell'infrastruttura.

2. Descrizione delle attività svolte e risultati

I capitoli successivi (da cap. 3 a cap. 7) descrivono le attività svolte e i risultati ottenuti nell'ambito della presente Linea di Attività.

In particolare, nel capitolo 3 vengono analizzati i migliori progetti blockchain partendo prima da Bitcoin, il quale ha dato inizio alla rivoluzione della blockchain utilizzata per pagamenti peer to peer, ed Ethereum che ha rivoluzionato il settore con il concetto degli Smart Contracts; per poi vertere su una panoramica delle caratteristiche tecniche dei migliori progetti blockchain per capitalizzazione al fine di ottenere i requisiti per il successo di un nuovo progetto. Inoltre, grazie alla suddetta analisi, è stato possibile individuare le piattaforme per Smart Contracts che fanno utilizzo di strumenti di sviluppo maturi e che permettono di superare il grande problema di scalabilità presente ad oggi su Ethereum.

Nel capitolo 4 sono stati analizzati i meccanismi di incentivi ai nodi per il mantenimento del consenso e quindi della sicurezza all'interno del network. In particolare, siccome il meccanismo di consenso Proof of Work (PoW) è il più maturo, ne è stata approfondita la storia, i meccanismi di decentralizzazione (ASIC resistance) e gli algoritmi.

Nel capitolo 5 sono state valutate le piattaforme individuate nella presente Linea di Attività per la compatibilità delle suddette con l'infrastruttura ENEA.

Nel capitolo 6 vengono analizzati e valutati i meccanismi di custodia delle chiavi private, organizzando una strategia per la minimizzazione del rischio nella gestione dei fondi ENEA destinati alla nascente infrastruttura basata su blockchain.

Infine nel capitolo 7 sono riportate le conclusioni che sono state raggiunte nel lavoro presentato e che rappresentano la base per la costruzione delle attività future.

3. Stato dell'arte: i migliori progetti blockchain

In questa attività sono state analizzate le migliori piattaforme blockchain, con particolare attenzione alle tecnologie inizializzate da Bitcoin (blockchain) ed Ethereum (Smart Contracts). Mettendo a nudo le caratteristiche tecniche dei migliori progetti disponibili sul mercato e i punti di forza, abbiamo ottenuto un duplice obiettivo:

- individuazione della migliore piattaforma blockchain dal punto di vista della sicurezza e scalabilità sulla quale sviluppare gli Smart Contracts ENEA;
- estrazione dei requisiti di successo e diffusione di un nuovo token.

3.1 Bitcoin

Fino al 2009 si cercava una soluzione al problema del double spending delle monete digitali peer to peer. Un file che rappresentasse una moneta, poteva essere copiato e speso più volte. Quando Satoshi Nakamoto, anonimo inventore di Bitcoin, rilascia il proprio whitepaper [1], si inizia a parlare di una soluzione di distributed ledger per pagamenti peer to peer, dove la "trustness" delle transazioni è una combinazione di firme digitali e algoritmi di consenso. Il tutto salvato su di un database distribuito e ridondante chiamato blockchain. La blockchain ha alcune caratteristiche molto importanti come l'immutablità, la resistenza ai fault, la non manipolabilità, la trasparenza e la non ripudiabilità delle transazioni. Tutte queste caratteristiche la rendono perfetta per molteplici campi di appicazioni. Nel 2009 è nata una nuova era della Computer Science grazie a questo lavoro. A quel tempo, Nakamoto capì per prima cosa l'importanza di:

- creare una moneta digitale che non dipenda dalle banche centrali;
- creazione di un meccanismo, chiamato proof of work, che garantisca un consenso pubblico sul sistema delle transazioni;
- garantire la scarsità della moneta, la cui estrazione viene costantemente ridotta fino a raggiungere un massimo di 21 milioni di unità al fine di limitarne l'inflazione fino ad annullarla.

Per quanto riguarda il primo punto, possiamo facilmente comprendere l'importanza di una moneta peer-to-peer decentralizzata online, trasformando qualsiasi transazione in un baratto digitale innovativo, evitando i costi di intermediazione e gli accessori. Anche sul secondo punto e sul suo impatto sulla Comunità ci sarebbe molto da dire; ci limitiamo ad evidenziare il potenziale più importante della blockchain, cioè la capacità di scrivere e tenere traccia delle transazioni su un sistema altamente distribuito e decentralizzato, quindi difficile da violare e manipolare, le cui transazioni fanno parte di una catena potenzialmente planetarie, ma che allo stesso tempo preserva la privacy e la sicurezza delle informazioni, dal momento che gli attori coinvolti nella transazione stessa sono pseudonimizzati.
Il terzo punto è una caratteristica puramente finanziaria che garantisce che la moneta non venga inflazionata. Per un periodo, la blockchain è stata confusa, o meglio, identificata con Bitcoin. Forse per quest'ultima ragione la blockchain sembra spesso associato a un concetto di denaro e di pagamento. In realtà questa tecnologia, grazie alle proprietà precedentemente descritte, può essere utilizzata in innumerevoli campi. Sebbene la sua popolarità sia direttamente proporzionale al suo utilizzo nel settore delle monete digitali, la sua capacità tecnologica è già oggetto di discussione per un uso specifico in contesti reali come:

- effettuare operazioni sicure in contesti in cui i regimi politici repressivi inibiscono l'uso degli organi delegati a controllarli;
- può fungere da registro pubblico o privato, da cui si può tracciare, controllare e scambiare qualunque tipo di dato che sia concreto (case, libri, auto) o astratto (proprietà intellettuale, dati sanitari);
- può essere utilizzata per la tracciabilità nella filiera produttiva o in qualsiasi altro contesto che richieda tracciamento di operazioni. In realtà, questi elementi si stanno dimostrando un'efficace

rivoluzione concettuale con possibili implicazioni e applicazioni a qualsiasi campo cognitivo e alle diverse possibili attività reali.

Il whitepaper di Bitcoin definisce come moneta elettronica una catena di firme digitali. Ciascun proprietario trasferisce moneta al successivo firmando digitalmente la transazione contenente la chiave pubblica del destinatario. Colui che riceve un pagamento può verificare le firme digitali per validare la catena delle proprietà (Figura 1).

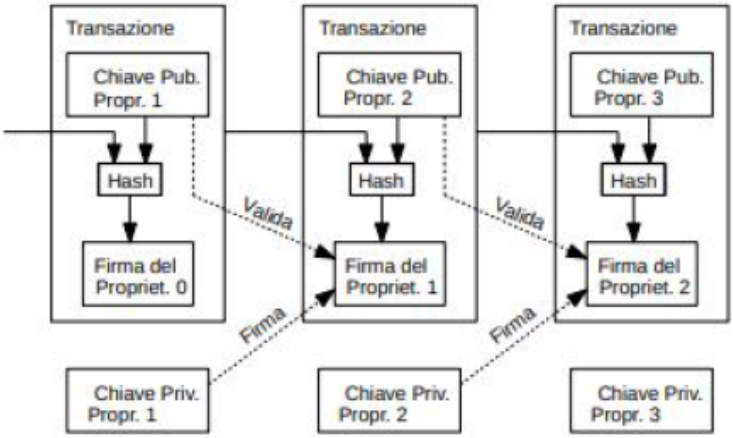

Figura 1. Catena di firme digitali per le transazioni Bitcoin.

In un contesto dove viene implementata soltanto una catena di transazioni, il problema è che il beneficiario non può verificare che ciascuno dei proprietari precedenti non abbia speso due volte lo stesso ammontare. Una soluzione comune è quella di introdurre un'autorità fiduciaria centrale, o zecca, che controlli tutte le transazioni. Dopo ogni transazione, la moneta deve essere restituita alla zecca la quale emette una nuova moneta, e si crede che solo le monete emesse direttamente dalla zecca non siano state spese due volte. Il problema di questa soluzione è che il destino di tutto il sistema monetario dipende dalla società che gestisce la zecca ed ogni transazione deve passare attraverso di essa, proprio come una banca. Satoshi Nakamoto ha definito un meccanismo per far sì che il beneficiario sapesse che i precedenti proprietari non avessero firmato alcuna transazione precedente a quella che lo riguarda. La prima operazione è quella che conta e non importa nulla dei tentativi successivi di doppia spesa. L'unico modo per confermare l'assenza di una transazione è di essere a conoscenza di tutte le transazioni. Nel modello basato sulla zecca, quest'ultima era a conoscenza di tutte le transazioni e decideva quale era avvenuta per prima. Per ottenere lo stesso risultato ma senza un'autorità di fiducia, le transazioni devono essere annunciate pubblicamente e si ha bisogno di un sistema attraverso il quale i partecipanti possano concordare su un singolo passato nell'ordine in cui esse sono state ricevute. Il beneficiario ha bisogno di una prova che, al momento di ogni transazione, la maggior parte dei nodi è d'accordo sul fatto che essa è la prima ricevuta. La soluzione proposta da Nakamoto parte da un server di marcatura temporale. Un server di marcatura temporale agisce computando l'hash (una funzione one way che codifica una stringa di lunghezza arbitraria in una di lunghezza predefinita) di un blocco di oggetti in modo che siano marcati temporalmente. Dopodichè ne pubblica l'hash, ad esempio su un quotidiano o in un post su Usenet. La marcatura temporale prova che i dati devono essere esistiti in quella determinata data, in quanto si trovano nell'hash. Ogni marcatura temporale comprende quella precedente nel suo hash, formando una vera e propria catena e ogni marcatura temporale rafforza quelle precedenti (Figura 2).

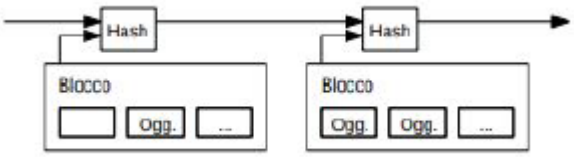

Figura 2. Catena di blocchi in Bitcoin. Ogni blocco è legato al blocco precedente attraverso l'hash delle informazioni contenute nel blocco stesso.

Per implementare un server di marcatura temporale distribuito su base peer-to-peer, Bitcoin usa un sistema simile a quello di Hashcash di Adam Back [2], piuttosto che basarsi sui messaggi di quotidiani o Usenet.
Bitcoin utilizza un sistema di consenso chiamato Proof of Work (PoW). Esso comporta la ricerca di un valore che, una volta sottoposto ad hash (ad esempio, in Bitcoin, con SHA-256), restituisca un valore che inizia con un numero target di zero bit. Il lavoro medio richiesto è esponenzialmente proporzionale al numero di zero bit richiesti e può essere verificato eseguendo un unico hash.
Per la rete di marcatura temporale, Bitcoin implementa la PoW incrementando un iteratore inserito nel blocco, il quale fa cambiare il valore dell'hash e che viene chiamato nonce. Esso viene incrementato fino a quando non viene trovato un valore che, nell'hash del blocco, restituisce gli zero bits necessari. Una volta che l'impegno della CPU è stato speso per soddisfare la PoW, il blocco non può essere modificato senza rieseguire il lavoro. Poiché i blocchi successivi sono incatenati dopo di esso, il lavoro necessario per cambiare il blocco dovrebbe includere il rifacimento di tutti i blocchi successivi. La PoW risolve anche il problema della determinazione della rappresentatività in un sistema di decisioni prese a maggioranza. Se la maggioranza fosse basata sul principio "un indirizzo IP-un voto", potrebbe essere sovvertita da chiunque fosse in grado di allocare molti IP. La PoW invece segue essenzialmente il principio "una CPU-un voto". La decisione di maggioranza è rappresentata dalla catena più lunga, su cui è stato speso il massimo sforzo di computazionale. Se la maggioranza di potenza della CPU è controllata da nodi onesti, la catena onesta crescerà più velocemente e supererà eventuali catene concorrenti. Per compensare l'aumento della velocità dell'hardware e il variare dell'interesse dei nodi operativi col tempo, la difficoltà della PoW è determinata da una media mobile che ha come obiettivo la creazione di un numero medio di blocchi ogni ora. Se i blocchi vengono generati troppo velocemente, la difficoltà viene aumentata. Per convenzione, la prima transazione in un blocco è una transazione speciale che "conia" una nuova moneta di proprietà del creatore del blocco. Questo fornisce un incentivo ai nodi affinché sostengano la rete; inoltre fornisce un modo per la distribuzione iniziale di monete in circolazione dato che non vi è alcuna autorità centrale che possa emetterle. L'aggiunta costante di una data quantità di nuove monete è analoga al processo dei minatori d'oro, i quali spendono risorse per incrementare la quantità di oro in circolazione. In questo caso, viene spesa potenza CPU e viene consumata energia elettrica. L'incentivo può essere anche finanziato attraverso i costi di transazione. Se il valore di uscita di una transazione è inferiore al suo valore di ingresso, la differenza è una tassa di transazione che viene aggiunta al valore di incentivazione del blocco contenente la transazione. Nel momento in cui sia entrato in circolazione un ammontare predeterminato di monete, l'incentivo può migrare interamente ai costi di transazione e essere completamente privo di effetti inflazionari. L'incentivo contribuisce ad incoraggiare i nodi a rimanere onesti. Se un utente malevolo fosse in grado di assemblare più potenza computazionale rispetto a tutti i nodi onesti, dovrebbe scegliere tra un utilizzo truffaldino, effettuando double spending o un utilizzo volto a coniare nuove monete. Dovrà necessariamente trovare più redditizio comportarsi secondo le regole, dato che tali regole lo favoriscono con più monete nuove di tutti gli altri messi insieme, piuttosto che minare la sicurezza del sistema e la validità della propria ricchezza.
Attualmente il protocollo Bitcoin, perfino senza nessuna estensione, facilita una debole versione del concetto di "Smart Contracts". Unspent transaction output (UTXO) è il nome delle transazioni Bitcoin e rappresentano

le monete non spese dopo aver effettuato una transazione. Nella figura 3 è rappresentato un esempio di UTXO.

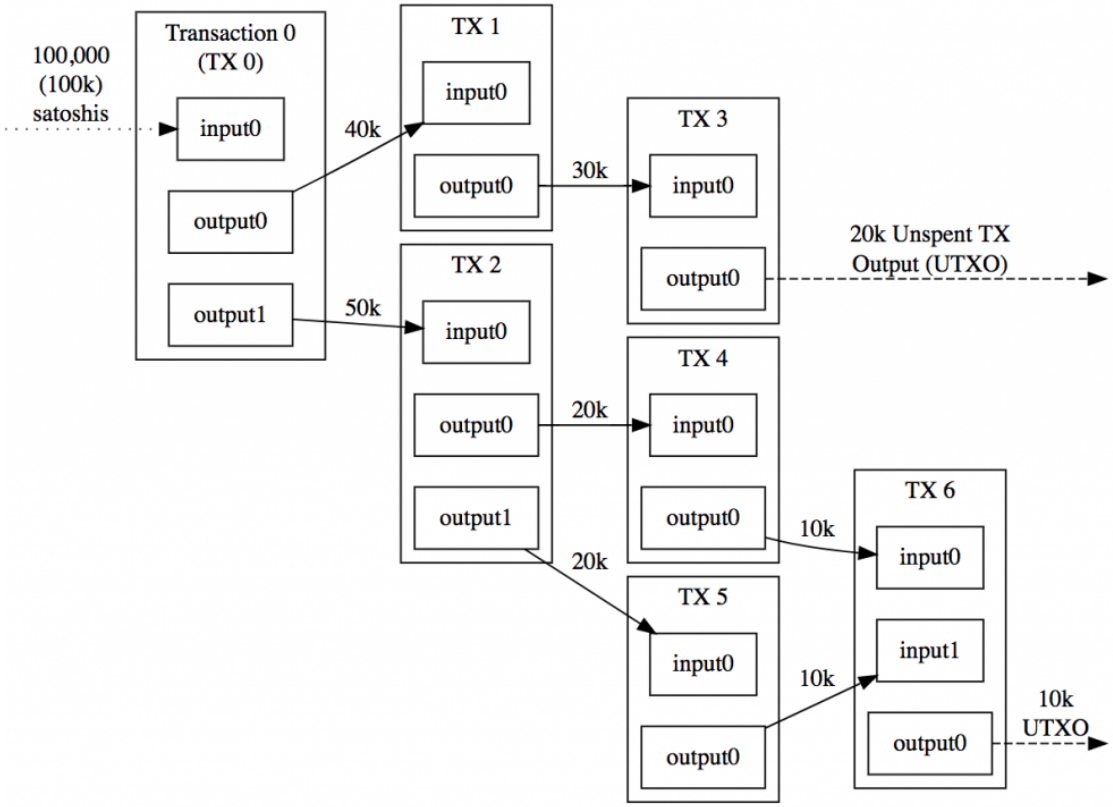

Figura 3. Esempio di albero di Unspent transaction Output (UTXO).

Ad esempio, un wallet di Bitcoin con una quantità di monete di 100 BTC è composto da tanti UTXO. Esso potrebbe avere due UTXO del valore di 50 o un insieme di UTXO del valore di 37, 18, 40 e 5 Bitcoin. Se un wallet inviasse 35 bitcoin contenendo solo UTXO pari a 15, 17, 28 e 40 Bitcoin ciascuno, il wallet non avrebbe un UTXO di 35 Bitcoin, ma non è possibile dividere le UTXO; sarebbe quindi impossibile pagare i 35 Bitcoin esatti. Allora in questo caso, verrebbero spesi i 40 Bitcoin UTXO, o una qualsiasi altra combinazione di UTXO, ad esempio 17 BTC e 28 BTC. In quest'ultimo esempio, la rete conia due nuovi UTXO: uno del valore di 35 Bitcoin, uno del valore di 5 Bitcoin. Il wallet destinatario riceve la UTXO di 35 Bitcoin mentre, come resto, si ricevono 5 Bitcoin UTXO. Anche le commissioni di transazione sono incluse nelle transazioni e sottratte dall'UTXO che si riceve come resto. Formalmente un nuovo UTXO viene calcolato nel seguente modo:

$$NewUTXO = (\sum_{i=1}^{N} UTXO_i) - a - f.$$

Dove a è l'importo della transazione ed f l'importo delle commissioni. Inserendo i dati dell'esempio precedente e contando un Bitcoin di commissione, si ottiene:

$$NewUTXO = (17 + 28) - (35) - (1) = 9\,BTC.$$

UTXO, in Bitcoin può essere posseduta non solo come chiave pubblica, ma anche da uno script più complesso espresso in un linguaggio di programmazione stack-based. Infatti, il meccanismo base della proprietà della chiave pubblica è implementato con uno script: lo script riceve una firma come input, confrontando quest'ultima con la transazione e l'indirizzo che possiede la UTXO e restituisce 1 se la verifica è andata a buon fine, 0 altrimenti. Altri script più complessi esistono per diversi casi. Per esempio, si può costruire uno script

che richieda firme da più chiavi private impiegate per validare una transazione (multisignature). Questo è utile per conti di società, che mettono al sicuro i fondi e che forniscono ai commercianti funzioni di escrow.
Gli script possono anche essere utilizzati per pagare premi per la soluzione di problemi computazionali e si può anche costruire uno script che indichi che si può scambiare un Bitcoin se si è in grado di provare che si sono inviati Ether ad un dato indirizzo; consentendo essenzialmente un cambio tra monete digitali.
Tuttavia, il linguaggio di scripting, così come implementato nel Bitcoin, presenta alcune importanti limitazioni:

- manca di Turing-completezza del linguaggio di scripting: vale a dire che, anche se esiste un grande sottoinsieme di istruzioni che il linguaggio di scripting di Bitcoin supporta, quest'ultimo non offre molte possibilità. La categoria principale che viene meno è il ciclo. Questa limitazione è imposta al fine di evitare cicli infiniti durante la verifica delle transazioni; teoricamente ciò è un ostacolo sormontabile per i programmatori di script, in quanto qualsiasi loop può essere simulato semplicemente ripetendo il codice sottostante tante volte con un'istruzione condizionale, implicando però script inefficienti dal punto di vista dello storage. Per esempio, l'implementazione di un algoritmo alternativo di firma a curva ellittica necessiterebbe 256 rounds di moltiplicazioni ripetute e tutte incluse individualmente nel codice;
- cecità del valore: non c'è un modo per un UTXO di fornire un controllo sul valore economico del Bitcoin. Per esempio, volendo implementare un contratto oracolo con un contratto sottostante, dove A e B depositano $ 1000 in BTC. Questo contratto, dopo 30 giorni, smista il controvalore di $1000 in BTC ad A ed il resto a B. In questo caso si necessiterebbe di un oracolo. Quest'ultimo dovrebbe determinare il valore di 1 BTC in USD, ma anche in questo caso c'è un incremento esponenziale, sia in termini di fiducia che di infrastruttura necessaria, in quanto si avrebbe bisogno di soluzioni completamente centralizzate;
- mancanza di stato: UTXO può avere solo due stati: speso e non speso; non c'è possibilità per contratti o scripts multi-stage di mantenere altri stati interno. Ciò rende difficile creare contratti di opzioni multi-stage ed exchange decentralizzati (DEX). Questo inoltre significa che UTXO può essere soltanto usato per costruire contratti semplici, ma è limitato nella creazione di più complessi contratti "stateful" come le organizzazioni decentralizzate (DAO) e di meta-protocolli complessi. Lo stato binario, combinato con la cecità del valore, limita anche un'altra importante applicazione, il prelievo in FIAT;
- cecità della BC: UTXO è cieca alla BC. È quindi cieco al nonce dell'hash precedente. Questo pregiudica applicazioni nel campo del gioco d'azzardo e altre molte categorie che fanno uso delle variabili casuali, privando il linguaggio di scripting di una fonte potenzialmente preziosa di pseudocasualità.

Quindi, esistono tre approcci per costruire applicazioni avanzate sull'apice dell'infrastruttura BTC: costruire una nuova BC; usare lo scripting implementato da BTC; o costruire un meta-protocollo sull'apice di BTC. Costruire una nuova BC permette una illimitata libertà nel costruire un insieme di funzionalità, richiedendo però molto più tempo per lo sviluppo, sia dal punto di vista delle criticità relative alla fase iniziale che da quello di messa in sicurezza del sistema. Lo scripting sulla base di BTC è semplice da implementare e standardizzare, ma implica delle limitazioni nelle capacità. Al contrario i meta-protocolli, soffrono di difetti di scalabilità.
Nel 2014, nasce Ethereum, dalla mente di Vitalik Buterin [3]. Con Ethereum, viene costruito un framework alternativo, che fornisce benefici ancora maggiori in termini di semplicità di sviluppo con client estremamente più leggeri, permettendo allo stesso tempo alle applicazioni di condividere l'ambiente economico e la sicurezza della BC.

3.2 Ethereum

Nel 2015 viene lanciata una nuova rivoluzione a questa già importante innovazione: si chiama Ethereum, concepita da Vitalik Buterin e sviluppata in team con altre personalità conosciute oggi nel mondo dell'high-tech.
Ethereum [3] è una piattaforma web 3.0 decentralizzata per la creazione, la pubblicazione peer-to-peer e l'esecuzione automatica di contratti digitali, da cui la definizione di Smart Contracts (SC). Ethereum rappresenta la prima implementazione della blockchain 2.0. La sua vera innovazione consiste proprio negli Smart Contracts. Essi sono algoritmi che hanno al loro interno elementi contrattuali tra persone, che vengono automaticamente eseguiti dai miners Ethereum in modo distribuito, senza avvocati, notai o altri intermediari, ma solo per la volontà espressa dagli attori, con una chiara riduzione di costi accessori e possibili controversie.
Grazie ad Ethereum, nei suoi primi anni di vita, è stato possibile inizializzare campagne di crowdfunding chiamate Initial Coin Offering (ICO), dove gli sviluppatori mostravano la propria idea con un whitepaper agli investitori, i quali potevano contribuire economicamente al progetto in cambio di token creati ad hoc sulla BC Ethereum. Col passare del tempo, questo tipo di operazione è andata via via scomparendo e con essa la fiducia degli investitori, a causa di molte persone che approfittavano del trend per raccogliere fondi e fuggire con i guadagni, lasciando gli investitori con token che non avevano alcun valore. Attualmente, sempre grazie agli Smart Contract, è esplosa una nuova tendenza chiamata finanza decentralizzata (DeFi). Qui gli investitori possono ricevere degli interessi sulle proprie monete digitali bloccate in un contratto, collateralizzare i propri averi al fine prenderne in prestito diverse o di generare stable coins, scambiare le proprie monete su exchange decentralizzati (DEX), ecc. Tutto questo sembra essere solo l'inizio di una tecnologia che è ancora immatura e non ha ancora strumenti perfetti anche dal punto di vista dello sviluppo software e della sicurezza.
Da un punto di vista della storia della Computer Science, la BC ed in particolare, gli SC sembrano seri candidati a divenire il web 3.0.
Il termine "Web 2.0" è stato utilizzato per la prima volta da Darcy Di Nucci nel 1999 ed è diventato popolare grazie a Tim O'Reilly e Dale Dougherty i quali nel 2004 hanno dato vita alla prima conferenza sulla "nuova versione" del Web. I vantaggi che quest'ultima ha portato, si racchiudono in due parole: dinamicità e interazione. Come affermato da Graham Cormode e Balachander Krishnamurthy

"the essential difference between Web 1.0 and Web 2.0 is that content creators were few in Web 1.0 with the vast majority of users simply acting as consumers of content, while any participant can be a content creator in Web 2.0 and numerous technological aids have been created to maximize the potential for content creation".

Col Web 2.0 gli utenti diventano, dunque, parte attiva della rete, la quale non è più soltanto un luogo di consultazione di informazioni: diventa bensì un punto di condivisione di queste e chiunque può partecipare caricando i propri contenuti. I siti web permettono un'elevata interazione con gli utenti, viene data importanza all'utente specifico il quale ha ora la possibilità di creare un profilo personale, con le sue informazioni identificanti (data di nascita, sesso, localizzazione, ecc.). Il termine Web 3.0, invece, è apparso per la prima volta agli inizi del 2006 in un articolo di Jeffrey Zeldman critico verso il Web 2.0 e le sue tecnologie associate. Nel maggio 2006, Tim Berners-Lee affermava:

"People keep asking what Web 3.0 is. I think maybe when you've got an overlay of Scalable Vector Graphics - everything rippling and folding and looking misty - on Web 2.0 and access to a semantic Web integrated across a huge space of data, you'll have access to an unbelievable data resource."

Ancora oggi non è ancora ben chiaro quale potrà essere esattamente la definizione più congrua di "Web 3.0". Con la diffusione di Ethereum è stato definito "Web 3.0" una rete decentralizzata. Se queste reti si diffonderanno a sufficienza da essere considerate la nuova internet, l'innovazione più importante sarà la decentralizzazione: gli utenti possono scegliere di far partecipare il proprio computer o dispositivo al funzionamento della rete stessa e si potranno scambiare beni digitali fra utenti come un baratto 2.0. Le

informazioni vengono automaticamente duplicate su ogni computer che partecipa, distribuendo il calcolo fra tutti i nodi della rete, piuttosto che centralizzandolo su alcuni server noti, come avviene nella attuale rete internet. Ciò garantisce la resistenza della rete a qualsiasi tipo di censura selettiva, manipolazione, fault e attacchi informatici. Attualmente, però, Ethereum sembra ancora acerba per divenire la nuova internet. Nonostante ne abbia tutte le potenzialità, il network soffre di difetti di scalabilità enormi. Basti pensare che con la diffusione della DeFi, le commissioni di Ethereum sono schizzate ai massimi storici, ed anche una semplice operazione di scambio fra token può arrivare a costare l'equivalente di decine di dollari in Ether (ETH). Questo difetto di scalabilità è stato superato da diversi progetti che propongono Proof of Stake (PoS) come algoritmo di consenso, ma che sono meno conosciuti e meno utilizzati. Nonostante questo difetto, Ethereum continua a mantenere la maggioranza dell'utenza e di conseguenza rimane la piattaforma che raggruppa la maggior parte dei progetti BC sulla propria chain. Con il rilascio di Ethereum 2.0 con PoS, si spera che i difetti di scalabilità vengano superati e che si abbia finalmente una piattaforma che raccoglie utenza e abbia allo stesso tempo alta scalabilità.
Discorso a parte meritano gli ancora acerbi strumenti di sviluppo di Smart Contracts di cui parleremo più avanti. Tirando le somme, si ha la sensazione che le piattaforme BC abbiano ancora molto da mostrare siccome offrono potenzialità enormi.

3.2.1 Approfondimento sugli Smart Contracts

Ethereum si definisce una piattaforma web 3.0 decentralizzata per la creazione, la pubblicazione peer-to-peer e l'esecuzione automatica di contratti, da cui la definizione di Smart Contracts. Gli SC hanno al loro interno elementi contrattuali tra persone, che vengono automaticamente eseguiti da una macchina, senza avvocati, notai o altri intermediari, ma solo per la volontà espressa dagli utenti, con una chiara riduzione di costi accessori e possibili controversie, in quanto è completamente gestito da codice informatico. Il concetto base dietro gli SC è semplice, un contratto è un frammento di codice scritto nel linguaggio di programmazione Solidity, questo viene eseguito dai miner sui loro computer in modo distribuito (Figura 4).

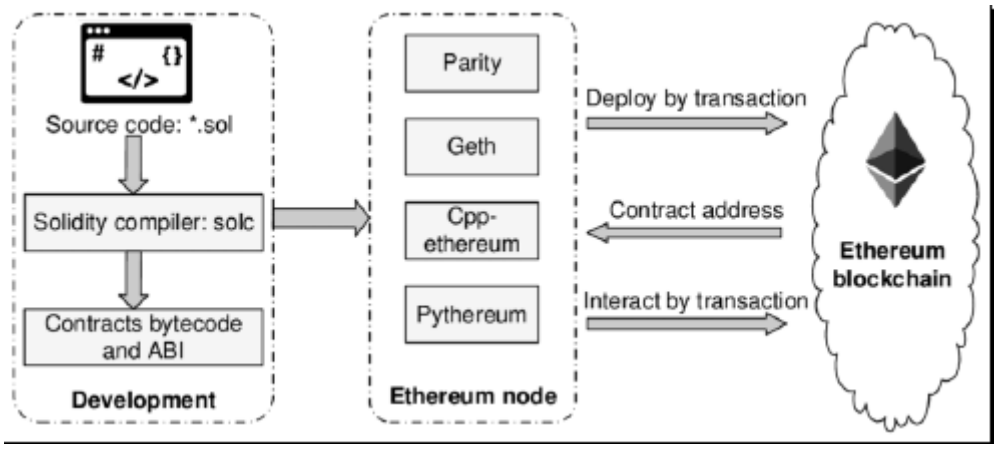

Figura 4. Struttura di uno Smart Contract in Ethereum.

