Fedcoin

A Blockchain-Backed Central Bank Cryptocurrency

Sahil Gupta

sahil.gupta@yale.edu

Patrick Lauppe

patrick.lauppe@yale.edu

Shreyas Ravishankar

shreyas.ravishankar@yale.edu

Advised by Dr. Joan Feigenbaum

Dept. of Computer Science

Yale University

5.10.2017

1. Abstract

In the latest instance of software eating the world, cryptocurrencies were created with the intention to make central banks, the traditional bastions of monetary policy, redundant in the face of a peer-to-peer electronic cash. But there is no small irony in the fact that nine years after the publication of the Bitcoin whitepaper, cryptocurrencies may be best utilized by the very institutions they were meant to subvert.

Blockchain, the distributed ledger technology underpinning Bitcoin, is the tool that can be extended to a central bank cryptocurrency. In this report, we propose that the Federal Reserve, the central bank of the United States, create a blockchain-backed digital coin called *Fedcoin*. As legal tender along with the U.S. Dollar, Fedcoin has the potential to be a “good money,” in that it can have a stable long-run store of value and a stable short-run rate of return – assured by the Fed enforcing a 1:1 exchange rate with the dollar.

Most of our money is digitized already, whether in bank reserves with the Fed, or in checking accounts at the local bank. Only a fraction of our money supply is in paper dollar bills in circulation. But our digital money, locked up in private ledgers and exchanged through dozens of heterogenous databases en route from creditor to debtor, lacks the speed, stability, scalability, and security of a good cryptocurrency. A successful Fedcoin would make bank notes, credit card companies, and Bitcoin obsolete, while transforming the nation’s medium for money.

This report presents a proof-of-concept central bank cryptocurrency, and the accompanying codebase simulates users making transactions on an active blockchain. Fedcoin improves on Danezis and Meiklejohn’s RSCoin – a cryptocurrency framework – with a Node.js implementation, a permissioned public blockchain, a system to maintain KYC rules, and a plan to provide anonymity with zero-knowledge proofs. Consensus does not come from proof-of-work mining, but from a Two-Phase Commit where the central bank relies on a decentralized set of authorized nodes to verify transactions and prevent double spending. Under federated consensus, transaction throughput and settlement latency are more than two orders of magnitude higher and lower than under Bitcoin, respectively.

2. Introduction

2.1 Cryptocurrency and Blockchain

A *cryptocurrency*, a subset of digital currencies, is a medium of exchange that depends on cryptography to secure transactions and to control the creation of new units of currency. A *protocol*, more generally, is a payment system or a set of rules for crediting accounts. Meanwhile, a *blockchain* is a data structure that serves as a public digital ledger and is shared across a distributed network of computers. As an immutable record, it stores transactions in the form of a time-ordered series. The blockchain protocol describes a chain of *blocks*, where a block is a group of transactions that have been sealed and added to the existing chain at the same time.

Any participant in the blockchain network can add a new block to the chain, as long as a majority of the other participants in the network ratify the addition. When a node proposes the addition of a new block, the other nodes check the blockchain transaction history to ensure the new transactions proposed are valid. If a majority of the network approves the new block, it is appended to the last block in the blockchain, increasing the length of the chain. The newly added block contains a hash of the contents of the block to which it is chained, which timestamps the block in the chain. Every new block is guaranteed to have appeared chronologically after the previous block, because the previous block's hash value would be otherwise unknown. The network only considers the longest chain (the chain with the most blocks) at any given point to be the working blockchain, which is continually ratified by at least 50% of the network. This stipulation, along with "proof-of-work" (computationally intensive hashing puzzles), makes it near impossible to double-spend a coin or modify a transaction once added to the ledger. The example proof-of-work problem in the Bitcoin white paper "involves scanning for a value that when hashed… with SHA-256, the hash begins with a number of zero bits."[2] This is an especially useful problem because "the average work required is exponential in the number of zero bits required," which means the difficulty of the problem can be scaled up easily, and because the solution in constant time "can be verified by executing a single hash." The first node to solve the hash puzzle is rewarded by the network with newly instantiated currency, increasing the money supply.

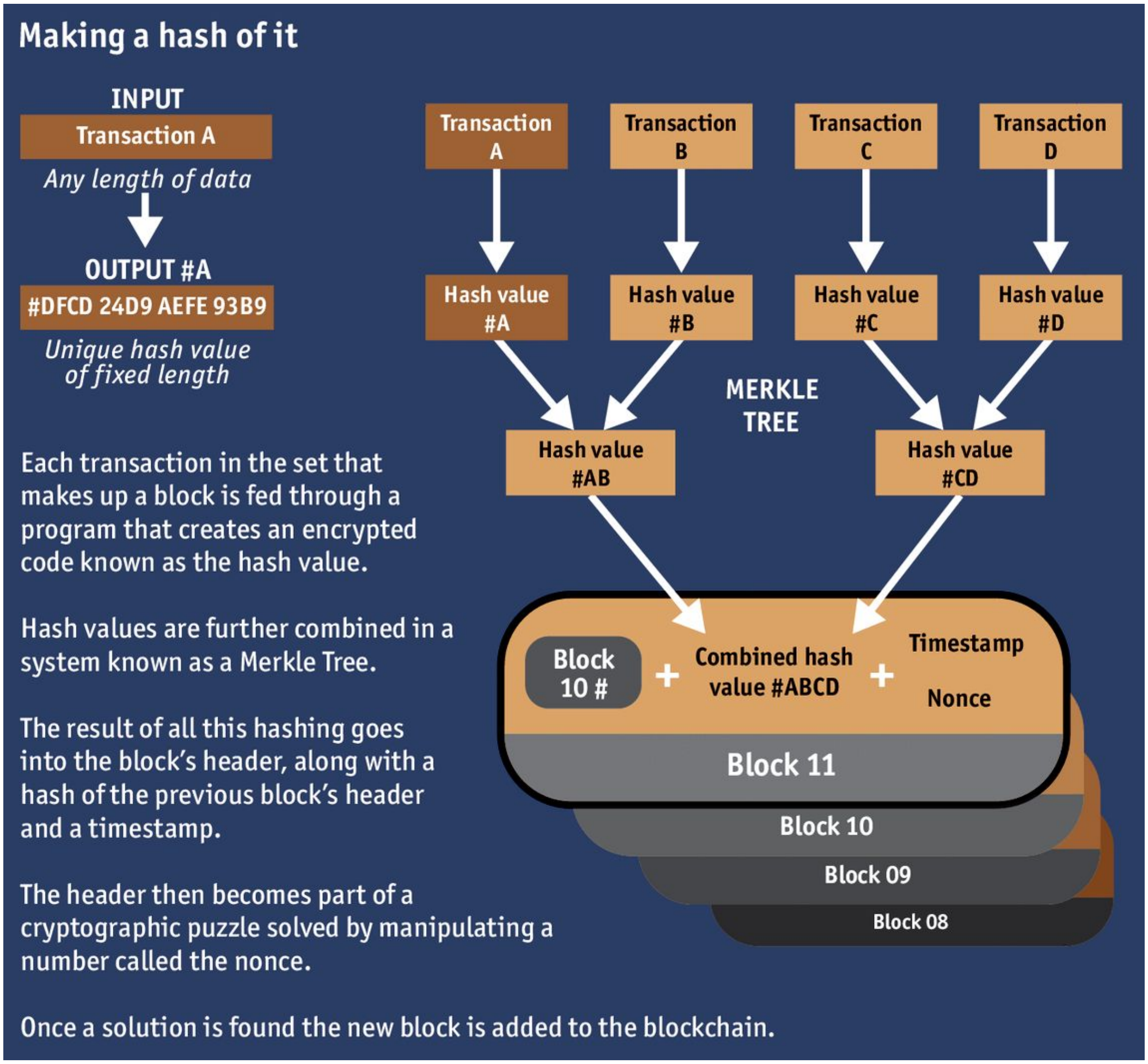
The blockchain protocol was first proposed in 2008 in a white paper entitled "Bitcoin: A Peer to Peer Electronic Cash System," by the mysterious Satoshi Nakamoto.[2] The paper argues it is possible to replace centralized authorities that verify currency – commercial and central banks

– with a decentralized public blockchain of transactions. People trust that dollars used in everyday monetary transactions have value because they are guaranteed by the Federal Reserve, because they can be used to pay your taxes to the U.S. government, and because it is impossible for anyone to spend the same dollar more than once. A blockchain can offer trust in a currency system and solve the double-spending problem, sans central bank.

