Viacoin Whitepaper

Viacoin Dev Team

September 12, 2017

Last updated on September 20, 2017

Abstract

Viacoin is an open source crypto-currency created in 2014 and is derived from the [6]Bitcoin protocol that supports embedded consensus with an extended OP_RETURN of 120 byte support. Viacoin features are Scrypt Merged mining also called Auxiliary proof of work or auxpow and has 25x faster transaction. Viacoin mining reward halving takes place every 6 months with a total supply of 23,000,000 coins. The inflation rate and mining reward is very low. To keep the miners interested in mining Viacoin, Merged mining (AuxPoW) is implemented. Viacoin is being mined by one of the biggest mining pools at the moment (F2Pool) with a very high hashrate. Other features include a mining difficulty adjustment algorithm to address flaws in Kimoto's Gravity Well (DarkGravityWave), Versionbits for simultaneous Soft Fork changes to be implemented 29 at a time, Segwit and The Lightning Network

Note: The whitepaper, documentation, designs are in research and development phase and subject to change.

1 Scrypt

In cryptography [7]Scrypt is a password based key derivation function created by Colin Percival. The algorithm was designed to make it costly to perform large-scale custom hardware attacks by requiring large amounts of memory. In 2012 the algorithm was published by IETF as an internet draft intended to become an informational RFC but a version of Scrypt is now used as a proof of work scheme by cryptocurrencies like Viacoin.

Scrypt is a memory hard key derivation function, it requires a reasonable large amount of Random Access Memory to be evaluated This makes implementation in special purpose custom hardware (ASICs) require more VLSI area which would make it unfeasible to build. The requirement of Scrypt algorithm is a large array of pseudo random bits to be held in memory and a key that is derived from this. The algorithm is based on TMTO (Time-Memory Tradeoff). Asic advantage in Viacoin is reduced by a factor of 10 compared to Bitcoin.

Scrypt uses the following parameters to generate a derived key:

- Passphrase: String of characters to hash
- Salt: Random string provided to Scrypt functions
- N: Memory/CPU cost parameter
- P: Parallelization parameter
- R: Blocksize parameter
- dkLen: Intended length of the key derived key in bytes

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

Viacoin parameters where N=1024, R=1, P=1 and S= random 80 bytes producing a 256-bit output

2 Merged Mining Auxpow

Viacoin [2]Merged mining aims to reuse the mining power of any other [7]Scrypt coin to add security to the Viacoin blockchain. Allowing a miner to mine for more than one blockchain at the same time. A miner can mine Viacoin and Litecoin or any other Scrypt coin together with Viacoin.

Every hash the miner contributes is for the total hashrate of both cryptocurrencies and results to being more secure. An AuxPOW is a type of block similar to Bitcoin standard block with two differences. The hash of the block header does not meet the difficulty level of the blockchain. Secondly, it has additional data elements that shows that the miner who created a block did mining on the parent blockchain and that works meet the difficulty level of the aux blockchain.

Miners would not stop mining mining Viacoin even if the reward is too low because they can mine any other scrypt coin with Viacoin for “free”. This leads to less and less inflation every 6 months than other altcoins that don’t have merged mining.

3 Dark Gravity Wave

[3]Dark Gravity Wave (DGW) is an open sourcer difficulty algorithm. DGW was authored by Evan Duffield, the developer and creator of X11/Darkcoin/Dash. The algorithm designed to address flaws like the Time warp attack in Kimoto Gravity Wave algorithm.

Dark Gravity Wave was first introduced in Dash (Darkcoin). DGW makes use of multiple exponential moving averages and simple moving averages to smoother the readjustment mechanism.
Formula:

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

Dark Gravity Wave version 3 is the latest version and allows improved difficulty retargeting compared to the well known Kimo Gravity Well algorithm.

4 Segwit

Viacoin has [12]Segwit (BIP 141) activated. It helps to shrink the size of a transaction and the UTXO growth. Segregated Witness means it separates the witness from the transaction. It also aims to increase the per-block transaction throughput 2x or 3x while simultaneously making blocks syncing faster for new nodes.

