Viacoin Whitepaper

Viacoin Dev Team

September 12, 2017

Обновлено: 12 июня 2018 г.

Аннотация

Viacoin - криптовалюта с открытым исходным кодом, отделившаяся от Биткоина [7] в 2014 году. Основные преимущества Viacoin - объединенный майнинг (Auxiliary Proof Of Work), алгоритм шифрования Scrypt, транзакции в 25 раз быстрее, чем в сети Биткон и расширенный OP_RETURN до 120 байт. Награда за добычу блока снижается в 2 раза каждые 6 месяцев, а общий оборот составляет 23,176,392.41459 токенов. Инфляция Viacoin мала из-за маленькой награды за добычу блока. Так как награда мала, майнеры поощряются к добыче новых блоков из-за совмещенного AuxPoW. В данный момент Viacoin добывается крупнейшими из майнинговых пулов в мире, например, F2Pool.
Другие преимущества - модифицированный алгоритм перераспределения сложности Anti Gravity Wave. Также есть поддежка Segwit'a, Lightning Network и Soft Fork.

Документация, дизайн и код находятся на стадии разработки и будут дополняться.

1 Scrypt

В криптографии [8] Scrypt это деривационная функция на основе кодовых слов, созданная Коллином Персивалем. Алгоритм был создан таким образом, чтобы создать ощутимые сложности для проведения масштабных атак из-за необходимости в большом количестве оперативной памяти. В 2012 году алгоритм был опубликован IEFT, а версия Scrypt сейчас широко используется в PoW криптовалютах, в том числе и в Viacoin.

Scrypt это деривационная функция, которая требует большого количества оперативной памяти для вычисления, что делает создание ASIC'ов более затратным и невыгодным. Алгоритм основывается на TMTO (Time-Memory Tradeoff). Создание и эксплуатация ASIC'ов для Viacoin минимум в 10-20 раз менее выгодна, чем для Биткоина.

Scrypt использует следующие параметры для генерации деривационного ключа:

- Кодовая фраза: символы преобразуются в хеш
- Salt: случайная комбинация символов, используемая как аргумент для Scrypt
- N: параметр стоимости RAM/CPU
- P: параметр параллелизации
- R: размер блока
- dkLen: предполагаемая длинна ключа в байтах

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

Параметры Viacon: N=1024, R=1, P=1 и S= случайные 80 байт, производящие 256-битный выход.

2 Объединенный Майнинг AuxPoW

[2] Объединенный майнинг направлен на переиспользование вычислительной мощности для повторной добычи любой другой Scrypt криптовалюты. Добавляя защищенность в блокчейн Viacoin, такой майнинг позволяет добывать блоки более чем в один блокчейн в момент времени. Например, майнер может добывать Viacoin и Litecoin, или же другую Scrypt криптовалюту практически без потери хешмощности на обоих блокчейнах.

Каждый майнер вносит свой вклад в общий хешрейт двух сетех, что приводит к большей защищенности и надежности двух блокчейнов. Блок AuxPoW отличается от обычного блока Биткоина двумя вещами: хеш заголовка блока не соответствует уровню сложности блокчейна, а дополнительный элемент в блоке показывает, что майнер, вычисливший блок, выполнил нужную работу, а количество работы соответствует двум блокчейнам.

Майнеры стимулированы добывать Viacoin, ведь, несмотря на низкую награду, они все равно могут добывать вторую криптовалюту, при этом не теряя хешрейт на обоих блокчейнах. Данное решение позволяет Viacoin иметь низкий процент инфляции по сравнению с криптовалютами, не поддерживающими объединенный майнинг.

3 Anti Gravity Wave

Anti Gravity Wave (AGW) это алгоритм переопределения мощности сети с открытым исходным кодом. Он создан на основе Dark Gravity Wave (DGW) [4], который был разработан Даффилдом, разработчиком и создателем X11/Darkcoin/Dash. Алгоритм был создан для того, чтобы предотвратить атаку TimeWrap, возможную при использовании Kimoto Gravity Wave. DGW и AGW постоянно перераспределяют сложность, используя статистику по последним найденным в сети блокам.

