White Paper

Eä Mining Federation

PEER-TO-PEER BITCOIN MINING SYSTEM

frea.network

eascan.org

2022

Abstract. Blockchain Eä: A Peer-to-peer Bitcoin Mining System (www.eascan.org) is an exclusively peer-to-peer (peer-to-peer) version of the bitcoin mining solution that allows you to work independently in a solo mining mode without any existing centralized mining pools.

Digital signatures are part of the system. We offer a solution to the problem of the honesty of calculating the miner's reward using a peer-to-peer network. The network fixes timestamps tied to the blocks of the Bitcoin blockchain, forming a chain of hashed Proofs-of-Work. The records made in this way cannot be changed without re-confirming the work done on data processing. Thus, the chain not only serves as proof of a sequence of events, but also becomes the proof of being a result of computer calculations of all the participants of decentralized bitcoin mining. The essence of the network structure is quite simple. Messages are broadcast in the shortest time possible, based on the principle of least cost, by the efforts of the nodes themselves. Nodes can leave the network and rejoin it at will, accepting the final chain as confirmation of the changes that occurred in the chain during their absence.

1. Introduction

Mining via the Bitcoin network without your own capacity of several percent of the entire network almost in all work cases makes you rely on intermediaries, pools, acting as trusted third parties. Pools work quite well, but they still have the disadvantages inherent in a trust-based model. The cost of such mediation increases the operating costs of miners and brings a whole range of possible uncertainties, such as block holding (block concealment), delay in waiting (delay in the solution which may also damage the pool), differing principle and amount of reward in different pools, a pool commission for distribution and the distribution of only newly issued coins for the found block among the participants, understatement of payments to ordinary miners, the dominance of large players and their private agreements with pool owners on special conditions and the resulting risks of injustice for small and medium-sized pool participants. These costs and billing uncertainty can be avoided by using your own pool, but there is no mechanism to make the work transparent for all third-party pool participants without a trusted third party.

This requires a system to register all miners' solutions based on cryptographic evidence, not on trust, which allows any participant to be confident in the transparency of accounting and calculating the proportion of work done without third-party mediation. Hashes that are impractical to recalculate by computer for reversibility will protect miners from fraud. In this document, we propose a solution to this problem using a distributed peer-to-peer network consisting of nodes (servers) that generate computational confirmations of the chronological order of the work done by miners. The system lies in the security zone as long as honest nodes collectively control more computing power than any combination of attacking nodes.

2. Hashes

We see all the work done by all miners as a chain of digital signatures. When creating their local work, each miner includes there a link to all the actual shares that they have found to that moment. Miners publish shares as messages in the following form: “my address, nonce, extraNonce, status hash, link to the template used”.

If the share is more difficult than the one set by the consensus, it becomes the basis for the “snapshot” header, which saves all other shares mentioned to the pool chain.

In order to get rid of the intermediary, the shares must be published. It also requires a system that allows participants to agree on a single order of the history of the work done. All participants need some proof that most nodes agreed to count the hash when it is saved. The chain of snapshots is organized in such a way that an arbitrary third party can reassemble and recheck the solutions for all the problems mentioned in them.

3. Snapshot server and trusted time source

Our solution begins with a server that synchronizes the system's time and uses Bitcoin network blocks as a trusted source of timestamps. The idea is to hash the block of elements to be timestamped and to openly publish the hash, just like an ad, for example, in a newspaper. A timestamp proves that the data existed at a specific time, which is why it was included in the hash. Each timestamp includes the previous timestamp in its hash, forming a chain with each additional timestamp, strengthening all the previous ones in the chain.

4. Proof-of-Work

To implement a distributed timestamp server on a peer-to-peer basis we will need a “Proof-of-Work” system similar to the Bitcoin network system.

The task of a Proof-of-Work system is to find a value that, when hashing by means of SHA-256, will give a hash that starts with a certain number of zero bits. The standard amount of performed work is the quantitative amount of iterated solutions which depends on the number of zeros but, it will be enough to calculate the hashing function only once in order to check the found value.

In our snapshot and timestamp server, the search for a value with the desired hash occurs by iterating through the value of the iterated field - a random one-time password (OTP) in the data block. Once a satisfying the condition block is found its contents cannot be changed without doing the whole work again. If it is not the last element of the chain, this work also includes the recalculation of all the blocks following it.

