Viacoin Whitepaper

Viacoin Dev Team

September 12, 2017

Last updated on June 12, 2018

Abstract

Viacoin is an open source crypto-currency created in 2014, derived from the [7]Bitcoin protocol that supports embedded consensus with an extended OP_RETURN of 120 byte. Viacoin features Scrypt Merged mining, also called Auxiliary proof of work or AuxPoW, and 25x faster transactions than Bitcoin. Viacoin mining reward halving takes place every 6 months and has a total supply of 23,176,392.41459 coins. The inflation rate of Viacoin is low due to minimal mining reward. As the block reward of Viacoin is low, miners are given incentive to mine Viacoin through Merged mining (AuxPoW). Viacoin is currently mined by one of the biggest mining pools (F2Pool) with a very high hashrate.

Other features include a mining difficulty adjustment algorithm to address flaws in Kimotos Gravity Well (DarkGravityWave), Versionbits to allow for 29 simultaneous Soft Fork changes to be implemented at a time, Segwit and the Lightning Network

CRYP2NOVA

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

Archived copy · cryp2nova.com

1 Scrypt

In cryptography, [8]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 the 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 reasonably 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 unprofitable to build for the purpose of mining Viacoins. 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 [8]Scrypt coin to add security to the Viacoin blockchain, allowing a miner to mine for more than one blockchain at the same time. For example, a miner could mine Viacoin and Litecoin or any other Scrypt coin together with Viacoin with little to no impact on the hashrate of either one.

Every hash the miner contributes is for the total hashrate of both cryptocurrencies and results in a more secure blockchain. An AuxPoW block is a type of block similar to a standard Bitcoin 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 have an incentive to mine Viacoin even if the reward is low as they are able to mine any other Scrypt coin simultaneously Viacoin for free. As Viacoin mining isn't driven by large block rewards, this allows Viacoin to have a lower rate of inflation compared to other cryptocurrencies that do not support merged mining.

Archived copy · cryp2nova.com

3 Anti Gravity Wave

Anti Gravity Wave (AGW) is an open source difficulty algorithm. It comes from the Dark Gravity Wave (DGW) [4] algorithm that had been authored by Evan Duffield, the developer and creator of X11/Darkcoin/Dash. The algorithm had been designed to address flaws like the Time warp attack in Kimoto Gravity Wave algorithm. Both DGW and AGW readjust block difficulty by using blockchain statistics on recently found blocks.

Anti Gravity Wave is a Via modification of the DGW. As a DGW, AGW makes use of simple and exponential moving averages of block actual timespans in the blockchain in order to smoothen the readjustment mechanism. In Anti Gravity Wave difficulty readjustes every block by the following rule:

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

Where D_m is the difficulty of the block m. Given the following sequence (1), the 72nd term a_{72} is found. Then two timespans are determined, T_{actual} and T_{target}. T_{actual} is the actual time of the last 72 blocks had been calculated by the network, whereas T_{target} is the nominal target value.

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

Anti Gravity Wave algorithm can also readjust the target if it is too big or too small for the network. Final block difficulty is determined by as following:

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

Anti Gravity Wave allows improved difficulty retargeting compared to the well known Kimo Gravity Well algorithm.

4 Segwit

Viacoin has [13]Segwit (BIP 141) activated. Segregated Witness helps to shrink the size of a transaction and cope with the UTXO growth. Segregated Witness is a transaction format where witness data is segregated from the transaction. It also aims to increase the per-block transaction throughput by a factor of 2 or 3, while simultaneously making block syncing faster for new nodes.

The main purpose of Segwit implementation in Viacoin is not to increase capacity however, it is to fix malleability and make scripting easier to upgrade. Fixing malleability allows for the addition of features in Viacoin like [1]atomic swaps, bidirectional payment channels and Lightning networks that could increase Viacoin interoperability with Bitcoin.

Segwit includes versioning for scripts so that additional opcodes (that would normally require a hard-fork in non-segwit transactions) can be used instead. Easier changes to script opcodes will make advancing Viacoin easier. This makes the addition of Schnorr signatures, sidechains, MAST and other features possible.

5 The Lightning Network

[9]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. This enables improvements of several orders of magnitude in transaction throughput by moving the majority of

Archived copy · cryp2nova.com

transactions outside the consensus ledgers into Payment channels. This allows millions to billions of transactions per second across the network. A capacity that blows away legacy payment rails. This is made possible by supporting on-chain scripts in which parties enter into bilateral stateful contracts, in which the state can be updated by sharing a digital signature and can be closed by publishing evidence onto the blockchain.

