
VERGE
The most privacy focused cryptocurrency
BLACKPAPER

# 1.0 Introduction

Bitcoin wurde 2009 als Antwort auf die inhärenten Fehler entwickelt und veröffentlicht, welche sich in der Art und Weise äußerten, wie Transaktionen über das Internet abgewickelt worden. entwickelt und veröffentlicht. In seinem „Whitepaper“ erklärte Nakamoto dass “Der Handel im Internet sich fast ausschließlich auf Finanzinstitute verlassen hat, die als vertrauenswürdige Dritte dienen, um elektronische Zahlungen zu verarbeiten. Während das System für die meisten Transaktionen gut genug funktioniert, leidet es immer noch an den inhärenten Schwächen des vertrauensbasierten Modells.” [1]. Seit seiner ursprünglichen Gründung im Jahr 2009 wurde Bitcoin schnell in die heutigen modernen Marktplätze integriert. Ein primäres Thema durch die schnelle Annahme von Bitcoin´s ist die Zunahme der Nachfrage an der ursprünglichen Blockchain, um unterschiedliche Grade großer Transaktionen zu bewältigen. Durch die erhöhte Nachfrage entstehen erhöhte Transaktionswartezeiten. Dies hat in Versuchen zu höheren Transaktionsgebühren geführt weil man dadurch versuchte die längeren Transaktionsbestätigungszeiten zu beschleunigen.

Die Kerninnovation hinter Bitcoin ist die dezentrale Struktur. Im Gegensatz zu herkömmlichen Fiat-Währungen hat Bitcoin keine zentrale Kontrolle, kein zentrales Archiv von Informationen, kein zentrales Management und keinen zentralern Punkt des Versagens. Eine der Herausforderungen, vor denen Bitcoin steht, ist, dass die meisten der e-Services und E-Businesses, die um das Bitcoin-Ökosystem gebaut sind, zentralisiert sind. Aufgrund der zentralisierten Natur des derzeitigen Systems wird E-Commerce von Einzelpersonen an bestimmten Orten geführt, die anfällige Computersysteme nutzen, welche anfällig für legale Verstrickungen sind. Verge ist eine der wirklich dezentralisierten Währungen, die heute aufgrund seiner ständigen Verpflichtung zum Aufbau der Kerngrundlagen von Bitcoin zur Verfügung stehen, während dadurch eine völlig neue Ebene von Anonymität realisiert wird.

# 2.0 Tor Netzwerk

Tor, abgeleitet von einem Acronym für die ursprünglichen Softwareprojektnamen „The Onion Router“ ist ein IP-Verschleierungs Dienst, der über ein geschichtetes schaltungsbasiertes Netzwerk anonyme Kommunikation ermöglicht. Tor leitet den Internet-Verkehr durch ein kostenloses weltweites Freiwilligen-Overlay-Netzwerk, das aus mehr als siebentausend Relais besteht, um den Standort und die Nutzung eines Nutzers von jedem, der eine Netzwerküberwachung oder eine Verkehrsanalyse durchführt, zu verbergen. Die Schichten der verschlüsselten Adressinformationen, die verwendet werden, um die von Tor gesendeten Datenpakete zu anonymisieren, erinnern an eine Zwiebel, daher auch der Name. Auf diese Weise kann der Weg eines Datenpakets durch das Tor-Netzwerk nicht vollständig verfolgt werden. Die Verwendung von Tor beabsichtigt, die Privatsphäre der Nutzer zu schützen, sowie ihre Freiheit und ihre Fähigkeit, eine vertrauliche Kommunikation zu führen, indem sie ihre Internetaktivitäten vor Überwachung schützt.

Das Onion-Routing wird durch Verschlüsselung in der Anwendungsschicht eines Kommunikationsprotokollstapels implementiert, der wie die Ebenen einer Zwiebel verschachtelt ist. Tor verschlüsselt die Daten, einschließlich der nächsten Knoten-Ziel-IP, mehrmals und sendet sie durch eine virtuelle Schaltung, die aufeinanderfolgende, zufällig ausgewählte Tor-Relais umfasst. Jedes Relais entschlüsselt nur genug von dem Datenpaket-Wrapper, um zu wissen, von welchem Relais die Daten kamen, und welches Relais es sein muss, um es zum nächsten zu senden. Das Relais umwickelt dann das Paket in einem neuen Wrapper und sendet es weiter. Das endgültige Relais entschlüsselt die innerste Verschlüsselungsschicht und sendet die ursprünglichen Daten an sein Ziel, ohne die Quell-IP-Adresse aufzudecken oder gar zu kennen.

