Diskcoin: An energy-saving and scalable peer-to-peer crypto currency system

rick@diskcoin.org

www.diskcoin.org

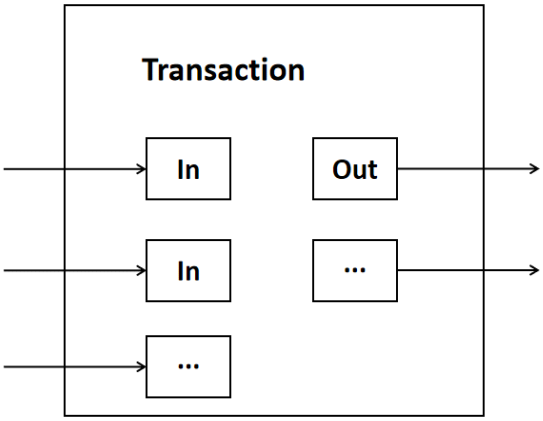
Abstract: This paper proposes a peer-to-peer crypto currency system that is more energy efficient than Bitcoin, retaining most of the features of Bitcoin, such as peer-to-peer networks, minimal network architecture, and security. The difference is that Diskcoin uses the Conditioned Proof Of Capacity (CPoC) consensus algorithm to reduce the consumption of electricity and lower the entry barriers in the process of crypto currency production, which is more decentralized, without affecting security.

1. Introduction

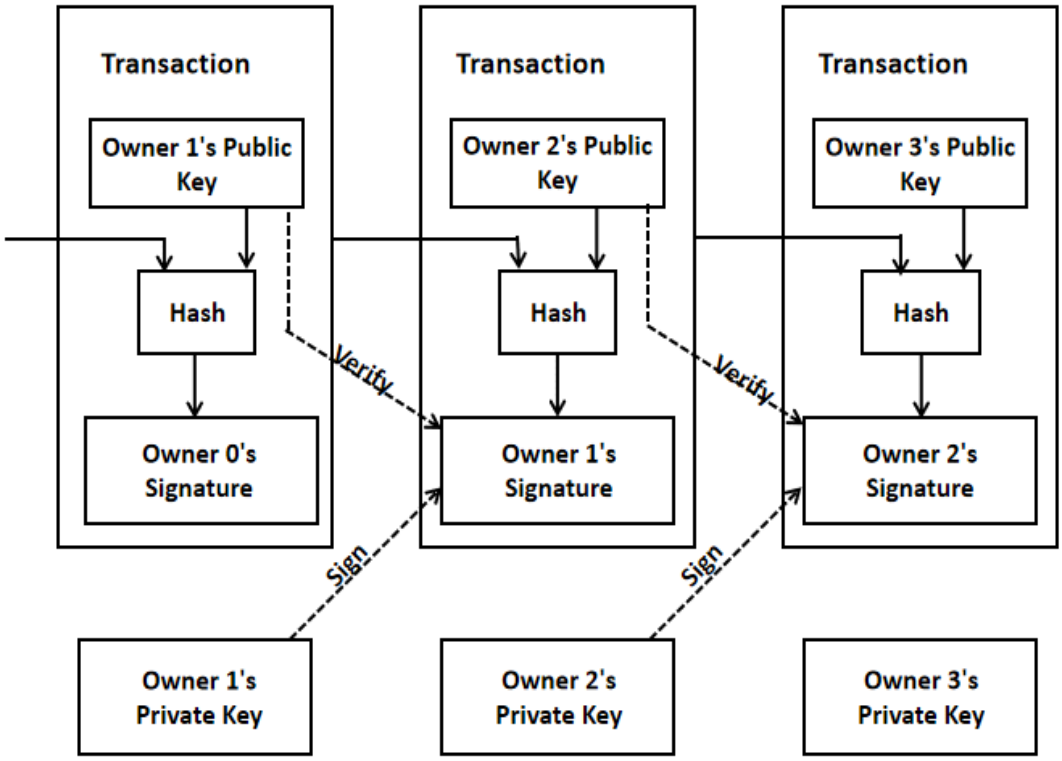
Bitcoin has proven that a peer-to-peer electronic cash system can indeed work and fulfill payments processing without requiring trust or a central mint. However, the PoW consensus algorithm used by Bitcoin has generated problems such as centralized hash power, tremendous energy consumption, not environmental friendly, and high entry barriers for mining. In response to this situation, the Burst team launched the innovative project of PoC mechanism in 2014 and gained a lot of supporters. This consensus algorithm is based on Proof Of Capacity, lowered the entry barriers and greatly reduced the energy consumption during the mining process. However, Burst has its shortcomings, because of the design flaws of its incentive mechanism, the users who entered Burst later can not get enough crypto currency rewards, and ultimately lead to insufficient enthusiasm for community participation. In 2018, BHD, which absorbed the advantages of Bitcoin and Burst, was born, and creatively added a dual incentive method to solve the above problems to some extent. However, BHD is still not good enough. Diskcoin absorbs the advantages of the above three and has carried out a series of optimizations.

