Timekoin

Open Peer to Peer Encrypted Currency System

timekoin@gmail.com

February 2, 2010

Abstract.

With the global economy taking shape, electronic transactions take place by the millions every day. In essence, all this data is merely a balance sheet that sits in a database server somewhere on the Internet. As long as you have trust in a central authority to be honest with the data, then it can be assured that anything being bought will have that authority to back up it's value for barter or trade.

While the data on these servers can be encrypted with the highest grade encryption know to exist and therefor nearly impossible to break; the biggest weakness is the central authority itself. This central authority already has the access and ability to change the account register as it sees fit. Be it political pressure or some elaborate theft, there always exist a way for the central authority to separate the funds that it protects from the people the funds belong to.

The weakness means that accounts can be frozen without permission from the owner. Accounts can have the balance changed without permission from the owner. All this power exist with the central authority that watches and controls the accounts. But.... without the central authority, one could not guarantee that the account could not be spent for more than it contains. Because of this, people have come to rely on these central authorities to be the clearing house of information. Information is power. The information that documents balances and transfer is absolute power.

Since the inception of computers, the means by which to maintain and secure this digital information was beyond the financial means of a single person. One would have to become bank with a staff, computer servers, and rules to follow if they plan to participate in any system of currency around the world. Behold the digital age where most people have a smartphone faster than even the best computers only 15 years earlier. The large divide between what it takes to maintain an electronic currency system has shrunk so much that even the typical desktop computer could be a bank.

Even with the processing power and storage capabilities of the modern computer, a system of encrypted currency could not be trusted to just one individual or computer. The temptation for cheating would be too high. The only way that any electronic currency will survive is if rules are created that all those that participate in the electronic currency network must follow. These rules would be similar in manner to how sports are played. Rules are set so that all players can be equal. If someone breaks the rules, everyone else is aware of it. The rule breaker is either ignored or removed from the game.

A system of electronic currency must have a means to prevent double spending. It needs a public register that everyone can see. When everyone can see the register, no one can spend more than they have. The system needs a way to ensure that past transaction can not be tampered with. The system needs a way to allow currency to enter the system at a rate that does not upset the market value of currency. The system needs to be organic and flexible to errors. The system needs to be self-repairing in case of attacks on the system. The system must be removed of all entitlement of the users that will depend on the system.

1. Introduction

While it may seem as though it's impossible to create a system that is fair and open to the whole world, one thing must be taken into account. The only way to secure any currency system is to ensure that the resources needed to destroy it are outweighed by the benefits of using it. The only benefit to any currency system is that rules are set to use the currency allow something physically to be secured. This can be land, precious metals like gold, or anything of a physical nature that has value to someone else. For an electronic currency system, rules must also be followed but electronic systems though suffer a major set back. There is nothing physical about an electronic currency.

While the database server the electronic currency sits on exist as a physical object, and this object may exist inside a bank, the actual concept of the electronic currency has nothing tangible about it. It's merely the banks word that if you try to withdraw from this electronic currency, it can be exchanged for something physical in the end like cash or food. When you purchase from this electronic currency like a debit card, you are not depleting a magic token somewhere. You are simply telling the bank to subtract one number from another and be honest that this new number will not be changed without your consent.

With an open online peer to peer based electronic currency system, you have no guarantee of trust at all. Each peer could be corrupt, only reporting what is in its best interest. Each peer can lie about what it thinks the balance of an account should be. The only way to enforce any currency in this system is to assume you can not trust any of your peers. The only job your peers should be tasked to do is simply keep track of a list of transactions. Each peer will only be able to generate transactions for its own self interest of spending to another peer. The entire system will be based on the dis-trust of the entire network. Instead trust will be built among each peer one at a time. This trust is a consensus to maintain the history of transactions for which tampering with, will not result in any gain for the peer. The gains are made by following the will of the majority of peers in unison. Any attempt to break the set rules or step outside the realm will result in the peer being ignored by the majority. In a way, each peer becomes part of collective whole with one will.

