



Viacoin Whitepaper

Viacoin Entwicklerteam
12. September 2017

Letzte Aktualisierung am 22. September 2017

Abstract

Viacoin ist eine 2014 entwickelte Open-Source-Kryptowährung, die vom [6] Bitcoin-Protokoll abgeleitet wurde, welches Embedded Consensus mit einem erweiterten OP_RETURN von 120 Byte unterstützt. Viacoin bietet Scrypt Merged Mining, auch als Auxiliary Proof of Work oder AuxPoW bezeichnet und 25-mal schnellere Transaktionen als Bitcoin. Die Profithalbierung des Viacoin-Minings findet alle 6 Monate statt und hat ein GesamtSupply von 23,176,392.41459 Coins. Die Inflationsrate von Viacoin ist aufgrund der minimalen Miningbelohnung niedrig. Aufgrund des geringen Block-Rewards von Viacoin erhalten Miner einen Anreiz, Viacoin über Merged Mining (AuxPoW) zu minen. Viacoin wird derzeit von einem der größten Mining-Pools (F2Pool) mit aktuell einer der höchsten Hashrates gemint.

Weitere Features sind ein Algorithmus zur Anpassung der Mining-Schwierigkeit, welcher die Behebung von Fehlern in Kimotos Gravity Well (DarkGravityWave) ermöglicht, Versionsbits, um gleichzeitig 29 Soft-Fork-Änderungen zu ermöglichen, Segwit und das Lightning-Network.

Hinweis: Das Whitepaper, die Dokumentation und die Designs befinden sich in der Forschungs- und Entwicklungsphase und können sich ändern.



Viacoin Whitepaper

1. Scrypt

In der Kryptographie ist [7] Scrypt eine von Colin Percival kreierte passwortbasierte Key-Derivation-Function. Der Algorithmus wurde entwickelt, um das Durchführen von groß angelegten Hardware-Angriffen durch das Erfordern großer Speichermengen teuer zu machen. Ursprünglich wurde sollte ein 2012 von der IETF veröffentlichter Entwurf ein Informational-RFC werden, aber eine Version von Scrypt wird nun als Proof of Work Schema von Kryptowährungen wie Viacoin verwendet.

Scrypt ist eine Memory-Hard-Key-Derivation, welche eine ziemlich große Menge an auszuwertender Random Access-Memory benötigt. Dies führt dazu, dass die Implementierung in spezieller anwendungsspezifischer Hardware (ASICs) einen größeren VLSI-Bereich erfordert, was das ASIC-Mining bei Viacoin unrentabel macht. Der auf TMT0 (Time-Memory Tradeoff) basierende Scrypt-Algorithmus erfordert eine große Anordnung von Pseudo-Random-Bits, die im Speicher gehalten werden sollen und davon abzuleitenden Key. Im Vergleich zu Bitcoin ist der Vorteil von ASIC in Viacoin um den Faktor 10 reduziert.

Scrypt verwendet die folgenden Parameter, um einen abgeleiteten Schlüssel zu generieren:

- Passphrase: Zeichenkette zum Hashen
- Salt: Zufällige Zeichenfolge für Scrypt-Funktionen
- N: Speicher / CPU-Kostenparameter
- P: Parallelisierungsparameter
- R: Blockgrößen-Parameter
- dkLen: Beabsichtigte Länge des abgeleiteten Keys in Bytes

`kd = scrypt(P, S, N, P, R, dkLen)`

Mit den Viacoin-Parametern N = 1024, R = 1, P = 1 und S = random 80 Bytes wird ein 256-Bit-Ausgang erzeugt.



Viacoin Whitepaper

2. Merged Mining AuxPoW

Das Viacoin [2] Merged Mining zielt darauf ab, die Mining-Power anderer [7] Scrypt-Coins wiederzuverwenden, um der Viacoin-Blockchain mehr Sicherheit zu geben und es einem Miner zu ermöglichen, gleichzeitig mehr als eine Blockchain zur gleichen Zeit zu minen. Zum Beispiel könnte ein Miner Viacoin und Litecoin, oder irgendeinen anderen Scrypt-Coin zusammen mit Viacoin minen, mit wenig oder keinem Einfluss auf die Hash-Rate beider.