A coin on a blockchain refers to the "chain of digital signatures" that make up the history of a transaction, where an exchange is a transfer of control of coins from the sender's wallet to the recipient's wallet.[2] The money transfer protocol for user X to transfer coins to user Y is as follows: user X's coin client arranges a set of prior transfers to X which, when added together, are of equal or greater value than the intended value to be sent to Y. If the value of prior transfers is greater than the amount to be sent, then X transfers the "change" value back to a new address of his own. Note that an address is a hashed form of a public key. X proves these transfers are genuine by signing them with his private key, affirming in a publicly verifiable way (via public key) that X and only X chose to execute the transaction. Accordingly, any transfer of currency contains the evidence that the transferor has the funds to backup the transaction.

A wallet is a cryptocurrency analogue to a conventional bank account. Wallets allow users to receive, store, and send digital money relying on public key cryptography. Wallets can generate new public-private key-pairs anytime, and reveal no information a priori on the identity of the user operating it.

As a single shared ledger, blockchain has the potential to solve the fragmented chaos of the modern financial system. With a single source of truth, transactions enjoy instant settlement instead of taking days, because payment *is* settlement -- which means improvements in transaction time, cost, transparency, and security. Recording, clearing, settlement, and reconciliation across multiple organizations are collapsed into one step.[9] Now what if money backed by the full faith and credit of the U.S. government were on a blockchain?



Making a hash of it

Each transaction in the set that makes up a block is fed through a program that creates an encrypted code known as the hash value.

Hash values are further combined in a system known as a Merkle Tree.

The result of all this hashing goes into the block's header, along with a hash of the previous block's header and a timestamp.

The header then becomes part of a cryptographic puzzle solved by manipulating a number called the nonce.

Once a solution is found the new block is added to the blockchain.

[8]

2.2 Literature Review of Fedcoin

A discussion of Fedcoin must ironically begin with an accounting of Bitcoin's flaws. Volatility is one serious problem, and is the currency's major hurdle to becoming mainstream. Speculators have the most to gain and lose, as do the world's poor if they make the unwise choice of investing in a currency whose value could fluctuate in double digit percentages by the day. Wild capital gains (or capital losses) on a zero interest-bearing asset leave much to be desired.

Anonymity is another risk, since black market transactions can take place without notice. While the blockchain is public, only addresses and amounts are, not identities (much like the internet protocol). While the *flow* of funds may be traced, neither their source nor the destination can be known for sure (or recovered should law enforcement need to). Payments are irreversible, structurally.

The centralization of Bitcoin is yet another problem. With a few major players with the fastest mining hardware confirming transactions, there is little incentive to run a node. In light of this trend, Bitcoin might lose its most valuable proclaimed asset: its distributed architecture. Plus the computational process of mining, which involves solving exponentially harder cryptographic puzzles, is a massive and wasteful use of CPU cycles and electricity.

Bitcoin mining is also slow, processing a peak of 7 transactions per second – a stark contrast to Visa's 50,000+ per second. At Bitcoin's block generation rate, transactions take at least ten minutes to verify, while some even get dropped. The world needs a money processing system to scale to its size and Bitcoin remains woefully underpowered.

The current low fees to get one's transaction verified will be far more expensive in the long run, because fees are subsidized by the network awarding miners new currency, which will go to zero as the money supply hits it limit, driving miners to monopoly.

Lastly, the 21 million coin fixed money supply presents a serious danger. By realistic measures, the money supply will flatline around 2025, turning the currency into an asset like gold to sit on and hoard. Fixed money supplies never work, as history shows. Spikes in demand cause unexpected deflationary events (whether via holiday shopping or a recession), and no elastic monetary policy would be in place to increase the supply of money during crisis to alleviate pressure, smoothing out price level effects.

In brief, Bitcoin suffers from volatility, liquidity limits, mining oligopoly, mining inefficiency, poor scalability, network latency, inability to handle micropayments, and the absence of monetary policy. We discuss these disadvantages further in Section 4.

Fedcoin begins with a blockchain created by the Federal Reserve, the public monetary authority in control of the production of money and formulation of monetary policy. The Fed would bless this ledger with certain properties: only the Fed would have authority to create and destroy ledger entries (i.e. Fedcoin), the Fed would use its creation and destruction ability to provide conversion between both its liabilities (the dollar and the Fedcoin) at a ratio of 1 to 1, and all Fedcoin transactions would be announced to a decentralized network of nodes for verification. In this way, non-Fed nodes would be responsible for the integrity of the ledger, while the Fed would bear responsibility for the integrity of the Fedcoin value, which would be anchored to the dollar. Should a paper note or reserve entry be destroyed, a Fedcoin would be instantiated, and vice versa.[5]

A cryptocurrency could structurally benefit from a central bank, and this is where Fedcoin shines. In the day-to-day use case, Fedcoin would be a sort of Fedwire for all.[5] Fedwire is the real-time gross settlement system between banks to transfer reserves among each other. It is a utility provided by the Federal Reserve, but if an equivalent service were open to citizens, one might have a direct account at the central bank, like a modern U.S. Postal Bank.

Janet Yellen and company need not worry about the blockchain impeding Fed monetary policy, because they do not cede control over varying the quantity of reserves or even interest paid on reserves. While the Fed still has the ability to perform quantitative easing, change the reserve ratio, or update the discount rate, the market could independently demand whatever balance of cash or Fedcoin it needed.

Moreover, digital cash has the advantage of eliminating the Zero Lower Bound problem that central banks currently face, which stems from the existence of paper currency. When short term interest rates are near zero, a central bank's ability to inject monetary stimulus by cutting interest rates is neutralized. People would prefer to withdraw cash from the formal banking system and hold onto paper currency than to subject their holdings to a negative interest rate. This severely restricts the powers of a central bank to jolt an economy out of depression, but the widespread use of a digital currency like Fedcoin would overcome this.

There is a major distinction between management of the money supply and the protocol in place for transferring value across accounts, but an immutable and permanent record of the national series of transactions would provide invaluable information and real time information on monetary policy. Transparency about cash flows would offer the Fed and the world the most ripe data set for analysis ever seen. Denial of service attacks would be much more unlikely, thanks to the difficulty of taking down a decentralized system. Peer-to-peer transactions of dollar amounts could take place at a fraction of the cost they do now. Even more, the public could shift their savings out of commercial banks and move their fiat directly into a blockchain account with the Fed, or in a private wallet. Anyone with an internet-connected device could digitally transfer value.

According to a Bank of England report, central bank digital currency issuance of 30% of GDP could permanently raise GDP by up to 3%, due to reductions in real interest rates, distortionary taxes, and monetary transaction costs. The central bank would also be more able to stabilize booms and busts of the business cycle.[6]

Identity, however, places no small burden on the design of such a system. KYC ("Know Your Customer") and anti-money laundering regulations would place restrictions on Fedcoin transactions. Imagine users sending Fedcoins to countries against whom economic sanctions have been placed. Fedcoin thus cannot be treated like cash because at least cash has the difficulty of shuttling bills across borders. In addition, many foreign countries currently using the U.S. dollar as the de facto currency (in place of their own volatile one), might be keen to adopt Fedcoin – yet again complicating KYC rules.

With Bitcoin, only the address of a coin is public while the identity of the transactor is private. In addition, addresses can be created on demand, so a law enforcement agency identifying an address will not necessarily lead to the tracking down of an individual. With Fedcoin, a KYC restriction might require every transactor to have an account with the central bank, preventing total anonymity. In Section 4.6, this paper proposes a compromise between total privacy and law enforcement capability with a key management system. *Confidential transactions* which obscure amounts but not addresses and *zero-knowledge proofs*, as implemented in the altcoin Zcash, are also investigated as tools for confidentiality. Zero-knowledge proofs, for example, offer the ability to prove the truth of a statement, such as proof of assets, liabilities, and solvency all without revealing an address – which would compromise an individual's purchases, a bank's trading strategies, etc.

Nations such as Senegal, Ecuador, and Tunisia have beaten the United States to the punch in implementations of blockchain currencies, but with the power of hindsight as well as careful forward-looking technical and legal analyses, the U.S. has a rare opportunity to upgrade the nation's money.