Segwit main purpose is not a capacity increase, it's fixing malleability and making scripting more easy to upgrade. With malleability fixed there are more things possible for Viacoin like [1]atomic swaps, bidirectional payment channels and Lightning networks that could increase Viacoin interoperability with Bitcoin.

Segwit includes a version number for scripts so that additional opcodes that would have required a hard-fork to be used in non-segwit transactions instead. Easier changes to script opcodes will make advancing Viacoin easier. This makes Schnorr signatures, sidechains, MAST and other ideas possible.

5 The Lightning Network

[8]The Lightning Network is a transfer network operating at a layer above the Viacoin blockchain using smart contract functionality in the blockchain to enable instant payments across a network of participants. Enabling improvements of several orders of magnitude in transaction throughput by moving the majority of transactions outside the consensus ledgers into Payment channels. Capable of millions to billions of transactions per second across the network. A capacity that blows away legacy payment rails. This is made possible by on-chain scripts which parties to enter into a bilateral stateful contracts where the state can be updated by sharing a digital signature and be closed finally by publishing evidence onto the blockchain.

The Lightning Network allows for exceptionally low fees For a low-value transaction, the Lightning Network is a silver bullet. It allows for new kinds of commerce. By opening a payment channel with many parties, participants in the LN can become a focal point for routing the payment of others leading into a fully connected payment channel. The payment are enforced using a script which enforces the atomicity via decrementing time-locks.

Another benefit is atomic cross-chain transactions, enabling users to trade viacoin, bitcoin, litecoin and other Segwit coins instantaneous making real efficient decentralized exchanges possible or a decentralized Shapeshift.

6 Schnorr signature

We will develop Schnorr signature aggregation. It has been proposed in Bitcoin too. It is the replacement of ECDSA for the more efficient algorithm. Until now it was not possible to implement it without a hardfork but now it is. That's why Segwit was important. All sig data is moved to the witness. Viacoin currently utilized Elliptic Curve Digital Signatures (ECDSA) as a zk proof of ownership in order to authorize the transfer from one output to another. In 2015 Daniel J. Bernstein proposed Schnorr like signature on top of an Elliptic Curve.

Some Advantages:

- Provably secure under standard assumptions
- immunity to malleability
- resistance to hash-function collisions
- Batch validation for a 2-3x speedup
- Native k-of-k Multisignatures ...

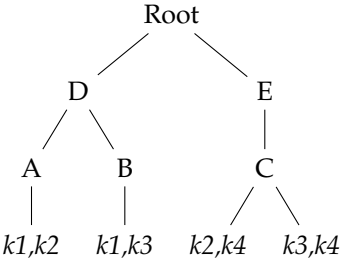
It supports batch validation, which means if you have a group of public key message signatures pairs rather than just a single one, you can verify if all of them or not all of them are valid at a higher speed than each of them individually which is exactly what we want since blocks are just big batches of signatures to validate. Native k-of-k multi signatures, the idea of Schnorr you can take multiple keys together and have a single signature that proves that all of them are signed. A group cat create a signature valid for the sum of keys. U1, U2 and U3 are the users. There's a 2 round interaction scheme where they all come up with a nonce k1, k2, k3 and they all compute a corresponding public point R1, R2, R3. They communicate those to each other and add them up with an overall R value. This overall R value signs this nonce with their own key resulting in an S1, 2, S3 and then you combine all the S values into one final S. A signature that will be valid for the sum of their keys. This has the advantage of the k-of-k multisig.

$$\left.\begin{array}{l} U_1 \to k_1,\, R_1 \\ U_2 \to k_2,\, R_2 \\ U_3 \to k_3,\, R_3 \end{array}\right| \longrightarrow R \longrightarrow \left|\begin{array}{l} U_1 \to (R,\, s_1) \\ U_2 \to (R,\, s_2) \\ U_3 \to (R,\, s_3) \end{array}\right| \longrightarrow (R,\, s) \tag{1}$$

Even if there is not a k-of-k situation, any other policy of what combination of keys can be signed and all one need is a merkle tree plus the ability for Schnorr to add up and build a tree where every node leave of the tree is a combination of keys that can be signed, hash them together and the root is the address. OP_CHECKSIG & OP_CHECKMULTISIG will be modified so that they can stack pubkeys, delinearize and associate validated inputs and produce a combined signature for the transaction resulting into a 20% reduction in block size.

