
VERGE
The most privacy focused cryptocurrency
BLACKPAPER

1.0 Introductie

Bitcoin is ontwikkeld en uitgebracht in 2009, als gevolg van de beperkingen in de manier waarop transacties op het internet werden verwerkt. In zijn whitepaper verklaart Nakamoto dat "Internethandel bijna uitsluitend is gebaseerd op financiële instellingen die Trusted third parties dienen om elektronische betalingen te verwerken. Hoewel het systeem goed werkt voor de meeste transacties, lijdt het nog steeds aan de zwakke punten van het vertrouwensmodel "[1]. Sinds de oorspronkelijke oprichting in 2009 is Bitcoin snel opgenomen in hedendaagse moderne markten. Het primaire probleem van de snelle adoptie van Bitcoin is de toenemende vraag naar de oorspronkelijke blockchain en het om gaan met wisselende omvang van grote transacties. Door de toenemende vraag en aantallen transacties, nam de duur van de transacties ook toe en wat vervolgens heeft geleid tot hogere transactiekosten om de transactietijd te versnellen.

De belangrijkste innovatie achter Bitcoin is de gedecentraliseerde structuur. In tegenstelling tot traditionele fiat valuta's, heeft Bitcoin geen centrale controle, geen centrale gegevensopslag, geen centraal beheer en geen centraal punt van mislukking. Een van de uitdagingen waar Bitcoin mee te maken heeft gehad, is echter dat de meeste e-services en e-businesses die rond het Bitcoin-ecosysteem zijn gebouwd wel gecentraliseerd zijn. Door de gecentraliseerde aard van het huidige systeem wordt e-commerce door particulieren op specifieke locaties geleid die kwetsbare computersystemen gebruiken, die vatbaar zijn voor juridische nasleep. Verge is een van de echt gedecentraliseerde valuta's die vandaag beschikbaar zijn. Door de basis beginselen van Bitcoin te gebruiken en hier hele nieuwe laag van anonimiteit over heen te bouwen is Verge ontstaan.

2.0 Tor Integratie

Tor, afgeleid van een afkorting voor de oorspronkelijke softwareprojectnaam "The Onion Router" is een IP-verberg-service, dat anonieme communicatie mogelijk maakt en gebaseerd is op een gelaagd circuit netwerk. Tor stuurt internetverkeer via een wereldwijd overlaynetwerk dat bestaat uit meer dan zevenduizend relais, om de locatie en het gebruik van een gebruiker te verbergen van iedereen die netwerkbewaking of

internetverkeersanalyse verricht. De verschillende lagen van de versleutelde adresgegevens die worden gebruikt om anoniem gegevenspakketen door Tor te verzenden, lijken op de structuur van een ui, vandaar deze naam. Op deze manier kan het pad van een datapakket door het Tor-netwerk niet volledig worden opgespoord. Tor's gebruik is bedoeld om de persoonsgegevens van de gebruikers te beschermen, evenals hun vrijheid en de mogelijkheid om vertrouwelijke informatie te verzenden zonder dat het mogelijk is om hun internetactiviteiten bij te houden.