2.3 Fedcoin in Detail

As a central bank cryptocurrency, Fedcoin will be a universal, electronic, 24x7 liability to the Fed's balance sheet. The use of a blockchain is essential to guarantee the resiliency of the system. Note that blockchain is at its core a data structure and does not have to be a distributed ledger. Fedcoin will not need the blockchain for consensus, because it relies on existing trust in the institution of the central bank.

Such a system could be implemented with the central bank maintaining the blockchain, public institutions maintaining copies of the ledger, or private sector agents doing so. Here we propose a *hybrid* model where the central bank primarily controls money supply, while it relies on a decentralized set of authorized nodes (Nodes) to verify transactions and prevent double spending. Nodes will be commercial banks. Under this regime, the expensive proof-of-work required by a cryptocurrency like Bitcoin can be avoided, while the permissioned ledger will dramatically reduce settlement latency. Fedcoin will thus offer high throughput and leave monetary policy under central bank control, building on Danezis & Meiklejohn's RSCoin.[1]

This paper augments their framework with a central bank cryptocurrency implementation in Node.js, a permissioned public blockchain, block production, a central bank operator, a system for adhering to KYC rules, and a plan to provide anonymity on the public blockchain for users using zero-knowledge proofs. This offers a significant advantage over Bitcoin's pseudonymity, where addresses and identity unlinkability is not guaranteed.

Ultimately, our proof-of-concept Fedcoin will offer speed, stability, scalability, and security and demonstrate this technology's potential to be the country's financial backbone. As per the Fed's guidance on distributed ledgers,[7] Fedcoin will

- Improve end-to-end processing speed and availability of assets
- Decrease need for reconciliation across many recordkeeping infrastructures
- Increase transparency and immutability in transaction recordkeeping
- Improve network resiliency by distributed data management
- Reduce operational and financial risks

3. Design

3.1 Source Code

Fedcoin's source code will be introduced before its architecture, for the benefit of readers already familiar with RSCoin. The prototype is available for download on Github, and its README offers steps to download the repo and run the simulation locally. Node.js was chosen as our runtime environment because it uses JavaScript across the stack, supports convenient package management with NPM, and was built to handle asynchronous I/O from the ground up, which was absent from the Python implementation of RSCoin.[1] Transaction, verification, and block generation will be non-blocking, to avoid bottlenecks in each of the three areas.

Key app logic resides in *app/fedcoin.js*, *app/blockchain.js*, and *app/world.js*, with the major technical achievements described below.

app/fedcoin.js

- Implemented Algorithms V.1, V.2, and V.3 from Danezis and Meiklejohn [1]
- Completed classes for User, Node, CentralBank, Vote, Addrid, Tx, and Wallet
- Developed a simpler concept of sharding, where each Node and each Addrid is mapped to a shard based on its name hash, and shard lookup is O(1)
- Optimized hashing by storing object hashes internally
    - Especially useful for fast Merkle Root calculation
- Used SHA-256 for hashing, the NIST standard
- Protected User passphrases by storing HMAC of passphrase with a secret key. Has effect of salting the passphrase and is immune to length-extension attacks
- Made architectural decision to replace RSCoin's use of Elliptic Curve Cryptography with RSA -- for signing, verification, and key-pair generation, specifically 2048-bit keys. RSCoin (and Bitcoin) relies on ECC for its digital signing algorithm, and Danezis concedes it is a bottleneck in verification speeds
    - *Key Generation:* ECC outperforms RSA at all key lengths. But this cost is tolerable because key generation can occur when wallets are idle
    - *Key Size:* ECC offers same security for smaller key than RSA, but trivial here
    - *Sig. Generation:* ECC and RSA are equally quick

    - *Sig. Verification:* RSA dramatically outperforms ECC. Solves Node bottleneck
- Separated addresses from public keys. If RSA is broken in near future, then Users' private keys are protected by hash algorithms RIPEMD-160 and SHA-256
- Used JavaScript Promises to prevent blocking during two-phase commit
- Developed a Deterministic Wallet
    - All keys are derived from a single string, the seed. Enables User to restore wallet and private and public key-pairs should the wallet be lost
    - Wallet manages used keys, hydrated keys, and spare keys
    - Wallet auto-generates spare keys when it detects User is running low, to prevent buffering during high volume transactions
- Implemented Node generation of low-level blocks at the end of an epoch
    - Epoch length is determined by a fixed number of transactions, not a fixed time
- Implemented CentralBank validation of low-level blocks, authorization to print money, and generation of high-level blocks, unlike original RSCoin paper

app/blockchain.js

- Built blockchain from scratch, with ability to add, verify, and output blocks. Not implemented in original RSCoin paper

app/world.js

- Initialization of 2 disjoint sets of Users, Nodes, and a CentralBank
- Nodes are split between 2 shards
    - In the extreme case, if there were 1 shard, then every tx needs a majority of all Nodes for verification. If there were (# Nodes) shards, then every tx just needs 1 Node to verify, which is unreliable
- Fed prints money and seeds 1 User in each set
- Simulation begins and Users start a cycle of transactions in their set
- Cycles execute asynchronously waiting on Promises of completed transactions
    - Transactions can be chained, unlike with credit cards
- When this file is run via the command line, the console logs initiation, queries, commits, votes, and blocks generated
- After a certain number of txs, Users pause and Nodes write their blockchain to text files

3.2 Federated Consensus

In the RSCoin design, which we augment for Fedcoin, consensus is achieved with a Two-Phase Commit (2PC).[1] Nodes listen for *query* and *commit* messages from clients to whom they are mapped. This address mapping is the result of a *sharding* of the total address space, with multiple Nodes assigned to each shard. Nodes will check for double spending. The algorithms involved are more specifically outlined in Danezis & Meiklejohn.[1]

Participants

- Central bank (CB)
    - Monetary authority
    - The only trusted entity in the network
    - Root of trust
- Authorized nodes (Nodes)
    - Institutions authorized by the central bank for validating transactions
    - May be commercial banks like JPMorgan, Bank of America, Citibank
    - “Mintettes” as described by Danezis & Meiklejohn
    - Nodes exist for input (sender) and output (receiver) addresses
    - Not trusted to degree of central bank, because misbehavior can be audited
- Users
    - Fedcoin holders who send and receive transactions (txs)

