Vanderbilt University Department of Economics Working Paper Series
Nashville, TN 37235-1819

Vanderbilt University Department of Economics Working Papers 17-00007

Blockchain Cryptocurrency Backed with Full Faith and Credit

John P. Conley
Vanderbilt University

Abstract

The major advantages of blockchain based cryptocurrencies are the independent verifiability of transactions and the anonymity that they allow. Blockchains can also process transactions at much lower cost than banks and credit card companies. On the other hand, the value of cryptocurrencies is quite volatile. In addition, the crypto-ecosystem is not easy to access for many less technologically savvy consumers and it is especially difficult to make financial connections to the outside world. These factors limit the utility of cryptocurrencies as a store of value and a medium of exchange, respectively. This paper proposes the creation of CryptoBucks, a cryptocurrency backed 100% by dollars. CryptoBucks solve the problem of volatility and offer various levels of privacy and anonymity depending on how the system is implemented.

This paper was completed while the author was visiting researcher at Microsoft Research. I would like to thank Microsoft for their hospitality. The author takes sole responsibility for the content of this paper.
Citation: John P. Conley, (2017) "Blockchain Cryptocurrency Backed with Full Faith and Credit", *Vanderbilt University Department of Economics Working Papers*, VUECON-17-00007.
Contact: John P. Conley - j.p.conley@vanderbilt.edu.
Submitted: June 06, 2017. **Published:** June 06, 2017.
URL:http://www.accessecon.com/Pubs/VUECON/VUECON-17-00007.pdf

Blockchain Cryptocurrency Backed with Full Faith and Credit[1]

John P. Conley[2]

Vanderbilt University

June 2017

Abstract

The major advantages of blockchain based cryptocurrencies are the independent verifiability of transactions and the anonymity that they allow. Blockchains can also process transactions at much lower cost than banks and credit card companies. On the other hand, the value of cryptocurrencies is quite volatile. In addition, the crypto-ecosystem is not easy to access for many less technologically savvy consumers and it is especially difficult to make financial connections to the outside world. These factors limit the utility of cryptocurrencies as a store of value and a medium of exchange, respectively. This paper proposes the creation of CryptoBucks, a cryptocurrency backed 100% by dollars. CryptoBucks solve the problem of volatility and offer various levels of privacy and anonymity depending on how the system is implemented.

[1] This paper was completed while the author was visiting researcher at Microsoft Research. I would like to thank Microsoft for their hospitality. The author takes sole responsibility for the content of this paper.

[2] j.p.conley@vanderbilt.edu.

John P. Conley
Department of Economics
Vanderbilt University
Nashville, TN, 37235

jpc@jpconley.com
http://jpconley.wordpress.com/

Introduction

The major advantages of blockchain based cryptocurrencies are the independent verifiability of transactions and the anonymity that they allow. Using coin tumblers and employing other reasonable precautions permit users to make completely anonymous and untraceable transaction. Blockchains also have the potential to process transactions at much lower cost than banks and credit card companies. On the other hand, the value of cryptocurrencies is quite volatile. In addition, the crypto-ecosystem is not easy to access for many less technologically savvy consumers and is it is especially difficult to make financial connections to the outside world. These factors limit the utility of cryptocurrencies as a store of value and a medium of exchange, respectively.

Bitcoins themselves have no intrinsic value. They trade on exchanges for whatever the market will bear. News of break-ins at exchanges and coin vaults that result in the theft of bitcoins undermines trust and is responsible for much of the cryptocurrency's volatility. Of course US dollars have no intrinsic value either, but trust in the Federal Reserve System is far greater. This paper proposes the creation of CryptoBucks, a cryptocurrency whose value is linked directly to the US dollar. The CryptoBuck ecosystem makes use of a public blockchain to record transactions and guarantee the honesty and integrity of the system. Using a blockchain also makes it possible significantly lower the cost make financial transactions. Depending on how the ecosystem is implemented, it can provide the same degree of privacy and anonymity as Bitcoin, Ethereum and other established cryptocurrencies.