2 out of 4 (k1...k4)

$O(1)$ verification time
$O(\log n)$ signature size
$O(n)$ signing time



It is possible to do aggregation over all signatures in a single transaction. The idea behind it is to enable system validators like Viacoin nodes to compute a single key for every input of all transactions.

7 Non-atomic flushing

In order to make the system robust, the state on the disk has to be persistent with a block. With an unexpected shutdown of the wallet we can startup and rollback or roll forward inside of it and be able to get a consistent tip on the disk. Normally whenever the cache would fill up, we would force flush If it is present at startup it means we crashed during flush, and we rollback/roll forward blocks inside of it to get a consistent tip on disk before proceeding.

8 Colored coins

Viacoin scripting language allows to store small amounts of metadata on the blockchain which can represent asset manipulation instructions. A Viacoin transaction can be encoded that x units of a new asset where issued and are credited to a Viacoin address. The term is derived from the idea of "coloring" a nominal amount of coins. By coloring a viacoin it turns into a token that can represent anything a user wants to trade like a company stocks or real world value. This looks a lot like Counterparty but there are some key differences. It uses the Viacoin blockchain (e.g NXT).

It does not issue an auxiliary coin (e.g Counterparty and Mastercoin). The medata gives it meaning to a [9]colored coin transaction which is usually stored in one of the OP_RETURN opcode. The output containing the OP_RETURN is called a marker output. This marketcout can have a zero or non-zero value. The marker outputs starts with the OP_RETURN opcode and can be followed by any sequance of opcodes which must contain a PUSHDATA opcode containing a parsable open Asset market Payload. The asset quantity list field is used to determine the quantity of each output of the asset and each integer is using LEB128 encoding. If this exceeds 9 bytes, the market output is deemed invalid. The maximum asset quantity for an output is $2^63 - 1 units$. The colored coins [4]Open Asset Protocol sits on top of the Viacoin protocol. It does not require any changes to the Viacoin protocol.

9 MAST (Merkelized Abstract Syntax Trees)

[10]Mast allowing Viacoin transaction validation scripts to be stored in partially-hash form and allow nodes to interact with Merkle Trees. "When spending, users may provide only the branches they are executing, and hashes that connect the branches to the fixed size Merkle root. This reduces the size of redemption stack from $O(n)$ to $O(\log n)$ (n as the number of branches). This enables complicated redemption conditions that is currently not possible due to the script size and opcode limit, improves privacy by hiding unexecuted branches, and allows inclusion of non-consensus enforced data with very low or no additional cost."

It is important because MAST allows smart contracts to be created without clogging up the blockchain. Usually all smart contracts would be visible on the blockchain and take up space. MAST to only reveal the smart contracts that have been completed with saving space because nodes only read the top layer of the Merkle Tree. This sounds familiar to Ethereum but there's a difference. Ethereum access to a VM and VIA will also obtain access to a VM though RootStock (RSK). RSK aims to be what Ethereum is (or should have been) decentralized, Turing-complete smart contract platform.

10 Viacoin RSK smart contracts

[5]Rootstock is a smart contract platform which has a two-way peg. The idea is the enable it to work with smart contracts. Rootstock runs a turing complete Virtual machine called Rootstock Virtual Machine and is also compatible with Ethereum virtual machine and allows solidity compiled smart contracts to run. It could work by merge mining with Viacoin which allows the RSK blockchain to have the same security level as Viacoin. It should allow around the 2000 transactions per second on chain and 20000 transactions per second off-chain.

11 Anonymous transactions

[11]An Unlinkable Anonymous Atomic Payment Hub For Viacoin based on Tumblebit.
https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf

References

[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 Transactions 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. 2013.

[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. *Merkelized 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.