Karan Mirani

UFID:64319219

CIS 6930/4930

Bitcoins And Anonymity

Abstract: Bitcoin is a P2P form of electronic payment system. It allows end-users to create pseudo-anonymous financial transactions; instead of disclosing personal information, users create any number of Bitcoin identities/addresses, in the form of cryptographic keys, which are used to accept and send bitcoins. In this report, I first explore the working of the bitcoin system. Then, I state the anonymity issues with the bitcoin system. In the end, I state a protocol which makes the bitcoin system more robust.

Introduction: The only person who ever took credit for the creation of the Bitcoin was Satoshi Nakamoto. It is a pseudonym and no one really knows his true identity. The first bitcoin transaction took place on January 12th ,2009 and since then the number of transactions have increased exponentially.

Advantages of bitcoins over other forms of electronic payments: The transactions on the bitcoin network are pseudonymous. A normal user of the system cannot link the true identity of a user with his real world identity. This feature of the bitcoin system makes it attractive for users who value their privacy.

The bitcoin system is decentralized i.e. there is no 3rd party required for 2 people to make a transaction. The users of the system pay relatively lesser amount as 'transaction fee' as compared to other forms of payments such as credit cards. For egs. The merchants have to pay credit card fees which runs anywhere from 2-5% plus $0.3 per swipe. Bitcoin transaction fees using the Coin Of Sale POS are only 0.59% and on top of that the merchants don't have to pay the swiping machine deposit or the monthly rental fee.

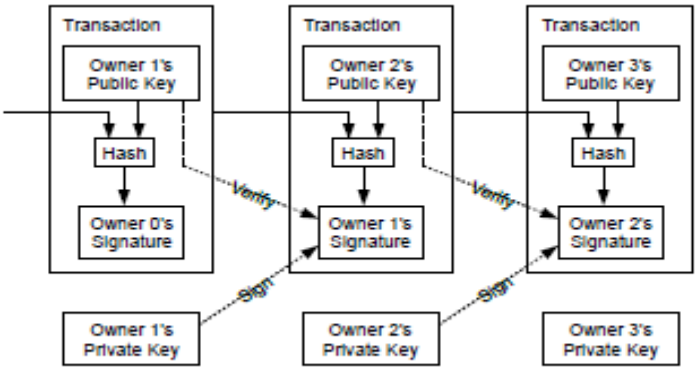
Anyone with an internet connection can start using bitcoins. There are approximately 8% people in the United States who don't have a bank account/credit card and approximately 2.5 billion people don't have access to banking services.

Building blocks of the bitcoin network

Transactions:

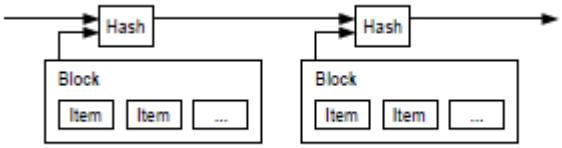
A bitcoin is nothing but an electronic chain of digital signatures. Transaction is a digitally signed declaration by one party of its intent to send a certain number of coins it possesses to another party. Transactions in the bitcoin ecosystem are atomic.

Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



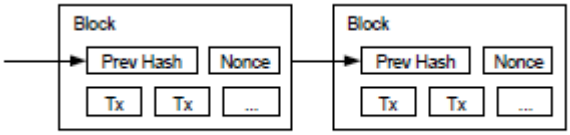
However, the user cannot verify whether the coins it received have not been double spent.

Timestamp Server: The bitcoin network addresses the issue of double spending by using a timestamp server. The timestamp server timestamps a hash of a block of items and broadcasts it. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.



Proof Of Work:

To implement the timestamp server on a P2P basis the Bitcoin network uses a proof of work system. A *proof of work* is a piece of data which is difficult (costly, time-consuming) to produce but easy for others to verify and which satisfies certain requirements. They are analogous to puzzles i.e. they are not easy to solve and require serious computation. Proof of work techniques are used to deter spam and Ddos attacks. The proof-of-work involves scanning for a value that when hashed, the hash begins with a number of zero bits. The average work required is exponential in the number of zero bits required and can be verified by executing a single hash.