Jeder Hash, den der Miner beisteuert, ist für die gesamte Hashrate beider Kryptowährungen und führt zu einer sichereren Blockchain. Ein AuxPoW-Block ist eine Art von Block, ähnlich einem Standard-Bitcoin-Block mit zwei Unterschieden. Der Hash des Blockheaders entspricht nicht dem Schwierigkeitsgrad der Blockchain. Zweitens hat es zusätzliche Datenelemente, die zeigen, dass der Miner, der einen Block erstellt hat, auf der Parent-Blockchain Mining durchgeführt hat und dass der Schwierigkeitsgrad der Aux-Blockchain erfüllt ist.

Miner haben einen Anreiz, Viacoin zu minen, auch wenn die Belohnung niedrig ist, da sie in der Lage sind, jeden anderen Scrypt-Coin gleichzeitig "kostenlos" zu gewinnen. Da das Mining von Viacoin nicht durch große Blockprämien vorangetrieben wird, kann Viacoin eine niedrigere Inflationsrate im Vergleich zu anderen Kryptowährungen aufweisen, die den kombinierten Miningprozess nicht unterstützen.

3. Dark Gravity Wave

[3] Dark Gravity Wave (DGW) ist ein Open-Source-Schwierigkeitsalgorithmus, welcher von Evan Duffield, dem Entwickler und Schöpfer von X11 / Darkcoin / Dash, geschrieben wurde. Entwickelt wurde der Algorithmus, um Fehler wie den Time-Warp-Angriff im Kimoto Gravity Wave-Algorithmus zu beheben.

Dark Gravity Wave wurde zuerst in Dash (Darkcoin) eingeführt. DGW verwendet mehrere exponentielle gleitende Mittelwerte und einfache gleitende Mittelwerte, um den Nachstellmechanismus zu abzurunden. Formel:

$$2222222/([(Difficulty + 2600)/9]^2)$$



Viacoin Whitepaper

Dark Gravity Wave Version 3 ist die neueste Version und ermöglicht eine verbesserte Retargeting-Schwierigkeit im Vergleich zum bekannten Kimo Gravity Well Algorithmus.

4. Segwit

Viacoin hat [12] Segwit (BIP 141) implementiert. Segregated Witness hilft dabei, die Größe einer Transaktion zu verringern und das UTXO-Wachstum zu bewältigen. Weiterhin ist Segregated Witness ein Transaktionsformat, bei dem Zeugendaten von der Transaktion getrennt werden. Es zielt auch darauf ab, den pro-Block-Transaktionsdurchsatz um einen Faktor von 2 oder 3 zu erhöhen, während gleichzeitig die Blocksynchonisierung für neue Nodes beschleunigt wird.

Der Hauptzweck der Implementierung von Segwit in Viacoin besteht nicht darin, die Kapazität zu erhöhen, sondern die Formbarkeit zu verbessern und das Scripting einfacher zu aktualisieren. Durch die Verbesserung der Formbarkeit können in Viacoin Features wie [1] Atomic-Swaps, bidirektionale Zahlungskanäle und Lightning-Networks hinzugefügt werden, die die Interoperabilität von Viacoin mit Bitcoin erhöhen.

Segwit enthält eine Versioning für Skripte, so dass zusätzliche Opcodes (die normalerweise in Nicht-Segwit-Transaktionen einen Hard-Fork erfordern würden) verwendet werden können. Einfachere Änderungen an Skript-Opcodes erleichtern den Fortschritt von Viacoin. Dies ermöglicht das Hinzufügen von Schnorr-Signaturen, Sidechains, MAST und anderen Features.

5. Das Lightning-Network

[8] Das Lightning-Network ist ein Übertragungsnetzwerk, dass auf einer Ebene über der Viacoin-Blockchain arbeitet und die Smart-Contract-Funktionalität in der Blockchain nutzt, um sofortige Zahlungen über ein Netzwerk von Teilnehmern zu ermöglichen. Dies ermöglicht Verbesserungen des Transaktionsdurchsatzes um mehrere Größenordnungen, indem die Mehrzahl der Transaktionen außerhalb der Consensus-Ledger in Zahlungskanäle verschoben wird. So werden Millionen bis Milliarden Transaktionen pro Sekunde über das Netzwerk ermöglicht, eine Kapazität, die alte Zahlungsschienen in den Schatten stellt. Dies wird durch die Unterstützung von Skripten ermöglicht, bei denen die Parteien bilaterale Statusverträge abschließen, bei denen bilaterale zustandsabhängige Verträge durch die gemeinsame Nutzung einer digitalen Signatur aktualisiert werden kann und durch die Veröffentlichung von Beweisen auf die Blockchain geschlossen werden kann.