È evidente la semplicità di una logica sottostante di questo tipo e le ampie potenzialità in termini di complessità, generalizzazione, uso e articolazione. Ciò incoraggia l'emergere dei Data Access Object o delle organizzazioni autonome decentralizzate (DAO), che sono SC a lungo termine che gestiscono le risorse e codificano lo statuto di un'intera organizzazione. Quindi uno SC corrisponde a un insieme di stati, una sorta di semaforo con più di tre elementi preordinati, nella quale prima dell'inizio del contratto, tutti gli stati sono inizializzati a "false", durante l'esecuzione alcuni stati saranno diventati "true", fornendo così l'attuale livello di esecuzione in cui si trova lo SC. Al completamento, tutti gli stati saranno "true". Da questo punto di vista, è chiaro che uno SC è un sistema dinamico e l'esecuzione di uno SC è una funzione di transizione di stati

predefiniti (gli elementi fondamentali del contratto) all'interno del sistema di transizioni di stato (cioè per semplicità lo SC). Le applicazioni e gli usi che è possibile costruire sulla base concettuale appena descritta, sono praticamente infiniti, ma come si può vedere dal white paper di Ethereum, possono essere classificati in tre categorie principali:

- applicazioni finanziarie (altre monete digitali, derivati finanziari, contratti di copertura, gestione patrimoniale, gestione degli investimenti, ecc.);
- applicazioni con ripercussioni economiche indirette (gestione di beni di qualsiasi tipo che, attraverso attività reali, creano valore che può essere poi monetizzato);
- applicazioni non finanziarie (voto, governo, gestione, sociale, identità, reputazione, ecc.).

Il motore dell'esecuzione delle transazioni Ethereum è il GAS. Esso è la commissione che ci si impegna a pagare ai miner per l'esecuzione di ogni operazione in una transazione. Il GAS viene pagato in Ether (ETH), la moneta digitale di Ethereum ed una unità di GAS equivale all'esecuzione di un'operazione bytecode. Per aumentare la velocità con cui si esegue l'operazione, chi richiama la transazione, può aumentare il prezzo del GAS. Il prezzo del GAS viene quindi definito GASPRICE. Questo meccanismo ad oggi in Ethereum si è rivelato controproducente in quanto favorisce i possessori di grandi quantità di ETH che non hanno problemi ad aumentare il costo del GAS per transazioni più veloci, a discapito dei piccoli investitori che si trovano a pagare l'equivalente di decine di dollari solo per trasferire le proprie monete. In questo modo, si sta sempre più generando un'asta al rialzo sul prezzo del GAS.
Al fine di evitare esecuzioni infinite che siano malevole o accidentali si definisce il limite di GAS che può essere utilizzato in una transazione. Esso viene definito STARTGAS o GASLIMIT.
Dal whitepaper si può analizzare la funzione di transizione di stato di Ethereum. Essa può essere definita in passi come segue:

- controlla se la transazione è ben impostata (cioè che abbia il giusto numero di valori), che la firma sia valida e il nonce corrispoda a quello dell'account del mittente. In caso contrario, si ottiene un errore;
- calcola la commissione di transazione come STARTGAS * GASPRICE e determina l'indirizzo del mittente dalla firma. Sottrae la commissione dal bilancio dell'account del mittente e ne incrementa il nonce. Se il bilancio non è sufficiente, si ottiene un errore;
- inizializza GAS = STARTGAS e sottrae una certa quantità di GAS per byte al fine di pagare i byte nella transazione;
- trasferisce il valore della transazione dall'account del mittente all'account del destinatario. Se l'account del destinatario non esiste, lo crea. Se l'account del destinatario è un contratto, esegue il codice del contratto fino al completamento o fino a quando l'esecuzione non termina il GAS;
- se il trasferimento fallisce perché il mittente non possiede abbastanza ETH, il codice di esecuzione termina il GAS, ripristina tutti i cambiamenti di stato, ad eccezione del pagamento della commissione e aggiunge le commissioni sul conto del miner;
- altrimenti, rimborsa al mittente le commissioni per il GAS rimanente ed invia al miner le commissioni utilizzate per il GAS.

Il codice nei contratti Ethereum è scritto in un linguaggio di basso livello, cioè il linguaggio bytecode a cascata, ed è denominato "codice Ethereum Virtual Machine (EVM)". Il codice consiste in una serie di bytes, dove ogni byte rappresenta un'operazione. In generale, l'esecuzione del codice è un loop infinito che consiste nel realizzare ripetutamente l'operazione al contatore del programma attuale (che inizia con zero), incrementando il contatore del programma (PC) di uno fino a che non si arriva alla fine del codice, ad un errore, ad uno STOP, o se è rilevata l'istruzione RETURN. Le operazioni hanno accesso a tre tipi di spazio nel quale registrare i dati:

- lo stack, un last-in-first-out, che è un contenitore nel quale i valori possono essere inseriti o rimossi;
- la memoria, un array di byte espandibile all'infinito;
- lo storage a lungo-termine del contratto, si tratta di uno store a modello chiave/valore. A differenza dello stack e della memoria dove i valori si resettano dopo la fine del calcolo, lo storage è persistente.

Il codice può anche accedere al valore, all'indirizzo del mittente e ai dati del messaggio in arrivo, così come ai dati dell'header del blocco. Esso può anche restituire un array di dati come output. Mentre la EVM

funziona, tutto il suo stato computazionale può essere definito dall'insieme di dati (stato del blocco, transazione, messaggio, codice, memoria, stack, PC, gas), dove lo stato del blocco è lo stato globale che contiene tutti gli accounts e include i bilanci e lo storage. All'inizio di ogni turno di esecuzione, l'istruzione corrente viene recuperata attraverso l'i-esimo (con i=PC) byte del codice (o 0 se PC è maggiore o uguale alla lunghezza del codice) e ogni istruzione ha la propria definizione di come interagisce con l'insieme di dati. Per esempio, ADD recupera due oggetti dallo stack e ne inserisce la loro somma risultante, riduce gas di 1 e incrementa PC di 1. SSTORE recupera due oggetti dalla cima dello stack ed inserisce il secondo oggetto nello storage del contratto all'indice specificato dal primo oggetto. Sebbene ci siano molti modi di ottimizzare l'esecuzione della EVM attraverso la compilazione, un'implementazione base di Ethereum può essere scritta in poche centinaia di righe di codice. La blockchain di Ethereum è in molti versi simile a quella di Bitcoin, seppur con qualche differenza. La differenza principale tra la blockchain Ethereum e quella di Bitcoin è nell'architettura. Contrariamente a quella di Bitcoin, i blocchi di Ethereum contengono una copia sia dell'elenco delle transazioni sia dello stato più recente. Inoltre, il numero di blocco e la difficoltà, vengono memorizzati nel blocco stesso.
Sia APPLY(S,Tx)->S' una funzione con input uno stato S ed una transazione Tx e un output un nuovo stato S', l'algoritmo di validazione del blocco alla base in Ethereum funziona nel seguente modo:

- controlla che il precedente blocco di riferimento esista e che sia valido;
- controlla che la marcatura temporale del blocco sia più grande di quella del blocco di riferimento precedente ed inferiore di 15 minuti;
- controlla che il numero del blocco, difficoltà, l'origine della transazione, la transazione derivata ed il GASLIMIT siano validi;
- controlla che la PoW del blocco sia valida;
- sia S[0] lo stato alla fine del blocco precedente; sia Tx la lista delle transazioni del blocco, con n transazioni; per tutte le transazioni Tx[i] con $0 \leq i \leq n-1$, S[i+1] = APPLY(S[i],Tx[i]). Se qualsiasi APPLY(S,Tx)->S' restituisce un errore o se il GAS totale è consumato nel blocco fino a che eccede il GASLIMIT, viene restituito un errore.
- Sia S FINAL = S[n] lo stato finale, il quale comprende la ricompensa per il blocco pagata al miner, controlla che lo stato originario del Merkle tree S FINAL sia uguale allo stato finale originario fornito nell'intestazione del blocco. In tal caso, il blocco è valido; in caso contrario, quest'ultimo non è valido.

Un quesito comune che ci si pone frequentemente è "dove" il codice del contratto venga eseguito, in termini di hardware fisico. Questa è una risposta semplice: il processo di esecuzione del codice del contratto è una parte della definizione della funzione di transizione di stato che, a sua volta, è una parte dell'algoritmo di validazione del blocco, così che se una transazione viene aggiunta al blocco B l'esecuzione del codice generata da questa transazione sarà eseguita da tutti i nodi, nel presente e nel futuro, scaricando e validando il blocco B.

3.2.2 Strumenti di sviluppo per Smart Contracts

Come detto in precedenza, gli strumenti di sviluppo di Smart Contracts sono ancora acerbi. Nonostante gli evidenti limiti, gli Smart Contracts, al momento sono nel loro massimo storico utilizzo grazie alla già citata DeFi. In questa sezione analizziamo lo stato dell'arte degli strumenti di sviluppo per Smart Contracts EVM.

Linguaggi di programmazione ad alto livello

Nonostante la EVM utilizzi il linguaggio a cascata bytecode, esistono diversi linguaggi di programmazione ad alto livello per sviluppare Smart Contracts EVM: i più diffusi sono Vyper e Solidity.

Vyper

Questo linguaggio è basato su Python ed ha come punti di focus la leggibilità e la sicurezza. Al fine di garantire la trasparenza per chi esegue i contratti, Vyper semplifica enormemente la scrittura di Smart Contracts, eliminando ereditarietà, overload delle funzioni o degli operatori, modificatori e ricorsività. Nessuno dei citati è necessario al fine di ottenere un linguaggio Turing-completo e questo garantisce una maggiore leggibilità del codice per chi non è un programmatore. All'aumentare della complessità dei concetti citati, aumentano i problemi di sicurezza. Oltre al problema che i modificatori possono favorire la scrittura di codice ingannevole. Gli sviluppatori di Vyper hanno dichiarato che Vyper "*vieterà alcune funzionalità deliberatamente o renderà le cose più difficili qualora lo ritenga opportuno per l'obiettivo di aumentare la sicurezza*". Quindi Vyper non mira ad essere un sostituto di Solidity, ma si propone come linguaggio di programmazione da utilizzare quando la sicurezza, la semplicità e la trasparenza sono prioritarie.

Solidity

Solidity è un linguaggio di programmazione orientato agli oggetti per la scrittura di Smart Contracts. Esso fornisce eredità degli oggetti, librerie e dati tipati. È famoso per essere utilizzato per l'implementazione di Smart Contracts Ethereum, ma viene utilizzato anche per altre blockchain come Tron e Binance Smart Chain (BSC) che sono compatibili con la EVM. Solidity può quindi essere compilato in Bytecode e venire eseguito dalla EVM. Ad oggi, Solidity ha raggiunto un buon livello di maturità ed è quindi la prima scelta per la programmazione di Smart Contracts EVM.

Compilatori Solidity

Negli anni sono pochi gli strumenti che sono stati sviluppati per la compilazione di Smart Contracts Solidity essendo una tecnologia ancora molto giovane. Molti di quelli che sono stati proposti, sono deprecati. Gli unici compilatori che hanno raggiunto una buona maturità sono Remix e la suite Truffle.

Remix

Remix è un compilatore Solidity online, ma che ultimamente ha rilasciato anche un'IDE desktop. È ottimo per la compilazione ed il deploy di Smart Contracts semplici e per chi vuole iniziare ad imparare a programmare Smart Contracts. L'interfaccia è estremamente semplice, il deploy di un contratto si divide in tre passi:

- creazione del contratto;
- compilazione;
- deploy.

Creazione del contratto: una volta entrati nell'IDE, sulla sinistra (Figura 5) troviamo i file a disposizione, tra i quali possono essere creati nuovi file Solidity, è possibile importare file da github o organizzare i file in cartelle. Dalla figura si può comprendere come Remix sia un ottimo tool per lo sviluppo di progetti semplici, con pochi contratti, ma che diventa confusionario quando i contratti diventano numerosi.

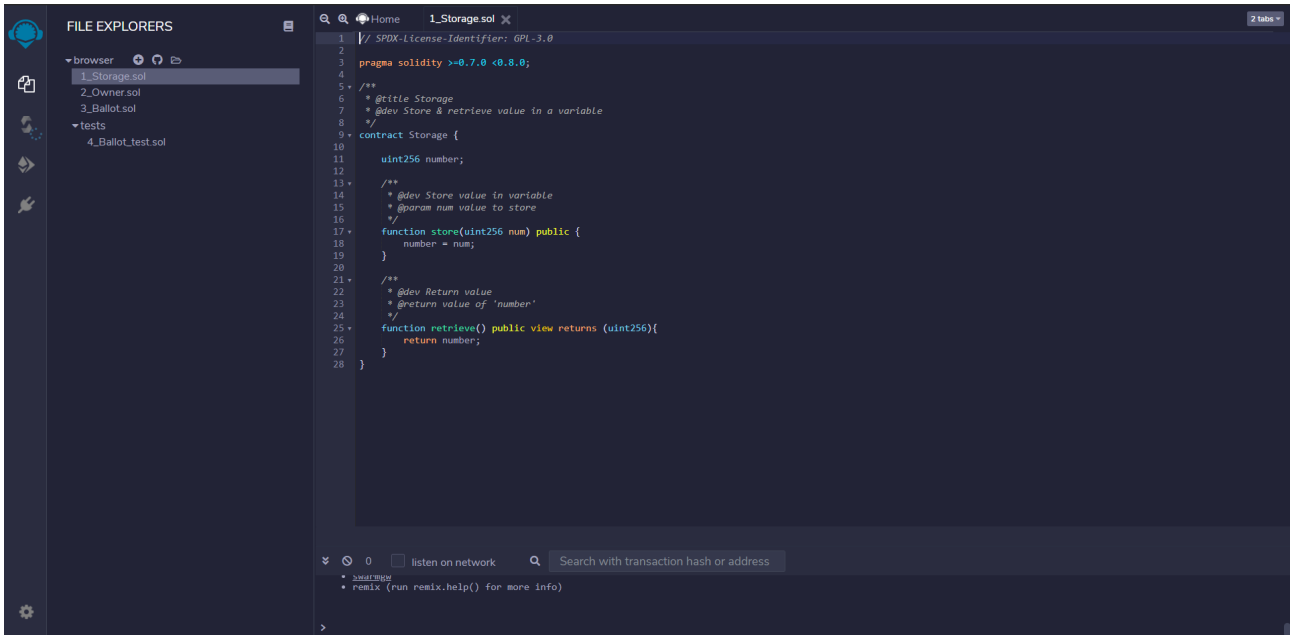

Figura 5. Interfaccia IDE Solidity.

Compilazione: Terminata la scrittura del contratto è possibile compilarlo nella sezione “compilazione” (Figura 6). Qui è possibile selezionare la versione del compilatore (dichiarata nel contratto attraverso l’istruzione Pragma). Molto importante è l’opzione di ottimizzazione della compilazione. Grazie a questa opzione, il bytecode generato viene ottimizzato e si ottiene una discreta riduzione dei costi di GAS. Dopo aver modificato le opzioni, si deve cliccare sul bottone “Compile” per dare inizio alla compilazione del contratto.

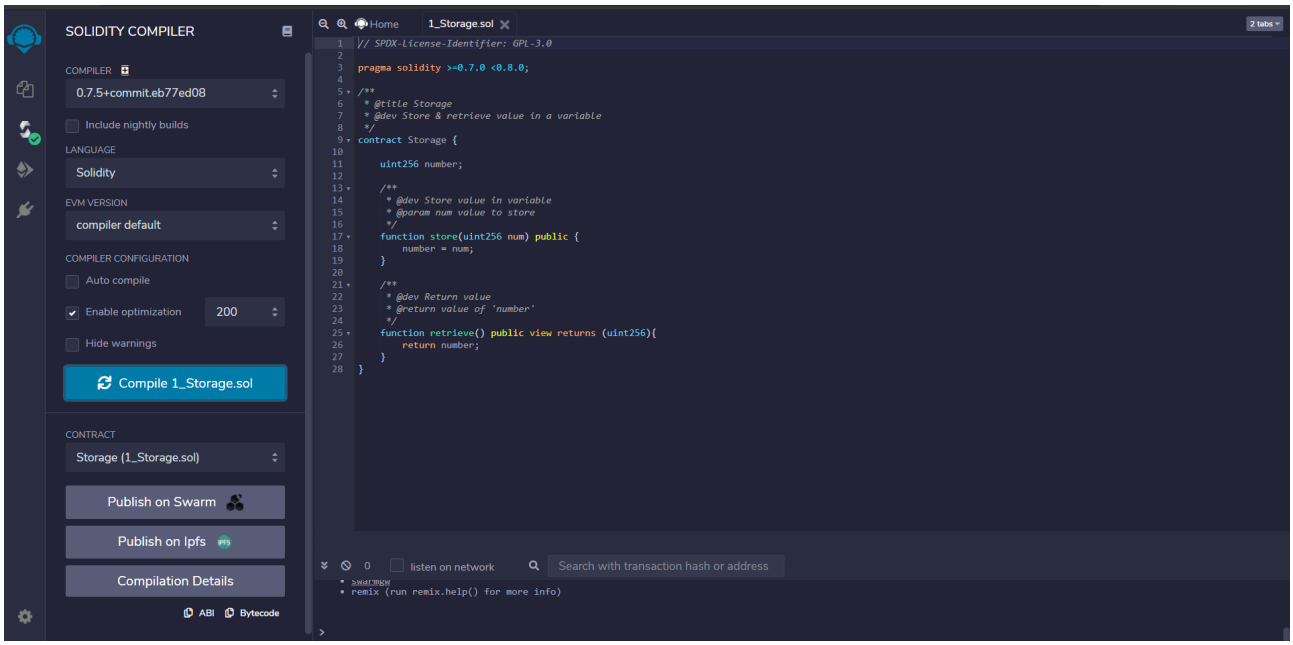

Figura 6. compilazione di un contratto.

Deploy: Dopo aver compilato il contratto, la fase finale è la sua pubblicazione su rete compatibile EVM. Utilizzando Ethereum, da Remix è possibile pubblicare un contratto sulla Mainnet Ethereum dalla sezione “Deploy” (Figura 7) selezionando come ambiente “Injected Web3”, utilizzando Metamask in mainnet. Al fine di utilizzare una delle testnet a disposizione per contratti EVM, basterà selezionare la relativa rete su

Metamask prima di effettuare il deploy del contratto; allo stesso modo è possibile selezionare una Blockchain alternativa compatibile con EVM come Tron o BSC. È altresì possibile collegare un full node Ethereum selezionando "Web 3 provider" collegando ad esso un nodo Geth (Ethereum full node). Selezionato l'ambiente, bisogna selezionare l'indirizzo da cui si vuole fare il deploy ed il contratto da pubblicare. Una volta pubblicato il contratto, è possibile interagire con esso direttamente dall'ambiente Remix, dalla sezione "Deployed Contracts".
Selezionando come ambiente "JavaScript VM" è possibile utilizzare l'ambiente di test Remix per testare i contratti in maniera rapida e più deterministica rispetto ad una rete di test pubblica.

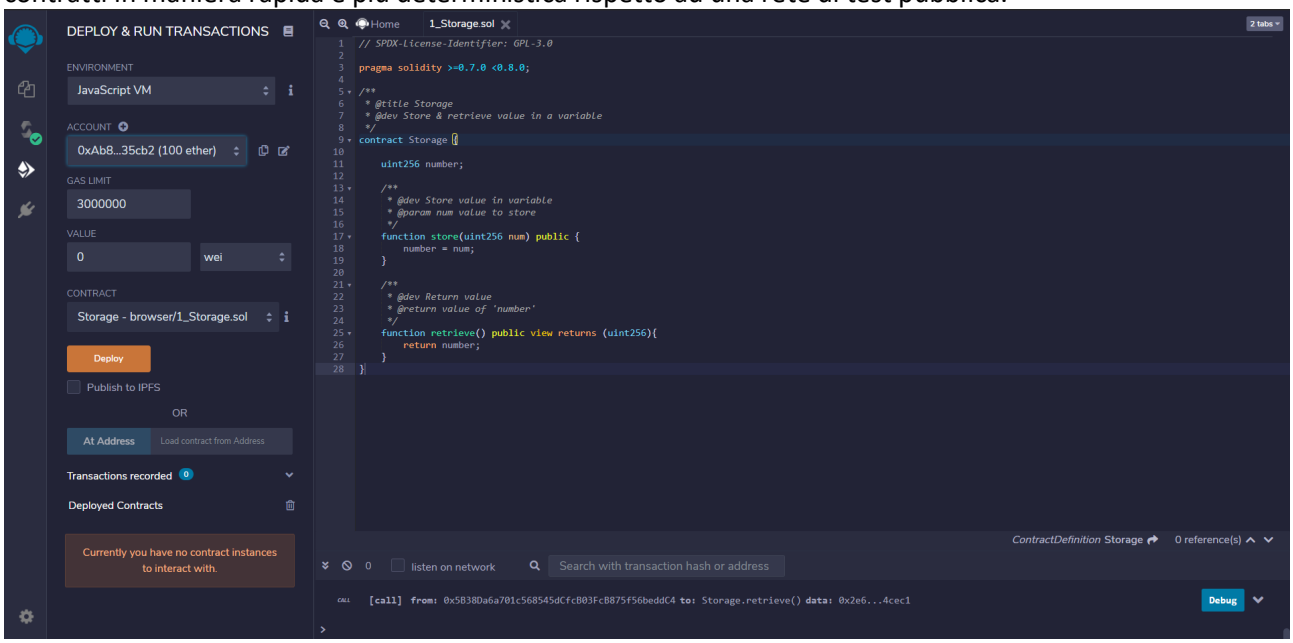

Figura 7. Deploy di un contratto.

Suite di Truffle

La suite di Truffle è un framework completo per lo sviluppo di Smart Contracts Solidity. Essa si divide in quattro moduli:

- Truffle: si tratta di un framework per sviluppare, testare e rilasciare Smart Contracts Solidity su diverse blockchain. In particolare, per Ethereum è possibile depositare contratti sia su mainnet che su testnet, ma anche su altre reti compatibili EVM. È inoltre possibile testare i contratti su una blockchain locale grazie a Ganache.
- Ganache: è una blockchain locale per lo sviluppo rapido di applicazioni distribuite EVM e Corda. Consentendo di sviluppare, distribuire e testare le applicazioni decentralizzate in un ambiente sicuro e deterministico. Ganache UI supporta sia la tecnologia Ethereum che Corda. Una versione Ethereum di ganache è disponibile come strumento da riga di comando: ganache-cli (precedentemente noto come TestRPC).
- Drizzle: è una raccolta di librerie front-end che rendono più semplice la scrittura del front-end delle applicazioni decentralizzate.
- Truffle teams: permette di gestire e monitorare lo stato di salute delle applicazioni blockchain. Esso include: tracciamento e dati Dapp; test automatici continui degli Smart Contract; distribuzioni

automatizzate; monitoraggio di transazioni, stati ed eventi di uno SC distribuito; visualizzazione cronologia della build e dello stato corrente nel flusso di lavoro.

Truffle suite, quindi, è la migliore scelta per la progettazione e lo sviluppo di SC e applicazioni decentralizzate di discreta grandezza, le quali comprendono lo sviluppo di diversi SC e l'interazione fra loro.

Debug

Il più grande pregio degli SC, dal punto di vista degli utilizzatori è che una volta che essi sono stati programmati e rilasciati non possono più in alcun modo essere modificati nella sintassi. Se dal punto di vista della trasparenza e della fiducia, questa è una grande innovazione, non possiamo dire lo stesso dal punto di vista dello sviluppatore che ha, quindi, bisogno di effettuare test approfonditi al fine di azzerare il rischio di malfunzionamento del codice. È quindi estremamente importante rilasciare SC privi di bug ed effettuare test accurati, evitando di rilasciare codice non accuratamente analizzato e testato, soprattutto in luce del fatto che gli SC gestiscono per la maggior parte, prodotti finanziari i quali offrono incentivi maggiori agli attaccanti. Giocano quindi un ruolo essenziale le già citate testnet le quali sono presentate in maniera più approfondita nel paragrafo successivo.

- **Testnet**

Siccome gli Smart Contracts non sono modificabili dopo il rilascio, è di vitale importanza utilizzare una testnet al fine di verificare il corretto funzionamento del codice. Le reti di test sono di due tipi: private e pubbliche. Le testnet private, come Ganache, sono già state presentate in precedenza; esse consentono di rilasciare contratti in un ambiente deterministico. Per testare i contratti in un ambiente più dinamico, sono disponibili diverse reti di test Ethereum, ognuna con delle caratteristiche differenti, esse sono:

- Ropsten: è la prima rete di test ed è quella più simile alla mainnet siccome utilizza la PoW. È possibile fare mining di ETH di test oppure riceverne tramite faucet. È supportata anche in Geth;
- Kovan: utilizza la Proof of Authority (PoA) [4]. Si tratta di un algoritmo di consenso basato sulla reputazione. I nodi validatori vengono selezionati arbitrariamente come entità affidabili e sono quindi limitati. Questo garantisce prestazioni e scalabilità superiori. Gli ETH di test Kovan sono ottenibili solo tramite faucet. Non è supportata in Geth.
- Rinkeby: come Kovan utilizza la PoA. Gli ETH di test Rinkeby sono ottenibili solo tramite faucet. Non è supportata in Geth.
- Goerli: anche essa utilizza la PoA. Gli ETH di test Goerli sono ottenibili solo tramite faucet. È la testnet più stabile ed è supportata in Geth.

In conclusione, se si cerca una rete più simile possibile alla mainnet, si dovrebbe utilizzare la rete Ropsten. Se invece si cerca una rete di test stabile, conviene utilizzare Goerli.

- **Strumenti di analisi dei costi**

Essendo quello dello sviluppo di Smart Contracts un settore relativamente giovane, non esistono strumenti di analisi dei costi delle transazioni. Questo è un punto focale per un'azienda che vuole proporre una soluzione Blockchain e la mancanza di tool di analisi dei costi è un'assenza molto pesante dal punto di vista del risk management. L'unico modo per analizzare i costi attualmente, è quello di utilizzare Metamask su testnet attivando l'opzione "mostra conversione nelle reti di test" e simulando i diversi prezzi del gas in previsione della mancanza di scalabilità di Ethereum.

■ Analisi della scalabilità

Altro importante fattore per la gestione del rischio, è l'analisi della scalabilità degli Smart Contracts. Anche in questo caso non esistono tool al momento che permettano di analizzare la scalabilità in modo efficace. L'unico modo per analizzare la scalabilità degli Smart Contracts prodotti, è utilizzare i test della suite Truffle e le reti di test, procedendo manualmente.

Verifica Etherscan

Completato il deploy degli SC è importante, al fine di garantire la trasparenza ai potenziali utenti del sistema proposto, effettuare la verifica e la conseguente pubblicazione del codice degli SC su Etherscan (https://etherscan.io/). Al fine di effettuare la verifica del contratto è sufficiente recarsi all'indirizzo dello SC su Etherscan, selezionare il tab "Contract" e seguire il procedimento di verifica del codice dello SC.

Sistemi per token

Di particolare interesse per tutti e tre i tipi di applicazioni SC presentati in precedenza è il sistema di token, i quali sono asset digitali che rappresentare una sorta di azioni, biglietti o voucher a seconda del caso, che vengono forniti ai vari attori coinvolti nel progetto come donatori, finanziatori, sviluppatori, utenti, investitori, ecc. Il meccanismo di base dei token è fondamentalmente un database che tiene conto di come vengono distribuiti i token. In altre parole, se n è il numero di token posseduti da A e A ha bisogno di cedere x unità a un secondo attore B, allora lo Smart Contract dovrà eseguire principalmente le seguenti operazioni:

- verificare che x sia minore o uguale ad n per A (in altre parole che A abbia le unità necessarie);
- verificare che B sia disposto e abbia ragione di accettare x da A.

Il codice base per implementare un sistema di token attraverso il linguaggio Serpent è il seguente:

```
def send(to, value):
        if self.storage[msg.sender] >= value:
        self.storage[msg.sender] = self.storage[msg.sender] - value
        self.storage[to] = self.storage[to] + value
```

Teoricamente, i sistemi di token basati su EVM, che fungono da submonete, possono potenzialmente includere un'altra importante caratteristica basata sulla mancanza di meta-monete sulla blockchain di BTC: l'abilità di pagare le commissioni di transazione direttamente in token. Il modo in cui questo potrebbe essere implementato consiste nel far mantenere al contratto un saldo di ETH con cui risarcire quelli che il mittente ha utilizzato per pagare le commissioni. Il contratto, ricaricherà poi il saldo ETH raccogliendo le unità di Token raccolte, rivendendole. Gli utenti avrebbero bisogno di "attivare" i loro accounts con ETH, ma una volta che esso si trova nel wallet, sarebbe riutilizzabile perchè il contratto lo risarcirebbe ad ogni operazione. Al fine di implementare questa soluzione, si ha bisogno di utilizzare un oracolo per ottenere il prezzo di cambio attuale del token con ETH.

Standard ERC 20 (token fungibili)

Sin dai tempi delle Initial Coin Offering (ICO), si è diffuso uno standard per l'implementazione di token su rete Ethereum. Questo standard è stato battezzato ERC20 (Ethereum Request for Comment). Per appartenere a questo standard, un token deve implementare alcune funzioni che permettono alle altre applicazioni di riconoscere il token. Le funzioni sono le seguenti:

- totalSupply(): restituisce il numero di token coniati fino al momento dell'invocazione della funzione;
- balanceOf(address owner): restituisce il numero di token che l'account possiede;

- transfer(address to, uint256 amount): trasferisce il numero di token passato come parametro (variabile amount), dall'account che richiama la funzione all'indirizzo passato come parametro (variabile to);
- approve(address spender, uint256 amount): permette ad un account terzo, passato come parametro (variabile spender) di utilizzare un numero di token (variabile amount) per conto dell'utilizzatore della funzione. Questa funzione è utile nel caso in cui un contratto abbia bisogno di effettuare operazioni con i token dell'indirizzo che lo utilizza. Lo spender quindi, dovrebbe essere una risorsa di cui ci si fida in quanto può utilizzare le monete digitali del wallet che effettua l'approve;
- transferFrom(address from, address to, uint256 amount): permette di inviare I token da un indirizzo ad un altro, specificati nei parametri. Questa funzione può essere utilizzata solo se l'indirizzo "from" ha precedentemente effettuato un approve in favore dell'account che sta richiamando questa funzione.

Oltre alle citate funzioni, ne possono essere implementate altre personalizzate a seconda dei bisogni dello sviluppatore e dei requisiti del progetto. Le funzioni più utilizzate e non presenti nello standard sono quelli di mint e burn, le quali permettono di coniare nuove monete o bruciare una parte di quelle in circolazione (solitamente solo dal proprio account).

