POLITECNICO DI TORINO

Blockchain e Criptoeconomia

LA CRIPTOMONETA DASH

Gaia Galizia s319707
Domenico Pittalis s333999
Giovanni Pizzenti s332941
Marco Rosella s319706
Andrei Zarau s334073

Anno Accademico 2023-2024

Indice

Sommario

Nel Gennaio del 2014, Evan Duffield ha lanciato la criptomoneta XCoin, nata come fork di Litecoin, a sua volta fork di Bitcoin. Negli anni ha cambiato più volte nome, passando da DarkCoin e infine diventando Dash, corto per *Digital Cash*. Questa criptovaluta nasce dalla necessità di risolvere alcuni problemi relativi alla rete Bitcoin, focalizzandosi sulla riservatezza elle transazioni e riducendo i tempi necessari per confermarle. Con queste nuove implementazioni, la rete Dash consente di inviare denaro con bassi costi e in modo rapido ovunque nel mondo, basta essere connessi ad Internet. Nelle pagine seguenti spiegheremo le caratteristiche di questa criptomoneta e vedremo quali sono i suoi punti di forza, evidenziandone vantaggi e svantaggi.

Capitolo 1

Introduzione

Dash è una criptovaluta basata su blockchain decentralizzata, su cui gli utenti possono effettuare delle transazioni che vengono salvate sulla rete in maniera anonima. Come molte criptomonete, il metodo di generazione della moneta è basato sul mining. In questo breve capitolo abbiamo riportato alcune utili definizioni per la comprensione di quello che riguarda la trattazione seguente.

1.1 Blockchain

La blockchain è una tecnologia basata su registri distribuiti che permette di memorizzare dati in maniera decentralizzata ma al contempo affidabile. Il sistema è composto da blocchi collegati tra di loro contenenti insiemi di transazioni o di dati, in maniera da poter formare una sequenza continua e verificabile definita catena. Grazie al modo in cui vengono implementati questi collegamenti, i vari blocchi vengono resi interdipendenti, cosi da non poter alterare un blocco senza influenzare i successivi, e questa è una delle sue caratteristiche piu importanti in quanto la rende resistente alle manomissioni esterne. Questa struttura è alla base delle criptovalute come Dash, ma può trovare impiego anche in molteplici ambiti tra cui smart contracts, supply chain o votazioni elettroniche.

1.2 Wallet

I wallet sono dei portafogli digitali usati per gestire critpovalute. Sono dei conenitori sicuri in cui memorizzare le chiavi crittografiche necessarie per effettuare transazioni all'interno della blockchain ma non contengono fisicamente le criptovalute. All'interno dei wallet le chiavi pubbliche

servono come indirizzo per ricevere i fondi e quelle private per autorizzare le transazioni in uscita. La perdita della chiave privata è sinonimo della perdita del wallet e dei conseguenti contenuti, perciò va custodita con cura.

1.3 Transazioni

Le transazioni all'interno di una blockchain iniziano quando un utente desidera inviare denaro o dati a un altro utente. Il mittente crea una transazione firmata digitalmente con la sua chiave privata, specificando importo e destinatario (identificato dalla chiave pubblica). Una volta dichiarata, la trandsazione viene immessa nella rete di nodi che partecipano alla blockchain in questione. I nodi effettuano le opportune verifiche di validità della transazione e una volta confermata viene raggruppata assieme ad altre in un unico blocco. Questo nuovo blocco deve essere validato attraverso i cosiddetti protocolli di consenso dai membri della blockchain: i protocolli che variano in base alla specifica soluzione adottata. Una volta validato, il blocco viene aggiunto alla blockchain e la transazione viene considerata confermata e permanente.

1.4 Mining

Il mining è un processo attraverso il quale nuove transazioni vengono verificate e aggiunte alla blockchain. Nei sistemi che possiedono protocolli di consenso basati sulla Proof of Work, il mining prevede la risoluzione di problemi matematici usando potenza computazionale, in modo da dimostrare un "lavoro" fatto prima di inserire un blocco. Questo lavoro è computazionalmente lungo, a seconda dei requisiti richiesti, e assicura che la rete non venga invasa da blocchi illeciti. Chiunque può diventare un miner, a patto che abbia accesso alle opportune risorse, e competere con altri miner per riuscire a risolvere per primo i problemi computazionali, venendo cosi anche remunerati.

Capitolo 2

Dash

2.1 Cos'è Dash e perché utilizzarlo

Dash nasce nel 2014 da un'idea di Evan Duffield per offrire una soluzione ai problemi di privacy, scalabilità, velocità delle transazioni ed efficienza energetica di Bitcoin. Dal momento che è nato come fork di Litecoin, a sua volta fork di Bitcoin, Dash è completamente decentralizzata e possiede un database con tutte le transazioni, conservato su migliaia di computer in tutto il mondo, che viene utilizzato per effettuare i dovuti controlli sulla correttezza delle transazioni. La rete Dash è quindi distribuita e le transazioni vengono verificate da persone che contribuiscono nella rete e che quindi sono parte integrante dell'intero sistema.
Con Dash è possibile inviare denaro con bassi costi e in modo rapido ovunque nel mondo, basta essere connessi ad Internet, e può essere utilizzato indipendentemente dal paese in cui ci si trova, dall'orario e dall'importo che si desidera trasferire. Le criptovalute come Dash, hanno al loro interno delle implementazioni che garantiscono matematicamente che tali scambi (transazioi) siano corretti, ovvero non vi sia il problema del *double spending*[1].
Inoltre, le commissioni per le transazioni Dash sono convenienti, con costi inferiori a un centesimo, indipendentemente dall'importo inviato: questo suggerisce che Dash possa essere un'ottima soluzione per il commercio e gli scambi. Anche la funzionalità di privacy consentita

[1]Per via dei tempi di validazione della transazione un utente potrebbe usare gli stessi DASH per effettuare contemporaneamente due transazioni

da *PrivateSend* [2.4] è un ottimo valore per gli utenti, poiché mantiene l'anonimato nelle transazioni. Infine, il funzionamento di *Masternodes* [3] protegge Dash dagli attacchi, poiché un utente malintenzionato dovrà possedere almeno il 51% della rete totale per attaccarla. Approfondiremo in seguito la questione.

