Viscoin

Money made decentralized.

Viscoin is an experimental digital currency that lives on the internet. Payments can be made by anyone, to anyone, any time, anywhere in the world, and are carried out collectively by the network with the use of peer-to-peer technology. Cryptography makes trusting a central authority obsolete when anyone with a computer can verify that a transaction is valid.

Blockchain

Blockchain is the technology that allows transactions to be stored on a public decentralized ledger. It does so by chaining together blocks which contain transactions using hashes. These hashes are what miners find by mining.

Mining

Mining is collectively carried out by the network. Mining is a task where the miner tries to generate a hash that meets the difficulty of the block. The difficulty is automatically adjusted by the protocol to ensure that the target block time is 1 minute. The difficulty updates every time a block is mined and while a block is being mined. If the time since the last mined block is less than 1 minute the difficulty is increased one step. On the other hand if the time since the last mined block exceeds 1 minute the difficulty is decreased one step.

Proof of work

The mining algorithm used in Viscoin is Argon2d. Argon2 is a key derivation function. Argon2 was selected as the winner of password hashing competition in July 2015. Argon2d maximizes resistance to GPU cracking attacks. By accessing the memory array in a password dependent order it reduces the possibility of time-memory trade-off which is ideal for a mining algorithm whose purpose is to only be effective on CPU. The CPU mining algorithm was chosen with two factors in mind.

- First of all, CPUs are a lot more common in personal computers than GPUs allowing for the hashpower to be more decentralized.

- Secondly, CPUs generally draw less power than GPUs making it a more environmentally friendly alternative.

Addresses

Addresses are what coins are associated with on the blockchain. An address can receive (input) coins and send (output) coins. The address is essentially 20 bytes of data. An address can be derived from a private key.
private key (32 bytes) → **public key** (65 bytes) → **address** (20 bytes)

To make addresses humanly readable they are converted to strings using base58 encoding.
address (20 bytes) → **base58 string** (most commonly 33 chars)

Transactions

Transactions are essentially transfers of value. The blockchain doesn't store individual balances of addresses. Instead it stores all transactions included in the blockchain. The balance of an address can be calculated by adding the address's input total and subtracting its output total.

A signed transaction contains the following data.

To	The receiver's address.
Amount	Amount of coins to be transferred.
From	The sender's address.
Fee	Amount of coins the miner will get for including the transaction in the next block.
Timestamp	When the transaction was signed / when the transaction can be included in a block.
Signature	The ECDSA signature that proves the transaction was signed by the owner of the wallet it's sending from.

Timelock

A transaction can't be included in the next block if the transaction's timestamp is greater than or equal to the timestamp of the block it is going to be included in. It can also not be included in the next block if it's timestamp is less than the timestamp of the previous block.

This makes it so that if a transaction is signed and not immediately included in the next block the sender can feel comfortable that the transaction will never go through.

Merkle Tree

Merkle trees link together all the transactions in the block in a way that makes it possible to verify that a transaction is part of the block without the need of knowing all the transactions in the block.

References

1. Wikipedia contributors. (2021, September 9). Argon2. In *Wikipedia, The Free Encyclopedia*. Retrieved 21:03, November 7, 2021, from https://en.wikipedia.org/w/index.php?title=Argon2&oldid=1043304588
2. Wikipedia contributors. (2021, October 5). Elliptic Curve Digital Signature Algorithm. In *Wikipedia, The Free Encyclopedia*. Retrieved 15:17, November 9, 2021, from https://en.wikipedia.org/w/index.php?title=Elliptic_Curve_Digital_Signature_Algorithm&oldid=1048367356
3. Wikipedia contributors. (2021, November 5). Merkle tree. In *Wikipedia, The Free Encyclopedia*. Retrieved 15:19, November 9, 2021, from https://en.wikipedia.org/w/index.php?title=Merkle_tree&oldid=1053653005
4. Wikipedia contributors. (2021, November 9). Bitcoin. In *Wikipedia, The Free Encyclopedia*. Retrieved 15:20, November 9, 2021, from https://en.wikipedia.org/w/index.php?title=Bitcoin&oldid=1054306086

See also Bitcoin whitepaper.