Standard ERC721 (token non fungibili)

Al fine di ottenere beni digitali unici, nasce una estensione dei token ERC20, l'ERC721. In questo standard, si conia un token alla volta, fornendogli un numero identificativo (ID). In questo modo, ogni token diventa unico ed ha caratteristiche proprie. Un generico caso d'uso è l'implementazione di token che rappresentano oggetti collezionabili. Ogni oggetto ha una rarità propria e determinate caratteristiche. Siccome, come detto in precedenza, conservare dati molto lunghi in BC è molto costoso, è di uso comune conservare i dati delle caratteristiche del token su una struttura dati diversa dalla BC e mantenere in essa solo un riferimento a questi dati. Una tecnologia che si sposa bene con questo approccio è l'IPFS (InterPlanetary File System) la quale consente di effettuare lo storage di dati multimediali su nodi decentralizzati; quando si depositano i dati di un file, l'IPFS ne calcola l'hash il quale viene utilizzato come riferimento. Nel caso degli ERC721, è di comune usanza inserire il riferimento (l'hash) al file in BC.

Token di governance

Recentemente si è diffuso un approccio che permette agli utenti che partecipano al progetto mantenendo token di sceglierne la direzione strategica e di sviluppo. Questo tipo di token vengono chiamati token di governance e sono una estensione dei token ERC20 a cui vengono aggiunte funzioni di voting per proposte che vengonoinserite in un contratto di governance. I voti vengono pesati in base a quanti token l'utente possiede. Ciò permette contemporaneamente di non incentivare la vendita dei token, magari guadagnati dagli utenti attraverso la DeFi la quale ha metodi molto inflazionistici, evitando cali di prezzo e di soddisfare i bisogni degli utenti.

3.3 Analisi tecniche migliori piattaforme blockchain per capitalizzazioni

Dopo aver approfondito dal lato tecnico le maggiori rivoluzioni di questo ambito (Bitcoin per la nascita delle monete digitali basate su BC ed Ethereum per la nascita del concetto di SC), analizziamo lo stato dell'arte dei progetti BC (aggiornati all'anno 2020) presentandone i motivi del successo, l'utilità, le caratteristiche tecniche e gli algoritmi che sono implementati alla base di essi. Algoritmi che verranno approfonditi nella prossima attività. La lista è ordinata per capitalizzazione e può facilmente variare nel corso del tempo siccome il settore è in piena esplosione e quindi in continua trasformazione. Alcuni progetti sono menzionati nell'elenco per la alta capitalizzazione, altri per la rivoluzione che hanno portato nel settore. Al fine evitare ridondanze, non sono stati riportati protocolli troppo simili ad altri già esistenti e più capitalizzati.

1 Bitcoin (BTC)

BTC è la prima moneta digitale basata su BC concepita e, da quando è nata e fino ad oggi, è la più grande per capitalizzazione. Essa nasce come moneta digitale per implementare pagamenti peer-to-peer sicuri, ma con il passare del tempo si è trasformata in asset digitale da investimento. Fu lanciata nel 2009 da Satoshi Nakamoto, lo pseudonimo dell'anonimo gruppo o persona che ha concepito e sviluppato il progetto. Nakamoto, nel whitepaper di BTC promette di eliminare il bisogno di una terza parte fidata che contabilizzi i pagamenti, assicurando transazioni pseudo-anonime. Ad oggi Bitcoin è molto di più. Potrebbe, in futuro essere il nuovo Sistema monetario standard e ad oggi è considerato l'oro digitale siccome per alcuni aspetti è simile all'oro: è scarso, viene generato attraverso un lavoro e la fornitura è limitata. In altre parole, il network ha un numero fisso di monete coniabili dal mining e, similmente all'oro, vengono spese risorse (energia elettrica) per la coniazione. La coniazione avviene ad ogni rilascio di un blocco in BC e ogni quattro anni la ricompensa per blocco viene dimezzata. Ad oggi, sono circa 18.5 milioni le monete in circolazione ed è possibile ottenere 6.25 Bitcoin per ogni blocco generato. A vantaggio rispetto all'oro, Bitcoin è altamente divisibile, facilmente trasportabile e scambiabile, inoltre nell'ultimo anno grazie alla DeFi può essere collateralizzato al fine di generare altre monete digitali. Nonostante non sia il sistema di pagamento perfetto (il network BTC riesce a processare solo sette transazioni al secondo), essendo la moneta digitale più conosciuta e con il network più sicuro, gli investitori si approcciano a questo mercato necessariamente passando da BTC. Per questo motivo, la popolarità e l'utilizzo di BTC al giorno d'oggi sembra inscalfibile e diventa difficile immaginare che un'altra moneta digitale possa superarlo per capitalizzazione.

Panoramica caratteristiche

- Bitcoin per blocco: 6.25 al momento;
- Monete circolanti: 18.5 milioni al momento;
- Monete coniabili: 21 milioni;
- Tempo rilascio blocco: 10 minuti;
- Transazioni al secondo: 7;
- Consenso: Proof of Work;
- Algoritmo di mining: SHA256.

Considerazioni finali

In conclusione quello che è diventato BTC, probabilmente si discosta da quello che Satoshi Nakamoto voleva proporre nel 2009. Il più grande vantaggio di BTC è quello di essere nato per primo ed aver acquisito popolarità e solidità del network e di prezzo nel tempo grazie alla forte decentralizzazione del possesso delle monete, trasformando Bitcoin in uno standard ed un prodotto finanziario simile all'oro più che un sistema di pagamento peer-to-peer. Di fatti, molti sostenitori del primo BTC hanno creato un fork chiamato Bitcoin Satoshi Vision, il quale ha l'obiettivo di fare di BTC il sistema di transazioni peer-to-peer perfetto che aveva immaginato Satoshi Nakamoto. Di contro, il network Bitcoin è caratterizzato da una forte lentezza e alto

costo di processamento delle transazioni e richiede ormai attrezzature specializzate per effettuare il mining. Attrezzatura estremamente dispendiosa in termini di energia elettrica, il che rende la PoW di BTC molto dispendiosa anche in termini di emissioni di Co^2. Per risolvere i problemi dei costi di transazione, è in fase di sviluppo la tecnologia Lightning Network, una tecnologia che fa utilizzo degli SC, al fine di ottenere una infrastruttura su un livello superiore della BC in modo da "scaricare" le transazioni su di essa, rendendole più economiche e scalabili rispetto all'infrastruttura sottostante.

2 Ethereum (ETH)

L'Ether è la moneta digitale del network Ethereum. Questo network permette agli utenti di sviluppare applicazioni decentralizzate (dApps) le quali implementano come backend gli SC. Essi sono indipendenti dalle dApp e hanno la caratteristica di far automaticamente rispettare le clausole a chi partecipa al contratto. Ethereum viene concepito da Vitalik Buterin nel 2013 e lanciato nel 2015. Gli ETH non hanno un limite di monete coniabili e vengono coniate distribuendo ETH ogni volta che viene validato un blocco al miner del blocco stesso. La ricompensa originale nel 2015 era di 5 ETH per blocco, che in seguito è scesa a 3 ETH alla fine del 2017 e poi a 2 ETH all'inizio del 2019. Il tempo medio necessario per estrarre un blocco Ethereum è di circa 13-15 secondi. Ethereum utilizza la PoW come algoritmo di consenso. In particolare l'algoritmo di mining è Ethash, un algoritmo teoricamente resistente agli ASIC, evoluzione di Dagger Hashimoto e nella quale è prevista anche l'esecuzione di codice EVM. Nonostante Ethereum sia il primo ecosistema ad introdurre nel settore il concetto di SC, il problema di scalabilità è sempre più evidente ed al momento della scrittura, i costi di transazione di Ethereum sono arrivati a prezzi esorbitanti a causa dell'esplosione della DeFi. Al fine di correre ai ripari aumentando la scalabilità di Ethereum, gli sviluppatori sono in procinto di migrare Ethereum ad Ethereum 2.0 che utilizza come algoritmo di consenso la Proof of Stake (PoS). La PoS dovrebbe rendere Ethereum 2.0 più scalabile rispetto alla sua precedente versione. A causa del citato problema di scalabilità e della lentezza di Ethereum al passaggio a PoS, stanno prendendo sempre più piede le BC alternative ad Ethereum più scalabili e compatibili con EVM come la BSC.

Panoramica Caratteristiche

- Ethereum per blocco: 2+fee transazioni al momento;
- Monete circolanti: 113.7 milioni;
- Monete coniabili: nessun limite;
- Tempo rilascio blocco: 15 secondi circa;
- Transazioni al secondo: 20;
- Consenso: Proof of Work;
- Algoritmo di mining: Ethash.

Considerazioni finali

Come BTC, Ethereum è poco ottimizzato e scalabile al momento, ma è stata la prima piattaforma ad introdurre gli SC ed è tuttora la più famosa, per questo motivo i volumi e i progetti più importanti si concentrano su di essa. Anche in questo caso e ancora meno di BTC, Ethereum non più essere definito un sistema di pagamento peer-to-peer, ma è molto di più siccome offre un ecosistema che non ha limiti in quanto a casi d'uso. I contro di questa piattaforma sono, come visto, la poca scalabilità e, dal lato dello store of value, il fatto che non ci sia limite agli ETH coniabili, cosa che rende ETH una moneta più inflazionaria di BTC. I costi di transazione, se si considera solo lo scambio di monete digitali, sono di gran lunga più economici di quelli di Bitcoin.

3 Ripple (XRP)

XRP è la moneta digitale utilizzata sulla piattaforma di pagamento chiamata RippleNet, la quale è implementata come un un libro mastro distribuito chiamato XRP Ledger. RippleNet è gestito da una società chiamata Ripple, XRP Ledger è open-source e non è basato su blockchain, ma sul database distribuito precedentemente menzionato. La piattaforma di pagamento RippleNet è un sistema di regolamento lordo in tempo reale (RTGS) che mira a consentire transazioni monetarie istantanee a livello globale ed è utilizzato anche da alcune banche e istituzioni finanziarie come Santander e American Express. Sebbene XRP sia la moneta digitale originaria di XRP Ledger, è possibile utilizzare qualsiasi valuta per effettuare transazioni sulla piattaforma. Mentre l'idea alla base della piattaforma di pagamento Ripple è stata espressa per la prima volta nel 2004 da Ryan Fugger, è stato solo quando Jed McCaleb e Chris Larson hanno rilevato il progetto nel 2012 che Ripple ha iniziato a essere sviluppato (all'epoca si chiamava anche OpenCoin). XRP è stato concepito da Ripple per essere un'alternativa rapida, meno costosa e più scalabile sia ad altre risorse digitali che alle piattaforme di pagamento monetario esistenti come SWIFT. Il libro mastro di RippleNet è gestito dalla community XRP, con la società Ripple come membro attivo. Il registro XRP elabora le transazioni all'incirca ogni 3-5 secondi o ogni volta che i nodi di convalida indipendenti giungono a un consenso attraverso un low-latency Byzantine agreement protocol [11] [5]. Il consenso viene raggiunto sia sull'ordine che sulla validità delle transazioni XRP. Chiunque può essere un validatore e l'elenco è attualmente composto da Ripple insieme a università, istituzioni finanziarie e altri importanti enti.

Panoramica caratteristiche

- Monete circolanti: circa 45 miliardi;
- Monete coniabili: 100 miliardi pre-coniati;
- Transazioni al secondo: 1500 costante, ma può arrivare fino a 50000;

Considerazioni finali

XRP è forse la moneta digitale fra le più capitalizzate che più si avvicina al concetto di pagamento peer-to-peer ottenendo un'altissima velocità di transazioni al secondo e l'immunità all'attacco 51%. Questo, però viene ottenuto a discapito della poca decentralizzazione della moneta e della rete. Nonostante venga definita decentralizzata, è ovvio che l'azienda Ripple ne controlli il ciclo di vita e spesso e volentieri, in passato, ne ha controllato il prezzo, vendendo a scaglioni le proprie riserve. Ripple è stata altresì accusata dalla Securities and Exchange Commission (SEC) di aver ceduto gli XRP senza averli considerati come titoli dell'azienda Ripple (vendite che secondo la SEC dovevano essere registrate come vendite di titoli).

4 Tether USD (USDT)

Tether USD, precedentemente chiamata Realcoin, è una stablecoin legata al valore del dollaro americano emessa dall'azienda situata nelle isole Vergini britanniche Tether Limited. Il suo valore ha sempre fluttuato tra i 0.96$ ed I 1.06$. Un USDT viene rilasciato solo quando c'è un dollaro americano a coprirne il valore nelle riserve dell'azienda Tether Limited[12]. Il ciclo di vita di Tether può essere rappresentato dal diagramma in figura 8.

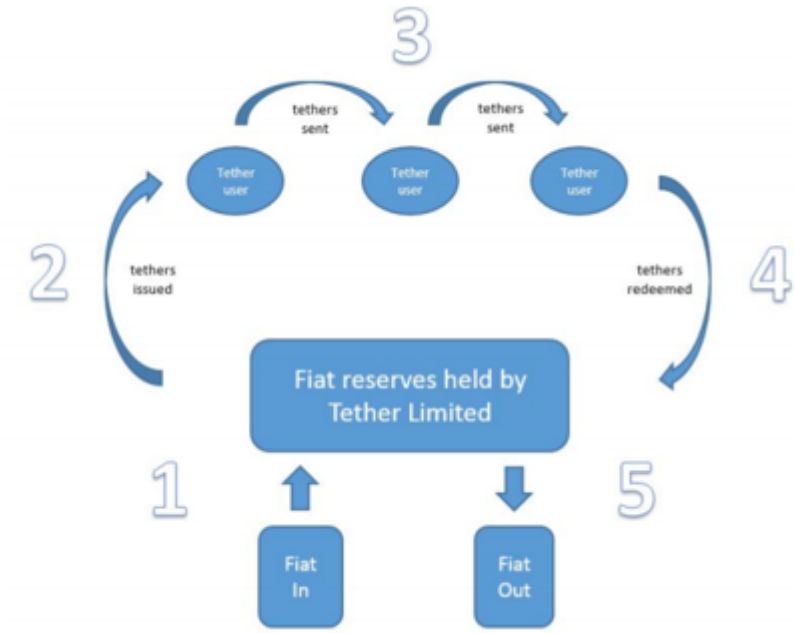

Figura 8: ciclo di vita della stablecoin USDT.

Dal diagramma si nota come quando un utente acquisisce USDT (Figura 8, punto 1), e quindi inserisce valuta fiat nelle riserve Tether, l'azienda emette USDT (Figura 8, punto 2). Quando un utente vende (Figura 8, punto 5), rimuove valuta fiat dalle reserve Tether, e l'azienda rimuove USDT dal mercato (Figura 8, punto 4). USDT è basata sulla Piattaforma Omni, ma è presente anche su altre BC e attualmente è la moneta digitale che movimenta più volumi, questo perché viene utilizzata dai trader per gli scambi con le monete digitali più speculative. Esistono anche altre stablecoin di Tether legate ad altre valute come l'euro e lo yuan, ma quella legata al dollaro americano è la più utilizzata.

Panoramica caratteristiche

Monete circolanti: circa 20 miliardi;
Monete coniabili: nessun limite;
Rilascio: 1 USDT per 1 USD nelle riserve Tether Limited;
Transazioni al secondo: Dipendente dalla Blockchain in uso;

Considerazioni finali

Nonostante USDT abbia una storia molto controversa, è ancora la stablecoin più utilizzata nel mercato. Negli anni sono stati spesso sollevati dubbi sul fatto che non sia molto chiaro se Tether Limited abbia i fondi necessari a coprire totalmente le riserve di USDT. Inoltre Tether Limited ha rapporti stretti con Bitfinex, la quale è stata accusata di aver manipolato il prezzo di BTC nel 2017 proprio con emissioni che potevano risultare scoperte di USDT. Tutte le accuse mosse a Bitfinex e a Tether non sono però, ad oggi, state dimostrate.

5 Litecoin (LTC)

Stando alle parole di Charlie Lee, founder di Litecoin, esso è nato per essere l'argento nel mondo delle monete digitali, dove BTC è l'oro. Ciò è stato ottenuto nel 2011 dagli sviluppatori, riutilizzando il codice sorgente di BTC e aumentando le unità massime coniabili ad 84 milioni. Oltre questa fondamentale differenza, il team ha

migliorato il troughput delle transazioni, cambiato l'algoritmo di mining da SHA256 a Scrypt, aumentato il tempo di validazione del blocco e allungato il tempo di halving.

Panoramica caratteristiche

- Litecoin per blocco: 12.5 al momento;
- Monete circolanti: circa 66 milioni al momento;
- Monete coniabili: 84 milioni;
- Tempo rilascio blocco: 2.5 minuti;
- Transazioni al secondo: 56;
- Consenso: Proof of work;
- Algoritmo di mining: Scrypt.

Considerazioni finali

Non si può dire molto su Litecoin oltre al fatto che sia definito "l'argento rispetto all'oro del Bitcoin" dal suo creatore. Il progetto, dalla sua nascita, non ha apportato notevoli migliorie e i suoi unici vantaggi rimangono l'alto troughput delle transazioni, anche se al momento la rete sembra piuttosto congestionata, costringendo gli utenti ad aspettare ore per una transazione e il suo algoritmo di mining, che utilizza la memoria per le computazioni e rende il mining di Litecoin difficile da risolvere per gli ASIC. Oltre alla poca cura al progetto, è importante segnalare che il suo founder ha spesso e volentieri venduto le proprie riserve di Litecoin durante gli anni, generando cali di prezzo anche piuttosto gravi. Nonostante questo, Litecoin è una delle prime monete digitali nate e per questo motivo rimane ancora una delle monete digitali più famose ed utilizzate.

6 Bitcoin Cash (BCH)

Bitcoin cash è la moneta digitale che si è creata dall'hard fork di Bitcoin nell'agosto 2017. In quel periodo, la lentezza delle transazioni di BTC iniziava a pesare, e diverse migliorie erano state proposte al fine di aumentarne la velocità. Una delle soluzioni proposte era di aumentare la capacità massima dei blocchi da 1 MB a 8 MB, mentre chi voleva trattare BTC più come un prodotto da investimento che come una moneta digitale transazionale era orientato all'adozione di BIP91 (Bitcoin Improvement Proposal 91) che implementava SegWit, protocollo che aumentava la scalabilità di BTC senza cambiare la grandezza dei blocchi. Il risultato è stato che chi era favorevole all'ingrandimento dei blocchi utilizzava il client con questa modifica, mentre chi era sfavorevole, utilizzava il client che aveva adottato BIP91. Per questo motivo si sono create due blockchain che avevano la stessa storia solo fino al momento della divisione, dopodichè sono diventate indipendenti. Attualmente la grandezza dei blocchi di Bitcoin Cash è aumentata ancora, raggiungendo i 32 MB.

Panoramica caratteristiche

- Bitcoin Cash per blocco: 6.25 al momento;
- Monete circolanti: circa 1.5 milioni al momento;
- Monete coniabili: 21 milioni;
- Tempo rilascio blocco: 10 minuti;
- Transazioni al secondo: 60;
- Consenso: Proof of work;

- Algoritmo di mining: SHA256.

Considerazioni finali

Bicoin Cash cerca di risolvere il problema della scalabilità di BTC incrementando la capacità dei blocchi da 1 a 32 MB: il limite basso della grandezza dei blocchi di Bitcoin, lo rende un asset poco adatto ad un protocollo transazionale, anche se ha comunque introdotto SegWit, il quale ha portato con sé un nuovo parametro chiamato block weight, che in qualche modo rappresenta un escamotage e permette ai blocchi di pesare di fatto più di 1 MB, fino a un massimo di 4. La soluzione di Bitcoin Cash ha un problema e cioè che la sua blockchain alla lunga peserà, in termini di Gigabyte, molto di più rispetto a quella di BTC. Il troughput delle transazioni e del broadcast della BC agli altri nodi aumenta e si ha bisogno di connessioni internet più veloci, questo fa centralizzare di più il mining verso miner di paesi più sviluppati tecnologicamente. Inoltre, facendo più di un passo nel futuro, ricordiamo che i miner sono incentivati a partecipare al network in cambio di Bitcoin/Bitcoin Cash derivati dalla ricompensa di blocco e dalle fee del network e che la ricompensa del blocco si dimezza ogni quattro anni fino a tendere a zero. Quando le ricompense di BTC e BCH saranno tutte in circolo, l'unico reward dei miner saranno i costi delle transazioni. Quando il network si congestiona, le commissioni di BTC aumentano e questo garantisce un buon ritorno ai miner. Al contrario, le transazioni di Bitcoin Cash sono più economiche anche se c'è congestione e i miner BCH hanno ritorni più bassi rispetto a quelli di BTC. È per questo motivo che la maggior parte dei miner, preferisce di più fare mining sulla catena di BTC che su quella di Bitcoin Cash. Anche alla luce del fatto che BTC ormai sia visto più come un asset da investimento che una moneta transazionale.

7 Chainlink (LINK)

Chainlink è un servizio di oracoli decentralizzati [13]. Siccome gli SC, come visto in precedenza, sono ciechi a dati esterni dalla BC, senza un oracolo, per gli SC è impossibile prendere decisioni basate su eventi esterni. Un caso d'uso potrebbe essere quello di codificare uno SC che tokenizza il raccolto di un'azienda agricola. Nel caso in cui sia previsto un temporale che potrebbe distruggere il raccolto, lo SC vende il token. Al contrario, se il tempo è sereno, mantiene il token. In questo modo, l'agricoltore, può economicamente mantenere al sicuro quello che ha prodotto durante l'anno. Chainlink permette quindi l'utilizzo di API esterne da parte degli sviluppatori di SC. Il token e la piattaforma sono sviluppati su BC Ethereum. I partecipanti al network di Chainlink sono incentivati attraverso i rewards a fornire i dati esterni agli SC che li richiedono.

Panoramica caratteristiche

- Monete circolanti: circa 400 milioni al momento;
- Monete circolanti massime: 1 miliardo;
- Transazioni al secondo: vedi Ethereum;
- Consenso: Sistema reputazione basato sui dati forniti;

Considerazioni finali

Chainlink è un progetto interessante e fondamentale, in quanto sopperisce alla cecità degli SC ai dati esterni permettendo di sviluppare progetti a 360 gradi in ambito BC. Con la nascita della DeFi, Chainlink ha acquisito un posto fondamentale fra i progetti BC, in quanto la maggior parte dei progetti DeFi ha bisogno di diversi

oracoli sicuri e affidabili per funzionare correttamente e non permettere attacchi malevoli che mirano alla manipolazione dei prezzi al fine di trarne profitto.

8 Cardano (ADA)

Cardano è una piattaforma per SC e applicazioni decentralizzate che utilizza come algoritmo di consenso per il suo token ADA, la Proof of Stake (PoS). ADA è anche una moneta di governance in quanto coloro che la detengono hanno il diritto di votare su qualsiasi modifica proposta al software. Cardano è una delle più grandi piattaforme ad aver implementato con successo la PoS.

Panoramica caratteristiche

- Cardano per blocco: 3506 al momento;
- Monete circolanti: circa 51 miliardi al momento;
- Monete coniabili: 45 miliardi;
- Tempo rilascio blocco: 20 secondi al momento;
- Transazioni al secondo: 1000, scalabili teoricamente fino ad un milione;
- Consenso: Proof of stake.

Considerazioni finali

Cardano è uno dei progetti più seri in circolazione, in quanto è sostenuto dalla ricerca accademica. Prima di svilupparlo, è stato scritto un articolo scientifico peer reviewed [6] che ne descrive le caratteristiche. Inoltre la PoS garantisce un mining sostenibile, economico e scalabile.

9 Binance coin (BNB)

Binance coin è la moneta di uno degli exchange centralizzati più diffuso: Binance [14]. Nato come token ERC20 su rete Ethereum e poi migrato su Binance Chain e Binance Smart Chain (BSC), quest'ultima è molto simile alla blockchain di Ethereum in quanto è compatibile con EVM e consente quindi lo sviluppo di applicazioni decentralizzate anche tramite linguaggio Solidity. Binance coin ha diverse finalità: la più utilizzata è quella per il pagamento delle fee per gli scambi sull'exchange; se i trader decidono di pagare le commissioni con BnB, ottengono uno sconto. Altre finalità interessanti sono lo staking sul launchpool, dove si possono ottenere rewards in monete digitali appena nate e affiliate a Binance e il pagamento del GAS per gli SC su BSC. Ogni trimestre vengono bruciati BnB da Binance in base ai volumi di scambi avvenuti sull'exchange.

Panoramica caratteristiche

- BnB per blocco: 0+commissioni transazioni;
- Monete circolanti: circa 144 milioni al momento;
- Tempo rilascio blocco: 3 secondi al momento;
- Transazioni al secondo: 2000;
- Consenso: Tendermint Byzantine fault tolerance.

Considerazioni finali

Dopo la migrazione su Binance chain e BSC, BnB diventa una seria competitor di Ethereum, in quanto è compatibile con EVM ma scalabile, con transazioni veloci ed economiche. Essendo tutti i BnB portati in

circolazione, l'operazione di burning trimestrale è un'operazione intelligente che garantisce scarsità e ottima attenzione verso questa moneta digitale da parte dei trader. Senza contare tutte le operazioni di Binance che invogliano l'utente a mantenere il possesso dei BNB. L'unico difetto di questa moneta digitale sembra essere la poca decentralizzazione in quanto essa è in ogni caso dipendente dalle scelte della piattaforma Binance e da un sistema di consenso che comprende pochi nodi nel caso della BSC.

10 Monero (XRM)

Monero è stata lanciata nel 2014. La particolarità di questa moneta digitale risiede nel fatto che si tratta di una privacy-coin. La BC di Monero, grazie all'uso di tecniche avanzate di crittografia, riesce ad offuscare le transazioni e allo stesso tempo validarle[15]. Nessuno può quindi analizzare I partecipanti ad una transazione Monero e il numero di monete scambiate a meno di complesse analisi forensi [7].

Panoramica caratteristiche

- Monero per blocco: 1.27 al momento;
- Monete circolanti: circa 18 milioni al momento;
- Monete coniabili: non precisato;
- Tempo rilascio blocco: 2 secondi;
- Transazioni al secondo: 56;
- Consenso: Proof of work;
- Algoritmo di mining: Cryptonight.

Considerazioni finali

L'offuscamento delle transazioni garantisce resistenza alla censura e alle penalizzazioni di analisi esterne sugli indirizzi. Per questo motivo è una moneta che rende partecipi anche transazioni illegali. Il suo algoritmo di consenso CryptoNight è ASIC e GPU resistant, ciò rende il mining di Monero molto decentralizzato siccome può essere eseguito solo dalle CPU. Essendo una privacy-coin il pericolo di subire pesanti attacchi da parte della legislazione è alto e gli exchange potrebbero essere costretti in futuro ad effettuare il delisting delle privacy-coin.

11 Wrapped Bitcoin (WBTC)

Una menzione particolare meritano le monete digitali "wrapped". Un esempio è Wrapped Bitcoin, è il token ERC20 che rappresenta BTC su BC Ethereum. Sulla scia di questo token, sono nate tante altre monete "wrapped" su qualsiasi BC che concedesse la creazione di token [16]. È supportato da BTC con un rapporto 1: 1 tramite una rete di commercianti e custodi monitorati automaticamente, assicurando che il suo prezzo sia ancorato a BTC in ogni momento e consenta agli utenti di trasferire liquidità tra le reti BTC e ETH in modo decentralizzato ed autonomo. In altre parole, il meccanismo è simile a quello di USDT: se un attore vuole ricevere un WBTC in cambio di un BTC non dovrà fare altro che depositare un BTC nelle riserve di WBTC ed in cambio riceverà un WBTC su rete Ethereum. Allo stesso modo, per ricevere il BTC depositato in precedenza, l'attore dovrà restituire il token ricevuto che verrà quindi bruciato.

Panoramica caratteristiche

- Monete circolanti: circa 118000 al momento;
- Monete coniabili: 21 milioni;
- Transazioni al secondo: vedi Ethereum;

Considerazioni finali

La tokenizzazione consente a BTC di essere completamente integrato nell'ecosistema Ethereum permettendo scambi con costi ridotti e decentralizzati, servizi di prestito crittografico, mercati di previsione e altre applicazioni di finanza decentralizzata (DeFi) abilitate per ERC-20 mantenendo il possesso dell'asset.

12 Tron (TRX)

L'ecosistema Tron è stato pensato al fine di costruire un sistema di intrattenimento decentralizzato consentendo ai creatori di contenuti di ottenere il pieno controllo sui propri progetti eliminando gli intermediari [17]. La piattaforma può contenere musica, film, immagini, giochi, ecc. Ogni content creator viene incentivato a pubblicare sulla piattaforma con i compensi in TRX, la moneta digitale di Tron.

Panoramica caratteristiche

- Trx per blocco: 32 al momento;
- Monete circolanti: circa 71 miliardi al momento;
- Monete coniabili: non precisato, al momento circa 100 miliardi;
- Tempo rilascio blocco: 3 secondi;
- Transazioni al secondo: 2000, teoricamente scalabile fino a 10000;
- Consenso: Delegated proof of stake.

Considerazioni finali

Tron è un progetto molto interessante sia tecnicamente, in quanto la sua BC riesce ad ottenere buone prestazioni, sia in termini di utilità in quanto una piattaforma libera da censure che permette ai creatori di contenuti di mantenere la proprietà sui dati ed essere compensati per ciò che creano è qualcosa di estremamente utile ed uno dei casi d'uso fondamentali della tecnologia BC.

13 Neo (NEO)

NEO è stato spesso definito come la versione cinese di Ethereum. Anche esso permette lo sviluppo di dApp e SC. Il network NEO viene costantemente aggiornato ed ha come token nativi il NEO ed il GAS. Come Ethereum, il GAS viene utilizzato per pagare le commissioni sul network, con la differenza che il GAS in NEO, è una moneta digitale a parte con un proprio valore. Quando si hanno dei NEO nel portafoglio, vengono automaticamente generati dei GAS in proporzione ad essi.

Panoramica caratteristiche

- NEO per blocco: i NEO sono stati generati al lancio della blockchain e vengono distribuiti annualmente, il 50% della distribuzione viene venduto, l'altro 50% viene diviso fra gli sviluppatori e NEO Cuncil;
- Monete circolanti: circa 70.5 milioni al momento;

- Monete coniabili: 100 milioni;
- Tempo rilascio blocco: 15 secondi;
- Transazioni al secondo: 1000;
- Consenso: Delegated Byzantine fault tolerance.

Considerazioni finali

NEO è un buon progetto, con idee chiare, buone prestazioni e transazioni economiche. La parte di NEO destinata al Council viene investita in altri progetti BC su piattaforma NEO. Le transazioni, al momento possono essere eseguite anche a costo zero se non superano una certa soglia e nel caso si vogliano velocizzare quelle più consistenti è possibile utilizzare il GAS accumulato. I difetti di NEO sono la poca decentralizzazione e la non divisibilità.

