De Freeman Familie

4 Juli, 2019

EPIC CASH

EPISCH PRIVÉ INTERNETGELD

Een Peer-to-Peer Electronisch Geldsysteem

WAARDEOPSLAG + RUILMIDDEL + REKENEENHEID

1,7 miljard volwassenen hebben geen toegang tot het mondiale financiële systeem, en nog eens 1,3 miljard worden achtergesteld. Epic Cash ontsluit menselijk potentieel door individuen met de wereldmarkt te verbinden. Het is snel, vrijwel gratis te gebruiken en voor iedereen toegankelijk.

Versie 7.1b Dutch

Inhoudsopgave

I. Abstract

Epic Cash is de laatste stap op de weg naar het echte P2P-internetgeld, het fundament van een privé financieel systeem. De Epic-valuta streeft ernaar 's werelds meest effectieve privacy beschermende vorm van digitaal geld te worden. Om dat doel te bereiken, vervult het de drie belangrijkste functies van geld:

1. **Waardeopslag** – opslag, opname en uitwisseling op een later tijdstip en het heeft een voorspelbare waarde op het moment van opname;
2. **Ruilmiddel** – alles wat als een waardestandaard aanvaard wordt en voor goederen of diensten inwisselbaar is;
3. **Rekeneenheid** – de eenheid waarmee de waarde van een ding wordt verantwoord en vergeleken.

	$ USD	BTC	EPIC
Waardeopslag	✗	✓	✓
Ruilmiddel	✓	✗	✓
Rekeneenheid	✓	✗	✓

In 2009 kwam Bitcoin als de eerste op blockchain gebaseerde digitale valuta naar voren, en bepaalde daarmee drie kenmerken waarmee andere cryptovaluta's worden geëvalueerd:

- ✓ **Geen nood aan vertrouwen** – niemand hoeft een gecentraliseerde entiteit of tegenpartij te vertrouwen om het netwerk te laten functioneren;
- ✓ **Onveranderlijkheid** – transacties kunnen niet ongedaan worden gemaakt;
  a. Het moet zeer onwaarschijnlijk of moeilijk zijn om de geschiedenis te herschrijven;
  b. Niemand anders dan de eigenaar van een privé sleutel kan fondsen die aan die privé sleutel gekoppeld zijn verplaatsen;
  c. Alle transacties worden op de blockchain opgeslagen.
- ✓ **Decentralisatie** – "Blockchains zijn politiek gedecentraliseerd (niemand controleert ze) en architectonisch gedecentraliseerd (geen infrastructureel faalpunt) ..."[1].

Bitcoin heeft op technologisch gebied nieuwe wegen ingeslagen terwijl het zich aan beproefde basisprincipes in de structuur van zijn monetaire beleid heeft gehouden. Het succes van Bitcoin is sterk aan het beperkte aanbod in combinatie met een vertrouwde, onveranderlijke en gedecentraliseerde blockchain gerelateerd. Epic Cash emuleert Bitcoin's monetaire beleid van afnemende inflatie en een beperkt aanbod om ervoor te zorgen dat de Epic-valuta als een effectieve waardeopslag kan dienen. Ondanks het succes van Bitcoin zijn er sinds de oprichting 10 jaar geleden bepaalde tekortkomingen aan het licht gekomen. Andere projecten hebben geprobeerd deze tekortkomingen te verhelpen en we hebben de beste hiervan onderzocht om als uitgangspunt te gebruiken. We besloten de codebasis van Grin en het uitstekende werk van verschillende andere projecten te gebruiken om ons te helpen op een perfecte manier aan de zwaarbevochten prestaties en ontdekte fouten van de voorgangers van Epic Cash te werken. Epic Cash bezit de belangrijkste eigenschappen om een ideale valuta te zijn:

- ✓ **Vervangbaarheid** – De waarde van een gegeven eenheid van Epic moet altijd aan een andere eenheid van Epic gelijk zijn, net zoals een Yen of Yuan altijd gelijk aan een andere Yen of Yuan is en er door vervangen kan worden. Het bereiken van vervangbaarheid hangt grotendeels van privacy af.
- ✓ **Schaalbaarheid** – Epic Cash onderhoudt een ruimtebesparende blockchain, waarop gemakkelijk nieuwe knooppunten kunnen worden gezet, en dit zonder apparatuur die veel middelen vereist. De Epic Cash-blockchain kan in vergelijk met Bitcoin tot twee maal zo veel transacties doorvoeren.
- ✓ **Privacy** – De Epic Cash-blockchain beschermt de anonimiteit van Epic-eigenaren en gebruikers door de details van transacties van derden te beschermen, en is ontworpen om zowel niet traceerbaar als onzichtbaar voor bewaking te zijn.
- ✓ **Snelheid** – De Epic Cash-transacties verlopen soepel, continu en worden veel sneller uitgevoerd dan bij blockchain technologie van eerdere generaties. Hoewel Bitcoin zes blokken van 10 minuten nodig heeft om een volledige transactiebevestiging te bereiken, vinden Epic-transacties, zodra een blok van 1 minuut gedolven is, binnen een enkele blokbevestiging plaats.

[1] Buterin, Vitalik, ***The Meaning of Decentralization***, 6 Februari, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. Privacy

Het moderne gebruik van geld kan als de collectieve overdracht van rekeneenheden tussen mensen en instellingen worden begrepen. Het monetaire landschap kan op een bepaald tijdstip door de volgende vragen te beantwoorden in kaart worden gebracht:

1. *Wie bezit het, en hoeveel bezitten ze?*
2. *Wie doet transacties met wie, en voor hoeveel?*

We kunnen die vragen voor traditionele fiat-valuta's, en inderdaad ook voor Bitcoin, beantwoorden. Hierdoor kan er veel over het leven van mensen, zoals consumptiepatronen, eigendom en transactionele tegenpartijen, worden onthuld. Door waardeoverdrachten te traceren kunnen redelijk nauwkeurige conclusies over iemands interesses en intenties worden getrokken. Zonder privacy kunnen transactiegegevens gevaarlijke informatie in handen van roofzuchtige derden zijn.

Het gebruik van cryptovaluta toont in het afgelopen decennium een continuüm van "privacy" in verschillende blockchain-implementaties aan. De te overwegen privacyschaal varieert van open en berucht aan de ene kant tot anoniem aan de andere kant. Naarmate de privacy afneemt, wordt een essentieel kenmerk van cryptovaluta, de betrouwbaarheid, gedegradeerd. Zoals blijkt uit het succes van analysediensten van de Bitcoin-blockchain, bevindt Bitcoin zich meer in de richting van het notoir transparante einde van het privacyspectrum. Gebruikers moeten steeds meer stappen ondernemen om ervoor te zorgen dat ze niet onbedoeld transacties in gekende Bitcoin uitvoeren. De Epic Cash-oplossing zwaait de naald naar anoniem en herstelt deze essentiële eigenschap door ervoor te zorgen dat zowel de privacy van het individu als de privacy van transacties op een fundamenteel niveau in het systeem zijn ingebouwd.

