Published November 2017

Tibado: Everyday Cash implemented as Electronic Coins

Dr David Everett
Tim Jones CBE
www.tibado.com

Abstract

Emulating the properties of cash for making payments on the internet is technically challenging. Physical cash is a flexible product which allows people to totally control their money and to make immediate payments to others in private without transaction fees because no intermediaries are involved in the payment. Recently there has been an emergence of digital currencies based on the Blockchain or Distributed Ledger Technology (DLT) such as Bitcoin but these architectures have run into cost and scalability problems which have led to further considerations on their future[1]. Here we propose a solution that has all the properties of physical cash but in an electronic form factor referred to as electronic coins.

The technology is based on the use of an Autonomous Finite State Machine (AFSM) which makes the change of state in the set of coins in circulation to be rule based and autonomously enforced thereby removing the need for community consensus necessary with the Blockchain. This avoids the costs and scalability issues and also provides an Originator role that collateralises the digital cash against traditional fiat currencies thereby avoiding the volatility of virtual currencies such as Bitcoin.

Whereas traditional cash is based on a paper or metallic form factor modern technology can provide an electronic coin token protected by cryptographic means that makes the work function to create an unauthorised coin economically unacceptable. As with Bitcoin the intrinsic difficulty with digital currencies is preventing the double spend given that a copied coin is indistinguishable from the original. The AFSM validation protocol described here implements a centralised trust model using the concept of an immutable transaction ledger from which the Live Coin Database (LCD) is derived that is implemented in a distributed fashion thereby providing the best of both worlds, no single point of failure but without the performance or cost overheads of the Blockchain consensus mechanism.

Introduction

Electronic payments using credit and debit cards have become widespread as well as other electronic payments between businesses and between banks. These payment systems overcome the practicalities of handling cash but do so by changing the trust model. Cash is a bearer instrument and accordingly payments relate to a local asset transfer. Conventional electronic payments by comparison result in some trusted third party, usually a bank, holding the assets on behalf of the owner. Payments are effected by the asset owners instructing the bank or other third party to make a remote asset transfer.

It is clear that the owner doesn't have direct control of the money, they have to rely on the third party to reliably look after their money and to correctly authenticate their instructions and to process them accordingly. This third party is an intermediary and is involved in every transaction. This leads to two problems, participants have to trust the intermediary which has to resolve disputes between the transacting parties in some equitable fashion. As a consequence the intermediary needs to charge a transaction fee to cover costs.

It was these issues that lead to the design of Bitcoin[2] but we can show that this particular solution as a fully scalable operation for digital cash is flawed because of the consensus process. Bitcoin is a remote transfer of ownership transaction recorded on an immutable data base or ledger called a Blockchain. In order to add a new block to the chain a set of validators called miners agree the correctness of all the transactions in the new block. This involves doing cryptographic work and the only way to motivate the miners is to give them an incentive. These rewards come in two forms, as new bitcoins intrinsic in the new block generation which led to the term miner and as transaction fees defined as part of each transaction. Since the new bitcoin reward decreases with time the fundamental reward long term remains with transaction fees.

Since Bitcoin is a remote transfer of virtual ownership, the participants do not directly control their assets. For example the participants rely on the miners to add their transaction to a new block and at the current time because of the limited block size and transaction volumes the users have to balance transaction times against transaction fees. It is not obvious that other digital currencies developed on this same Distributed Ledger Technology[3] would fare any better.

Electronic payments today are traditionally manged by the 4-Party model where an Issuer (1) provides their customer a card holder (2) with a card. At the point of sale the card holder presents the card to the merchant (3) to construct a message for the payment. The merchant then passes this payment message to a merchant acquirer (4) to collect the payment. However this underlying 4-Party model is fundamentally based on the use of intermediaries with the attendant problems referred to earlier and as such cannot possibly reach this digital cash goal.

What is really required is a payment instrument with all the properties of cash but in an electronic form factor. A physical coin is a piece of metal fabricated with security features to make it difficult to counterfeit. There is absolutely no reason why you can't have a coin message incorporating cryptographic security features making it very difficult to create without the necessary secret keys. The disadvantage of a digital message is that can easily be copied leading to a potential double spend. In this paper we describe a new solution that prevents a double spend while preserving all the properties of physical cash. Users obtain and manage digital coins just as they would physical coins and they use a pocket application on their PC or mobile device to help manage their coins. These coins can be stored with an arbitrary level of security as necessary to meet the user's risk appetite.