2.2 Tipi di Nodi

Esistono tre tipi di nodi nella blockchain Dash:

1. **Nodi ordinari**: Come in ogni altra criptovaluta, sono considerati la spina dorsale della catena e la loro funzione principale è quella di rendere sicura la blockchain e di prevenire il double spending. Memorizzano dati parziali del registro della blockchain, scaricando solo le intestazioni dei blocchi.

2. **Nodi completi**: Detengono un'intera copia della blockchain in tempo reale e possono inoltre connettersi a oltre 124 altri nodi, mentre gli altri nodi possono connettersi solo a 8. Questa maggiore connettività permette ai nodi completi di avere una visione più completa della rete, migliorare la propagazione delle transazioni e dei blocchi, e supportare funzionalità avanzate come *InstantSend* e *PrivateSend*.

3. ***Masternodes*** : Hanno una copia completa della blockchain e per svolgere questo copito devono depositare 1000 DASH in un fondo che funge da garanzia. Questi DASH possono essere ripresi in qualsiasi momento, ma questo fa perdere lo status di Masternode al nodo. Solo i *Masternodes* possono votare le proposte di modifica di Dash e per questo motivo hanno molto potere, ma la quantità di DASH depositata li disincentiva dal commettere abusi sfruttando il loro status.

2.3 *InstantSend*

In una situazione di vendita al dettaglio nel mondo reale, commercianti e clienti necessitano di conferme veloci per le transazioni. Le criptovalute decentralizzate tradizionali devono attendere un certo periodo di tempo affinché un numero sufficiente di blocchi venga aggiunto alla blockchain, sia per garantire che una transazione sia irreversibile, sia per evitare tentativi di double-spending. Questo processo richiede tempo da alcuni

minuti minuti a un'ora nei protocolli più comuni. Altre invece ottengono tempi di conferma delle transazioni più rapidi attraverso un'autorità centrale che governa la rete. Dash non soffre di nessuna di queste limitazioni grazie alla sua rete di *Masternodes*, che permette di implementare la funzione *InstantSend*:

1. **Blocco temporaneo delle monete**: Quando un utente decide di utilizzare *InstantSend*, le monete coinvolte nella transazione vengono temporaneamente bloccate tramite una rete di *Masternodes*.

2. **Verifica da parte dei *Masternodes***: Un gruppo di *Masternodes* selezionato casualmente (Quorum) viene incaricato di verificare e confermare la transazione. Questi *Masternodes* eseguono una serie di controlli per assicurarsi che le monete siano disponibili e che la transazione sia valida. Una volta che la maggioranza di questo gruppo approva la transazione, essa viene considerata bloccata e pronta per l'inclusione nel blocco successivo della blockchain.

3. **Conferma istantanea**: La transazione viene confermata in pochi secondi, permettendo al destinatario di considerarla immediatamente valida e sicura.

4. **Inclusione nel blocco successivo**: Anche se la transazione è confermata istantaneamente dai *Masternodes*, essa viene comunque inclusa nel successivo blocco della blockchain per garantire una registrazione permanente e immutabile.

I compromessi sono però:

- **Commissioni**: Le transazioni *InstantSend* possono comportare commissioni leggermente più elevate rispetto alle transazioni standard per compensare i *Masternodes* che partecipano al processo di verifica.

- **Importi delle transazioni**: *InstantSend* è progettato per funzionare al meglio con transazioni di dimensioni moderate. Le transazioni molto grandi potrebbero non essere supportate o potrebbero richiedere tempi di conferma più lunghi.

2.4 *PrivateSend*

PrivateSend non è altro che l'implementazione in Dash del meccanismo Coinjoin, ovvero una strategia di elaborare le transazioni che viene utilizzata per mantenere l'anonimato sulla rete. Per illustrare la strategia

adottata in sintesi, i propri DASH vengono mescolati con quelli delle transazioni di almeno altri due utenti in modo tale da ottenere che gli ingressi nel proprio portafoglio siano costituiti da transazioni provenienti da utenti diversi.

Le fasi che caratterizzano *PrivateSend* sono:

1. **Denominazioni standard**: Si inizia suddividendo l'input della propria transazione in denominazioni standard: 0.001, 0.01, 0.1, 1 e 10 DASH, simili ai tagli delle banconote in uso nelle valute come l'Euro.

2. **Richiesta ai *Masternodes***: Dal proprio wallet vengono inviate richieste ai *Masternodes*, informandoli dell'itenzione di utilizzare *PrivateSend*. Nessuna informazione identificabile viene inviata ai *Masternodes*, quindi non è possibile nemmeno per loro rintracciare il richiedente.

3. **Inizio della sessione**: Quando almeno altri due utenti decidono di inizializzare una transazione con *PrivateSend* indicando che desiderano usare monete della stessa denominazione, inizia una sessione. Il *Masternode* mescola queste denominazioni e le ridistribuisce a dei nuovi indirizzi controllati da ciascun utente (chiamati indirizzi di cambio).

4. **Ripetizione del processo**: Un wallet può ripetere questo processo più volte per ogni denominazione. Ogni processo di questo tipo si chiama "round" e un utente può scegliere quanti effettuarne in un range che va da 2 a 16 round.

5. **Round aggiuntivi**: I fondi passano attraverso il numero di round specificato. Dash 0.16 include un aggiornamento noto come *Random Round CoinJoin*, che unisce una determinata denominazione per tre round extra per migliorare ulteriormente la privacy.

Questo processo avviene in background senza alcun intervento da parte dell'utente. Ogni qual volta egli desiderasse effettuare una transazione utilizzando i propri fondi denominati, può farlo senza la necessità di attendere altre operazioni.
Le transazioni *PrivateSend* vengono arrotondate per far sì che tutti gli input della transazione vengano spesi. Eventuali DASH in eccesso vengono utilizzati per coprire le commissioni di transazione. Ogni wallet contiene solo 1000 di questi indirizzi di cambio. Ogni volta che viene creata una transazione *CoinJoin*, uno dei propri indirizzi viene utilizzato

e una volta che vengono esauriti, il portafoglio deve creare dei nuovi indirizzi.
I vantaggi di *PrivateSend* sono:

1. **Privacy**: Il processo di mixaggio rende difficile per chiunque tracciare l'origine e la destinazione delle monete. Anche se qualcuno analizzasse la blockchain, non sarebbe in grado di determinare con precisione quali monete appartengono a quale utente.

2. **Facilità d'uso**: *PrivateSend* è integrato nel wallet Dash, rendendo facile per gli utenti comuni utilizzare questa funzionalità senza bisogno di configurazioni complicate.