Identiteitsprivacy

Transactionele Privacy

Identiteitsprivacy

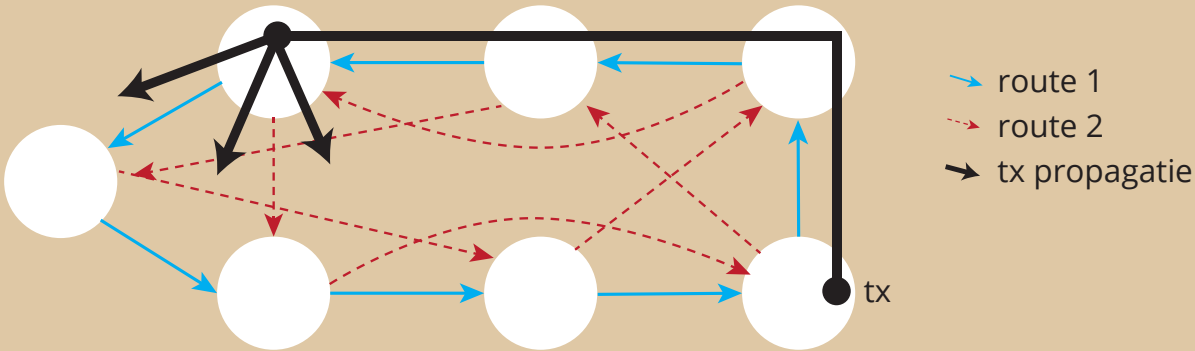
De meeste cryptovaluta's zoals Bitcoin worden in portemonnees, waarvan de adressen naar openbare sleutels die van de privésleutels van de portemonnee zijn afgeleid, verwijzen, opgeslagen. Deze adressen kunnen als opzoekers van iemands privékluis in de digitale wereld worden gezien. De Epic Cash-blockchain elimineert adressen volledig en past in plaats daarvan één grote multisignatuur toe waaruit alle openbare en privésleutels voor eenmalig gebruik worden gegenereerd.

Omdat het adres van een Bitcoin-portemonnee een kluis in de digitale wereld representeert, kan die portemonnee tot het IP-adres van de eigenaar, die de eigenaar op een bepaald moment op een unieke locatie aan een computer verankert, worden herleid. Eenvoudig uitgelegd: wanneer een Bitcoin-transactie plaatsvindt, wordt de transactie via een communicatiehub met de naam 'knooppunt' uitgezonden en vervolgens aan andere knooppunten, de 'peers' doorgegeven. De informatie verspreidt zich vervolgens snel naar alle peers van die knooppunten in het hele netwerk. Dit proces wordt toepasselijk het "roddelprotocol" genoemd. Elke Bitcoin heeft zeer eenvoudig gezien een zichtbare online positie en een fysieke locatie waar het, of liever de eigenaar van de Bitcoin, kan worden gevonden. Zoals journalist Grace Caffyn opmerkte, is Bitcoin 'niet geheimer dan een Google-zoekopdracht vanaf een internetverbinding thuis'.[2]

Naast het elimineren van portemonnee-adressen, beveiligt de Epic Cash-blockchain de identiteitsprivacy door ervoor te zorgen dat IP-adressen niet kunnen worden getraceerd. Dit gebeurt door de integratie van het ***Dandelion++ Protocol***. Het ***Dandelion++ Protocol*** is als een verbetering van zijn voorganger, het originele ***Dandelion Protocol***, het resultaat van het voortdurende werk van zeven onderzoekers om deanonymisatie-aanvallen op de blockchain te bestrijden. Via ***Dandelion++*** worden transacties via willekeurig vervlochten routes of 'kabels' doorgegeven en vervolgens plotseling naar een groot netwerk van knooppunten, zoals de zaden van een paardenbloem wanneer ze uit hun stengel worden geblazen (figuur 1), verspreid. Dit maakt het bijna onmogelijk om transacties naar hun oorsprong, en dus hun oorspronkelijke IP-adressen, terug te voeren.

Figuur 1: Transacties anonimiseren met het *Dandelion++ Protocol.*

Dandelion++ stuurt berichten door via een van de twee met elkaar verweven routes op een 4-dimensionale grafiek en zendt deze vervolgens met diffusie uit. In de figuur verspreidt de transactie zich over de effen blauwe route[3]. Dit proces maakt het uiterst moeilijk om transacties naar hun bron terug te voeren, waardoor de privacy behouden blijft.



[2] F2Caffyn, Grace, ***Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,*** 14 Maart, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, S B, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', ***Proc. ACM Meas. Anal. Comput. Sys.***, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

Transactionele Privacy

De Epic Cash-blockchain verzekert de transactionele privacy door de bedragen en de relatie tussen de zender en ontvanger van een transactie te verdoezelen. Dit wordt bereikt door ideeën die onder de naam ***Vertrouwelijke Transacties (CT)***[4] en ***CoinJoin***[5], methoden die grotendeels door Gregory Maxwell (Bitcoin Core ontwikkelaar, Mede-Oprichter en CTO van Blockstream) zijn ontwikkeld, toe te passen..

CT werd oorspronkelijk door Adam Back gemaakt en later door Maxwell verfijnd en functioneert door transacties via homomorfische codering, een methode waarbij berekeningen op gecodeerde informatie worden uitgevoerd zonder deze eerst te decoderen om de privacy te behouden, in kleinere delen op te splitsen. Eenmaal verdeeld kunnen waarnemers de feitelijke bedragen van de transacties niet zien vanwege verblindende factoren en een systeem dat willekeurige getallen in de mix van transactiefragmenten gooit om de waarden van die fragmenten te verbergen. Uiteindelijk kennen alleen de partijen die transacties verzenden de waarde van een uitwisseling, en wordt de transactie door het netwerk geverifieerd door de bevestiging dat de som van de uitvoerwaarden gelijk is aan de som van de invoerwaarden, en de som van de verblindende factoren van de uitvoer gelijk is aan de som van de verblindende factoren van de invoer.

Om de taak van de nieuwsgierige blikken nog ingewikkelder te maken, worden alle Epic Cash-transacties met ***CT*** gecamoufleerd en vervolgens vermengd om de verbindingen tussen transacties te verbergen. Dit gebeurt via het tweede concept van Maxwell, ***CoinJoin***.

Om ***CoinJoin*** op een eenvoudige manier te illustreren, kunt u zich voorstellen dat A, B en C Epic respectievelijk naar X, Y en Z sturen. De Epic wordt via het ***CoinJoin***-medium verzonden, en het enige dat bekend is, is dat A, B en C verzenden en X, Y en Z ontvangen, terwijl de transactiebedragen onzichtbaar blijven. Het ***CoinJoin***-systeem is voor Epic Cash door middel van Samengestelde één-richting Signaturen (OWAS), die alle transacties binnen een blok tot één transactie combineren, van fundamenteel belang.

