The K-Y Protocol: The First Protocol for the Regulation of Crypto Currencies (E.g.-Bitcoin)

Hegadekatti, Kartik and S G, Yatish

23 February 2016

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

Dr.Kartik H & Dr.Yatish S.G

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

Abstract- Crypto currencies like Bitcoin are gaining prominence as a medium of exchange. They have several benefits like very low transaction cost, fungibility etc. But Crypto currencies are also identified with their use in crimes, illegal activities and speculation. Part of the reason for their prominence as well as notoriety is the fact that they have no Sovereign Backing whatsoever and also because they are decentralized. To make Crypto currencies acceptable by the people and also curb their misuse, the authors have proposed a protocol containing a set of standards and procedures. By using this procedure, any nation can create its own Sovereign Backed crypto currency called NationCoin. A commission will be established which will hold a certain quantum of money loaned by the Government. This loaned money will provide the Sovereign backing to the Crypto Currency. A Controlled Block Chain Protocol is used. The Genesis Block of several NationCoins is then provided to the banks in the country to use them for interbank settlements. These Interbank transactions will lead to the mining (generation) of additional NationCoins by the commission which will hold it without releasing it to the public. Once there are sufficient numbers of NationCoins so as to be equal to the loaned amount unit-for-unit, it shall be released to the public for use.

INTRODUCTION

A Crypto currency is storage of some value and a medium of exchange. It uses cryptographic techniques to protect transactions and also manage the generation of money.

Crypto currencies are decentralized, meaning that it is outside the control of central banks. Crypto currencies also have a decentralized ledger system which makes it possible to verify and confirm transactions over the entire network. It also makes possible for each unit of crypto currency to be tracked right from creation to the most recent transaction. They are outside the control of central Banks, and are explicitly NOT RECOGNISED. As such, they are outside the ambit of regulation. The absence of regulation no doubt makes the system free from the supervision of Governments and appears to give more freedom and rights to the people using Crypto currencies. The privacy, anonymity and personal space appear to be "enhanced" in the absence of regulation. But since they are unregulated, Crypto currencies have been misused for money laundering and criminal activities by various anti-social elements. The personal freedom and rights that were "enhanced" due to the absence of

regulation will be usurped by powerful antisocial elements that do not respect any law or have any ethical considerations.

To protect people's rights and also optimize economic activity, it is necessary to regulate Crypto currencies. But we need to do it in a way that it eliminates all (or a majority) of the shortcomings of Crypto currencies. At the same time we need to enhance its benefits. People tend to think of decentralization as an inherent, inseparable character of Crypto currencies. They are led to believe that the Crypto currency concept will fail if regulation and sovereign backing is introduced. But debates around Crypto currencies tend to discount the fact that it is possible and feasible to regulate Crypto currencies.

Bitcoin is the first and most famous Crypto currency. It has recently gained widespread usage. But it is not regulated or backed by any sovereign authority and is thus susceptible to misuse.

Advantages of a Regulated and Sovereign Backed (RSB) Crypto currency-

1) Minimal or no transaction cost to the public- The people can use the RSB Crypto currency without any trepidation as it will be guaranteed by the Government. Nil transaction cost is the basic feature of a crypto currency. Lack of transaction cost will allow seamless and unhindered exchange of money leading to increased economic activity. It will also leave more money in the hands of the public.
2) Money Accountability- It will be possible for Governments to account for all the money in the system. This way, the counterfeit and parallel economy can be curbed, Money laundering can be detected and flow of money to possible illegal activities can be monitored.
3) No need for Bank Accounts- Banks need to be paid to maintain bank accounts. Bank accounts also need to have a minimum balance so as to be viable. But Crypto currencies do not need accounts. Having only a digital wallet is enough. RSB crypto currencies can be maintained in digital wallets at no cost to the owners.
4) Easy transfer of funds-Governments can transfer funds or social security benefits to citizens' wallets in an instant, free of cost. Citizens' digital wallets can be linked to their social security number or other Government mandated IDs.
5) Easy Taxation- A person's money holding can be inferred by the Government when necessary. The Government can automatically deduct taxes without the need for people to file tax returns. It can wind up its tax collecting infrastructure and invest those resources somewhere else.
6) Certification- Assets can be certified, recorded and maintained using the same protocols that a RSB crypto currency will use. The protocol for RSB crypto currency will be called as Controlled Block Chain.