2. Transaction Security

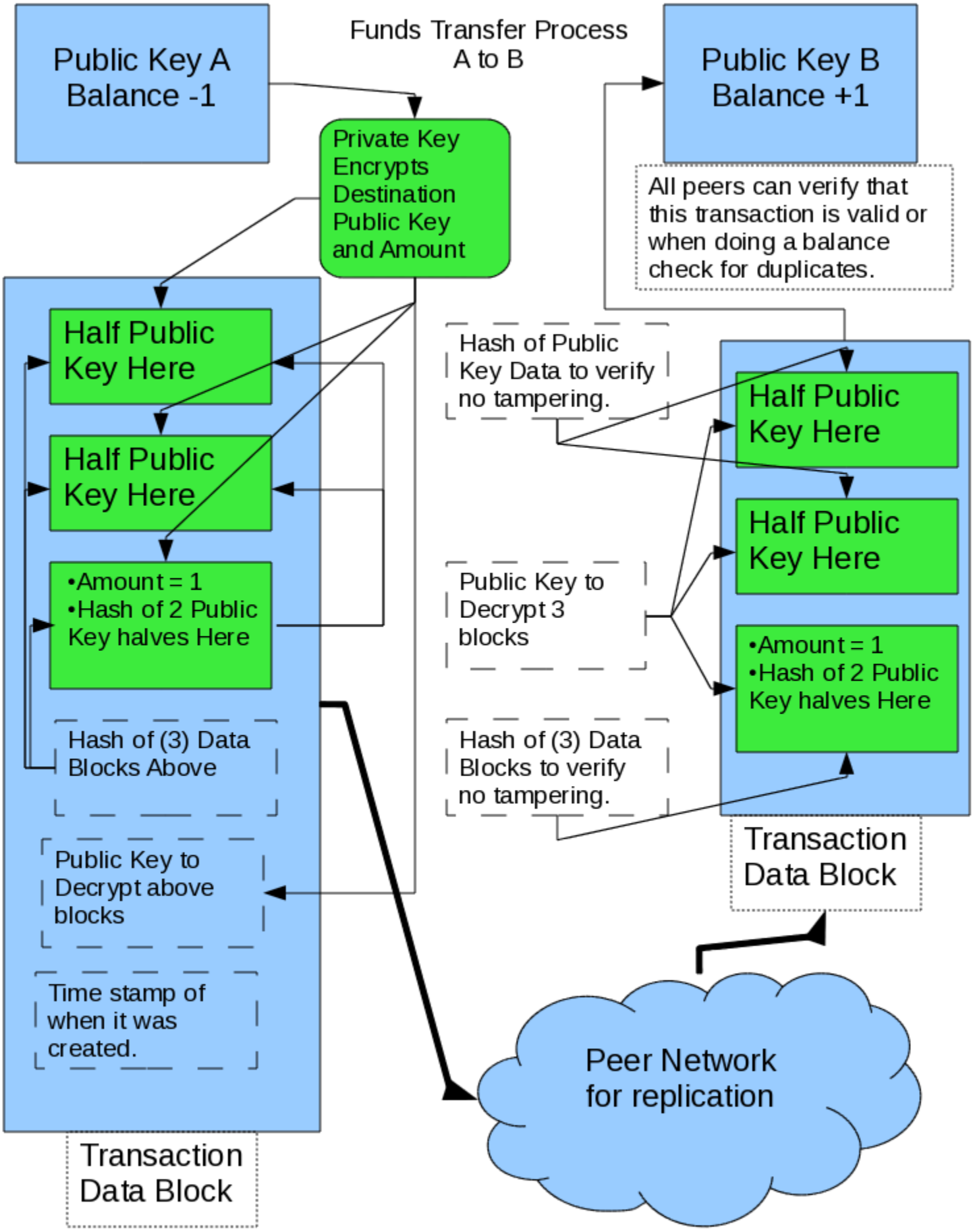
There are many systems already in existence for transaction security. One that has started to become popular is Bitcoin. This software uses a type of block chain that builds off the previous transactions block. The chain is secured against tampering by each computer in the peer network competing to solve a calculation that will advance the block. In the process, the winner awards itself currency. All the losers start again by building off the winner's block and the process for competition begins again. The more computers in the peer network, the faster winners appear to build the next block. The system has a form of throttle control in which the faster winners appear, the more difficult the calculations become to find the next winning block in an attempt to wrangle in how fast blocks (and thus currency) is created.