Coins

The digital coins represent a digitally signed message token which defines the value and currency of the particular coin. This signature which is actually created using symmetric cryptography to minimise the coin size is provided by the originator of the currency. The use of asymmetric cryptography is redundant because only the originator can vouch for the avoidance of the double spend and accordingly the system can take advantage of the higher performance of symmetric cryptographic algorithms. The digital coin has the following format,

Identification Number	Coin Value Definition	Cryptographic Authentication Code

Each coin is unique and is normally communicated between participants as a coin image incorporating a bar code. Although we refer to the coin as a digital image it is clear that at any point in time it could adopt a physical form factor. A coin owner for example could print a copy of the coin image on a piece of paper and send it as a present or even store the printed images under their mattress. Equally the coin tokens can be managed as a message of the data contents which is just 64 bytes.

These coins can be sent between participants using email or any other social media communication system. As ownership is an intrinsic property of these digital coins it is for the users to decide the required level of security in their storage and transmission. WhatsApp for example enciphers all messages between users. The users obtain their coins from agents who in turn get their coins from the originator.

The Originator

Cash is a bearer instrument which means it carries no record of ownership. The holder of the cash is assumed to be the owner and they may pass that to another person who then becomes the new owner. This leads to a number of properties that define the use of cash in our economy,

- The owner holds the cash (it is not held in an account managed by a third party)
- It is an anonymous transaction (or as anonymous as the participants agree)
- There is no payment intermediary (e.g. no bank is involved in the transfer of ownership), no permission is required to make a payment, it is censorship resistant
- It is irrevocable (there is no concept of charge backs or dispute resolution)
- There are no financial status requirements, you don't have to have a bank account or credit card which provides financial inclusion
- The transfer of ownership is immediate, when you pass a $ bill to somebody they have it and you don't, as before nobody else is involved and nobody else knows about the transaction

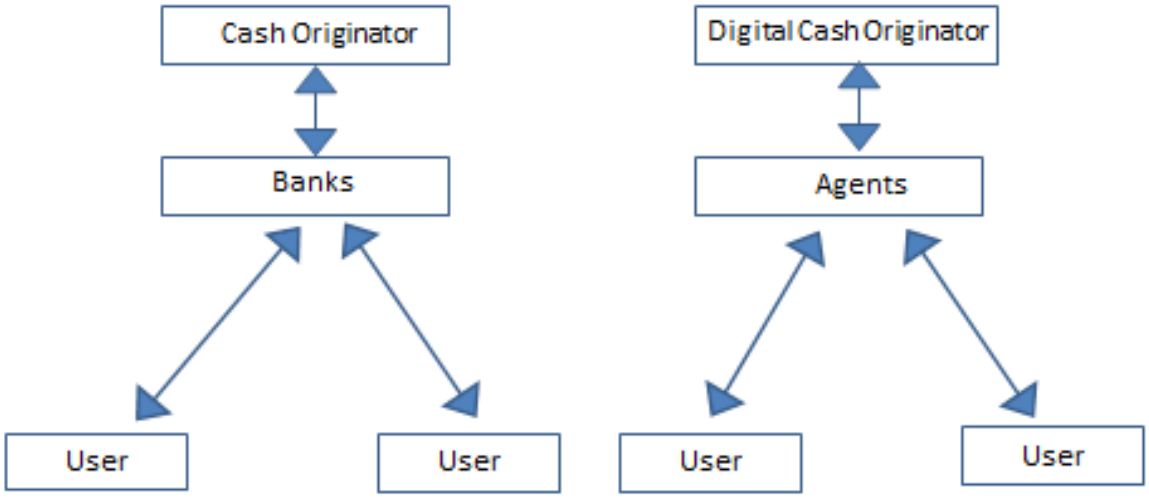
In the case of physical cash the owners must provide adequate physical protection of the cash in their possession and when they receive cash from another party they must be adequately assured that it is genuine. There is an implied authenticity check.

By definition any digital cash instrument must have the same properties as physical cash, it must be a bearer instrument so all the properties described for a physical cash instrument must apply to the digital cash instrument. Digital cash is physical cash just in a different form factor, Instead of notes and metal coins digital cash is digital data.