2.1 Tor Integratie

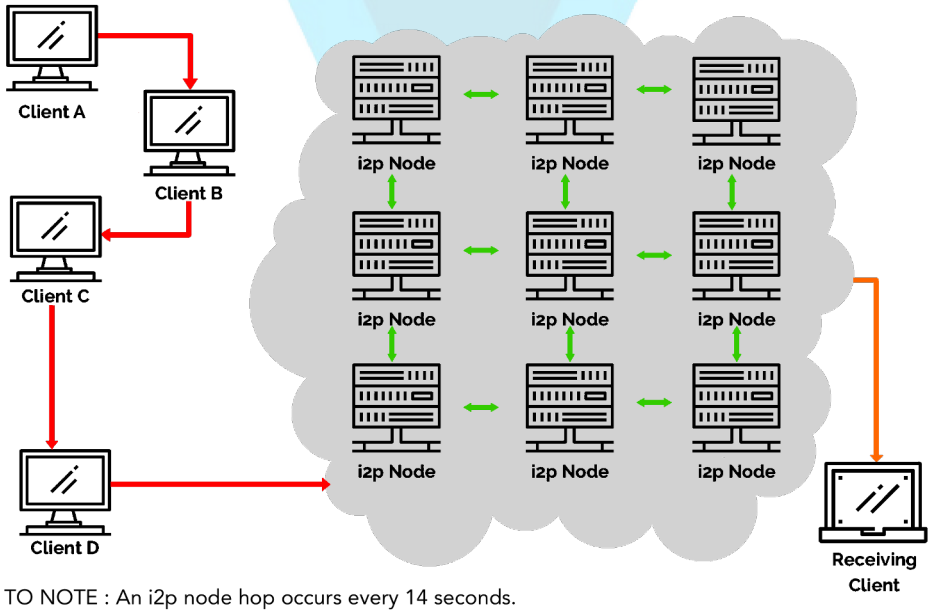
Onion routing wordt geïmplementeerd, door een encryptie in de applicatie laag van een communicatie protocol stack te plaatsen zoals de lagen van een ui. Tor versleuteld de data, inclusief de destination IP van de volgende node en verstuurd het meerdere malen door een virtueel circuit dat bestaat uit opeenvolgende, willekeurig geselecteerde Tor-relais. Elk relais ontcijfert niet meer dan nodig van de Data Packet Wrapper, om te weten van welke relais de gegevens vandaan komen en naar waar het doorgestuurd dient te worden. Het laatste relais ontcijfert de binnenste laag van encryptie en stuurt de oorspronkelijke gegevens naar de bestemming zonder het bron IP-adres te onthullen of zelfs te weten.

Doordat de routing van de communicatie tijdens elke hop in het Tor netwerk gedeeltelijk wordt verborgen, elimineert deze methode de mogelijkheid om een gesprek tussen twee mensen te traceren (internet toezicht). Om het te traceren moet zowel de bron als de bestemming bekend zijn

3.0 I2P Integratie

I2P is oorspronkelijk gebouwd om verborgen diensten te verlenen, waardoor mensen servers op onbekende locaties kunnen hosten. I2P biedt veel van dezelfde voordelen die Tor doet. Beiden maken anonieme toegang tot online content mogelijk, ze maken beiden gebruik van een P2P-stijl routingstructuur, en beide werken met gelaagde encryptie. Echter, i2P was ontworpen om een "netwerk binnen het internet" te zijn (zie afbeelding 2.1) met verkeer dat binnen deze grenzen bleef. I2P voert pakket-based routing uit, in tegenstelling tot het Tor's circuit based routing. Dit biedt het voordeel om met i2P dynamisch, opstoppingen en storingen op het internet om te leiden op een manier die vergelijkbaar is aan IP-routing van het internet. Dit zorgt voor een hoger niveau van betrouwbaarheid en redundantie van het netwerk.

Figure 2.1
How an i2p Transaction Occurs



TO NOTE : An i2p node hop occurs every 14 seconds.