14 Makerdao (MKR, DAI)

Makerdao ha coniato due monete digitali su piattaforma Ethereum: Maker che è il token di governance di Makerdao e DAI, una stablecoin legata al dollaro americano [18]. La particolarità di Dai è che è collateralizzata da asset digitali tramite SC. Ogni utente può depositare del collaterale a garanzia al fine di coniare DAI. La collateralizzazione garantisce che ogni DAI sia coperto da diverse altre monete digitali depositate nello SC e chi decide di collateralizzare e coniare DAI ha bisogno di mantenere un certo limite di coniazione entro il quale le monete digitali depositate vengono liquidate e deve quindi fare attenzione alla volatilità del collaterale. La stabilità di prezzo di DAI viene gestita dalla community, in particolare se il prezzo di DAI sale, essi vengono utilizzati per comprare Maker che viene poi bruciato, al contrario, se il prezzo del DAI scende, viene acquistato con del Maker appena coniato.

Panoramica caratteristiche

- Maker circolanti: circa 1 milione;
- DAI circolanti: circa un miliardo;
- Transazioni al secondo, consenso ed algoritmo di mining: Vedi Ethereum;

Considerazioni finali

Si può dire che Makerdao sia la piattaforma che ha dato via all'esplosione della DeFi. Gli utenti che vogliono mantenere Maker o altri asset digitali, possono mantenerli depositandoli come collaterale per coniare DAI ed utilizzare questi ultimi su applicazioni decentralizzate create dagli utenti o da Makerdao stessa dopo averli coniati, guadagnando interessi, sfruttando i movimenti di prezzo di DAI, o utilizzandoli per fare acquisti senza effettivamente vendere gli asset posseduti che possono in futuro essere recuperati restituiendo i DAI coniati in precedenza.

15 AAVE

Aave è un protocollo di DeFi per borrower e lenders su BC Ethereum [19]. Gli utenti possono depositare le proprie monete digitali al fine di guadagnare interessi sui depositi. D'altro lato, altri utenti possono prendere in prestito le monete digitali garantendo del collaterale e pagando degli interessi una volta restituito il prestito. Al momento Aave è uno dei protocolli di borrow and lend con più monete digitali offerte. Il token

AAVE è un token di governance che permette di utilizzare il protocollo con sconti sulle commissioni e può anche essere mantenuto in staking al fine di rendere il protocollo più sicuro ricevendo interessi sull'importo bloccato.

Panoramica caratteristiche

- AAVE circolanti: circa 12 milioni;
- Emissione: 400 AAVE al giorno agli stakers;
- Monete coniabili: 16 milioni;
- Transazioni al secondo, consenso ed algoritmo di mining: Vedi Ethereum;

Considerazioni finali

È importante menzionare AAVE non tanto per il suo protocollo, in quanto simile concettualmente a Makerdao, quanto per alcune importanti caratteristiche che la piattaforma offre. La più interessante è quella di poter effettuare Flash Loans. I Flash Loans sono prestiti senza collaterale, a patto che essi vengano restituiti nello stesso blocco nel quale è stata effettuata la prima transazione e con una commissione dello 0.09%; se i requisiti appena menzionati non vengono rispettati la transazione viene invertita. È quindi possibile in questo modo eseguire arbitraggi con grosse somme di monete digitali senza realmente possederle, effettuare scambi di collaterale ed autoliquidazioni. Attraverso i Flash Loans è purtroppo anche possibile manipolare prezzi ed oracoli al fine di trarne profitto a danno dei protocolli [8]. Questa è un'azione che in diversi casi è stata individuata come exploit, ma che non è ancora ben definita seppur sia una azione che va a danneggiare il protocollo. È un requisito fondamentale, quindi, per ogni applicazione decentralizzata che abbia bisogno di fare riferimento ad un oracolo per controllare i prezzi delle monete digitali e di conseguenza effettuare azioni, tenere conto di questo pericolo.

16 IOTA (IOTA)

Anche Iota, come alcune delle monete digitali menzionate, non utilizza una BC come network. Esso utilizza un grafo aciclico diretto chiamato "Tangle" [20] come struttura dati ed è un distributed ledger per l'Internet of Things (IoT). Il Tangle è a prova di sistemi quantici siccome ogni mittente di una transazione è anche miner, difatti, non esistono commissioni per queste ultime. La validazione delle transazioni è semplice: se un dispositivo ha bisogno di effettuare una transazione, quello che deve fare è validarne due. In questo modo ogni transazione viene matematicamente coperta. Per evitare l'inondazione malevola di transazioni, ogni nodo, al fine di validare una transazione, deve completare una leggera PoW. Siccome sono stati emessi 2.779.530.283.277.761 di IOTA, il valore di riferimento è il milione di IOTA (MIOTA). Il consenso viene raggiunto grazie ad un nodo coordinatore.

Panoramica caratteristiche

- Monete circolanti: 2.779.530.283 MIOTA;
- Monete coniabili: 2.779.530.283 MIOTA;
- Transazioni al secondo: teoricamente, non c'è limite sul throughput delle transazioni IOTA;

Considerazioni finali

IOTA è una moneta digitale molto particolare, in quanto non utilizza una BC. Questo rende il network scalabile, veloce ed economico. Anche IOTA però è poco decentralizzata, a causa del nodo validatore operato dalla IOTA foundation.

17 Uniswap (UNI)

Uniswap è un exchange decentralizzato (Dex) su rete Ethereum. In questa gli utenti possono fornire liquidità ad un cross di asset sul Dex depositando il 50/50 delle monete del cross. Questo protocollo incentiva gli arbitraggi in quanto non c'è nessun market maker, ma le due monete depositate tendono a mantenere il rapporto 50/50 grazie ad essi [21], questo sistema viene chiamato Automated Market Making (AMM). Gli utenti vengono incentivati a depositare le coppie sul DEX grazie alle commissioni sugli scambi del cross che vengono distribuite proporzionalmente ai fornitori di liquidità. Per un certo periodo, coloro che hanno utilizzato il DEX, hanno ricevuto UNI, il token di governance di Uniswap; siccome il piano di distribuzione prevedeva che il 15% della supply andasse agli utenti che avevano utilizzato il DEX. Dato che si può creare qualsiasi cross su questa piattaforma, a patto che si parli di token ERC20, sono nati diversi progetti che distribuiscono i loro token di governance a patto che l'utente depositi liquidità per quel progetto in coppia con asset già ampiamente diffusi.

Panoramica caratteristiche

- UNI circolanti: circa 12 milioni;
- Monete coniabili: 1 miliardo;
- Transazioni al secondo, consenso: Vedi Ethereum;

Considerazioni finali
Uniswap ha ancora una volta rivoluzionato il mondo delle monete digitali nel 2020 attraverso la seconda versione della sua piattaforma. Uniswap è probabilmente una delle innovazioni più grandi fra i casi d'uso degli SC in quanto, similmente alle ICO nel 2017, stanno nascendo molti progetti basati sul meccanismo di questo DEX. Unico difetto sono le transazioni costose in quanto gli SC sono sviluppati su rete Ethereum. Inoltre un rischio molto sottovalutato dagli utenti che forniscono liquidità alle coppie è quello dell'impermanent loss che è una perdita economica temporanea che avviene quando il valore dei due asset forniti in liquidità è molto decorrelato.

18 Ethereum Classic (ETC)

Nel Maggio 2016 un fondo chiamato DAO sviluppato su Ethereum, aveva raccolto circa 168 milioni di dollari con l'intenzione di investirli in alcuni progetti utilizzando gli SC. Nello stesso mese, fu rilasciato un paper che forniva dettagli sulle vulnerabilità dei contratti di DAO [9]. Nel mese di giugno, furono rubati 3.6 milioni di ETH (in quel momento circa 50 milioni di dollari) dagli account di DAO sfruttando le vulnerabilità descritte nel paper diffuso nel Maggio 2016. A quel punto ci fu un dibattito tra la community di Ethereum e i membri di DAO per comprendere cosa si sarebbe potuto fare per risolvere la situazione. A Luglio 2016 ci fu una votazione per decidere se effettuare un hard fork nel codice Ethereum, che permetteva di muovere gli Ether rubati su un nuovo Smart Contract che avrebbe permesso ai proprietari degli Ether di riaverli. Questa proposta vinse e l'hard fork avvenne con successo. Ethereum Classic nasce perché alcuni dei membri che non accettarono questo cambiamento, continuarono ad utilizzare la BC originale in nome del principio della BC immutabile. Il primo blocco di Ethereum Classic che non fu incluso nella blockchain Ethereum, fu il numero 1900000.

Panoramica caratteristiche

- Ethereum per blocco: 2+fee transazioni al momento;
- Monete circolanti: 113.7 milioni;
- Monete coniabili: nessun limite;
- Tempo rilascio blocco: 15 secondi circa;
- Transazioni al secondo: 20;
- Consenso: Proof of Work;
- Algoritmo di mining: Ethash.

Considerazioni finali

Per quanto Ethereum Classic rappresenti la versione coerente con quello che è la tecnologia BC, esso è di gran lunga il client meno utilizzato. Per questo motivo c'è molto meno interesse rispetto alla versione modificata anche per quanto riguarda il mining. Anche a causa del mining poco decentralizzato, Ethereum Classic ha sofferto di numerosi attacchi 51% negli anni.

19 Algorand (ALGO)

Algorand è una piattaforma open source scalabile, sicura e decentralizzata. Fondato dal vincitore del premio Turing e professore del MIT Silvio Micali, Algorand è un protocollo blockchain con meccanismo di consenso proof-of-stake. A differenza dei meccanismi di consenso di prima generazione, la tecnologia di Algorand finalizza i blocchi in pochi secondi e fornisce la finalità immediata della transazione prevenendo i soft fork. Inoltre i validatori non ricevono compensi, e sono incentivati a fornire le giuste informazioni in quanto in caso di azioni malevole, il loro patrimonio verrebbe dimezzato. Gli Algorand vengono distribuiti con il massimo della trasparenza a chi partecipa al progetto sviluppando, facendo ricerca, attraverso premi di partecipazione e tramite vendite.

Panoramica caratteristiche

- Algorand per blocco: non sono previsti rewards ai validatori;
- Monete circolanti: circa 1.10 miliardi al momento;
- Monete coniabili: 10 miliardi;
- Tempo rilascio blocco: meno di 5 secondi;
- Transazioni al secondo: più di 1000, scalabili;
- Consenso: Proof of stake;

Considerazioni finali

Anche Algorand come Cardano ha una base scientifica in quanto il suo whitepaper è stato pubblicato come articolo scientifico [10]. Inoltre le caratteristiche tecniche di Algorand sono state misurate attraverso benchmarking ottenendo ottimi risultati sia in termini di scalabilità che di prestazioni.

20 Basic Attention Token (BAT)

Basic Attention Token (BAT)[22], è il token che alimenta una nuova piattaforma di pubblicità digitale basata su blockchain progettata per premiare equamente gli utenti per la loro attenzione, fornendo agli inserzionisti

un migliore ritorno sulla spesa pubblicitaria. Questa esperienza viene fornita tramite il browser Brave dove gli utenti possono guardare annunci che preservano la privacy e ricevere premi BAT per farlo. D'altra parte, gli inserzionisti possono pubblicare annunci mirati per massimizzare il coinvolgimento e ridurre le perdite dovute a frodi e abusi pubblicitari. Lo stesso Basic Attention Token è l'unità di ricompensa in questo ecosistema pubblicitario e viene scambiato tra inserzionisti, editori e utenti. Gli inserzionisti pagano le loro campagne pubblicitarie in token BAT. Di questo budget, una piccola parte viene distribuita agli inserzionisti, mentre il 70% viene distribuito agli utenti, mentre gli intermediari che in genere aumentano i costi pubblicitari vengono esclusi dall'equazione per migliorare l'efficienza dei costi. BAT è sviluppato su BC Ethereum.

Panoramica caratteristiche

- Monete circolanti: circa 1.491 miliardi al momento;
- Monete coniabili: 1.5 miliardi;
- Tempo rilascio blocco, transazioni al secondo e consenso: vedi Ethereum;

Considerazioni finali

Come nella maggior parte dei progetti di questo tipo, BAT permette agli inserzionisti di non perdere la maggior parte delle monetizzazioni grazie all'eliminazione degli intermediari.

21 CELO (CGLD)

Celo è un ecosistema BC incentrato sull'aumento dell'adozione di monete digitali tra gli utenti di smartphone [23]. Utilizzando i numeri di telefono come chiavi pubbliche, Celo spera di introdurre i miliardi di possessori di smartphone nel mondo, compresi quelli senza accesso bancario, alle transazioni in monete digitali. La rete consente anche la creazione di SC e dApps, come parte della DeFi. La piattaforma ha due token nativi. CELO è un token che utilizza come algoritmo di consenso la PoS. CELO è utilizzato per le commissioni di transazione, la partecipazione alla governance e le attività correlate. In futuro la piattaforma punta ad ospitare varie stablecoin, di cui una, il Celo Dollar (CUSD), è già in uso.

Panoramica caratteristiche

- Celo per blocco: nessuna informazione;
- Monete circolanti: circa 125 milioni al momento;
- Monete coniabili: 1 miliardo;
- Tempo rilascio blocco: 5 secondi;
- Transazioni al secondo: nessuna informazione;
- Consenso: Proof of stake.

Considerazioni finali

Il principale punto di forza di Celo risiede nella sua attenzione agli utenti di smartphone. L'azienda sostiene che il numero di possessori di smartphone stia aumentando in modo esponenziale, ma il numero di persone che utilizzano le monete digitali sta aumentando a un ritmo molto più lento. La moneta digitale è inoltre particolarmente adatta alle regioni in cui un'ampia fascia della popolazione non ha accesso al settore bancario, ma ha uno smartphone. Colmare il divario tra le due tecnologie è ciò che Celo mira ad ottenere.

22 Swipe (SXP)

Swipe è una piattaforma che cerca di formare un ponte tra i mondi fiat e monete digitali [24] con i suoi tre principali prodotti esistenti: il portafoglio mobile multi-asset Swipe, la carta di debito Swipe finanziata da monete digitali e Swipe (SXP), un token ERC20. Il portafoglio Swipe funge da punto di accesso principale all'ecosistema Swipe e può essere utilizzato per archiviare e gestire un'ampia varietà di risorse, incluse sia le monete digitali che le valute legali. Il portafoglio può anche essere utilizzato per gestire la carta di debito Swipe. La carta consente agli utenti di spendere le proprie monete digitali presso i terminali di pagamento Visa. Questo ecosistema è alimentato dallo Swipe Token (SXP), che funge da carburante per la rete Swipe e viene utilizzato per il pagamento delle commissioni di transazione. I titolari di token SXP hanno diritto a sconti esclusivi sull'app Swipe e il token può essere utilizzato per effettuare pagamenti fiat con la carta di debito Swipe.

Panoramica caratteristiche

- Monete circolanti: circa 80 milioni al momento;
- Monete coniabili: 300 milioni;
- Tempo rilascio blocco, transazioni al secondo e consenso: vedi Ethereum;

Considerazioni finali

Una delle principali caratteristiche di Swipe è la sua usabilità. Swipe è progettato per essere accessibile a utenti di tutti i livelli di esperienza, rendendo semplice l'archiviazione e la gestione di monete digitali sull'app del portafoglio Swipe o spendere monete digitali utilizzando la carta di debito Swipe Visa. Gli utenti dovranno detenere un importo minimo fisso di SXP per poter ordinare una carta di debito Swipe Sky, Steel o Slate al fine di beneficiare dei vantaggi offerti. I vantaggi sono: fino all'8% di rimborso su tutti gli acquisti, limiti di spesa migliorati e zero commissioni sulle transazioni estere. Oltre a sbloccare una serie di vantaggi per i titolari, SXP può anche essere utilizzato per creare e votare proposte di governance, consentendo ai titolari di contribuire a plasmare lo sviluppo dell'ecosistema Swipe.

23 Statis Euro (EURS)

Prodotto da STASIS, EURS è stato sviluppato per creare una stablecoin legata all'Euro. L'EURS rispecchia il valore dell'euro sulla BC Ethereum ed è supportato da meccanismi di garanzia della liquidità che combinano la fiat globale con la trasparenza, l'immutabilità e l'efficienza della BC. Come le classiche stablecoin, gli EURS sono completamente supportati da riserve collaterali 1: 1. EURS è un token ERC20 su blockchain Ethereum.

Panoramica caratteristiche

- Monete circolanti: circa 39 milioni;
- Monete coniabili: nessun limite;
- Rilascio: 1 EURS per 1 EUR nelle riserve STATIS;
- Tempo rilascio blocco, transazioni al secondo e consenso: Vedi Ethereum;

Considerazioni finali

Grazie a questo token, anche coloro che utilizzano Euro tutti i giorni possono detenere una stablecoin senza preoccupazioni di cambio. L'azienda EURS mira a promuovere la trasparenza fornendo estratti conto

giornalieri da fornitori di account insieme a verifiche settimanali e audit trimestrali da parte di una delle 5 principali società di contabilità globale.

24 Grin (GRIN)

Grin è una moneta digitale open source minimalista e leggera, che implementa il protocollo Mimblewimble per un equilibrio unico tra privacy e scalabilità. La catena non ha indirizzi, importi e non ha necessità di memorizzare i dati degli output spesi. Non c'è una singola entità dietro di esso, lo sviluppo di Grin è finanziato da donazioni ed è volontario. Tutti possono discutere, influenzare o lavorare sul suo sviluppo. Il blocktime di Grin è di 1 minuto, ciascuno con una ricompensa coinbase di 60 grins, creando così 1 unità al secondo, per sempre. Questa emissione lineare crea un aumento costante dell'offerta, ma un tasso di inflazione decrescente; rendendo disinflazionistica l'emissione. Questo design semplice serve a garantire sia la sicurezza a lungo termine della catena che un equo processo di distribuzione delle monete a tutti i partecipanti. Nell'agosto 2016, una persona anonima che utilizzava il soprannome "majorplayer", si è registrata su un canale IRC di ricerca BTC, lasciando un collegamento ad un documento, quindi si è disconnesso. Il documento intitolato "Mimblewimble"[25] è stato scritto con lo pseudonimo di Tom Elvis Jedusor. Diversi sviluppatori si sono interessati, uno di loro è Andrew Poelstra, che in seguito ha pubblicato un documento che ha aggiunto diversi perfezionamenti e una descrizione tecnica dettagliata del white paper originale [26]. Nell'ottobre 2016, uno sviluppatore con lo pseudonimo di Ignotus Peverell ha iniziato a lavorare allo sviluppo di un'implementazione del protocollo e presto è stato raggiunto da altri nel tentativo di costruire il progetto che alla fine è diventato noto come Grin. È stato lanciato il 15 gennaio 2019.

Panoramica caratteristiche

- Grin per blocco: 60;
- Monete circolanti: circa 59 milioni al momento;
- Monete coniabili: nessun limite;
- Tempo rilascio blocco: 1 minuto;
- Transazioni al secondo: 10;
- Consenso: Proof of work;
- Algoritmo di mining: Cuckaroo/Cuckatoo.

Considerazioni finali

Grin è un interessante spunto per la coniazione di monete digitali PoW sia ASIC resistant per l'avvio del progetto che a favore dell'ASIC mining nel lungo termine. Grin ha introdotto due algoritmi di PoW. Quello primario è progettato per essere compatibile con ASIC e quello secondario resistente agli ASIC. Al lancio, la PoW secondaria rappresentava circa il 90% dei blocchi validati mentre quello primario circa il 10%. Questa percentuale evolve in modo tale che a due anni dal lancio, il 100% dei blocchi verrà validato da ASIC, incoraggiando così i produttori di ASIC a sviluppare una macchina per l'algoritmo primario. Questo meccanismo consente una decentralizzazione sana del mining che inizialmente può essere effettuato da tutti tramite CPU, successivamente entreranno in gioco le grandi farm di mining. Nonostante offra interessanti spunti tecnici per l'implementazione di nuove monete digitali basate su PoW, Grin ad oggi ha perso molto interesse nella community BC.

25 Energy Web Token (EWT)

Energy Web Token (EWT) [27] è il token nativo di Energy Web Chain, una BC pubblica EVM appositamente progettata per supportare applicazioni di livello aziendale nel settore energetico. Oltre al suo token nativo,

la catena EW supporta tutti gli standard ERC. The Energy Web Chain è stata lanciata nel giugno 2019 da Energy Web Foundation, un'organizzazione no profit globale che libera il potenziale della BC nel settore energetico e dal suo consorzio globale di membri che include società energetiche, servizi pubblici, operatori di rete, sviluppatori di software e fornitori di tecnologia.

Panoramica caratteristiche

- EWT per blocco: 0.90;
- Monete circolanti: circa 30 milioni;
- Monete coniabili: 100 milioni;
- Tempo di rilascio blocco: 5 secondi;
- Transazioni al secondo: 76;
- Consenso: proof of authority;

Considerazioni finali

Energy Web Token ha due utilità: la prima è proteggere la rete di Energy Web. La seconda è compensare i validatori tramite premi di convalida dei blocchi e commissioni di transazione. Al momento, solo le società energetiche che soddisfano gli standard elevati di EWF possono diventare validatori sulla rete. Insomma, al momento Energy Web Token non offre grosse utilità, come anche ammesso dai leader EWF, ma è un progetto molto giovane e si prevede l'aumento di utilità in futuro. Di particolare interesse per ENEA, però è la Energy Web Chain che offre Smart Contracts compatibili EVM ad alta scalabilità e a commissioni basse e un SDK orientato alle risorse energetiche rinnovabili.

3.4 Requisiti emersi dall'analisi effettuata

Dopo aver dato uno sguardo ai diversi progetti BC sul mercato, possiamo analizzare i requisiti di un buon progetto BC che garantiscano una buona adozione del token nelle community:

- originalità del progetto: è difficile che qualcuno adotti come moneta digitale un token che è una copia (magari anche migliorata) di un progetto già esistente. Immaginiamo di produrre l'ennesima fork migliorata di BTC. È molto difficile che abbia successo, in quanto i competitor nel settore sono molti e gli investitori preferiscono un asset poco ottimizzato, ma solido piuttosto che un progetto ottimizzato, ma con poche garanzie. Questo è il principale motivo per cui troviamo come monete più capitalizzate, quelle esistenti da più tempo, anche se non offrono grosse innovazioni in termini di tecnologia, o sono state oggetto di controversie;
- incentivi e semplicità di accesso ad essi: la parola d'ordine in questo tipo di progetti è "incentivi", affinché un utente sia invogliato ad utilizzare il nuovo token, sembra quasi obbligatorio fornirgli un reward che premi la partecipazione al network. È di fondamentale importanza la facile accessibilità al metodo di mining, siccome l'utente vuole ricevere gli incentivi nel modo più semplice ed immediato possibile;
- trasparenza: una buona presentazione del team e delle idee sono la base per un progetto BC di successi. È bene presentare la serietà del team facendo in modo che esso non sia anonimo, ma anzi,

sono visti di buon occhio progetti facenti parte di aziende di successo che strizzano l'occhio ai principi della decentralizzazione. Per presentare le idee, è importante scrivere un whitepaper o ancora meglio un articolo scientifico peer reviewed che possa essere letto dagli investitori e dai partecipanti al progetto, al fine di averne ben chiari i meccanismi, la distribuzione dei token e gli sviluppi futuri;

- stabilità del prezzo: Agli investitori non piace la volatilità di prezzo, al contrario, un prezzo con oscillazioni non violente, aumenta la fiducia in chi ne possiede. La limitazione delle oscillazioni si ottiene decentralizzando il possesso delle monete, più la ricchezza è distribuita, più diminuiscono i violenti cali di prezzo e la speculazione. Inoltre si ha bisogno di favorire l'utilità del token, in quanto un token molto speculativo è soggetto a vendite e acquisti costanti, mentre un token che ha grossa utilità, è più soggetto ad essere mantenuto e non venduto.
- aggiornamenti continui: il settore è estremamente giovane e muta con estrema velocità. Per questo motivo, al fine di non divenire obsoleto, un progetto BC ha bisogno di mantenersi al passo con la tecnologia e l'innovazione continuamente;
- transazioni economiche: a meno che non si tratti di token altamente speculativi, le transazioni molto costose non sono viste di buon occhio. È bene cercare di diminuire i costi delle transazioni e gestirne la scalabilità evitandone l'aumento durante la congestione del network;
- sicurezza: la sicurezza è importantissima, in un progetto BC lo è ancora di più, in quanto si tratta di risorse finanziarie con valore di mercato. Per i progetti che fanno uso di oracoli e SC è importante cercare di evitare errori di programmazione in quanto questi ultimi sono immutabili ed in caso di errori devono essere sostituiti è inoltre importante tenere conto dei flash loan [8] e della manipolazione degli oracoli, di cui discusso nel progetto AAVE;
- sostenibilità dell'inflazione: come abbiamo visto, durante il ciclo di vita di una moneta digitale, nella maggior parte dei casi essa viene distribuita ai partecipanti al network. D'altro canto, quando la moneta viene distribuita sta venendo inflazionata siccome, a pari liquidità, si stanno aggiungendo monete nuove al mercato. È, quindi, di buona norma evitare un'inflazione troppo aggressiva, in quanto potrebbe generare grosse vendite e di conseguenza abbassamenti di prezzo, causando una perdita di interesse verso il progetto.

Mostrati i migliori progetti Blockchain ed analizzati i requisiti di un buon progetto, possiamo analizzare i tipi di meccanismi di mining e di consenso. Ne offriamo una panoramica nella prossima sezione.

4 Tipi di mining

Nel mondo delle monete digitali uno dei pilastri di tutto l'ecosistema è il sistema di incentivi agli utenti per garantire la sicurezza della rete. In questa attività vengono analizzati i diversi tipi di algoritmi di consenso fra i nodi e i sistemi di incentivi di partecipazione al network per i nodi stessi. Dopo l'analisi, viene approfondita la PoW, il sistema di consenso più sicuro ed utilizzato al momento nel mondo delle monete digitali ed in particolare gli algoritmi di hashing, con una particolare attenzione all'ASIC resistance.

4.1 Incentivi per il consenso

Proof of work (PoW)

La proof of work è il primo algoritmo di mining e di consenso concepito per le monete digitali. Il primo ad implementare un mining con questo tipo di consenso è ovviamente BTC. In questa moneta digitale, si eseguono delle computazioni SHA256 al fine di validare il blocco corrente. Ogni blocco contiene diverse informazioni. In Bitcoin ogni blocco contiene l'hash del blocco che lo precede, le transazioni validate nel

blocco stesso, il nonce, il timestamp, la difficoltà di mining e la grandezza del blocco. Tutte le informazioni che si trovano nel blocco da validare, vengono convertite in una stringa e ne viene calcolato l'hash, variando il nonce (Figura 9). Il blocco risulterà valido se e solo se il suo hash inizia con un numero target di zero, questo numero target dipende dalla difficoltà di mining che è variabile. Questo è un meccanismo di consenso efficace, in quanto la verifica della validità dei blocchi è molto semplice. Basta rigenerare l'hash del blocco, controllare che il target di zero sia valido e confrontare l'hash ottenuto con quello che è stato comunicato dagli altri nodi.