3. **Trasparenza**: Anche se le transazioni sono mescolate, tutte le transazioni di *PrivateSend* sono ancora registrate sulla blockchain pubblica di Dash. Questo garantisce che Dash rimanga una criptovaluta trasparente e verificabile, pur offrendo una maggiore privacy.

Gli svantaggi invece sono:

1. **Costo**: L'uso di *PrivateSend* può comportare commissioni aggiuntive rispetto alle transazioni normali, poiché richiede più transazioni e il coinvolgimento dei *Masternodes*.

2. **Limitazioni di importo**: *PrivateSend* è più efficace per importi che possono essere facilmente suddivisi nelle denominazioni standard. Importi molto grandi o molto piccoli possono essere più difficili da mixare efficientemente.

3. **Velocità**: Il processo di mixaggio può richiedere tempo, soprattutto se la rete è congestionata o se ci sono pochi utenti che utilizzano *PrivateSend* in un dato momento.

2.5 Governance

La governance in Dash è un sistema di decision-making decentralizzato che consente ai possessori di DASH, in particolare ai *Masternodes*, di partecipare attivamente alla gestione e allo sviluppo della rete. Questo meccanismo di governance consente alla comunità di prendere decisioni collettive riguardo alle modifiche del protocollo, al finanziamento di progetti e ad altre questioni cruciali per il futuro della criptovaluta, grazie anche al sistema di tesoreria che permette al sistema di essere autofinanziato.

2.5.1 Fattori principali

1. ***Masternodes***: Oltre a fornire funzionalità avanzate come *InstantSend* e *PrivateSend*, partecipano attivamente alla governance.

2. **Proposte di Governance**:

   - Chiunque può presentare una proposta di governance alla rete Dash. Le proposte possono riguardare modifiche al protocollo, finanziamento di nuovi progetti, marketing, eventi della comunità o qualsiasi altra iniziativa che possa migliorare l'ecosistema Dash.
   - Per presentare una proposta, è necessario pagare una piccola commissione (attualmente 5 DASH). Questa commissione serve a prevenire spam e garantisce che solo le proposte serie e ben pianificate vengano presentate.

3. **Votazione delle proposte**:

   - I *Masternodes* hanno il compito di votare sulle proposte presentate. Ogni masternode ha un voto.
   - Le proposte vengono discusse e votate durante un periodo di 30 giorni. Una proposta deve ottenere una maggioranza di voti positivi (meno i voti negativi) per essere approvata. In genere, una proposta deve ricevere almeno il 10% del totale possibile dei voti dei *Masternodes* per essere approvata.

4. **Implementazione delle decisioni**:

   - Le proposte approvate ricevono i fondi richiesti dalla tesoreria al termine del ciclo di votazione. I fondi vengono distribuiti direttamente all'indirizzo indicato nella proposta.
   - Le decisioni riguardanti modifiche al protocollo vengono implementate dagli sviluppatori di Dash, con il supporto e la supervisione della comunità.

2.5.2 Vantaggi

1. **Inclusività e Partecipazione**:

   - La governance di Dash permette a chiunque di presentare proposte e partecipare attivamente al futuro della rete. Questo sistema democratico garantisce che le decisioni siano rappresentative degli interessi della comunità.

2. **Flessibilità e Rapidità di Adattamento**:

    - La struttura decentralizzata consente a Dash di adattarsi rapidamente ai cambiamenti e di finanziare nuovi progetti senza dover dipendere da entità centralizzate o esterne.

3. **Sostenibilità Finanziaria**:

    - Per fare questo quando un DASH viene minato il 10% viene depositato nella tesoreria.
    - Il sistema di tesoreria di Dash assicura che ci siano sempre fondi disponibili per supportare lo sviluppo, il marketing e altre iniziative cruciali per la crescita della rete.

4. **Trasparenza e Responsabilità**:

    - Tutte le proposte e i risultati delle votazioni sono pubblici, garantendo trasparenza nel processo decisionale. Gli operatori dei *Masternodes* sono incentivati a prendere decisioni che beneficiano la rete nel suo complesso, poiché il loro investimento è direttamente legato al successo di Dash.

2.5.3 Svantaggi

1. **Coordinazione**:

    - La decentralizzazione implica che il processo decisionale può essere più lento e richiedere maggiore coordinazione tra i partecipanti, rispetto a una struttura centralizzata.

2. **Partecipazione Attiva**:

    - Per garantire che le decisioni siano rappresentative, è importante che un numero sufficiente di *Masternodes* partecipi attivamente al processo di votazione. La scarsa partecipazione potrebbe portare a decisioni non ottimali.

3. **Qualità delle Proposte**:

    - È cruciale che le proposte siano ben pianificate e dettagliate, affinché i *Masternodes* possano prendere decisioni informate. La commissione di presentazione delle proposte aiuta in questo, ma la comunità deve comunque vigilare sulla qualità delle proposte.

2.6 *ChainLocks*

Dash ha implementato *ChainLocks* che, secondo quanto riferito dagli sviluppatori, "eliminerà" la minaccia di un attacco del 51% dal protocollo. Questa è una caratteristica che garantisce sicurezza quando si accettano dei pagamenti. Questa tecnologia, soprattutto quando unsata assieme a *InstantSend*, contribuisce allo svoluppo di un ambiente in cui le transazioni vengono accettate subito e si evita qundi il rischio di "Blockchain Reorganization Events", ovvero possibili sovrapposizioni di blocchi allo stesso livello. Di solito si fronteggia questo problema richiedendo più conferme gli utenti ma questo rallenta la rete e rende più pesante l'esperienza per l'utente. Dash invece implementa proprio la strategia del *ChainLocks*, in cui gli attori principali sono i *Masternodes*. Ecco come funziona *Chainlock*:

1. Ogni 12 ore viene sorteggiato un nuovo Long-Living Masternode Quorum (LLMQ) di alcuni centinaia di masternode (solitamente 300-400)

2. quando viene minato un blocco, ciascun membro del Quorum diffonde agli altri membri un messaggio firmato contenente il primo blocco della catena che vede a livello attuale. Gli LLMQ sono costituiti da masternode selezionati casualmente, il che li rende ampiamente rappresentativi dell'insieme totale. Poiché gli LLMQ sono peculiari della rete Dash, questa è l'unica rete in grado di implementare *Chainlocks*.

