Ixcoin: An environment friendly
Peer-to-Peer Electronic Cash System

Decentralised Ixcoin Community

info@ixcoin.info

www.ixcoin.info

Abstract. Ixcoin is a peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double spending. Like in in the case of Bitcoin, we propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions are similarly hashed into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The main difference is the environment friendly approach, called merge mining. Ixcoin is natively designed to be anonymous as well as bitcoin, but with the aim to become, once the technology will allow it, biometrically attached to a person or a group of people. In order to maintain its decentralised state, Ixcoin project will encourage the participation of single users in becoming a node of the network.

1. Introduction

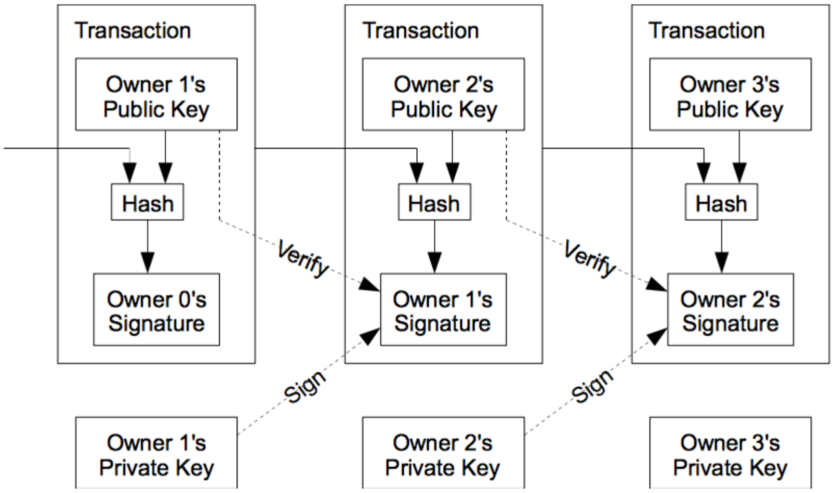
As Satoshi explained, commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust-based model. Completely non-reversible transactions are not possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services.

A problem Bitcoin has to face is the increasing cost of its non-reversible transactions, since the escalating cost of mining must be compensated by an escalating cost of each transaction, encouraging miners to prefer users offering a higher fee, making difficult to little investors and owners to send virtual currency to an affordable price.

Ixcoin project is not simply an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. It takes advantage of existing computational power already “wasted” for Bitcoin blockchain, as already mentioned called **merge mining technology**, and from now on shortened in MMT.

2. Transactions

Equally to Bitcoin, 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.

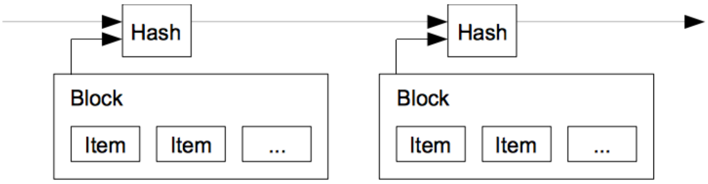


The only way to confirm the absence of a transaction is to be aware of all transactions. In the mint based model, the mint was aware of all transactions and decided which arrived first. To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction, the majority of nodes agreed it was the first received.

In the case of Ixcoin, since it has been designed to face the challenges related to the "**end of minting**" decades before Bitcoin, after less than 4 years it started to rely on the willingness of miners to continue include Ixcoin in their mining portfolio.

3. Timestamp server

A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash. 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.



4. Sustainable Proof-of-work

Like explained by Satoshi, the proof-of-work solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of- work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains.

To compensate for increasing hardware speed and varying interest in running nodes over time, the proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. If they're generated too fast, the difficulty increases.

Since the proof-of-work needs a high value of mining to remain secure, the risk is an overly expensive and a great amount energy wasted. Ixcoin has no aim to substitute Bitcoin, but to reinforce the concept behind Bitcoin serving as sidechain and as an alternative project as well, with the goal to address Bitcoin limitations in a more affordable way.

The cost of bitcoin structure, designed by Satoshi Nakamoto with the goal to be minimal, is becoming an environment problem, since it required a significant amount of electric energy “wasted” in computational work. The MMT allows Ixcoin to guarantee **cheaper on chain transactions** to users looking for a peer-to-peer cash system.

5. Distributed Network

The steps to run a distributed network are as follows:

- New transactions are broadcast to all nodes.
- Each node collects new transactions into a block.
- Each node works on finding a difficult proof-of-work for its block.
- When a node finds a proof-of-work, it broadcasts the block to all nodes.
- Nodes accept the block only if all transactions in it are valid and not already spent.
- 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.
- Future **nodes distribution on single users** portable and home electronic devices

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. In future updates, **single users** will be able to be **independent nodes**, even partial, contributing to the security of the network.

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 CPU time 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 CPU power 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.
There is the risk it will be more profitable not to play by the rules, especially once the all coins have been generated. The reduction of costs using **MMT**, along with a **future distribution of the coins mined in the first 6050 blocks**, should keep miners active and willing to mine Ixcoin.