Weil das Routing der Kommunikation bei jedem Sprung in der Tor-Schaltung teilweise verborgen ist, beseitigt diese Methode jeden einzelnen Punkt, an dem die kommunizierenden Peers durch Netzwerküberwachung bestimmt werden können, die auf dem Erkennen ihrer Quelle und ihres Ziels beruht.

# 3.0 I2P Integration

I2P wurde ursprünglich entwickelt, um versteckte Dienste bereitzustellen, die es Menschen ermöglichen, Server an unbekannten Orten zu hosten. i2P bietet viele der gleichen Vorteile, welche auch Tor bietet. Beide erlauben anonymen Zugriff auf Online-Inhalte, nutzen eine P2P ähnliche Routing-Struktur und beide arbeiten mit Layer-Verschlüsselung. Allerdings wurde i2P als "Netzwerk im Internet" konzipiert, wobei der Verkehr nur in diesen Grenzen stattfindet. i2P führt paketbasiertes Routing im Gegensatz zu Tor's Circuit Based Routing durch. Dies bietet den Vorteil, dass i2P dynamisch Staus und Dienstunterbrechungen in ähnlicher Weise wie das IP-Routing des Internets umgehen kann. Dies bietet eine höhere Zuverlässigkeit und Redundanz für das Netzwerk selbst.

Das erste Mal, wenn ein Client einen anderen Client kontaktieren möchte, macht er eine Abfrage gegen die vollständig verteilte "Netzwerkdatenbank" - eine benutzerdefinierte, strukturierte verteilte Hash-Tabelle (DHT), die auf dem Kademlia-Algorithmus basiert [2]. Dies geschieht, um die eingehenden Tunnel des anderen Clients effizient zu finden, aber nachfolgende Daten zwischen ihnen enthalten in der Regel diese Informationen, so dass keine weiteren Netzwerkdatenbank-Lookups erforderlich sind.

I2P ist ein hochverschleierter Tunneling-Service mit ipv6, der alle Verge-Daten, die über das Netzwerk gesendet werden, anonymisiert. Jede Client-Anwendung hat ihre i2P "Router", um mehrere eingehende und ausgehende "Tunnel" zu bauen - eine Folge von Peers, die Daten in eine Richtung (bzw. von dem Client) [2] übergeben. Im Gegenzug, wenn ein Client Verge-Daten an einen anderen Client senden will, übergibt die Anwendung die Nachricht durch einen ihrer ausgehenden Tunnel, die auf einen der eingehenden Tunnel des anderen Clients gerichtet sind und schließlich das Ziel erreichen.  Anstatt sich auf einen zentralen Satz von Verzeichnisservern wie Tor zu verlassen, verwendet i2P zwei verteilte Hash-Tabellen, um den Status des Netzwerks zu koordinieren.

Verteilte Hash-Tabellen oder DHTs sind ein verteilter und oft dezentralisierter Mechanismus für die Zuordnung von Hash-Werten mit Inhalt. Der Hauptvorteil für DHT ist ihre Skalierbarkeit. Ein erfolgreiches dezentrales P2P-Netzwerk erfordert eine gute Skalierbarkeit seiner Dienste, um sicherzustellen, dass die Größe des Inhalts oder der Transaktionen nach Bedarf weiter wachsen kann. Darüber hinaus verweist i2P nicht auf einen vertrauenswürdigen Verzeichnisdienst, um Routeninformationen zu erhalten. Stattdessen werden Netzwerkrouten gebildet und ständig dynamisch aktualisiert, wobei jeder Router ständig andere Router auswertet. Schließlich stellt i2P zwei unabhängige Simplex-Tunnel für den Verkehr her, um das Netzwerk zu und von jedem Host zu bewegen, im Gegensatz zu Tors Bildung einer einzelnen Duplex-Schaltung.