3. Se abbastanza membri (almeno il 60%) hanno indicato lo stesso blocco come blocco di livello corrente, diffondono al resto della rete un messaggio *Chainlock Signature* (CLSig) e propagarlo a tutti i nodi nella rete.

4. Se un nodo riceve un messaggio CLSig valido, deve respingere tutti i blocchi alla stessa altezza che non corrispondono al blocco specificato nel messaggio CLSig.

Il fatto che gli LLMQ sono una parte dei masternode scelti causalmente è una soluzione all'attacco del 51% poiché non si ha sempre la sicurezza che il 51% dei sorteggiati per LLMQ di un determinato blocco sia appartenente al 51% totale.

2.7 Commissioni

Le commissioni in Dash possono essere applicate in varie occasioni:

- **Transazione**: Ogni transazione sulla rete Dash comporta una piccola commissione, che viene pagata ai miners per includere la transazione nel blocco successivo della blockchain. Questa commissione varia a seconda della dimensione della transazione e della congestione della rete. Attualmente le commissioni si aggirano attorno a 0.00022 DASH/KB ($\sim$ 0.006€/KB) per transazioni ad alta priorità, 0.00018 DASH/KB ($\sim$ 0.005€/KB) per media priorità e 0.00014 DASH/KB ($\sim$ 0.004€/KB) per bassa priorità. Quindi, supponendo che una transazione ha una dimensione media di 0.25 KB e supponendo di spendere 1€ = 0.036 DASH (al prezzo attuale di inizio giugno 2024 pari a circa 1 DASH = 30$), la spesa totale per una transazione ad alta priorità sarà pari a circa 0.036 DASH + 0.00022 DASH/KB * 0.25 KB = 0.036055 DASH = 1.0015€, quindi la commissione totale ammonta a una frazione di centesimo di euro.

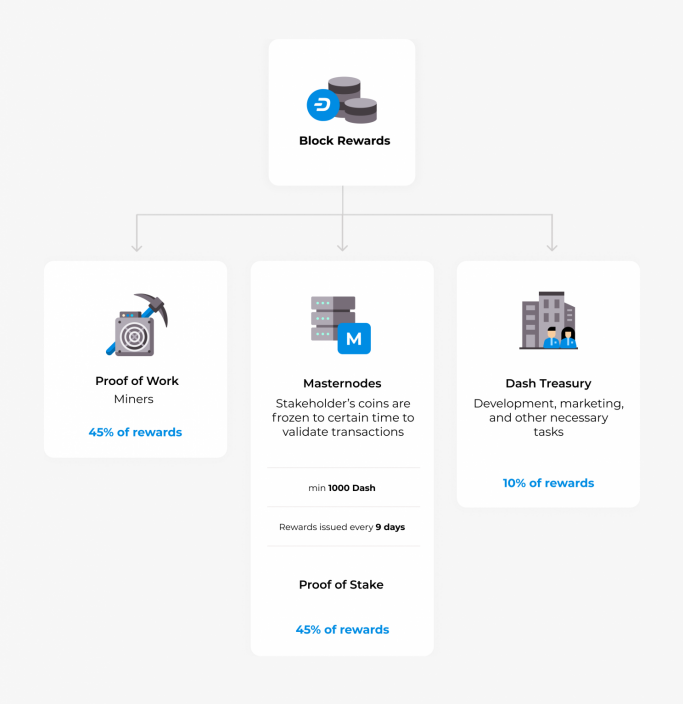
- **Proposte di governance**: Per presentare una proposta di governance alla rete Dash, è necessario pagare una commissione di presentazione (attualmente 5 DASH). Questa commissione serve a prevenire l'invio di proposte non serie e a garantire che solo proposte ben pianificate e significative vengano presentate alla comunità per la votazione.

- **Rimborso**: Questi sono in realtà dei rimborsi delle commissioni pagate dagli utenti che hanno fatto proposte. Il rimborso però viene effettuato solo se la proposta viene approvata e finanziata dalla tesoreria di Dash. Questo meccanismo incentiva i proponenti a presentare proposte di alta qualità che possano ricevere il sostegno della comunità.

- Per utizzare *InstantSend* o *PrivateSend*

2.8 Mining in Dash

Dash condivide l'idea del sistema di mining con Bitcoin e quindi è basato su una Proof of Work[2]. Infatti, tra le grandi differenze con la criptomoneta da cui discende, abbiamo la modifica dell'algoritmo di hashing utilizzato in questa fase, che in Dash si chama X11. Altro aspetto fondamentale è la suddivisione dei compensi quando viene creata nuova moneta. Secondo il whitepaper, il reward totale del blocco appena minato non viene assegnato interamente al miner ma a questo spetta solo il 45% del totale. La restante parte viene divisa tra i *Masternodes* e il fondo di tesoreria comune (un fondo comunitario con cui si paga per lo sviluppo continuo, il marketing e altro ancora) assegnando il 45% del totale ai primi e all'altra il restante 10%. Dopo una proposta[3] approvata nel 2023, dalla v.20.0 di Dash Core è stata introdotta la suddivisione 60-20-20, raddoppiando il quantitativo di DASH che viene posto nel fondo comune e auentando il reward per i masternodes al 60% del totale del blocco, lasciando ai miners il restante 20%.



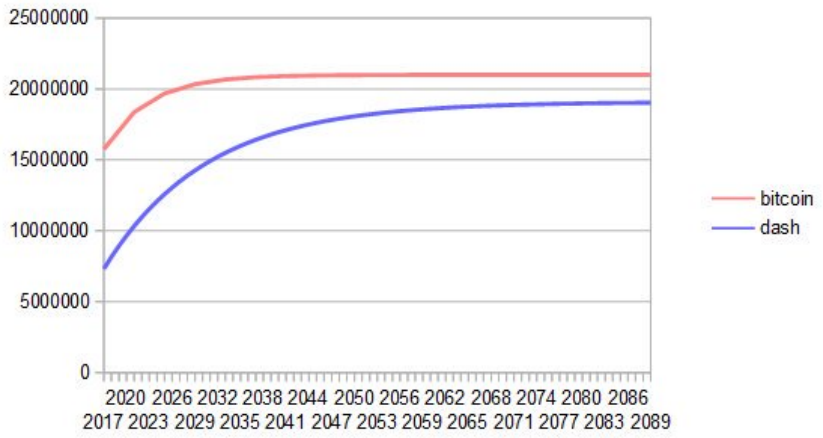
[2]E' il processo attraverso cui si richiede ai miner (partecipanti alla rete Bitcoin) di risolvere complessi problemi matematici per convalidare le transazioni e creare nuovi blocchi, essi in seguito riceveranno un quantitativo (pari al tasso di compenso) di DASH come compenso per il lavoro svolto