In the same way the holders of digital cash must provide adequate security protection against loss and it must be possible for the holder to be assured of its authenticity.

Central banks are the normal originator of fiat cash. They are responsible for the creation of the coins and notes and put them into circulation by selling the coins and notes to the retail banks. These retail banks have sight deposits at the central bank which are debited when the retail bank requests cash. As with any double ledger transaction the central bank ends up with a float account to the value of the cash put into circulation. This float represents a liability to repay if the retail bank returns cash to the central bank. In practice however the value of the float for a given economy is relatively stable and

provides the central bank a method of earning interest. Seigniorage originally from Old French meaning the ‘right of the lord to mint money’ is defined as the interest earned by the central bank less the cost of producing and distributing the coins and notes. In general central banks do not recirculate coins.



Consumers, businesses, governments, banks and merchants

Consumers and merchants deal with the retail banks, it would not be normal for them to have accounts with the central bank. In a normal economy the consumers buy cash from their bank to pay the merchant. At the end of the day the merchant would lodge the cash collected during the day to credit their account with the bank. Merchants may recirculate some or all of their cash to pay their employees and suppliers. This system works because everybody trusts the central bank and they of course are responsible for the security of the system. If it was too easy to copy the coins and notes then their (float) liability would be higher than the original deposits received.

Similarly for digital cash you would expect some legal authority to be responsible for the origination of the digital cash. Users of the system need to trust this authority and to be assured that adequate security controls have been applied to assure them against the loss of value. As with any security system authority and responsibility must rest with the same legal entity. Digital currencies operating on a Distributed Ledger Technology cannot bypass this fundamental requirement which casts aspersions on some of the more popular currencies.

The Live Coin Data Base

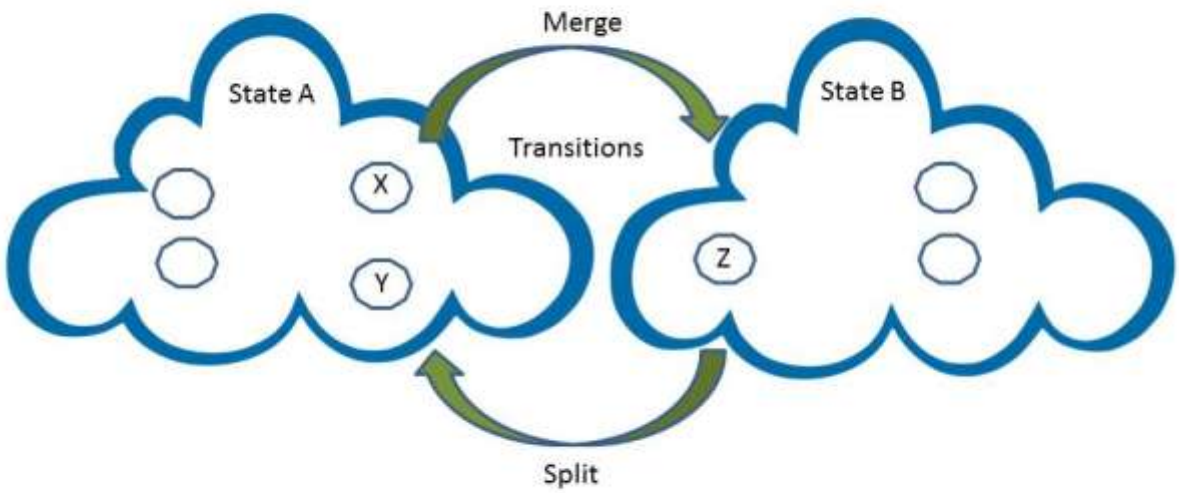
The Distributed Ledger Technology referred to earlier maintains an immutable ledger data base that records the total transaction history. Bitcoin for example has suffered a scaling problem due to the size of this database which is currently over 90 GBytes. In practice each full node also maintains a

Unspent Transaction Output data base which is a record of all the bitcoins available to be spent. This is of course much smaller and more practical to operate. However this is not part of the consensus process and is more of a convenience to the full nodes. Tibado follows a similar approach but avoids the consensus complexity. The system maintains a list of all unspent coins, i.e. live coins in circulation. If you were to compare Tibado with the number of unspent outputs, currently 44 million the equivalent Tibado live coin data base would be only 2.8GBytes. However in addition this database can be partitioned because the coins are uniquely identified and could be associated with a particular subset of the live coin data base.. which could be distributed as required. In the same way as an originator is responsible for its currency the originator is be default responsible for the live coin data base for its currency which can be defined to any arbitrary security level.