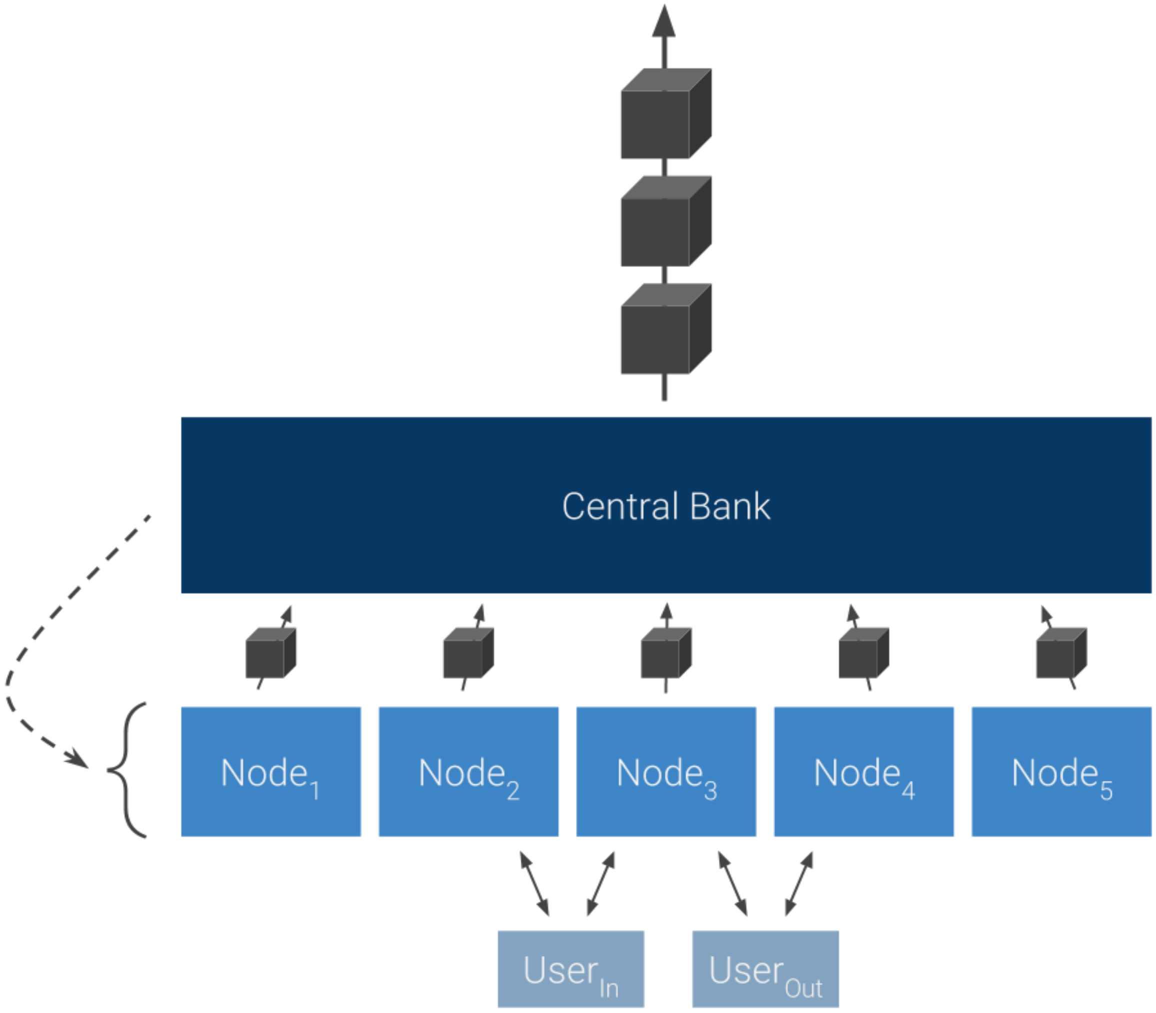
The key assumption here is that each tx is processed by a subset of Nodes with an honest majority, using lists of unspent tx outputs (utxos). We continue discussion of 51% attacks and our threat model in Section 4.8.

Functions of Participants

- CB
    - Authorization of Nodes for period of time using public key infrastructure (managing digital certificates) by signing the public key of the Node, and each low-level block must contain one of these signatures to be valid

    - Form high-level block every unit of time called a *period*, from a set of cross-hashed low-level blocks sealed by Nodes by building unique set of txs (every tx will appear in multiple low-level blocks due to sharding)
    - Verify that each tx has been included in low-level blocks by a majority of Nodes mapped to the tx output address
    - Allocate reward fee to Nodes for processing txs, with a bonus to faster Nodes
    - Audit Nodes periodically
    - Manage supply of money
- Node
    - Certify there is no double-spending in txs for input addresses to which the Node is assigned. Double-spending occurs in txs when the same input address is linked to multiple output addresses
    - Coalesce txs into own low-level block every unit of time called an *epoch,* and send a commit to user that tx will be included in high-level block
    - Provide low-level blocks to CB to then form high-level block
    - Pursue incentive for private orgs to invest in fastest, most secure infrastructure
    - Does not directly interact with other Nodes, but has cross-hashing for others' low-level blocks, a form of indirect communication between them
- User
    - Query Nodes for proof that Fedcoin sender did not double-spend
    - Commit the proof to receiver's Node in order to receive digitally signed confirmation that tx will be included in high-level block
    - Note that txs are divided between Nodes into shards, where each tx is processed by a subset of Nodes

The diagram below maps out the logical flow of information during a transaction between two users, processed by their Nodes, and sealed by the Central Bank. (Node_1 and Node_5 are idle.)



1. User_{In} wants to pay User_{Out} so begins 2PC with the set of Nodes mapped to the shards of User_{In}'s addresses. He queries that the input addresses are unspent and gets votes on their validity. That bundle of votes is then committed to the set of Nodes mapped to the shards of User_{Out}'s addresses, to get proof the tx was saved in a low-level block.
2. Nodes collect user txs and seal them in a low-level block every *epoch*, to then post the block to the Central Bank.
3. The Central Bank validates the in-order queue of low-level blocks it has received during the *period*. At the end of *period*, the Central Bank first notifies all Nodes to halt generation of new low-level blocks (see dotted arrow). The CB then seals the unique validated set of global transactions in a high-level block in the publicly visible blockchain. Once sealed, the Central Bank notifies Nodes to resume low-level block generation.

3.3 Fedcoin Properties

The implemented prototype maintains the following properties thanks to the RSCoin framework.[1]

- No double spending -- Guaranteed by two-phase commit (2PC)
- Non-repudiable sealing -- Nodes are held to their confirmation promises by users when they provide receipt of a “commit”
- Auditability -- Using a rolling hash chain of tx verification, Nodes cannot retroactively modify or omit txs in the blockchain
- Exposed inactivity -- Participants record all entries every time a *query, commit,* or *closeEpoch* takes place in the 2PC protocol
- Irreversible transactions -- Chargebacks (return of funds from seller to buyer) are impossible
- Privacy -- User’s finances are invisible to the public when a new address is generated per incoming tx. However, some linking is possible for multi-input txs, which reveal their inputs were controlled by the same user
- Security -- User’s wallet holds encrypted funds, and all txs must be digitally signed
- Fungibility -- All coins are equal and have the same value, though can be white/blacklisted
- Decentralization -- Unlike the distributed set of Bitcoin nodes, Fedcoin nodes will be a decentralized group of trusted institutions selected by the central bank. All authorized nodes are equal, none having more control over txs or the system than other nodes

3.4 Scalability

From Danezis & Meiklejohn’s scalability analysis,[1] let

N = # of Nodes T = set of txs/second *K = # of Nodes that own each address*

For a tx with m inputs and n outputs, with $m > n$, a user sends and receives Km messages at most in the first phase of two-phase commit and at most K messages in the second phase. Thus, each tx requires at most $2Km + 2K$ messages. Therefore

$$Work_{Node} = \Sigma_{tx \in T} \; 2K(m_{tx} + 1) / N$$

Note this scales infinitely, because with more Nodes added to the system, the per-Node work decreases. Scalability here is defined as latency between User and Node to execute a 2PC per transaction as well as the throughput in tx/s/(# Nodes).

While the rate of Bitcoin transactions is fundamentally limited by the block size to approximately 7 tx/s, the hybrid Fedcoin model can scale to as many transactions as needed. The decentralized model of Nodes with sharding of txs enables tx verification to scale up with each additional Node added to the network by the central bank. In other words, tx speeds scale linearly, which is crucial to a national currency which must handle a national velocity of money. The solution can scale endlessly because the space of tx identifiers is divided into shards, of which each is controlled by as many Nodes as desired.

3.5 Privacy

Fedcoin as implemented has no greater privacy guarantees than Bitcoin. Namely, pseudonymity -- that addresses are unlinkable to identity while transactions are public. However, currency attempting to be legal tender needs to be more than pseudonymous. This paper proposes *confidential transactions* as a solution to preserving security while obscuring transaction values.[13] Under the implementation of The Elements Project (which uses ECC as opposed to RSA), amounts transferred are only visible to the tx participants, while still verifying that no more currency is spent than is available. *Confidential transactions* are not implemented in this prototype, yet they exist in Blockstream's production.[14] In conjunction with every user creating a new address for every incoming transaction, users can ensure a greater degree of privacy than the status quo by obscuring tx values.

Zcash is another cryptocurrency which offers insight into privacy protecting measures.[12] Unlike mixing techniques like CoinJoin which provide modest unlinkability, the zero-knowledge proofs of Zcash offer a tool for complete confidentiality.[4] Where existing anonymity-enhancing technologies only add anonymity "on top of the core protocol… Zcash incorporates anonymity at the protocol level."[3] ZK proofs offer the ability to prove the truth of a statement, such as proving assets, liabilities, and solvency all without compromising address privacy. At the same time, they support regular, traceable transactions. A free society depends on privacy, which means an agent's purchases should by default not be viewable to family, employers, thieves, or the government. Mixing techniques such as CoinJoin can limit linkability, but it is Zcash that can completely guarantee shielded txs that hide the sender, recipient, and value on the blockchain.