[3]https://www.dashcentral.org/p/TREASURY-REALLOCATION-60-20-20

2.9 Emissione

Dash modifica significativamente il tasso di emissione delle monete per offrire una riduzione più graduale nel tempo se confrontata con Bitcoin: mentre Bitcoin riduce il tasso di emissione delle monete del 50% ogni 4 anni, Dash riduce l'emissione di un quattordicesimo (circa il 7,14%) ogni 210240 blocchi, che corrispondono a circa 383,25 giorni considerando che il tempo di inserimento medio di un blocco è 155 secondi. Ai ritmi attuali, attorno a inizio luglio 2024, avverrà la decima riduzione dal lancio della criptomoneta con l'inserimento del blocco numero 2102401, e il reward per l'inserimento di un blocco passerà dai 2.48734 DASH attuali a 2.30974 DASH.
Per quanto riguarda la quantità totale totale di DASH che verranno emessi, questa è la somma di una serie geometrica che tende al valore 18.9 mln DASH, ma il quantitativo totale finale è incerto perché non è possibile sapere quanto del 20% della parte riservata alle proposte di bilancio verrà effettivamente allocato, poiché ciò dipende dal comportamento futuro dei votanti. Secondo alcune stime, Dash continuerà a emettere monete per circa 192 anni prima che in un anno completo di mining venga creato meno di 1 DASH. Dopo il 2209 verranno creati solo altri 14 DASH e l'ultimo DASH richiederà 231 anni per essere generato, iniziando nel 2246 e terminando quando l'emissione si fermerà completamente, ovvero nel 2477. In base a questi numeri, è possibile calcolare una stima dei quantità massima e minima di monete nell'anno 2254 tra:

- 17.742.696 DASH (senza allocazione della tesoreria)
- 18.921.005 DASH (con allocazione completa della tesoreria)



2.10 Dash nella vita quotidiana

Dash offre pagamenti istantanei peer-to-peer con commissioni molto basse ed è attualmente accettato da migliaia di commercianti in tutto il mondo. La comunità Dash sta spingendo soprattutto i commercianti all'adozione della propria criptomoneta attraverso una serie di programmi divulgativi e la sua continua innovazione. E' chiaro che la velocità di conferma è un elemento fondamentale per le transazioni negli acquisti quotidiani e questa caratteristica è sicuramente molto importante per un qualsiasi venditore o acquirente ed è la stessa ragione per cui per le transazioni quotidiane si preferisce la valuta reale rispetto all'assegno. Infatti, mentre una trasferisce immediatamente il valore, l'altra deve essere trasformata. Dash si distingue da altre monete digitale presentando idee innovative per soddisfare i requisiti di velocità, dando una vera possibilità per l'adozione diffusa di questa criptomoneta in tutti i settori.
Un esempio di utilizzo di Dash, è Dash Text, uno strumento popolare in Spagna, Venezuela, Colombia, Stati Uniti e altri paesi. Dash è stato integrato per l'utilizzo con Telegram ed è stato adottato dall'app di messaggistica. Il Dash Text consente l'invio e la ricezione di DASH tramite messaggi di testo ed è disponibile direttamente sugli smartphones. Ciò rende possibile l'inclusione di più persone anziché di pochi utenti che hanno competenze avanzate a livello informatico. Queste idee aprono l'adozione a chiunque, ovunque, con o senza competenze tecniche e aumenteranno l'inclusione finanziaria.

2.11 Evoluzione di Dash

Il team di Dash ha lavorato a un progetto chiamato Evolution, che porterà Dash a diventare molto popolare e utilizzata. Dash Evolution ha lo scopo di consentire l'utilizzo della criptovaluta ai venditori al dettaglio e ai commercianti, sebbene le specifiche tecniche siano complesse. Gli utenti saranno in grado di scambiarsi fondi con nomi utente anziché con indirizzi anonimi, rendendo l'intera piattaforma molto più facile da usare. Dash Evolution è una piattaforma di pagamento decentralizzata basata sulla tecnologia blockchain Dash il cui obiettivo è fornire un accesso semplice alle funzionalità e ai vantaggi unici di Dash per assistere nella creazione di tecnologia decentralizzata. Dash introduce un design di rete a più livelli, che consente agli utenti di svolgere vari lavori per la rete, insieme all'accesso API decentralizzato e a un file system decentralizzato. Inoltre, Evolution consentirà agli sviluppatori di

creare applicazioni decentralizzate senza la necessità di eseguire un nodo completo, poiché tale sviluppo verrà eseguito su hosting decentralizzato.

Capitolo 3

Proof of Work: algoritmo X11

Dash, come altre criptomonete, utilizza la proof of work (PoW) come algoritmo di consenso per autorizzare le transazioni attraverso il mining di nuovi blocchi che vengono di volta in volta aggiunti alla fine della blockchain. Come Bitcoin, l'obiettivo di un miner di Dash è quello di competere con gli altri miners sulla risoluzione di un complesso problema matematico, attraverso l'utilizzo di un determinato algoritmo. Questo problema consiste nell'applicare una funzione hash a un valore composto dal blocco precedente e da un *nonce* per trovare un numero inferiore a un valore target, rendendo quindi la ricerca del nonce il vero lavoro difficile per il miner. Chiaramente, il primo che raggiunge l'obiettivo è colui che riceverà la ricompensa in DASH (come abbiamo detto, il 45% della ricompensa totale del blocco che si sta inserendo). La particolarità di questa criptovaluta in questa specifica fase, è quella di utilizzare l'algoritmo X11 come algoritmo di mining: questo, al posto di servirsi di una singola funzione hash (come fa SHA-256 di Bitcoin), ne raccoglie 11 che vengono applicate in un ordine specifico al nonce per ottenere il valore che risolve il problema della proof of work.

