# Generation, Security and Distribution of NationCoins by a Sovereign Authority

Hegadekatti, Kartik and S G, Yatish

21 December 2016

# GENERATION, SECURITY AND DISTRIBUTION OF NATIONCOINS BY A SOVEREIGN AUTHORITY

**Dr.Kartik H & Dr.Yatish S.G**

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

## ABSTRACT

NationCoins are cryptocurrencies backed by Sovereign Authority (Simply put, they are Government issued Bitcoin-like cryptocurrencies). In this paper, we explain the generation, security and distribution of NationCoins by a Sovereign Authority. We begin by explaining the concept of cryptocurrencies (also referred to as cryptocoins in this paper). We then discuss the concept of Regulated and Sovereign Backed Cryptocurrencies (RSBCs). Then we envision a scenario where cryptocoins are a main medium of exchange in an economy. The generation, security and distribution of NationCoins by a Sovereign Authority are deliberated. Finally, the paper concludes by outlining the functions of the Sovereign Authority vis-a-vis NationCoins.

## 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), are government backed cryptocurrency akin to paper currency, but in digital form. In the RSBC system, the cryptocoins (known as NationCoins) are backed by Sovereign Guarantee.

They are run on a highly secure Controlled BlockChain(CBC) in which Sovereign backed Cryptocurrencies will be transacted without any hassles.

A Controlled BlockChain is different from a BlockChain per se. A BlockChain is a permissionless Distributed Database, whereas a Controlled BlockChain will be Permission Based. The Permission here, being provided by the Sovereign Authority. NationCoins will thus be completely managed by the Sovereign Authority i.e. the Government.

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].

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 BlockChain in which Sovereign backed Cryptocurrencies will be transacted without any hassles. It will be a Controlled BlockChain.

(A Controlled BlockChain is different from a BlockChain per se. A BlockChain is a permissionless Distributed Database, whereas a Controlled BlockChain will be

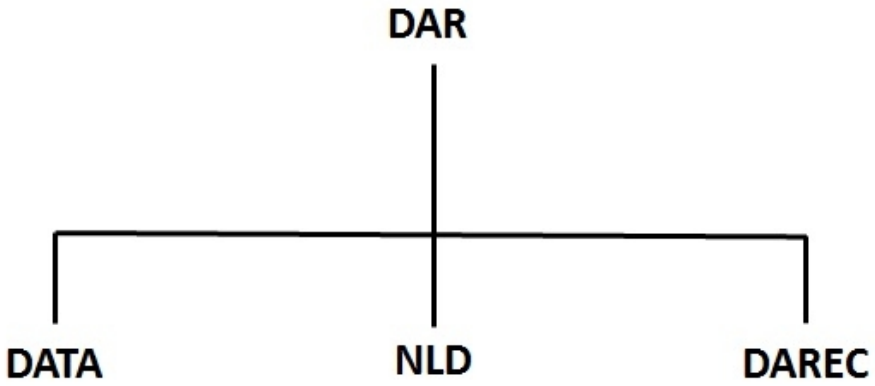
Permission Based. The Permission for access and operation, being provided by the Sovereign Authority.)

A Controlled BlockChain (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.

BlockChain- 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.

The Digital Assets Reserve will consist of the following organisational structure:




The DAR will have 3 departments directly under it. The departments will have following functions.

**DATA:**

It is the technical department of the DAR. DATA is short for DIGITAL ASSETS TRACKING & ADMINISTRATION. It will be the technical wing of DAR and Its functions comprise setting up of the hardware and software infrastructure to run and sustain the RSBCs. It will set up the nodes, Hard-code the K-Y Protocol into software, and setup the distributed computing network. It will Manage and keep the various IT infrastructure needed for RSBCs.

**NLD**: It is the National Ledger Database. It is the ledger which will record all transactions that involve the respective NationCoins. Its copy is present in all the nodes. Every NationCoin, after sovereign stamping and certification will pass through the NLD where it will be

registered. The NLD will keep an updated account of NationCoins in existence.

If loss or other emergencies occur, it will, with DATA's help and DAR's concurrences liquidate certain NationCoins and remove them from circulation (Akin to destroying old and torn currency notes).