# 4.0 Electrum

Die Stärke von Electrum ist Geschwindigkeit und Einfachheit, mit geringer Ressourcennutzung. Es verwendet sichere Remote-Server, die die kompliziertesten Teile des Verge-Netzwerks behandeln und es den Benutzern ermöglichen, ihre Wallets mit einer geheimen Wort-Phrase wiederherzustellen. Darüber hinaus bietet Electrum eine einfache und einfach zu bedienende "Cold Wallet"-Lösung. Dies ermöglicht es Benutzern, alle oder einen Teil ihrer Währung offline zu speichern. Darüber hinaus ist Electrum eine der einzigen Wallets, die native Tor- und i2P-Unterstützung bieten. Durch die Integration von Electrum mit Tor und i2P kann man bei der Verwendung der Desktop- bzw. mobilen Wallet Anonymität erreichen. Sowohl die IP-Adresse als auch die Transaktionsinformation sind gesichert und werden nicht durch die Verbindungsserver verraten; Erhöhung der Privatsphäre des Nutzers.

Electrum ermöglicht Multi-Signatur-Unterstützung, die mehr als einen Schlüssel benötigt, um eine Electrum-Transaktion zu autorisieren. Standardtransaktionen im Verge-Netzwerk könnten als "Single-Signatur-Transaktionen" bezeichnet werden [4], da Transfers nur eine Signatur erfordern - vom Eigentümer des privaten Schlüssels, der mit der Verge-Adresse verknüpft ist. Eine Electrum-Transaktion mit Multi-Signatur-Unterstützung erfordert die Signatur von mehreren Personen, bevor die Währung übertragen werden kann. Verge benötigt dann viele verschiedene Adressen mehrerer Parteien zur Verfügung gestellt, um etwas mit ihnen zu tun.

Hier ist ein Beispiel:

> "Eine Electrum Wallet ist auf deinem primären Computer, die andere auf deinem Smartphone - die Währung kann nicht ohne Signatur von beiden Geräten ausgegeben werden. So muss ein Angreifer Zugang zu beiden Geräten erhalten, um die Währung zu stehlen."

## Hauptmerkmale der Electrum Wallet:

### Deterministische Schlüsselgenerierung

Wenn du deine Wallet verlierst, kannst du sie aus deiner Wort-Phrase wiederherstellen. Sie sind vor Ihren eigenen Fehlern geschützt.

### Sofort verfügbar

Der Client lädt die Blockchain nicht herunter, er fordert Blockchain-Informationen von einem Server an. Keine Verzögerungen, immer up-to-date.

### Transaktionen werden lokal signiert

Ihre privaten Schlüssel werden nicht mit dem Server geteilt. Du musst dem Server nicht bei deiner Währung vertrauen.

### Freiheit und Privatsphäre

Der Electrum Server speichert keine Benutzerkonten. Sie sind nicht an einen bestimmten Server gebunden, und der Server muss Sie nicht kennen. In der Tat, die Verge und i2P Electrum Server erhalten nicht einmal eine IP-Adresse vom Client. Sie können auch Ihre privaten Schlüssel exportieren, d.h. Sie besitzen Ihre Adresse.

# 5.0 Multi-Algorithmus Unterstützung

Verge ist eine auf Multi-Algorithmus basierende Kryptowährung, welche entworfen wurde, um Menschen mit verschiedenen Arten von Mining-Geräten zu ermöglichen, in gleicher Weise Coins zu schürfen. Es ist eine der einzigen Kryptowährungen, welch 5 Hash-Funktionen auf einer Blockchain unterstützt. Dies führt zu erhöhter Sicherheit und einer breiteren Palette von Personen und Geräten, die Verge minen können. Daher ist die Verteilung von Verge für jeden gleich. Die Gesamtversorgung von Verge beträgt 16,5 Milliarden Münzen.

Was Verge von anderen Kryptowährungen abhebt, sind die 5 Proof-of-Work-Algorithmen, die auf seiner Blockchain laufen, nämlich Scrypt, X17, Lyra2rev2, myr-groestl und blake2s. Alle 5 Algorithmen haben eine 30-Sekunden-Block Zielblockzeit. Die Schwierigkeit wird nur durch die Hash-Rate des Algorithmus beeinflusst. Dies ermöglicht eine verbesserte Sicherheit und Schutz gegen 51% Angriffe.