The CryptoBuck Ecosystem

The essential idea of CryptoBucks is to create a cryptocurrency based on a dollar standard, that is, backed 100% by dollars. This requires a financial bridge between the real and cyber worlds. Two two types of institutions are needed to do so. The first is a financial intermediary based solely in cyberspace. The second is a financial institution based in the real world with access to the existing banking and financial system.

The ecosystem could contain many of each type of entity. This would require the creation of some sort of clearing house mechanism to attribute incoming and outgoing transactions to the correct cyber and real world banks. This is not very difficult to do, but in order to make the idea clear, we describe a system with only one of each.

CryptoBuck Incorporated (CBI) is an entity set up to intermediate transactions between users and the real world financial system. CBI may also create transactions at the request of users that make it difficult or impossible to connect private key accounts (PKA), with biological humans or account numbers in the real financial system.

Brick and Mortar Bank (BMB) is a *corresponding bank* in the real world connected to the existing banking system. Being a corresponding bank means that there exists a relationship whereby BMB uses CBI to conduct business on BMB's behalf in the cyberworld, and CBI uses BMB to do the same in real space.

The element that holds the CryptoBuck system together is a public blockchain that records transactions of behalf of CBI and individuals. Proof of work is the gold standard to guarantee the integrity of blockchains, but has many problems. Proof of work is costly and would not easily scale up to thousands of transactions per second. Whether to use some modification of proof of work, proof of stake, or some other approach is not clear. This is a problem for all blockchains and many startups are working on better alternatives. Whatever best practice emerges to create trustworthy large-scale public ledgers would serve the purposes of the CryptoBuck system.

How CryptoBucks Work

Below we outline how a simple implementation of to a dollar backed cryptocurrency would work.

1. A customer buys a credit token for X dollars at BMB. Any ordinary way of transferring money to BMB can be used for this. The credit token itself is an encrypted, signed promise to pay the X on demand to whomever presents the token. In essence, the token is crypto-cashier's check (CCC).

2. The customer creates an order through CBI on some interface to transfer X dollars to his PKA on the blockchain and attaches the CCC.

3. CBI presents the CCC to BMB which verifies it, cancels it, and puts X dollars into CBI's real world account. CBI then creates a transaction crediting the customer's PKA with X dollars to be written to the blockchain.

4. Transactions and orders are collected for a fixed time interval, and then sent as a group to be written on the blockchain. CBI keeps a running total of how much it claims that BMB should have credited CBI's account in the current time interval. This includes both incoming credits from cashing CCCs and outgoing transactions described below. BMB does the same in reverse. Thus, both CBI and BMB will generate a claim of net deposits BMB makes in CBI's real world account.

5. At the end of the time interval, CBI sends a bundle with all the transactions it wishes to execute and its net deposit claim to be written in the blockchain. BMB creates a signed document which indicates its net deposit claim for the interval, as well as the total CBI has on deposit at BMB at the end of the interval. This is also sent out to be recorded in the blockchain.

6. Depending on how the Blockchain is constructed, miners, designated stakeholders, trusted intermediaries, or other block builders, receive CBI's transaction bundle and verify that the total net number of CryptoBucks that CBI wants to credit or deduct to PKAs equals its net deposit claim. Block builders also verify that CBI's net deposit claim is the same as the claim received from the BMB and that the total in CBI's account equals the sum of net deposits since the account began. If everything checks out, the bundle is written to the next block of the public chain.

7. Within the CryptoBuck blockchain, transactions take place in the ordinary way. Individual PKAs create transaction orders and send them individually to be recorded in the next block. This is a little different from the bitcoin approach since CryptoBucks have no existence as separate objects. Bitcoins each have their own cryptographic identity. Transactional integrity is assured by checking that all the bitcoins currently owned by any PKA can be tracked backwards to their

creation, and that each bitcoin exists only once in the current record. The integrity of the CryptoBuck blockchain, on the other hand, is assured by verifying balances. If a dollar is added to a PKA it must come from another PKA which has it balance reduced by a dollar, or from a net deposit to CBI's BMB account.

