Roadmap for a Controlled Block Chain architecture

Hegadekatti, Kartik and S G, Yatish

13 August 2016

Roadmap for a Controlled Block Chain architecture

Dr.Kartik H & Dr.Yatish S.G

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

Abstract- the K-Y Protocol envisages the introduction of RSBCs (Regulated and Sovereign Backed Cryptocurrencies). In this paper we discuss in detail the establishment of a Controlled Block Chain based on the K-Y Protocol. It is primarily accomplished using the NationCoin system. There are two aspects to the NationCoin system. The software and the hardware aspect. The software necessary to write and run the Block Chain on the hardware is envisaged. The hardware needed to run and sustain the blockchain is then deliberated. A host of institutions have also been envisioned to create, support and run the NationCoin system. The DAR will be the main institution responsible for creating the Controlled Block Chain architecture. The costing, timeline and the interplay of institutions are also outlined.

INTRODUCTION

The earliest Central Banks were created to manage assets and provide loans to a nation's government. In the digital age, we will need institutions similar to Central Banks with a mandate to manage a nation's digital assets. For this express purpose, we have envisaged the creation and development of a Digital Asset Reserve-A DAR. The DAR is part of a larger 'Protocol'- The K-Y Protocol [1]. A short explanation of terminologies is given.

RSBC- Regulated and Sovereign Backed Cryptocurrency- government backed cryptocurrency akin to paper currency, but in digital form.

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 any hassles. It will be a Controlled Block Chain [1].

(A Controlled Block chain is different from a Block Chain per se. A Block Chain is a permissionless Distributed Database, whereas a Controlled Block Chain will be Permission Based. The Permission for access and operation, being provided by the Sovereign Authority.)

A Controlled Block Chain (hereby referred to as CBC) resulting from the K-Y Protocol has several money and non-money uses. In its complete form, it will have a wide spectrum of applications ranging from banking, taxation, and contracting to space research, automation and public services.

Block Chain- A blockchain is a public ledger of all cryptocurrency transactions that have ever been executed. 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.

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

DATA: it is the technical arm of the DAR. Its functions consist of setting up of the hardware and software infrastructure required to run and sustain the RSBC. It will set up the nodes, hard-code the K-Y Protocol into software, and setup the computing network. It will Manage and maintain the various IT infrastructure needed for RSBCs.

DAREC: It is the Digital Asset Regulatory and Exchange Commission. A subsidiary of DAR which will manage overseas transactions involving many NationCoins-for e.g. - converting JapanCoins to IndiaCoin etc. DAREC will act as a regulator between RSBCs and other international RSBCs of other nations. DAREC will carry out the policies and decisions of DAR with respect to RSBCs and other digital assets. On the directions

of the DAR, DAREC will also regulate non-RSBC digital assets and their exchanges wherever necessary.

NLD-National Ledger Database- The custodian of the Controlled Block Chain. It is the ledger which will record all transactions that involve the respective NationCoins and other digital assets.

To make the coinage system more accurate and organized, Mints were created. Simply put, Mints are facilities which manufacture coins in a standardised procedure. After coming out of a mint, coins can be used as currencies.

Emperors commissioned Mints and put a person in charge of it. The person in-charge was usually a very trusted and loyal servant to the emperor. To Mint more coins and also propagate their usage to the far reaches of the kingdoms, branches were opened in several far flung cities, away from the capital.

Now if a coin is overweight or underweight, how do you tell which Mint it came from?

Moreover, how do you fix responsibility if a corrupt official puts less precious metal in the coin than necessary?

To pinpoint such problems and solve them, Mint marks were introduced.

Mint marks were security and indicative features which made Mints accountable. Usually the Mint *mark* was an inscription which indicated where the coin (or currency note) was produced. The existence of Mint marks provided accountability and made counterfeiting difficult as also easily detectable.

Apart from the weight issue, inscriptions on coins tried to eliminate the Counterfeiting problems.
Counterfeiting of money leads to inflation, erosion of value and loss of trust in the government.

In spite of inscriptions, people continued to fake coins. When this happened, Mints would abandon a particular design and create a new design for inscription.

In the 1860s USA was emerging from the throes of a devastating civil war. It was estimated that close to half USA's currency was counterfeit.