Privacy: Samenvatting

De Epic Cash blockchain beschermt de privacy van individuen en hun transacties door:

- **Portemonnee-adressen te elimineren – Er zijn geen locatie-ID's voor digitale kluizen op de blockchain. Transacties worden direct van persoon tot persoon op basis van portemonnee tot portemonnee geconstrueerd;**
- ***Vertrouwelijke Transacties* – Verdeelt transacties in meerdere delen en introduceert verblindende factoren in de verzameling van die delen, zodat de waarden van de delen en andere transactieparameters niet bekend kunnen zijn;**
- *Dandelion++ Protocol* **– verduistert de digitale paden van een transactie vanaf het IP-adres van de afzender van de transactie;**
- *CoinJoin* **– combineert transacties in bundels om de relaties tussen transacties te maskeren.**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III. Vervangbaarheid

Charlie Lee , de creërder van Litecoin, verklaarde dat vervangbaarheid de enige eigenschap van gezond geld was dat Bitcoin en Litecoin misten, en gaf toe dat privacy en vervangbaarheid de volgende uitdagingen voor de betreffende munten zijn[6]. Andreas Antonopoulos , een van 's werelds belangrijkste blockchain-experts, beweerde dat "... gekende munten destructief zijn. Als je de vervangbaarheid en privacy verbreekt, vernietig je de valuta."[7]

Vervangbaarheid is de eigenschap van een set goederen of activa die ervoor zorgt dat de afzonderlijke eenheden van die set van gelijke waarde en uitwisselbaar zijn. Het is wat de vroegste valutavormen van hun voorgaande ruilsystemen onderscheidt. Zonder vertrouwen in de vervangbaarheid van geld, verliest dat geld snel zijn nut. Zoals hieronder zal worden geïllustreerd, is de vervangbaarheid van de meeste cryptovaluta's onzeker, terwijl de privacyarchitectuur van Epic Cash ervoor zorgt dat deze voor dezelfde bedreigingen ongevoelig is.

De meeste cryptovaluta's die met Bitcoin vergelijkbaar zijn, kunnen door de aard van de transparante blockchains waarop ze bestaan, aantoonbaar door elke portemonnee waarin ze werden bewaard, getraceerd worden. Zowel particuliere derden als overheden bewaken de Bitcoin-blockchain met steeds geavanceerdere middelen om snel munten die bij eerdere activiteiten zijn gebruikt, te identificeren. Dit leidt natuurlijk tot de bezorgdheid dat gekende munten op een dag uit transacties kunnen worden verbannen, waardoor hun eigenaren verlies zouden lijden.

Op 19 maart 2018 kondigde het Amerikaanse Hof voor de Controle van Buitenlandse Activa (OFAC) aan dat het overweegt digitale valuta-adressen in de lijst met Speciaal Aangewezen Onderdanen (SDNs), op te nemen. Dit zijn entiteiten waarmee het voor Amerikaanse personen of bedrijven verboden is transacties uit te voeren. Nog verontrustender is dat de OFAC niet heeft uitgesloten dat adressen die momenteel gekende munten bevatten op de SDN-lijst worden geplaatst, waardoor onschuldige eigenaren van gekende cryptovaluta vanwege de associatie met de betreffende munten op een criminele zwarte lijst zouden komen te staan. Dit heeft ertoe geleid dat Andrew Hinkes, professor in de rechten van de Universiteit van New York stelde: "tot ziens vervangbaarheid", en dat het publiek "een premie op vers geslagen munten of getraceerde schone munten moet verwachten..."[8].

Met deze ontwikkelingen in het achterhoofd is het niet moeilijk om een omwenteling op de cryptomarkt en het lijden of zelfs uitsterven van veel gevestigde cryptovaluta's voor te stellen. Epic is echter een van de weinige cryptovaluta's die dit probleem vanwege de sterke privacyfuncties die eerder in dit document zijn beschreven, volledig vermijdt. Door de koppeling tussen identiteit en eigendom en de relatie tussen transacties te verwijderen, kan Epic nooit aan een persoon of een activiteit verbonden worden. Als zodanig blijft de waarde van Epic onafhankelijk van zijn gebruikers en biedt het een hoge mate van privacy en veiligheid die niet gemakkelijk door kwaadwillende actoren in criminele, financiële of politieke arena's gemanipuleerd kan worden.

> **"...GEKENDE MUNTEN ZIJN DESTRUCTIEF. ALS JE DE VERVANGBAARHEID EN PRIVACY VERBREEKT, VERNIETIG JE DE VAUTA."**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. Schaalbaarheid

Epic Cash is een MimbleWimble blockchain-implementatie die door middel van een ruimtebesparend ontwerp dat overbodige transactiegegevens verwijderd vooruitgang in de schaalbaarheid oplevert. De doorsnijdingsfunctionaliteit die hiervoor verantwoordelijk is, zorgt ervoor dat de blockchain in tegenstelling tot de meeste cryptovaluta's, met inbegrip van Bitcoin, in de loop van de tijd efficiënter wordt en dat nieuwe knooppunten met minimale investeringen in geheugen en rekenkracht kunnen worden gecreëerd. Door ruimtebesparend te blijven, maakt het een wijd verspreid netwerk mogelijk en bevordert het decentralisatie. Hoewel elk Bitcoin-knooppunt de hele keten moet opslaan, kunnen Epic Cash-knooppunten bovendien op basis van een kleine subset blokken aan de netwerkbeveiliging bijdragen.

De meeste cryptovaluta's vereisen een onbeperkte opslag van alle transactiegegevens op hun blockchain. De Bitcoin-keten wint momenteel elke dag 0,15353 GB geheugen, terwijl de keten van Ethereum met een nog hogere snelheid van 0,2719 GB per dag toeneemt. Als de keten van Bitcoin met zijn huidige snelheid blijft groeien, zal ze in het jaar 2140, wanneer het laatste beloningsblok gedolven wordt, ongeveer 6 TB groot zijn. Ethereum zal rond dat moment de 10 TB overtreffen[9]. In de meeste blockchains zonder MimbleWimble moeten transacties door knooppunten over de hele wereld geverifieerd worden. Naarmate het aantal gegevens toeneemt, neemt ook de belasting voor elk knooppunt toe. Zelfs bij slechts 200 GB (de geschatte grootte van de huidige Bitcoin-keten) vereist het synchroniseren van de gegevens een stabiel netwerk en een snelle lees- en schrijfcapaciteit van de schijf.

Hierdoor is mining steeds meer gecentraliseerd door grote conglomeraten die van kostbare computerbronnen gebruik maken. **Als de volledige blockchain-geschiedenis van Bitcoin daarentegen op de Epic Cash-blockchain zou worden opgeslagen, zou deze bijna 90% minder ruimte innemen.** Kleiner is sneller omdat het voor elke transactie minder tijd kost om verzonden en beveiligd te worden.

MimbleWimble lost dit opslagdilemma met een innovatieve methode om de blokken te verkleinen, die ook wel doorsnijding wordt genoemd, op. Om te begrijpen hoe doorsnijding functioneert, is het het beste om eerst te kijken hoe transacties en blokken binnen een MimbleWimble-blockchain zijn samengesteld.