(A Controlled Block chain is different from a Block Chain per se [1]. A Block Chain is a permissionless Distributed Database, whereas a Controlled Block Chain will be Permission Based. The Permission here being provided by the Sovereign Authority.)

7) Price stability-Presently, crypto currencies like Bitcoin are highly volatile. This is because a lack of backing has led to rampant speculation. Consequently, Bitcoin has undergone many Boom-and-bust cycles. RSB crypto currencies will provide stability in value so as to be a reliable medium of exchange.
8) Manageable Deflationary and Inflationary indices- Because RSB crypto currency will be backed by Government; it will have a manageable inflation and deflation index.
9) Environmental advantage- Printing currency notes and maintaining them in circulation is costly both for the economy as well as the environment. In the long run, RSB crypto currencies will replace paper currency. It will thus save a lot of trees from being cut and used for paper.
10) Easy convertibility- People from one country will be able to invest more freely in other countries. This will lead to the emergence of a loan market which is highly competitive. This will make cheap and safe credit available to the neediest. This is presently not possible due to existing monetary, fiscal and distance barriers.

THE K-Y PROTOCOL

The K-Y Protocol aims to make Regulated and Sovereign Backed (RSB) Crypto currencies a practical reality. The authors have designed this protocol carrying their initials in abbreviated form as the name of the protocol. The Protocol consists of a set of rules and procedures.

(*)NationCoin- abbreviated as NC, it is a generalized designation for any RSB Crypto currency (RSBC). For example USA's RSB Crypto currency can be called USCoin, India's as IndiaCoin, China's as ChinaCoin etc. Each nation can have only one NationCoin i.e. RSB Crypto currency.

Since various countries have currencies of their own with differing Exchange rates, we have defined a **NationCoin Unit** as-

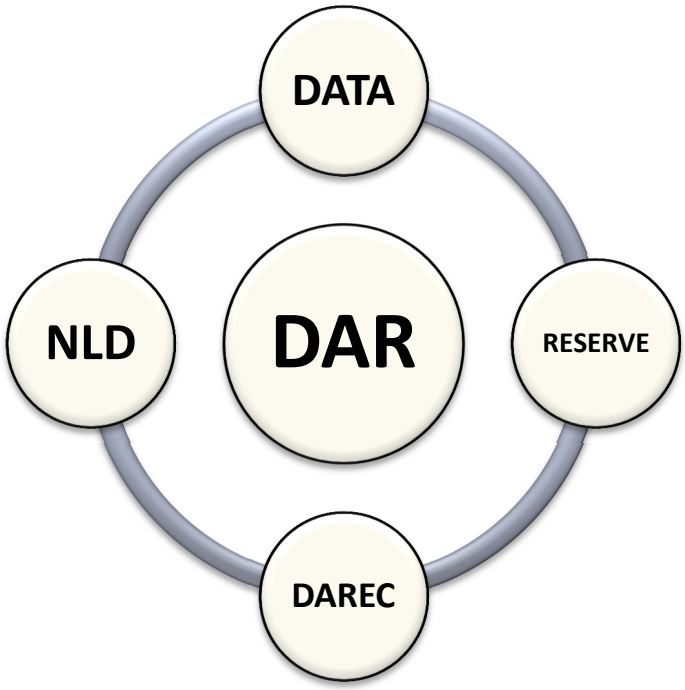
One NationCoin **Unit**=One NationCoin X Exchange rate of the currency with the US Dollar.

For example, in case of Rupee IndiaCoin unit
One IndiaCoin **Unit**= 1IndiaCoin X 68 =68 IndiaCoins.
One ChinaCoin **Unit**=6.5 ChinaCoins
One EuroCoin **Unit**=0.88 EuroCoins
One JapanCoin **Unit**=112 JapanCoins
One BritishCoin **Unit**=0.69 BritishCoins
(1 USD=0.88 Euros=0.69 Pounds=112 Yen=6.5 Chinese Yuan=68 Indian Rupees; as on 12/02/2016)

Note that NationCoin Unit is different from NationCoin. A NationCoin Unit is generic in nature. One NationCoin Unit is always equal to one US Dollar. Whereas One NationCoin is equal to one unit of native currency in that particular nation.