It is clear that the responsibility of the Mint is to provide security features for the currency that makes it difficult to counterfeit. Added to this, Mints also ensure accountability and fix responsibility.
It is because of the Mint that a government knows exactly how many coins and notes are circulating in the economy.

As we enter the age of digital economy we need something akin to the Mint that produces secure, reliable and authentic RSB crypto currencies. We need an institution like the Mint, which standardizes digital coinage. For this purpose, DATA has been envisaged. DATA is short for Digital Assets, Tracking and Administration.

DATA will be the Mint of the new digital economy. It will setup hardware and software systems, gain expertise, train personnel, provide cyber security and make detailed technical specifications to make the digital economy possible.

DATA will play a vital role under DAR to bring the K-Y protocol into practice. The DATA is the technical organization that will keep the RSBC up and running. It will technically initiate, maintain and sustain the RSBC and thus the entire digital economy that will be based on RSBCs.

The NationCoin System and The RSBC Code

Man uses language to speak to man. Whereas computers use the Binary system. Basically, a computer converts all expressions into binaries i.e. sets of 1s and 0s. For example "Hi" is represented as 01001000 01101001 (as per ASCII specifications) [2].

A computer has a huge working memory (what we call RAM-Random Access Memory). This huge memory base and computational power is what makes a computer superfast. It can process large amounts of information in a very short time.

Programmers write a program in a language that the computer can understand. Based on that program the computer executes a function that it is asked to execute. To make Bitcoin possible programmers wrote the Bitcoin protocol. The Bitcoin protocol is nothing but a set of instructions and rules in the computer's own language telling it what functions to execute. It is written in a manner that the computer understands. Using the program, the computer talks to other computers on the network and implements the orders that are given to them. It will function in such a way that the rules of the protocol are followed.

Ethereum, the entity that uses ethers as cryptocurrency units runs on Solidity, a computer program used to run smart contracts on ethereum. The Bitcoin Protocol and Solidity were written using a combination of computer languages like C++, Java, Python etc. These languages are used to write the cryptocurrency codes i.e. Bitcoin Protocol or Solidity.

We have envisaged a set of rules and instructions that will form the RSBC code. RSBC code is a generic term that we use to refer to any code that is related to any Regulated and Sovereign Backed Cryptocurrency. A NationCoin System is another term that we use to refer to both the hardware and software aspect of the RSBC.As such, RSBC code is a part of the NationCoin System.

One such RSBC code is MANU- Main frames And Networks Unifier- which will be the main and central software that will make RSBCs a reality. MANU basically denotes the cache of regulations that computer networks should follow so as to make RSBC practical. It will do the work of integrating the network and the hardware into a single entity so as to run the K-Y Protocol. DATA will be in-charge of establishing the whole setup.

We can use Mainframe computers and closed user interface networks connecting the Mainframes. These Mainframes will be integrated and will work in sync over the closed network. They will have a secure user-interface. The Mainframes will have MANU as the RSBC code which will allow them to execute the K-Y Protocol. MANU will be written by certified programmers who will also hard code the K-Y protocol into MANU.

RSBC Hardware–To set up MANU and execute the K-Y protocol we will need a set of hardware. This hardware will be a semi-closed system which will have MANU hard-coded into it by certified programmers. We can choose from a range of hardware options. But we must go for only those which will give us an optimum yield.
There are several kinds of computing systems. We shall now discuss them in detail.

Supercomputers can work out problems whose main restraint is calculation speed. For example, predicting weather. Weather is influenced by a large number of factors like humidity, air pressure, temperature, cloud cover etc.

A supercomputer will take inputs from its memory banks about weather and give an output which can be a fairly accurate prediction of the weather over the next 24 hours. Climate modelling is also done in a similar manner.

Super computers are ideal for performing complex calculation on a large amount of data stored in memory caches that run into several terabytes.

On the other hand Mainframe Computers are used to execute functions that are repetitive or of the same nature.

For example, handling 10,000 business transactions a second. Mainframes, rather than taking inputs from memory banks, take inputs from external sources like credit card company website. Mainframes basically deal with problems which are restrained by input/output quantities.

A Mainframe computer processes this data and in a fraction of a second, verifies the transaction and clears the bill. Moreover, Mainframes have reliability. They double check and verify data. This is very important in situations where data integrity is paramount. For example, in commercial or large business transactions.