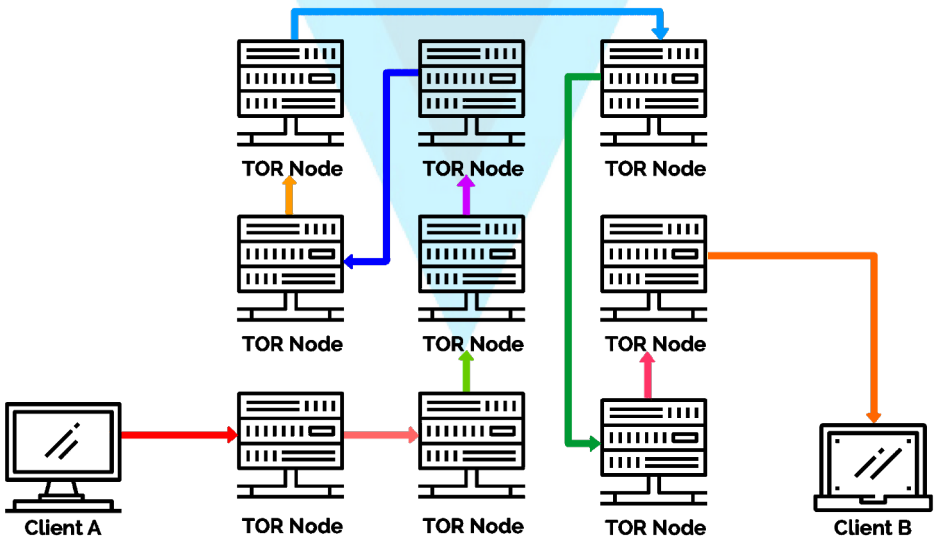
3.1 I2P Integratie

De eerste keer dat een klant contact opneemt met een andere klant, maken zij een query tegen de volledig gedistribueerde "netwerkdatabase" een aangepaste gestructureerde gedistribueerde hash-tabel (DHT), gebaseerd op het Kademlia-algoritme [2]. Dit is gedaan om de inkomende tunnels van de andere cliënt op een efficiënt manier te vinden, de opvolgende data bevat dit normaal gesproken waardoor er geen verdere gegevensuitwisseling noodzakelijk ia.

I2P is een krachtige verduistering tunneling service, dat met ipv6 alle Verge data anonimiseert dat wordt verzonden via het netwerk. Elke client applicatie heeft hun i2P "router" meerdere inkomende en uitgaande "tunnels" worden opgebouwd en een reeks peers die gegevens in één richting versturen (naar en van de klant respectievelijk) [2]. Wanneer een klant Verge gegevens naar een andere client wil verzenden, wordt de boodschap door een van hun uitgaande tunnels doorgestuurd naar een van de andere inkomende tunnels van de andere client, waardoor uiteindelijk de bestemming wordt bereikt.

In plaats van te vertrouwen op een gecentraliseerde set directory-servers zoals Tor, gebruikt i2P twee gedistribueerde hash-tabellen om de toestand van het netwerk te coördineren. Gedistribueerde hash-tabellen of DHT's zijn een gedistribueerd en vaak gedecentraliseerd mechanisme voor het associëren van hash-waarden met inhoud. Het belangrijkste voordeel van DHT's is hun schaalbaarheid. Een succesvol gedecentraliseerd P2P-netwerk vereist een goede schaalbaarheid van zijn diensten om ervoor te zorgen dat de inhoud of het delen van transacties kan blijven groeien zoals nodig is. Bovendien vertrouwt i2P niet op een vertrouwde directory service om routebeschrijving te krijgen. In plaats hiervan worden netwerkroutes gevormd en dynamisch bijgewerkt, waarbij elke router steeds andere routers evalueert. Ten slotte stelt i2P twee onafhankelijke simplex tunnels voor, om het netwerkverkeer van en naar elke gastheer te doorbreken in tegenstelling tot Tor's vorming van een enkelvoudig duplex circuit (zie figuur 1.1).

Figure 1.1
How a TOR Transaction Occurs



TO NOTE: A TOR nod hop occurs every 10 minutes.

4.0 Electrum

De kracht van Electrum is de snelheid en eenvoud, met een laag gebruik van middelen. Het maakt gebruik van beveiligde externe servers die de meest gecompliceerde onderdelen van het Verge-netwerk hanteren en ook gebruikers toestaan hun wallet te herstellen met een geheime Seed phrase. Daarnaast biedt Electrum een eenvoudige en gebruiksvriendelijke Cold storage oplossing aan. Hiermee kunnen gebruikers alle of een deel van hun munten op een offline manier opslaan. Bovendien is Electrum een van de weinig wallets die native Tor en i2P ondersteuning aanbied. Door het integreren van Electrum met Tor en i2P kan men een hoge mate van anonimiteit bereiken tijdens het gebruik van de desktop / mobiele wallets. Zowel het IP-adres als de transactiegegevens zijn beveiligd en lekken geen gegevens aan de verbindingsservers; Toenemende gebruikers privacy.

Electrum biedt ook ondersteuning aan multi-signature, waarbij meer dan één sleutel is vereist om een Electrum-transactie goed te keuren. Standaard transacties op het Verge-netwerk kunnen met "Single-signature transacties" [4] worden uitgevoerd. Omdat overdrachten slechts één handtekening nodig hebben van de eigenaar van de privé sleutel die geassocieerd is met het Verge adres. Een Electrum transactie, met ondersteuning voor meerdere handtekeningen, vereist de handtekeningen van meerdere personen of apparaten alvorens de munten kunnen worden overgedragen.

