# eRupiah: RBI’s Virtual Cash 3

**Introduction:** No currency has ever been used in the human history which did not have the stamp of an authority. Bitcoin is a medium of payment but it is not money for the same reason. Nonetheless, the technology underlying Bitcoin is a significant one with great potential. A central bank, issuer of paper currency, can use some selected components of Bitcoin technology to replace paper currency with virtual currency, retaining all the important features of paper currency. The most important of them is that a central bank note is a freely negotiable bearer bond and a legal tender in the hand of its holder. It does not require any third party verification. Counterfeiting a central bank note is not impossible but difficult and costly. The central bank neither authenticates any transaction made with that particular note nor does it keep any record of that transaction. The note remains as a liability on the book of the central bank till it comes back to it, either for reissue or its destruction. The physical nature of the note ensures that no double spending is possible with the same note by its current holder. In case of digital cash, the main issue that a central bank has to **resolve is the issue of double spending without depending on third party verification of the same**. What follows hereunder is an outline of a system that any central bank can implement to issue its own currency retaining most, if not all, of the desired properties of a paper currency.

I am presenting below a system based on digital currency on a mobile phone. There is no compelling reason to believe that the same system cannot be implemented on a specially designed smart card with embedded chip. The system outlined below is described within the currency management framework of the Reserve bank of India (RBI). With little tweaking the same can be customized by any central bank.

**RBI Currency Management Framework**:

RBI carries out its currency management function through its 19 Issue Offices located across the country. There is a network of 4281 currency chests and 4044 small coin depots in selected commercial bank branches. These chests store currency notes and rupee coins on behalf of RBI. The note distribution mechanism is summarized in the following diagram.

RBI places indents for notes with note printing press

Press remits notes to various issue offices

Issue offices remit the notes to banks and releases notes through its counters

Public

Notes comes back to banks and the currency chests

Note is returned to RBIBI

For issuance of digital currency, each currency chest would function as a data center for hosting the ledger book of notes issued from it. Similarly each issue office of RBI would have a copy of the entire ledger book of notes. A folio would be opened in the note ledger book when the first time a specific note is issued. Each data center will have complete inventory of wallets issued by RBI. An wallet could be a mobile app downloaded on a person’s mobile phone or it could be a smart card to be issued by RBI. The details are given below.

Every bank branch would have a digital cash dispenser. Any wallet holder would be able to replenish her wallet with digital currency by pairing it with the dispenser via Bluetooth or NFC communication channel. Similarly every ATM would have similar facility. At the time of cash dispensation from bank branch or ATM would require Aadhaar based biometric verification of wallet. For cash transfer between wallets of two individuals this verification is not a necessary requirement.