8. If a customer wishes to take X dollars out of the CryptoBuck system, he writes a special transaction order to move CryptoBucks out of his PKA to an "exit" PKA owned by CBI. The transaction order includes encrypted instructions that can be read by only by BMB that indicate where the money is to be deposited or transferred. For example, a check could be issued, and EBT initiated, or cash paid to someone with the correct credentials.

9. CBI receives this transaction order from the user's PKA and forwards it to BMB with the encrypted instructions. It also deducts X dollars from the running total it claims as net deposits to BMB this interval and finally destroys all CryptoBucks in its exit PKA.

10. BMB deducts X dollars from CBI's account and disburses them according the encrypted instructions. It also deducts X dollars from the running total it claims as net deposits to CBI's account.

What CryptoBucks Accomplish

The main advantage of CryptoBucks is that their value is not volatile. There is a fixed exchange rate of one between CryptoBucks and real dollars. In the 19th and 20th century, paper gold and silver certificates issued by the US Mint could be converted on demand into real gold or silver. Similarly, CryptoBucks can converted into dollar bills on demand. People still chose to carry and transact in gold and silver certificates instead of specie because it was more convenient. The same is true of CryptoBucks.

An almost equally important advantage of CryptoBucks is that the costs of executing transactions within the ecosystem should be dramatically less than they would be using real world financial institutions. Credit cards charge merchants 1% - 4% in transactions fees, much of which is needed to cover fraud. Banks also charge significant fees, and transactions costs are too high to make micro-payments feasible. Depending on how the verification/mining system is set up, the cost of writing transactions on a blockchain can be very extremely small. If the ecosystem becomes large, many transactions can take place without ever having to contact real space. Employers can pay wages, companies can pay invoices to vendors, ordinary people can pay their utility bills and so on. Small transactions such a buying a newspaper, paying for access to web content, paying a bus fare or a parking meter, can stay within the system and then be transferred out later to the real world as a unit if needed. Money only needs to move in or out of the CryptoBuck system if one of the parties to a transaction has no PKA.

A third advantage is that even in this simple form, the CryptoBuck system allows for a great deal of anonymity and privacy. Some might argue this is a bad thing. It facilitates tax evasion and money laundering. This is a deeper policy and philosophical question. We explore this in more detail below.

The Case for Privacy and Anonymity

As the financial system stands now, tax evasion and the black economy are huge in many countries. Although the US has relatively low rates of tax evasion, this is largely because we have a culture of compliance and not because of careful monitoring and auditing of the financial system. It is estimated that approximately 70% of US currency is held overseas. Some of this is because US dollars are a better store of value than local currencies, but most is to facilitate off-book or criminal transactions. Cash only works in real space, but bitcoins and anonymously purchased gift cards make it possible to conduct untraceable transactions online. The point is that the current financial system does a poor job of preventing illegal activity. Those who wish to hide their transaction do not have to go to very much effort to do so.

Nevertheless, the existing financial system is tightly regulated and supervised. Even if it were not, there are only two Automated Clearing Houses (AHC) in the US that facilitate all interbank transactions (direct deposits, billpay, checks, and everything else involving a bank account), and Visa, MasterCard, and AmEx together handle about 95% of all US credit card transactions. In other words, five companies collectively know essentially all transactions made by every American.

Americans pay a very high cost in loss of privacy due to government regulations and the extreme centralization of their financial records. They get very little in return. The current system allows for easy financial monitoring of generally honest, ordinary people who do not take the small amount of trouble to hide their transactions. Anyone with real criminal intent can easily sidestep the system. These privacy costs will grow as systems are become able to do sophisticated analytics on big data, and the potential downsides of this information being used in the wrong way are frightening.