Such Proof-of-Work also solves the problems by determining decision-making by majority vote. If one IP address is counted as a voice, such a scheme can be hacked if the distributed majority of distributed addresses are controlled.

In order to compensate for the increase in computing power and fluctuations of operating nodes in the network, the hashing difficulty must change to ensure a uniform block generation rate per hour. If they appear too quickly the difficulty increases and vice versa.

5. The network

Rules of the network:

1) New templates are sent to all nodes.

2) Each node collects the solutions found in a block.

3) Each node selects the appropriate complexity for the Proof-of-Work for its block.

4) As soon as such a Proof-of-Work hash is found, this block is sent to all nodes of the network.

5) Nodes accept a block only if all decisions in it are correct and fully verified.

6) Nodes express their agreement with the new data by working on the next block in the chain and using the hash of the previous block and the new template as the basis.

The longest chain is always considered correct and the nodes work to lengthen it. If two nodes publish different versions of the next block at the same time, one of the other nodes would receive one version earlier and someone else will receive another one. In this case, the nodes will work on the node that has been received first, but keeping another branch of the chain, in case it becomes longer. The final decision comes as soon as Proof-of-Work is received for a new block that will continue any of the branches, and the nodes that used to work on the disputed branch of the chain would switch to the correct one.

It is not necessary that new transactions have to reach all nodes. As soon as they reach a sufficient number of nodes they soon fall into one of the blocks. The principles of the communication between blocks are tolerant towards lost messages. As soon as the node that has missed one of the blocks receives the next one, and realizing that it has missed the previous one, it requests the missing information to fill the gap in the chain.

6. Impetus

According to the convention, the first transaction in the block is a special one; its output distributes the reward of the backbone network participants. This adds motivation for nodes to maintain the network and provides a way to distribute fairly without any centralized supervisory authority. Stable and long-term work has analogies with the work of gold miners who have also invested their funds and resources to extract gold and include it in commercial circulation. In our case, such means and resources are computing power and time and, of course, electricity.

One more impetus may be the miner's commission for the found block. The current sum is 0.25% of the value of the block found. The work motivation of the node is 0.5% of the cost of the block found by the miner working on it, it also helps to encourage participants to install and maintain network nodes, as well as to remain honest. If any node, driven by greed, tries to change the commission, damaging all honest participants' efforts, this theft attempt will cancel the block it has found in the Bitcoin network and deprive it of its own remuneration for the work done.

The option of "playing by the rules adopted by the community" is much more profitable, which ensures that you receive more rewards than anyone else, rather than undermining the system and, as a result, your own capital.

7. Disk space optimization

As soon as the last record is embedded in a sufficient number of previous blocks, all the records preceding it in the chain can be deleted in order to clean up your disk space. For the block hash to remain unchanged, all the transactions in the block are stored as a Merkle hash tree, only its root is included in the block hash. The size of old blocks can be reduced by removing unnecessary branches of this tree, it is not necessary to store intermediate hashes.

Keeping

An approximate possible estimate of the minimum average growth rate of the chain will be 60-90 gigabytes per year. The presence of a complete chain in the public access allows you to run the PPLNS calculator for any selected period of time, and not only in the present. You can see what reward distribution has taken place and between whom, at any time in the past.

The header of an empty block will be somewhat 48 bytes. Based on the calculation of the block generation rate once every thirty seconds, we get 48*120*24*365 = 50 MB per year. Data storage will not be a problem even if all block headers are in memory.

Snapshots refer to their predecessors in the same way that blocks in the Bitcoin chain do.

Speed

The current implementation allows you to check snapshots at a speed of 300 pieces per second on MacBook Pro M1which is about 20000 times faster than the average speed of their creation. That is, the full verification of the work solved by the network in 1 year will take approximately 1 hour.

Safety

The chain of snapshots is organized in such a way that an arbitrary third party can reassemble and recheck the solutions for all the problems mentioned in them.

The length of a chain is not limited by the protocol, it begins with genesis and ends at infinity.

Deduplication is applied to the chain in order to reduce the amount of stored and transmitted data.