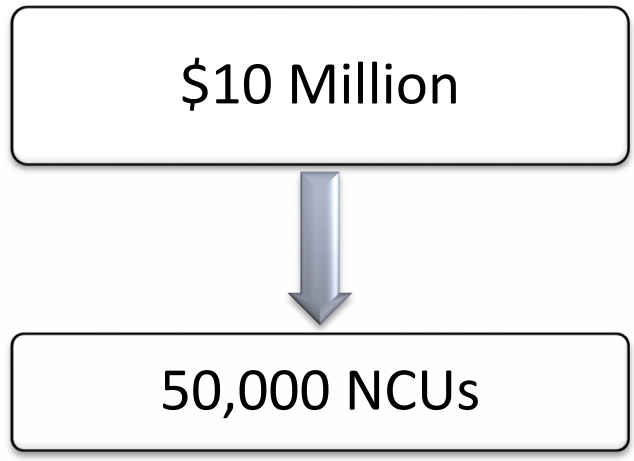
The KY Protocol is as follows

1. The Government of the country wanting to introduce the NationCoin will first setup the **"DIGITAL ASSETS RESERVE" (DAR)** by passing a law or amending existing laws as need be. It will also setup the **"DIGITAL ASSETS REGULATION & EXCHANGE COMMISSION" (DAREC)** which initially will have no role to play. Later on, when NationCoin becomes established as a primary mode of transaction, DAREC will play the role of an impartial regulator. The **NATIONAL LEDGER DATABASE (NLD)** is also created. It will be closely linked with the DAR. It will keep track of the transactions in its Block Chain Ledger whose copies will be distributed throughout the Network Nodes.
2. By a separate funding from the Government, DAR will setup "Grid Computing Clusters" with several nodes throughout the country. These networks will not be open to the public. These are the nodes that will mine the NationCoins. This will be done by **"DATA – DIGITAL ASSETS TRACKING & ADMINISTRATION"** which will be the technical wing and technical assistance arm of the DAR.
3. The Government will provide the DAR $10 million worth of loans. This will form The Corpus- to be used to back NationCoins.
4. DATA will also help the banks in the country to setup NationCoin compatible softwares. DATA will create block chain protocols for NationCoin.
5. The **RESERVE** will be the entity which will Sovereign stamp the Crypto Currencies and give it the RSB (Regulated and Sovereign Backed) certification. It will be an integral part of the DAR.

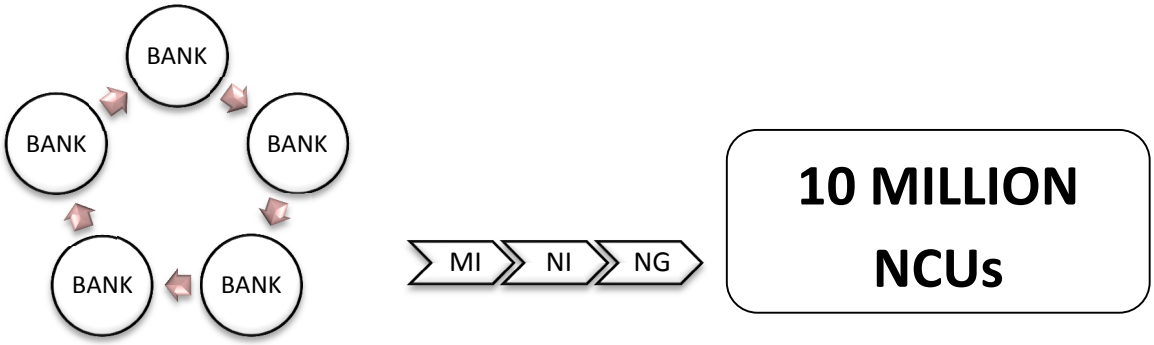


6. The networks so formed will be tested in trial runs involving NationCoin transactions, interest payments and exchange procedures. This is the System Configuration Stage.

7. The Government will provide a soft loan of $10 million worth of assets in any form (either in $ or National currency) to the DAR. This $10 million will be called “THE CORPUS”.
8. When the corpus is in place it will be securely locked up physically in vaults and the “GENESIS BLOCK” [2] (the First Block in the Block chain) of 50,000 NationCoin Units (NCUs) will be generated.
9. The 50,000 NationCoin Units will be provided to the banks for their daily interbank clearances. These 50,000 NationCoin Units will be pegged to $10 million in the Corpus giving each NationCoin a value of $200. This Backing will be certified by the Governor of DAR.