7. Payment verification: from PoW to RPoW

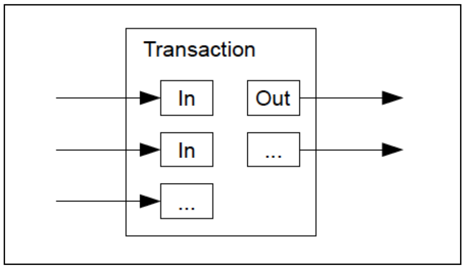
As designed by Satoshi, it is possible to verify payments without running a full network node. A user only needs to keep a copy of the block headers of the longest proof-of-work chain, which he can get by querying network nodes until he's convinced he has the longest chain, and obtain the Merkle branch linking the transaction to the block it's timestamped in. One strategy to protect against this would be to accept alerts from network nodes when they detect an invalid block, prompting the user's software to download the full block and alerted transactions to confirm the inconsistency.
An important feature of Ixcoin will be the future inclusion on mobile devices working as nodes, with a **pruned blockchain**, holding memory of the last 1000 blocks only, serving to reinforce the network against attacks. In order to reduce the chance of an attack another function will be the use of **randomly chosen mobile devices** as confirmation. Once the **Random Proof of Work** (RPoW) is implemented, the number of confirmation will be progressively increased, adding a security layer to the network.

8. Contribution system

Ixcoin Project cares as much about anonymity in receiving likewise in giving.
Since minting is concluded since the 14th of October 2014, miners have supported themselves by means of transactions fees only.
In order to support miners, Ixcoin future updates will include the “**re-mining**” of the coins contained in the first 6050 blocks, officially. The first 6050 produced blocks equal to 96*6050= 580,800 IXC
The coins in the 6050 blocks will be distributed to miners with a flat rate of 1 IXC/block, till all the equivalent amount of coins sent in the first 6050 are produced.
This will mean that if User A sends 2 IXC to one of the first 6050 addresses, the 2 IXC will be added to the total amount of coins to be minted. This will create a system that in the future will find in **anonymous donations** a way to support miners as long as Ixcoin exists.

9. Combining and Splitting Value

Although it would be possible to handle coins individually, it would be unwieldy to make a separate transaction for every cent in a transfer. To allow value to be split and combined, transactions contain multiple inputs and outputs. Normally there will be either a single input from a larger previous transaction or multiple inputs combining smaller amounts, and at most two outputs: one for the payment, and one returning the change, if any, back to the sender.



10. Privacy and security

Despite all transactions are public, privacy can be maintained by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.
Ixcoin aim is not achieve anonymity “at any cost”, having no desire to foster illicit use of blockchain technology. In the other hand, Ixcoin project has in mind to “connect” public keys to biometric data to increase security in the use of blockchain. The risk of losing permanent access to a personal wallet could be mitigated by including **biometrical information**, encrypted in the blockchain, enabling the user to retrieve the wallet even in case the wallet password is lost.

11. Consensus

In order to implement all the new features Ixcoin has the potential to develop, consensus among miners is fundamental.
Ixcoin Community is trying to convince miners to realize the advantages in updating to the last client.

12. Conclusions

The evident advantage of Ixcoin is the cheapest mining cost taking advantage of MMT and consequent cheaper txs.

The security of the blockchain will be increased through:

- the participation of single users on their mobile devices working as pruned nodes;
- the implementation of RPoW, adding a layer of security to the blockchain;
- the distribution to miners of the coins in the first 6050 along with future donations to one of that addresses (consensus for an hard fork needed);
- the (facultative) implementation of biometrical information of users;
- the possibility to send anonymous donations to miners to support the network;

Ixcoin Community follows these basic principles:

Laws & Culture: Respect the laws, culture and customs of every nation and contribute to economic and social development through engaging communities.

User Engagement: Engage and focus on users then all else will follow.

Equality: Judge people on the basis of their contribution, not on personality, education, background, culture, orientation or preferences.

Innovation: Help create products and services that will have a positive impact on humanity and the environment.

Supportive Community: Nurture a culture that enhances individual creativity and teamwork with a focus on community, while honouring mutual trust and respect.

Decision Making: Decisions should be based on facts and objectively considered, not influenced by emotions or prejudices.

Community Engagement: Interact with the wider cryptocurrency community to research, create and achieve stable long-term growth and synergies.

References

[1] W. Dai, "b-money," http://www.weidai.com/bmoney.txt, 1998.

[2] H. Massias, X.S. Avila, and J.-J. Quisquater, "Design of a secure timestamping service with minimal trust requirements," In 20th Symposium on Information Theory in the Benelux, May 1999.

[3] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[4] D. Bayer, S. Haber, W.S. Stornetta, "Improving the efficiency and reliability of digital time stamping," In Sequences II: Methods in Communication, Security and Computer Science, pages 329-334, 1993.

[5] S. Haber, W.S. Stornetta, "Secure names for bit-strings," In Proceedings of the 4th ACM Conference on Computer and Communications Security, pages 28-35, April 1997.

[6] A. Back, "Hashcash - a denial of service counter-measure," http://www.hashcash.org/papers/hashcash.pdf, 2002.

[7] R.C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

[8] W. Feller, "An introduction to probability theory and its applications," 1957.

[9] Satoshi Nakamoto, " Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.