While I admire the system's genius, I do see some flaws from a resource standpoint. The process and math for Bitcoin is sound, but the means by which it functions is a wasteful process. The more computers that join the network, the more resources (in the form of CPU) is needed to create the currency and secure transactions. As the peer network grows, so does the resources it consumes to maintain itself. Ultimately, the peer network could grow so large that there will be no incentive for an individual to participate in the Bitcoin network because currency generation will only happen for those that can afford the most CPU power (multi-core systems in server racks). Not to mention that Amazon offers super computer time for rental. If the currency becomes popular enough, it might be feasible to rent super computer time to out-pace currency/block generation of the entire peer network.

A system of transaction security can be done without depending on raw CPU power to secure it. One can not predict the future and where computers will go. Bitcoin seems to be design around the false premise that computers in the future will not make some exponential leap in speed that would send currency generation and thus wasted CPU and power out of control. For that reason, a system needs to be setup that has the strengths that Bitcoin has with a peer to peer network but without the weakness of depending on something uncertain like CPU speeds.

Timekoin can do this without requiring massive amounts of CPU speed. In theory, even the slowest PC could participate in the Timekoin network. Every transaction in Timekoin will be secured via 1,536 bit OpenSSL RSA encryption. That's not a typo, but that's what a typical Celeron 1GHz computer can handle if dedicated to just encrypting and decrypting simple transaction information. Each transaction is created with a private key, but only the encrypted data and public key will be sent to all the peers. The transaction can only be unlocked with the public key. The public key will unlock inside the transaction, another public key and an amount. The only purpose of this information is to represent to the entire peer network that this public key belongs to an unknown private key that created the transaction is sending an amount to another public key. Because the private key will not be known to the peer network, there is no way for another peer to create a transaction fake or duplicate that will fit the public key to decrypt it. If the peer network is presented with fake transaction, the public key will not able to unlock it, thus the contents will remain unknown, thus no transaction of any kind could or would take place.

To secure against complex transaction data substitution, the encrypted data inside the transaction will contain a SHA256 hash of it's own data for which the currency is meant to transfer to. This would prevent a peer from taking the transaction amount inside and trying to redirect it to its own public key through falsifying it's own transaction history and trying to replicate this out to other peers. Basically, each transaction is built upon a 3-way confirmation of which if any hash or key is tampered with, the whole thing will implode mathematically. Each peer can only observe what is inside already.


Public Key A
Balance -1
Funds Transfer Process
A to B
Public Key B
Balance +1
Private Key
Encrypts
Destination
Public Key
and Amount
All peers can verify that this transaction is valid or when doing a balance check for duplicates.
Half Public
Key Here
Half Public
Key Here
•Amount = 1
•Hash of 2 Public
Key halves Here
Hash of (3) Data
Blocks Above
Public Key to
Decrypt above
blocks
Time stamp of
when it was
created.
Transaction
Data Block
Hash of Public
Key Data to verify
no tampering.
Public Key to
Decrypt 3
blocks
Hash of (3) Data
Blocks to verify
no tampering.
Half Public
Key Here
Half Public
Key Here
•Amount = 1
•Hash of 2 Public
Key halves Here
Transaction
Data Block
Peer Network
for replication