3.1 Origine

X11 è nato a marzo 2014, quando lo sviluppatore Evan Duffield ha presentato il progetto di criptovaluta DarkCoin, oggi noto con il nome Dash. Duffield aveva evidenziato come Bitcoin avesse alcuni difetti che potevano essere superati grazie a questa idea. Tra questi, la mancanza di scalabilità, un miglioramento della privacy, una migliore possibilità

di anonimato e resistenza agli ASIC per evitare la centralizzazione del mining. Egli riteneva, infatti, che in Bitcoin l'eccessiva semplicità dello SHA-256 avrebbe potuto causare un brusco crollo dei prezzi della criptovaluta poiché era probabile che la maggior parte di essa fosse nelle mani di poche grandi mining pool, come in effetti avviene oggi. L'introduzione dell'hashing sequenziale, ha aumentato significativamente la protezione contro l'hacking: lo sviluppatore stesso ha ripetutamente sottolineato che molti investitori hanno paura di investire in Bitcoin e altre monete a causa del fatto che l'algoritmo di SHA-256 non può essere definito al 100% protetto dall'hacking. La presentazione di questo progetto ha attirato l'attenzione della comunità crittografica, soprattutto per la sua capacità di offrire l'anonimato e, naturalmente, questo suo straordinario algoritmo di mining. Questo algoritmo era qualcosa di nuovo e mai visto, per cui molti nella comunità hanno deciso di studiarne le possibilità di applicazione. Di conseguenza, è nato uno sviluppo completamente nuovo, tra cui algoritmi come X13 e X17, che seguono lo stesso schema di lavoro di X11 ma utilizzando delle funzioni hash in più per svolgere il proprio lavoro.

3.2 Algoritmo X11

La peculiarità di X11 è la concatenazione di undici algoritmi di hashing che vengono quindi implementati uno dopo l'altro. L'input di questo algoritmo è una sequenza binaria di lunghezza arbitraria e la successione di funzioni produce in conclusione un digest di 256 bit (32 byte). Gli algoritmi di hashing implementati sono i seguenti e vengono eseguiti in questo ordine:

1. **BLAKE**: Progettato per essere rapido e sicuro, è stato finalista nel concorso SHA-3. Utilizza una struttura di compressione basata su ARX (Addizione, Rotazione e XOR).

2. **BMW (Blue Midnight Wish)**: Conosciuto per la sua velocità e sicurezza, BMW utilizza una struttura di compressione unica che è stata progettata per essere altamente parallela.

3. **Groestl**: Questo algoritmo di hash utilizza una funzione di permutazione interna basata su AES (Advanced Encryption Standard). È particolarmente forte contro attacchi di pre-immagine e collisione. Finalista del concorso SHA-3.

4. **JH**: Ancora un finalista di SHA-3, utilizza una rete a sostituzione e permutazione con un'architettura a più fasi. È progettato per offrire un alto livello di sicurezza.

5. **Keccak** [vedi 3.2.1]: Vincitore del concorso SHA-3, Keccak utilizza una costruzione a spugna che permette un alto grado di sicurezza e flessibilità. E' noto per la sua resistenza alle collisioni e agli attacchi di pre-immagine.

6. **Skein**: Basato su una rete di cifratura chiamata Threefish, Skein è altamente flessibile e può essere configurato per diverse dimensioni di output. È noto per la sua velocità e sicurezza. Finalista anch'esso del concorso SHA-3.

7. **Luffa**: Utilizza una rete di permutazione che è efficiente sia in termini di velocità che di sicurezza.

8. **CubeHash**: Progettato con una struttura a permutazione a cubi, è noto per la sua semplicità e robustezza contro attacchi crittografici.

9. **SHAvite-3**: Quest'algoritmo è progettato per essere semplice e sicuro, utilizzando una struttura di rete basata su AES (Advanced Encryption Standard).

10. **SIMD**: Utilizza una struttura basata su una rete di Feistel e offre un alto livello di sicurezza e prestazioni.

11. **ECHO**: Echo è progettato per essere sicuro e performante, con un'architettura che permette un'efficiente implementazione su diverse piattaforme hardware.

Si vede come questo algoritmo abbia dentro di sé implementate le 5 funzioni hash finaliste del concorso indetto dal NIST per la selezione del nuovo standard SHA-3 (Blake, Grostl, JH, Keccak, Skein), tra cui anche la vincitrice Keccak, e 6 delle semifinaliste del medesimo concorso (BMW, CubeHash, ECHO, Luffa, SHAvite-3, SIMD): in pratica, implementa quelle che erano le migliori funzioni hash a disposizione al momento della sua scrittura (e tutt'ora lo sono), considerando che tra queste è presente la funzione da cui è stato preso l'attuale standard SHA-3. Questo garantisce che X11 sia un algoritmo costruito su una tecnologia sicura e collaudata. Di seguito approfondiamo la funzione hash Keccak a solo scopo divulgativo, per dare un'idea generale della complessità della cifratura di X11.

3.2.1 Keccak

Keccak (pronunciato ['kɛʧæk]) è un algoritmo di hashing crittografico ideato da Guido Bertoni, Joan Daemen, Michaël Peeters e Gilles Van Assche, e nel 2012 è stato selezionato come vincitore del concorso SHA-3, organizzato dal National Institute of Standards and Technology (NIST) per la scelta del nuovo standard SHA-3. SHA è una famiglia di funzioni hash crittografiche progettate dall'NSA (National Security Agency) a partire dal 1993, pubblicato poi dal NIST come standard federale negli Stati Uniti. SHA-0 e SHA-1 però sono presto risulate vulnerabili agli attacchi e per questo motivo nel 2002 sono state introdotte altre quattro funzioni hash addizionali (SHA-224, SHA-256, SHA-384 e SHA-512) che hanno preso il nome di funzioni SHA-2. Anche se non erano state riscontrate delle particolari vulnerabilità nella famiglia SHA-2, nel 2007 il NIST ha indetto un concorso per determinare un nuovo standard SHA-3. Il team Keccak è stato scelto come vincitore del concorso nel 2012, dopo quattro anni di selezioni, venendo quindi dichiarato come l'algoritmo più sicuro tra i 64 che erano stati presentati al concorso. Nel 2014, il NIST ha apportato alcune leggere modifiche alla presentazione di Keccak e nell'agosto 2015 ha pubblicato il FIPS 202 (Federal Information Processing Standards), che annunciava ufficialmente lo "*SHA-3 standard: permutation-based hash and extendable output functions*". Come SHA-2, anche la famiglia SHA-3 include quattro funzioni hash crittografiche (SHA3-224, SHA3-256, SHA3-384, SHA3-512) e in più anche due funzioni a ouptut estendibile (SHAKE128, SHAKE256).
Keccak è quindi una famiglia di funzioni hash crittografiche basata sulle "funzioni spugna" e i suoi utilizzi principali sono quello di funzione hash crittografica, l'autenticazione, la crittografia e la generazione di numeri pseudocasuali. La funzione spugna è una funzione che lavora in più fasi: una fase di assorbimento dell'input (absorbing phase) e una in cui viene rilasciato l'output (squeezing phase). In questo tipo di funzioni l'ingresso è una stringa di lunghezza variabile e l'uscita è ugualmente una stringa di lunghezza variabile basata su una permutazione di lunghezza fissa.
Cerchiamo qui di riportare in maniera schematica come funziona l'algoritmo nel suo utilizzo più tipico:

1. **Inizializzazione**: si inizia con uno stato interno di $b = 1600$ bit (calcolato come $(5 \times 5 \times w)$, dove $w = 2^l$, e $l = 6$ per cui $b = 1600$), organizzato come una matrice tridimensionale di dimensioni 5x5x64 bit (5 righe, 5 colonne e ogni cella è una stringa di 64 bit). Questo stato viene inizializzato a zero.

2. **Fase di Assorbimento (Absorbing Phase)**: l'input viene diviso in blocchi di dimensione r bit, dove r è il "rate" della funzione spugna (per SHA3-256, $r = 1088$ bit). I bit rimanenti dello stato interno ($b - r = 1600 - r = 512$ bit) costituiscono la "capacità" c. Sempre in questa fase, a ogni blocco di input viene applicata un'operazione di XOR (operazione di somma esclusiva bit a bit) con i primi r bit dello stato interno. Dopo ogni operazione di XOR, viene applicata una funzione di permutazione chiamata *Keccak-f* all'intero stato interno.

3. **Permutazione *Keccak-f***: è una trasformazione complessa composta da 24 round, ognuno dei quali include cinque passaggi principali:

   - θ (theta): ogni bit dello stato viene aggiornato in base ai bit della stessa colonna e delle colonne adiacenti.
   - ρ (rho): ogni bit dello stato viene ruotato di un numero specifico di posizioni.
   - π (pi): i bit dello stato vengono riorganizzati secondo una permutazione specifica.
   - χ (chi): ogni bit viene aggiornato in base ai valori dei bit nella stessa riga, usando una funzione booleana.
   - ι (iota): un valore di round-specific viene XORato con uno dei bit dello stato.

   Secondo il documento scritto dagli ideatori, in un round bisogna applicare prima θ e poi le altre possono essere applicate in un ordine arbitrario, ma quello riportato è quello che viene solitamente utilizzato, motivato dalle proprietà di questi step.

4. **Strizzatura (Squeezing Phase)**: una volta assorbito l'intero messaggio, i bit di output desiderati vengono "strizzati" dallo stato, tipicamente in blocchi delle dimensioni del rate. Tra ogni operazione di strizzatura, viene applicata nuovamente la permutazione fino a raggiungere almeno la lunghezza di bit desiderata.

5. **Troncamento**: l'output strizzato viene troncato alla lunghezza hash desiderata (es. 256 bit per SHA3-256).

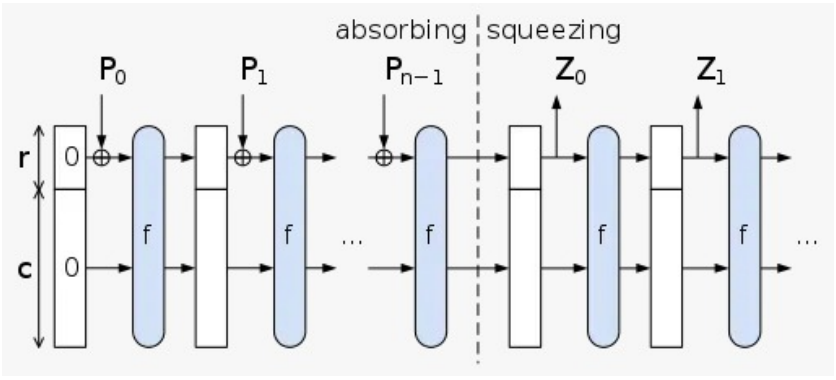


Figura 3.1. r: rate, c: capacità, f: *Keccak-f*, P_i: inizio round i, Z_i: output squeezing i

3.3 Vantaggi e svantaggi di X11

Come Duffield aveva pensato, questo algoritmo offre diversi vantaggi:

- **Livello di sicurezza più elevato rispetto alle funzioni hash come SHA-256**: visto che X11 concatena 11 diversi algoritmi di hashing, risulta piuttosto inattaccabile nel caso venisse trovata una falla in una delle funzioni. Infatti, la rete Bitcoin potrebbe avere dei problemi nel momento in cui qualcuno trovasse il modo di rompere la funzione hash SHA-256, dal momento che viene implementata solo quella nell'algoritmo, mentre se si trovasse, per esempio, il modo di rompere la funzione hash *Blake* (la prima delle 11 di Dash), resterebbero comunque altre 10 funzioni da attaccare.

- **Prestazioni migliori in termini di potenza di calcolo e consumo energetico**: possiamo distinguere due periodi: prima e dopo la realizzazione degli ASIC per X11. Per quanto riguarda il periodo prima della realizzazione degli ASIC specifici, i miner erano costretti a lavorare solo con GPU e CPU. Rispetto a una "somma" di ASICS, le GPU sono più efficienti dal punto di vista energetico perché sono ottimizzate per svolgere un'ampia gamma di operazioni in parallelo e quindi hanno un buon rendimento quando devono fare operazioni complesse come X11. Dopo la commercializzazione degli ASIC specifici per X11, questi sono risultati generalmente più efficienti di quelli per SHA-256, perché devono essere ottimizzati per una varietà di algoritmi e non per uno solo. Questo di solito costringe a un design dell'hardware che deve bilanciare meglio il consumo di energia e le prestazioni. Per di più, la combinazione di più algoritmi di hashing riduce la probabilità che l'hardware diventi

estremamente caldo durante il funzionamento continuo, il che è una delle principali cause di inefficienza energetica. Minori temperature operative significano meno energia necessaria per il raffreddamento, che è un componente significativo del consumo energetico totale nei data center di mining.