The key guarantee of Zcash is *unlinkability*. To be unlinkable, three criteria must be met: high difficulty to link different addresses of a user, link different txs made by the user, and link the sender to his receiver. However, this simultaneously presents a problem with KYC and anti-money laundering restrictions. Law enforcement should be able to attach identity to an address with a warrant, and government should be able to identify addresses so it can tax its people or even pay interest. How does Fedcoin address this dual dilemma?

3.6 Fed Accounts

Know Your Customer (KYC) is an ethical requirement for financial operators to identify and verify the identity of their clients. KYC also refers to Anti-Money Laundering (AML) rules, which would have to govern a legal tender cryptocurrency. These include potential liability and reporting requirements for banks that participate in high-risk txs. To avoid liability, banks must keep good records on their clients and their activities.

Bitcoin and the Fedcoin prototype guarantee pseudonymity, but we must guarantee linkability between address and identity, should a warrant be provided. The protocol follows.

To spend or receive a Fedcoin, one must have an account with the Fed. For the benefit of the underbanked, getting a Fed account should be easier than getting a bank account. The application should require certain identifying information such as name, date of birth, and proof of address. Now in every Fedcoin tx, a user requires a public key and an address -- the hashed public key. Thus this protocol mandates that every time a user creates an address, i.e. by creating a new public-private key-pair, that address be posted to his Fed account. Third-party wallets can promote compliance. The incentive is that if a user fails to post his address, his txs will not be whitelisted by the CB, making his txs unverifiable, consistently declined, and absent from the high-level blockchain. In other words, his transactions shall not pass.

Whitelisting may be optimized at the Node-level if the CB provides them the list.

In our vision of the Fedcoin system, should the government need to link an identity with an address, it must seek a warrant. This would be the only means to look up an individual’s Fed account and his addresses. The Fed will never have access to the individual’s private keys, preventing the government from spending a private citizen’s coins. It can, though, freeze coins by blacklisting his address. Different institutions are welcome to design their own checks and balances to prevent abuse of power.

4. Discussion

4.1 Goals

Due to the success of cryptocurrencies like Bitcoin, governments throughout the world have gained interest in developing their own cryptocurrencies. Russia, China, Iceland, the UK, Canada, and the Philippines have all made efforts or signaled plans to build national cryptocurrencies. In part, these efforts represent the desire of policymakers to leverage the potential efficiency gains of cryptocurrencies over the existing forms of money transfer. Additionally, these currencies are an attempt to reassert government control over monetary policy when faced with the threat of an essentially untraceable, distributed cryptocurrency like Bitcoin. It is no coincidence that authoritarian governments like Russia and China make the shortlist. Federal cryptocurrencies represent a possible means of undermining the development of distributed cryptocurrencies while introducing a form of money transfer over which governments might assert unprecedented levels of surveillance and control.

We developed a blockchain-based cryptocurrency that the U.S. Federal Reserve could adopt with a few overarching policy goals in mind. Above all, we wanted to bring the efficiency gains of blockchain technology to a broader set of consumers. As of 2017, Bitcoin and other cryptocurrencies are still a fairly fringe phenomenon in the US. While estimates of how many people transact in Bitcoin are highly speculative, the difficulty of finding businesses that will accept Bitcoin or other cryptocurrencies is still considerable, even in large cities.[18] As a result, most people are unable to transact in Bitcoin for the majority of day-to-day transactions.

Bitcoin and other cryptocurrencies are still primarily used as an investment vehicle, so much so that the IRS has recognized cryptocurrency income as investment income, rather than foreign currency income (discussed *infra*). Bitcoin's lack of general acceptance results from a variety of factors, above all its instability and the general lack of awareness and trust in the currency among the general public. Therefore a large part of what we seek to address with a federally backed cryptocurrency is lack of public trust that prevents blockchain technology from gaining the widespread acceptance it deserves.

Second, we wanted to make a cryptocurrency that would better facilitate government efforts to track transactions and identify particular users when necessary for the purpose of enforcing the law. Bitcoin's pseudonymity poses a massive threat to every government's ability to regulate and tax the economic behavior of its citizens. In the US, Bitcoin has brought into question how the government will enforce a variety of laws governing money transfers, including Anti-Money Laundering laws and the income tax laws. Bitcoin challenges the sovereign state, so our implementation of Fedcoin sought to design a system with law enforcement in mind.

Next we elaborate on the features of Fedcoin introduced above that would make its adoption by the Fed good policy. We outline the variety of technical and legal advantages that a system like Fedcoin has over the current landscape of money transfer systems in the US.

4.2 Efficiency

Bitcoin is computationally intensive due to the distributed proof-of-work consensus algorithm which requires wasteful solving of hash puzzles. Fedcoin, though, has a consensus algorithm which involves a two-phase commit involving authorized nodes relaying blocks to the central bank for final vetting. In the absence of a trustless network, Fedcoin avoids the one-CPU-one-vote trust mechanism and saves costly CPU cycles.

Having proved linear scalability, Fedcoin shows it can scale to as many users who demand it. The system is auditable, transparent, and offers a way for central banks to offload computationally-intensive transaction verification to the private sector, while guaranteeing a volume of txs on par with credit card processors.

Under Fedcoin, the Federal Reserve has substantially more control over the money supply by changing the interest rate on Fedcoin liabilities, even perhaps making it negative to stimulate the economy during a recession.[9] In addition, the Fed can perform quantitative easing depending on macro conditions as well as control the reward fee allocated to Nodes depending on their performance in tx verification.

	Credit Cards	Bitcoin	Fedcoin
Money Generation	Centralized	Distributed	Centralized
Ledger Generation	Decentralized	Distributed	Decentralized
Anonymity	Linkable	Pseudonymity	Pseudonymity
Comp. Intensity	Mid	High	Low

4.3 Network Security

Security is critically important for a centrally banked cryptocurrency and market participants will demand the network is safe from internal and external threats before making transactions. The United States Financial Industry Regulatory Authority (FINRA) offers the following questions that market participants ought to consider in a blockchain network, and our answers to these questions succeed them.

- "How are the cryptographic keys used to sign and encrypt blocks protected from unauthorized access, modification or loss throughout their lifecycle? Will keys be rotated regularly to guard against brute-force cracking attempts?"
    - User, Node, and CB private keys are encrypted locally. User private keys can also be recreated through a deterministic wallet. Wallets, whether developed by the Fed or third-parties, will encourage keys to be rotated regularly.
- "What key sizes and cryptographic algorithms provide adequate protection against attacks on the cryptographic security of the DLT network?"
    - 2048-bit RSA keys offer security for the short- and medium-term as recommended by NIST standards.
- "If a key is compromised, how will fraudulent transactions be identified and reversed?"
    - Fraudulent transactions cannot be reversed, as with cash. However, fraudulent addresses and accounts can be blacklisted (i.e. asset freezes).
- "What parties will be responsible for this? Can historical transactions involving a compromised key be trusted?"
    - The Fed is the only trusted entity in the network. Compromised keys once sealed in the high-level blockchain are irreversible, but can be blacklisted for the future.
- "What are the incentives or disincentives to ensure completeness, integrity and accuracy of the blockchain?"
    - Nodes are paid a fee by the central bank for their transaction processing performance. Moreover, Nodes should be resistant to censorship. By sharding of address space, a DOS attack on one or even several Nodes does not impact the reliability of the system.
- "Who covers the cost of fraud? Will participants be made whole? How about customers/clients?"

    - Users will bear the cost of fraud, as with cash. However, a system could be designed for handling consumer fraud loss on an appeal basis, similar to the current credit card infrastructure. While transactions cannot be reversed, a fund could be set up for at least partially reimbursing fraud losses. Plus, the government has the power to punish particular addresses, accounts, and users associated with fraudulent conduct by blacklisting them from the system or bringing legal action against them.
- "How will appropriate notifications of security events be handled with respect to varying parties (e.g., participants, clients, regulatory bodies, law enforcement or insurers)?"
    - Should law enforcement need to inspect a user's account, it should obtain a warrant from the courts. Should users want to report fraud, they should have a portal to message the central bank.
- "What methods have been considered to enhance the security of assets?"
    - Methods include deterministic wallets, Fed accounts, and multi-sig wallets.
- "What if an employee or hacker gets a hold of one of the federated keys?"
    - The Fed would issue a new block HEAD with a message that invalidates transactions signed with that particular key for blocks after HEAD - 1. With Fedcoin, there exists a very high risk of the currency going bust in that if the private key enabling the Fed to create or destroy money is stolen, the hacker could create or destroy money on demand. Counterfeiting dollars can only alter the money supply so far, but counterfeiting Fedcoins rapidly could render the currency bust. However, assets stored in wallets (local) versus accounts (remote) make the Fedcoin banking system more resilient to asset theft or seizure, digital signing resists unauthorized transactions, and the permanent blockchain prevents rewriting of past transaction history.