10. Banks will be mandated to use these NationCoin Units in their Intra-day and Inter-day settlements and clearances. For this purpose, Banks will be provided their own NationCoin wallets maintained by DATA.
11. Each Bank is mandated to use at least 25 cents worth of NationCoin Units per $100 in settlements and interbank transactions.
12. These transactions will be verified by DATAs Network nodes. Once verified, these will be categorized into blocks of between 45 kb to 85 kb and “Mined”. The Mining will be done by DATA's systems only and will not be open to public. Once mined, 190 NationCoin Units will be generated every 10 minutes. Therefore the Block time for each block will be 10 minutes. Reward per block will be 190 NationCoin units.



13. The NationCoin Units so mined will go into HOLDING. HOLDING is a Digital vault of DAR which is not connected to the public Network and will not to be released to the banks either. The NationCoin Units in HOLDING are not yet sovereign backed.
14. The DAR will hold the NationCoin Units in HOLDING until it accumulates 9.95 Million NationCoin Units. Along with the 50,000 NationCoin Units used by banks, there are now a total of 10 million NationCoin Units altogether.
15. When there are 10 Million NationCoin Units in Toto, it reaches the next crucial stage called the Equation.
16. **Equation:** When there are 9.95 Million NationCoin Units, DAR will start pegging its Corpus to the 9.95 Million NationCoin Units that it holds. Once sovereign stamped and certified, these 10 Million NationCoin Units will be exactly equal to $10 Million in the Corpus. When one NationCoin Unit= One Dollar in the Corpus, then Equation is said to have been achieved.

    [*As mentioned earlier, since various countries have currencies of their own with differing Exchange rates, we have defined a NationCoin Unit.

    One NationCoin Unit=One NationCoin X Exchange rate of the currency with the US Dollar.

    For example, in case of Rupee IndiaCoin unit

    One IndiaCoin Unit = 1 X 68 IndiaCoins=68 IndiaCoins.

    10 Million Dollars=10 Million IndiaCoin Units=680 Million IndiaCoins=680 Million Rupees
    Therefore, when there are 680 Million IndiaCoins, each IndiaCoin will be equal to One Indian Rupee and Equation is said to have reached. In case of Yen, Equation will be attained at 1,120 Million JapanCoins, for Euro it will be 8.8 Million EuroCoins, For Chinese Yuan it will be65 Million ChinaCoins and so on.]
17. Once Equation is reached, two things will happen in parallel.
    1. **First Parallel**: - DAR will release this 10 Million NationCoin Units to the Banking System in 4 phases over a period of 4 weeks. 2.5 Million NationCoin Units will be released every week. This is necessary so as to release NationCoins Units in a controlled manner without overloading or harming the Computing Systems.
    2. **Second Parallel**: This is the most important step. A process called Scaling is initiated. The number of NationCoin Units mined per Block is increased to more than 15 times the mining rate per block before Equation. The block size will also dramatically increase due to the large number of inter-bank transactions that will be taking place (as more and more NCUs are pumped into the system).The block size will increase to around 5 MB. The Block time will reduce from 10 minutes to 1 minute and number of NationCoin Units mined per block will be 2,850 NCUs. Thus the total rate of NationCoin Units generation will increase by 150 times the rate it was before Equation.

18. All the NCUs mined will flow into the HOLDING and is not backed in any manner. It will not be released to the public. But Banks can buy them by paying requisite currency which will go into the Corpus and an equivalent number of NCUs are released.