**The protocol for issue of eRupiah**

1. RBI would maintain ledgers of each currency note in a distributed database.
2. Currently RBI issues notes through its Issue offices. The distributed database will be created according to issue departments of RBI. Each Issue office of RBI will be able to issue new digital currency and destroy old digital currency. Destruction of old digital currency would help RBI to keep the number of entries in the ledger folio of a particular note within a limit. Every Issue offices would maintain record of all notes issued by it as well as copies of corresponding records of 3 neighboring Issue offices.
3. Each currency chest will have a database of notes received by it from RBI’s Issue department.
4. Each currency chest will also have replicated database of its three nearest neighbor
5. The system will issue new digital currency when an account holder wants to withdraw cash from its account with RBI. It would be optional, to start with. An account holder can withdraw cash or digital currency according to her discretion.
6. The account holder would specify how much of its cash withdrawal would be in digital form. This facility would be provided for an interim period when both forms of currency would be in circulation.
7. To incentivize issue of digital cash, RBI may reward with a fixed amount that could be related to the cost of producing physical cash.
8. RBI is banker to the Central and State Governments. It also functions as banker to the banks and thus enables settling of inter-bank obligations. These large account holders of RBI would get digital cash in their **Jumbo Wallet** which would be a server in the account holder’s custody. It would be like a till holding cash. An authorized person can withdraw e-Rupiah from the till as and when required.
9. The RBI’s Note ledger would comprise ledger folios of each currency notes issued.
10. Each record in the Note ledger would comprise the following attributes: (1) a sequential no, (2) unique identity / sr no of a note, (3) hashed value of the note serial no, (4) identity of the issue department, (5) denomination, , (6) time stamp of transaction, (7) hashed value of identity of paying wallet (first time payer would be RBI), (8) hashed value of identity of receiver wallet, (9) active flag, (10) hashed value of first 9 attributes , (11) hash value of the first 9 attributes of earlier transaction record of the same note. The identity of a wallet is described below.
11. RBI will also maintain database of each wallet downloaded from its website.
12. The wallet database will have a header record with the following attributes (1) IMEI no of each phone, (2) Aadhaar No of the phone owner, (3) timestamp of successful downloading of the wallet, (4) the GPS location of the phone at the time of downloading of the wallet, (5) a unique private key generated for each wallet and (6) the corresponding unique public key generated for each wallet. This data would also be hashed and encrypted with RBI’s private key and will be part of the header record. RBI’s public key would also form a part of the header record. The private and public key of each wallet would be generated by RBI at the runtime. The hashed value of attributes 1 to 6 would be the identity of each wallet.
13. Each wallet will have its own database of transactions. Each record in the transaction database will represent a note that has been loaded into the wallet. Each record will have the following attributes: (1) unique identity of the note, (2) note denomination, (3) digitally signed (with the private key of the paying wallet) hashed value of the concatenated string of serial no and denomination, (4) digitally signed ( with the private key of the paying wallet) hash value of concatenated string of attributes 1 and 2 of the header record with private key of payer wallet, (7) public key of the paying wallet, (8) timestamp of last transaction( i.e. timestamp of receipt of the note , (9) timestamp of the payment transaction, (10) payment status (paid or unpaid), (10) hashed value of the earlier transaction of the note(attributes 1,2,3,4,5).
14. A transaction between two wallets would involve “note data” transfer from the paying wallet to receiving wallet. [A separate note is given to explain how such transfer can happen with QR codes}. Every note that gets transferred from the payer’s wallet to the recipient’s wallet would essentially mean transfer of the entire record from the former to the latter. In the process of data transfer two insert / update activities take place in the receiver’s and payer’s wallet respectively. The receiver’s wallet inserts a new note record while the payer’s wallet updates the concerned note’s existing record.
15. Once the receiving wallet gets a new e\_Rupiah note, it checks the authenticity of the note by calculating hash value of the concatenated string of attribute 1 and 2 of step at 13. In the payer’s wallet the status flag would get changed to “paid” while in the receiver’s wallet it would continue to have the status flag as “unpaid”.
16. Any wallet would have a limit in terms of number of records / notes. When the database has reached its limit then the wallet would have to be uploaded to RBI and a new wallet has to be downloaded.
17. At any point of time a single wallet would be subject to 2 limits- holding limit of no of transactional records and total value of a single transaction. For a high value transaction two factor authentications would be required. (say above one lac). Both paying wallet as well as receiving wallet has to simultaneously establish connection with RBI and get their credential verified.
18. As and when no of records in a wallet’s transactional database reaches its limit, the database has to be downloaded in an ATM or at a bank branch. The wallet would be purged of the all transaction records with status as “paid”. The wallet holder then can download more E\_Rupiah from an ATM or from a bank brunch. RBI will update its ledger book of individual notes thus uploaded from each wallet.
19. Any fraudulent transactions identified in the process of uploading would get notified and thorough automated forensic audit perpetrator of fraud would get identified.

**Downloading of Wallet**:

1. The user sends a sms to a designated no with the Aadhaar no of the sender. Each sms would cost the user 1 INR. RBI would send a link to the phone and clicking on the same the app would be automatically downloaded. To activate the app, the user has to sign-in with his/her Aadhaar no. For additional security one may think of incorporating biometric signature of the wallet holder as another feature of the wallet; every use of the downloaded wallet would require signing in biometrically by the wallet holder.