Anti Gravity Wave это модификация DGW, созданная командой разработчиков Viacoin. Как и DGW, AGW использует экспоненциальную и простую скользящие средние для того, чтобы сгладить результат переопределения моности. В Anti Gravity Wave сложность перераспределяется следующим образом:

$$a_{i+1} = \frac{a_i + D_{LastBlock-i}}{i+1} \tag{1}$$

Где D_m - сложность m-о блока. Используя данную (1) прогрессию, можно найти a_{72} член.
После этого необходимо найти два временных лимита T_{actual} и T_{target}. T_{actual} - фактическое время вычисления последних 72-х блоков в сети, а T_{target} - номинальное значение.

$$T_{actual} = T_{LastBlock} - T_{LastBlock-72}$$
$$T_{target} = (72-1) * 24$$

Anti Gravity Wave может также менять сложность, если она получается слишком большой или маленькой для данной сети. Окончательное значение определяется следующим образом:

$$Target = \frac{a_{72} * T_{actual}}{T_{target}}$$

AGW позволяет улучшенное переопределение сложности по сравнению с известным алгоритмом Kimo Gravity Wave.

4 Segwit

Viacoin активировал [13] (BIP 141). Segregated Witness позволяет значительно уменьшить размер транзакции и предотвратить рост комиссий. SegWit это формат транзакции, в которой часть данных вынесена за транзакции для увеличения количества пропускной способности в 2-3 раза, при этом делая синхронизацию между узлами более быстрой.

Основная цель реализации Segwit в Viacoin - не увеличение скорости и количества транзакций в блоке (однако это следствия реализации), а уменьшение размеров и облегчение дальнейшей разработки. Уменьшение размеров позволяет реализовать [1] атомарные свапы, двунаправленные транзакционные каналы и Lightning Network.

Segwit включает в себя контроль версий для скриптов, так что дополнительные ОП-коды (что обычно требует хардфорка) могут быть использованы, переопределены или внедрены, а подписи Шнорра, сайдчейны и MAST становятся возможными для реализации.

5 Lightning Network

[9] Lightning Network это протокол передачи транзакций, в котором используется слой выше, чем блокчейн - используются смарт-контракты для обеспечения мгновенных платежей в сети участников. Это обеспечивает

увеличение пропускной способности транзакций в несколько раз, перемещая большиство транзакций из блокчейна в платежные каналы, обеспечивая от сотен тысяч до миллионов транзакций в секунду. Это возможно благодаря поддержке он-чейн скриптов, с помощью которых участники транзакций заключают контракты, в которых состояние участника может быть обновлено через совместное использование цифровой подписи, и может быть закрыто через публикацию доказательства транзакции в блокчейне.

Lightning Network позволяет совершать транзакции с невероятно маленькой, приближенной к нулю комиссией, позволяя эффективно проводить микротранзакции и открывая новые возможности для коммерции. Открыв платежный канал с многими сторонами, участники в такой сети могут стать связующим звеном для остальных в сети, таким образом не только ускоряя свои транзакции, но и повышая безопасность и надежность сети.

Более того, Lightning Network предоставляет возможность совершать атомарные кросс-чейн транзакции, позволяя пользователям совершать обмен viacoin, litecoin, decred, биткоинов или других поддерживающих Segwit криптовалют непосредственно без участия третьей стороны и становясь децентрализованным аналогом 'Shapeshift.io'. Viacoin поддерживает атомарные свапы, тестирование которых завершено [3] с блокчейнами litecoin, decred и биткоина.

6 Подписи Шнорра

Подписи Шнорра - это технология, уже внедряемая в Viacoin. Аналогичный фукнционал уже был предложен в блокчейн Биткоина как аналог ECDSA. До недавних пор, в Viacoin, как и в других криптовалютах, было невозможно внедрить подписи Шнорра без хардфорка, однако, после внедрения Segwit теперь это реализуемо. Все данные подписи переносятся в свидетельство. Viacoin на данный момент использует цифровые подписи, основанные на эллиптических кривых (ECDSA) как доказательство владения, необходимое для подписи транзакции. В 2015 году Daniel J. Bernstein предложил использовать подписи Шнорра поверх эллиптических кривых.