Invoer:

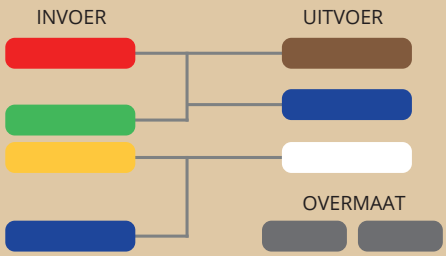
Verwijzingen naar oude uitvoerswaarden;

Uitvoer:

Uitvoerwaarden van vertrouwelijke transacties en **rangeproofs**;

Overmaat:

Het verschil tussen de in- en uitvoerwaarden, plus **handtekeningen** (voor authenticatie en om de deflatie te bewijzen).



Figuur 2:
De onderdelen van een MimbleWimble transactie.

[9] Li, Crypto, ***Blockchain's Big Data Problem,*** 27 Januari, 2019, https://www.longhash.com/news/blockchains-big-data-problem

Alle Epic Cash blokken bevatten:

Merkle Bomen van transactie-invoer;

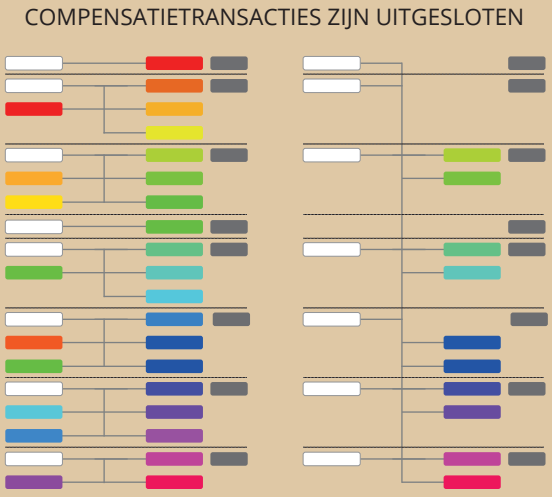
Merkle Bomen van transactie-uitvoer en rangeproofs;

Een lijst met overmaatwaarden en handtekeningen.

Figuur 2 en 3 zijn aangepaste afbeeldingen van de presentaties van Andrew Poelstra[10] en geven nieuw gewonnen Epic als witte invoercellen weer. Identiek gekleurde cellen vertegenwoordigen de uitvoer met de bijbehorende gebruikte invoer. Met het doorsnijdingsproces wordt de invoer en de bijpassende gebruikte uitvoer verwijderd om ruimte binnen het blok vrij te maken, waardoor de hoeveelheid gegevens die op de blockchain opgeslagen moet worden, wordt verminderd. Terwijl de transacties uit het grootboek worden weggelaten, documenteren de resterende overtollige kernen (slechts 100 bytes) permanent dat de transacties hebben plaatsgevonden. Naarmate er blokken worden gemaakt, past MimbleWimble een doorsnijding op de blokken toe, zodat op de lange termijn alleen de kopteksten (ongeveer 250 bytes), niet-gebruikte transacties en transactiekernen (ongeveer 100 bytes) overblijven. Grin, de tweede gelanceerde MimbleWimble-implementatie, toonde aan dat een MimbleWimble-keten met een vergelijkbaar aantal transacties als de Bitcoin-keten bijna 10% van de omvang van de keten van Bitcoin inneemt. Bovendien is de grootte van een knooppunt "in de orde van enkele GB voor een keten in bitcoin-formaat, en mogelijk tot enkele honderden megabytes te optimaliseren."

Dit staat in schril contrast met Bitcoin, waar elk knooppunt de hele blockchain moet opslaan. Naarmate de ruimte-efficiëntie van de Epic Cash-blockchain ten opzichte van de Bitcoin-blockchain toeneemt, zullen de kostenbesparingen ten opzichte van de deelname van knooppunten in het Epic Cash-netwerk ook toenemen. Lagere hindernissen om deel te nemen zorgen voor cruciale veerkracht op het niveau van de knooppunten binnen het netwerkontwerp. Door de implementatie van MimbleWimble en de keten door middel van het doorsnijdingsproces te verkleinen, biedt de Epic Cash-blockchain schaalbaarheid op een manier die vaak door de cryptovaluta-gemeenschap over het hoofd wordt gezien. Het is er een die de essentie van Bitcoin en gelijkgestemde projecten vangt, namelijk een gedecentraliseerde. Ongeacht het aantal transacties per seconde dat een munt kan verwerken, wat voor nut heeft een munt als het niet door een breed en divers netwerk ondersteund kan worden? Als de geheugenvereisten zodanig zijn dat validatie uiteindelijk door sterke mining-conglomeraten wordt aangetrokken, zijn alle inspanningen van de cryptovaluta-gemeenschap om een gedecentraliseerd ecosysteem te creëren, tevergeefs. Om voor extra doorvoer te zorgen, plannen we als een doelstelling op de korte termijn een tweede laagsimplementatie in Lightning-stijl in de ontwikkelingsplannen van Epic Cash.

Figuuur 3:
MimbleWimble transacties voor en na de doorsnijding.



[10] SF Bitcoin Developers, ***MimbleWimble with Andrew Poelstra,*** 24 November, 2016, https://www.youtube.com/watch?v=aHTRlbCaUyM&t=940s

[11] Grin Forum, ***Grin Blockchain Size,*** December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, ***Introduction to Mimblewimble and Grin,*** 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V. Het Monetaire Beleid

Het monetaire beleid van Epic Cash en Bitcoin lijkt sterk op elkaar. Het circulerende aanbod van Epic Cash breidt eerst snel uit en synchroniseert vervolgens in 2028 met het circulerende aanbod van Bitcoin. Het neemt daarna met een dalende snelheid toe totdat er in 2140 een maximaal aanbod van 21 miljoen Epic bereikt wordt. Epic Cash heeft de kwaliteiten om een veilige waardeopslag voor de lange termijn te worden omdat de circulerende aanbod op elk punt van de emissie levenscyclus bekend is en in een vast maximaal aanbod culmineert. Het monetaire beleid van Epic Cash wordt door de volgende vier kenmerken gekenmerkt:

- Een snelle emissie gedurende de eerste negen jaar, gedurende welke 20.343.750 Epic (96.875% van het totale aanbod) moeten worden gedolven. De exacte emissiepercentages worden in het gedeelte Emissieschema in dit document beschreven;
- Het maximale aantal van 21 miljoen Epic zal in het jaar 2140 worden bereikt. En dit op ongeveer hetzelfde moment als wanneer Bitcoin een maximaal aanbod van 21 miljoen eenheden bereikt;
- Het circulerende aanbod en de emissiesnelheid van Epic komen op de Epic Singulariteit rond 24 mei 2028 met die van Bitcoin overeen. Na de Singulariteit neemt de emissiesnelheid met een toenemende snelheid af, terwijl het circulerende aanbod met een afnemende snelheid groeit;
- Epic wordt in 8 decimalen opgedeeld, zodat: 1 Epic gelijk is aan 100.000.000 freeman (net zoals 1 Bitcoin aan 100.000.000 satoshi gelijk is).