2. Transactions

Diskcoin transaction structure is the same as Bitcoin, called UTXO (unspent transaction output).

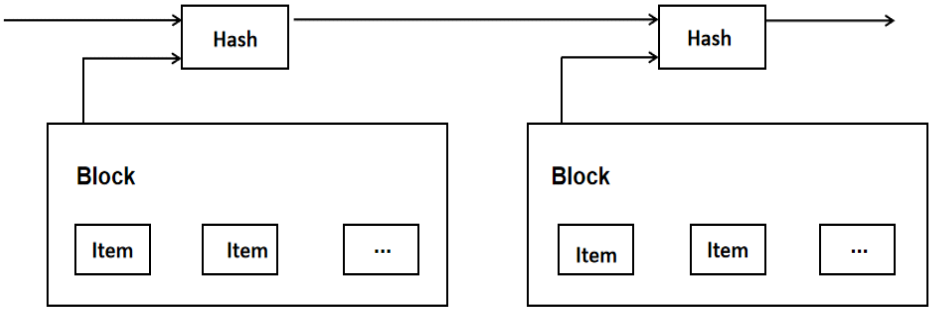


We define an electronic coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



The problem of course is the payee can't verify that one of the owners did not double-spend the coin. We need a way for the payee to know that the previous owners did not sign any earlier transactions. For our purposes, the earliest transaction is the one that counts, so we don't care about later attempts to double-spend. The only way to confirm the absence of a transaction is to be aware of all transactions.

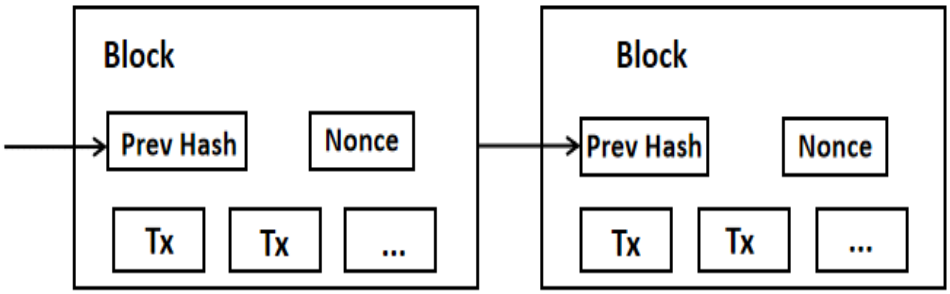
The solution we propose begins with a timestamp server. A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash.



Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

3. Block

Similar to Bitcoin, the ledger of Diskcoin transactions is built and stored in a linked series of blocks, known as a blockchain. This ledger provides a permanent record of transactions that have taken place, and also establishes the order in which transactions have occurred.