The wallet will have the following features:

1. It will recognize another wallet in its vicinity using NFC technology. Alternatively Bluetooth technology for pairing two cell phones can be also used. Both the wallets would then exchange their digital identity and verify them with public keys of both and RBI’s public key. After two wallets have been paired, the payer’s / payee’s wallets would prompt the respective wallet owners to initiate the intended actions on their part. The payer will have to initiate payment action and would type in amount of money to be paid. The wallet would automatically prompt for denominations – a built in program would provide the best possible composition nearest to the amount indicated by the payer. The payer would have the right to change the composition and the resulting total value.
2. Once the payer approves payment the required data transfer takes place without seeking any third party verification at that time. For a transaction above a certain threshold value, at the discretion of the transactors, the receiver’s wallet may be connected with Aadhaar database and a biometric confirmation of the payer’s bonafide may be authenticated.
3. If any wallet holder commits a fraud by hacking the wallet’s database and changing the header record, it would be considered as an act of counterfeiting of notes. As and when any receiver uploads data to RBI website, the same would get immediately detected when RBI updates its ledger folio of notes involved. The concerned wallet holder would be notified with the fraudulent transactions and details thereof. It would be a matter of time to nab the fraudster.
4. For merchants, wallets can function like mPOS (mobile point of sales) machine. A merchant’s wallet would authenticate the payer’s wallet and notes therein by directly connecting to RBI’s ledger of notes.

**How the system will function:**

Alice downloads the mobile app/wallet from RBI website. Alice visits it nearest ATM or bank branch and loads its wallet with required e-Rupiah. On a single day Alice would not be allowed to load her wallet with more than, say, fifty thousand value of e-Rupiah. The cash dispenser, say ATM, would be configured accordingly.

Alice wants to pay, say one thousand rupees, to Bob; the Alice keeps her wallet bearing mobile to Bob’s wallet and taps the application on her mobile. The respective apps recognize each other and Alice keys in the amount to be disbursed to Bob. If Alice has necessary denominations then the application would give nearest amount higher than that amount and which can be transacted. The balance can be paid back by Bob.

**Loss of Wallet**

In case of loss of a wallet, the holder of the wallet would be required to register the loss with RBI and provide its mobile number and Aadhaar number. RBI would broadcast the IMEI no of the wallet to all mobile service providers, thus blocking any further use of the mobile. In due course, the stolen wallet can be traced and, in case of theft, required action by law enforcing agencies can be initiated. If a fraudster wants to use a stolen wallet by replacing the original header record, it would need to replace all unpaid notes’ records with values consistent with corresponding values of the new fraudulent header record. This would be very costly and may not be worthwhile. Furthermore, it would not be possible to download any further notes from an ATM or a bank branch.

**Cost of Issuing E-Rupiah**

As on end March 2017, around 201 billion pieces of notes including coins (one rupee and above) were in circulation. In that year, India’s adult population (15 years and above) was estimated to be around 916 million. If all adults hold one wallet each, the estimated size of all header records would be around 320 GB, not a very big number by any yardstick. The size of transaction database, assuming 1000 transaction for each note during its lifetime, would be around 71 petabyte or .07 Exabyte. Amazon Redshift Spectrum Query service charges $5 per Terabyte of Query. If in the extreme case we assume that all notes are transacted once every day of one year, then the cost would be around 132 million US dollar or 862 crore of Indian rupees. Taking storage cost, it would be well below the cost of printing notes that RBI incurs today.

**Digital Currency and Corruption**

With digital currency it would be very difficult for anybody to make huge cash transaction for drug trafficking, bribing and other illegal purposes. In the Netflix original TV serial Narcos, the Columbian drug cartels are seen to carry out most of their transactions in cash. So much so, they had to store cash buried in fields. Central Bank Digital Currency would be the most effective antidote to cash mediated corruption and illegal transactions.