Voorbeeld:

"Een Electrum wallet is geïnstalleerd op de computer, de andere op je smartphone, de munten kunnen niet worden uitgegeven zonder een handtekening van beide toestellen. Zo moet een aanvaller toegang hebben tot beide apparaten om de munten te stelen"

Belangrijkste eigenschappen van een Electrum wallet

Deterministic Key Generation

Als de wallet kwijt is geraakt of niet meer toegankelijks is, kan dit met een Seed Phrase worden hersteld.

Instant On

de client downloadt geen blockchain, het vraagt om blokchain informatie van een server. Geen vertragingen, altijd up-to-date.

Locally signed Transactions

Uw privé sleutels worden niet gedeeld met de server. U hoeft de server niet te vertrouwen met uw munten.

Freedom and Privacy

De Electrum-server bewaart geen gebruikersaccounts. U bent niet gebonden aan een bepaalde server, en de server hoeft u niet te kennen. De Verge en I2P Electrum servers krijgen zelfs geen ip-adres van de klant. U kunt ook uw eigen sleutels exporteren, wat betekent dat u uw adres bezit.

5.0 Multi-Algoritme Ondersteuning

Verge is een multi-algoritme cryptocurrency die is ontworpen om mensen met verschillende soorten mining hardware in staat te stellen even veel munten te minen. Het is een van de weinige cryptocurrencies die 5 hash functies ondersteunt en ze heeft gecombineerd op één blockchain. Dit verhoogd de beveiliging van de blockchain en zorgt ervoor dat het beter verspreid wordt, het voor een grotere groep toegankelijk is en eerlijk wordt verdeeld

In totaal zijn er 16.5 miljard munten. Wat ervoor zorgt dat Verge zich van andere cryptocurrencies onderscheidt, zijn de 5 verschillende Proof-of-Work-algoritmen die op de blockchain draaien, namelijk Scrypt, X17, Lyra2rev2, myr-groestl en blake2s. Alle 5 algoritmen hebben een 30 seconden block target time. De moeilijkheid wordt enkel beïnvloed door het hash rate van het algoritme. Dit zorgt voor verbeterde beveiliging en bescherming tegen 51% van de aanvallen.

6.0 Android Tor + I2P

Verge is een van de koplopers op het gebied van innovatie in de mobiele cryptocurrency's. We hebben gepionierd en hebben twee zeer unieke en eerste in hun soort android wallets ontwikkeld. Een daarvan werkt uitsluitend op The Onion Router Network (Tor) en de andere werkt uitsluitend op het Invisible Internet Project (i2P). De Verge Tor en I2p wallet zijn gebouwd met als doel de anonimiteit van de eigenaar te beschermen. De wallet heeft geen ingebouwde mogelijkheid om gebruikersinformatie over Clearnet te verbinden of uit te zenden. Transacties worden voltooid via Simple Payment Verification (SPV), een techniek beschreven in het papier van Satoshi Nakamoto, waarmee de wallet transacties kan verifiëren door middel van bewijs van opname; Een methode om te controleren of een bepaalde transactie in een blok is opgenomen zonder het gehele blok te downloaden (vergelijkbaar met hoe een Electrum-wallet functioneert).

SPV zorgt er voor dat betalingen bijna direct worden bevestigd, omdat het als een light client werkt die alleen de block headers hoeft te downloaden welke kleiner zijn dan de volledige blokken. De Verge Tor en i2P wallet hebben daarnaast ook beveiligingsfuncties ingebouwd, zoals een 4-cijferige pincode en biometrische vergrendelingsmogelijkheden voor een extra fysieke beveiliging. Daarnaast kunnen de Verge Tor- en i2P wallets ook P2P QR-code scannen, de transacties zijn direct geverifieerd en overgemaakt. Met deze wallets is het ook mogelijk om een QR code te scannen van een paper wallet om zo saldo uit de paper wallet te halen (Cold storage).