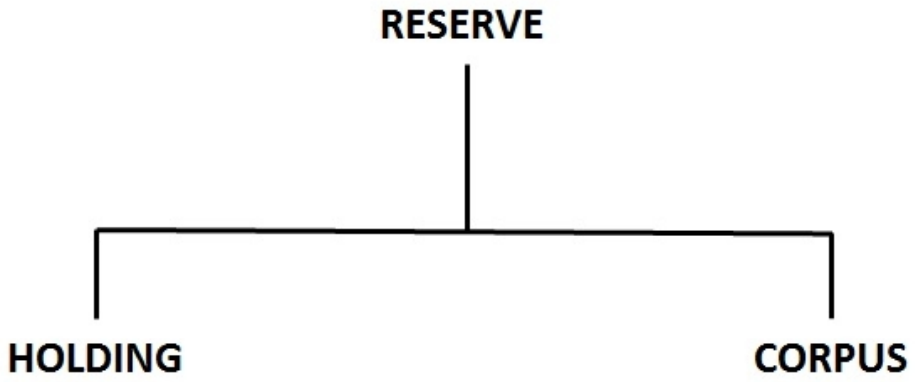
The NLD will also act as a ledger to record other digital assets which have non-currency applications. I.e. non-RSBC digital assets like certificates, receipts, land records, etc.

**DAREC**:

It is the Digital Asset Regulatory and Exchange Commission. When RSBCs increase in quantity and scope, 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 about RSBCs and other digital assets. On the directions of DAR, DAREC will also regulate non-RSBC digital assets and their exchanges wherever necessary.

The DAR, in actuality contains the reserve. In fact, it is THE RESERVE itself. What is under the DAR (NLD, DAREC, and DATA) is demarcated from what is within the DAR. The DAR will contain THE RESERVE, the one entity that gives RSBCs their identity. The reserve will

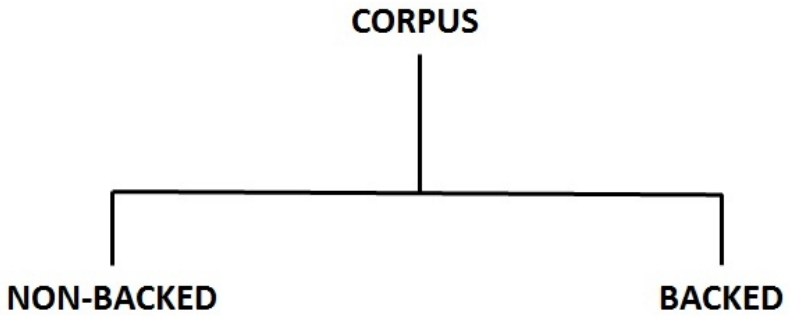
provide the Sovereign Stamping and Certification that will give RSBCs the sovereign backing. The reserve will consist of two parts.




Holding will consist of freshly mined RSBCs which have not yet been Sovereign Stamped. The corpus (physical assets) will contain the money that will provide the freshly mined cryptocurrencies their sovereign backing. For ease of operations and record keeping, the corpus is divided into two parts.

**Non-Backed Corpus**: comprises those physical assets which have not yet provided any backing to any NationCoin.

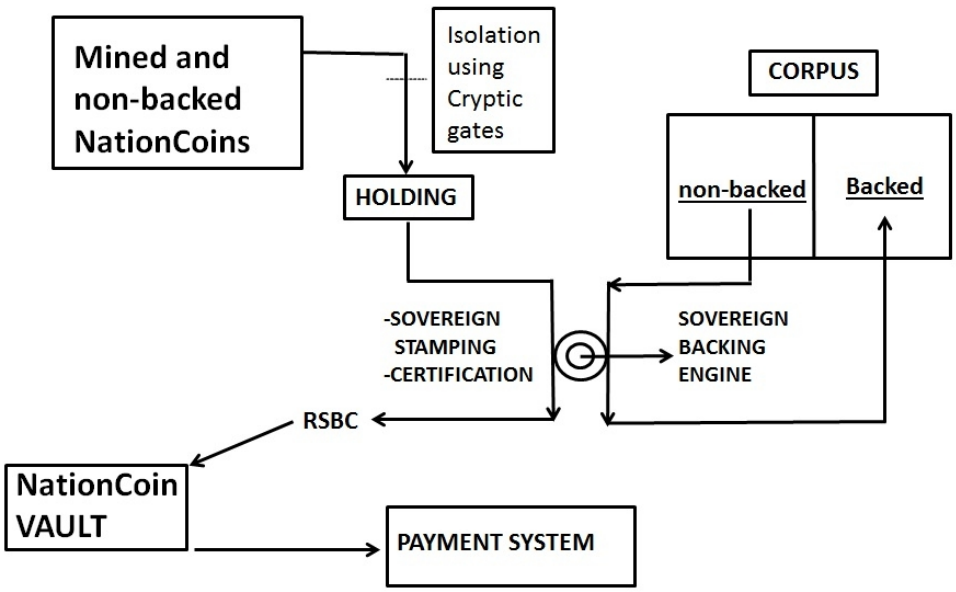
**Backed Corpus**: It will consist of those physical assets which have already provided backing to the NationCoin.