Основные преимущества:

- Более защищенная технология
- Устойчивость к коллизиям хешфункции
- Ускорение валидации в 2-3 раза
- Нативные k-of-k мультиподписи ...

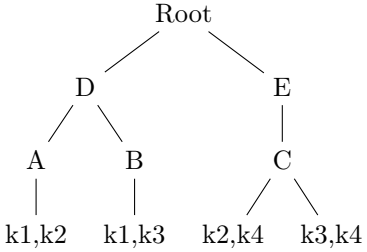
Подписи Шнорра поддерживают пакетную валидацию, что значит, что можно группировать публичные ключи и аутентифицировать их значительно быстрее, чем по отдельности. Этот метод значительно ускоряет валидацию блоков, так как с этой точки зрения блок - всего лишь большое количество подписей для валидации.
Нативные k-of-k мультиподписи Шнорра - технология, благодаря которой можно выделять группу ключей и генерировать одну-единственную подпись, которая может подтвердить истинность всей группы. Рассмотрим пример: $U1$, $U2$ и $U3$ - пользователи, которые генерируют nonce(одноразовый (псевдо)случайный код, используемый лишь единожды) $k1, k2, k3$ и публичные ключи $R1, R2, R3$ соответственно. После объединения в группу и обработки, получается финальное значение R, подписываемое каждым ключем. Результат S получается из комбинирования данных подписанных значений R $S1, S2, S3$.

$$\left.\begin{array}{l} U_1 \to k_1,\, R_1 \\ U_2 \to k_2,\, R_2 \\ U_3 \to k_3,\, R_3 \end{array}\right| \longrightarrow R \longrightarrow \left|\begin{array}{l} U_1 \to (R,\, s_1) \\ U_2 \to (R,\, s_2) \\ U_3 \to (R,\, s_3) \end{array}\right| \longrightarrow (R,\, s)$$

Даже если использование k-of-k подписей не требуется, может быть любая другая комбинация. Единственное необходимое в таком случае - хеш-дерево (дерево Меркла) и возможность построить дерево, где каждая листовая вершина - комбинация ключей, которые могут быть подписаны. После этого корневой узел дерева содержит необходимый адрес. OP_CHECKSIG & OP_CHECKMULTISIG будут модифицированы таким образом, что благодаря технологии подписей Шнорра удастся уменьшить размер блока на 20%.

2 из 4 (k1...k4)

$O(1)$ время верификации
$O(\log n)$ размер подписи
$O(n)$ время подписания



Более того, используя подписи Шнорра, возможно агрегировать все подписи в единственную транзакцию, что позволит валидаторам сети Viacoin вычислять лишь один ключ для каждого входа всех транзакций.

7 Неатомарный Сброс

Для увеличения надежности системы, состояние базы данных, в которой хранится блокчейн, всегда должно быть синхронизированным с блоком. При аварийном завершении приложения может быть произведена сихнронизация с диском и тем, что хранится в кеше или оперативной памяти.

8 Цветные Токены

Скриптовый язык Viacoin позволяет сохранять небольше объемы метаданных в блокчейне, которая может быть использована для инструкций. Транзакция в блокчейне Via может быть зашифрована так, что x токенов нового типа могут быть созданы и "направлены"на другой адрес. Это является основной идеей для "покраски"токенов. "Крася"токен, можно рассматривать его как абстракцию любого объекта, который пользователь хочет хранить, обменять или передать - акции компании, патент или физический предмет. Идея во многом схожа с Counterparty, однако существуют существенные различия.

В блокчейне Via не используются вспомогательные токены (как это происходит в Counterparty или Mastercoin). Метаданные придают значение "покрашенному"токену [10] и транзакции с его участием. Метаданные обычно хранятся и передаются с помощью OP_RETURN ОП-кода. Вывод данного ОП-кода называется маркирующим выводом, и он начинается с OP_RETURN ОП-кода, и далее может быть сопровожден любой последовательностью ОП-кодов, которые должны содержать PUSHDATA ОП-код. Поле количества используется для определения и указания количества каждого выхода, и каждое число форматируеся с применением LEB128. Если оно превышает 9 байт, то маркирующий вывод признается недействительным. Таким образом, максимальное количество выходов: $2^{63} - 1$. Протокол [5] Open Asset находится на верхнем уровне протокола Viacoin, поэтому для изменения протокола не понадобится вносить поправки в протокол Via.