- **Possibilità di riconfigurare l'algoritmo per utilizzare altre funzioni hash invece delle 11 specificate all'avvio**: è possibile anche aggiungere funzioni hash in coda come avviene nel caso di X13 o X17, che non sono altro che varianti di X11 con rispettivamente due e sei funzioni in più.
- **Ottime prestazioni di mining su CPU e GPU**: offre un buon livello di guadagno a chi estrae con questo tipo di dispositivo.

Dal lato svantaggi, abbiamo:

- **Perdita della resistenza agli ASIC**: come è stato detto, X11 è stato progettato per essere ASIC-resistente grazie alla sua complessità. Tuttavia, ora sono stati sviluppati gli ASICs in grado di estrarre l'algoritmo X11 e si sta rivelando complessa l'idea della decentralizzazione del mining.
- **Difficoltà di modifica**: a causa dell'elevato numero di funzioni hash all'interno dell'algoritmo, modificarlo per migliorare alcune funzioni può essere complesso.

Capitolo 4

Conclusioni

Dash è riuscita a trovare lo spazio giusto nel mercato delle criptomonete in un momento in cui la necessità per il mondo reale era quella di avere una moneta che fosse utilizzabile tutti i giorni e non solo per delle transazioni sporadiche. Abbiamo visto come Evan Duffield non ha ritenuto necessario introdurre tecnologie estremamente innovative e stravolgenti, ma ha rielaborato in maniera ragionata quello che di meglio offrivano già i mondi dell'informatica e della matematica. In ogni caso, le strategie adottate in Dash hanno avuto a modo loro un'impatto rivoluzionario per il mondo delle monete digitali, basti solo pensare all'introduzione di X11 come algoritmo di hashing all'interno del processo di creazione di nuova moneta o alla modalità di redistribuzione del guadagno all'inserimento di un nuovo blocco nella rete. La rete Dash ha vinto le sfide che si era posta all'inizio del suo sviluppo, ponendo al centro la sicurezza degli utenti e la velocità delle transazioni, unendole a commissioni bassissime. Ciò che ha permesso a questa criptomoneta i suoi risultati abbiamo visto essere stata in primo luogo l'introduzione di un sistema di *masternodes*, che hanno una responsabilità decisionale maggiore rispetto a un utente "standard" della rete senza però far venire meno la decentralizzazione della blockchain, cuore pulsante dell'idea di Bitcoin. Questi nodi hanno consentito l'adozione del sistema di coinjoin ottimizzato *PrivateSend* e lo sviluppo del sistema *ChainLocks*, importante novità della rete Dash. Oltre a questi, i *masternodes* consentono l'attuazione del processo di *InstantSend*, altro vero punto di forza della rete che rende possibile effettuare le transazioni con conferma istantanea. In poche parole, una combinazione di quello che di meglio offriva la tecnologia per dare un senso nel mondo reale alla tecnologia delle criptomonete.
Quella di Dash quindi non è tanto una sfida a Bitcoin, quanto più un

modo di trovare le strategie migliori per rendere l'idea di Satoshi Nakamoto realmente utile alle persone nella loro vita quotidiana. Oggi, per chi ha fiducia nella criptomoneta Dash, risulta quindi realmente possibile vendere o acquistare prodotti di ogni tipo, sia online sia in un negozio fisico. Come scritto sul sito ufficiale dash.org, "*grab a coffee, buy a plane ticket, or pay your phone bill*", *(prendi un caffè, compra un biglietto aereo o paga la bolletta del telefono)*, con una grande tutela per la propria sicurezza e delle commissioni estremamente basse. Attualmente utilizzano la rete più di 159mila tra commercianti e servizi con un'attività giornaliera che conta più di 8220 transazioni e più di 54300 indirizzi attivi, portando la rete a un volume totale di pagamento che si aggira sui $4.48mld e posizionando Dash tra le prime 200 criptovalute considerando il market cap.

Bibliografia

Proposal "treasury-reallocation-60-20-20". URL https://www.dashcentral.org/p/TREASURY-REALLOCATION-60-20-20.

Competizione nist per funzioni hash, a. URL https://it.wikipedia.org/wiki/Competizione_NIST_per_funzioni_hash.

Sha-3, b. URL https://it.wikipedia.org/wiki/SHA-3.

X11. URL https://bitcoinwiki.org/it/wiki/x11#.

Gabriele Ayala. Cos'è l'algoritmo di mining x11. URL https://academy.bit2me.com/it/que-es-algoritmo-mineria-x11/.

Guido Bertoni, Joan Daemen, Michaël Peeters, Gilles Van Assche, Seth Hoffert, and Ronny Van Keer. Keccak specifications summary. URL https://keccak.team/keccak_specs_summary.html.

Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. The keccak reference. 2011. URL https://keccak.team/files/Keccak-reference-3.0.pdf.

Inc. Dash Core Group. Dash features, a. URL https://docs.dash.org/en/stable/docs/user/introduction/features.html#coinjoin.

Inc. Dash Core Group. Dash governance, b. URL https://docs.dash.org/en/stable/docs/user/governance/understanding.html.

Inc. Dash Core Group. Features, c. URL https://docs.dash.org/en/stable/docs/user/introduction/features.html.

Inc. Dash Core Group. Dash website, d. URL https://www.dash.org/.

Information Technology Laboratory. Sha-3 standard: Permutation-based hash and extendable-output functions. Technical report, National Institute of Standards and Technology, 2015. URL https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.202.pdf.

Nathaniel Luz. *Digital is the Cash.* 2020.

National Institute of Standards and Technology. Nist selects winner of secure hash algorithm (sha-3) competition. *NIST website*, 2012. URL https://www.nist.gov/news-events/news/2012/10/nist-selects-winner-secure-hash-algorithm-sha-3-competition.

unknown. Dash emission projection. URL https://docs.google.com/spreadsheets/d/1JUK4Iy8pjTzQ3Fvc-iV15n2qn19fmiJhnKDDSxebbAA/edit#gid=205877544. proiezione della stima del numero totale di DASH che verrà emesso.

Reddit user @_moocowmoo_. URL https://www.reddit.com/r/dashpay/comments/7fc2on/comment/dqb4pjn/.

NiceHash website. Dash halving countdown. URL https://www.nicehash.com/countdown/dash-halving-2024-15-06-12-00.

Astha Yadav. Keccak function. URL https://medium.com/coinmonks/keccak-function-5bbb6981bdce.