Het monetaire beleid van Epic Cash is om de volgende redenen naar dat van Bitcoin gemodelleerd:

- Overeenstemming met de economische fundamenten van Bitcoin, namelijk dat schaarste en de voorspelbaarheid van het circulerende aanbod ten grondslag aan de sterke voorraad waardevaststellingen ligt;
- Het publiek kent het model van Bitcoin en zijn bewezen staat van dienst in de afgelopen tien jaar sinds zijn oprichting. Door ongeveer met het circulerende aanbod van Bitcoin te synchroniseren en de maximale aanbod- en deelbaarheidsstructuur van Bitcoin te spiegelen, neemt Epic in de richting van massa-acceptatie de weg van de minste weerstand.

VI. Het Emissieschema

Epic Cash heeft in totaal 33 mining-fasen. Elke fase is gedefinieerd door dalingen in de blokbeloningen in vergelijking met de vorige fase. De Epic Genesis, de datum waarop Epic blok #1 wordt gedolven, vindt op augustus 2019 plaats. Blokken worden met één per minuut gedolven. De eerste vijf fasen produceren bijna 97% van het maximale Epic-aanbod, hetgeen in negen jaar met ongeveer 20 jaar Bitcoin-emissie overeenkomt. Dit kan voor degenen die de spectaculaire opkomst van Bitcoin hebben gemist als een kans om 'de klok terug te draaien' worden gezien.

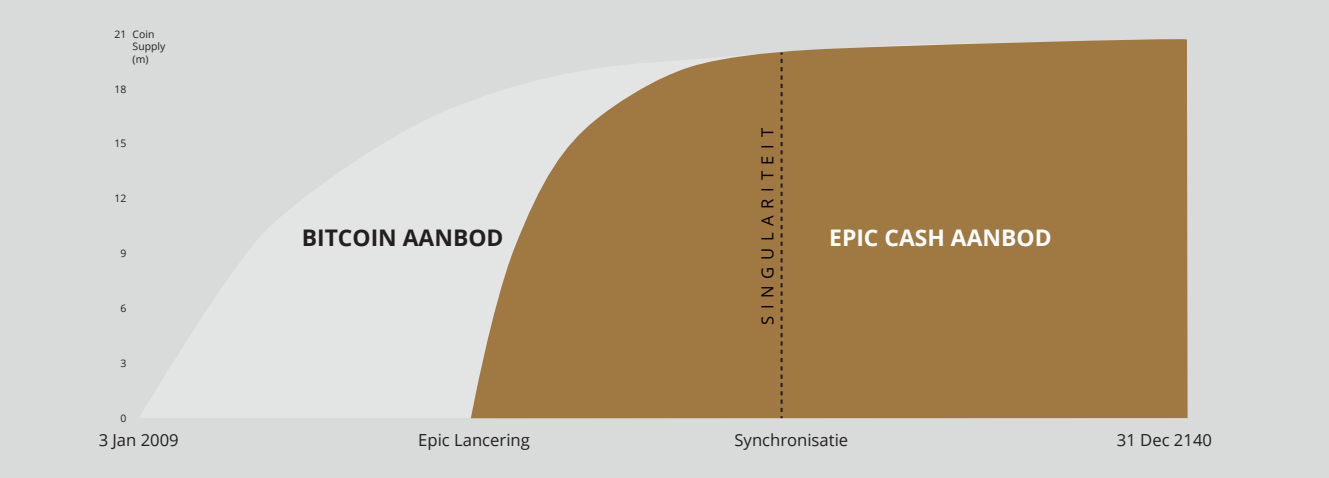
Het emissieschema in tabel 1 geeft de begin- en einddatum van de eerste zeven mining-fasen, hun bijbehorende blokbeloningen en het daaropvolgende circulerende aanbod voor elk fase weer. Fase 8 tot 33 zijn omwille van de duidelijkheid niet in de tabel opgenomen. Voor die fasen is het voldoende om te begrijpen dat elke volgend fase, zoals bij Bitcoin een blokbeloning zal hebben die de helft van het bedrag van de beloning van de voorgaande bedraagt. De hoeveelheid Epic die tijdens elk van deze fasen wordt vervaardigd is de som van de blokbeloningen binnen de 4-jarige fase (ongeveer 1460 dagen).

Ten tijde van de Epic Singulariteit (2028) komt het circulerende aanbod van Epic met het circulerende aanbod van Bitcoin overeen, en neemt Epic Cash het blokbeloning- en halveringspatroon van Bitcoin aan, waardoor de blokbeloningen elke vier jaar met de helft afnemen. De enige uitzondering is dat de blokken van Epic nog steeds met een snelheid van één per minuut, versus de snelheid van Bitcoin van een blok om de tien minuten, worden gedolven. Door dit te doen, behoudt het circulerende aanbod van Epic bij benadering de pariteit met het circulerende aanbod van Bitcoin voor de rest van hun bestaan.

Tabel 1: Emissieschema voor de eerste zeven mining-fasen. De datums zijn benaderd.

Tijdperk	1	2	3	4	5	SINGULARITEIT	6	7
Blokbeloning	16	8	4	2	1		0.15625	0.078125
Startdatum	1 Aug, 2019	29 Jun 2020	11 Okt, 2021	3 Jun 2023	10 Aug 2025		24 Mei 2028	22 Mei 2032
Einddatum	J29 un , 2020	11 Okt 2021	3 Jun 2023	10 Aug 2025	24 Mei 2028		22 Mei 2032	20 Mei 2036
Lengte (in dagen)	334	470	601	800	1019		1460	1460
Het Beginaanbod	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
Het Eindaanbod	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
% van het Maximale Aanbod	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

Figuur 4: Het Emissieschema van Epic en Bitcoin.



VII. Mining

De Epic Cash-blockchain streeft naar decentralisatie door een breed scala aan computerhardware te verwelkomen. Epic mining is in eerste instantie voor CPU's, GPU's en ASIC's, met behulp van drie respectieve hashing-algoritmen: RandomX, ProgPow en CuckAToo31+, beschikbaar. Algoritmen kunnen triviaal worden gewisseld zonder de integriteit van de keten in gevaar te brengen.

1 RandomX en CPU's

RandomX is een Proof-of-Work (PoW) algoritme dat voor CPU's voor algemene doeleinden geoptimaliseerd is. Het gebruikt gerandomiseerde programma-uitvoeringen met verschillende geheugengebonden technieken om de volgende doelen te bereiken:

- De preventie van de ontwikkeling van ASIC's met enkelvoudige chips;
- Het efficiëntievoordeel van gespecialiseerde hardware ten opzichte van CPU's voor algemene doeleinden te minimaliseren.