In short, supercomputers have a range of areas where they can be used. In case of supercomputers, data precision is difficult to verify as the events have not yet occurred. For instance, climate modelling done by supercomputers is difficult to verify as the changes will not yet have occurred. Scientists use supercomputers to predict and model financial markets, military scenarios and climates which are still in the future.

On the other hand, Mainframes are used where high precision and data verification is needed. For example, let us examine a payment system. The payment system's Mainframe computer verifies that it is indeed you and that your account has the money that you desire to spend.
It will do this process many times over, so that every time it gets the same answer i.e.
(1) It is you only who has accessed the account and
(2) Your account has to have the money that you desire to spend.
This greatly increases reliability of the authentication process. All this happens in a fraction of a second for several thousand transactions in that single second.
Mainframes are thus used for reliable task completion.

MAINFRAMES	**SUPERCOMPUTERS**
1. Many simultaneous users are supported.	1. They are actually a grid or cluster of small computers functioning collectively on a particular problem they are instructed to solve. Usually single user at a given time.

2. Can operate on several different kinds of operating systems (z/OS, Linux, etc.).	2. Usually operate on a version of Linux as the operating system.
3. Can run Continuously for years-on-end	3. Have periods of Peak performance which can vary over time.
4. Operate multiple programs simultaneously.	4. Concentrate computing ability to run a small number of commands or programs as rapidly as possible. Devoted to accomplish high speed and augmented performance.
5. Are sufficiently adaptable so as to execute wide varieties of applications and accomplish diverse commercial workload.	5. Have specific objectives like scientific modelling or research. Are normally run at maximum power, positioning the computer's full processing capacity toward cracking a specific problem.
6. Operation speed is determined in Millions of Instructions per Second (MIPS).	6. Operation speed is gauged in Floating Point Operations per Second (FLOPS).
7. Can run on previous versions of software. Can be easily upgraded. They are thus backward compatible.	7. They push the limits of software and hardware technology. They have many novel and innovative features that augment their capacity.
8. Carry out tasks on vast quantities of external data.	8. Run complex computations utilising a huge internal memory

One may think that cloud storage and computation may be a possible alternative to either mainframes or supercomputers. The cloud is a remarkable technology. It is the practice of working a network of remote servers hosted on the Internet. It is used to process, manage, and store data, compared to a local server or computer. Ability to work on the data is limited only by one's ability to access the internet. Let us now analyse Mainframes vis-a-vis the Cloud systems.

Mainframe vis-a-vis the Cloud

- One advantage that big businesses enjoy with respect to Mainframe computers is full control over their own data. With Mainframes, one need not worry about anyone fiddling with their data. Mainframes can be easily customized more than cloud services possibly can. This is because the hardware is in control of the user himself. Mainframe computers do not take up much of the internet bandwidth. This is a great value addition as it lessens bandwidth usage and permits operation even when the internet is down.
- When using cloud services, you are assuming that a 3rd party won't tinker with your data.
- One main problem with cloud computing is its dependence on a strong and fast internet connection. It is preferable that the connection will hopefully not go down. In such situations a Mainframe becomes necessary.

If we analyse the needs of the job at hand, it is evident that Mainframe computers are the systems that we should go for.
The job (to be done by DAR) involves assets, transactions, authentication etc. which a Mainframe computer is in fact built to work with. But for the magnitude of the work involved, we need not one, but several Mainframe computers.

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 work on a particular proof-of-work [3] for the said block.
d) When a node finds the solution to a proof-of-work, 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.
Bitcoin runs on 5226 nodes distributed throughout the globe [4]. Ethereum runs on 7489 full nodes [5]. Since the K-Y protocol has the sovereign authority as the Trusted Third Party, lesser number of nodes will be needed. Moreover the multi-tiered security structure and the closed nature of MANU eliminate the need for a large number of nodes.

Nevertheless, the K-Y protocol is designed to deal not just with currencies but with digital assets as a whole. As such, we need to keep in mind the large (virtual) infrastructure that we may need when the DAR expands its activities in various spheres where digital assets are involved.

About 10,000 high capacity nodes for a $2 trillion economy can be comfortably managed by a group of custom-built powerful Mainframe computers (which will run on MANU).

