Makta

A decentralized peer-to-peer rewards, loyalty, and social media platform

Amiré Najie

www.Makta.org

Abstract: Decentralized currencies have emerged at a relatively fast pace since the last decade. With decentralization, we have managed to eliminate central authorities from our trades and transactions by designing a chain of blocks that can be validated and verified by the network itself. But in addition to security and privacy, they need to be fast enough to be accepted globally. Makta proposes a faster response time in addition to improvements to security and privacy so that businesses can accept money online, and people can send, receive, and spend money without needing to wait for the blocks to be shaped.

On the other side, social media platforms have been upgraded to offer better speed, reliability, and user experience, but because they are being run and managed by central authorities, they lack security, free speech, and privacy. With its decentralized structure, Makta proposes the highest privacy and security for users in addition to the highest speed so that people can communicate in a real-time manner without fear of being censored, monitored, or banned by a central authority.

To validate transactions to be legit and also to prevent double-spending, we propose a proof-of-presence mechanism (POP), in which the majority of nodes will decide which transaction is legit and which is not at any time a transaction or block is created. Nodes will be ranked dynamically based on multiple factors and the network will use their ranks to conduct verification inquiries.

Introduction:

Makta is a completely decentralized reward, loyalty, and social media platform that utilizes money transferring, messaging, and social networking globally without any interference or control of any kind in a real-time manner. Its mission as it is registered in its first block is "to give people freedom back and to tackle inflation they struggle with".

Fast transaction verification and broadcasting make it an ideal solution for online and in-store (point-of-sale) payments, rewarding customers and loyalty programs, and also for real-time chat, messaging, and social media posts and activities.

Technically, it's entirely based on nodes who contribute and facilitate this feature all around the world. The more people attend to the network as Noders, the more stable and fast it becomes. Noders will also make money through rewards for their contribution (Noding).

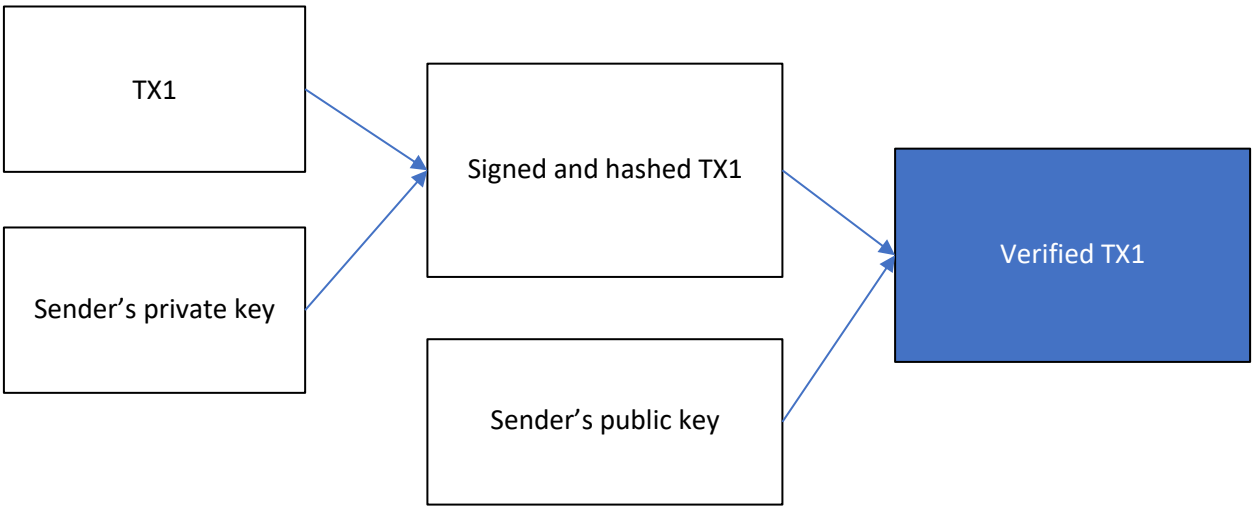
Definitions:

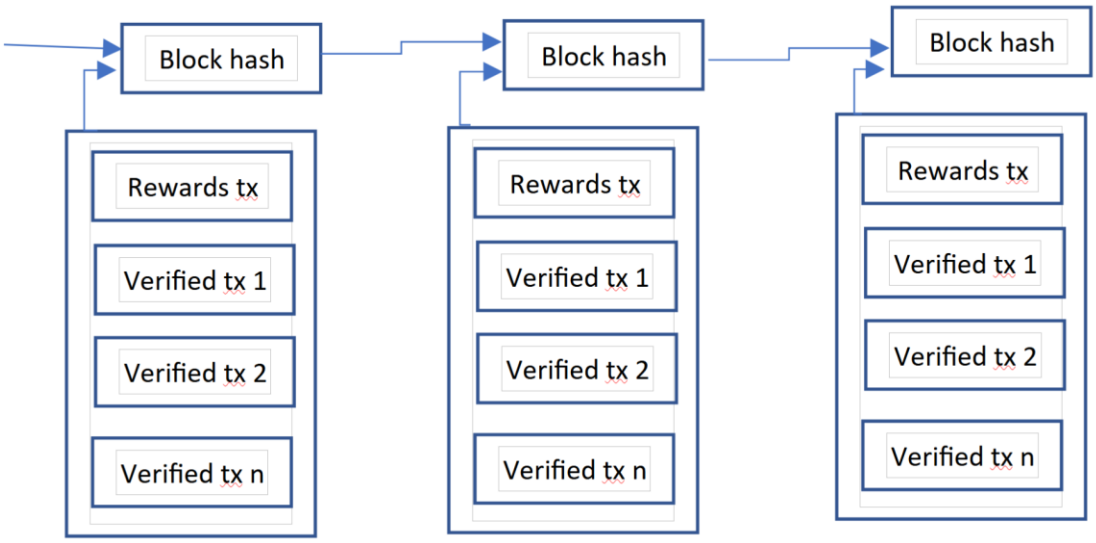
To node or Noding blocks: refers to the participation of nodes to validate transactions or building blocks of the blockchain. (The process by which they will get Noding rewards)

Transactions:

Transactions are the lowest level of entities in the blockchain, and they consist of the sender and recipient information (Account ID and wallet address), body, timestamp, and other control fields. This information will then be used to generate the transaction's hash to seal it and to make sure it can never be changed or reverted later on. Makta uses this hash as well as the sender's private key to sign the transaction before broadcasting it to the network for validation.

Every transaction made and broadcasted to the network is validated by the majority of nodes through the Proof-of-Presence (POP) mechanism to make sure it is a legitimate transaction.





Native Currency:

While people don't necessarily need to have any coins to spend and can start using the platform for collecting points, redeeming, and social media activities immediately after creating their first wallet and getting their universally unique digital ID, for money transactions they will need to have some coins to spend. Makta's native coin is called MAK which people can obtain by collecting and redeeming points, buying it, or Noding by participating in the Noding process.

Wallets:

The first step to start using Makta is to create a wallet. When creating wallets, you will be asked to choose an ID for yourself (which will be validated by the network to make sure it's unique universally). This ID will be your digital ID and offers the ability to be used by 3rd-party applications in the future to identify your credentials as a digital ID gateway. The system then generates a random 12-word seed phrase as your restore key and asks you to set a local password to sign transactions before sending anything out from your wallet. **The most important thing** is to keep that 12-word seed phrase in an extremely safe place because that will give you the ability to restore your wallet in case you need to restore your wallet on the same or other machines in the future.

Social media:

Makta introduces a universal digital ID in which you can choose your own ID as your Account ID as opposed to your wallet address which is a long string generated automatically and randomly by the system. You can then send or receive messages or money through your digital ID (Account ID) instead of remembering or using long wallet addresses. For example, if your ID is “Bob” and someone wants to send you a message or some money, they don’t necessarily need to have your wallet address. They can use your Account ID to send you messages or money.

Makta introduces a built-in contacts management system as well. So, you can save and manage your contacts easily within your wallet.

Anti-spam:

Wallet addresses can be used to send or receive messages or money as well. When sending money, it can be sent to either a contact from the list, an Account ID, or a wallet address. But for sending messages, the destination ID must be saved in your contacts list first as a method to protect the network from spam.

Privacy:

Makta’s network is spread amongst the internet, and it eliminates any third-party control or authorization. It ensures that people have full control over their money, messages, social media activities, and privacy by applying digital signature methodology through cryptography when creating transactions.

Network security and Proof-of-Presence (POP):

Since there will be no central trust or organization to validate the transactions for the network, the biggest challenge is to keep the network highly secure and accurate. This means that we need to prevent double-spending, making false transactions (spending money someone does not own), or manipulating transactions after they are confirmed by nodes.