# 6.0 Android Tor + I2P

Verge sitzt an der Spitze der Innovation im mobilen Krypto-Raum. Wir haben zwei in ihrer Art sehr einzigartige Antdroid Wallets entwickelt und ihnen den Weg bereitet. Eines davon arbeitet ausschließlich auf dem Onion Router Network (Tor) und das andere ecklusiv auf dem Invisible Internet Project (i2P). Die Verge Tor und I2P Wallets sind um die Prämisse der Anonymität gebaut. Die Wallets haben keine Möglichkeit, Benutzerinformationen über das Clearnet zu verbinden oder zu verbreiten. Transaktionen werden durch Simple Payment Verification (SPV) abgeschlossen, eine Technik, die in Satoshi Nakamotos Papier beschrieben ist, welche es erlaubt, die Wallets zu verifizieren, um Transaktionen durch den Nachweis der Einbeziehung zu überprüfen; eine Methode zum Verifizieren, ob eine bestimmte Transaktion in einem Block enthalten ist, ohne den gesamten Block herunterzuladen (ähnlich wie eine Electrum-Wallet funktioniert).

SPV ermöglicht fast sofortige Zahlungsbestätigungen, da es als Thin Client fungiert, der nur die Blockheader herunterladen muss, die drastisch kleiner als Vollblöcke sind. Die Verge Tor- und i2P Wallets haben auch Sicherheitsmerkmale wie einen 4-stelligen PIN-Code und biometrische Sperroptionen für eine zusätzliche Ebene physischer Sicherheit eingebaut.

Darüber hinaus sind die Verge Tor und i2P Wallets in der Lage, P2P QR-Code-Scan-Transaktionen mit sofortiger Überprüfung zu behandeln. Die Clients können auch QR-Codes aus Paper Wallets importieren, um Guthaben aus dem "Cold Wallet" zu ziehen, falls erforderlich.

# 7.0 Zukünftige Entwicklung : RSK

Rootstock, oder gemeinhin als RSK bezeichnet, ist eine Zwei-Wege-Zacken-Sidechain, welche "Smart Contracts"-Funktionalität auf das Verge-Netzwerk anwendet. Es stellt auch ein Off-Chain-Protokoll für Fast-Sofort-Zahlungen vor. RSK ist eine unabhängige Blockchain, welche kein eigenes Token hat, sondern stützt sich auf bestehende Token (wie zB. Verge). RSK ist in der Lage, dies zu tun, indem man sein Smart Token an Verge anpasst, so dass der Wert eines RSK-Tokens genau dem eines Verge-Tokens entspricht. Benutzer haben die Fähigkeit, ihre Tokens hin und her zwischen den beiden Chains zu bewegen.

Ein Smart Contract arbeitet, indem er die Verge eines Nutzers in eine Art Reserve packt, in welcher es gesperrt ist und dann als Rückhalt für den RSK-Token verwendet wird, auch bekannt als smartXVG. Ähnlich als wenn deine Verge in ein Girokonto gepackt werden und dann das RSK-Netzwerk genutzt wird, um das Geld zu versenden. Es ist wichtig zu beachten, dass einfache Kontrakte für Bitcoin vorhanden sind, die es Benutzern ermöglichen, Kontrakts zu erstellen, wie mutlisig, die zwei oder mehr Benutzer benötigen, um sich bei einer Zahlung abzumelden, bevor sie veröffentlicht werden kann. Mit der Implementierung von RSK auf Verge werden einfache Smart Kontrakts auf eine ganz neue Ebene gebracht, mit kompletten Smart Kontract-Fähigkeiten, die Kopf-an-Kopf mit Ethereums aktuellen Angeboten gehen werden.