In Diskcoin, each block will try to fit as many of transactions possible until it hits the limit of 8MB which is similar to Bitcoin Cash, all prefaced by a block header that contains identifying parameters. Each transaction in a block is represented by common transaction data. The maximum block size is 8M. All blocks contain the following parameters:

Block Header

Block headers are serialized in the 136-byte format comprising ten fields: version, previous block hash, merkle root hash, timestamp, difficulty target, nonce, generation signature, base target, ploter ID, deadline.

The block header requires the following ten fields. Note that the hashes are in internal byte order; all other values are in little-endian order.

Coinbase Transaction

The first transaction in the body of each block is a special transaction called the coinbase transaction which is used to pay miners of the block. The coinbase transaction is required, and must collect and spend any transaction fees paid by transactions included in the block.

A valid block is entitled to receive a block subsidy of newly created diskcoin value, and it must also be spent in the coinbase transaction. Together, the transaction fees and block subsidy are called the block reward. A coinbase transaction is invalid if it tries to spend more value than is available from the block reward. The subsidy plus fees is the maximum coinbase payout, but note that it is valid for the coinbase to pay less.

The coinbase transaction must have one input spending from 000000000000000. The field used to provide the signature can contain arbitrary data up to 100 bytes. The coinbase transaction must start with the block height to ensure no two coinbase transactions have the same transaction id (TXID).

Block Serialization

Blocks must be serialized in binary format for transport on the network. Under current Diskcoin consensus rules, a Diskcoin block is valid if its serialized size is not more than 8MB. All fields described below count towards the serialized size limit.

4. CPoC

The PoC (Proof Of Capacity) consensus algorithm was derived from Burst, which began in 2014 and was upgraded to PoC2 in 2018.

Diskcoin uses CPoC (Conditioned Proof Of Capacity), which is based on PoC2 and adds the Staking mechanism. Miners who are involved in mining need Staking the corresponding

Diskcoins to get the most benefit. In the absence of Staking, the miner can get 40% of the mining reward; if the staking is sufficient, the miner will receive nearly 100% of the mining reward, and the others will be contributed to the Diskcoin Foundation to cover project development costs, promotion costs, and as a fund to support related ecological projects.

The CPoC economic model is learned from BHD, but Diskcoin has carried out a series of optimizations. One of the differences is that in Diskcoin mining, the proportion of coins that need Staking is not simply fixed or decrease progressively. Instead, for the first 1800 blocks, the miners would get 40% block reward at a fixed proportion, and from the block height of 1801, an algorithm named the DES(**the Dynamic Equilibrium Staking**) will be activated. The DES will automatically adjust the staking percentage according to the difficulty of mining, the amount of produced Diskcoins and the percentage of Diskcoin staking to ensure the good operation of the whole system.

5. Network

The network of Diskcoin is similar to Bitcoin. The steps to run the network are as follows:

1) New transactions are broadcast to all nodes.

2) Each node collects new transactions into a block.

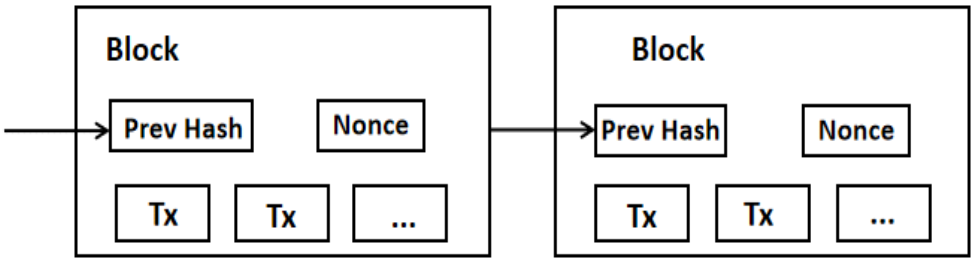
3) Each node works on finding a difficult proof-of-capacity for its block.

4) When a node finds a proof-of-capacity, it broadcasts the block to all nodes.