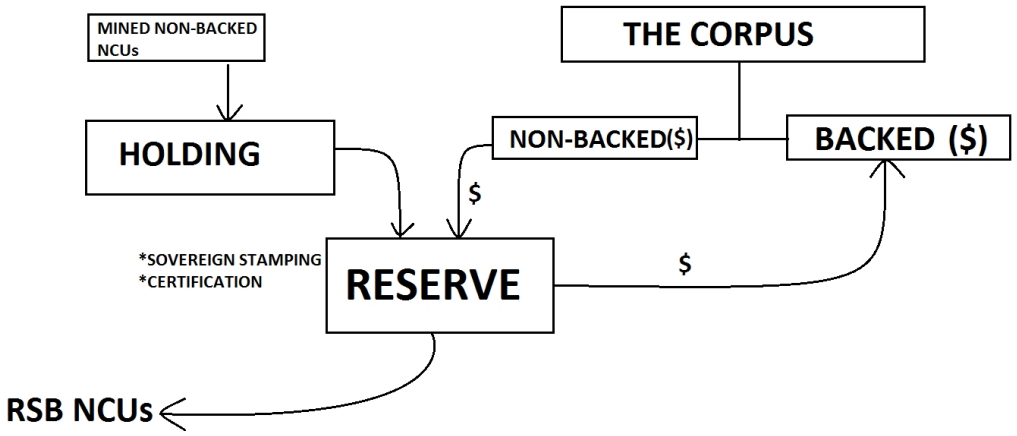
Equation is important for several reasons.

1. For the sake of public convenience, One Dollar has to be equal to One NationCoin Unit. The public may get confused with any other value and this may cause chaos and panic leading to adverse economic outcomes. By Equation, we ensure that people still identify One Dollar with One NationCoin Unit.

   [In case of Euro, 1 Euro=1 EuroCoin
   Yen, 1 Yen=1 JapanCoin
   Rupee, 1 Rupee=1 IndiaCoin
   Pound, 1 Pound =1 BritishCoin and so on]

2. Say, for instance 1 NationCoin Unit is equal to 2 Dollars, then speculators may see 1 NationCoin Unit as more valuable and may begin to hoard it, this will cause many problems for the society both in long and short term.
3. In case, One Dollar is equal to 2 NationCoin Units, people may see NationCoins as less valuable and may not prefer to use it for transaction. Then the whole idea of RSB Crypto currency will become impractical.

Freshly Mined NationCoin Units will not be backed by anything and as such will have no value. They are put into Holding. HOLDING will always contain non-backed NationCoin Units. These non-backed NationCoin Units will have a unique identity that sets them apart from RSB NCUs. The non-backed NCUs, when backed, will be certified as Backed NCUs by the DAR. These Backed NCUs, after Sovereign Stamping and Certification will be known as RSB NCUs. As soon as they are backed, they will undergo a change in their identity which will make them recognisable by the DAR and other Network nodes as RSB NCUs, fit for use in transactions.



This change in identity and certification will happen electronically in the Reserve.

19. Equation will happen one year after the Genesis Block. Scaling will start immediately after Equation.

20. From the end of first year to the end of second year around 1.5 Billion NCUs (NationCoin **Units**) will be generated which will be put in HOLDING.

21. From the beginning of the third year the Government can start paying a small part (around 1%) of the Government salaries through RSB NCUs. Say, the Government decides to pay 1 Million NCUs as salary. It will provide $1 million to the DAR. DAR will then provide 1 Million RSB NCUs to the Government to pay salaries.

22. The National Coin Wallets (NCW) of employees will be created and maintained by DATA free of cost. This NCW will be linked to the social security number or any ID system depending on the country (In case of the US it will be linked to the Social Security Number. In case of India it will be linked to PAN number).

23. Joe is a Government employee drawing $10,000 per month as salary. The Government decides to pay 1% of salaries in NCUs i.e. $ 9,900 will be in Dollar form and $100 worth in NCUs. Now Joe decides that he does not want NCUs. All that he has to do is access his bank account via internet and give back NCUs to the DAR (There will be a facility provided for this purpose). The DAR will credit $100 into Joe's account in lieu of 100NCUs.

24. Say Joe wants to transfer $1000 to Alice; he can do it in Dollars by paying around 25 cents as transaction cost. But if he transfers 1000 NCUs to Alice, he can do it freely without any transaction cost. International transaction costs of money transfers in native currencies will be even higher. But for RSB NCUs it will be minimal or zero.

25. The Bitcoin Protocol follows the practice of halving, every 4 years the number of bitcoins mined per block will halve. This will go on till there are 21 Million Bitcoins in the system. But for RSB NCUs, this is not the case. The RSB NCUs' primary objective is to make it widely utilized among the public. As such we need a large supply of RSB NCUs so as to replace a proportion of paper currency in circulation. For this reason, the RSB NCUs will undergo a process called Doubling.

26. Doubling: One year after Scaling has taken place, the process of Doubling will occur. Block time will remain 1 minute only. Number of NCUs mined per block will now be 5,700 NCUs (it was 2,850 NCUs after Scaling). The block size may (or may not be depending on number of transaction) double to 10 MB.