This suggest that it may be good policy to allow a greater degree of anonymity in financial transactions than we have today. Identity theft, credit card fraud, and large-scale hacks of financial data are an integral part of the current system. Moving transactions to a public blockchain would be far more secure in these regards, would protect the privacy of ordinary people, and we suspect, would not greatly increase the criminal uses of the financial system.

Privacy and Anonymity in Practice

The United States government is very concerned about terrorism. US banks are required to comply with know your customer (KYC) and anti-money laundering (AML) laws largely as a result of the USA Patriot Act of 2001. Similar requirements have been since enacted in the majority of countries to combat crime and tax evasion as well as terrorism. Failing to comply can result in large fines.[3]

Cryptocurrencies such as bitcoin make enforcement of these types of regulations difficult. Given the decentralized nature of the blockchain, there is no agent that can be forced verify the identities of users.[4] As long as transactions stay on the blockchain, everything is fine. However, moving money in, and especially out, of bitcoin is more problematic. The easiest and lowest cost ways of converting bitcoin to fiat currency involves banks or other real world financial institutions that must comply with KYC and AML rules.[5]

Ripple[6] is a very successful blockchain company that have ventured into fiat currency. Ripple is a real-time gross settlement system (RTGS) which facilitates currency exchange and remittance transfers using a consensus ledger approach. The ledger contains records of transactions between members of its network denominated in dollars and other currency units. Since transactions go both directions, the net amount that needs to be settled at the end of the day is much less the gross volume. The is means that if banks and other agents on Ripple are willing to trust one another to a limited degree, they can avoid the cost and delay of using wires for each transactions, and make relatively cheap and rapid transactions on the blockchain. When settlement on net balances needs to be made, it can be accomplished by a single wire.

[3] For example, the US fined BNP Paribas $8.9B for violations of AML regulations.

[4] It should be mentioned he structure of bitcoin's protocols limit privacy and anonymity. The nature of it public blockchain makes it possible to infer about users by looking at record of transactions. The Ethereum protocol does a much better job of protecting user's privacy and anonymity.

[5] There are more elaborate ways such as selling on EBay, meeting someone in person using Craig's list, going to local bitcoin group meetings to buy and sell, having an online merchant who takes bitcoin send you merchandise that you can resell, etc. All of these have high transactions costs and some are risky.

[6] Ripple also has a native crypto-token that is used to prevent spam transactions, facilitate transfers and exchanges, and which can be used to represent gold, securities, or anything else that users might wish to trade. See Ripple.com for more details.

Originally, Ripple allowed individuals to transfer remittances internationally. The transactions fees that workers must be pay to send part of their earnings home are very large. This seemed like a natural and socially beneficial service to offer. Unfortunately, this put Ripple in violation of Bank Secrecy Act and it was fined $700K. Their response was to stop dealing with individuals and focus on banks who already were in compliance with the necessary regulations.

Tether[7] is another interesting startup that is very similar to CryptoBucks. They offer a cryptocurrency that is tied to dollar and backed one for one with deposits in accounts in two banks in Hong Kong and Taipei. Taking a lesson from Ripple's experience, Tether has registered in the US as Money Services Business, complies with Hong Kong's version of KYC and AML, and is attempting to establish corresponding relationships with US banks. How far they will get is unclear. On the one hand, they are attempting make connections to the real world banking sector and to be compliant. On the other, they are a Hong Kong based company and it may be difficult for the US Treasury department to fully verify compliance. Users may be reluctant to trust the Chinese government to safeguard the deposits that back up Tether, or the legal framework under which they would have to seek redress. In any event, there is no attempt to keep the identity of users transferring money out of Tether and into the real world banking system private.