The Lightning Network allows for exceptionally low fees. For a low-value transaction, the Lightning Network is the 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 payments are enforced using a script which enforces the atomicity via decrementing time-locks.

Another benefit is the possibility of atomic cross-chain transactions, enabling users to trade viacoin, bitcoin, litecoin and other Segwit coins instantaneously, allowing for extremely efficient, decentralized exchanges or a decentralized form of 'Shapeshift.io'. Viacoin already supports atomic swaps, which had been tested [3] with litecoin, decred and bitcoin blockchains.

Archived copy · cryp2nova.com

6 Schnorr signature

Schnorr signature aggregation is part of upcoming developments as well. This functionality has also been proposed in Bitcoin as the successor of ECDSA as it is a more efficient algorithm. Until recently, in Viacoin and in many other cryptocoins, it was not possible to implement Schnorr signatures without a hardfork. Now with the malleability of Segwit, it is possible. All signature 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 to use a 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 ...

Schnorr signature supports batch validation, which means that if you have a group of public key message signature pairs rather than just a single one, you can verify the authenticity of the group as a whole at a higher speed than each of them individually. This method is ideal since blocks are just big batches of signatures to validate.
Native k-of-k multi signatures, the idea of Schnorr is that you can take multiple keys together and have a single signature that proves that all of them are signed. A group can create a signature valid for the sum of keys. U1, U2 and U3 are the users. Theres 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.

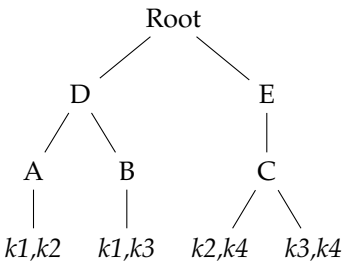
$$\left.\begin{array}{l} U_1 \to k_1,\, R_1 \\ U_2 \to k_2,\, R_2 \\ U_3 \to k_3,\, R_3 \end{array}\right| \longrightarrow R \longrightarrow \left|\begin{array}{l} U_1 \to (R,\, s_1) \\ U_2 \to (R,\, s_2) \\ U_3 \to (R,\, s_3) \end{array}\right| \longrightarrow (R,\, s)$$

Even if there is not a k-of-k situation, any other policy of what combination of keys can be signed. All one needs is a merkle tree plus the ability for Schnorr to add up and build a tree where every node leaf of the tree is a combination of keys that can be signed. These then need to be hashed 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

Archived copy · cryp2nova.com



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.

CRYP2NOVA

Archived copy · cryp2nova.com

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, a flush would be forced. 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 were 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 company stocks or physical goods. This seems very similar to '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 metadata gives meaning to a [10]colored coin transaction which is usually stored in one of the OP_RETURN opcodes. The output containing the OP_RETURN is called a marker output. This marker output can have a zero or non-zero value, and it starts with the OP_RETURN opcode and can be followed by any sequence 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 [5]Open Asset Protocol sits on top of the Viacoin protocol. It does not require any changes to the Viacoin protocol itself.

9 MAST (Merkelized Abstract Syntax Trees)

[11]MAST allows Viacoin transaction validation scripts to be stored in partially-hashed form and allows 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 the 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. With MAST it is possible to only reveal the smart contracts that have been completed, saving space as nodes only have to read the top layer of the Merkle Tree. This may seem familiar to Ethereum's smart contract system but there is a difference.Ethereum accesses a VM directly whereas VIA will obtain access to a VM though RootStock (RSK). RSK aims to be what Ethereum should have been: a decentralized, Turing-complete smart contract platform.

10 Viacoin RSK smart contracts

[6]RootStock is a smart contract platform which has a two-way peg. The idea is to enable it to work with smart contracts. Rootstock runs a turing complete Virtual machine called Rootstock Virtual Machine (which 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 for approximately 2000 transactions per second on-chain and 20000 transactions per second off-chain.

Archived copy · cryp2nova.com

11 Anonymous transactions

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

CRYP2NOVA

Archived copy · cryp2nova.com

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] 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 and 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 and 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.

CRYP2NOVA

Archived copy · cryp2nova.com