The K-Y Paradox: Problems in Creating a Centralised Sovereign Backed Cryptocurrency on a Decentralised Platform

Hegadekatti, Kartik

29 March 2017

THE K-Y PARADOX: PROBLEMS IN CREATING A CENTRALIZED SOVEREIGN BACKED CRYPTOCURRENCY ON A DECENTRALIZED PLATFORM

Dr.Kartik H

Author's email-dr.kartik.h@gmail.com

ABSTRACT

Cryptocurrency networks and Blockchains are decentralized systems, functioning on distributed consensus. Fiat currencies on the other hand are issued, maintained and supervised by a sovereign central authority. RSBCs are Regulated And Sovereign Backed Cryptocurrencies (based on the K-Y Protocol) i.e. they are essentially decentralized cryptocurrencies floated by a central (sovereign) authority; it presents a paradox; known as the K-Y paradox. This paper explores the various dimensions of the K-Y paradox and its resolution.

INTRODUCTION

A cryptocurrency is a medium of exchange using cryptographic techniques to safeguard transactions and also manage the formation of additional units of the currency.

A BlockChain is a widely disseminated archive of data that maintains a continually-expanding register of records fully and reliably protected from any alteration or modification. Each block has a timestamp and link to the preceding block.

A Crypto wallet is an encrypted electronic device that allows an individual to make electronic cryptocurrency transactions. Each wallet will have a public key visible to anyone. But it can be operated by only a person who has a private key.

Transactions on the cryptocoin network are usually anonymous. When people send cryptocoins to each other, someone has to keep account of who spent how much at what time. In case of fiat money (or paper money) it is done by banks (known as Trusted Third Parties, for which they charge a commission).But in case of Cryptocoins, it is registered on a ledger called BlockChain (with nil or minimal transaction fees).

The cryptocoin network makes free (or inexpensive) transactions possible by detailing all the transactions made during a certain timeframe into a list. This list is known as a block. A certain set of people called 'miners' verify these transactions mathematically and register them on the BlockChain.

Those bona-fide miners who have successfully verified the transactions are paid freshly created Cryptocoins. This is how miners are rewarded, and new cryptocoins are generated. This is also the reason why no transaction costs are levied, as the network (in the form of miners) verifies the transactions.

Bitcoin is a peer-to-peer based cryptocoin which is not backed by any commodity and (unlike fiat money) carries no sovereign guarantee whatsoever. It is Unregulated and non-backed cryptocurrency with no sovereign guarantee. Regulated and Sovereign Backed Cryptocurrencies (RSBC), on the other hand are government backed cryptocurrency akin to paper currency, but in digital form.

In this system, the cryptocoins (known as NationCoins) are backed by Sovereign Guarantee. They are run on a highly secure Controlled BlockChain (CBC) [1]. NationCoins are completely managed by the Sovereign Authority i.e. the Government. This system is based on the K-Y Protocol [2]. The K-Y Protocol is a set of rules and instructions to implement the Regulated and Sovereign Backed Cryptocurrency (RSBC) system.

DIFFERENCES BETWEEN RSBC AND UNREGULATED CRYPTOCURRENCY

	CONTROLLED BLOCKCHAIN (RSBCs)	**UNREGULATED BLOCKCHAIN (BITCOIN,ETHEREUM)**
Contract Execution	Possible (based on K-Y Protocol)	Possible in only some Blockchains
Sovereign Guarantee	Provided by Government	Not provided by governments
Legal Recognition	Can be mandated by legislation	Gives scope for ambiguity
Security	Highly Secure	Depends on the Blockchain and its development team
Turing completeness	Yes	Depends on the Blockchain. (Bitcoin is Turing Incomplete)
Trust	Trustless Network guaranteed by Sovereign Authority	Presumed Trustless Network not guaranteed by Sovereign Authority
Price Manipulation	Very Difficult, as Price is monitored by the Sovereign Authority and managed in effort to maintain Parity with Fiat currency	Can be easily speculated and manipulated by unscrupulous elements

A Fiat currency, by nature of being issued by Central Bank (which is a central authority), is essentially centralized. In fact, the need for uniformity, security and accountability implies that the notion of a national currency is a concept of Centralization by default.