Non-backed NationCoins will be in Holding. It's the only outlet is into the SBE: Sovereign Backing Engine, which will inscribe the sovereign stamp and give certification. SBE is the entity which will provide security features and authentication to the cryptocurrency.

After getting mined, the non-backed NationCoins will be stored in to a system not connected to the internet i.e. it is offline. It is within this isolated system that NationCoins will get sovereign backing.

The backed corpus will have guarded safe containing physical assets that have backed the NationCoins. The only way they can be released outside is, when the backed Nationcoins are destroyed i.e. if $1,000 worth of USCoins is destroyed, then, $1,000 from the Backed Corpus is released into the economy after confirmation.




Backing can be done in several ways. Say $100 million worth of USCoins are to be backed. Now a Hundred Million $1 bills are taken and their serial numbers are hard-coded into every USCoin. That means 100 million USCoins, each bearing a unique serial number corresponding to the serial numbers on the Dollar bills are created. These 100 million $1 notes will go into the backed corpus to be stored away safely. Now, these 100 million USCoins will enter the economy instead of 100 million $1 bills.

## Sovereign Stamping & Certification

In Certification, a unique item, unique to that country is coded into the NationCoin. For the USA it can be "E pluribus Unum". For India- "Satyameva Jayate" etc. These will ascertain the nationality of a particular NationCoin. It will have a hashed 64 digit version of the

country's unique national motto with an added number. Every one million NationCoins generated will contain the same hash number. This hash number will be maintained in the NLD Index registry. In future, to check the validity of a NationCoin, this hash number is searched in the index. If it matches, that means it belongs to that particular batch of NationCoins.

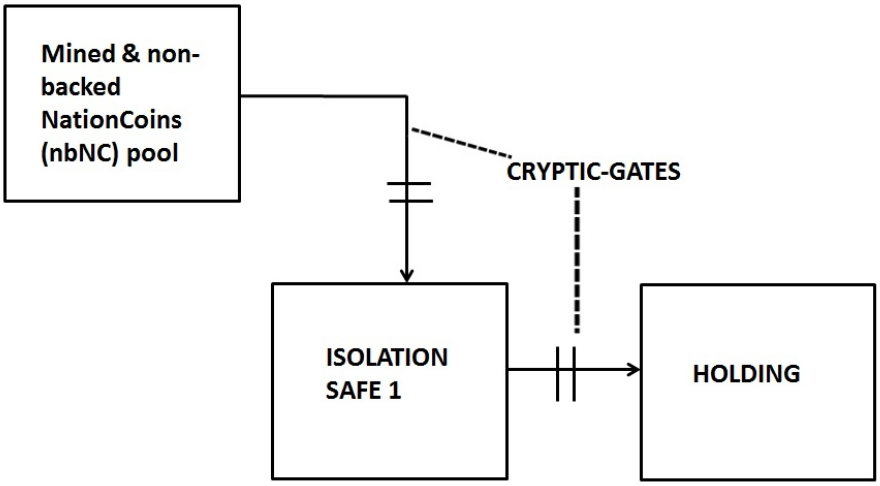
***Sovereign Stamping***- Sovereign stamping will give a unique Sovereign number to every NationCoin. Unlike Certificate number- which is common to NationCoins of a particular batch, sovereign number is unique for each NationCoin. Along with NationCoin number (like serial number on a currency note), Sovereign Number (given by sovereign stamping) and Certificate Number (given by certification) will provide added tiers of security to the NationCoin.

**Backing-**Backing occurs when physical assets in non-backed corpus are moved into the backed corpus in an accountable manner. If $10 million moves from non-backed to backed sections, then $10 million worth of NationCoins should be added to the RSBC vault.

