Proof-of-Sovereignty (PoSv) as a Method to Achieve Distributed Consensus in Crypto-Currency Networks

Hegadekatti, Kartik and S G, Yatish

1 September 2016

Proof-of-Sovereignty (PoSv) as a method to achieve Distributed Consensus in Crypto-Currency Networks.

Dr.Kartik H & Dr.Yatish S.G

Authors' Email: dr.kartik.h@gmail.com; dryatish.blr@gmail.com

ABSTRACT

In this paper, a method to implement K-Y protocol using Distributed Consensus is discussed. Firstly, the various available methods are discussed. Then, Proof - Of - Sovereignty (PoSv) is proposed. Its mechanism is deliberated and its advantages are described vis-a-vis other methods of distributed consensus. Finally a summary of all the procedures involved in 'NationCoin Mining' is explained.

INTRODUCTION

Crypto currencies use cryptography to secure transactions and create additional units in a decentralized network. This process needs consensus among various computers which are

part of the network. Consensus is necessary because certain processes within the network may be faulty or less reliable. If the computers can communicate among themselves then the faultiness can be detected, arrested and rectified. Moreover, when the computers agree on the value of output, network reliability greatly increases. This forms the premise of many autonomous and self-regulated network systems.

Block Chain- A blockchain is a public ledger of all cryptocurrency transactions that have ever been executed. It is distributed in nature. It continually grows as 'verified' blocks are added to it with a new dataset for every block. The blocks are added to the blockchain in a linear, chronological order.

Verification-It is done by Miners taking into account only those blocks those follow the rules of transactions. There are several processes like checking the validity of inputs, that the output isn't greater than the input, ensuring that coins aren't double-spent, etc. Verification is done by a

series of complex cryptographic programs run by the computer.

There are several ways to achieve distributed consensus. Crypto currency networks use many such methods. Few of them are:-

(1)Proof-of-Work - One of the most used and familiar methods. The best example is Bitcoin and Ethereum mining. In this process, partial hash inversions are used to prove that work was done. It requires some work to be done to prove that the worker is a bona-fide and interested USER. Only then will the worker be made party to mining on the network.

(2)Proof-of-Stake - Here the network demands that the user prove ownership of a certain quantum of money, which is the user's stake in the system. Once they prove their stake, they get to verify transactions and "mine" the crypto currency.

Mining - Network members need to be rewarded to help authenticate transactions. Without such a reward, there is no motive for anyone to spend

precious computation capacity just to help authenticate someone else's transactions. If network members do not use that power, then the entire system becomes useless.

Hence there is provision for incentives to members who help in authenticating transactions. Specifically, we can reward anyone who successfully confirms a block of transactions by giving them some units of cryptocurrency.

In the K-Y Protocol, this authentication process or validation is called mining.

Mining Nodes give their processing power to the network in exchange for the opportunity to be rewarded by Cryptocurrency units.

Miners validate new transactions and record them on a distributed ledger-the BlockChain.

A Mining node will do the following:

a) Collect transactions to prepare for the next block.

b) Check all transactions in the memory pool and remove any that were included in the earlier block.

c) Prepare remaining transactions in the memory pool which are unconfirmed for future blocks.

d) Searching for a solution to the Proof-of-Work.

Independent combination of the transactions into new blocks by mining nodes, coupled with working on a proof of work algorithm is done by every mining node.

Later, after the Proof-of-Work is solved, independent verification of each transaction by every full node takes place. This culminates in the adding of the block to the BlockChain.

For every block of transactions successfully authenticated, the victorious miner gets a cryptocurrency reward.