The lesson here is that navigating the interface between the real and the virtual with any sort of crypto-token is perilous. Governments might not be able to enforce any rules within the CryptoBuck system, but it could forbid any contact with real world banks under its jurisdiction. Determined users could probably find workarounds. For example, a blind intermediary known and properly identified to the bank could purchase CCCs and send them to anonymous email address where they would be picked up by customers. The government would have to be able to distinguish such intermediaries from other bank customers if it wished to prevent this. If any country chooses not to enforce the KYC rules, its banks could issue CCCs for use by customers living in more restrictive countries. Customers would need to find a way to transfer funds to the foreign bank, and also move money from the foreign bank to a domestic one. The restrictive country might try to cut the foreign bank off from its domestic banking system, but to do so, it would have to sever links with any bank

[7] About $50M "Tethers" are in circulation as of April 2017. See tether.to for more details.

or country that was willing to transact with the nonrestrictive bank. In the end, this adds transactions cost, but for those who really are engaged in illegal activity, this is simply and inconvenience.

Problems with the CryptoBuck System

Entering or exiting the CryptoBuck system means interacting with the real world banking system. Fees may be involved, but adding more corresponding banks to the system would create competition to at least minimize these. The fact that inbound and outbound transactions are highly automated cryptographically verified electronic orders that can be directly ingested and processed by a bank with no human intervention should also help. Nevertheless, sending a physical check, having a teller put money into the hands of a customer, fees banks must pay to make EBTs, etc. are real cost, and the CryptoBuck system does nothing to reduce them.

There are a number of other weakness in the system, some of which are easily solved, and others that are more challenging

1. Customer must trust that the CCC given by BMB is genuine and will be honored.

Of course, this is a problem that already exists in the real world. Trusting a BMB to honor its CCC is not much different from trusting it to honor a paper cashier's check. Since a CCC is generally held for only a few minutes as the transaction through CBI clears, the risk is substantially smaller. In addition, If BMB rejected a signed, verified CCC, it would become obvious at the ending of the current interval. It would also be provable that BMB was committing fraud and it would not be allowed to participate in the CryptoBuck system until it made good. The benefit of committing this type of fraud is low compared to the cost. Note that Ripples' approach ultimately requires that the participating financial institutions agree to recognize the entries on the block chain as representing real world financial obligations. This means that trust must be extended for days or longer.

2. In the longer run, BMB holds all the real dollars backing CBI's CryptoBucks and promises to pay them out following verified instructions from CBI. BMB might commit fraud, embezzle, or go out of business.

This is a problem that already exists in the real world. It might be addressed by requiring the CBI purchase private deposit insurance, or that the BMB submit to transparent electronic auditing standards. Tether probably started in Hong Kong because of the difficulty finding a US bank willing to take on the risk of dealing with a cryptocurrency. If trust in the US and Hong Kong financial and legal systems are the same, then the observations above apply. Otherwise, users of Tether must assess the additional risks.

3. If a customer purchases a CCC using a check, credit card or bank transfer, he reveals his identity to the BMB and this can be linked to the specific CCC issued. CBI, on the other hand, knows the PKA to which any CCC is credited, but not the name of the owner. Unfortunately, the pooled information links the customer to a PKA. For outbound transactions, the CBI knows sees the ciphertext of the instructions going to the BMB. BMB sees the ciphertext, and when it reads the cleartext, it sees the name on the account to which it is deposited or the name of the person for whom it is used to pay a bill. This creates at least a probable connection of the encrypted instruction to a person, and pooling information with CBI, connects the person to the PKA.

This could be addressed in a number of ways. The most direct is to make it part of the verifiable CryptoBuck protocol that once a CCC is cashed, all data linking it to a transaction is deleted. The same could be done to the ciphertext instructions to the bank on outgoing transactions. More sophisticated zero-knowledge transactions strategies could also be used. On the real world side, customers could use intermediaries as outlined above. This would allow them to purchase CCCs without linking them to their identity. This would require that the intermediary be trusted, or that the intermediary accept cash or forms of payment that could not be linked to the purchaser. It would also require that the customer trust the intermediary long enough for the transaction to be completed and confirm that a genuine CCC was delivered. However, since the customer transfers the CCC to a PKA almost immediately, this trust only needs to last for several minutes. Again, the benefits of such a small potential theft compared to the cost of being cut out of the CryptoBuck system make this type of dishonesty a poor choice.