9 Абстрактные Синтаксические Деревья Меркла)

[11] MAST(Merkle Abstract Syntax Trees, или Абстрактные Синтаксические Деревья Меркла) позволяют транзакциям в блокчейне Via хранить скрипты в частично хешированной форме, а узлам сети - взаимодействовать между собой с помощью хеш-дерева (дерево Меркла). "Во время траты токенов, пользователи могут предоставить только части ОП-кодов, которые они выполняют, и хеши, которые соединяют эти части с фиксированным в размерах корнем хеш-дерева. Это уменьшает количество стека с $O(n)$ до $O(\log n)$ где n - номер ветвей. Это позволяет строить более сложные коды, что на данный момент невозможно из-за ограничений в размере скрипта и лимита ОП-кодов. Также это позволяет включение дополнительных данных с близкой к нулю стоимостью".

Это очень важно, так как MAST позволяет смарт-контрактам создаваться без непосредственного внедрения и засорения блокчейна. Обычно все смарт-контракты видимы в блокчейне и занимают в нем место, однако с MAST возможно оставить в блокчейне только небольшую часть смарт-контракта, сохраняя место.
Это может быть похожим на систему смарт-контрактов Ethereum, однако между имплементацией Via и Ethereum есть разница - Ethereum имеет прямой доступ к своей виртуальной машине, в то время как Via будет иметь доступ к виртуальной машине через RootStock (RSK). RSK это платформа наподобие Ethereum - платформа со смарт-контрактами и Тьюринг-полным языком, однако более децентрализованная.

10 Смарт-контракты RSK

[6]RootStock это платформа для выполнения смарт-контрактов с двухсторонней привязкой. Основная идея RSK состоит в подключении виртуальной машины RootStock Virtual Machine с Тьюринг-полным языком смарт-контрактов (который в то же время совместим с виртуальном машиной Ethereum). Данная виртуальная машина может работать с merged майнингом Viacoin'а. Пропускная способность составляет примерно 2000 транзакций в основном чейне и 20000 транзакций вне основного блокчейна.

11 Анонимные транзакции

[12]Полностью анонимные атомарные платежи для Viacoin, основанные на Tumblebit.
https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf

Список литературы

[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] hotshot viacoin dev. So How Do I Really Do An Atomic Swap. https://hackernoon.com/so-how-do-i-really-do-an-atomic-swap-f797852c7639. 2018.

[4] Evan Duffield и Kyle Hagan. Darkcoin: PeerToPeer CryptoCurrency with Anonymous Blockchain Transactions and an Improved ProofOfWork System. https://cryptopapers.info/assets/pdf/darkcoin.pdf. 2014.

[5] Flavien Charlon. Open Assets Protocol (OAP/1.0). https://github.com/OpenAssets/open-assets-protocol/blob/master/specification.mediawiki. 2013.

[6] Sergio Demian Lerner. RSK White paper overview. http://www.the-blockchain.com/docs/Rootstock-WhitePaper-Overview.pdf. 2015.

[7] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf. 2008.

[8] Colin Percival. Stronger key derivation via sequential memory-hard functions. https://www.tarsnap.com/scrypt/scrypt.pdf. 2009.

[9] Joseph Poon и Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. https://lightning.network/lightning-network-paper.pdf. 2016.

[10] Meni Rosenfeld. Overview of Colored Coins. https://bitcoil.co.il/BitcoinX.pdf. 2012.

[11] Jeremy Rubin, Manali Naik, Nitya Subramanian. Merkelized Abstract Syntax Trees. http://www.mit.edu/~jlrubin/public/pdfs/858report.pdf. 2014.

[12] 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.

[13] Eric Lombrozo, Johnson Lau, Pieter Wuille. Segregated Witness (Consensus layer). https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki. 2015.