3. Crypto Currency Generation

No matter how secure you make a transaction on a public peer network, it will all be for nothing if there exist nothing to spend. There is where the time of Timekoin comes in. Using the forward movement of time, currency will be generated by elected peers in the network. There will exist no bias on the peer election as it will be a completely random process. Peers come into the network and if they wish to produce currency, broadcast a request to all peers. If no other peer wishes to compete in the election, the first one to submit is the automatic winner. The peer's public key is added to the pool of public keys allowed to generate in the network. After 1 hour has passed, the public key is allowed to submit self-creating transactions of 1 unit to the network. As each transaction is approved, this will slowly increase the balance of the public key. In essence currency is being created from the void of nothingness 1 unit at a time for each public key participating. The forward movement of time limits how much can be created at a time as well as the number of peers in the network. The more peers that join the network, the more than can be created in very small and time controlled amounts. Since these self-generating transaction are stored in the transaction history, it is in the best interest of all peers to maintain an in sync and non-tampered transaction history or risk losing the amounts of currency they or anyone else has have created.

The longer the peer participates in the network, the more currency it will be allowed to generate at a time. This makes it non-feasible to join as many peers to the network as possible for currency creation because the amounts created are smaller than the expense it would take to maintain all the peer computers to create it. Any government or corporate authority that tried to flood the timekoin generation would quickly find the limited rate and randomness of the entire system more expensive and resource hogging to maintain than the benefit of generation would produce. The whole currency generation relies more on the individual user than a large server farm with lots of IPs at someone else's disposal.

4. Data Integrity

Even the best encryption and generation scheme is only as strong as the integrity of the data that the peer network maintains. If the transaction history is littered with errors and mistakes, it only slows down the peer network and produces extra processing overhead to step around broken transactions or those that don't decrypt due to tampering with keys or hashes. As such, each peer will basically spot check all it's other peers and point out errors in the transaction history. The process is completely random, so anyone trying to hide forged or modified transactions will have the odds against them that it won't be discovered and purged from the network.

To avoid deep transaction tampering, the entire peer network will be building transaction foundations ever few days. These foundations are large chunks of time in which the entire data blob is hashed and stored for comparison among other peers. Each foundation will incorporate some part of another foundation. The further back in time you go, the more foundations exist and become interconnected; built over top of those transactions. Each foundation hash will be a way for peers to quickly compare large blocks of time for tampering in the transaction history. Any tampering will be easy to spot and purge with this method without requiring a large amount of processing overhead to maintain it.

Basically, the further back in time you try to tamper, the harder it is due to the sheer amount of encryption data and hashes on top of it that would have to be defeated first. To the point of being impossible with modern super-computers of the world.

5. Final Summary

This system for peer to peer electronic encrypted currency relies on a 3-prong security defense of high encryption keys and hashes connected in a such a way to simulate a virtual Quantum state for the transaction data where tampering with any part of the process would collapse the entire attempt of tampering. Due to this virtual entangled state of the data, there is no way to observe and predict what is inside the transaction until you look inside with the public key. A which point, there is no way to change the inside of the transaction without tampering with the outside components that constructed it all.

The strength of this system is that vast amounts of CPU power are not required to maintain it. Disk space is actually what is needed the most and given how cheap large drives are and how small all the transaction data is, it will never be outpaced. Another strength of this system is that it starts building from the ground up of not trusting any peer on the network. Instead, trust is only mutual because all peers benefit from this collective work and any attempts to tamper with the system results being ignored by the collective peers as a whole.

The weakness to this system is how complex it will be to setup. For this to be a feasible currency of the future, it needs to be able to run on today's computer that the typical home user has sitting under their desk and not some high-powered server farm owned by a large corporate entity or government authority. The software will have to be so well optimized that anyone can run it without having to spend thousands in hardware upgrades or else the future of currency will remain with as it does, those with the most money and resources to own it.

– KnightMB