5) Nodes accept the block only if all transactions in it are valid and not already spent.

6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Nodes always consider the longest chain to be the correct one and will keep working on extending it. If two nodes broadcast different versions of the next block simultaneously, some nodes may receive one or the other first. In that case, they work on the first one they received, but save the other branch in case it becomes longer. The tie will be broken when the next proof-of-capacity is found and one branch becomes longer; the nodes that were working on the other branch will then switch to the longer one.



New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach many nodes, they will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

6. Incentive

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant of amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is disk space and electricity that is expended. The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free. The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more disk space than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

7.Distribution & Mining

The total supply of Diskcoin is 21 million, halved every four years, distributed by mining. Comparison of Diskcoin and Bitcoin:

Parameter	Bitcoin	Diskcoin
Total supply	21000000	21000000
Block time	10 mins	4 mins
Block size	1 MB	8 MB
Initial block reward	50 BTC	20 DISC
Halving cycle	Every 4 years	Every 4 years

8. Block Creation (Forging)

Three values are key to determining which miner eligible to generate a block, which miner earns the right to generate a block, and which block is taken to be the authoritative one in times of conflict: deadline, base target value, target value and generation signature .

8.1 Algorithms and Acronyms

8.1.1 Deadline

When you mine and process your plot files, you will end up with resulting values called deadlines. The values represent the number of seconds that must elapse since last block was forged before you are allowed to forge a block. If no one else has forged a block within this time, you can forge a block and claim a block reward.

8.1.2 Block Reward

If you are lucky enough to forge a block, you will get Diskcoin as a reward. This is called a block reward. For every 525000 blocks, the block reward is reduced by 50%. The initial reward is 20 Diskcoins per block. If you mining without any staking, you will get 40% reward per block. The more you staking, the closer your reward are to 100% per block, and the rest will be transferred to the Diskcoin Foundation.

8.1.3 Base Target

Base target is calculated from every block. This value adjusts the difficulty for the miners. The lower the base target, the harder it is for a miner to find a low deadline. It gets adjusted in a way that Diskcoin can have an average of 4 minutes for each block.

8.1.4 Network Difficulty

Network Difficulty, or NetDiff in short, is a value that can be read as an estimate on the total amount of space in terabytes dedicated to mine Diskcoin. This is a value that changes with every block in relation to base target.

8.1.5 Block Height

Every block forged gets an individual number. Every new block forged gets the previous block' s number + 1. This number is called block height, and can be used to identify a specific block.

8.1.6 Generation Signature

Generation signature is a based from the previous block generation signature and block generator. This value is then used by miners to forge a new block. Generation signature is 32bytes long.

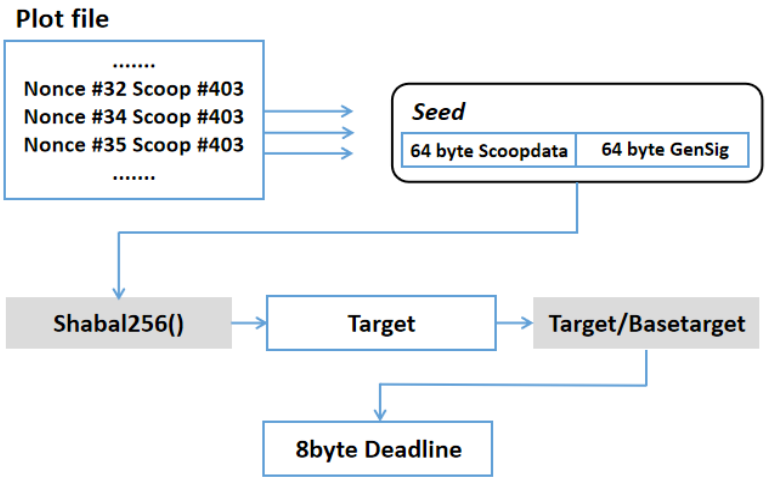
8.2 Mining Process

The first thing that happens when you start mining, is that the miner talks to the wallet and asks for mining information. This information contains a new generation signature, base target, and the next block height. Before the wallet sends over this info, it creates the generation signature by taking the previous generation signature together with previous block generator and runs this though shabal256 to get the new hash. The miner will now take the new 32byte generation signature, and the 8byte block height, and put them together as a seed for Shabal256. The result will be a hash value called Generation hash.