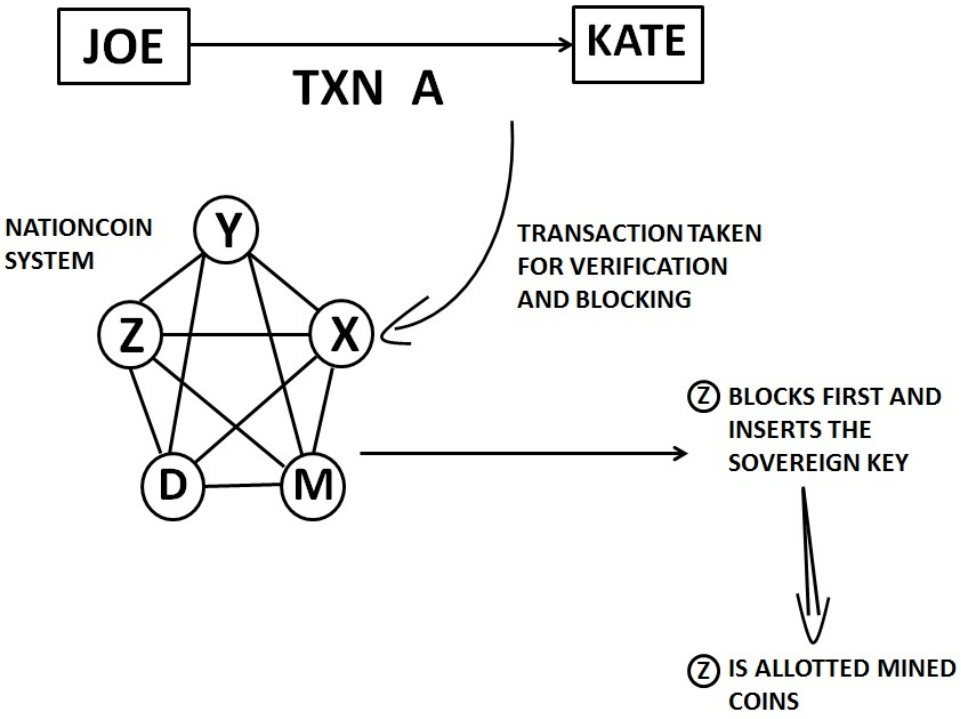
This Proof-of-Work in needed to confirm that the said node is a bona-fide entity and a serious candidate to 'mine' cryptocurrencies.

PoSv - POSV is a method to achieve distributed consensus in the NationCoin system as described by the K-Y Protocol [1].

The K-Y Protocol is a set of rules and instructions to implement the Regulated and Sovereign Backed Cryptocurrency (RSBC) system. It envisages a highly secure Controlled Block Chain in which Sovereign backed Cryptocurrencies will be transacted without minimal hassles. It is primarily accomplished using the NationCoin system. There are two aspects to the NationCoin system; the software aspect and the hardware aspect. The software aspect consists of mining using the PoSv.

DAR-Digital Asset Reserve- Organisation which will frame policies and manage the system based on K-Y Protocol.

The NationCoin system is a totally sovereign network dedicated to run the K - Y Protocol.



TXN-Transaction

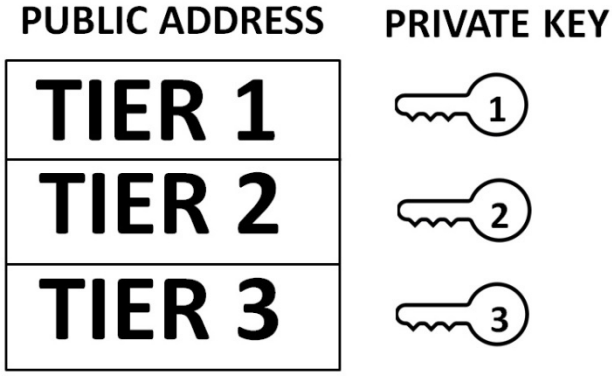
**Blocking is a process in which Transactions are collected, verified and arranged in a block by the nodes.*

In PoSv, each sovereign node which participates in the 'mining' process has to show that it is a sovereign node. The node that verifies transactions fastest (or in a pre-determined order) and proves sovereignty will be 'mining' the NationCoins. Sovereignty is proved by a multi-tiered encryption key which we call as the "Sovereign Key" (SK).

The DAR (The main institution envisaged by the K-Y Protocol) will provide the Sovereign Key. But this Sovereign Key will not be permanent. The DAR will randomly and periodically keep changing the Sovereign Key. The changed Sovereign Key will be updated in all the nodes by DAR on an individual DAR-to-node basis through Quantum Key Distribution [2].

The nodes will mine NationCoins turn-by-turn. After submitting every block, each node will prove its genuineness by providing the Sovereign Key. This will prove to the network and DAR that the mining node is a Sovereign Node.

The Sovereign Key will be in the form of multi-tiered interconnected public addresses each tier having a unique private key.