Clearly the originator is not motivated to allow any unauthorised additions to the live coin data base because that would increase their float liability. They are also prevented from unauthorised deletions because they aren't capable of presenting a live coin necessary to remove a coin from the live coin data base.

Autonomous Finite State Machine - Coin Processing Module

The coin processing module is a web API provided by the originator to help users manage their coins. As previously mentioned the users store and use coins as their business requires but clearly there are times when a cash exchange function is required. A Tibado coin can be of any value but may not be the right value to send to another person or merchant.



Split Coin (State B → State A)

The Coin Processing Module (CPM) allows a user to submit a coin of any value and to request two coins in return where the value before and after the function is a constant,

Value of coin (Z) → Value of coin(X) + Value of coin(Y)
Number of coins in State A = number of coins in State B + 1
Value of all coins in State A = Value of all coins in State B = Constant

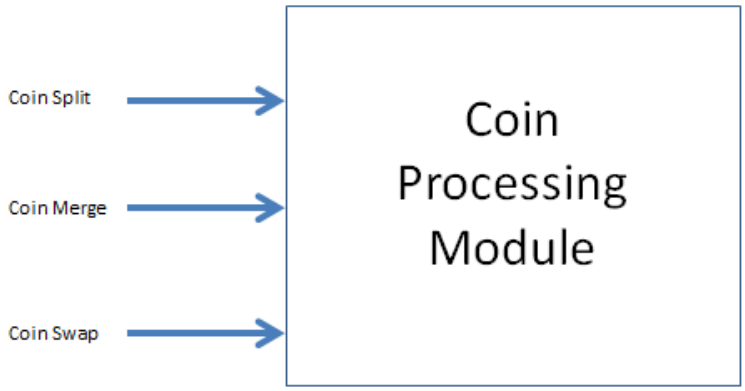
At the end of the transaction the original coin has been removed from the live coin database to preserve constant value. This function is called split coin.

Merge Coins (State A → State B)

In a similar fashion a user may require to merge two coins into one. The same rules apply and the sum of the value before and after the transaction must remain a constant,

Value of coin(X) + Value of coin(Y) → Value of Coin(Z)
Number of coins in State A = number of coins in State B + 1
Value of all coins in State A = Value of all coins in State B = Constant

At the end of the transaction coinA and coinB will have been removed from the live coin data base. This function is called merge coin.



There is a third function that users will find useful which is a coin swap. If somebody has presented you with a coin you know they still have a copy of that coin and until you do something with that coin they could in principle re-spend the coin. However once you put that coin into your pocket then the coin is refreshed with a new identification number, effectively a new coin is created for the same value and the original coin is retired from the live coin data base. The function used to do this is called coin swap.

Pockets

In order set up a working eco system it is envisaged that developers will create pockets. This is an application that runs on a PC or mobile device to manage the user's coins.

The structure of all Tibado coins is the same and a pocket may choose to handle multiple coins or to use the Coin Processing Module (CPM) to merge a set of coins. In any event the pocket application has access to the CPM and can optimise its functions accordingly. In general we would expect the application when presented with a new coin to use the CPM to swap the coin in order to prevent the provider of the coin from making a double spend.

Conclusions

We have proposed an electronic cash system with all the properties of physical cash, it is just cash in the form of an electronic coin. In addition just like cash it has a similar trust model where the participants place their trust in the originator of the currency. This avoids the cost and scaling problems with digital currencies operating on top of a Distributed Ledger Technology solution. We have also shown the potential flaws in trying to avoid a centralised trust model.

The system operates by means of digital coins that are protected by a live coin data base. All payment transactions are undertaken without the need for an intermediary which truly avoids the need for transaction fees inherent in all other electronic payment systems. By this means the user's privacy is always protected.

The users prepare the coins prior to making payments by accessing the Coin Processing Module which is an Autonomous Finite State Machine (AFSM) that enforces the security of the system. The users can split or merge coins and in addition they can swap an old coin for a new coin but with a different identity.

References

[1] Distributed Ledger Technology: beyond block chain
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

[2] Bitcoin: A Peer-to-Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf

[3] Centrally Banked Cryptocurrencies
http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/ndss16currencies.pdf