Fiat currencies are sovereign guaranteed instruments i.e they are government backed. Unregulated crypto currencies on the other hand are peer-to-peer based currencies which have no sovereign involvement whatsoever (except regulation by certain nations).

The K-Y protocol envisages a centralized RSBC in which geographically distributed systems carryout 'mining' activities in order to generate new units of NationCoin.

As we have seen, the power of Blockchains is due to its decentralized nature. But by introducing Nationcoins we are centralizing the system. How do we now harness the power of decentralization by centralizing a system? Will the system not lose its strength by us doing the opposite of what the system is made for? Since RSBCs are cryptocurrencies which are floated by government (a central authority). How does one harness the advantages of a decentralized system in a centralized framework? This presents a unique paradox.

This inconsistency is labelled as The K-Y paradox. It is counter intuitive in that we are trying to centralize and take advantage of a system that, for all purposes, is defined by its decentralized nature.

A THOUGHT EXPERIMENT:

Envisage a system of Networks which functions efficiently due to its decentralized nature. But because of certain overarching reality demands, we need to centralize the network. But the decentralized nature of the network is its inherent strength. Nonetheless by centralizing (which is the exact opposite of decentralization) the network, how can we expect the (hitherto decentralized) network to function correctly and efficiently?

To resolve the K-Y paradox, we need to come up with a method in which a decentralized system like a cryptocurrency network functions efficiently in spite of introducing centralization through RSBCs.
If we observe the process of cryptocurrency formation (eg:- Bitcoin) we see the following-

A. All transactions in a particular time frame are bundled together.

B. These transactions are independently verified by each 'node'.

C. The nodes then solve a problem and give PoW (Proof-of-Work). In other cryptocoins like Peercoin, Proof-of-Stake (PoS) is given.

D. The network comes to 'know' (through data consensus mechanisms) that the node which gave POW and verified the transaction is a 'bonafide' one. This is realized through other nodes verifying solutions to PoW.

E. The block is made part of Blockchain and the node is rewarded cryptocoins (Bitcoins in this case).

In case of RSBCs the work of the network is done by a centralized authority, like the DAR.

The K-Y paradox can be addressed in the following manner. The steps 'A' and 'B' will be carried out by independent nodes in the network (preserving decentralization). In steps 'C' and 'D' the process of PoW or PoS is replaced by Proof-of-Sovereignty (PoSv)[3] where each node will, through a secret key inform the DAR (central authority) of its sovereign (i.e. Bonafide) nature. Step 'E', after assent by central authority will be completed by the nodes of the network.

CONCLUSION

We have observed that The K-Y Paradox defines a contradiction (seen in The K-Y Protocol) in which a system, whose inherent strength is its decentralized nature, is centralized. It appears as if the system will collapse due to this contradiction.

But we have also seen that a solution is possible where only steps which concern the Sovereign authority are centralized, thus conserving the efficiency of the system. This is done mainly through Proof-of-Sovereignty (PoSv).

REFERENCES

[1] Hegadekatti, Kartik and S G, Yatish, Roadmap for a Controlled Block Chain Architecture (August 13, 2016). Available at SSRN: https://ssrn.com/abstract=2822667.

[2] Hegadekatti, Kartik and S G, Yatish, The K-Y Protocol: The First Protocol for the Regulation of Crypto Currencies (E.g.-Bitcoin) (February 13, 2016). Available at SSRN: https://ssrn.com/abstract=2735267 or http://dx.doi.org/10.2139/ssrn.2735267

[3] Hegadekatti, Kartik and S G, Yatish, Proof-of-Sovereignty (PoSv) As a Method to Achieve Distributed Consensus in Crypto-Currency Networks (September 1, 2016). Available at SSRN: https://ssrn.com/abstract=2833194