8. Privacy

The traditional model of pools is maintained at a level of confidentiality where access to information is provided only to the parties involved and a trusted intermediary. The need to publicly announce all transactions precludes this method, but privacy can still be maintained by the anonymity of public keys. Only the information that someone has found a hash will be public, but without information on a specific hash to a specific person. This is similar to the information published by stock exchanges, where the time and volume of individual transactions are published openly but without specifying who exactly are the parties of such transactions. In order to increase the level of information security, a digital signature management solution is proposed by analogy with the work of certification centers. The node owner creates a master key and stores it offline. With it, he signs a token key which, in turn, signs blocks. In case of discrediting the token key, the node owner signs a new token key using the master key and announces the old one invalid. It is the node owner's responsibility to ensure comprehensive security of some offline storage of the master key and its inaccessibility to third parties. The network periodically generates verification blocks and sends them to nodes to monitor the correctness of their validation process.

9. Calculations

We consider the main goal of a decentralized network of independent pools (a node) a fair and transparent distribution of profitability among miners and network participants, in proportion to their freely verifiable contribution to the work on bitcoin mining. Therefore, the network does not imply the collection of any arbitrary commissions and deductions. To work together on the network, miners only need to have any computing equipment that supports the stratum protocol and follow the requirements of the instructions defined by the protocol, which the community has agreed upon during their individual work. The current consensus of the distribution of rewards among participants implies the distribution of the value of the entire block, including newly issued coins and the cost of all commissions from all transactions in the block. At the same time, network participants accept the importance of economic impetus for those participants who invest in the creation and maintenance of their own independent network nodes. That's why the owners of a node (a pool) should receive a percentageof the value of the block found on their node (pool) agreed by the community. Nodes that generate templates and distribute them over the net also should be economically stimulated, in the event that the template created by them becomes a block in the Bitcoin network. The project community should ensure the development of software for the operation of independent bitcoin mining pools, and continue to work on its support and development. By accepting and understanding this, participants determine the budget allocated to developers, the means of developing and promoting the project in the world. We also consider fair paying a bonus as a percentage of the block value directly to the miner whose equipment has found the block, thereby rewarding his luck and, as a result, the luck of all network participants. The element of luck is important in the short term and is leveled in the long term. Therefore, it is important that miners remain active members of the network for as long as possible. To do this, the network uses a smoothed proportional distribution of PPLNS (Pay Per Last N Shares) with a window length of 7 days in the past from this moment which is extremely effective for both the pool and stable miners. The participant's payment is calculated as a proportion of the sum of the products of all his shares multiplied by their complexity, stored in the blockchain network over the past seven days relative to all the saved shares of all participants multiplied by their complexity. Payments occur after the pool (node) finds the next block. The owners of the node (pool) with which miners work, using equipment without restrictions on the size of a Coinbase transaction, should strive to use direct payments directly through a Coinbase transaction. If direct payments are not possible due to technological limitations of the equipment or are not required by the individual decision of the node (pool) owner, then payments will be made by the node that has generated the template, like ordinary bitcoin transactions, but with the retention of the standard transaction commission in the bitcoin network at the time of such payment.

Thus, the PPLNS system smooths out the influence of the randomness factor, although it cannot exclude it completely and rather suits miners who constantly work in a decentralized distributed Peer-to-Peer mining network with a direct data exchange between participants.

The table of the current distribution of rewards adopted by the community

Income recipient	**The share of the value of a block, including commissions from transactions in it**
All working miners owners, in proportion to their participation in the PPLNS system with a window length of 7 days	98%
Network growth, development and society fund	1%
The owner of the node whose miner has found the actual block	0.5%
The owner of the node whose template has become the bitcoin network node	0.25%
The owner of the computing equipment (miner) that has found the block	0.25%

100% of the block cost and all commissions are distributed among the participants.

Reward coefficients and rules for the distribution of income between network participants can be revised by the consensus of the community at any time and adopted by installing appropriate software updates.

10. Conclusion

We have proposed a system of joint mining not based on trust. The construction of the structure began with a description of the main problems of centralized pools. We have solved this problem by means of a peer-to-peer network and a Proof-of-Work scheme to record the public history of all the shares found. Attempts to attack the network computationally, without most of the network resources, in order to change some old records, become almost impossible if honest nodes control most of the network power. The network is reliable in its unstructured simplicity. All nodes work independently with a small amount of coordination among themselves. They must not be identified, since messages are not sent to any specific location and are delivered only following the principles of "least cost". Nodes can leave the network and reconnect taking the longest chain of blocks as a confirmation of the missed history. They confirm their agreement to accept the correct block into the chain using their computing efforts to lengthen this chain or disagreement, rejecting incorrect blocks, refusing to work with such blocks. Via the consensus mechanism, any necessary rules and impetus can be enforced.