These 10,000 nodes can be distributed over a considerable geographic area depending on the size of that country's economy.
We have to realize that the way the Mainframes are connected to each other is also important. In this, there are two types.
One type of arrangement is known as Grid Computing the other type is known as Cluster Computing.

Grid computing is, simply put, a collection of computer power from many systems to complete a common task. The computers involved, at the same time will also be working on other problems.

On the other hand, Cluster computing consists of a set of computers that perform the same task and that task alone. In many respects, computers working in a cluster can be considered to be a single system.

We assess that each country can have a node set up in its provincial capital. Say, a country has 30 provinces. It can set up 30 main nodes. One main node in each province.
But how do we accommodate 10,000 nodes? Let us analyse.
Each main node will have a number of machines which will act in the form of a cluster. i.e. the entire RSBC network will be a Grid of Clustered Mainframes.

Each (of the 30) main node will have 4 powerful Mainframe computers. Each Mainframe computer will have 100 virtual machines inside the Mainframe.

(Virtual machines are nothing but a Mainframe running several different instances of operating systems at the same time. This allows the system to be managed as if they were physically distinct computers).

30 main cluster nodes, with 4 Mainframes in each main cluster node and each Mainframe running 100 virtual machines running on MANU in Grid Clustered format allows us to operate a total of 30x4x100=12,000 high capacity nodes; more than sufficient for any future expansion and development of the digital economy.

MF-Main Frames

Each of the 30 main nodes will be a cluster of 4 Mainframes each or 400 virtual machines.

A Mainframe has many advantages over distributed computing. Using distributed computing with individual computers for RSBCs like Bitcoin is one more option. But it too has many drawbacks.
Mainframes need less manpower than individual distributed computers. Moreover, economies of scale reduce the cost of Mainframes over a medium time period. It is easier to manage, takes lesser space, power and also cost comparatively less.

Mainframes can be customized and are also easy to maintain. To execute the K-Y Protocol, a $2 trillion economy will need around 120 Mainframes. This may cost close to $100 million. Staffing may cost another $10 million.
We should be Adding to it $100 million in cabling costs and $250 million to write MANU (on which the network will run) and other costs. This comes to around $500 million investment for a $2 Trillion economy.

That is about 0.025% of the entire economy. It means that for every $100 in any economy, only 2.5 cents need to be invested in setting up the NationCoin network. This appears to be a very reasonable cost. Annual maintenance cost may be around $200 million. This implies that once a capital investment is done, there is substantially lesser investment per year on maintenance.

DATA will maintain 2 ledgers. One will be a public transaction ledger with the NLD. The other will be a more secure Reserve ledger which will have a constantly updated register of mining, holding, backing, and sovereign stamping etc. i.e. everything related to the DAR ledger.

20% of the nodes will be maintaining the Reserve Ledger. Unlike the public transaction ledger, the reserve ledger will be directly controlled by the DAR (and not the NLD). These 20% nodes will be as widely dispersed as possible. Every 3 months, the nominated nodes running the reserve ledger will change by a process called Randomized Periodicity. By a system of randomizations, nodes are nominated every three months which will run a copy of the reserve ledger. No node can run the reserve ledger for a period of more than 2 quarters.

DATA will have several functions that will make it a very important technological institution.

(1)Writing MANU

DATA will ensure that MANU is fully written, trial tested and ready to work before the NationCoin System goes online.

As already discussed, MANU-Mainframes and Networks Unifier is the Software on which the entire NationCoin system will run. MANU will be written using a combination of languages like C++, Java, and Python. MANU will have several redundancy features built-in which will make it fail-safe and as reliable a system as possible.

(2) Setting up the Mainframes network

DATA will select the places where nodes will be established. It will choose from the Mainframes that will be best suited to run the NationCoin system on MANU. DATA will ensure that there is network

compatibility and also the grid clustered Mainframes are optimally connected.

(3)DATA will write the code for the Reserve Ledger.
This is of utmost importance as it is the basis of creation of the NationCoin itself. DATA will ensure that maximum cyber security is provided to the entire system, especially the reserve in particular. This is necessary to maintain integrity of the NationCoin system.

