Analysis of Contracts in Various Formats of Blockchain

Hegadekatti, Kartik

27 December 2016

ANALYSIS OF CONTRACTS IN VARIOUS FORMATS OF BLOCKCHAIN

Dr.Kartik H

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

ABSTRACT

One of the important features of Blockchain is that it allows the hosting and execution of contracts. Such a contract in the digital world is known as a Smart Contract.

But the process and consequences of a contract vary radically from one format of Blockchain to another. One of the formats (and the most common at present) is the Unregulated Blockchain (like Bitcoin and Ethereum) with no government supervision whatsoever.

Another format is the Controlled Blockchain which is managed and guaranteed by the Government. It is this difference that is vital in understanding the impacts and consequences of entering into and abiding by Smart Contracts.

Firstly, the concept of cryptocurrencies (also referred to as cryptocoins in this paper) is explained. Then the concept of Regulated and Sovereign Backed Cryptocurrencies (RSBCs) is discussed. Later on, I explain how contracts vary between the two Blockchain formats. Finally, the paper concludes as to how smart contracts can be best executed and on which format of Blockchain.

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 fees).

The cryptocoin network makes this 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.

Regulated and Sovereign Backed Cryptocurrencies (RSBC), on the other hand are government backed cryptocurrency akin to paper currency, but in digital form. It is based on 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.

In this system, the cryptocoins (known as NationCoins) are backed by Sovereign Guarantee. They are run on a highly secure Controlled BlockChain(CBC)[2] in which Sovereign backed Cryptocurrencies will be transacted without any hassles. NationCoins are completely managed by the Sovereign Authority i.e. the Government.

RSBCs are Government backed Cryptocurrencies which work on a Controlled Blockchain.

Bitcoin and Ether are non-backed cryptocurrencies that work on unregulated Blockchain.

Contracts are basically enforceable agreements. The fact that they are enforceable means that a third party is somehow

involved and that third party is usually the government, its representative or an authorized intermediate (Eg: - Banks).

In case of Bitcoin, banks (and other financial intermediaries) have no role in verifying transactions. Ethereum provides such a kind of a platform.

Smart contracts are computer protocols that facilitate, verify, or enforce the negotiation or performance of a contract, or that make a contractual clause unnecessary. Smart contracts among other things will usher in the Internet–Of–Things (IOT).

Many intermediaries (attorneys, will executors, banks, insurance agents etc) may be bypassed by smart contracts.

Smart Contracts are highly objective and provide very little room for any dispute. Even the Dispute Resolution Mechanism can be built into the contract. But a totally free smart contract system can (in certain situations) be manipulated or misused for private gains. Regulation in some way then becomes a necessity.

Bitcoin per se will not be able to execute smart contracts as it cannot operate sidechains [3]. Ethereum can and so do RSBCs.

RSBCs have the added advantages of-

(1) Sovereign guaranteed “Double Verification” where the trust worthiness of parties in a contract is verified by government simply by the fact that they are part of the Controlled Block Chain and also because their wallets will be pre-verified by the government.

(2) Non – speculative nature of RSBC. RSBCs will have value more stable than Ether or other crypto currencies, as RSBC value will be managed by Sovereign Authority.

(3) More safe and secure transactions and contracts as they will all take place on RSBC platform.

(4) Traceability of parties in case of dispute or fraud.

(5) No fear of illegal contracts being transacted or money laundering, as it will be an RSBC platform.

(6) It is possible to deal with Sovereign Currencies on the Controlled Blockchain. Because of this, Smart contracts can be more inclusive as even the most downtrodden in society can participate in economic activities and add value to society.

Thus, RSBCs have every feature of Bitcoin/Ethereum sans the disadvantages. RSBC based Smart Contracts (on Controlled Blockchain) provide the safety and security that Ether or Bitcoin cannot provide and that feature is mainly because of the Sovereign backing that RSBCs will have.

CONCLUSION

We have seen that the two major formats of Blockchains have different features when it comes to Smart contract execution. Nevertheless, unregulated blockchains have gained prominence and popularity because of the innovative and novel nature of Blockchain Technology.

But such unregulated cryptocurrencies are controlled by a few who do not have the public mandate. When people invest in such ventures, they are risking their life's savings.

Hence to make Smart Contracts more inclusive and attractive to the public, we need to introduce Controlled Blockchains in a big way. This will bridge the trust deficit inherent in new technologies. People will begin to trust blockchains. Blockchain utilities will improve and hence a shift to a completely digital economy covering all aspects (taxation, loan, voting, Contracting etc.) can be made.

REFERENCES

[1] 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

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

[3] Enabling Blockchain Innovations with Pegged Sidechains Adam Back, Matt Corallo, Luke Dashjr, Mark Friedenbach, Gregory Maxwell, Andrew Miller, Andrew Poelstra, Jorge Timón, and Pieter Wuille.2014-10-22 (commit 5620e43)