The Master node, i.e the DAR can ask any node for the Private Key of any tier randomly to check for authentication. The DAR, apart from common network connectivity- i.e all nodes being connected and part of network- will also be individually connected to every node. The updated Sovereign Key will not be propagated by one node to the other. Only DAR will upgrade the nodes individually about the change in Sovereign Key.

The PoSv process will ensure many things.

(1)Network security - Any third party like a hacker will not be able to prove sovereignty without the Sovereign Key.

(2)Network competitiveness - In proof of stake, the nodes get to 'mine' coins in a predetermined sequence. But in POSV, every node will have the Sovereign Key. Therefore, to become a winner node, each node will have to confirm and verify transactions faster. In case of Quasi-Autonomous Nodes where mining of NationCoins is outsourced, PoSv will increase Network

competitiveness. This will provide incentive to each node to work to upgrade its hardware and software configurations, yet be compatible with the NationCoin Network.

This way, each node has a reason to work faster and better, thus improving competitiveness (The only bottleneck will be the speed of transaction verification).

(3) Network reliability - If the Sovereign Key gets changed (by DAR) and if one or many nodes cannot update the Sovereign Key, then it points to a problem (in that node or the network or both) which can be detected and rectified.

(4)Full control by sovereign authority - The sovereign authority (i.e. the DAR) has full control of all nodes at all times. If any node turns 'rogue' or is problematic, that node can be excluded from the mining process by simply denying it the Sovereign Key.

(5)Decentralised working in a Centralised Framework-

(a) A Federal Network is one where a sovereign authority is concerned only with the authentication of nodes and not the network details. It only verifies the credentials of the nodes and is not bothered about the minutiae of work done, as long as it is valid

(b) A Unitary network is one where all aspects of the network is micromanaged by the Sovereign Authority.

The NationCoin network will be a Federal Network and PoSv will make it possible.

Cryptocurrency Networks (Crypto Networks for short) are essentially decentralised. This has several advantages. Sovereign Authority is usually considered a centralising figure. As such the NationCoin network managed by a Sovereign Authority may thus appear centralised in Nature. By Centralising Crypto Networks we may lose out on several essential characteristics that would be advantageous. PoSv makes it possible to preserve

and benefit from the decentralised nature of a Sovereign Crypto Network.

In PoSv, The Sovereign Authority is only concerned about the sovereign nature of the nodes. PoSv leads to the creation of a federal network. At the same time, the Sovereign Authority can keep control of the NationCoin Network through the Sovereign Key.

This makes it uniquely decentralised in a Centralised Framework.

A Summary of events in PoSv Mining.

Transactions obtained from network by nodes A, B, C, D, E, F....

Node B takes it for verification

Verification completed by node B

Verified transactions put into a block by node B

B inserts the Sovereign Key and provides POSV

Network confirms node B's POSV

B's block is accepted and it becomes part of sovereign block chain

B is 'awarded' NationCoins- to be put into public circulation.

The Network formed by the NationCoin system will function as follows-

a) New transactions occurring on the network are broadcast to every other node on the network.

b) Every node will collect the new transactions into one block.

c) Every node will provide PoSv for the said block.

d) One of the nodes is chosen to make the transactions into blocks. Or in case of Quasi-autonomous nodes, the node which blocks fastest is a 'winner node' and allowed to 'mine' NationCoins.

d) When a node successfully provides PoSv, it broadcasts the block to all the nodes.

e) The other Nodes will agree on the block validity provided all the transactions in it are authentic and are not already spent.

f) The Nodes will communicate their agreement of the block and its contents by working on generating the next block in the chain, using the hash of the accepted block as the previous hash.

CONCLUSION

The Proof of Sovereignty (PoSv) ensures that the network is secure, reliable and competitive for the NationCoin system. At the same time, it is assured that the sovereign authority remains in control of the Network at all times. Even though the NationCoin system appears to be a centralized network, The DAR, through PoSv can maintain a decentralization NationCoin network. This, in essence makes it a Federal Network rather than a Unitary Network

Moreover, large-scale capital investment necessary in Proof-of-Work and Proof-of-Stake is also avoided. Thus PoSv guarantees the successful implementation of the NationCoin System.

References

[1] THE K-Y PROTOCOL: THE FIRST PROTOCOL FOR THE REGULATION OF CRYPTO CURRENCIES (E.g-Bitcoin)

[2] THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY BY SIMON SINGH