27. All the NCUs mined will follow the process of flowing into the Holding, to be backed and certified in the Reserve when funds flow into the CORPUS or as and when mandated by the Government(on being provided equivalent backing in currency).

28. All this time, the NLD (National Ledger Database) whose copy is present in all the nodes of the DAR network is promptly updated from time-to-time duly following the Controlled Block Chain protocol. The NLD keeps track of all RSB NCUs through its NCU ledger.

29. The DAR shall aim for replacement portion of around 50% of all total currency in circulation over a period of 10 years.

30. For the US Dollar, at present rates it will take about 8-10 years to replace half the currency in circulation by USCoin.

31. Linkage: Linkage here means that the NationCoin is allowed to be freely traded in the International Market. When around 50% of circulating currency is RSB NCUs, then Linkage with international markets can be allowed. 50% replacement is necessary so as to have a robust amount of NCUs which will not be affected by minor speculation. For the purpose of Linkage, NLD copies will be uploaded into satellites, so that they will act as a network node. For example take JapanCoin, if Joe sends a JapanCoin from Argentina to Alice who is in South Africa, the transaction is recorded and beamed to a Network Node in space (Japanese satellite). This will in turn update all other nodes in Japan, thus upgrading the Ledger.

32. Later on, every National Capital can host at least one network node of every other nation as part of a diplomatic treaty.

33. Once Linkage occurs, the Government (through the DAR of the country) can decide if it will allows "Free Float" of its NCU or a "Managed Float".

34. In case of "Free Float", market forces will determine the value of NCUs whereas in case of Managed float, DAR will allow the rates to float up to a particular range. Beyond that range it will manage NCU rates as it presently manages its native paper currency.

35. After a certain level is reached, say 50% of total circulating currency, Doubling can be stopped and NationCoins generated at a steady rate every year, accounting for inflation if necessary. Eventually RSB NCUs will replace paper currencies to a large extent.

36. RSB Crypto Currencies can also be introduced at the International Level. A WorldCoin can be created based on the K-Y Protocol. Only, the WorldCoin will be backed by SDRs (Special Drawing Rights) of the IMF. Exchange rates of various NationCoins vis-à-vis the WorldCoin will decide the inter-relations between the several RSB Crypto Currencies.

CONCLUSION

We have proposed a system for the creation of Regulated and Sovereign Backed (RSB) Crypto currencies. They will eventually replace, to a large extent, paper currencies of their respective nations. We began with the setting up of the Digital Assets Reserve which will be a sovereign authority. The first cache of NationCoins generated in the Genesis Block [2] will be given to banks for their internal settlements. This will ensure that the system continues to generate NationCoins subsequent to transaction verification as per the Controlled Block Chain Protocol. It will also test the robustness of the system before the NationCoins are released to the public.

Equation defines the unit-for-unit equivalency of NationCoin Units with the native currency. Scaling after Equation is used to cater to the huge demand that the Crypto currency will face. Doubling is aimed at replacement of a particular nation's currency with NationCoins. Linkage will enable the NationCoin to be used across borders.

The unique feature of The K-Y Protocol is that it can be used by any Sovereign Authority to create a credible RSB Crypto Currency. The people stand to benefit from all the advantages accruing from such a currency. Nations with a larger and more diverse economy will take longer to shift to NationCoins from paper currencies as the common medium of exchange. Smaller Economies can shift faster.

To make the NationCoin secure, several security features at various stages have been incorporated. Holding, Corpus Backing, Sovereign Stamping, Certification and National Ledger Database are some of the built-in security features. Hence it has a Multi-tiered security structure. The introduction of RSB NationCoins will usher in an era of **Cashless Liquidity**. The National Ledger Database can also be used for Non-Financial Block Chain uses where object ownership is decoupled from functional Utility.

ABBREVIATIONS

DAR-Digital Assets Reserve

DAREC-Digital Assets Regulation and Exchange Commission

DATA- Digital Assets Tracking and Administration

NCU- NationCoin Units

NCW-National Coin Wallet

NLD-National Ledger Database

RSB-Regulated and Sovereign Backed

REFERENCES

[1][2]-Bitcoin: A Peer-to-Peer Electronic Cash System-Satoshi Nakamoto

****