Het aanwinnen van Epic met CPU's vereist een aaneengesloten toewijzing van 2 GB fysieke RAM, een 16 KB L1 cache, een 256 KB L2 cache, en een 2 MB L3 cache per mining-locatie[13]. Windows 10-apparaten vereisen 8 GB of meer RAM. Het is niet ondenkbaar dat op een dag in de niet al te verre toekomst mobiele telefoons levensvatbare mining-knooppunten kunnen worden. Vroege CPU-integratie in het mining-netwerk van Epic Cash is voor velen met slechts bescheiden computermiddelen een uitstekende gelegenheid om blokbeloningen te verdienen door het Epic Cash-netwerk te beveiligen.

2 ProgPow en GPU's

Programmatische Proof-of-Work (ProgPow) is een algoritme dat afhankelijk van de geheugenbandbreedte en de kernberekening van gerandomiseerde wiskundige reeksen is, hetgeen van veel van de computerfuncties van een GPU profiteert en daardoor efficiënt de totale energiekosten van de hardware vastlegt. Omdat ProgPow specifiek is ontworpen om volledig van basis-GPU's te profiteren, is het zowel moeilijk als duur om via gespecialiseerde hardware aanzienlijk hogere efficiëntie te bereiken. Als zodanig vermindert het ProgPow-algoritme stimulansen voor grote ASIC-verzamelingen om GPU's te verslaan, zoals vaak met veel andere PoW-algoritmen, zoals de SHA-256 van Bitcoin wordt gezien. GPU's zijn, hoewel niet zo gangbaar als CPU's, nog steeds algemeen beschikbaar. GPU´s kunnen met technologische ontwikkeling die door giganten zoals NVIDIA en AMD wordt aangedreven, ten opzichte van CPU´s per eenheid meerdere veelvouden aan mining-oplossingen verwerken. Het is vanwege deze combinatie van alomtegenwoordigheid en hoge verwerkingskracht dat GPU's tijdens de initiële fases het fundament voor een groot deel van de mining-activiteit, zoals aangegeven in tabel 2, zullen vormen.

3 CuckAToo+31 en ASIC's

CuckAToo31+ is een ASIC-vriendelijke permutatie van het Cuckoo Cycle-algoritme, dat door de Nederlandse computerwetenschapper John Tromp ontwikkeld is. Als familielid van de ASIC-resistente CuckARoo29, genereert CuckAToo31 + willekeurige bipartiete grafieken en geeft het mijnwerkers de taak om een lus met een gegeven lengte 'N' die door de hoekpunten van de grafiek loopt te vinden.

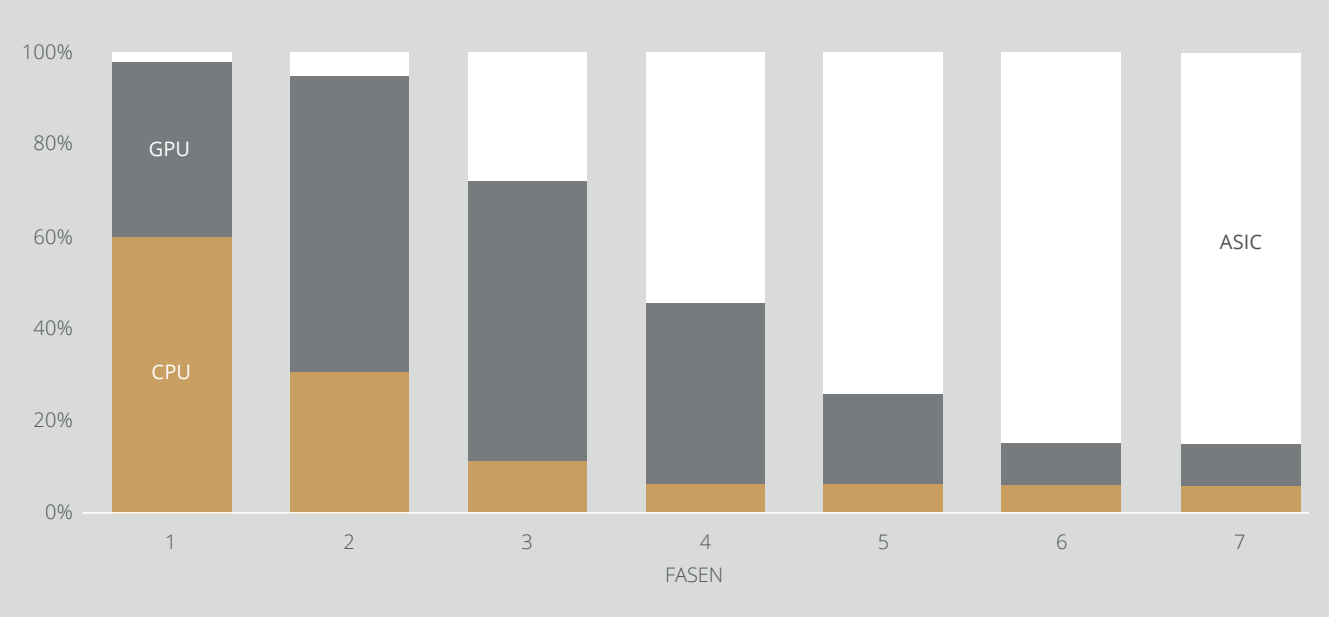
[13] Tevador, ***RandomX***, 28 March, 2019, https://github.com/tevador/RandomX

Dit is een geheugengebonden taak, hetgeen betekent dat de oplossingstijd eerder door de geheugenbandbreedte dan door de onbewerkte processor of GPU-snelheid bepaald wordt. Als gevolg hiervan produceren de Cuckoo Cycle-algoritmen minder warmte en verbruiken ze aanzienlijk minder energie dan traditionele PoW-algoritmen. De ASIC-vriendelijke CuckATOo31+ maakt efficiëntieverbeteringen ten opzichte van GPU's mogelijk door honderden MB SRAM te gebruiken, maar blijft door I/O[14] geheugen afgekneld. Uiteindelijk bieden ASIC's de grootste potentiële schaalvoordelen van de drie mining-opties. In het belang van inclusiviteit nemen ASIC's, hoewel ze ten opzichte van CPU's en GPU's echter een klein deel van de mining-beloningen toegewezen krijgen, uiteindelijk, in de veronderstelling dat er een concurrerend ecosysteem van fabrikanten voor CuckATOo31+ zal zijn, een meerderheidsbelang in de gewonnen blokbeloningen.

Tabel 2: De toewijzing van de Mining-beloningen. Onder voorbehoud van herziening. Toewijzingen zullen op maximale decentralisatie worden gericht en consistent met de langetermijnbelangen van het netwerk zijn.

Fasen	1	2	3	4	5	6	7
Dagen	334	470	601	800	1019	1460	1460
CPUs	60%	30%	10%	5%	5%	5%	5%
GPUs	38%	65%	62%	40%	20%	10%	10%
ASICs	2%	5%	28%	55%	75%	85%	85%

Figuur 5: De toewijzing van de Mining-beloningen voor elk fase volgens tabel 2. Onder voorbehoud van herziening.