How does this level of network security contrast with the status quo? Today, payment cards are the predominant mechanism for monetary transfers in the United States. Plastic card purchases comprised two-thirds of in-person transactions in the U.S. in 2012 and are the primary means of e-commerce.[19] As e-commerce becomes a larger portion of retail sales in the U.S. every year,[20] the ubiquity of payment cards is likely to increase.

The growth of payment cards has come at the cost of security. The main vulnerability of credit card transaction processing comes from the time delay between authorization and settlement of transactions. When a consumer uses a debit card to buy a product from a merchant, the merchant's bank sends a query to the consumer's bank to determine if the consumer has sufficient funds in his account to make the transaction. If the consumer has sufficient funds, then the bank authorizes the transaction. However, money is not immediately transferred from the consumer's bank to the merchant's bank. There is a substantial time delay between this authorization phase of the transaction and the settlement phase, when the money is actually transferred. During this period, the merchant is required to keep track of the authorized transactions it has yet to settle, including the consumer's account information. As a result, each merchant is required to maintain a database of consumer information related to unsettled transactions.

Such merchant databases represent a major point of attack for hackers. Of course, each merchant can take a variety of cybersecurity precautions to decrease the risk of a breach, and the payment card industry has a set of mandatory security standards. Nonetheless, since each merchant is required to maintain a database of consumer information related to pending transactions, the system as a whole is only as safe as the merchant with the weakest security. Accordingly, breaches abound.

A blockchain-based cryptocurrency like Fedcoin solves this security vulnerability inherent to payment cards by collapsing authorization and settlement into a *single* step. The transfer of money happens as soon as the 2PC is complete (or more stringently, when the transaction appears in the high-level blockchain). Settlement happens in milliseconds, and the merchant does not have to store any of the consumer's sensitive information. In fact, the one piece of sensitive information -- the consumer's private key -- never transfers hands.

4.4 Stability

Volatility is one of the primary obstacles for Bitcoin on its path to everyday use as a currency by the general public. Since 2009 when the first Bitcoin client was released, Bitcoin's value has undergone major boom and bust cycles, most prominently the crash of 2013-14. After peaking around $1,100 at the end of 2013, the value of Bitcoin rapidly and then steadily declined over the course of 2014, eventually reaching a low point of around $200. In that case, the crash was linked to a warning issued by the Chinese government indicating that Bitcoin was not legal tender.[21] Other, smaller crashes have occurred as a result of the SEC's rejection of a Bitcoin-based exchange traded fund and the hacking of the Mt. Gox exchange.[22, 23] This is one of the disadvantages of a global currency: its value will react to material events in whatever countries it is held, cascading opportunities for crashes.

Explanations for this highly volatile behavior include the small supply of the currency and its widespread use as a speculative investment vehicle.[24] If volatility remains at present levels, merchants and consumers will remain wary, keeping Bitcoin at the fringes of the U.S. economy.

Fedcoin avoids the volatility problem because its value is pegged to the U.S. dollar. While not a perfectly stable store of value, the dollar is a reserve currency and is a great deal more stable than Bitcoin because it has a far larger supply and its value is actively stabilized by the Fed's monetary policy. For its stability, Fedcoin will be more trusted than peer cryptocurrencies, and merchants are likelier to accept it.

4.5 Non-Deflationary Approach

Bitcoin rewards mining at a fixed rate that halves every 210,000 transactions, or approximately once every 4 years.[25] The mining rate will eventually decrease to zero, permanently setting the number of Bitcoin in circulation at 21 million. This is the mark of a deflationary currency, since once the maximum value is reached, no further Bitcoin can be introduced into the system, regardless of whether the number of users increases.

Bitcoin's deflationary aspect makes it a bad fit for a currency backed by the Federal Reserve or any other central bank. The Federal Reserve needs to be able to adjust the U.S. monetary supply as the economy changes. Therefore, it is hard to imagine the Federal Reserve supporting a system that introduces new currency at a fixed rate that changes a predetermined amount every four years, and which will eventually level out to a fixed supply.

Under Fedcoin, the Federal Reserve has substantially more control over the money supply by changing the interest rate on Fedcoin liabilities, even perhaps making it negative to stimulate the economy during a recession. In addition, the Fed can perform quantitative easing depending on macro conditions as well as control the reward fee allocated to Nodes depending on their performance in transaction verification.

4.6 KYC and Identity

Bitcoin is a pseudonymous medium of exchange. A user can set up as many different addresses as needed, allowing him to continually transfer assets between addresses and thereby hide the fact that a single person is associated with a set of transactions. As a result, there is no obvious way for the government to link a particular address to a person. At the same time, Bitcoin addresses (hashes of public keys) are themselves public and visible to anyone. If anyone links an individual's Bitcoin address to an identity, all other transactions interacting with that address may be are compromised.

While the pseudonymity of Bitcoin provides users a certain amount of privacy, it presents a problem for governments. If a particular address cannot be traced back to a particular person, this undermines the government's ability to perform several essential roles.

First, the pseudonymity of Bitcoin prevents the government from accurately calculating an individual's tax liability. A taxpayer may have received thousands of dollars in payment through Bitcoin within a given year, but unless the value is reported on tax returns, the IRS can neither trace nor audit the payment. The IRS is likely left to rely on the records of a middleman like a Bitcoin exchange, which are required to keep records on their customers per FINCEN's guidance.[26] However, these will only take into account instances where the user has exchanged Bitcoin for USD. Thousands of Bitcoin could have accrued in wages over many years tax-free.

Second, Bitcoin's pseudonymity prevents law enforcement from tracking the movement of money in order to identify illegal activities like money laundering and drug trafficking. If law enforcement is unable to tie Bitcoin addresses to names, then it is likely to be hindered in tracking money movement for investigations.

To avoid such issues, Fedcoin is implemented in a way that allows the government to map all of an individual's addresses to his identity. In order to begin transacting in Fedcoin, a user will first have to set up an account with the Federal Reserve (more in Section 3.6). Once a user has an account, he can generate a public-private key-pair through a Fedcoin wallet that allows him to begin transacting Fedcoin.

As with Bitcoin, a user can generate as many of these public-private key-pairs as needed, allowing for the same kind of pseudonymity in Bitcoin. However, in order for the Federal Reserve to begin recognizing the transactions associated with a given address, it must be able to link that address to an account, and therefore to a particular identity. For this reason, before a user begins transacting with a particular public key and address, the user must report that address to the government to ensure that all transactions associated with that address are recognized in the central ledger. Any wallet provider will have an incentive to streamline this process, so as to prevent users from accidentally transacting with a given public-private key-pair without first reporting the address to the government. This arrangement ensures that individuals have the benefits of pseudonymity to the public, while also guaranteeing that the government will be able to link any finalized transaction to a particular person.

The inability to trace an address to a particular person is one of the serious threats that Bitcoin poses to the ability of governments throughout the world to carry out their duties. Many Bitcoin users perceive this as one of the currency's greatest strengths, and even we consider Bitcoin to be a net societal good. But Bitcoin naturally undermines every government's ability to detect and prosecute unlawful behavior, expropriate ill-gotten gains, and tax its citizens -- some of a government's core functions. The U.S. government has long been wary of cash as a vehicle for monetary exchange for the same reasons. Policymakers have even discussed the possibility of discontinuing other high-value cash denominations denominations like the $100 dollar bill.[27] Bitcoin is like cash without its physical limitations. It can cross borders in massive quantities with impunity.

While Fedcoin can exist alongside with Bitcoin, the former will likely be more popular and prevalent while providing government a means to trace transactions when necessary.