Viacoin Whitepaper

Das Lightning-Network ermöglicht außergewöhnlich niedrige Gebühren. Für eine Transaktion mit geringem Wert ist das Lightning-Network die Königsdisziplin. Es ermöglicht neue Arten des Handels. Durch das Öffnen eines Bezahlkanals mit vielen Parteien können Teilnehmer in der LN zu einem zentralen Punkt für die Weiterleitung von Zahlungen an andere werden, was zu einem vollständig verbundenen Bezahlkanal führt. Die Zahlungen werden mithilfe eines Skripts erzwungen, das die Atomizität durch Dekrementierung von Zeitsperren erzwingt.

Ein weiterer Vorteil ist die Möglichkeit von atomaren Cross-Chain-Transaktionen, die es Benutzern ermöglichen, Viacoin, Bitcoin, Litecoin und andere Segwit Coins sofort zu handeln, was einen extrem effizienten, dezentralen Austausch oder eine dezentrale Form von „Shapeshift.io“ ermöglicht.

6. Schnorr Signature

Ein weiterer Teil der kommenden Entwicklungen ist Schnorr Signature Aggregation Entwicklungen. Diese Funktionalität wurde auch in Bitcoin als der Nachfolger von ECDSA vorgeschlagen, da dieser Algorithmus effizienter ist. Bis vor kurzem war es in Viacoin und in vielen anderen Kryptocoins nicht möglich, Schnorr- Signaturen ohne Hardfork zu implementieren, dies ist jedoch nun durch die Flexibilität von Segwit möglich. Alle Signaturdaten werden zum Zeugen übertragen. Viacoin verwendet derzeit Elliptic Curve Digital Signatures (ECDSA) als einen ZK Proof of Ownership, um die Übertragung von einem Ausgang zu einem anderen zu autorisieren. Im Jahr 2015 schlug Daniel J. Bernstein vor, eine Schnorr-ähnliche Signatur auf einer elliptischen Kurve zu verwenden.

Einige Vorteile:

- Erheblich sicher unter Standardbedingungen
- Immunität gegenüber Formbarkeit
- Widerstand gegen Hash-Function Collisions
- Batch-Validierung für eine zwei- bis dreifache Beschleunigung
- Native k-of-k Multisignaturen . . .



Viacoin Whitepaper

Die Schnorr-Signatur unterstützt Batch Validation, wenn man also eine Nachrichten-signaturpaaren mit öffentlichen Schlüsseln und nicht nur einem einzigen hat, kann die Authentizität der Gruppe als Ganzes mit höherer Geschwindigkeit als jede einzeln überprüft werden. Diese Methode ist ideal, da Blöcke nur große Chargen von zu validierenden Signaturen sind.

Die Idee von Schnorr ist, dass mehrere Schlüssel mit Hilfe einer einzigen Signatur validiert werden können, dieser Vorgang heißt Native k-of-k Multi-Signaturen. Eine Gruppe kann eine Signatur erstellen, die für die Summe der Schlüssel gültig ist, U1, U2 und U3 sind die Benutzer. Es gibt ein 2-Runden-Interaktionsschema, indem aus n k1-, k2- und k3-Werten an einem entsprechenden öffentlichen Punkt R1, R2, R3 berechnet werden. Diese R-Werte wiederrum werden miteinander kommuniziert und zu mit einem Gesamt-R-Wert summiert. Der Gesamt-R-Wert signiert diese Nonce mit ihrem eigenen Schlüssel, was zu S1, S2, S3 führt. Anschließend werden alle S-Werte zu einem letzten S kombiniert. Eine Signatur, die für die Summe ihrer Schlüssel gültig ist, hierdurch ergibt sich der Vorteil des k-of-k multisig.

$$\begin{array}{c|c} \begin{array}{l} U_1 \rightarrow k_1, R_1 \\ U_2 \rightarrow k_2, R_2 \\ U_3 \rightarrow k_3, R_3 \end{array} & \longrightarrow R \longrightarrow \end{array} \begin{array}{c|c} \begin{array}{l} U_1 \rightarrow (R, s_1) \\ U_2 \rightarrow (R, s_2) \\ U_3 \rightarrow (R, s_3) \end{array} & \longrightarrow (R, s) \end{array} \quad (1)$$

Selbst wenn es keine k-of-k-Situation gibt, kann jede andere Richtlinie zur Kombination von Schlüsseln signiert werden. Alles, was man braucht, ist ein Merkle-Baum plus die Fähigkeit für Schnorr, einen Baum zu addieren und aufzubauen, wobei jedes Knotenblatt des Baums eine Kombination von Schlüsseln ist, die signiert werden können. Diese müssen dann zusammengehashed werden und die Wurzel ist die Adresse. OP_CHECKSIG & OP_CHECKMULTISIG werden so modifiziert, dass sie Pubkeys stapeln, validierte Eingaben delinearisieren und assoziieren und eine kombinierte Signatur für die Transaktion erzeugen können, die zu einer 20% Reduzierung der Blockgröße führt.