To achieve this, Makta is introducing the Proof-of-Presence (POP) mechanism to make sure every single transaction is confirmed and verified by the majority of nodes who are present in the consensus process.

Nodes then will participate in the Noding blocks through the consensus process as same as for the transactions. That means the majority of nodes have to validate blocks before shaping and adding them to the blockchain (the process of Noding).

Transactions and noded blocks will get validated by either n/2+1 total nodes or n/2+1 participating nodes in a timeframe of maximum "m" minutes to make sure every node with different processing power or internet speed will get equal chances to vote.

Once a transaction or block is approved by the network, nobody literally can manipulate it or remove it from the blockchain as a ledger.

If two or more blocks get noded by different nodes, (and all contain valid transactions), we will end up having multiple instances of blockchain with different hash tables. To prevent this, nodes will get Noding permission from the network through an inquiry process before starting the Noding process, and even if after this inquiry process, we still have two or more valid blockchains with the same length, the network will keep the one with the oldest shaped blocks and ignore the rest.

MAK coin circulation and Noding rewards:

Nodes will get rewards in MAK coins for their participation in validating the blockchain. Blocks will have reward transactions in their transactions list. This is to give nodes incentives and to distribute coins into circulation alongside the loyalty rewards people collect by spending at stores.

In the Makta economy, Noders will not compete with each other to win the rewards, but contrariwise, they will contribute and cooperate to keep the network secure. Noding rewards will then be calculated and spread amongst all participating nodes based on their ranks.

The network continuously and dynamically calculates nodes' ranks by taking multiple measures into account like joining date, syncing history, response time, network stability, etc.

Nodes can leave and re-join the network at will, and if they don't present in a Noding of a specific block, they will only miss the reward of that particular block.

While there will be no fees for sending messages or using social media features, money transactions can have fees that can be determined by the sender when spending their coins. This fee will be spread amongst the participating nodes as well alongside the Noding rewards. After the coins in circulation reach the maximum predefined amount, nodes will receive transaction fees only as their incentive.

Disk space:

Makta is using compression methods to reduce the size of data that is stored or broadcasted to the network to accelerate the broadcasting process. This means that the system will need as low disk space as possible to keep itself up and running. The network's accumulated computing power of nodes and memory pool will be tremendous as well for the future developments of ocean computing.

Conclusion:

We have proposed a peer-to-peer ecosystem that does not rely on any central authorization or trust. To achieve this, We have implemented decentralized digital ID and digital coins using digital signature algorithms to make sure everyone owns their money solely. To prevent the network from fraud or double-spending, we proposed Proof-of-Presence (POP) mechanism so that the majority of nodes that have legit transactions ledger will control the flow of transactions.

Nodes are spread on the Internet and they cannot be identified as transactions will be broadcasted to the network through different and shortest routes. They can leave and re-join the network at will but they will only get rewards for their participation in validating transactions and blocks in which they were present. They will be re-synced when they join the network back to have the latest blockchain while they were absent.

References:

1) J.Jin Kang, K.Fahd, S.Venkatraman, “Trusted Time-Based Verification Model for Automatic Man-in-the-Middle Attack Detection in Cybersecurity”, https://www.mdpi.com/2410-387X/2/4/38, 2018

2) A. Mohammed and N. Varol, “A Review Paper on Cryptography”, https://www.researchgate.net/publication/334418542_A_Review_Paper_on_Cryptography, 2019

3) “Security Engineering: A Guide to Building Dependable Distributed Systems”, https://www.cl.cam.ac.uk/~rja14/Papers/SE-05.pdf

4) Abiodun O. Odedoyin, Helen O. Odukoya, Ayodeji O. Oluwatope, "A QUANTUM CRYPTOGRAPHY PROTOCOL FOR ACCESS CONTROL IN BIG DATA", 2018

5) S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2

6) R.K Gupta, "A Review Paper On Concepts Of Cryptography And Cryptographic Hash Function", 2020

7) Dwi Liestyowati J. Phys.: Conf. Ser. 1477 052062, "Public Key Cryptography", 2020

8) R. Azarderakhsh; K.U. Järvinen; M.Mozaffari-Kermani, "Efficient algorithm and architecture for elliptic curve cryptography for extremely constrained secure applications", https://ieeexplore.ieee.org/abstract/document/6693767,2014

9) W.J Caelli, E.P Dawson, S.A Rea, PKI, elliptic curve cryptography, and digital signatures, 1999