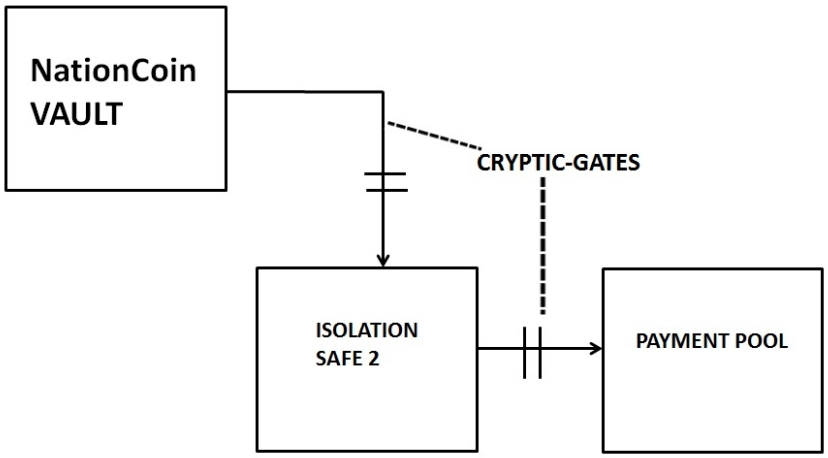
**RSBC Vault:** This is a safe area where non-backed NationCoins, after **Backing** arrive as RSBCs. It is offline and not connected to the network.

Right from Holding to RSBC vault, the entire reserve system is isolated by using Cryptic Gate technology.

**Cryptic Gates**: They are isolation mechanisms which keep the reserve offline to improve its security and protect it from external tampering.




It follows a simple mechanism. When nbNC (non-backed NationCoin) pool is connected to ISOLATION SAFE, the isolation safe is cut-off from Holding. When isolation safe is connected to Holding, it is cut-off from nbNC pool. It is an either-or relation i.e. ISOLATION SAFE can at any given time be only connected to one other unit- either Holding or nbNC pool.




A similar thing happens at the other end where RSBCs are created. RSBCs after creation go to the NationCoin vault. We may have to use multi-tiered Cryptic Gates with 2 or even 3 isolation pools between RSBC vault and payment pool. These RSBCs will go into the *Isolation Pool* 2 guarded by cryptic gates. [Since RSBCs are ready-to-use currencies, we need added security features]. The Isolation Pool 2 at any given time is connected to only one unit- Either to RSBC vault or the payment pool.

The DAR will have the following functions related to NationCoins.

**1) Sovereign Backing**: This is the core and the only main role of the DAR. All other functions of DAR and its departments are submissive to this function.

The DAR will provide sovereign backing through sovereign stamping and certification process. It will

keep the Corpus with correct account of non-backed and backed assets in the corpus. It will make sure that Sovereign Backing of NationCoins happens in a secure environment in a non-inflationary way. (If, after sovereign backing, backed corpus assets are released into the economy, it will cause inflation due to increased money supply in society). The DAR will have physical, high security vaults with restricted access and multiple checks and balances.

**2) RSBC Destruction**: As a corollary to the first (and main) function, DAR will also be responsible to verify authenticity of NationCoins already in circulation in the economy. If there are counterfeited, fake or tampered NationCoins, the DAR will seize them. After examining and investigating the NationCoin(s) in question, the DAR can destroy the said NationCoin(s). It will then decide to reintroduce a batch of fresh RSBCs instead of the ones already destroyed.

**3) Distribution** - Once generated securely in the above mentioned mechanism, The DAR will distribute the NationCOins as per the K-Y Protocol.

This is akin to a Central Bank detecting and weeding out counterfeit or damaged currency notes from circulation.

## CONCLUSION

The NationCoin system is based on multi-tiered steps which enhance security and ensure steady production of NationCoins. These NationCoins have several money and non-money uses. The system has enough built-in features to ensure reliable and safe system for transaction of RSBCs. The totally new innovations such as Cryptic-gates make sure that the NationCoin system is highly tamper-proof and accountable. The methodology outlined in the paper make it possible for the Sovereign Authority to introduce Digital Currency into the economy. Not only that, the Sovereign Authority is assured of a steady supply of NationCoins to transition to a fully digital economy over a period of time.

## 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 or http://dx.doi.org/10.2139/ssrn.2735267