4.7 Tax Status

One of the primary advantages of Fedcoin over Bitcoin is the fact that if it were adopted by the Federal Reserve and deemed legal tender, it would generate more reasonable tax consequences for everyday users of the currency. Since 2014, the IRS has treated Bitcoin and other cryptocurrencies as property for determining users' income tax liability.[28] This means that instead of treating Bitcoin and other cryptocurrencies like foreign currency, the IRS treats them like stock or real property. Since Bitcoin's exchange rate has been so volatile, it has become a popular investment vehicle amongst some users. The IRS sought to take this into account by treating cryptocurrencies as investments.

The tax consequences of this decision are enormous. Above all, classifying Bitcoin as property made tax compliance for users a nightmare. If Bitcoin is treated as property, then a user who acquires Bitcoin and transfers them away at a later date is treated as having a capital gain or loss based on the difference in the currency's value between purchase and sale. In order to comply with this requirement, a user must record the exchange rate for each bundle of Bitcoin he acquires, so that he can later calculate the appreciation or depreciation in value of the Bitcoin at the time of sale. This imposes an onerous accounting burden on any user who spends Bitcoin on day-to-day transactions, thereby favoring the use of Bitcoin as an investment vehicle. As a result, day-to-day users are unlikely to comply with these tax requirements.[29]

The simplest solution to this problem would be for the IRS to reverse its policy and begin treating Bitcoin as a foreign currency. However, this is unlikely to happen, especially since there is a sound policy ground for the IRS's determination. Bitcoin and other cryptocurrencies have indeed proven to be uniquely volatile currencies, and there are many users who treat the currencies as investment vehicles as a result. If the IRS were to treat Bitcoin as any other foreign currency, it would lose out on its ability to tax the gains realized by these investor users. Therefore, before we can expect a change in the peculiar tax treatment of cryptocurrencies, we need to address the fundamental problem at the heart of that treatment: volatility.

Fedcoin escapes the volatility problems of other cryptocurrencies since it is a form of legal tender issued by the Federal Reserve, akin to the U.S. dollar. The value of the currency is pegged to the value of the U.S. dollar and backed by the same institution, removing pressure for arbitrage. Fedcoin would not need to be considered stock or property.nIn fact, the tax treatment that would result -- i.e. treating Fedcoin just as cash is currently treated for tax purposes -- would even be more reasonable than the policy that would result if the IRS reversed its determination and began treating cryptocurrency as foreign currency. Foreign currency is generally treated as cash for tax purposes unless the gains that a given user realizes due to price fluctuations exceeds $200.[30] If an individual's gains from exchange rate fluctuations exceed that value, then he is right back in the position of an investor: he has to compare the exchange rates at purchase and sale in order to determine tax liability.

With Fedcoin's cash treatment, users can spend the currency in day-to-day transactions free of onerous accounting requirements.

4.8 Risk of 51% Attacks

One of the essential elements of the Bitcoin protocol is the fact that a block of transactions cannot be added to the distributed ledger until the block has been mined by a network node. By design, the mining process is extremely time consuming for an individual computer. Mining requires a computer to find a string of text, a *nonce*, that when hashed with the block data, generates a value less than a given target. The only known way to find the golden nonce is to randomly generate and test them, a process that is likely to take any individual computer years to complete. However, if every computer in the network (or a substantial portion of them) is working on this operation simultaneously, then there is a good chance that one of the computers will come across a solution within 10 minutes. The Bitcoin protocol maintains the 10-minute interval by periodically checking the number of mining nodes in the network and adjusting the difficulty of the hashing problem accordingly. The computer that first finds a solution to its hashing problem gains the privilege of determining the next block to be added to the global blockchain.

Mining is key to maintaining the fundamental cash-like features of Bitcoin. Above all, the mining requirement prevents an individual user from double-spending a particular quantity of Bitcoin. Since an individual computer cannot mine a block within a reasonable timeframe, an individual user does not have the power to change the blockchain at will. The lottery-style system ensures that the odds any particular user will get to add the next block are infinitesimal.

The effectiveness of this system relies on the fact that Bitcoin users are not working in concert. Problems emerge when a group of users colludes to flood the system with self-serving blocks. While the lottery system ensures that groups of several users are not substantial enough to change the odds of a mining victory, if a group becomes large enough and its odds of a mining victory high enough, it can threaten the proper functioning of the protocol.

The grouping problem is most salient when a group gains control of over 50% of the nodes in the network (a *51% attack*). At this point, it is more likely that a group member will win the hashing contest on any given mining cycle than not, giving the group the power to determine the contents of the next block more than half the time. This is a difference in degree rather than kind: if a group controls any sizable portion of the network's nodes, it already has a far larger amount of power over the fate of the blockchain than any individual user. This power grows with percentage control.

Once a group has gained substantial control, it has administrator-like powers over the blockchain that are antithetical to the decentralized nature of Bitcoin. The group can allow its member nodes to double-spend Bitcoin by overwriting transactions in which Bitcoin is transferred to a counterparty. It can also block particular addresses from the network by excluding transactions involving those addresses from any of the blocks that it puts together. With enough control, it can even go back and replace a block already set deep in the blockchain, then mine a new series of blocks fast enough to beat the progress of the previous blockchain and replace it.

The grouping problem is widely acknowledged to be one of the primary dangers of the Bitcoin protocol. Scholars have identified three main regulatory approaches to addressing this problem,[31] although all three are likely to fail.

The incentive-based model is the one that is currently assumed to be in place. This model is based on the fact that Bitcoin users are sufficiently invested in the fate of the currency that they will naturally avoid forming groups large enough to threaten the proper functioning of the currency. For example, when the membership of the GHash mining pool was approaching 50% of network nodes at one point, the mining pool pledged to do everything in its power to cap membership at 39.99% so as to ensure it would not control a majority of the network.[32] While such behavior is heartening, it is unlikely to be sufficient to stave off 51% attacks permanently. The main driver of this behavior is the fact that if a particular group were to attain 51% of control over the network, the value of Bitcoin would tank immediately once the threat became public knowledge, costing the group more than the gains it would likely be able to obtain through its new administrative powers. However, this calculus may not necessarily remain the same as Bitcoin grows, and the possibility of massive short-term gains for a controlling majority may increase.

In addition, the incentive-based model seems predicated on the current cultural and political discourse surrounding Bitcoin. It is a young and revolutionary currency that many people think rightfully undercuts the power of governments to assert control over the money supply and track transactions. Accordingly, many users have an interest in preserving the currency that extends beyond a strict monetary interest. In this climate, it is easy to have faith that Bitcoin users will not threaten to undermine the currency. However, if the currency becomes more mainstream, more users are likely to own Bitcoin for purely monetary reasons (i.e. as an investment vehicle or a means of transacting), thereby limiting the influence of users who are inspired to protect the currency from monopolies. For this reason, it is likely that the incentive-based model's effectiveness will decrease over time.

Another regulatory model for limiting the growth of monopoly in Bitcoin is an approach analogous to that which is currently used to enforce antitrust laws. When a pool of users is deemed to be too large according to some threshold, then the government or an injured private party can bring legal action against them to dissuade their further collusion with the risk of fines. This approach has been criticized as a mere "stop-gap measure," inadequate for dealing with this fundamental vulnerability of the Bitcoin protocol.[31] However, the same could be said for the antitrust laws and a variety of other regulatory regimes in the US, so this critique is not sufficient to foreclose this regulatory strategy.

The larger problem with this model is that Bitcoin's pseudonymity makes it resistant to regulation by litigation. Mining pools are an obvious target for litigation, because these tend to be above-board companies. However, if mining pools were subject to litigation, then it is likely that Bitcoin users would form more secretive mining pools that could easily evade litigation. In all likelihood, these pools already exist. Any antitrust litigator knows that collusion is difficult to trace. Additionally, even if a mining pool with too much control could be traced, an *ex post* litigation approach is likely to be inadequate because all of the earnings the pool could make from exploiting the protocol would be stored in pseudonymous Bitcoin accounts resistant to expropriation. As a result, litigation will likely not be a successful deterrent to 51% attacks.

After finding the above two approaches inadequate for addressing Bitcoin's monopoly problem, Samtani and Baliga advocate for rewriting the Bitcoin source code to make collusion impossible at a large enough scale to exploit the protocol.[31] They do not specify how this coded solution would work. A coded solution that would completely prevent the possibility of a 51% attack while preserving Bitcoin's present form is likely to remain elusive. Modifying the Bitcoin protocol so as to prevent a group of users from having too much influence on the network is likely to be a fundamental change to the protocol that will have major costs. Bitcoin's vulnerability to 51% attacks results from the set of features that make it a functional currency. If it were possible, changing the code so as to prevent collusion would be likely to harm the delicate balance that makes Bitcoin work.