7.0 Toekomstige ontwikkeling: RSK

Rootstock, of ook wel aangeduid als RSK, is een smart contractfunctionaliteit dat in twee richtingen op het Verge netwerk wordt geïntegreerd. Het introduceert ook een off-chain protocol voor onmiddellijke betalingen. RSK is een onafhankelijke blockchain die geen eigen token heeft, maar bestaat op bestaande tokens (zoals Verge). RSK kan dit doen door zijn smart token aan Verge te koppelen, zodat de waarde van een RSK-token gelijk is aan die van een Verge token. Gebruikers hebben de mogelijkheid om hun tokens heen en weer te verplaatsen tussen de twee blockchains.

Een smart contract werkt door het plaatsen van x aantal Verge's van een gebruiker in een soort reserve, waar het is vergrendeld en vervolgens wordt gebruikt om de RSK-token ook wel bekend als smartXVG te gebruiken. Neem als voorbeeld dat Verge op een rekening wordt gezet en dat het RSK netwerk wordt gebruikt om het geld uit te geven. Het is goed om op te weten dat er voor Bitcoin ook eenvoudige contracten zijn opgezet waarmee gebruikers contracten kunnen maken, zoals bijvoorbeeld multisig dat twee of meer gebruikers vereist voor goedkeuren van een betaling voordat het kan worden vrijgegeven. Met de implementatie van RSK op Verge worden eenvoudige slimme contracten naar heel nieuw niveau gebracht, die de concurrentiestrijd zullen aan gaan met Ethereum met betrekking tot de slimme contracten.

Een ander voordeel van RSK is het vermogen om op te schalen. RSK realiseert momenteel 400 betalingen per seconde, dat is een enorme toename in vergelijking met onze huidige vaste transactiecapaciteit; Ongeveer 100 per seconde. Het RSK ontwikkelingsteam heeft in een verklaring aangegeven dat het uiteindelijke doel is om de lat nog hoger te leggen en in de toekomstige 2000 transacties per seconde te verwerken door gebruik te maken van een tweede laag technologie genaamd Lumino. Zoals vermeld in de LCTP-whitepaper, is het Lumino netwerk een betalingssysteem dat gebaseerd is op een protocol dat bekend staat als het Lumino Transaction Compression Protocol. De LTCP kan worden vergeleken met het Lightning Network, een oplossing voor die oorspronkelijk is ontworpen voor bitcoin dat momenteel op Litecoin wordt getest.

8.0 Toekomstige ontwikkeling: Discord & Telegram P2P

Peer-to-Peer (P2P) transactie ondersteuning voor Telegram en Discord zijn momenteel in ontwikkeling en wordt in augustus worden vrijgegeven. Telegram is een gratis cloudbased instant messaging service die op Android, IOS, Windows Phone, Windows NT, MacOS en Linux draait. Telegram maakt gebruik van een symmetrische encryptie schema genaamd MTProto. Het protocol is ontwikkeld door Nikolai Durov en andere ontwikkelaars bij Telegram en is gebaseerd op 256-bits symmetrische AES-encryptie, RSA 2048-encryptie en Diffie-Hellman-sleutelwisseling. Discord is een proprietary freeware VoIP applicatie die wijdverspreide adoptie in de crypto community heeft. Discord heeft, draait net zoals Telegram, op Windows, MacOS, Android, iOS en heeft een browser-toegankelijke webclient. Het implementeren van Verge P2P-mogelijkheden op deze platforms stelt gebruikers in staat om geld te verzenden en ontvangen, ongeacht waar ze zijn (ongeacht of ze een eigen portemonnee hebben geïnstalleerd of niet).

P2P is een online technologie waarmee gebruikers munten kunnen overbrengen via internet of smartphone. Om dit te doen moeten de consumenten een online applicatie, of in dit geval een bot gebruiken om een hoeveelheid munten overdragen naar de ontvanger. De ontvanger wordt aangewezen door hun gebruikersnaam en zodra de overdracht is gestart door de afzender, ontvangt de ontvanger dan een melding om de online bot te gebruiken en dat hij een betaling heeft ontvangen op een nieuw verborgen adres. De gebruiker wordt dan toegelaten om de bot te tweet te sturen en met een simpel commando, zoals "! Withdraw" wordt vervolgens instructies opgevraagd over hoe ze hun nieuw verworven Verge kunnen ontvangen. Deze service vereist geen aanvullende informatie behoudens de alias/naam en het aantal Verge dat naar de ontvanger moet worden verzonden.Er worden geen privacygegevens zoals IP-adressering, locatie, naam bewaard tijdens dit proces. Uw persoonlijke identiteit buiten het initiëren van de transactie blijft volledig anoniem.