[14] Le Sceller, Quentin, ***An Introduction to Grin Proof-of-Work,*** 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 Mining Bijdragen

Met aanvang van de Epic Genesis (2019) en eindigent bij de Epic Singulariteit (2028), is er tijdens het mining-proces een toewijzing van Epic die als mining-bijdragen aan de EPIC Blockchain Stichting zal worden toegewezen.

De EPIC Blockchain Stichting is toegewijd aan de technische ontwikkeling en het bevorderen van de bekendheid en het nut van het Epic Cash-project tijdens de eerste jaren van zijn oprichting, en doet dit door marketingactiviteiten te creëren en partnerschappen binnen de industrie van de de financiële technologie te ontwikkelen.

Na de singulariteit wordt de rol van de EPIC Stichting door de EPIC Gedistribueerde Autonome Corporatie (EDAC), die voorafgaand aan de overdracht door de stichting zal worden ontwikkeld, overgenomen.

De EPIC Blockchain Stichting wordt gefinancierd door een percentage van mining-beloningen, waarvan de blokbeloningen afgetrokken zijn, en dit volgens de volgende jaarlijkse tarieven:

Tabel 3: Jaarlijkse tarieven voor de mining-bijdragen voor de Stichting als percentage van de mining-beloningen.

Jaar	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
% van de Mining Beloningen	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. Conclusie

Epic streeft ernaar als gedecentraliseerd digitaal zilver, een ruilmiddel als tegenhanger van Bitcoin's erkende positie als gedecentraliseerd digitaal goud, erkend te worden. Door verloren vervangbaarheid opnieuw op een veel energie-efficiënter en milieuvriendelijker hardware-fundament te introduceren, brengt Epic Cash de krachtsverhoudingen in het voordeel van individuele gebruikers terug, en dit in schril contrast met recente centraliserende trends. De combinatie van Bitcoin-economie, speltheorie en een bewezen proof-of-work-formule met het beste van de hedendaagse blockchain-technologie resulteert in een betrouwbare, onveranderlijke en gedecentraliseerde valuta (Epic) die schaalbaar en vervangbaar is en die de privacy van zijn gebruikers beschermt. De Epic Cash blockchain is open, openbaar, grenzeloos en bestand tegen censuur. Het bewaart de privacy en rijkdom van zijn gebruikers en beloont degenen die hun hardware voor de ondersteuning van het netwerk via mining inzetten. Elke Epic wordt door middel van proof-of-work gewonnen. Het aantal begint bij nul en de lancering van het netwerk wordt, met een functioneel testnetwerk dat momenteel wordt uitgevoerd, als eerlijk beschouwd.

De belangrijkste Epic Cash Feiten:

- **De Mining-activiteiten beginnen op Augustus 2019.**

- **De Epic Cash blockchain is op MimbleWimble gebaseerd.**

  Bepalende kenmerken van het protocol zijn:

  1. **Doorsnijding** – het verwijderen van redundante informatie uit de blockchain om ruimte-efficiëntie te bevorderen, grootschalige deelname aan netwerkvalidatie aan te moedigen en de decentralisatie te controleren;
  2. ***CoinJoin*** – het bundelen van transacties binnen een blok om de vervangbaarheid van de Epic-cryptovaluta te waarborgen;
  3. ***Dandelion++ Protocol*** – de verspreiding van transacties door via met elkaar verweven kanalen te communiceren en deze over een breed netwerk van knooppunten te verspreiden, waardoor verbindingen tussen transacties en hun oorsprong worden verbroken;
  4. **Geen Portemonnee-adressen** – het gebruik van een grote meervoudige handtekening om voor partijen die transacties uitvoeren privésleutels voor eenmalig gebruik te genereren, waardoor de noodzaak voor portemonnee-adressen volledig wordt geëlimineerd.

- **Het monetaire beleid van Epic Cash** is ontworpen om het circulerende aanbod van Epic in ongeveer negen jaar met dat van Bitcoin te synchroniseren en om in het jaar 2140 tegelijkertijd met Bitcoin hetzelfde maximale aanbod van 21 miljoen eenheden te bereiken. Dit afnemende inflatoire beleid garandeert transparantie en voorspelbaarheid van het aanbod en schaarste, waardoor de veiligheid van waardeopslag op de langer termijn wordt bevorderd.

- **Mining** met CPU's, GPU's en ASIC's via overeenkomstige RandomX-, ProgPow- en CuckAToo31 + -algoritmen om de massale acceptatie en netwerkefficiëntie te vergemakkelijken.

IX. Technische Specificaties

Projectnaam: Epic Cash
Valutanaam: Epic
Bloktijd: 60 seconden
Blokgrootte: 1 MB
Startaantal: 0
Het Totale Aanbod: 21,000,000
Genesis Blok: Augustus, 2019
Consensus: RandomX (CPU's), ProgPow (GPU's) en CuckAToo31+ (ASIC's)

Links:

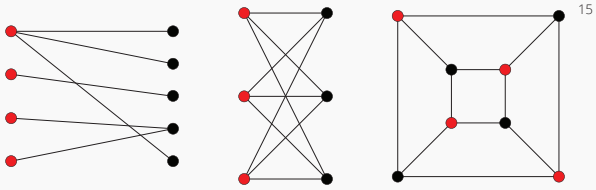
www.epic.tech

t.me/EpicCash – Telegram

X. Woordenlijst

ASIC Toepassingsspecifieke geïntegreerde schakelingen; chips die voor een enkelvoudig doel ontworpen zijn

Tweedelige Diagram een reeks grafiekhoeken opgesplitst in twee onsamenhangende reeksen zodat geen twee grafiekhoekpunten binnen dezelfde reeks aangrenzend zijn.



Verblindende Factor een willekeurig element dat in een digitaal bericht geïntroduceerd wordt om de codering te vergemakkelijken; een gedeeld geheim tussen de twee partijen dat de in- en uitvoer van die specifieke transactie, evenals de openbare en privésleutels van de transactiepartijen codeert.[16].

Blokbeloning de nieuwe Epic die door het netwerk als beloningen voor berekeningen die zijn uitgevoerd om de transacties binnen een nieuw blok te verifiëren, wordt verspreid.

Cache een hardware- of softwarecomponent die gegevens opslaat zodat toekomstige verzoeken om die gegevens sneller kunnen worden bediend.

Circulerend Aantal Het aantal Epic dat op een bepaald tijdstip bestaat.

CPU Centrale Verwerkingseenheid: computercomponent die verantwoordelijk is voor het interpreteren en uitvoeren van de meeste opdrachten van de andere hardware en software van de computer.

Doorsnijding een MimbleWimble blockchain-proces waarbij invoer- en bijpassende gebruikte uitvoerwaarden worden verwijderd om ruimte binnen het blok vrij te maken, waardoor de hoeveelheid gegevens die op de blockchain moet worden opgeslagen wordt verminderd.

Decentralisatie de staat van verspreiding van de activiteiten en het bestuur van een netwerk.