It is unlikely that such a change would be possible. Bitcoin mining pools are groups of users who have decided to cooperate under the agreement that if any one of them wins a mining reward, he will share that reward with the rest of the group. It is hard to imagine how the Bitcoin source code could detect and prevent this sort of behavior. Even if this sort of behavior were detectable, it is likely that a coded solution would simply incentivize more subtle forms of collusion that the code could not detect.

Additionally, banning collusive behavior via code is likely not a wise policy decision, since cooperation between users has become an essential part of Bitcoin. For many Bitcoin users with computers of ordinary processing power, the likelihood of winning a mining reward on one's own is so small that the cost of electricity consumed through the additional processing outweighs the average value of mining. Many users have no incentive to mine. This has poor distributive consequences, since it raises barriers to entry. Mining pools are a partial remedy to this situation, since they can increase the average value of mining for an individual enough that it makes mining profitable. Nonetheless, mining pools are a way of turning Bitcoin's proof-of-work requirement into a more egalitarian system that allows a larger population of users to sustain the network.

Any of the above approaches for regulating Bitcoin's monopoly problem is likely to cut into the beneficial cooperation between Bitcoin users that happens every day. The fundamental issue with regulating this problem away is that it requires finding the right balance between curbing group influence and eroding the features that make Bitcoin functional and attractive in the first place. Certainly, this is not an impossible policy problem but it is an undesirable one. It shows that Bitcoin does have some fundamental flaws that may keep it from ever becoming as mainstream and trustworthy as a federally backed currency like Fedcoin.

One of Fedcoin's main advantages over Bitcoin is the fact that it dramatically mitigates the risk of 51% attacks, thereby sidestepping the policy puzzle outlined above. Fedcoin's threat model is based on the assumptions that the central bank is honest, the protocol's cryptography is secure, and that each transaction is processed by a set of Nodes with an honest majority. Should these hold true, double-spending will not be possible and commits issued by Nodes will be non-repudiable. As said in Section 3.3, the Fed has total and complete auditability of Nodes, the low-level blocks they issue, and the logs they print, in order to cement the system's integrity. Moreover, Nodes have the incentive to provide honest service from the fee paid to them by the central bank for their performance in transaction verification.

5. Conclusion

We intend to continue developing Fedcoin through the near future to create a production ready system. Here are high priority feature requests.

- Confidential transactions. First, obscured values. Second, Zcash-style anonymity.
- Calculations of throughput and latency across many numbers of Users and Nodes
    - This paper's abstract, which mentions a two orders of magnitude of improvement over Bitcoin, was based on local testing at fixed User/Node sizes
    - Host app on cloud infrastructure (Azure, AWS, etc.)
- Testing framework
- Blockchain explorer. Example
- Multi-signature wallets with m-of-n transactions
- Creation of User accounts (not wallets) at the CentralBank
    - CentralBank whitelisting of addresses that were broadcast to accounts
- Wallet UI for the browser
    - Convenient generation of secure and memorable passphrases
        - Humans are not the best source of entropy
- Byzantine fault tolerance, should all Nodes mapped to an address space fail

Financial services are being revamped from the ground up, and blockchain technology is their driving force. Private companies like Monetas, Ripple, and Chain are building enterprise-grade blockchains.[11, 15, 16, 17] Meanwhile foreign central banks are preparing to issue blockchain-backed currency.[10] Domestically, however, Fedcoin has the potential to become the flexible, distributed, secure payments system that the United States severely needs. While Fedcoin holders would enjoy fast transactions and cheap fees, they would also be guaranteed the stability in purchasing power that comes with a central bank backing the currency.

Where Bitcoin struggled with speed, stability, scalability, and security, Fedcoin will not. This project's prototype demonstrates the theoretical and experimental benefits of federated consensus, and why individuals and central banks can trust the mechanism. Economic exchange depends on *trust*, and any good money must make that a given.

6. Acknowledgements

We would like to thank our advisor, Professor Joan Feigenbaum, for her feedback throughout our project; Dr. George Danezis and Dr. Sarah Meiklejohn for their work on RSCoin; Matthew Sheppard for his insight on implementation; David Andolfatto for writing about Fedcoin and speaking to us over the phone as were designing the project; and Satoshi Nakamoto for being a straight up legend.

7. References

1. Danezis, G. and S. Meiklejohn. *Centrally banked cryptocurrencies*. 2015. Link.
2. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*. 2008. Link
3. Narayanan, A., J. Bonneau, and E.W. Felten. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Princeton UP (186). 2016. Link.
4. Tschorsch, F. and B. Scheuermann. *Bitcoin and beyond: A technical survey on decentralized digital currencies*. IACR Cryptology Archive. 2015. Link.
5. Andolfatto, D. *Fedcoin: On the Desirability of a Government Cryptocurrency*. 03 Feb 2015. Link.
6. Barrdear, J. and M. Kumhof. *The Macroeconomics of Central Bank Issued Digital Currencies*. Bank of England. Staff Working Paper No. 605. 2016. Link.
7. Mills, D., et al. *Distributed ledger technology in payments, clearing, and settlement*. Finance and Economics Discussion Series, Federal Reserve Board. 2016. Link.
8. *The Great Chain of Being Sure about Things*. The Economist. 31 Oct 2015. Link.
9. Ludwin, A. *Why Central Banks Will Issue Digital Currency - Chain*. Chain. 06 Jun 2016. Link.
10. Popper, N. *Central Banks Consider Bitcoin's Technology*. The New York Times. 11 Oct 2016. Link.
11. Shin, L. *Chain, With Visa, Citi, Nasdaq And Others, Releases Blockchain Protocol For Financial Networks*. Forbes. 02 May 2016. Link.
12. ZCash. *Zcash - All Coins Are Created Equal*. Link.
13. Blockstream. *Confidential Transactions - The Elements Project*. Link.
14. Chain. *Hidden in Plain Sight: Transacting Privately on a Blockchain*. 07 Feb 2017. Link.
15. Monetas. *Technology - Monetas*. Link.
16. Ripple. *Technology | Ripple*. Link.
17. Chain. *Chain Core*. Link.
18. Davidson, J. *No, Big Companies Aren't Really Accepting Bitcoin*. Money. 09 Jan 2015. Link.
19. New, C. *Cash Dying As Credit Card Payments Predicted To Grow In Volume.* Huffington Post. 07 Jun 2012. Link.

20. *E-Commerce Retail Sales as a Percent of Total Sales.* Federal Reserve Bank of St. Louis. Link.
21. Hiltzik, M. *Bitcoin crash of 2013: Don't you feel silly now?* Los Angeles Times. 07 Dec 2013. Link.
22. Wieczner, J. *What the SEC Bitcoin ETF Decision Means for the Future of Cryptocurrency*. Fortune. 10 Mar 2017. Link.
23. Satter, R. *Mt. Gox crash spells trouble for Bitcoin.* Japan Times. 26 Feb 2014. Link.
24. Barker, J.T. *Why Is Bitcoin's Value So Volatile?* Investopedia. 22 Feb 2017. Link.
25. Donnelly, J. *What is the 'Halving'? A Primer to Bitcoin's Big Mining Change*. CoinDesk. 12 Jun 2016. Link.
26. *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies.* 18 Mar 2013. Link.
27. Summers, L. H. *It's time to kill the $100 bill.* Washington Post. 16 Feb 2016. Link.
28. *IRS Virtual Currency Guidance: Virtual Currency Is Treated as Property for U.S. Federal Tax Purposes; General Rules for Property Transactions Apply.* IR-2014-36. 26 Mar 2014. Link.
29. Pagliery, J. *New IRS rules make using Bitcoins a fiasco*. 31 Mar 2014. Link.
30. 26 U.S.C. § 988.
31. Samtani, S. and V. Baliga. *On Monopolistic Practices In Bitcoin.* Indian J. L. & Tech. 2015. Link.
32. Higgins, S. *GHash Commits to 40% Hashrate Cap at Bitcoin Mining Summit.* CoinDesk. 16 Jul 2014. Link.