2 von 4 (k1 ... k4)

O(1) Verifikationszeit O(log n) Signaturgröße O(n) Signierzeit

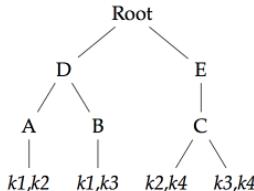
2 de 4 (k1...k4)

O(1) tiempo de verificación

O(log n) tamaño de firma



Viacoin Whitepaper



Es ist möglich, Aggregation über alle Signaturen in einer einzigen Transaktion durchzuführen. Die Idee dahinter ist es, Systemvalidatoren wie Viacoin-Nodes zu ermöglichen, einen einmaligen Schlüssel für jede Eingabe aller Transaktionen zu berechnen.

7. Non-Atomic Flushing

Um das System robust zu machen, muss der Zustand auf dem Datenträger mit einem Block persistent sein. Bei einem unerwarteten Herunterfahren der Wallet können wir das System starten, zurücksetzen oder vorwärts rollen und einen konsistenten Hinweis auf der Festplatte erhalten. Normalerweise würde, wenn der Cache voll wird, ein Flush erzwungen. Wenn es beim Start vorhanden ist, heißt das, dass während des Flush eine Absturz zustande kam und die Blöcke in ihm werden vor dem Fortfahren zurückgesetzt, um einen konsistente Hinweis auf der Festplatte zu erhalten.

8. Colored Coins

Die Viacoin-Skriptsprache ermöglicht es, kleine Mengen von Metadaten in der Block-chain zu speichern, die Anweisungen zur Asset-Manipulation darstellen können. Eine Viacoin-Transaktion kann so codiert werden, dass x Einheiten eines neuen Vermögenswertes ausgegeben und einer Viacoin-Adresse gutgeschrieben werden. Der Begriff leitet sich von der Idee ab, eine bestimmte Anzahl von Coins zu "färbigen". Durch das „Einfärben“ eines Viacoins wird es zu einem Token, das alles repräsentieren kann, was ein Benutzer handeln möchte, z.B. Aktien oder physische Güter. Dies scheint der "Counterparty" sehr ähnlich zu sein, aber es gibt einige wichtige Unterschiede, die Viacoin-Blockchain (z.B. NXT) wird verwendet .



Viacoin Whitepaper

Es gibt keinen Hilfs-Coin (z.B. Counterparty und Mastercoin). Die Metadata gibt einer [9] Colored Coin Transaction Bedeutung, die normalerweise in einem der OP_RETURN-Opcodes gespeichert ist. Der Ausgang, der den OP_RETURN enthält, wird als Market-Output bezeichnet, welcher einen Wert von Null oder von Nicht-Null haben kann. Market-Outputs beginnen mit dem OP_RETURN-Opcode und können von einer beliebigen Sequenz von PUSHDATA-Opcode enthaltenden Opcodes gefolgt sein. Dieser PUSHDATA-Opcode muss eine „parsable open Asset market Payload“ enthalten. Das Asset-Quantity-List- Field wird verwendet, um die Menge jeder Ausgabe des Assets zu bestimmen, jeder Integer benutzt LEB128-Encoding, falls dieser Vorgang 9 Bytes übersteigt, ist der Market-Output ungültig. Die maximale Asset-Quantity für einen Output beträgt 263-1units. Die farbigen Coins [4] Open Asset Protocol befindet sich über dem Viacoin-Protokoll, dadurch sind keine Änderungen am Viacoin-Protokoll selbst erforderlich.