Verge is een van de enige cryptocurrencies met P2P oplossingen voor Twitter, Reddit, Internet Relay Chat (IRC), Slack and Steam te bieden. Met deze P2P-aanbiedingen kunnen gebruikers Verge overbrengen aan iedereen binnen hetzelfde sociale platform.

9.0 Referenties

[1] Nakamoto, S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

[2] I2P: A scalable framework for anonymous communication - I2P. (n.d.). Retrieved from https://geti2p.net/en/docs/how/tech-intro

[3] Multisignature - Bitcoin Wiki. (n.d.). Retrieved August 8, 2017, from https://en.bitcoin.it/wiki/Multisignature

[4] Voegtlin, T. (n.d.). Welcome to the Electrum Documentation! — Electrum 2.5 documentation. Retrieved August 8, 2017, from http://docs.electrum.org/en/latest/

Aanvullende referenties:

Gribble, S., Brewer, E., Hellerstein, J., & Culler, D. (2000, October 23). Scalable, Distributed Data Structures for Internet Service Construction. Retrieved from https://www.usenix.org/legacy/events/osdi2000/full_papers/gribble/gribble_html/index.html

Anonymity and the Block Chain • IHB News™. (2014, November 18). Retrieved August 08, 2017, from https://ihb.io/2014-11-17/news/anonymity-block-chain-13570

Holden, E. (2017, July 18). An Introduction to Tor vs I2P. Retrieved August 08, 2017, from https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p

Distributed hash table. (n.d.). Retrieved August 08, 2017, from http://infoanarchy.org/Distributed_hash_table

Scharr, J. (2013, October 23). What Is Tor - How Does Tor Work - How to Use Tor. Retrieved August 08, 2017, from https://www.tomsguide.com/us/what-is-tor-faq,news-17754.html

Durumeric, Z., Wustrow, E., & Halderman, J. (2013). ZMap: Fast Internet-Wide Scanning and its Security Applications. Retrieved from https://zmap.io/paper.pdf

Voegtlin, T. (2015). Simple Payment Verification — Electrum 2.5 documentation. Retrieved from http://docs.electrum.org/en/latest/spv.html

SPV, Simplified Payment Verification - Bitcoin Glossary. (2017). Retrieved from https://bitcoin.org/en/glossary/simplified-payment-verification

https://atlas.torproject.org/#search/flag:authority

http://torstatus.blutmagie.de/

10.0 Contributors

As an open source project we find it very important to thank our contributors who have given us a helping hand in order for us to get to where we are today.

To that we say

Thank you

Translators

CryptoRekt

The Author

CryptoRekt

O.G Verge Development Team

Sunerok
Gfranko
CryptoRekt

Contributors

Core Marketing Team

@Spookykid
@CryptoRekt
@gfranko
@DJ_Erock23
@Crypto_K1NG
@JtheLizzard
@lucklight
@Cryptonator92
@feyziozsahin
@Slemicek
@Trilla6six6
@Dabbie USA
@Cyrus7at
@Thehunter9 Netherlands
@GGWeLost
@Jeanralphio69
@Crypth
@deheerlen
@Twomanytimes
@ScagFX
@TraderNILW

Github Contributors

Sunerok
Gfranko
CryptoRekt
Mkinney
badbrainIRC
Grinfax
Swat69
NeosStore
Koenwoortman
Hellokarma
Kirillseva
Fuzzbawls
Buzztiaan
Spiralmann666
stshort
alcy0ne
chisustation
ShapeShifter499
Infernoman
pallas1
bearsylla
2Dai
31percent
Racoooon
ceasarpolar
enewnanwebdev
giovanni1186
labelmeagod

Contact Info

Twitter Telegram Slack Facebook IRC Reddit Steam Verge Discord BitCoinTalk Radio Station