Emissie de creatie van nieuwe Epic die door mining in blokbeloningen wordt verdiend. Epic wordt elke 60 seconden gemaakt als transacties op de blockchain worden bevestigd.

Epic Singulariteit het moment waarop het circulerende aantal Epic met dat van Bitcoin overeenkomt (Mei 2028).

Overmaat (MimbleWimble) het verschil tussen de in- en uitvoerwaarden, plus handtekeningen (voor authenticatie en om deflatie te bewijzen).

Vervangbaarheid de eigenschap van een goed of handelswaar waarbij afzonderlijke eenheden in wezen onderling uitwisselbaar zijn en elk van zijn onderdelen niet van een ander te onderscheiden zijn

Genesis (Evenement) het delven van het eerste Epic-blok en de officiële start van de blockchain.

GPU Grafische verwerkingseenheid: een eenheid met een programmeerbare logische chip (processor) die voor weergavefuncties gespecialiseerd is. GPU's voor consumenten kunnen voor mining zeer geschikt zijn.

Halvering (voor Bitcoin) vindt elke 4 jaar plaats. De emissie daalt met 50% na elke halvering.

Hash een waarde die op basis van een basisinvoernummer met behulp van een hashingfunctie berekend word.

Hashing Algoritme (functie) een wiskundig algoritme dat gegevens van willekeurige grootte aan een hash van een vaste grootte die voor het genereren en verifiëren van digitale handtekeningen, berichtauthenticatiecodes (MAC's) en andere vormen van authenticatie wordt gebruikt, toewijst.

Homomorfische Encryptie een methode voor het uitvoeren van berekeningen op gecodeerde informatie zonder deze eerst te decoderen.

Onveranderlijkheid (bij programmeren) de status waarin een object nadat het gemaakt is niet kan worden gewijzigd.

Invoer (MimbleWimble) het onderdeel van een MimbleWimble-transactie die de verzendende partij van de transactie vertegenwoordigt; op basis van de uitvoerwaarden van eerdere transacties vervaardigd.

I/O invoer/uitvoer; de communicatie tussen een informatieverwerkingssysteem, zoals een computer, en de buitenwereld, mogelijk een mens of een ander informatieverwerkingssysteem.

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, ***Grin Coin and MimbleWimble: An Introductory Guide***, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

Maximum Aanbod	het aantal Epic dat moet worden bereikt op welk punt het circulerende aantal daarna niet meer zal toenemen (21.000.000 Epic).
Memory-Hard	het gebruik van veel RAM om te voorkomen dat gelijktijdige verbindingen parallelle pogingen uitvoeren. Memory-hard functies zijn algoritmen waarvan de berekeningstijden voornamelijk door het beschikbare geheugen om gegevens te bewaren worden bepaald. Ze staan ook als geheugengebonden functies bekend.
Merkle Boom	een gegevensstructuur die in informatica-applicaties wordt gebruikt. In blockchains zorgen Merkle-bomen voor een efficiënte en veilige verificatie van de inhoud in grote gegevensstructuren.
MimbleWimble	een protocol dat door een pseudonieme bijdrager, onder de naam Tom Elvis Jedusor, in de chatroom van Bitcoin-ontwikkelaars opgesteld werd.
Multisignatuur	een schema voor digitale handtekeningen waarmee een groep gebruikers een enkel document kan ondertekenen. Gewoonlijk produceert een algoritme een gezamenlijke handtekening die compacter dan een verzameling afzonderlijke handtekeningen van alle gebruikers is.[17]
Knooppunt	een computer die verbinding met een blockchain-netwerk maakt en zich naar andere knoop-punten in het netwerk vertakt om informatie over transacties en blokken op een peer-to-peer-manier te verspreiden.
Samengestelde éénrichting Signatuur (OWAS)	een transactiehandtekening die uit vele handtekeningen bestaat en die op een bepaalde manier is gecodeerd, zodat het erg moeilijk is om de afzonderlijke handtekeningen te berekenen.
Uitvoer (MimbleWimble)	het onderdeel van een MimbleWimble-transactie die de ontvangst van de transactie vertegen-woordigt; wordt als invoer voor volgende transacties gebruikt.
Pedersen Vastleggingsschema	een cryptografische primitief waarmee een bewijzer zich aan een gekozen waarde kan committeren zonder er enige informatie over te onthullen en zonder dat de bewijzer in staat is om naar de waarde terug te keren.
Privésleutel	een klein stukje code dat aan een openbare sleutel verbonden is om algoritmen voor tekstcodering en decodering in werking te stellen. Het wordt tijdens de asymmetrische sleutelcodering in de cryptografie gecreëerd en wordt gebruikt om een bericht te decoderen en in een leesbaar formaat om te zetten.
Proof of Work (PoW)	een aantal gegevens die moeilijk (duur en tijdrovend) is om te produceren, maar voor anderen gemakkelijk te verifiëren is en dat aan bepaalde vereisten voldoet. Proof of Work wordt vaak bij het genereren van cryptovaluta-blokken gebruikt.
Openbare Sleutel	een openbare sleutel wordt in de coderingscryptografie voor openbare sleutels gecreëerd die coderingsalgoritmen met asymmetrische sleutels gebruiken. Openbare sleutels worden gebruikt om een bericht naar een onleesbaar formaat om te zetten.
RAM (Werkgeheugen)	chips voor gegevensopslag die snel toegankelijk zijn in een computerapparaat waar het besturings-systeem (OS), applicatieprogramma's en gegevens die momenteel worden gebruikt, worden bewaard, zodat ze snel door de processor van het apparaat kunnen worden bereikt.
Rangeproof	een verbintenisbevestiging die verifieert dat de som van een transactie-invoer groter is dan de som van de transactie-uitvoer en dat alle transactiewaarden positief zijn. Rangeproofs zorgen ervoor dat er niet met het geldbedrag is geknoeid.
(Digitale) Signatuur	een standaardonderdeel van een blockchain-protocol, dat voornamelijk voor het beveiligen van transacties en transactieblokken, de overdracht van informatie, contractbeheer en alle andere gevallen waarin het opsporen en voorkomen van externe manipulatie belangrijk is, gebruikt wordt. Ze bieden drie voordelen voor het opslaan en overdragen van informatie op de blockchain: • Ze laten zien of er met de verzonden gegevens geknoeid is; • het controleert de deelname van een bepaalde partij aan de transactie; • Kan juridisch bindend zijn.
SRAM (het Statische Werkgeheugen)	het werkgeheugen (RAM) dat gegevensbits in zijn geheugen bewaart zolang er stroom wordt geleverd.
Doorvoer	het aantal transacties die per seconde met een bepaald cryptovaluta-protocol kunnen worden uitgevoerd.
Geen Nood aan vertrouwen	de kwaliteit van een cryptovaluta-netwerk om zich zonder handhaving door een centrale partij aan de regels van een protocol te houden.

[17] Bellare, Mihir, Neven, Gregory, 2007, ***Identity-based Multi-signatures from RSA***, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

EPISCH PRIVÉ INTERNETGELD