Ein weiterer Vorteil von RSK ist seine Skalierbarkeit. RSK erreicht derzeit 400 Zahlungsvorgänge pro Sekunde, was im Vergleich zu unserer derzeitigen Transaktionsrate ein großer progressiver Sprung ist. Etwa 100 pro Sekunde. Das RSK-Entwicklungsteam hat erklärt, dass es das Ziel ist, die Messlatte mit zukünftigen Zielen sogar noch höher zu stecken, um 2.000 Transaktionen pro Sekunde mit einer zweiten Technikebene namens Lumino zu unterstützen. Wie im LCTP-Whitepaper angegeben, ist das Lumino-Netzwerk ein off-chain-Zahlungssystem, das auf einem Protokoll basiert, das als das Lumino Transaction Compression Protocol bekannt ist. Der LTCP kann mit dem Lightning Network verglichen werden, einer Skalierlösung, die ursprünglich für Bitcoin entwickelt wurde, welche derzeit auf Litecoin getestet wird.

# 8.0 Zukünftige Entwicklung : Discord & Telegram P2P

Peer-to-Peer (P2P) Transaktionsunterstützung für Telegramm und Discord (bereits freigegeben) befindet sich derzeit in der Entwicklung und es ist geplant dieses der Öffentlichkeit im Monat August freizugeben. Telegramm ist ein kostenloser Cloud-basierter Instant Messaging Service, der Android, iOS, Windows Phone, Windows NT, MacOS und Linux unterstützt. Telegramm verwendet ein symmetrisches Verschlüsselungsschema namens MTProto. Das Protokoll wurde von Nikolai Durov und anderen Entwicklern bei Telegram entwickelt und basiert auf symmetrischer 256-bit AES-Verschlüsselung, RSA 2048 Verschlüsselung und Diffie-Hellman Schlüsselaustausch. Discord ist eine proprietäre Freeware-VoIP-Anwendung, die eine weit verbreitete Verwendung in der Krypto-Community hat. Wie Telegramm wird auch Discord auf Windows, MacOS, Android, iOS unterstützt und hat einen per Browser zugänglichen Web-Client. Die Implementierung von Verge P2P-Fähigkeiten auf diesen Plattformen ermöglicht es Benutzern, Geld zu senden und zu empfangen, egal wo sie sind (egal ob sie eine tatsächliche Wallet installiert haben oder nicht).

P2P ist eine Online-Technologie, die es Benutzern ermöglicht, Währungen über das Internet oder Mobilgeräte zu transferieren. Um dies zu tun, verwenden die Verbraucher eine Online Anwendung oder in diesem Fall einen Bot - um die Menge der zu übertragenden Währung zu benennen. Der Empfänger wird nur durch seinen Benutzernamen benannt und sobald die Übertragung vom Absender eingeleitet wurde, erhält der Empfänger dann eine Benachrichtigung, um den Online-Bot zu nutzen. - Dass er eine Zahlung bei einer neu gegründeten Einzahlungsadresse erhalten hat. Der Benutzer kann dem Bot dann mit einem einfachen Befehl wie "!withdraw" Anweisungen geben und festlegen, wie dieser die neu erworbenen Verge erhalten möchte. Dieser Dienst benötigt keine zusätzlichen Informationen außer über den Betrag, den du senden möchtest und an den er gesendet werden soll. Während dieses Vorgangs werden keine Datenschutzinformationen wie IP-Adressierung, Standort, Name beibehalten. Ihre persönliche Identität außerhalb der Einleitung der Transaktion bleibt völlig anonym.

Verge ist eine der einzigen Kryptowährungen, welche bereits P2P-Lösungen für Twitter, Reddit, Internet Relay Chat (IRC), Slack und Steam anbieten kann. Diese P2P-Angebote erlauben es Benutzern, Verge an jeden zu senden, welcher sich auf der gleichen sozialen Plattform befindet wie er selbst.

# 9.0 Referenzen

[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/

## Weitere Referenzen:

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 Mitwirkende

Als Open-Source-Projekt finden wir es sehr wichtig, unseren Mitwirkenden zu danken, welche uns eine helfende Hand gereicht haben, um da zu sein, wo wir heute sind.

Dazu sagen wir:

Vielen Dank!

## Übersetzer

**@CYANO**

## Der Autor

**CryptoRekt**

## Core Entwickler von Verge

**Sunerok**
**Gfranko**
**CryptoRekt**

## Mitwirkende

### Verge Werbeabteilung

**@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 Mitwirkende

**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