9. MAST (Merkelized Abstract Syntax Trees)

[10] MAST ermöglicht das Speichern von Viacoin-Transaktions-Validierungsskripten in teilweise gehaschter Form und gleichzeitig die Interaktion von Nodes mit Merkle-Bäumen. "Bei Ausgaben können Benutzer nur die auszuführenden Zweige und Hashwerte, die die Zweige mit dem Fixed-Size-Merkle-Root verbinden. Dies reduziert die Größe des Redemption-Stacks von $O(n)$ auf $O(\log n)$ (n als die Anzahl der Verzweigungen). Dies ermöglicht komplizierte Einlösungsbedingungen, die derzeit aufgrund der Skriptgröße und des Opcode- Limits nicht möglich sind, verbessert die Privatsphäre, indem nicht ausgeführte Zweige verborgen werden, und ermöglicht die Einbeziehung von nicht übereinstimmenden Daten mit sehr geringen oder keinen zusätzlichen Kosten. "

Es ist wichtig, weil MAST die Erstellung von Smart-Contracts ermöglicht, ohne die Blockchain zu blockieren. Normalerweise sind alle Smart-Contracts auf der Blockchain sichtbar und belegen Platz. Mit MAST ist es möglich, nur die abgeschlossenen Smart Contracts anzuzeigen, was Platz spart, da Nodes nur die oberste Ebene des Merkle-Baums lesen müssen. Dies mag Ethereums Smart-Contract-System ähnlich erscheinen, aber es gibt einen Unterschied. Ethereum greift direkt auf eine VM zu, wobei VIA durch RootStock (RSK) Zugriff auf eine VM erhält.

RSK soll das sein, was Ethereum hätte sein sollen: eine dezentrale, Turing-komplette Smart-Contract-Plattform.



Viacoin Whitepaper

10. Viacoin RSK Smart Contracts

[5] Rootstock ist eine Plattform für Smart-Contracts mit wechselseitiger Verbindung hat. Die Idee ist es mit Smart-Contracts arbeiten zu können. Der Rootstock führt eine komplette virtuelle Maschine mit dem Namen "Rootstock Virtual Machine" aus (die auch mit der virtuellen Ethereum-Maschine kompatibel ist!) und die Ausführung solid-er komplizierter intelligenter Verträge ermöglicht. Es könnte durch Merge-Mining mit Viacoin funktionieren, was der RSK-Blockchain die gleiche Sicherheit wie Viacoin ermöglicht. Es sollte etwa 2000

Transaktionen pro Sekunde on-chain und 20000 Transaktionen pro Sekunde off-chain ermöglichen.

11. Anonyme Transaktionen

[11] Ein nicht verknüpfbarer anonymer Atomic-Payment-Hub für Viacoin basierend auf Tumblebit.-

<https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf>



Viacoin Whitepaper

Verweise

- [1] Nolan back. Alt chains and atomic transfers.
https://en.bitcoin.it/wiki/Atomic_cross-chain_trading - 2013.
- [2] bitcoinwiki. Merged mining specification.
https://en.bitcoin.it/wiki/Merged_mining_specification - 2011.
- [3] Evan Duffield and Kyle Hagan. Darkcoin: PeertoPeer CryptoCurrency with Anonymous Blockchain Transac-tions and an Improved ProofofWork System.
<https://www.dash.org/wp-content/uploads/2014/09/DarkcoinWhitepaper.pdf> - 2014.
- [4] Flavien Charlon. Open Assets Protocol (OAP/1.0).
<https://github.com/OpenAssets/open-assets-protocol/blob/master/specification.mediawiki> - 2014
- [5] Sergio Demian Lerner. RSK White paper overview.
<http://www.the-blockchain.com/docs/Rootstock-WhitePaper-Overview.pdf> - 2015.
- [6] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system.
<https://bitcoin.org/bitcoin.pdf> - 2008.
- [7] Colin Percival. Stronger key derivation via sequential memory-hard functions.
<https://www.tarsnap.com/scrypt/scrypt.pdf> - 2009.
- [8] Joseph Poon and Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments.
<https://lightning.network/lightning-network-paper.pdf> - 2016.
- [9] Meni Rosenfeld. Overview of Colored Coins.
<https://bitcoil.co.il/BitcoinX.pdf> - 2012.
- [10] Jeremy Rubin, Manali Naik, Nitya Subramanian. Merkleized Abstract Syntax Trees.
<http://www.mit.edu/~jlrubin/public/pdfs/858report.pdf> - 2014.
- [11] Viacoin dev team. Styx: Unlinkable Anonymous Atomic Payment Hub For Viacoin.
<https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf> - 2016.
- [12] Eric Lombrozo, Johnson Lau, Pieter Wuille. Segregated Witness (Consensus layer). <https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki> - 2015.