Now, the miner will do a small mathematical operation on this hash to find out which scoop number to use when processing the plot files. This is done by taking the generation hash modulo 4096, as there are only that many scoops.

Next step for the miner is to read all the 64-byte long scoops from all nonces in all plot

files. It will process them individually through shabal256 together with the new generation signature to get a new hash called target. This target is now divided with base target and the first 8bytes of the result is the value deadline.



To prevent so-called "nonce spamming" to the wallet, the miner usually checks if the current deadline found is lower than the lowest one it has found so far. Usually there is also a max value that can be set, as ridiculously large deadlines are of no use to anyone. After these checks, the miner submits information to the wallet.

8.3 Block forging process

8.3.1 Handling deadlines

The wallet has now received the information submitted by the miner, and will now create the nonce to be able to find and verify the deadline for itself. After this is done, the wallet will now check and see if an equal amount or more seconds has passed as defined by the deadline. If not, the wallet will wait until it has. If a valid forged block from another wallet is announced on the network before the deadline has passed, the wallet will discard the mining info submitted since it is no longer valid. If the miner submits new information, the wallet will create that nonce and check if the deadline value is lower than the previous value. If the new deadline is lower, the wallet will use that value instead. When the deadline is valid, the wallet will now start to forge a block.

8.3.2 Forging

There is a limit for a block that a block payload can have max 8MB. The wallet will start by getting all of the unconfirmed transactions it has received from users or from the network. It will try to fit as many of these transactions possible until it hits the limit, or until all transactions are processed. For each transaction the wallet reads, it will do checks. For example, if the

transaction has a valid signature, if it has a correct timestamp, etc. The wallet will also sum up all of the added transactions amounts and fees.

9. Conclusion

We have proposed a system for electronic transactions without relying on trust. We started with the usual framework of coins made from digital signatures, which provides strong control of ownership, but is incomplete without a way to prevent double-spending. To solve this, we proposed a peer-to-peer network using proof-of-capacity to record a public history of transactions that quickly becomes computationally impractical for an attacker to change if honest nodes control a majority of disk space. The network is robust in its unstructured simplicity. Nodes work all at once with little coordination. They do not need to be identified, since messages are not routed to any particular place and only need to be delivered on a best effort basis. Nodes can leave and rejoin the network at will, accepting the proof-of-capacity chain as proof of what happened while they were gone. They vote with their disk space, expressing their acceptance of valid blocks by working on extending them and rejecting invalid blocks by refusing to work on them. Any needed rules and incentives can be enforced with this consensus mechanism.

References:

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2009.

[2] Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak3, "Proofs of Space", https://eprint.iacr.org/2013/796.pdf, 2013.

[3] Sunoo Park, Albert Kwon , Georg Fuchsbauer , Peter Gaˇzi , Jo¨el Alwen , and Krzysztof Pietrzak, " SpaceMint: A Cryptocurrency Based on Proofs of Space", https://eprint.iacr.org/2015/528.pdf, 2015.

[4] Seán Gauld, Franz von Ancoina, Robert Stadler, "The Burst Dymaxion", https://www.burst-coin.org/wp-content/uploads/2017/07/The-Burst-Dymaxion-1.00.pdf, 2017.

[5] 4142454647484a4b5054575a, "BitcoinHD: Te Crypto Currency System Based on CpoC", http://www.btchd.org/BHD-Whitepaper-1.0_en.pdf, 2018.

[6] https://www.bitcoincash.org/spec/block.html