4. The set of transactions recorded in the CryptoBuck blockchain might give clues to identities.

For example, it might be that a company makes its PKA public or that it is somehow discovered. If this company makes payments each month to a certain PKA in a certain amount, it might be possible to infer who owns the receiving PKA by seeing who is employed by the company and is making that salary. The fact that a PKA transferred X dollars out of CBI and a specific bank received an order to disburse exactly X dollars also could create a link. If there are enough transactions per time interval, however, it would be difficult to make clear identifications since many transfers in the amount of exactly X dollars are likely to have been made. Machine learning techniques might be able to find patterns of transfers that allow inference of the identities of PKA owners. To minimize such possibles, CBI could randomly delay writing transfers for a small number of intervals. Alternatively, a more complicated system of CBI intermediates could be set up. A user could make transfers from one or several PKAs packaged with encrypted instructions (readable by the intermediary) to create the intermediary's PKA. The intermediary could then create corresponding outgoing transactions to BMB or another PKA. There would be no way to link the originating and terminating PKA except the through the encrypted instruction set. As long as the intermediary does not reveal a cleartext version of the instructions, discards the instructions, or changes PGP pairs regularly and verifiable destroys the old key, no connection could be made.

More General Concerns

Three additional problems remain that hold for any cryptocurrency.

The first is the problem of key security. As long as the private key is known only to the owner of a PKA, only he can order transfers. However, there are far too many cases of keys on exchanges being discovered by hackers, or of individuals revealing or losing their keys. A better infrastructure needs to be found in general before any system using PKAs can hope to gain wide-spread use.

The second problem is making the system easy to use. In effect, cryptocurrencies operate like debit cards. If someone has the functional equivalent of a PIN, they can make transfers which cannot be reversed. A customer needs to able to use a card, a biometric, or a device, to create a transfer order, even for very small amounts, automatically. They need to know their balances and be able to prove that certain outgoing transfers were made (receipts). They may also need to know source of some incoming transfers so that they can reconcile accounts receivable. Creating hardware and interfaces that facilitate these things securely is a challenge, but hopefully not an insurmountable one.

The third problem is how to cover the system's costs. Block builders need to be compensated, private deposit insurance might have to be purchased, and a fund might need to be established to cover certain cases of fraud or bank default, for example. One source funding is the deposits that CBI has at BMB. These should be interest-bearing, but highly liquid accounts. For example a CBI that issues $100M in CryptoBucks would earn $1M per year at even 1% interest. This by itself may be enough to support the ecosystem. Alternatively, small fees could be attached to each transaction order. BMB will set its own fee structure to pay for issuing checks and running its physical infrastructure. A small extra fee could be added and kicked-back to CBI to pay expenses, There are other approaches a well, but the CryptoBuck system will have to generate ongoing revenues to pay for operations.

Conclusion

The CryptoBuck system outlined in this paper solves the problem of volatility that prevents existing cryptocurrencies from serving as a store of value. At the same time, it exploits the advantages of cryptocurrencies over real currencies as mediums of exchange. In particular, CryptoBucks do not require that any single agent or institution be trusted to keep an honest ledger, has low transactions costs, and offer increased security to customers. Within the bounds allowed by government regulators, CryptoBucks allow users to protect their private financial information from being revealed to anyone.

The technical elements needed to set up the CryptoBuck system all exist, and the only real challenge is getting regulatory permission for real world banks to be correspondents with CBI. With that accomplished, CryptoBucks have the potential to displace our current expensive and insecure financial system.