(4)DATA will develop and maintain "Digital Forex Vaults" (DFV) on behalf of the DAR.
DFVs are very important for handling international NationCoins that enter the country. For example, Indian DATA will manage DFV in which USCoin, Eurocoin, JapanCoin etc will be handled.
This is necessary to maintain a credible and a stable exchange rate.

(5)DATA will help the banks to make their systems compatible with MANU so as to run the NationCoin system.

(6)DATA will create and maintain clients' Nationcoin wallet. A client can be a single citizen, company, trust, organization etc.

(7)DATA will audit companies' and organizations' on invitation.
Computer network and systems and give accreditation and certification. Those who receive DATA accreditation will be able to interact and conduct transactions seamlessly over the Nationcoin network. This is important for security purposes and also developing DATA as an international brand.

(8)DATA will develop skill and expertise in block chain technology.
It will conduct research and development activities on both hardware and software aspects of block chain.
Due to the volatile and confusing nature of stock market dealings, the state came up with laws to regulate stock markets and protect public from securities or stock market fraud. Basically stock exchanges are places where stock traders, holders and brokers can sell and/or buy shares, bonds and various securities (a tradable financial asset)

Over a period of time governments set up institutions and organizations which could control, monitor and supervise securities trade. For example, USA has the US-SEC. India has SEBI, Europe has ESMA, Japan has SESC, China has CSRC and so on.

DAREC–The Digital Assets Regulations and Exchange Commission will be a type of a financial regulatory authority dealing exclusively with international digital assets.
DAREC will be the organization that will deal with the inter-relationships and dynamics of various digital assets in the digital economy.
DAREC's mandate will start to kick in once linkage[1] starts to occur. (Linkage in this case means that the NationCoin is allowed to be freely traded in the international market.)

As such, DAREC will be fully under the DAR. It will handle only those aspects where one NationCoin needs to be converted to another. It will also play an important role when a digital asset is being traded across borders, from one country to another. It will be the interface that will securely link NationCoin system of one country to another.

The DAREC will keep track of (but not control) the digital forex vaults.
Its primary mandate will be to assist DAR in its overseas operations and protect NationCoin by maintaining credible exchange rate.
It will be the overseas, or international interface arm of the DAR.
The DAREC will also, through the block chain regulate digital assets markets where a nations digital assets are traded overseas.

For example, Joe in the USA wants to obtain loan by mortgaging his home. The dealing will be handled no doubt by the US-NLD. But if Joe is availing a loan from Kate, who is in London, then the US-DAREC comes into the picture.

It will ascertain that BritishCoins to USCoins conversion takes place smoothly. This way, only USCoins will keep circulating in the US economy. In the absence of exchange integrity, any economy will

become a hodgepodge of several currencies. The above action will also ensure that ownership of US Digital assets and BritishCoins is not abused by unscrupulous elements for anti-social activities.

The main objective of DAREC is to protect citizens' money, maintain a free and fair environment in the NationCoin market. DAREC will also efficiently control NationCoin exchange market so as to ensure that there are no irregularities of any kind. DAREC will also provide NationCoin trade related information to the traders and citizens.
The DAREC will assist the DAR in the formation of capital. It will do this by supervising cross border trade in NationCoins and digital assets.

Conclusion

We have proposed the establishment of a Controlled Block Chain based on the K-Y Protocol. 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 part consists of writing the RSBC code. RSBC code is a generic term that we use to refer to any code related to any Regulated and Sovereign Backed Cryptocurrency (RSBC). One such RSBC code is MANU- Main frames And Networks Unifier. MANU will be the programmed cache of instructions that computer networks will follow to make RSBC practical. It shall integrate the network and the hardware into a single entity to run the K-Y Protocol. The hardware aspect consists of setting up a cluster of mainframes which will run virtual machines as nodes. These nodes will do the work of verifying and confirming transactions. They will be connected to each other and run MANU on their systems, broadcasting, verifying, and confirming transactions with a particular difficulty level. A host of institutions have also been envisaged to create, support and run the NationCoin system.

References

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

[2] http://www.unit-conversion.info/texttools/convert-text-to-binary/

[3]Bitcoin: A Peer-to-Peer Electronic Cash System-Satoshi Nakamoto

[4]https://bitnodes.21.co/ ;Retrieved 12 august 2016

[5]https://www.ethernodes.org/network/1 ; Retrieved 12 august 2016