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64 = 2^252.253458683
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8 = 2^255.868431117
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7 = 2^255.444730341
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965 = 2^254.782233115
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6 = 2^255.585082774
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9 = 2^239.61238653
```

Figura 9: Il processo della proof of work in Bitcoin: si esegue lo SHA256 del blocco che contiene il nonce (in figura rappresentato dalla stringa "Hello, world!+nonce") e si itera sul nonce fin quando non si trova l'hash che ha un target iniziale di zero.

Quando un miner trova un nonce che rende il blocco valido, quest'ultimo rilascia una quantità fissa di BTC al miner più le commissioni derivate dalle transazioni validate in quel blocco. La quantità fissa rilasciata ad ogni blocco, viene dimezzata ogni 210000 blocchi, che corrispondono all'incirca ai blocchi prodotti in quattro anni. Può capitare che nello stesso momento, vengano processati due nonce differenti che producono un hash valido per il blocco. In quel caso si ottiene ciò che è chiamato soft fork. Un soft fork, a differenza dell'hard fork dove le modifiche al software non sono retrocompatibili con i blocchi precedenti e si ottiene una clonazione della BC, è quindi una momentanea duplicazione della catena. I miner come regola principe, eseguono il mining sempre sulla catena più lunga, quindi, una volta che i miner confluiscono su una sola catena di blocchi, l'altra va a morire e tutte le transazioni che si trovavano in essa, vengono annullate. Per questo motivo, una transazione viene definita confermata, solo quando viene confermato un certo numero di blocchi dopo di essa. Questa caratteristica è vulnerabile ad un attacco che viene chiamato del 51%. In questo tipo di attacco, un miner malevolo che possiede la maggior parte delle risorse computazionali del network (maggiori del 51%), potrebbe effettuare il mining di una catena di blocchi alternativa e mantenerla in locale senza pubblicarla. Allo stesso tempo, potrebbe effettuare una transazione sulla BC pubblica, ricevendo in cambio dei servizi. Una volta completata la transazione, potrebbe rendere pubblica la catena che aveva validato in locale precedentemente, annullando così le transazioni della catena più corta nella quale aveva speso le sue monete digitali. In questo modo, l'attaccante avrebbe sia ottenuto il servizio e si ritroverebbe di nuovo le monete che aveva speso, nel proprio wallet. Nel network BTC, grazie all'alta decentralizzazione del mining, questo attacco è molto difficile da ottenere, in quanto il potenziale attaccante dovrebbe avere delle risorse economiche inimmaginabili per ottenere dispositivi molto potenti computazionalmente e risorse energetiche. Le BC più piccole e meno decentralizzate hanno in passato sofferto dell'attacco 51%. È il caso di Ethereum Classic e Bitcoin Cash.

Come visto, il meccanismo di consenso di PoW consente un tipo di mining che utilizza risorse computazionali. Di conseguenza, al fine di validare i blocchi delle BC basate su PoW, viene utilizzata anche energia elettrica in quanto i dispositivi vengono alimentati con essa. I dispositivi di mining, durante gli anni si sono evoluti di pari passo alla tecnologia BC. Inizialmente in BTC, il mining poteva essere effettuato efficacemente con un qualsiasi computer attraverso la CPU. Dopo qualche anno si è iniziata ad usare la GPU al fine di ottenere calcoli più veloci e specializzati che si adattavano alla difficoltà crescente di mining. Dopodichè si è passato alle Field-Programmable Gate Arrays (FPGAs) ed infine agli Application-Specific Integrated Circuit (ASIC), rendendo il mining BTC accessibile solo a grandi aziende specializzate che si trovano in nazioni con costi di elettricità accessibili. Un approfondimento sui dispositivi di mining PoW è presente nella prossima sezione.

I dispositivi di mining di BTC attualmente presenti sul mercato, sono dispositivi ad altissimo consumo energetico. Nella PoW è quindi presente un numero enorme di spreco di risorse elettriche. Già nel 2018, una transazione BTC costava, in termini di elettricità giornaliera, 1.5 volte in più rispetto una casa americana. La

rete BTC ottiene quindi 48Tw di consumi all'anno. Con la conseguenza di aver emesso 22.9 $MTCo^2$ solo nell'anno 2018 [28]. Questo valore si colloca fra le emissioni annue della Giordania e dello Srli Lanka. BTC e l'utilizzo delle monete digitali negli anni potrà solo crescere, difatti dalla sua nascita fino ai giorni nostri si sé visto un incremento di utilizzo esponenziale e si prevede che arriverà al pari dell'utilizzo del web.
Se l'utilizzo di BTC raggiungesse quello del web, potrebbe innalzare il riscaldamento globale di 2° in soli 3 decenni.
Le monete digitali stanno, quindi, lentamente passando ad altri meccanismi di consenso ed altri sistemi di mining, al fine di rendere il sistema più scalabile e meno dispendioso sia a livello economico che di emissioni di Co^2.

Proof of stake (PoS)

La Proof of Stake nasce al fine di risolvere i numerosi problemi della PoW. Come visto, la PoW è molto dispendiosa in termini energetici e poco scalabile. Oltre questo, è un meccanismo di mining molto ingombrante a causa dei dispositivi ASIC che sono gli unici a rendere il mining profittevole, ma solo in paesi nella quale i costi dell'energia elettrica sono più accessibili. Un singolo dispositivo ASIC, quando in funzione, è in grado di emettere fino ad 80 decibel di rumore ed aria a 80 gradi centigradi e consuma fino a 4000 KwH. È chiaro quindi che un dispositivo del genere non può essere mantenuto in casa e si ha bisogno di avere a disposizione strutture ed equipaggiamenti appositi al fine di rendere questa attività sicura e profittevole.
Per sopperire all'ingombranza della PoW in termini energetici, di scalabilità e di spazi, è stata studiata la PoS [29][30].
Grazie alla PoS, il validatore del blocco, viene scelto casualmente in modo pesato fra i membri interessati alla partecipazione al network. L'interesse viene calcolato basandosi sulla coin age che è una combinazione fra l'ammontare di monete digitali mantenute ed il tempo di mantenimento. Con questo meccanismo si è andato a creare un sistema di interessi che ha dato vita ad un vero e proprio business. Una volta che un validatore è stato scelto, la sua coin age si azzera. In questo modo si distribuisce la coin age, evitando di centralizzare il mining. Questo permette di effettuare il mining di una moneta digitale e di renderne sicuro il network, senza significativi sprechi di energia elettrica e senza bisogno di avere ingombranti attrezzature, aumentando altresì la scalabilità. In questo caso, l'utilizzo di energia elettrica è comparabile a quello di qualsiasi altro protocollo internet peer to peer. Un altro vantaggio della PoS è quello di rendere più difficili gli attacchi di tipo 51%, alzandone in modo significativo la soglia che diventa molto più alta. Un impotetico attaccante dovrebbe mantenere molto più del 51% di tutte le monete digitali in circolazione. Questo è dovuto all'azzeramento della coin age dopo la validazione del nuovo blocco. Di contro, se un'entità avesse più del 51% delle monete in circolazione e le vendesse, i danni sarebbero più devastanti rispetto ad un double spending in PoW, in quanto l'attacco genererebbe un drastico calo di prezzo.
Inoltre, anche se dipende dal preciso algoritmo di consenso, la PoS permette in generale di ottenere un network con transazioni molto più veloci e quindi economiche grazie alla sua leggerezza.
Anche se la PoS ha diversi vantaggi, essa ha anche alcuni problemi ed è meno matura e sicura rispetto alla PoW.
Il problema più grande viene chiamato "nothing at stake". Immaginiamo si crei un soft fork. Con la PoS, sarà indifferente su quale delle due catene si concentreranno i miner, in quanto la validazione del blocco è istantanea e addirittura si potrebbe continuare a fare mining su entrambe le catene siccome non si hanno costi, continuando a ricevere i premi dello staking qualunque catena diventi la principale. La non incentivazione della costruzione di una sola catena, rende il network molto più vulnerabile al problema del double spending siccome le catene concorrenti potrebbero andare avanti per diversi blocchi ed annullare molte più transazioni rispetto alla PoW. Nell'attacco "nothing at stake" un utente malevolo potrebbe effettuare una transazione e generare un soft fork, a questo punto, siccome gli altri miner non hanno un incentivo per effettuare mining sulla catena più lunga, anche con poche monete in stake ed effettuando mining su una sola catena, l'attaccante potrebbe generare nel proprio interesse una catena più lunga che avrà il fine di annullare la transazione effettuata in precedenza.

Un altro problema da tenere in considerazione nella PoS, è quello della selezione del validatore del blocco. Inizialmente si era pensato che il miner potesse essere selezionato attraverso un valore presente nell'hash del precedente blocco (Figura 10), questa selezione è chiamata Two-round-protocol, ottenendo una selezione pseudocasuale.

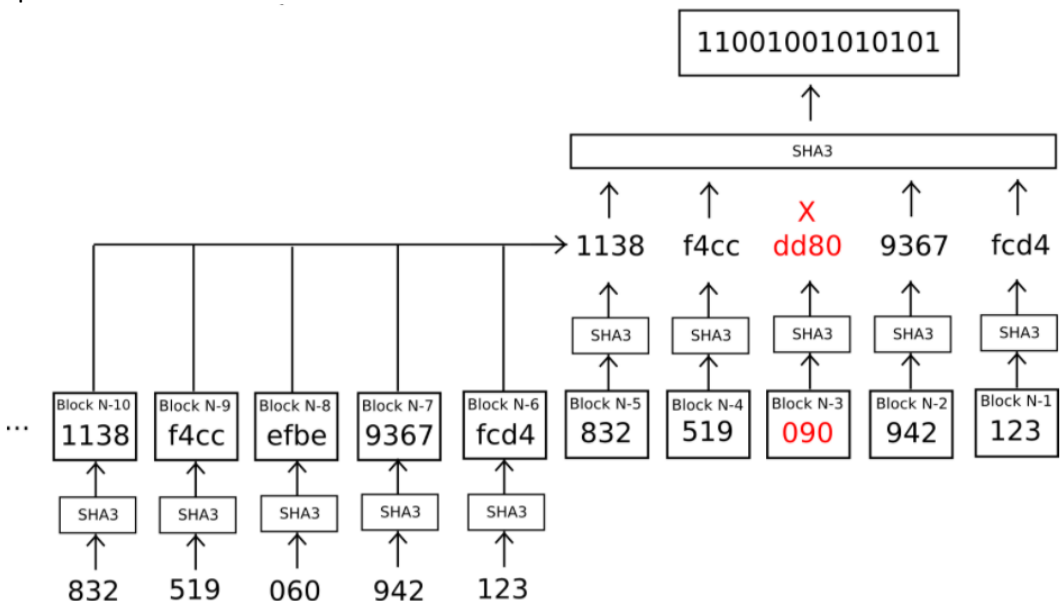

Figura 10: selezione del miner attraverso Two-round-protocol.

Tuttavia un utente malevolo che ha un minimo di monete digitali in staking, dopo aver validato un blocco, potrebbe essere capace di ricalcolare un alto numero di blocchi precedenti manipolando gli hash e facendo in modo che venga selezionato sempre il suo nodo come nodo validatore, saturando buona parte della BC che viene controllata dall'attaccante.

Tuttavia esistono numerose varianti di questo meccanismo di consenso che hanno superato i problemi appena descritti. Il problema del "nothing at stake" viene superato attraverso la consapevolezza delle azioni degli altri miner e quindi utilizzando approcci Game Theoretic; quello della selezione del miner viene superato attraverso diverse tecniche, la più semplice è l'utilizzo dei generatori decentralizzati e sicuri di numeri casuali. Insomma, i tutti i problemi che tormentavano il passaggio dalla PoW alla PoS, sono stati risolti nel tempo, difatti anche Ethereum nel momento della scrittura di questo documento, si sta preparando a passare alla PoS con Ethereum 2.0. Non è pensabile al momento un passaggio alla PoS per BTC, in quanto il mining tramite hardware di BTC è ormai un business ed i miner BTC che hanno investito molte risorse per le mining farm non sarebbero mai favorevoli al passaggio a PoS.

Delegated Proof of Stake (D-PoS)

L'algoritmo Delegated Proof of Stake (D-PoS) è un'ulteriore versione della Proof of Stake nella quale l'onere di generare i blocchi e creare moneta ricade potenzialmente non su tutti i partecipanti alla BC che possiedono monete, ma su un loro sottoinsieme chiuso e limitato, scelto attraverso una votazione fatta dall'intera rete. DPoS è stato implementato per la prima volta da Daniel Larimel sulla rete Bitshares. I nodi validatori vengono quindi eletti al fine di migliorare la sicurezza del network. Daniel, sostiene che la PoS pura sia poco protetta da nodi che hanno intenzioni dannose. Per questo motivo, propone una soluzione dove i validatori vengono eletti, in modo che i nodi che validano i blocchi siano tutti nodi verificati e fidati. Tutti possono provare ad entrare nell'insieme dei validatori, ma devono raccogliere un numero di voti sufficiente aumentando la propria reputazione e mostrando l'interesse alla partecipazione al network (Figura 11.1). Il sistema di votazione e i voti disponibili ai soggetti della rete dipendono a loro volta dalla quantità di monete possedute (Figura 11.2). Il network viene quindi diviso in due gruppi: i delegati e i testimoni. Ogni partecipante al

network può richiedere di diventare un testimone. I voti si basano sulla reputazione che ha un nodo e i partecipanti al network scelgono di votare un nodo al fine di eleggerlo a testimone allocando le proprie monete al voto (come nella PoS, le monete in questo modo non vengono spese, ma rappresentano solo la posizione presa dal testimone). Alla fine della votazione si otterrà una tabella di nodi witness basata su ranking (Figura 11.3). Se un nodo mostra interesse alla partecipazione al network allora acquista reputazione. Al contrario, se un nodo attua comportamenti malevoli, perde reputazione e viene sostituito da un testimone con più reputazione. I testimoni si occupano di creare e validare i blocchi.

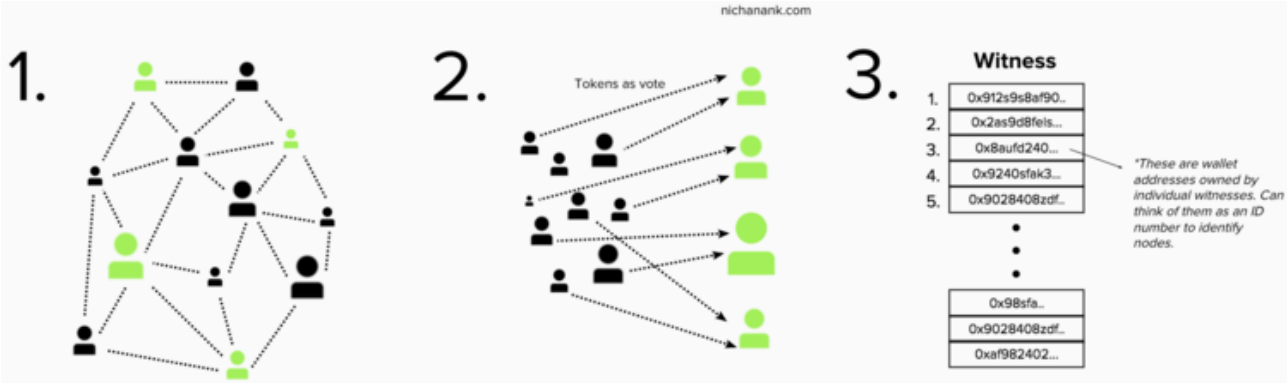

Figura 11: Elezione dei witnesses nella Delegated Proof of Stake.

Anche i delegati vengono votati. Un delegato non riceve alcun compenso in monete digitali, ma si occupa di governare il sistema e proporre le modifiche fondamentali, inoltre sovrintendono a parametri come le commissioni di transazione, le dimensioni dei blocchi, la retribuzione del testimone e gli intervalli di blocco della rete. Il voto elettorale è un processo continuo, quindi ogni testimone o delegato è sotto la pressione di perdere il suo posto a favore di un altro concorrente più popolare. Le perdite reputazionali e finanziarie sono la motivazione principale dell'astinenza dei nodi da comportamenti dannosi.
La maggior parte delle BC basate su DPoS tiene conto delle dimensioni delle parti interessate: il potere di voto dell'elettore è determinato dalla quantità di monete che il nodo detiene. Il fatto che l'opportunità di voto sia concessa a ogni utente della rete è ciò che rende DPoS l'approccio più democratico fra gli algoritmi di consenso. Le blockchain PoW non consentono agli utenti con una piccola potenza di calcolo di influenzare effettivamente la rete, che è la ragione principale dell'esistenza delle mining pool che attualmente sono le uniche entità che governano la rete BTC. La maggior parte delle BC a consenso di tipo PoS, invece, esclude i piccoli stakeholder dal prendere decisioni sulla governance della rete.
Questo meccanismo di consenso offre diversi vantaggi rispetto alla PoW ed alla PoS. Innanzitutto, le monete con consenso DPoS sono molto più scalabili di quelle PoW in quanto non richiedono un'elevata potenza di calcolo e sono generalmente accessibili agli utenti con attrezzature scadenti. Inoltre, le blockchain DPoS si sono dimostrate più veloci di quelle basate su PoW e PoS. Altro vantaggio è che la DPoS consente di avere monete digitali più democratiche e inclusive delle loro alternative offrendo più potere di governance agli utenti con piccole somme. Poiché la soglia per entrare nel network è molto bassa, il meccanismo di consenso DPoS è ampiamente considerato l'approccio più decentralizzato consentendo anche protezione maggiore contro gli attacchi double spending. Di contro, il mining diventa più centralizzato, in quanto si va a limitare il numero dei validatori dei blocchi.
Ogni progetto ha la sua versione di DPoS ed i ruoli ed i metodi possono differire.

Proof of Authority (PoAu)

Proof of Authority (PoAu) è un algoritmo di consenso basato sul concetto di reputazione ed è una delle soluzioni più ambita da imprese e reti che preferiscono partecipare a BC 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, dopodichè vengono selezionati attraverso una procedura. È una versione modificata della PoS, nella quale invece di essere le monete ad essere messe in staking, è la reputazione e l'identità del nodo. Per questo motivo i validatori rimangono sotto osservazione al fine di verificare il loro comportamento e scoprire eventuali atteggiamenti scorretti. In questo contesto per identità si intende la corrispondenza tra l'identificazione personale di un validatore sulla piattaforma con la documentazione rilasciata ufficialmente per lo stesso ente, vale a dire la certezza che un validatore è esattamente ciò che esso rappresenta. È bene notare che l'identita è scarsa per definizione, in quanto ogni validatore può avere solo una e soltanto una identità, a meno che non cada in comportamenti malevoli. Mettere in stake la propria identità significa rivelare volontariamente chi si è in cambio del diritto di convalidare i blocchi. Ciò significa che i benefici che ne derivano sono pubblici, così come le azioni nefaste che si potrebbero intraprendere. L'identità messa in gioco può fungere da grande equalizzatore, compresa e valorizzata allo stesso modo da tutti gli attori. Gli individui la cui identità (e reputazione per estensione) è in gioco per la sicurezza di una rete sono incentivati a preservarla.
Affinché il concetto funzioni in contesti reali e dal vivo è necessario soddisfare alcune condizioni: l'identità deve essere vera, ciò significa che deve esserci un processo standard e robusto per verificare che i validatori siano effettivamente chi affermano di essere. Inoltre l'idoneità per lo staking dell'identità dovrebbe essere difficile da ottenere, in modo che il diritto di essere un validatore sia guadagnato, apprezzato e sgradevole da perdere. La procedura per stabilire l'autorità deve essere la stessa per tutti i validatori, al fine di garantire che la rete comprenda il processo e possa fidarsi della sua integrità.
La semplicità del consenso PoAu arriva con la necessità di garantire l'indipendenza dei validatori e la necessità di fornire loro i mezzi per proteggere i nodi. Il costrutto PoAu Identity-at-Stake crea un modello di incentivi in cui agire nell'interesse della rete è la migliore linea d'azione che un validatore può intraprendere. L'efficienza in termini di costi e scalabilità di un tale costrutto lo rende un modello interessante per il consenso BC. Nonostante i notevoli vantaggi, la PoAu, come anche il nome suggerisce, si 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. In conclusione, mantenendo un numero di validatori limitato, questo algoritmo è altamente scalabile, veloce e inoltre non soggetto a sprechi di energia. D'altro canto, 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 Space (PoSpace)

La proof of Space (PoSpace) o proof of capacity (PoC) è stata introdotta per la prima volta da Dziembowski et al. [31] nel 2015. Questo algoritmo di consenso è molto simile alla PoW, con la differenza che se nella PoW sono le computazioni a fornire una prova dell'interesse alla partecipazione al network, qui si deve allocare un significativo spazio di hard disk per partecipare. Gli autori sostengono che, a differenza delle computazioni CPU, lo spazio del disco nella vita di tutti i giorni è largamente inutilizzato. Per questo motivo, un consenso di tipo PoSpace è meno ingombrante per l'utente ed è di certo meno dispendioso dal punto di vista energetico in quanto l'utilizzo del disco stressa molto di meno il dispendio di energia in confronto ad un utilizzo intensivo della CPU. La PoSpace consiste nel memorizzare diverse soluzioni del blocco su hard disk, se quest'ultimo contiene la soluzione al blocco più veloce, sarà in grado di validare il blocco. L'algoritmo di mining è estremamente complicato ed è impossibile calcolare le soluzioni in tempo reale, di contro i tempi di blocco sono così brevi (una media di 1 blocco ogni 4 minuti) che le soluzioni devono essere necessariamente memorizzate su disco rigido in anticipo. In definitiva, più soluzioni sono presenti sul disco rigido, maggiori sono le probabilità di avere la soluzione migliore per il blocco più recente. La PoSpace utilizza l'algoritmo Shabal. Shabal è un algoritmo di hashing molto lento, per questo motivo, i calcoli vengono eseguiti in precedenza e poi vengono distribuiti sugli hard disk che partecipano al network. I vantaggi sono diversi, a partire dal fatto che non servono macchine estremamente costose per il mining, sia dal punto di vista dell'hardware che dal punto di vista energetico. La PoSpace è inoltre più decentralizzata della PoW in quanto un hard drive ad alta capacità è più accessibile rispetto ai dispositivi ASIC ed ha bisogno di ricevere aggiornamenti continuamente.

Proof of importance (PoI)

L'algoritmo Proof of Importance è quello che regola la piattaforma NEM, la quale è stata anche testata in Giappone come meccanismo per gestire nuove forme di pagamento. Successivamente NEM è stata anche sperimentata da altri istituti di credito.
Tornando all'algoritmo, PoI è molto simile a PoS. Se nella PoS, l'utente mette in sicurezza la rete validando i blocchi ed il validatore viene scelto in maniera pesata basandosi su quante monete digitali ha "in stake", in questo algoritmo viene contabilizzato anche il numero di transazioni che effettua. Ciò significa che coloro che aiutano attivamente l'economia di NEM vengono premiati. Ad ogni utente viene assegnato un punteggio di affidabilità il quale è direttamente proporzionale alle possibilità di essere premiato.
Questo permette una distribuzione della ricchezza più uniforme; chiunque contribuisca può guadagnare XEM extra (la moneta digitale della rete NEM). La creazione del blocco da parte di un nodo può avvenire solo se si hanno 10000 XEM "vesting". Il vesting è un valore che si acquisisce mantenendo le monete sul proprio wallet: ogni giorno le monete vested aumentano del 10% del totale delle monete non vested, contenute nel portafoglio (Figura 12). Ad esempio, se un utente ha 100000 XEM, dopo 24 ore avrà 10000 XEM vested e potrà partecipare al mining. Questo incentiva a mantenere le proprie monete senza venderne.

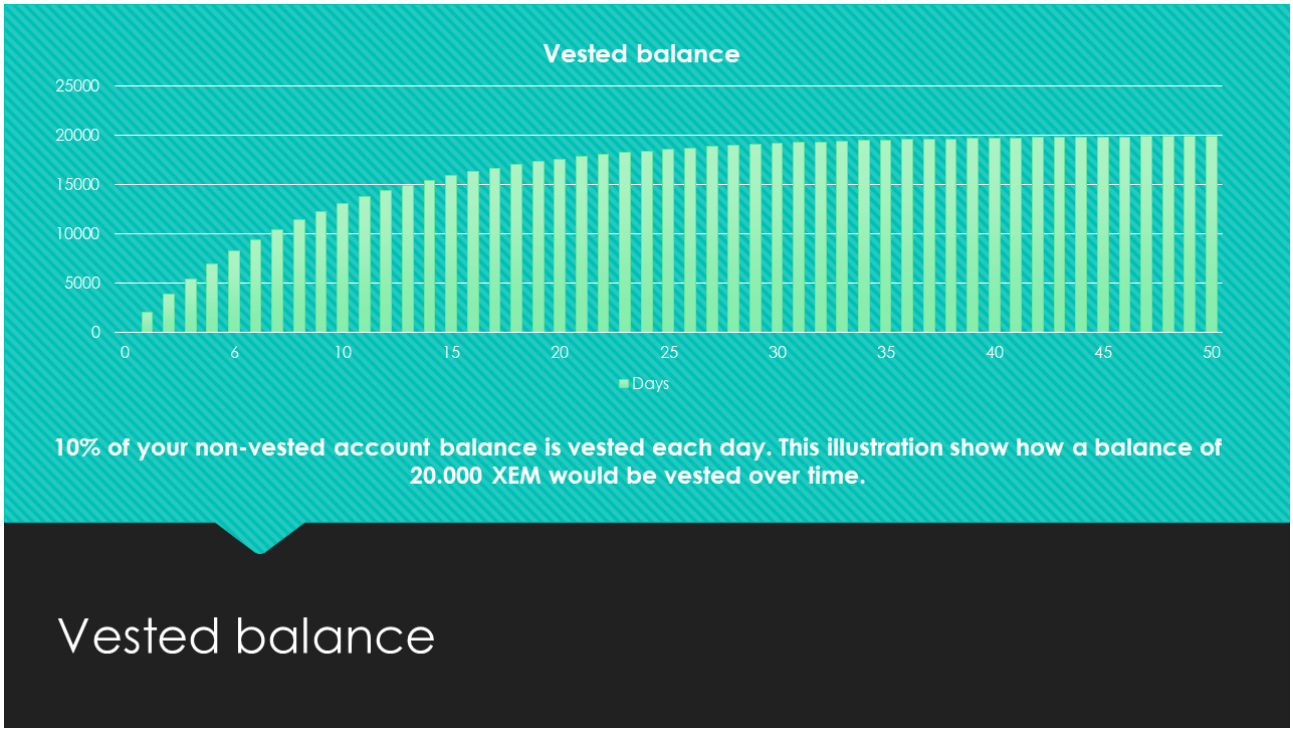

Figura 12: Vested balance. In questo caso, il 10% del saldo "non-vested" viene convertito in "vested" ogni giorno. Il grafico mostra come un saldo di 20.000 XEM diviene "vested" nel tempo.

Proof of Activity (PoA)

L'algoritmo di Proof of Activity cerca di unire i vantaggi dei due algoritmi di consenso PoW e PoS. In questo meccanismo, vengono separate le due attività eseguite dai miner: la creazione del blocco e la validazione. L'algoritmo di PoW, viene utilizzato per la creazione del blocco, che quindi è creato attraverso l'uso di una capacità di calcolo per poter soddisfare la struttura del blocco stessa. In seguito, i blocchi vengono validati attraverso la PoS, da un insieme di delegati scelti secondo l'algoritmo stesso.

Per proteggere una BC 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 il nothing at stake, se non implementato con le dovute precauzioni.
Questo algoritmo non è molto utilizzato.

Altro

In questa sezione parliamo di tipi di mining che non sono legati al consenso e alla messa in sicurezza del network tramite incentivi. Le monete generate con questi tipi di mining, si sostengono sempre su altre BC, in questo modo la sicurezza del network è garantita dall'infrastruttura sottostante.

Distribuzione o Airdrop

Altro tipo di mining può essere la distribuzione legata ad un qualche evento, sia interno che esterno alla rete. Le distribuzioni possono essere legate:

- a cambi di infrastruttura, è il caso degli airdrop dovuti alle hard fork nella quale chi era in possesso della moneta digitale originaria, al momento dell'inizializzazione della nuova catena, riceve lo stesso numero di nuove monete;
- promozioni di piattaforme che per festeggiare l'inizializzazione di un servizio, offrono dei rewards per incentivarne l'uso;
- quiz earn: alcune piattaforme offrono rewards in monete digitali se si guardano video che introducono il protocollo della moneta, incentivandone l'uso e l'acquisto;
- faucet: alcune piattaforme offrono piccole quantità di monete digitali che possono essere richieste ad intervalli di tempo;
- distribuzioni con eventi del mondo reale: il mining di una moneta potrebbe essere distribuito basandosi su eventi nel mondo reale, attraverso l'utilizzo di oracoli e sensori;
- emissione con copertura fiat o altri assets: come visto in precedenza, è il metodo utilizzato da gran parte delle stablecoin; dove ad ogni moneta fiat depositata in riserva, corrisponde l'emissione di una moneta digitale.

Liquidity mining/yield farming

Questo è un tipo di distribuzione che ha avuto molto successo nel 2020 e che ha portato alla nascita di diversi progetti estremamente speculativi. L'aggressività di queste piattaforme ricorda il periodo della diffusione delle ICO nel 2017. Al fine di comprendere questo tipo di distribuzione, riprendiamo il meccanismo di Uniswap: In questo protocollo, gli utenti possono fornire liquidità ad un cross sul DEX depositando il 50/50 delle monete del cross. Questo protocollo incentiva gli arbitraggi in quanto non c'è nessun market maker, ma le due monete depositate tendono a mantenere il rapporto 50/50 grazie ad essi [21]. Gli utenti vengono

incentivati a depositare grazie alle commissioni sugli scambi del cross che vengono distribuite proporzionalmente ai fornitori di liquidità. È di fondamentale importanza sapere che quando si fornisce liquidità ad una coppia, Uniswap rilascia un token speciale che rappresenta il cross. Il numero di token mantenuti da un account, rappresenta il peso che esso ha nella pool. Restituendo questi token al contratto di Uniswap è possibile riscattare i token detenuti in precedenza più le commissioni ricavate dai volumi del cambio.
A pochi mesi dalla pubblicazione della versione numero 2 di Uniswap, un anonimo sviluppatore, con lo pseudonimo di Chef Nomi, crea Sushiswap. Sushiswap esegue ciò che è stato chiamato vampire attack ai danni della liquidità di Uniswap.
Su Sushiswap era possibile depositare i token di liquidità di Uniswap di cui discusso in precedenza, al fine di fare mining di Sushi, il token di governance di Sushiswap con percentuali di guadagno annuali estremamente generose e che per essere sostenibili avrebbero dovuto generare dei volumi di acquisti estremamente alti. Questo tipo di mining viene successivamente chiamato Yield farming.
Tramite questo tipo di distribuzione si ottiene un duplice obiettivo: il primo è chiaramente dare un valore economico al token di governance mettendolo in pari su Uniswap con una moneta digitale che ha già mercato. Il secondo è aumentare la liquidità del token in modo da garantire scambi con poco slittamento di prezzo. Con questa tecnica, si ottiene quindi, un mining altamente speculativo e inflazionistico, che, se non gestito al meglio può degenerare molto facilmente fino al disinteresse della moneta emessa.

4.2 Tipi di hardware per la Proof of work

Dall'analisi sui tipi di mining e degli algoritmi di consenso più utilizzati nel mondo delle monete digitali, è emerso che il meccanismo di consenso di tipo PoW, continua ad essere quello più maturo e che negli anni ha dimostrato maggiore solidità in termini di sicurezza. In questa sezione descriviamo la "storia" dei dispositivi di mining di BTC, ottenendo una chiara panoramica su quali sono gli obiettivi e i requisiti da attuare in ogni epoca del ciclo di vita di una moneta digitale basata su PoW, al fine di mantenere alto l'interesse verso di essa.
Dalla nascita di BTC, i dispositivi ed il modo di fare mining si è evoluto molto negli anni. Alla nascita, l'unico hardware che serviva per fare mining di BTC era un semplice computer. Al fine di ricevere i rewards BTC per blocco, si eseguiva l'algoritmo SHA256 attraverso la CPU, quindi chiunque avesse un computer, anche non di prima fascia poteva effettuare mining in modo efficace. Ma le cose sono cambiate molto in poco più di dieci anni.
Nel 2009 i fortunati primi miner di BTC, utilizzavano delle classiche CPU multi-core, producendo BTC ad un rate di 50 BTC per blocco. In questo periodo, avendo in casa qualche computer inutilizzato, era possibile generare BTC per un controvalore di cinque dollari americani al giorno siccome la difficoltà di mining era estremamente bassa.
Nell'Ottobre del 2010, fu rilasciato al pubblico il codice per il mining di BTC tramite GPU. In questo periodo, la difficoltà di mining era cresciuta esponenzialmente e si aveva bisogno di hardware più dedicato al tipo di computazioni dell'algoritmo di hash SHA256. Le GPU, grazie alla loro architettura in grado di eseguire calcoli ad alta parallelizzazione, furono individuate come soluzione efficace. Anche in questo caso, il mining di BTC, richiedeva poche abilità tecniche nell'utilizzo di un computer e bastavano poche centinaia di dollari americani (nel caso non si avesse già una GPU performante) per effettuare con efficacia mining di BTC.
Ma le cose iniziarono presto a cambiare quando le monete digitali hanno iniziato a diffondersi fra le community, le quali iniziarono ad avere diverse idee riguardo gli hardware per il mining.
Secondo Taylor [32]:
"Efforts to scale hash rates through GPUs pushed the limits of consumer computing in novel ways. A crowdsourced standard evolved wherein five GPUs were suspended over an inexpensive AMD motherboard with minimum DRAM, connected via five PCI Express extender cables to reduce motherboard costs, and using a large high-efficiency power supply to drive all GPUs."

Insomma, le persone più interessate a questo ecosistema e che avevano qualche competenza tecnica informatica, iniziavano a creare hardware personalizzato dedicato al mining di BTC.
Come sempre, le prime persone che riuscivano ad ottenere questo tipo di hardware, potevano garantirsi un ottimo reddito. Ma ben presto, la difficoltà di mining continuò ad aumentare, fin quando i requisiti di alimentazione non divennero troppo alti per chi faceva del mining un hobby.
Nel giugno del 2011 i field-programmable gate arrays (FPGA) iniziarono a diffondersi (Figura 13) e furono la soluzione al problema della costosa alimentazione per il mining di BTC. Questo tipo di dispositivi, una volta acquistati, richiedevano di essere programmati per il mining.

Figura 13: insieme di FPGA, si nota come l'attività di mining Bitcoin inizi ad essere sempre più ingombrante rispetto agli inizi, dove bastava una semplice CPU.

Una volta che I FPGA furono modificati allo scopo, il mining BTC iniziò a scalare su di essi. Il principale vantaggio di questi dispositivi era il fatto che al fine di svolgere lo stesso compito delle GPU, il consumo di energia era di tre volte inferiore.
Ma ben presto, con l'aumentare della difficoltà, le FPGA furono sostituite dagli application-specific integrated circuit (ASIC, Figura 14) ed il mining BTC passò definitivamente dall'hobby all'industria.

Figura 14: un miner di tipo ASIC.

Laddove i FPGA richiedevano la programmazione degli stessi dopo l'acquisto, gli ASIC erano dispositivi specializzati per l'esecuzione di calcoli SHA256, che è il motivo per cui ancora ai giorni d'oggi, gli ASIC rimangono i dispositivi standard per il mining di Bitcoin.
Il futuro di BTC, ed in particolare il futuro dell'industria del mining, non è semplice da prevedere. Ma esistono molte monete digitali alternative al BTC (altcoins) che possono essere generate senza bisogno di investire grosse somme in hardware, grandi magazzini specializzati nel mining ed elettricità.
Ma, per chi è in grado di accedere a quello di BTC, il mining è ormai un mercato e permette di farne una professione, sia per chi effettivamente si dedica al mining, che per produttori di dispositivi hardware.
Proprio perché difficilmente accessibile, il mining ASIC non è ben visto nel mercato delle monete digitali, siccome il potere computazionale è in mano a poche persone (ricordiamo in particolare l'attacco 51%) e la divisione dell'hash rate diventa poco equa.
Per questo motivo, coloro che sviluppano monete digitali a consenso di tipo PoW, cercano di costruire algoritmi di mining che siano "ASIC resistant", in modo da non centralizzare il mining della neo nata moneta digitale.
Nel caso di BTC, l'esecuzione dell'algoritmo di hashing SHA256 su una stringa è un processo estremamente semplice per un computer. Le CPU possono eseguire calcoli anche molto più complessi rispetto a quelli implementati per lo SHA256.
Effettuare l'hash di una stringa non richiede tutto l'hardware che si trova in una CPU, ma soltanto alcune componenti specifiche. L'hashing si ottiene con semplici operazioni di somma, and, or, xor, right shift e right rotation. Una CPU è capace di effettuarli, ma tutta l'energia elettrica che serve per alimentare le componenti non utili al caso, viene dispersa. È quindi possibile costruire dispositivi più specifici rimuovendo dalla CPU le componenti non utili all'esecuzione dell'algoritmo di hashing, implementando nell'hardware solo quelle utili.
Un dispositivo del genere è meno costoso di una CPU, è quindi possibile serializzare questi nuovi dispositivi su un'unica scheda. In questo modo si ottiene un ASIC, il quale è molto più efficiente e specializzato.
Per rendere un algoritmo ASIC resistant, basta quindi rendere l'algoritmo di consenso il più generico possibile, facendo possibilmente uso anche della memoria.
Per quanto la PoW ASIC resistant non abbia aiutato molte altcoins ad avere successo (Figura 15), le ha sicuramente aiutate a non concludere la propria esistenza prematuramente.

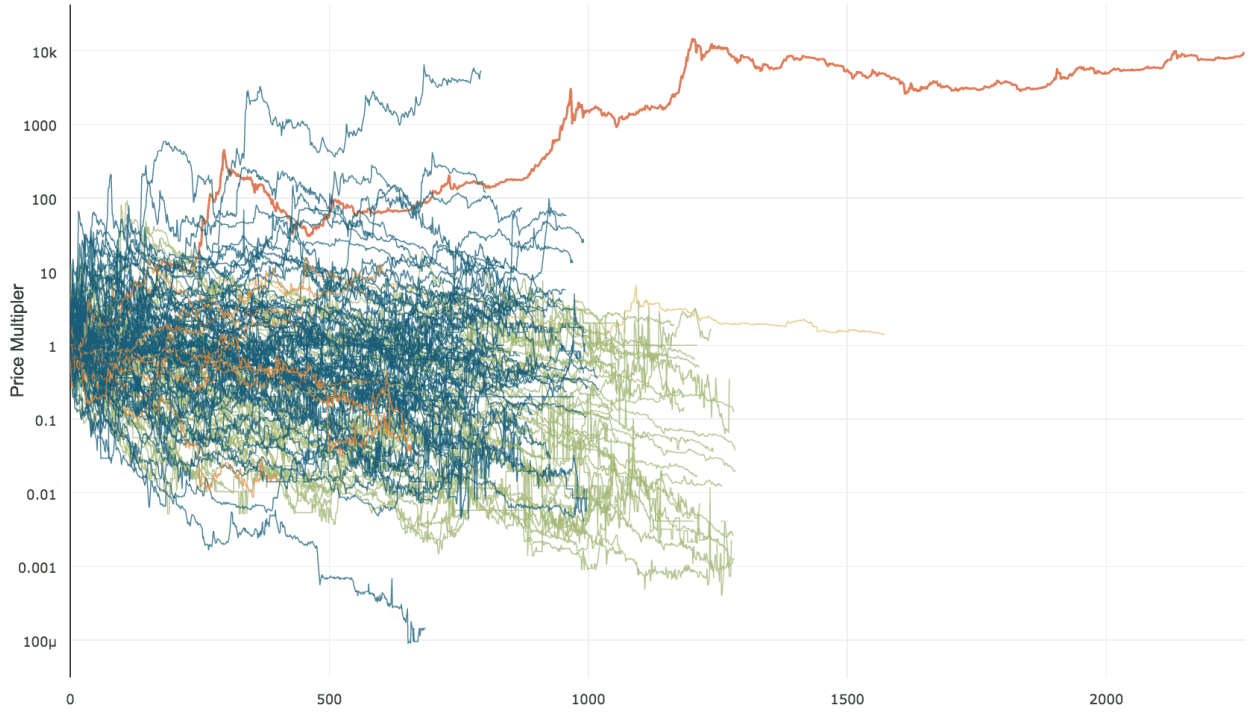

Figura 15: Prezzi di tutte le monete alternative (altcoin) dalla loro nascita, confrontato con il prezzo di Bitcoin (Grafico del 2018).

In figura 15 viene mostrato il prezzo di BTC fino al 2018 (in arancione) e viene confrontato con i prezzi di tutte le altcoin sul mercato. Si nota come l'unica moneta digitale che nel lungo termine non ha mai perso interesse è BTC.
Da questo grafico e dalle precedenti analisi si può concludere che:

1) Il successo di una altcoin non è legato all'ASIC resistance, ma le aiuta a non scomparire appena lanciate e permette sia di avere una moneta con prezzo non troppo volatile, che di rafforzare la resistenza ad attacchi 51% decentralizzando il mining.
2) Gli algoritmi di PoW non devono essere ingombranti.
3) In futuro il mining dovrà essere necessariamente spostato al 100% su energia sostenibile.
4) Il mining di BTC non è idealmente decentralizzato.
5) A meno che non venga trovata una vulnerabilità letale, BTC non potrà mai cambiare il suo meccanismo di consenso, in quanto il business del mining è troppo maturo e cambiare meccanismo andrebbe contro gli interessi degli stessi miner.

Dopo aver dato quindi uno sguardo alla storia dei dispositivi per il mining di BTC, nella prossima sezione analizziamo i principali algoritmi di PoW utilizzati dalle monete digitali più capitalizzate.

4.3 Algoritmi Proof of Work

In questa sezione, analizziamo i principali algoritmi di PoW in essere. In particolare, ne verrà analizzato il funzionamento a basso livello con un focus sul perché tali algoritmi siano resistenti ai circuiti specializzati (ASIC).

- SHA256 (Bitcoin)

L'algoritmo SHA256, viene utilizzato per il meccanismo di consenso di BTC, in quanto ha proprietà asimmentrica: un hash è semplice da calcolare e verificare, ma trovare la stringa che corrisponde ad un determinato hash è impossibile senza effettuare un bruteforce.
Lo SHA256 fa parte della famiglia di funzioni hash SHA-2 e prende in input una stringa di lunghezza arbitraria e restituisce una stringa a lunghezza fissa di 64 caratteri. L'algoritmo può essere riassunto nella figura 16.

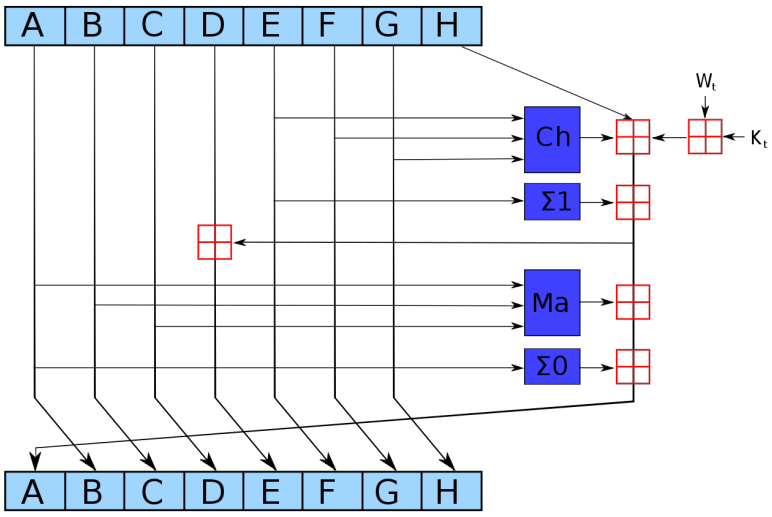

Figura 16: Una iterazione nella famiglia di algoritmi di hashing SHA-2.

Nell'algoritmo SHA256, le componenti in blu della figura 16, eseguono le seguenti operazioni:

$$Ch(E,F,G) = (E \wedge F) \oplus (\neg E \wedge G)$$
$$Ma(A,B,C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$$
$$\sum_0(A) = (A >>> 2) \oplus (A >>> 13) \oplus (A >>> 22)$$
$$\sum_1(E) = (E >>> 6) \oplus (E >>> 11) \oplus (E >>> 25)$$

Mentre le componenti in rosso eseguono l'addizione in mod 2^{32}.
Il risultato dell'hash del blocco permette di legare i blocchi fra di loro, siccome ogni blocco contiene il riferimento al blocco precedente. Il consenso viene raggiunto fra i nodi grazie alla semplice verifica della validità dei blocchi e della catena.
È quindi chiaro come sia semplice progettare dispositivi specializzati per questo tipo di computazioni, in quanto le uniche operazioni eseguite da questa funzione sono l'addizione, lo xor, l'and, l'or, lo shift a destra e la rotazione a destra.

- Scrypt (Litecoin)

Scrypt è un metodo di crittografia che utilizza un notevole volume di memoria e richiede molto tempo per essere computata, in quanto utilizza le funzioni di key derivation.
Scrypt è stato concepito da Colin Percival per la protezione dei servizi online che conservavano le copie di backup del sistema operativo UNIX [33].
L'algoritmo Scrypt è stato anche implementato al fine di essere utilizzato per il mining di alcune monete digitali e la proprietà di essere intensivo dal punto di vista della memoria gli permette di essere più complicato per la progettazione di circuiti ASIC specializzati. Il principio di funzionamento di questo algoritmo sta nel fatto che le computazioni che servono per risolvere un compito crittografico vengono complicate

artificialmente utilizzando del "rumore". Il rumore viene ottenuto con numeri generati casualmente a cui fa riferimento l'algoritmo Scrypt, i quali aumentano il tempo di lavoro necessario e intensificano pesantemente l'uso della memoria. Questo algoritmo, quindi, oltre a richiedere di generare velocemente numeri casuali, richiede anche di caricarli in memoria e di recuperarli prima di sottomettere l' hash calcolato.
In termini di hashing power, i protocolli basati su Scrypt, ottengono un hash rate molto più basso rispetto a quello dell'algoritmo SHA256.

L'algoritmo comprende i seguenti parametri:

- **Passphrase** – È la stringa di cui verrà calcolato l'hash.
- **Salt** – E' una stringa casuale di caratteri che modifica l'hash risultante e che permette di proteggere l'algoritmo da attacchi Rainbow table.
- **N** – parametro CPU/memory cost.
- **hLen** – La lunghezza della funzione di hash in ottetti.
- **MFlen** – La lunghezza dell'output della funzione di mixing in ottetti. E' definita come r * 128 in RFC7914 (algoritmo per la derivazione della chiave in Scrypt).
- **p** – Parametro di parallelizzazione; si tratta di un intero positivo dove p ≤ (232− 1) * hLen / MFLen.
- **dkLen** – E' la lunghezza desiderata dell'output; è un intero positivo dove dkLen ≤ (232− 1) * hLen.
- **r** – Rappresenta la grandezza dei blocchi, questo parametro deve essere ottimizzato per migliorare le performance della lettura della memoria. Comunemente questo parametro viene settato ad 8.

In pseudocodice:

```
Function scrypt
Inputs:
Passphrase: Bytes string of characters to be hashed
Salt: Bytes random salt
CostFactor (N): Integer CPU/memory cost parameter
BlockSizeFactor (r): Integer blocksize parameter (8 is commonly used)
ParallelizationFactor (p): Integer Parallelization parameter. (1..2^32-1 *
hLen/MFlen)
DesiredKeyLen: Integer Desired key length in bytes
Output:
DerivedKey: Bytes array of bytes, DesiredKeyLen long

Step 1. Generate expensive salt
blockSize ← 128*BlockSizeFactor //Length (in bytes) of the SMix mixing function
output (e.g. 128*8 = 1024 bytes)

Use PBKDF2 to generate initial 128*BlockSizeFactor*p bytes of data (e.g.
128*8*3 = 3072 bytes)
Treat the result as an array of p elements, each entry being blocksize bytes
(e.g. 3 elements, each 1024 bytes)
[B0...Bp-1] ← PBKDF2HMAC-SHA256(Passphrase, Salt, 1,
blockSize*ParallelizationFactor)

Mix each block in B 2^CostFactor times using ROMix function (each block can be
mixed in parallel)
for i ← 0 to p-1 do
Bi ← ROMix(Bi, 2^CostFactor)
```

```
All the elements of B is our new "expensive" salt
expensiveSalt ← B0‖B1‖B2‖ ... ‖Bp-1//where // is concatenation

Step 2. Use PBKDF2 to generate the desired number of bytes, but using the
expensive salt we just generated
return PBKDF2HMAC-SHA256(Passphrase, expensiveSalt, 1, DesiredKeyLen);
Function ROMix(Block, Iterations)

Create Iterations copies of X
X ← Block
for i ← 0 to Iterations−1 do
Vi ← X
X ← BlockMix(X)

for i ← 0 to Iterations−1 do
//Convert first 8-bytes of the last 64-byte block of X to a UInt64, assuming
little endian (Intel) format
j ← Integerify(X) mod N
X ← BlockMix(X xor Vj)

return X
```

Dove Integerify è una funzione biettiva da $\{0,1\}^k a \{0,\dots,2^k-1\}$. E Blockmix è definita come segue:

```
Function BlockMix(B):

The block B is r 128-byte chunks (which is equivalent of 2r 64-byte chunks)
r ← Length(B) / 128;

Treat B as an array of 2r 64-byte chucks
[B0...B2r-1] ← B

X ← B2r−1for i ← 0 to 2r−1 do
X ← Salsa20/8(X xor Bi)  //Salsa20/8 hashes from 64-bytes to 64-bytes
Yi ← X

return ← Y0‖Y2‖...‖Y2r−2 ‖ Y1‖Y3‖...‖Y2r−1
```

In Litecoin, come in BTC, ad un miner viene richiesto di trovare un nonce che, inserito nel blocco, restituisca un hash del blocco candidato che rispetta il numero target di zero. Anche in questo caso, il target rappresenta la difficoltà di mining; più il valore del target è basso, più è semplice generare un blocco valido in poco tempo e viceversa.
Come visto nelle precedenti sezioni, il tempo di rilascio di un blocco nel network di Litecoin è di 2.5 minuti pertanto il target si adatterà automaticamente in base alla difficoltà in modo che venga rilasciato esattamente un blocco ogni 2.5 minuti.
Quindi, nonostante l'algoritmo di hashing sia diverso, l'algoritmo di consenso funziona esattamente allo stesso modo di quello di BTC. Se un miner trova un nonce che soddisfa il target di zero nell'hash del blocco, esso può aggiungere il blocco alla catena e riceve un numero fissato di Litecoin come reward.

Nonostante Scrypt sia stato utilizzato in Litecoin al fine di ottenere l'ASIC resistance grazie al suo protocollo memory-intensive, anche questa resistenza è stata superata e sono stati sviluppati degli ASIC capaci di eseguire mining di monete digitali che utilizzano questo algoritmo di hashing con successo. Successivamente, al fine di recuperare l'ASIC resistance persa, è stato derivato Neoscrypt, ma questo algoritmo ha avuto scarso successo.
Anche il meccanismo di consenso e la struttura della BC sono identici a quelli di BTC.

- X11

L'algoritmo di hashing X11 è chiamato così perche utilizza 11 algoritmi di hashing:

- Blake;
- Bmw;
- Groestl;
- Jh;
- Kekkak;
- Skein;
- Luffa;
- Cubehash;
- Shavite;
- Simd;
- Echo.

Utilizzando diversi algoritmi di hash, si rallenta la produzione di ASIC dedicati alla moneta digitale che la implementa, in quanto si ha bisogno di trovare tutti i punti deboli e le operazioni a cui dedicare l'hardware di ogni algoritmo utilizzato. X11 è stato sviluppato inizialmente per Darkcoin (il primo nome della moneta digitale DASH) [34], la quale come algoritmo di consenso utilizza un ibrido fra PoW e PoS. DASH utilizza dei masternode che eseguono la PoW.

Elezione del masternode in Darkcoin

L'algoritmo di elezione è pseudo random deterministico ed è basato sugli ID delle transazioni nella DarkSend pool (che è l'insieme delle transazioni anonime di DarkCoin). Sommando gli ID delle transazioni nella pool, ed eseguendo l'algoritmo X11 sul risultato, viene generato un numero pseudo casuale.

Pseudo codice:

```
Target = X11 (txid1+txid2+txid3+txid4) // txid = Transaction ID
NodeValue = X11(txid1+outputPubkey1+outputPubkey2)
NodeValue2 = X11(txid2+outputPubkey3+outputPubkey4)
NodeValue3 = 0 //last node to enter pool can't be master
Score = Abs(Target-NodeValue)
Score2 = Abs(Target-NodeValue2)
```

Dove $txid_i$ è l'id della transazione i e $outputPubKey_j$ sono le chiavi pubbliche degli output delle transazioni.

Il numero casuale generato, per ogni nodo, viene confrontato con un numero target generato dall'hash della transazione e le chiavi pubbliche; questo confronto da vita ad uno score. Il nodo con score più basso viene eletto come master node, i rimanenti nodi a punteggio più basso vengono eletti come slave. Il compito degli slave è di sostituire il master node nel caso lasciasse la rete.

Master Node

La natura decentralizzata e anonima di DarkSend richiede che un nodo decida quali transazioni sono consentite nella pool. Il nodo master viene eletto ad ogni round per trasmettere la transazione finalizzata che sarà firmata dai partecipanti alla DarkSend pool. I partecipanti potranno verificare l'autenticità dei messaggi provenienti dal nodo master utilizzando le firme Elliptic Curve Digital Signature Algorithm (ECDSA) utilizzate per i suoi messaggi dopo l'elezione. I partecipanti alla DarkSend pool invece firmeranno la transazione finale solo se i loro input e output sono effettivamente quelli corretti. Dopo che la transazione è stata firmata e confermata come valida, il nodo master trasmetterà la transazione firmata e si dimetterà da master node, permettendo la rielezione.
Sulla base di X11 sono stati sviluppati altri algoritmi di hashing chiamati x12, X13, X14, X15, X16R e X17, aumentando semplicemente il numero di funzioni di hash utilizzate al fine di aumentare l'ASIC resistance.
È chiaro che l'unico obiettivo raggiunto con questi tipi di algoritmi è stato solo quello di ritardare lo sviluppo di ASIC, ma senza effettivamente risolvere il problema.

- SHA-3 (Keccak)

Rilasciato sempre dal NIST, è l'ultimo membro della famiglia Secure Hash Algorithm sviluppato [35]. Sha-3 è molto diverso da Sha1 e Sha2: esso utilizza le funzioni di sponge [36] (Figura 17).

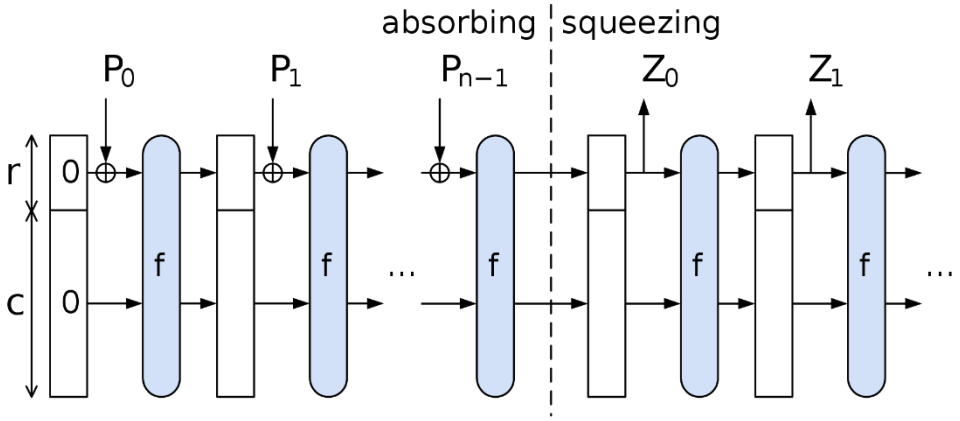

Figura 17: sponge function, r+c contengono una memoria a stati formata da b bits. F è una funzione che permuta o trasforma la memoria a stati, P è l'input, Z è l'output.

Le funzioni di sponge si dividono in due fasi: l'absorbing e lo squeezing e contengono diversi elementi:

- P è la stringa in input;
- Z è la stringa in output;

- C+r è una memoria che contiene diversi stati di cui C non viene utilizzata per la combinazione con l'input e viene chiamata capacità. r viene computata in xor insieme all'input;
- f è una funzione di permutazione.

Nella fase di absorbing i blocchi del messaggio vengono sottoposti a XOR con il sottoinsieme degli stati r, successivamente viene fatta la permutazione del risultato, insieme a c, formalmente:

$$f\big(c, xor(P_i, r)\big)$$

utilizzando la funzione di permutazione f. Nella fase "squeeze", i blocchi di output vengono letti dallo stesso sottoinsieme degli stati r, alternati dalla funzione di permutazione f. La capacità c determina la sicurezza dello schema. Il livello di sicurezza massimo è la metà della capacità.

Pseudocodice:

```
Keccak[r,c](M) {
 //Initialization and padding
 for(int x=0; x<5; x++)
   for(int y=0; y<5; y++)
     S[x,y] = 0;
 P = M || 0x01 || 0x00 || … || 0x00;
 P = P xor (0x00 || … || 0x00 || 0x80);
 //Absorbing phase
 forall block Pi in P
 for(int x=0; x<5; x++)
   for(int y=0; y<5; y++)
     S[x,y] = S[x,y] xor Pi[x+5*y];
   S = Keccak-f[r+c](S);
 //Squeezing phase
 Z = empty string;
do
{
 for(int x=0; x<5; x++)
   for(int y=0; y<5; y++)
     if((x+5y)<r/w)
       Z = Z || S[x,y];
   S = Keccak-f[r+c](S)
}  while output is requested
 return Z;
}
```

Seppur non esistano ancora ASIC dedicati allo SHA3, questa mancanza sembra essere dovuta di più al fatto che non ci siano monete digitali molto capitalizzate che fanno uso di questo algoritmo di hashing che di un effettivo problema di specializzazione dell'hardware. Il vantaggio di questo algoritmo è la maggior sicurezza e la teorica resistenza ai calcoli quantistici, proprietà da non sottovalutare nell'ambito delle monete digitali. Anche in questo caso, il mining ed il meccanismo di consenso delle monete digitali che utilizzano questo algoritmo di hashing, funzionano esattamente allo stesso modo di quello di BTC.

- NIST5

Come X11 e le sue funzioni derivate successivamente, NIST5 fa utilizzo di cinque diverse funzioni di hashing. Esse sono:

- Keccak (SHA3);

- Skein;
- BLAKE;
- Grøstl;
- JH.

Esso è un algoritmo efficiente dal punto di vista energetico. Seppur inizialmente fu resistente agli ASIC, con il rilascio di Baikal ASIC miner BK-X, ne è stata dimostrata la non resistenza, quindi si continua a preferire altri algoritmi che fanno utilizzo intensivo di memoria.

- DaggerHashimoto

Dagger-Hashimoto, è stato pensato da Vitalik Buterin e dal team di Ethereum. Era la versione primordiale dell'algoritmo di PoW di Ethereum, sostituito poi da Ethash.
Esso combina le caratteristiche generali degli algoritmi Hashimoto e Dagger, da cui il nome.
Dagger è utilizzato nell'algoritmo al fine di ottenere delle computazioni memory-hard. Esso utilizza i grafi aciclici diretti al fine di generare computazioni memory-hard dal punto di vista della generazione, ma memory-easy dal punto di vista della validazione.
Il principio fondamentale di Dagger è che ogni singolo nonce richiede solo una piccola porzione di un grande albero di dati totale e ricalcolare la sottostruttura per ogni nonce è proibitivo per effettuare il mining, ma va bene per il valore di verifica di un singolo nonce. Dagger doveva essere un'alternativa agli algoritmi esistenti come Scrypt, che sono memory-hard ma sono anche molto difficili da verificare quando la loro memory-hardness viene aumentata a livelli molto sicuri. L'algoritmo Dagger si è dimostrato vulnerabile ad attacchi di tipo shared memory speedup.
Hashimoto invece, previene effettivamente il mining su ASIC effettuando input-output con la BC che viene utilizzata come fonte dei dati prelevati.
L'idea dietro l'algoritmo Hashimoto originale è quindi, quella di utilizzare la BC come dataset, eseguendo delle computazioni che selezionano N indici dalla BC, ne estraggono le transazioni che si trovavano in quegli indici, ne fanno lo XOR e restituiscono l'output sotto forma di hash.
Dagger-Hashimoto, quindi unisce i due approcci:
la differenza tra Dagger Hashimoto e Hashimoto è che, invece di utilizzare la BC come origine dati, Dagger Hashimoto utilizza un set di dati da 1 GB generato in modo personalizzato, il quale si aggiorna in base ai dati del blocco ogni N blocchi. Il set di dati viene generato utilizzando l'algoritmo Dagger, consentendo il calcolo efficiente di un sottoinsieme dell'albero specifico per ogni nonce, sottoinsiemi utilizzati per l'algoritmo di verifica. La differenza tra Dagger Hashimoto e Dagger, invece, è che a differenza dell'originale Dagger, il set di dati utilizzato per interrogare il blocco è semipermanente, essendo aggiornato solo a intervalli occasionali. Ciò significa che la parte dello sforzo computazionale che va verso la generazione del set di dati è prossima allo zero, quindi il problema dell'attacco shared memory speedup diventa trascurabile.
Dopo diverse modifiche, questo algoritmo ha iniziato a ricevere aggiornamenti separatamente rispetto la versione originale ed è stato ribattezzato "Ethash".

- Ethash

Come il suo predecessore Dagger-Hashimoto, Ethash ha l'obiettivo di raggiungere l'ASIC resistance con computazioni memory-hard facilmente verificabili. Esso è stato l'algoritmo di consenso di Ethereum dalla sua nascita, fino ai giorni nostri, dove sta cercando di passare il testimone ad una più sostenibile PoS in Ethereum 2.0.
Ethash è l'ultima versione di Dagger-Hashimoto, la quale ha portato modifiche talmente drastiche rispetto alla versione originale che non poteva più essere considerato lo stesso algoritmo.

I passi dell'algoritmo sono i seguenti:

1. genera un seed computando tutti gli header dei blocchi generati fino al blocco attuale;

2. dal seed vengono generate delle cache pseudocasuali di 16MB. I light clients mantengono in memoria queste cache generate;

3. dalle cache, viene generato un dataset da un Gigabyte sotto forma di grafo aciclico diretto. Ogni elemento del grafo ha la proprietà di dipendere da una piccola parte di elementi provenienti dalla cache. I full node e quindi i miners mantengono in memoria questo dataset, il quale cresce in modo lineare nel tempo;
4. il mining consiste nell' utilizzare alcuni elementi di questo dataset, componendoli ed effettuandone l'hash. La verifica è semplice in quanto è sufficiente selezionare nella cache le parti specifiche che servono per rigenerare il sottoinsieme del dataset che serve per la verifica. In questo caso, quindi, serve solo utilizzare la memoria cache.

Il dataset viene aggiornato ogni 30000 blocchi, quindi la maggior parte dei miner dovrà solo leggere il dataset, senza effettuare scritture su di esso. Nonostante l'algoritmo fosse stato progettato per essere resistente alle computazioni degli ASIC, la popolarità di Ethereum ha portato i produttori di hardware ad investire pesantemente nella produzione di dispositivi, riuscendo alla fine a portare il mining basato su Ethash su ASIC con successo. Questo non ha comunque fermato Ethereum, che aveva ormai raggiunto una maturità tale da non doversi più preoccupare della centralizzazione del mining.

- Cryptonote e Cryptonight

Cryptonote permette di garantire la privacy nelle transazioni BC, ed implementa come algoritmo di PoW, Cryptonight.
CryptoNight è un algoritmo memory-intensive che permette anche di ottenere transazioni anonime. Esso, fu originariamente implementato come algoritmo di PoW nel protocollo di CryptoNoteCoin, una moneta digitale nata al solo scopo di mostrare le potenzialità della tecnologia CryptoNote.
CryptoNoteCoin non aveva quindi di per sé un valore commerciale; infatti il blocco genesis veniva spesso rigenerato per evitare che si accumulasse valore economico.
Alcune monete digitali come Bytecoin, che fu la vera prima fork di CryptoNote, e Monero, scelsero di effettuare il fork di questo algoritmo, grazie alle tecnologie che implementava e che permettevano di rendere le transazioni anonime, generando quindi delle privacy-coin.
Queste tecnologie comprendono:

- Ring signatures [37] (figura 18): sono un tipo di firma digitale per la quale un gruppo di possibili nodi vengono raggruppati per produrre una firma distintiva che può autorizzare una transazione. Una ring signature è composta da chi firma effettivamente la transazione, la cui firma viene combinata con quelle dei non signers per formare una struttura ad anello. Il nodo che firma effettivamente e i non signers in questo anello sono tutti considerati uguali e validi. La tecnologia ring signature aiuta il mittente a mascherare l'origine di una transazione assicurando che tutti gli input siano indistinguibili l'uno dall'altro.
- Stealth Address: garantiscono ulteriore protezione alla privacy dei partecipanti ad una transazione richiedendo al mittente di creare un indirizzo occasionale casuale da utilizzare solo per questa. Quando vengono condotte più transazioni che inviano fondi ad uno stealth address, invece delle transazioni che appaiono su BC come pagamenti multipli allo stesso indirizzo, ciò che verrà registrato saranno più pagamenti in uscita a indirizzi diversi.
- Limiti adattivi: si riferisce al ricalcolo continuo di diversi aspetti del protocollo CryptoNote, come la sua difficoltà di mining e la dimensione del blocco. La difficoltà è determinata sommando il lavoro totale svolto dai nodi negli ultimi 720 blocchi dividendolo per il tempo impiegato per raggiungere questo numero. Inoltre, il limite della dimensione del blocco viene calcolata utilizzando la dimensione media del blocco, ad esempio degli ultimi 100 blocchi, moltiplicandola per 2. Pertanto, se la

dimensione media del blocco degli ultimi 100 blocchi fosse stata 1 MB, il nuovo limite della dimensione del blocco sarebbe calcolata come 2 MB. Questo permette di mantenere un limite alla dimensione del blocco, evitando il flood di transazioni malevole, facendo crescere la dimensione del blocco nel tempo se necessario.

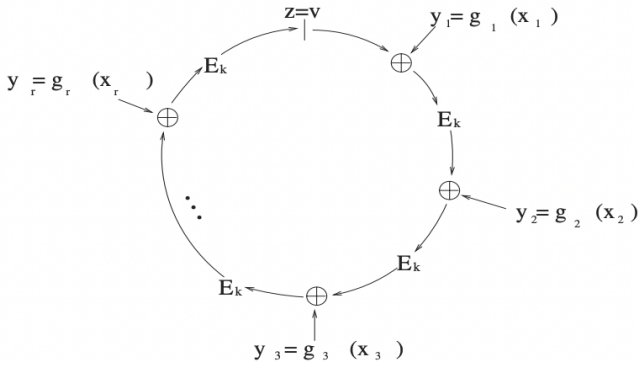

Figura 18: esempio di ring signature in [37]. Si nota come al fine di validare le transazioni di un gruppo, nascondendo gli input effettivi, vengono unite numerose firme. Vedi [37] per maggiori dettagli.

CryptoNight

CryptoNight è l'algoritmo di hashing utilizzato da CryptoNote.
CryptoNight è stato concepito come un algoritmo di hashing egualitario perché può essere calcolato da CPU e GPU, ma non è pratico per l'uso da parte degli ASIC. L'algoritmo CryptoNight sviluppa l'ASIC resistance grazie a:

• richiesta di accesso alla memoria: come detto in precedenza, gli ASIC tradizionali sono adatti agli algoritmi di hashing come SHA-256 poiché non richiedono al dispositivo di accedere alla memoria al fine di computare l'hash del blocco. L'ASIC è limitato semplicemente dal numero di calcoli che può eseguire al secondo. Le CPU e GPU, invece, hanno funzioni di memoria integrate, quindi, limitano intrinsecamente il numero di calcoli che possono eseguire. Inoltre, ogni volta che si accede alla memoria, CryptoNight ne richiede 2 MB. Questo è problematico per alcuni ASIC in quanto non hanno funzioni di memoria incorporate, questo rende CryptoNight un algoritmo memory hard;

• dipendenza dalla latenza: si riferisce al tempo necessario per l'emissione di un calcolo e la restituzione del risultato. Inoltre, la parola "dipendenza" si riferisce alla nozione che un secondo calcolo non può essere eseguito fino a quando non viene restituito il risultato del primo, cioè esiste una dipendenza dal primo calcolo affinché venga eseguito il secondo. Nel contesto dell'algoritmo CryptoNight, ogni nuova soluzione proposta da un dispositivo dipende da tutte le soluzioni proposte in precedenza.

Il meccanismo di PoW è in realtà un sistema di voting. Gli utenti votano per determinare qual è il giusto ordine delle transazioni, per l'abilitazione di nuove funzionalità nel protocollo e per l'onesta distribuzione dell'offerta di moneta. Pertanto, è importante che durante il processo di voting tutti i partecipanti abbiano pari diritti al voto. CryptoNote offre l'uguaglianza di voto attraverso una funzione di determinazione del prezzo egualitaria, che è perfettamente adatta per le CPU. Come visto in precedenza, questa funzione, utilizza istruzioni che sono molto difficili e troppo costose da implementare in dispositivi per scopi specialistici, inoltre utilizza operazioni con memoria a latenza bassa, ed è quindi impossibile sviluppare ASIC che implementino una memoria veloce.

Al momento della scrittura, Monero, il quale utilizza l'algoritmo CriptoNote/CryptoNight, grazie a queste caratteristiche, è una delle poche monete digitali che ha mantenuto l'ASIC resistance nel tempo, continuando a permettere il mining solo attraverso le CPU.

■ Equihash

Equihash è stato sviluppato da Alex Biryukov e Dmitry Khovratovich all' University of Luxembourg [38]. L'algoritmo Equihash è un algoritmo di PoW asimmetrico basato sul paradosso generalizzato del compleanno. Anche Equihash, è memory oriented e, quindi, memory hard. Di conseguenza, l'hashrate che può essere eseguita utilizzando l'algoritmo Equihash è determinato principalmente dalla quantità di memoria RAM, che un nodo possiede.
Anche l'algoritmo Equihash è stato progettato al fine di prevenire la centralizzazione del mining ASIC, portando l'algoritmo Equihash a essere definito come ASIC resistant. Equihash limita la centralizzazione da parte dei possessori di ASIC richiedendo che la generazione di hash faccia uso intensivo della memoria.
Equihash è asimmetrico ed è quindi difficile da computare, ma facile da verificare. Questo non è il caso della maggior parte degli algoritmi memory-hard, che sono simmetrici alla memoria.
Equihash si basa su tre parametri:

- n
- k
- d

Questi tre parametri vengono modificati al fine di determinare il tempo ed i requisiti di memoria dell'algoritmo.
La complessità temporale è pari a:

$$2^{\frac{n}{k+1}+d}$$

Mentre la complessità dell'uso della memoria è:

$$2^{k+\frac{n}{k+1}}$$

In questo caso, la PoW, consiste nel trovare degli i composti da n bit tali che $1 < i < k$ e:

$$H(i_1) \oplus H(i_2) \oplus \dots \oplus H(i_{2^k}), \quad hash = H(i_1 || i_2 || \dots || i_{2^k})$$

Con hash che soddisfa il numero target d di zero iniziali e H una funzione di hashing a scelta. L'algoritmo, utilizzando una lista di i ed ha bisogno di utilizzare la memoria per mantenerne i riferimenti. Nonostante questo algoritmo faccia utilizzo di memoria, sono stati sviluppati ASIC per la moneta digitale che lo implementa: Zcash.

■ Cuckatoo31 & Cuckaroo29 (Cuckoo Cycle)

Nel 2014 viene teorizzata da John Tromp un nuovo tipo di PoW chiamato Cuckoo Cycle [39]. Se nell'ambito del mining PoW si è sempre cercato di evitare l'acquisizione del mercato da parte degli utilizzatori di circuiti specializzati ASIC, gli sviluppatori della moneta digitale Grin credono che alla lunga, il mining con ASIC, sia inevitabile e dovrebbe essere incoraggiato. Mentre è assolutamente da evitare il silent mining al lancio delle monete digitali, che può essere effettuato con circuiti specializzati e che permetterebbe ai possessori di ASIC di distruggere la sicurezza del network in quanto una singola entità andrebbe a controllare una grande parte dell'offerta di moneta e dell'hashrate della rete.

Per questo motivo, Grin implementa due PoW basate sul lavoro di John Tromp:

Cuckatoo31

Esso è pensato per essere ASIC friendly e non verrà cambiato in futuro. I produttori di hardware ASIC sono incoraggiati a sviluppare macchine specializzate per il mining su questo algoritmo siccome non utilizza volontariamente operazioni che richiedono l'utilizzo della memoria.

Cuckaroo29

È la PoW pensata per essere ASIC resistant. Questo algoritmo viene aggiornato ogni sei mesi, al fine di scoraggiare i produttori di hardware a sviluppare macchine dedicate. Un dispositivo di tipo ASIC basato su questo algoritmo, quindi, diventerebbe obsoleto dopo soli sei mesi. Questo algoritmo PoW è esattamente lo stesso di quello precedente, con l'eccezione di alcune variabili differenti. Inoltre la difficoltà di estrazione del blocco, viene calcolata in maniera diversa.

Cuckatoo31 e Cuckaroo29 sono quindi, insieme, le due PoW della moneta digitale Grin. Al lancio, Cuckaroo29 contava circa il 90% di blocchi validati nella BC, mentre Cuckatoo31 ne contava il 10%. Questa percentuale cambierà durante il tempo, fin quando in due anni il 100% dei blocchi verrà validato dalla PoW Cuckatoo31, incoraggiando i produttori di ASIC a sviluppare delle macchine per questo algoritmo.
La differenza del numero blocchi validati dalle due PoW viene ottenuta modificando artificialmente le difficoltà.
Ogni blocco estratto con la PoW Cuckatoo31 tende ad aumentare lo scale factor di Cuckaroo29, il che significa che ogni volta che viene trovato un blocco con Cuckatoo31 diventa più facile estrarlo con l'algoritmo Cuckaroo29. Al contrario, quando viene trovato un blocco con Cuckaroo29 lo scale factor di Cuckatoo31 tende a ridursi e diventa più difficile estrarre con Cuckaroo29 e più facile da estrarre con Cuckatoo31.
Inoltre Grin si basa sul protocollo mimblewamble [26] al fine di proteggere completamente le informazioni sulle transazioni da terze parti. Consente inoltre di verificare le transazioni memorizzando dati minimi sulla blockchain.

5 Valutazione delle piattaforme Blockchain e compatibilità con infrastruttura ENEA

5.1 L'infrastruttura ENEA

L'infrastruttura ICT dell'ENEA è utilizzata per l'implementazione della piattaforma blockchain di progetto atta a trasferire token e registrare, certificare e tracciare gli smart contract che sono impiegati per eseguire automaticamente pagamenti e altre procedure dello smart district. 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.

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. In Italia ENEA è l'unico Ente di ricerca presente in questa graduatoria, oltre a CINECA che mantiene la posizione di leader nazionale. L'ENEA partecipa agli sviluppi nel settore HPC con un proprio sistema di calcolo CRESCO e un team con competenze specifiche per la sua gestione e utilizzo in progetti nazionali e internazionali. La collaborazione di ENEA con il CINECA, sviluppatasi in ambito EUROfusion, ha portato al ricono¬scimento, da parte di quest'ultimo, di ENEA come Tier-1 nazionale per i servizi di calcolo ad alte prestazioni. Operativamente questo si è tradotto nella realizzazione, presso il centro di calcolo di ENEA Portici, di un supercomputer da 1,4 Pflop/s di picco. Il supercomputer ENEA, deno¬minato CRESCO6 segue la lunga evoluzione dei supercomputer CRESCO, operativi presso il cen¬tro di Portici dal 2008. Nel novembre 2018 CRESCO6 si è classificato nella lista dei 500 su¬percomputer più potenti del mondo (al 420° posto) e costituisce dopo il CINECA, la maggiore risorsa di super¬calcolo a disposizione della comunità scientifica italiana. L'ultimo arrivo nella famiglia CRESCO è XCRESCO, supercomputer costituito da 45 nodi biprocessori Power8 ognuno con 4 GPU NVIDIA P100. Le risorse di calcolo sono preva¬lentemente al servizio delle attività progettuali dell'ENEA, ma nume¬rose sono le collaborazioni con Università, Enti di Ricerca Pubblici e soggetti privati che hanno l'opportunità di accedere ai servizi di calcolo ad alte prestazioni avendo a disposizione tutti gli strumenti per lo sviluppo software e un suppor¬to di elevato livello professionale. Nel corso dell'anno 2019, sebbene, ben 87,5 milioni di core-ora siano stati utilizzati dagli utenti sui sistemi CRESCO. Il risparmio realizzato in termini di costo progettuale può essere stimato moltiplicando il costo standard per core-ora (circa 0,02 EUR) per le ore di utilizzo: circa 1.75 M€.

Nello specifico, per la linea di attività in essere, è utilizzata parte dell'infrastruttura distribuita ENEA sulla quale verranno costituiti dei nodi blockchain dedicatati alla 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 BC.
Di particolare interesse per la presente linea di attività sarà il programma di realizzazione di test delle piattaforme BC attualmente sul mercato come ad esempio Ethereum che sono focalizzate su concetti chiavi quali:

- Smart Contracts (SC)
- Exchange decentralizzati (Dex)
- 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.

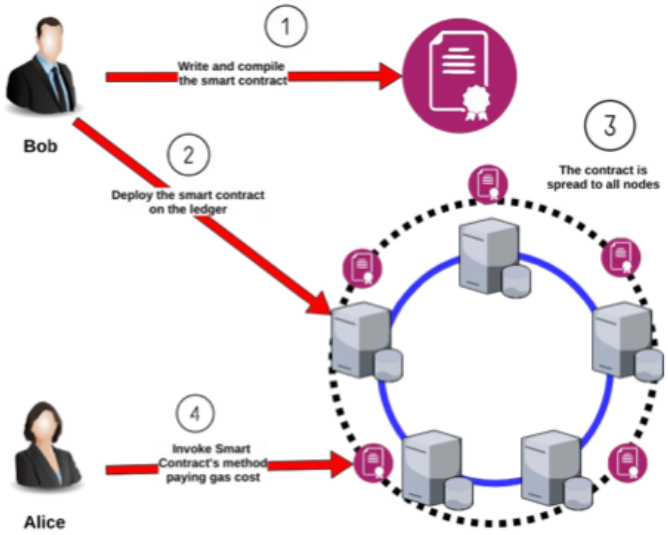

Figura 19: ciclo di vita di uno Smart Contract.

Considerando che gli SC 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 SC può contenere bug più o meno critici che possono essere sfruttati da altri sviluppatori tramite altri SC;
- Un bug critico può portare al furto di risorse come monete digitali o altre risorse più o meno sensibili;
- Una correzione di un bug comporta il ri-deployment di uno SC (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 le dApps:

- Con logica principale realizzata mediante SC;
- Con BC 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.

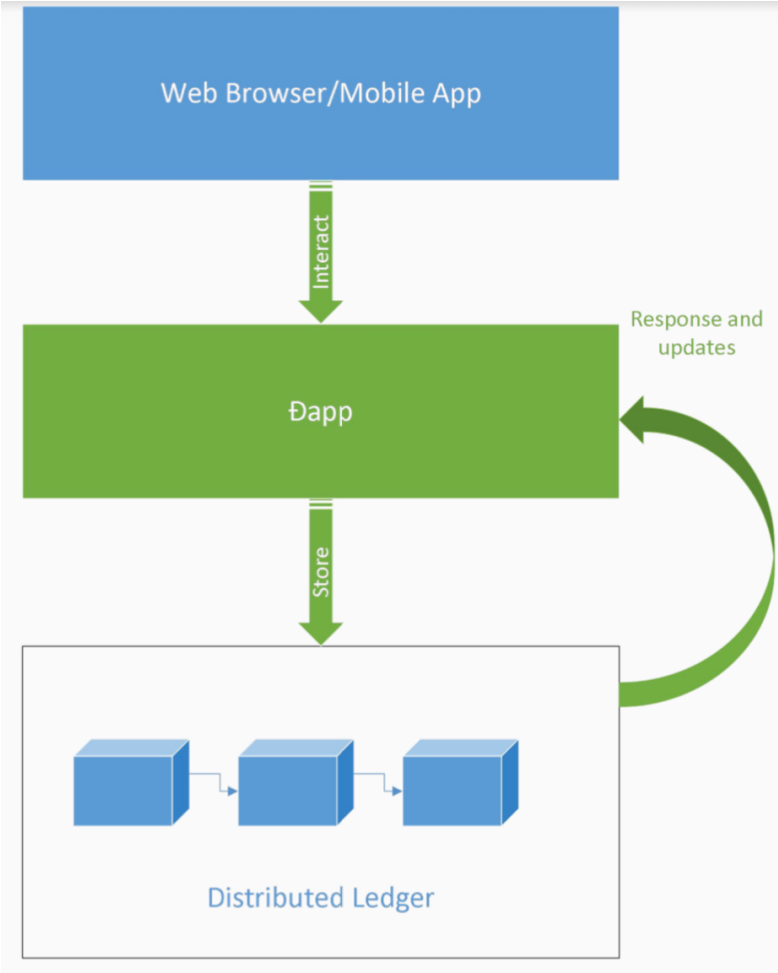

Figura 20: schema infrastrutturale funzione DAPP

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

Recenti studi [41] [42] identificano alcuni elementi che caratterizzano il comportamento di differenti BC rispetto alle problematiche intrinseche di uno specifico contesto di utilizzo. Infatti, essendo la tecnologia BC 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 possono distinguere 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;
- **Moneta digitale principale:** la disponibilità di una moneta digitale intrinseca della BC;
- **Consumi energetici.**

Transaction time: Il tempo medio che passa dalla richiesta di registrazione 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 creazione di

un blocco ed il successivo e il numero medio di transazioni registrate in n blocco. Nel caso della blockchain Bitcoin, il tempo medio 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 transazioni 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 BC 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 BC per la scrittura degli SC;
- la disponibilità di librerie aperte (API) di programmazione per l'accesso ai dati contenuti all'interno della BC.

Trasparenza: l'accesso alle informazioni contenute all'interno della BC 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 BC pongono questo elemento alla base stessa dell'infrastruttura.

Maturità: anche se la maggior parte (se non tutte) le BC 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 BC.

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

Consumi energetici: in una BC utilizzata da un'ampia community, 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 BC: algoritmi più aperti (ad esempio PoW) richiedono un maggior tempo di calcolo a garanzia del corretto comportamento dei partecipanti, aumentando notevolmente il costo in termini di consumo energetico; algoritmi più chiusi (ad esempio PoS) possono permettere una riduzione di questo costo.

Il presente lavoro ha identificato, in letteratura, alcune soluzioni di BC che possono essere valutate nei termini definiti sopra e che permettono l'implementazione di Smart Contracts e sistemi di token con linguaggio Solidity (compatibile EVM). La Tabella 7 fornisce un rapido colpo d'occhio delle differenze tra le varie BC.

Tabella 1: Confronto qualitativo tra le differenti BC compatibili EVM

	Transaction time (transazioni al secondo)	Algoritmo di consenso	Ease of integration (Turing-Language/ API)	Trasparenza	Privacy	Maturità	Consumi energetici	Supporto Energy	Costi
Ethereum	20	PoW	Si/Si	SI/Parziale	SI	Alta	Alti	No	Alti
Binance Smart Chain	2000	PoAu	Si/Si	SI/Parziale	SI	Alta	Bassi	No	Bassi
Energy Web	76	PoAu	Si/Si	SI/Parziale	SI	Media	Bassi	Si	Bassi
Tron	2000	DPoS	Si/Si	Si/Parziale	Si	Alta	Bassi	No	Bassi
Cardano	1000	PoS	No/No	Si/Parziale	Si	Media	Medi	No	Bassi

- **Comparazione qualitativa tra le differenti BC**

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 Ethereum con PoW 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. Cardano è la soluzione che risulta essere più performante da questo punto di vista siccome è teoricamente scalabile fino a 1 milione TPS.

Algoritmo di consenso: le performance e la sicurezza delle differenti implementazioni di BC dipendono dall'algoritmo di consenso utilizzato per il funzionamento. Alcuni algoritmi rendono la piattaforma particolarmente performante dal punto di vista del numero di transazioni al secondo e, dall'altra parte, dal punto di vista energetico. Da considerare anche che la scelta dell'algoritmo di consenso condiziona non solo le performance, ma anche la struttura stessa della BC, che nasceva in origine per eliminare del tutto le terze parti nella verifica delle transazioni: come descritto in precedenza, algoritmi più performanti possono richiedere l'introduzione di alcuni nodi speciali dedicati alla creazione dei blocchi, e quindi creando 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, è il caso della PoAu.

Ease of integration: elemento fondamentale per l'implementazione della piattaforma a supporto della Energy Community è la possibilità di utilizzare la tecnologia degli SC per registrare le transazioni e regolare gli accessi ai dati salvati. Tutte le altre implementazioni proposte forniscono un linguaggio completo dal punto di vista della "Turing-completeness" in quanto sono tutte compatibili con EVM. In particolare, Energy Web offre un'infrastruttura IoT già pronta per le aziende che fanno parte del settore energetico. Unica eccezione è Cardano che ha in progetto di implementare una infrastruttura EVM nel 2021, probabilmente Cardano è l'infrastruttura che ha più potenziale fra quelle menzionate, ma al momento è l'unica che non offre ancora la possibilità di implementare SC.

Trasparenza: l'accesso ai dati inclusi nella BC può essere regolata attraverso l'uso di SC che controllano l'identità di chi chiede l'accesso. In questo modo si possono creare contesti differenti che convivono (ad esempio una stessa BC 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 pseudonimizzazione degli utenti che utilizzano coppie di chiavi crittografiche per accedere ai propri profili ed ai wallet.

Maturità: a parte Energy Web che è più giovane rispetto alle altre piattaforme analizzate e Cardano che non ha ancora implementato l'infrastruttura SC, tutte le piattaforme hanno un alto livello di maturità. Essendo tutte compatibili EVM, la documentazione a supporto della tecnologia è ampiamente distribuita. 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 sono ampie e attive.
Cryptovaluta/Token: a parte Cardano, il quale lo offrirà in futuro, tutte le 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 BC 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 probabilità di successo di attacchi su un ampio numero di nodi. Questo porta ad una valutazione complessiva del consumo energetico alto per la PoW, medio per la PoS e basso per gli algoritmi di consenso a nodi limitati.

6. Meccanismi di custodia chiavi private

Nell'ottica dell'utilizzo delle monete digitali, soprattutto in ambito aziendale, è di fondamentale importanza mantenerle al sicuro da furti, smarrimenti o danni. In questa sezione illustriamo perché è fondamentale mettere al sicuro le chiavi private dei wallet utilizzati e le strategie da attuare per la custodia sicura delle monete digitali.

Chiavi private

Come visto in precedenza, tutto il mondo delle monete digitali, gira intorno alla crittografia.
Quasi tutte le monete digitali, al fine dell'esecuzione e della verifica della validità delle transazioni e dei blocchi in BC, utilizzano l'algoritmo asimmetrico di crittografia RSA (altre BC, utilizzano altri tipi di firma, ma il concetto è identico).
L'asimmetria è data dalla presenza di due chiavi, una privata che viene utilizzata per decriptare i messaggi ed è ovviamente conosciuta solo all'utente che ne è il possessore, ed una pubblica che è conosciuta da tutti e può essere utilizzata per cifrare un messaggio che poi sarà decifrato dal destinatario (Figura 21).

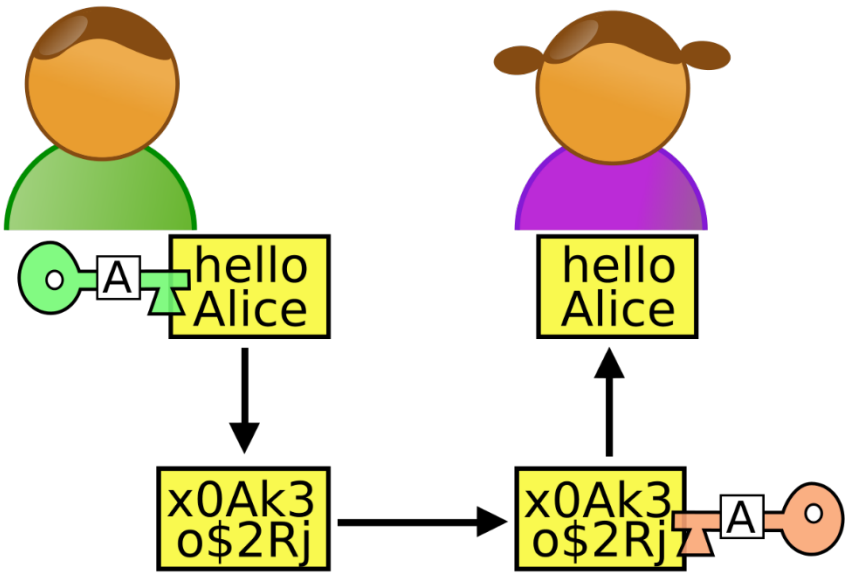

Figura 21: schema cifratura asimmetrica. Bob utilizza la chiave pubblica di alice per cifrare il messaggio. Quest'ultimo può essere decifrato solo dal possessore della chiave privata.

Formalmente, l'RSA si divide nei seguenti passi:

- Generazione di due numeri primi p e q;
- Calcolo di n=p*q
- Calcolo della funzione Charmichael's Totient: λ(n)=MCM(p-1,q-1);
- Calcolo di un numero e coprimo di $\lambda(n)$, con 1≤e≤ λ (n), la chiave pubblica è formata da e ed n;
- Calcolo della chiave privata d≡ e^{-1} (mod λ(n)) .

Allora sia m un messaggio, per cifrarlo useremo la formula:

$$C{=}m^e \ mod\, n,$$

Sia C il messaggio cifrato, per decifrarlo useremo la formula:

$$M{=}c^d \ mod\, n$$

Ma l'algoritmo RSA può essere utilizzato anche per firmare un messaggio, ed è proprio su questo principio che si basa tutta la tecnologia BC.
Sia m un messaggio da firmare, avendo a disposizione e, d ed n di cui discusso prima, allora la firma si esegue con la formula:

$$S{=}(H(m))^d mod\, n,$$

Dove S è il messaggio firmato, ed H una funzione di hashing.
Se un utente ha bisogno di verificare il messaggio firmato, allora dovrà avere a disposizione una copia del messaggio originale m^1 e calcolare:

$$m = S^e mod\, n,$$

se m corrisponde ad $H(m^1)$ allora la firma è valida.
Le transazioni BC, funzionano proprio con la firma digitale. Un wallet, nella maggior parte delle monete digitali, non è altro che una coppia di chiavi private e pubbliche, dove la chiave privata viene utilizzata per la

firma delle transazioni e la chiave pubblica, spesso utilizzata come indirizzo del wallet, viene utilizzata per la verifica delle transazioni. Quindi il possessore della chiave privata è in grado di firmare le transazioni, trasferendo dunque le monete digitali che si trovano nel wallet ad un altro indirizzo.
Spesso i wallet non generano una sola coppia di chiavi, ma utilizzano una frase seed per generare delle coppie di chiavi pseudocasuali.
Esistono diversi i pericoli che si incorrono quando non si custodiscono accuratamente le chiavi private e le frasi seed dei wallet. Dove si crea valore economico, ci sono persone che sono pronte ad approfittare di eventuali debolezze degli strumenti di custodia che possono essere soggetti a furti o frodi, ma è anche possibile che le chiavi vengano smarrite.
Essendo strumenti di tipo digitale, è anche possibile che le chiavi del wallet o la frase seed siano conservati su dispositivi non sicuri che potrebbero essere oggetto di attacchi informatici.
E', dunque, importante organizzare la gestione dei fondi e la custodia delle chiavi private attraverso alcune tecniche.
La tecnica più importante è quella della divisione dei wallet in cold wallet e hot wallet.

Cold wallet

Come intuibile dal nome, i cold wallet sono portafogli che hanno lo scopo di custodire fondi che si ha in mente di mantenere a lungo termine senza effettuare operazioni o transazioni. Questi wallet di solito, quindi, conterranno un quantitativo più grande di monete digitali rispetto agli hot wallet.
È importante non utilizzare mai la chiave privata dei cold wallet che verrà solo creata e salvata in un posto sicuro come un hardware wallet o un paper wallet, di cui discutiamo in seguito.
Dopodiché verranno inviati i fondi attraverso la chiave pubblica che non verranno più toccati fino al momento in cui si deciderà di trasferirli in un altro wallet.
La caratteristica fondamentale di questi portafogli è che dovrebbero essere conservati su dispositivi non connessi ad internet, per questo motivo i cold wallet sono sempre wallet non custodial (tipologia di wallet di cui si è in possesso della chiave privata e di cui parliamo in seguito).

Hot wallet

Gli hot wallet, invece, sono quei portafogli che contengono quei fondi che vengono utilizzati per effettuare operazioni come transazioni e operazioni con gli SC.
Questi wallet devono contenere solo la parte necessaria dei fondi da utilizzare in quanto sono più esposti al rischio di furto o frode. Fanno parte di questa categoria i software wallet e i wallet SPV. Gli hot wallet si distinguono dalla loro facilità d'uso, ma sono molto meno sicuri rispetto ai cold wallet. Quando si parla di hot wallet, e quindi si ha bisogno di effettuare operazioni con le monete digitali nel breve periodo, le soluzioni possono essere di due tipi: custodial o non custodial.

Portafogli custodial

I portafogli custodial, sono quei tipi di portafogli le cui chiavi private sono in mano solo a chi fornisce il wallet. Quando si pensa ad un wallet custodial, la prima categoria di servizi che viene in mente è quella degli Exchange centralizzati. Quando si utilizza un exchange centralizzato, non vengono mai fornite le chiavi private dei wallet. Questo anche perché molti scambi non avvengono effettivamente on-chain, ma vengono tracciati su un database per essere resi poi effettivi solo quando si ritirano i fondi. Questo escamotage viene utilizzato per abbassare i costi delle transazioni, che sarebbero altrimenti proibitivi. I wallet forniti come portafogli di deposito vengono utilizzati solo per raccogliere i fondi, i quali vengono poi spostati sull'hot wallet dell'exchange quando le commissioni sono vantaggiose.
Ma esistono tanti altri servizi che offrono wallet di tipo custodial.

I vantaggi di questa soluzione sono la semplicità d'uso e l'impossibilità di smarrire l'accesso al wallet, in quanto può essere recuperato in qualsiasi momento tramite operazioni di recupero sulla piattaforma che li offre.
Nonostante sia la soluzione più semplice e sembri quella più sicura in quanto è molto più simile ai metodi tradizionali come la custodia di fondi in banca e la maggior parte ha opzioni di sicurezza come l'autenticazione a due fattori e transazioni multifirma, mantenere i fondi su un wallet di questo tipo, può essere molto pericoloso siccome ci si affida ad una parte terza che può essere soggetta a frodi in quanto sono gli obiettivi più comuni degli hacker, ma può anche capitare che fallisca, o che in modo nascosto esegua operazioni illegalmente.
Inoltre, ci si deve affidare al fatto che la terza parte coinvolta accetti e confermi tutte le operazioni che si vogliono compiere.
Per esempio, nell'estate del 2016, alcuni hacker hanno rubato quasi 120mila Bitcoin dall'hot wallet dell'exchange Bitfinex. Né l'autenticazione a due fattori né la firma multipla hanno impedito il furto di fondi.
Un altro esempio è il recente problema che ha avuto l'exchange OKEx, che aveva sospeso il ritiro dei fondi dall'exchange per diversi mesi poiché il proprietario della chiave privata dell'hot wallet era stato oggetto di investigazioni da parte delle autorità. O ancora, la chiusura degli exchange MtGox e BTC-e, il primo a causa di una probabile frode, il secondo a causa dell'arresto dei proprietari.
Questi sono solo alcuni esempi dei clienti che avevano un wallet custodial su un exchange che hanno perso i propri fondi, ma i casi di problemi legati a questo approccio sono molti di più.
Un vantaggio di questi wallet, oltre alla semplicità d'uso, può essere quello di poter mantenere più monete digitali di natura diversa su un unico account.
Ma questo non può giustificare il rischio di conservare grosse somme su dei wallet custodial che sono per lo più centralizzati e vanno contro il principio di decentralizzazione della BC.
In conclusione, su questo tipo di wallet si dovrebbe custodire solo una piccola somma di monete digitali sulla quale si ha bisogno di effettuare operazioni che il servizio su cui si custodiscono le monete, offre.
Possono far parte di questa categoria anche alcuni light wallet di tipo mobile wallet e desktop wallet.

Portafogli non custodial

Fanno parte della categoria chiamata non custodial, quei wallet di cui si ha il possesso al 100% siccome si possiede la chiave privata ed a cui nessun'altra persona o ente ha accesso. Si ha quindi la piena custodia del portafoglio, senza affidarsi a terze parti che potrebbero essere meno affidabili di quanto sembri. Il vantaggio di questi portafogli è la sicurezza, ma solo se si riescono a proteggere adeguatamente. Di contro, se non adeguatamente protetti potrebbero essere facile preda di hacking o soggetti a smarrimento. Nel caso in cui si smarrissero le chiavi di questi wallet, diviene impossibile recuperare i fondi.
Un altro vantaggio dei portafogli non custodial è la possibilità di compiere qualsiasi operazione, senza effettuare il KYC, che in un wallet custodial potrebbe bloccare i fondi per diverso tempo e permette una maggiore privacy.
Ancora, quando avviene un hard fork su una moneta digitale che si detiene, con un wallet non custodial non si avrà nessun problema ad inviare fondi, mentre su un wallet custodial si potrebbero avere diversi problemi di manutenzione, con i fondi che potrebbero essere conseguentemente bloccati per diversi giorni.

I portafogli non custodial si dividono in altre due categorie, le elenchiamo di seguito:

Wallet full node

I wallet full node, sono desktop wallet e vengono creati e mantenuti dal client della moneta digitale che si sta utilizzando. Ad esempio, il full node di Bitcoin è Bitcoin Core.
Mantenere uno di questi wallet, permette all'utente di effettuare anche il mining in quanto gestisce un intero nodo del network. Questa è una soluzione di molti sviluppatori, che non vogliono fare riferimento a terzi affidandosi completamente ad un altro nodo che effettua fisicamente le transazioni.

Il wallet quindi avrà bisogno di sincronizzarsi con tutti gli altri nodi e verificherà la correttezza di tutte le transazioni della rete avvenute fino a quel momento.
Lo svantaggio di questo wallet è che per mantenerne uno si ha bisogno di scaricare tutta la BC sulla macchina che ha in funzione il nodo, e le BC che sono in vita da molto tempo e che contengono transazioni con grandi moli di dati, come Ethereum, possono arrivare a pesare più di 5 Terabyte.
Un wallet full node dovrebbe essere utilizzato soltanto come hot wallet siccome si tratta di un software wallet e può essere soggetto ad attacchi informatici.

Light wallet o Wallet SPV (Simplified Payment Verification).

Al contrario dei wallet full node, i light wallet non hanno bisogno di scaricare tutta la BC per il corretto funzionamento ed è quindi il modo più semplice ed economico per avere un wallet.
I light wallet si occupano di firmare le transazioni in locale, per poi delegarne il broadcast ad un full node terzo, oppure, nel caso di BTC (o di qualunque altra moneta digitale utilizzi i Merkle tree) un light wallet ha bisogno di scaricare solo il ramo Merkle di cui ha bisogno. La delega non è soggetta a problemi di sicurezza, in quanto si tratta soltanto dell'output di una transazione già firmata e che quindi non contiene la chiave privata.
Nel caso di BTC, proprio Satoshi Nakamoto nel suo whitepaper suggerisce un metodo per verificare i pagamenti in BTC senza eseguire un nodo di rete completo.
Questo metodo viene chiamato Simplified Payment Verification (SPV). In questo metodo, un portafoglio Bitcoin SPV di un utente ha bisogno solo di una copia delle intestazioni di blocco della catena più lunga, le quali sono disponibili interrogando i nodi di rete fino a quando è evidente che è stata ottenuta la catena più lunga. Quindi, il portafoglio che utilizza il client SPV ottiene il ramo Merkle che collega la transazione al suo blocco. Collegare la transazione a un punto della catena attiva dimostra che un nodo di rete l'ha accettata e così anche i blocchi aggiunti dopo aver stabilito la conferma.
Se parliamo di light wallet non custodial, ci stiamo avvicinando al tipo di wallet più sicuro sul mercato, in quanto alcuni di questi wallet permettono all'utente di possedere effettivamente la chiave privata e possono essere creati sia online che offline.
In questo paragrafo, parliamo solo di light wallet non custodial in quanto i wallet custodial sono già stati approfonditi in precedenza.
Essi si dividono, ancora, nelle seguenti categorie, li elenchiamo in ordine di sicurezza, partendo dai software wallet i quali sono meno sicuri, fino ad arrivare ai wallet più sicuri; e cioè gli hardware e paper wallet:

Software wallet

Come già ampiamente discusso, i software wallet, sono quei tipi di portafoglio che "contengono" monete digitali che vengono eseguiti su dispositivi informatici e che quindi, se creati ed utilizzati su un dispositivo connesso alla rete, può essere oggetto di attacchi informatici.
I software wallet possono essere di tre tipi:

- **Desktop wallet:** nella maggior parte dei casi, si tratta di wallet full node che hanno bisogno di scaricare tutta la BC per il corretto funzionamento e che possono contenere un solo tipo di moneta digitale a meno che non si tratti di BC che consentono lo sviluppo di token sulla propria infrastruttura. Ma esistono anche desktop wallet che fanno parte della categoria dei light wallet. L'esempio più famoso di desktop light wallet è Metamask. Esso, nel caso dell'utilizzo su dispositivo desktop, è un'estensione per browser che fa uso di Web3, una libreria Javascript che permette ai light wallet di interfacciarsi con nodi full. Metamask è in grado di interfacciarsi con molti siti web che offrono servizi BC e dApps, permettendo quindi di effettuare operazioni su piattaforme terze, utilizzando un wallet non custodial. Metamask ha anche una versione mobile che offre le stesse potenzialità della versione desktop.

- **Mobile wallet:** in un periodo storico dove gli smartphone sono diventati più utilizzati dei dispositivi desktop, si ha bisogno di offrire una valida alternativa mobile ai desktop wallet per la custodia di monete digitali. Di questa categoria, per ovvi motivi, fanno parte solo i light wallet ed al fine di favorire l'usabilità dell'applicazione, per la maggior parte, si tratta di portafogli custodial. Tuttavia esistono diverse eccezioni non custodial come Metamask mobile ed alcuni altri wallet, che permettono anche di interfacciarsi con dApp attraverso un browser integrato nell'applicazione.

Wallet multi signature

I wallet multi signature, come si comprende dal nome, sono wallet in cui si ha bisogno di più di una firma per l'esecuzione di una transazione.
Uno dei maggiori vantaggi delle monete digitali, come visto, è la possibilità di avere denaro programmabile e SC. Ottenendo transazioni che vengono eseguite automaticamente, dopo che sono state soddisfatte determinate condizioni predeterminate. Una delle forme più basilari dell'utilizzo di questa caratteristica, è l'implementazione di indirizzi multi-firma noti anche come multi-sig.
Gli indirizzi con più firme sono come conti bancari congiunti in cui le transazioni devono essere autorizzate da più di un titolare del conto. Ciò è estremamente utile per eseguire transazioni in cui non è stata stabilita la fiducia o per creare fondi gestiti dalla comunità. È possibile configurare facilmente un portafoglio multi-firma utilizzando servizi già pronti di cui le chiavi private per la multisignature non vengono salvate, ma la convalida può avvenire in modo centralizzato.
Per creare un wallet multisignature senza affidarsi a parti terze, possono essere utilizzati gli SC.
Per implementare un semplice wallet multisignature a due utenti, con gli SC, ad esempio in Solidity, il codice è il seguente:

```
pragma solidity^0.4.25;

contract SimpleMultisig {
        address one;
        address two;
        mapping(address => bool) signed;

        constructor(address signer1, address signer2) public {
                one = signer1;
                two = signer2;
        }

        function Sign() public {
                require (msg.sender == one || msg.sender == two);
                require (signed[msg.sender] == false);
                signed[msg.sender] = true;
        }

        function Send(uint256 amount, address payable to) public returns (string) {
                require (signed[one] == true && signed[two] == true);
                to.send(amount);
                signed[one] = false;
                signed[two] = false;
        }

        function () payable external {}
```

```
}
```

con questo esempio è possibile inviare Ethereum ad un wallet terzo, solo se entrambi i partecipanti hanno approvato la transazione firmando con la funzione Sign().
Esistono anche wallet multi signature che permettono di trasferire fondi per voting, ad esempio se avviene la firma del 51% dei partecipanti al wallet; questo può essere utile in caso di smarrimento di una delle chiavi private utilizzate per il wallet.
È chiaro come i multi-sig aumentino notevolmente la difficoltà di furto o manipolazione delle risorse collegate. Più il numero di partecipanti cresce, maggiore è la sicurezza dei fondi. Ad esempio, con un wallet a due firme, un ente deve mantenere le due chiavi su macchine separate o utilizzate da entità separate e assicurarsi che entrambe siano utilizzate per tutte le transazioni collegate all'asset. Ciò rende difficile il furto e la manipolazione in quanto richiederà la compromissione di entrambe le firme. In teoria, la tecnologia multi-firma non è diversa dagli accordi finanziari cartacei che possono richiedere più di una firma.
Un indirizzo a chiave singola non è solitamente l'opzione migliore per entità con più parti interessate coinvolte nella custodia di monete digitali. In tal caso, ricordiamo il problema che ha interessato recentemente l'exchange OKEx.
Un wallet multi signature implementato con SC, non si può chiamare propriamente software wallet, ma fa quindi parte della categoria particolare dei multi signature wallet.
Per quanto sicuro, la sicurezza del wallet dipende sempre dalla sicurezza delle chiavi private che servono per accettare la transazione. Se queste chiavi private non sono custodite in modo adeguato, anche i fondi che si trovano nel wallet multi signature non sono sicuri.

Brain wallet

Come suggerito dal nome, i brain wallet sono un tipo di portafoglio in cui l'utente memorizza la frase seed capace di generare la chiave privata del wallet che non viene scritta o conservata da nessun'altra parte.
Generalmente è difficile ricordare o memorizzare direttamente le chiavi private perché sono una lunga stringa di numeri alfanumerici ed una frase di senso compiuto, può facilmente aiutare l'utente a non perdere l'accesso al wallet.
In questo caso, se l'utente dimentica la frase seed o se a causa di problemi gravi, non può più accedere al portafoglio, le monete digitali associate ad esso vengono perse per sempre.
Qualsiasi generatore di brain wallet, consente ai suoi utenti di digitare parole casuali (cioè 4, 6, 8, 12 o 24 parole) e l'insieme di esse viene chiamato passphrase. A seconda del tipo di generatore che si sta utilizzando, ne viene effettuato l'hash, per generare una coppia di chiavi pubbliche e private.
Se questo può sembrare il metodo più sicuro per la creazione di un wallet, non è difficile che la passphrase possa venire dimenticata, magari anche per problemi di salute.
Altro problema di questo approccio è la più facile collisione di passphrase: è molto più facile che un altro utente possa pensare alla stessa passphrase, avendo la frase un senso compiuto, piuttosto che utilizzare l'approccio classico dove la probabilità di collisione tende allo zero. Inoltre è più vulnerabile ad attacchi bruteforce, rispetto alla generazione classica, anche se questi possono essere resi più difficoltosi utilizzando un salt.

Hardware wallet

Gli hardware wallet sono progettati per garantire un cold storage sicuro offline che offra sia i vantaggi del cold storage di un paper wallet, che la possibilità di effettuare transazioni sicure senza averne i problemi d'intralcio grazie al software che permette le transazioni senza esporre le chiavi private. Essi sono dispositivi che hanno in dotazione un piccolo schermo, uno o due pulsanti e permettono la semplice azione di memorizzare chiavi e firmare transazioni.

I portafogli hardware sembrano piccoli dispositivi USB e offrono un approccio minimalista, ma estremamente efficace alla sicurezza. Ciò si basa sulla logica secondo cui più un dispositivo è complesso, maggiori sono le opportunità che un utente malintenzionato ha di infiltrarsi.
Nel caso dei portafogli hardware, il dispositivo è così semplice che è praticamente impossibile da infettare o hackerare. I portafogli hardware, quindi, possono firmare una transazione in locale, ma per effettuare il broadcast della transazione si ha bisogno di collegarli ad un computer.
Una volta collegato al computer, bisogna scaricare il software del portafoglio oppure qualsiasi altro software wallet compatibile con l'hardware wallet.
La chiave privata non viene mai esposta al di fuori dell'hardware wallet, nemmeno quando esso è collegato al software per il broadcast della transazione.
La prima cosa da fare quando si inizia ad utilizzare un hardware wallet, è quella di annotare il set di parole che viene fornito durante l'inizializzazione del dispositivo.
Queste parole, sono le già note frasi seed che servono a ripristinare le chiavi private generate dall'hardware wallet.
La frase seed verrà conservata quindi successivamente su un paper wallet. In caso di smarrimento o rottura del dispositivo hardware, la frase seed potrà essere importata in un nuovo dispositivo.
Esistono diverse aziende che offrono questo tipo di dispositivi, la più famosa è Ledger, la quale è presente sul mercato con due dispositivi. I portafogli Ledger utilizzano BOLOS, un esclusivo sistema operativo brevettato sviluppato da Ledger. Questo sistema crea uno scudo individuale attorno ad ogni applicazione nel portafoglio Ledger per proteggerli dagli attacchi informatici.

Ledger nano S

Il nano S (figura 22) è il dispositivo Ledger più diffuso. Supporta oltre 30 monete digitali e tutti i token ERC20 (comprese tutte le monete digitali che hanno chiavi private, pubbliche e meccanismo di transazioni identiche a quelle di Ethereum). Il dispositivo è controllato solo da 2 pulsanti e tutte le azioni possono essere verificate sullo schermo. Inoltre, le applicazioni complementari di Ledger consentono di gestire facilmente le transazioni, per utilizzarle basta collegare il Ledger ad un computer tramite USB. Non è necessario un adesivo anti-manomissione per proteggere il dispositivo. Il chip di sicurezza controlla l'integrità del dispositivo ogni volta che viene acceso.

Figura 22: Ledger nano S.

Ledger nano X

Il Ledger nano X (Figura 23) è la versione potenziata del Ledger nano S. Esso, rispetto a questa versione, permette la gestione di 100 diversi tipi di monete digitali, dove il nano S ne permette soltanto 5 nello stesso momento. Nano X è leggermente più grande di Nano S in quanto è dotato di Bluetooth in modo che gli utenti possano collegare facilmente il proprio telefono cellulare con l'app Ledger live. Il portafoglio hardware Nano X supporta inoltre alcune monete digitali in più di nano S.

Figura 23: Ledger nano X.

La seconda azienda leader di questo settore è Trezor. Essa è stata la prima azienda a proporsi su questo mercato. Il vantaggio principale di TREZOR rispetto alla concorrenza è la reputazione dell'azienda. Uno dei fondatori dell'azienda è Marek Palatinus, che ha anche fondato la prima pool di BTC.

Trezor One

Il Trezor One (Figura 24) precedentemente noto come Trezor ha un design semplice e un'interfaccia intuitiva. Il prezzo di Trezor One è relativamente basso rispetto a Ledger Nano. Supporta anche più valute come Bitcoin Cash, Bitcoin Gold, Dash, Ethereum, Ethereum Classic, Litecoin, NEM, ecc. Tuttavia, è da segnalare il difetto per cui se è necessario aggiornare il portafoglio può capitare che debba essere reinizializzato con la frase seed.
Quindi, è necessario disporre della una frase di backup nel caso in cui sia necessario ripristinare il portafoglio. Come Ledger, Trezor è un portafoglio offline e non è connesso a Internet e come tale è completamente protetto. C'è un sigillo sulla porta USB, quindi all'acquisto è possibile controllare se il portafoglio è stato manomesso o meno. Per ulteriore spazio di archiviazione inoltre, è possibile utilizzare una microSD.

Figura 24: Trezor One.

Trezor T

Trezor T (Figura 25) è un'altra versione dei dispositivi Trezor ed è dotato di touch screen. Supporta più monete del portafoglio Trezor One. Ad esempio, Tezos. Questo portafoglio hardware Trezor è più costoso dei dispositivi mostrati in precedenza.
Esistono tanti altri dispositivi hardware per la custodia delle chiavi private, ma i dispositivi Ledger e Tresor sono i più affidabili del settore al momento.
La facilità di firma di una transazione e broadcast senza l'esposizione della chiave privata rende questi dispositivi un ottimo strumento sia per gli hot wallet che per i cold wallet. Essi sono infatti anche supportati da alcuni wallet come Metamask, che permette quindi di utilizzare dApp tenendo al sicuro le chiavi private.
Sebbene questi dispositivi siano effettivamente sicuri, essi potrebbero comunque essere compromessi. In primo luogo, c'è bisogno di fidarsi del fatto che la società che ha creato il portafoglio non abbia registrato tutte le chiavi private con un piano per razziare i portafogli in futuro. Questo vale per sia per quelli acquistati dalla società stessa, ma ancora più in particolare se un portafoglio hardware è stato acquistato di seconda mano. In nessun caso si dovrebbe comunque utilizzare un portafoglio hardware usato.

Figura 25: Trezor T.

- Paper wallet

Il metodo più sicuro per la custodia delle chiavi private, è un paper wallet. I paper wallet vengono utilizzati anche dagli hardware wallet per favorire il ripristino del dispositivo. Come si intuisce dal nome, un paper wallet è un portafoglio la cui chiave privata non viene mai utilizzata su dispositivi online, ma ne viene stampata la frase seed ed è perfetto per mantenere un cold wallet.
La stampa, quindi, deve essere conservata in un luogo sicuro. Solitamente le chiavi vengono stampate anche sotto forma di codici QR che si potranno scansionare in futuro per effettuare le transazioni. Il motivo per cui è così sicuro è che l'utente ne ha il completo controllo con il vantaggio di non incorrere negli stessi pericoli di perdita di un brain wallet o nella collisione della frase seed.
Questo tipo di portafoglio non favorisce le operazioni e le transazioni in quanto effettuare una transazione non è immediato come con un hardware wallet, ma permette di ottenere il massimo grado di sicurezza.
Esistono diversi siti sulla quale possono essere generati paper wallet, un esempio è wallet generator.net (Figura 26) che permette la creazione del wallet, è open-source, quindi è possibile controllare che le chiavi non vengano effettivamente salvati da terzi ed offre il template di stampa.

Figura 26: Generatore di paper wallet.

È comunque importante generare il paper wallet offline, siccome è esattamente il problema di avere un dispositivo connesso alla rete quello per cui si dovrebbe creare un paper wallet per il cold storaging.
Al fine di utilizzare il generatore di paper wallet offline, è necessario scaricare il sorgente da Github ed edeguire il file "index.html".
Completata l'operazione di generazione e stampa, è necessario eliminare il sorgente scaricato, dopodichè è possibile riconnettersi ad internet.
Se non ci si vuole comunque affidare ad un servizio terzo, è in ogni caso possibile generare una chiave privata offline e crearne il paper wallet manualmente.

Sebbene un paper wallet sia il metodo meno rischioso in ambito finanziario, non esiste nessun metodo capace di azzerare i rischi di una perdita di fondi.
Anche i paper wallet sono soggetti a problemi di sicurezza quali:

coercizione: ci saranno sempre persone disposte a infrangere la legge pur di ottenere qualcosa di prezioso. Un criminale potrebbe introdursi nel posto in cui viene custodito il portafoglio e appropriarsene con la forza;

fragilità: siccome si tratta pur sempre di carta, essa può danneggiarsi facilmente o usurarsi nel tempo. Per questo motivo, se ne dovrebbero sempre avere più copie;

furto: poiché è scritto su un pezzo di carta, chiunque possa leggerlo o fotografarlo può rubare le monete digitali contenute nel wallet;

non immune ai disastri: è solo un pezzo di carta, non è immune ai disastri naturali e può essere facilmente distrutto e generare una perdita se non ne è stato effettuato alcun backup;

tipo di stampante utilizzata: la qualità della stampante utilizzata può anche avere un effetto negativo. Le stampanti non laser possono far colare l'inchiostro se la carta si bagna;

errori umani: gli esseri umani sono inclini agli errori e si potrebbe semplicemente dimenticare la posizione del portafoglio o strapparlo accidentalmente.

In conclusione, il valore economico, per quanto si possano prendere tutte le precauzioni possibili, è sempre a rischio, nonostante le monete digitali offrano una sicurezza estremamente più alta rispetto ai metodi tradizionali è comunque possibile incorrere nella perdita degli asset posseduti.

7. Conclusioni

In questo documento abbiamo analizzato lo stato dell'arte e gli strumenti di sviluppo della tecnologia BC individuando i punti di forza ed eventuali mancanze dei progetti disponibili sul mercato e conseguentemente i requisiti di un progetto che sia scalabile, sicuro ed attraente.
Abbiamo analizzato come è possibile distribuire le monete digitali, mettendo in sicurezza il network attraverso gli incentivi, in modo che anche l'utente possa beneficiare del rapporto instaurato con il progetto in cui crede e con i relativi founder.
Abbiamo valutato la compatibilità della tecnologia BC con la già esistente infrastruttura ENEA in ottica del raggiungimento della scalabilità e della decentralizzazione e proposto le migliori piattaforme SC compatibili EVM che possono essere utilizzate con essa.
Abbiamo infine analizzato i requisiti di una sicura custodia delle chiavi private, al fine di ridurre al minimo il rischio della perdita dei fondi custoditi.

8. Riferimenti bibliografici

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, Cryptography Mailing list at https://metzdowd.com, (2009).
[2] A. Back, “Hashcash - A Denial of Service Counter-Measure”, (2002).
[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, (2014).
[4] S. De Angelis, L. Aniello, F. Lombardi, A. Margheri, V. Sassone, “PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain”, (2017).
[5] B. Chase, E. MacBrough, “Analysis of the XRP Ledger Consensus Protocol”, (2018).
[6] A. Kiayias, A. Russell, B. David, R. Oliynykov, “Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol”, In: Katz J., Shacham H. (eds) Advances in Cryptology – CRYPTO 2017, CRYPTO 2017, Lecture Notes in Computer Science, vol 10401, Springer, Cham. https://doi.org/10.1007/978-3-319-63688-7_12, (2017).
[7] M. Möser, K. Soska, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, J. Hennessey, A. Miller, A. Narayanan, N. Christin, “An Empirical Analysis of Traceability in the Monero Blockchain”. Proceedings on Privacy Enhancing Technologies. (2018) 143-163. 10.1515/popets-2018-0025.
[8] K. Qin, L. Zhou, B. Livshits, A. Gervais, “Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit”. ArXiv, abs/2003.03810, (2020).
[9] D. Mark, V. Zamfir, E. G. Sirer, “A Call for a Temporary Moratorium on ‘The DAO’”, (2016).
[10] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, N. Zeldovich, “Algorand: Scaling Byzantine Agreements for Cryptocurrencies”, Proceedings of the 26th Symposium on Operating Systems Principles, (2017).
[11]D.Schwartz, N. Youngs,A. Britto, “The Ripple Protocol Consensus Algorithm”, Ripple Labs Inc, (2014).
[12] Tether Limited, “Tether: fiat currencies on the Bitcoin blockchain”, (2016).
[13] S. Ellis, A. Juels, S. Nazarov, “ChainLink: A Decentralized Oracle Network”, (2017).
[14] Binance whitepaper, (2017).
[15] N. Van Saberhagen, “Cryptonote v 2.0”, (2013).
[16] Kyber Network, BitGo Inc., Republic Protocol, “Wrapped Tokens A multi-institutional framework for tokenizing any asset”, (2019).
[17] Tron Foundation, “Tron: Advanced Decentralized Blockchain Platform”, (2018).
[18] Maker Fundation, “The Maker Protocol: MakerDAO’s Multi-Collateral Dai (MCD) System”, (2017).
[19] AAVE Protocol Whitepaper, (2020).
[20] S. Popov, “The Tangle”, (2018).
[21] H. Adams, N. Zinsmeister, D. Robinson, “Uniswap v2 Core”, (2020).
[22] Brave Software, “Basic Attention Token (BAT) Blockchain Based Digital Advertising”, (2018).
[23] S. Kamvar, M. Olszewski, R. Reinsberg. “Celo: A Multi-Asset Cryptographic Protocol for Decentralized Social Payments”, (2018).
[24] Swipe whitepaper, (2019).
[25] T. E. Jedusor, “Mimblewimble”, (2016).
[26] A. Poelstra, “Mimblewimble”, (2016).
[27] Energy Web Foundation, “The Energy Web Chain: Accelerating the Energy Transition with an Open-Source, Decentralized Blockchain Platform”, (2018).
[28] M. J. Krause, T. Tolaymat, “Quantification of energy and carbon costs for mining cryptocurrencies”, (2018).
[29] Proof of Stake versus Proof of Work White Paper, (2016).
[30] V. Buterin, “On Stake”, (2014).
[31] S. Dziembowski, S. Faust, V. Kolmogorov, K. Pietrzak, “Proofs of Space”, (2015).
[32] M.B. Taylor, “The Evolution of Bitcoin Hardware”, (2017).
[33] C. Percival, “Stronger key derivation via sequential memory-hard functions”, (2009).
[34] E. Duffield, K. Hagan, “Darkcoin: Peer-to-Peer Crypto-Currency with Anonymous Blockchain Transactions and an Improved Proof-of-Work System”, (2014).
[35] G. Bertoni, J Daemen, M. Peeters, G. Van Assche, “Keccak and the SHA-3 Standardization”, (2013).
[36] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, ”Sponge Functions, Ecrypt Hash Workshop”, (2007).

[37] R. Rivest, A. Shamir, Y.T. Kalai, “How to leak a secret”, ASIACRYPT 2001. Volume 2248 of Lecture Notes in Computer Science (2001), pages 552–565.
[38] A. Biryukov, D. Khovratovich, “Equihash: Asymmetric Proof-of-Work Based on the Generalized Birthday Problem”. Ledger, 2, (2017), 1-30.
[39] J. Tromp, “Cuckoo Cycle: a memory bound graph-theoretic proof-of-work”, (2014).
[40] Top500. [Online]. Available: https://www.top500.org/.
[41] T. Kalmi, “Comparison of Blockchain-based Technologies for Implementing Community Currencies”, Aalto University, (2018).
[42] T. Kuo, H. Z. Rojas, L. O. Machado, “Comparison of blockchain platforms, a systematic review and healthcare examples”, (2019), pp. 462-478.
[43] Atmosphere Arc Ecosystem, https://www.atmospherearc.com, 2019.

9. Abbreviazioni ed acronimi

Se nel rapporto si fa uso di molte abbreviazioni e acronimi si suggerisce di inserire un elenco alla fine del documento, i termini devono comunque essere definiti anche all'interno del testo la prima volta che vengono utilizzati.

FPGA	Field Programmable Gate Array
BTC	Bitcoin
ETH	Ether
SC	Smart Contracts
ASIC	Application specific integrated circuit
PoW	Proof of Work
PoS	Proof of Stake
BC	Blockchain
ICO	Initial Coin Offering
DeFi	Decentralized Finance
DEX	Exchange decentralizzato
EVM	Ethereum Virtual Machine
UTXO	Unspent transaction output
DAO	Organizzazioni decentralizzate
PC	Program Counter o Contatore di Programma
BSC	Binance Smart Chain
PoA	Proof of Authority
IoT	Internet of Things

Appendice - breve curriculum collaboratori esterni ad ENEA

○ *Università degli studi di Salerno*

Gerardo Iovane è nato a Salerno il 05/05/1972. Fra gli studi e i titoli possiede: dottorato di Ricerca in Ingegneria ed Economia dell'Innovazione; dottorato di Ricerca in Matematica presso l'Universita' degli Studi di Salerno; dottorato di ricerca in Fisica, Università di Salerno; titolato IASD (Istituto Alti Studi della Difesa); laurea in Fisica conferita con Lode conseguita il 23 Luglio 1996 presso la Facoltà di Scienze Matematiche, Fisiche e Naturali dell'Università degli Studi di Salerno; diploma di Maturità Scientifica conseguito presso la Scuola Militare "Nunziatella" di Napoli.
E' Professore Associato in Analisi Matematica (MAT/05) presso il Dipartimento di Ingegneria dell'Informazione e Matematica Applicata dell'Università degli Studi di Salerno; esperto Scientifico Nazionale al Ministero delle Politiche Agricole e Forestali; esperto Scientifico Nazionale al Ministero dell'Università e della Ricerca; responsabile di diversi progetti di modelli matematici per analisi dell'immagine; responnonsabile Nazionale del FIRB "CASHMA"; coordinatore Scientifico del team di Ricerca FINTECH Blockchain (Financial Computing technologies and Blockchain); regional Editor for Europe di Chaos, Solitone & Fractals, edito dalla Elsevier; associated Editor di International Journal of Innovative Computing, Information and Control (IJICIC); editor in Chief della Rivista Internazionale "Mathematical Methods, Physical Models and Simulations in Science & Technology" della General Research Publications ed editor in Chief della Rivista Internazionale "Transaction on Applied Mathematics and Nonlinear Models".
Autore di monografie e libri e più di 100 articoli scientifici, saggi e discorsi per convegni nazionali e internazionali. E' il fondatore e coordinatore internazionale dell'ecosistema Blockchain Atmosphere Arc [43], presente su 24 Stati, avendo per primo coniato il termine di Economia Decentralizzata, dopo che l'ecosistema si è popolato con circa 20 iniziative di digital transformation, come nominato da Forbes USA nell'Ottobre 2020, quale esperienza nata in Italia, ma di interesse strategico globale, che accoglie non semplicemente diverse monete e token, ma piuttosto interi settori economico-produttivi, quali ad esempio, Energia, Ambiente, Logistica, Finanza, Sicurezza, Costruzioni, Bellezza, Salute, Sport, Benessere, ecc.

Antonio Rapuano è nato a Benevento il 23/05/1993. Si laurea in Informatica con lode all'Università degli Studi di Salerno nel 2018. Sempre all'Università degli studi di Salerno è, prima, assegnista di ricerca nel 2019 presso il Biometric and Image Processing Laboratory (BIPLAB) e poi PhD student in Financial Computing Technologies and Blockchain. Autore di diversi articoli scientifici in ambito blockchain, privacy, teoria della probabilità, robotica e biometria discussi a diverse conferenze internazionali. E' inoltre CTO dell'ecosistema Blockchain Atmosphere Arc [43].