The Bitcoin network uses proof of work similar to HashCash . It implements the proof of work by incrementing a nonce in the block until a value is found that gives the block's hash the required zero bits. Once the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be changed without redoing the work. As later blocks are chained after it, the work to change the block would include redoing all the blocks after it.

The proof of work is also provides security against double spending. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. To modify a past block, an attacker would have to redo the proof-of-work of the block and all blocks after it and then catch up with and surpass the work of the honest nodes.

The block of chains with the longest proof of work is considered sacrosanct. All the nodes in the system will start extending this block of chain and will discard any other block chains they receive.

The system is designed in such a way that a proof of work can be found in approximately 10mins. So, 2016 blocks should be generated every 2 weeks. After every 2 weeks the difficulty of the proof of work is recalibrated to compensate for increasing hardware speed and varying interest in running nodes over time. If significantly more than 2016 blocks are generated then the proof of work is made more difficult and vice versa

Transaction Fees and Coin Generation

Essentially, the first transaction in every block is a special transaction which starts creating a new coin owned by the creator of the block. This gives the other nodes in the network an incentive to provide support for the network. When the network was first released for public use, every Bitcoin miner who comes up with the first proof of work was awarded 50 Bitcoins. After every 210,000 blocks the number of bitcoins that a node is allowed to generate is halved. Currently, a node receives 25 bitcoins if it first comes up with the proof of work. The bitcoin system is designed in such a way that only 21 million bitcoins will ever be generated. It is estimated that all the bitcoins will be mined by 2140. After that, the nodes will not be able to generate new bitcoins and then the only way of incentivizing them would be through transaction fees.

Why is the transaction fee charged ?
The nodes help in verifying the flow of coins and validating transactions. They also help to keep double spending in check. All these tasks are done by the bitcoin miners which take efforts in terms of time and processing power for which these nodes need to be compensated.

What is a transaction fee?
When the sender of a transaction sends money, he has to incentivize the other nodes in the network for their work. The sender mentions the transaction fee along with the money he wants to send and a couple of other parameters.

The BitCoin Network:

The steps to run the network are as follows:
1) New transactions are broadcast to all nodes.
2) Each node collects new transactions into a block.
3) Each node works on finding a difficult proof-of-work for its block.
4) When a node finds a proof-of-work, it broadcasts the block to all nodes.
5) Nodes accept the block only if all transactions in it are valid and not already spent.
6) Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Anonymity Issues With Bitcoins:

Bitcoin allows users to use different addresses and public keys in every transaction. However, Bitcoin still exposes their users to a weak form of linkability. Specifically, multiple public keys of the same user can potentially be linked when the user pays change to herself, in which case two or more of a single user's public keys will appear in the same transaction.

"An Analysis of Anonymity in Bitcoin Using P2P Network Transactions" by Koshy and McDaniel shows how approximately 1000 bitcoin users could be mapped to their likely ip addresses.

The Mixcoin Protocol

Mix networks were introduced by Chaum in 1981 for anonymous communication. Significant research has analyzed the relationship between design parameters, such as route selection and flushing policies, and the resulting anonymity, much of which is broadly applicable to financial mixing.

Assumptions:

Multiple mixes M_i are available and are represented by a warranty-signing key KM_i .Mixes want to build a reputation in KM_i so these addresses are used consistently. To carry out profitable business all mixes will need to build trust within the network and we assume this is their only agenda. We consider the scenario where Alice wants to send some bitcoins to Bob through a mix network. Alice splits her funds into multiple chunks and performs multiple sequential rounds of mixing for each of the chunks. The chunk size should be the same for effective anonymity. Unlike the mixes, Alice does not need to maintain the same public key nor the public reputation. It is assumed that Alice will be able to communicate with a mix over a covert and anonymous channel. In practice this can be achieved by mixes running a dedicated Tor hidden service.

Freshness of Addresses:

The mix and Alice both create fresh K_{esc} and K_{out} addresses for each mixing. This is required because warranties include neither K_{in} nor K'_{esc} , so they will appear to be satisfied as long as *v* is transferred on time to K_{esc} and then K_{out} from any address.

Core Protocol:

The protocol mixes single chunk 'v' of Alice's funds. Prior to mixing, the mix gives Alice a signed warranty which will enable her to unambiguously prove if the mix has misbehaved. Dishonest mixes will quickly have their reputation destroyed and lose business.

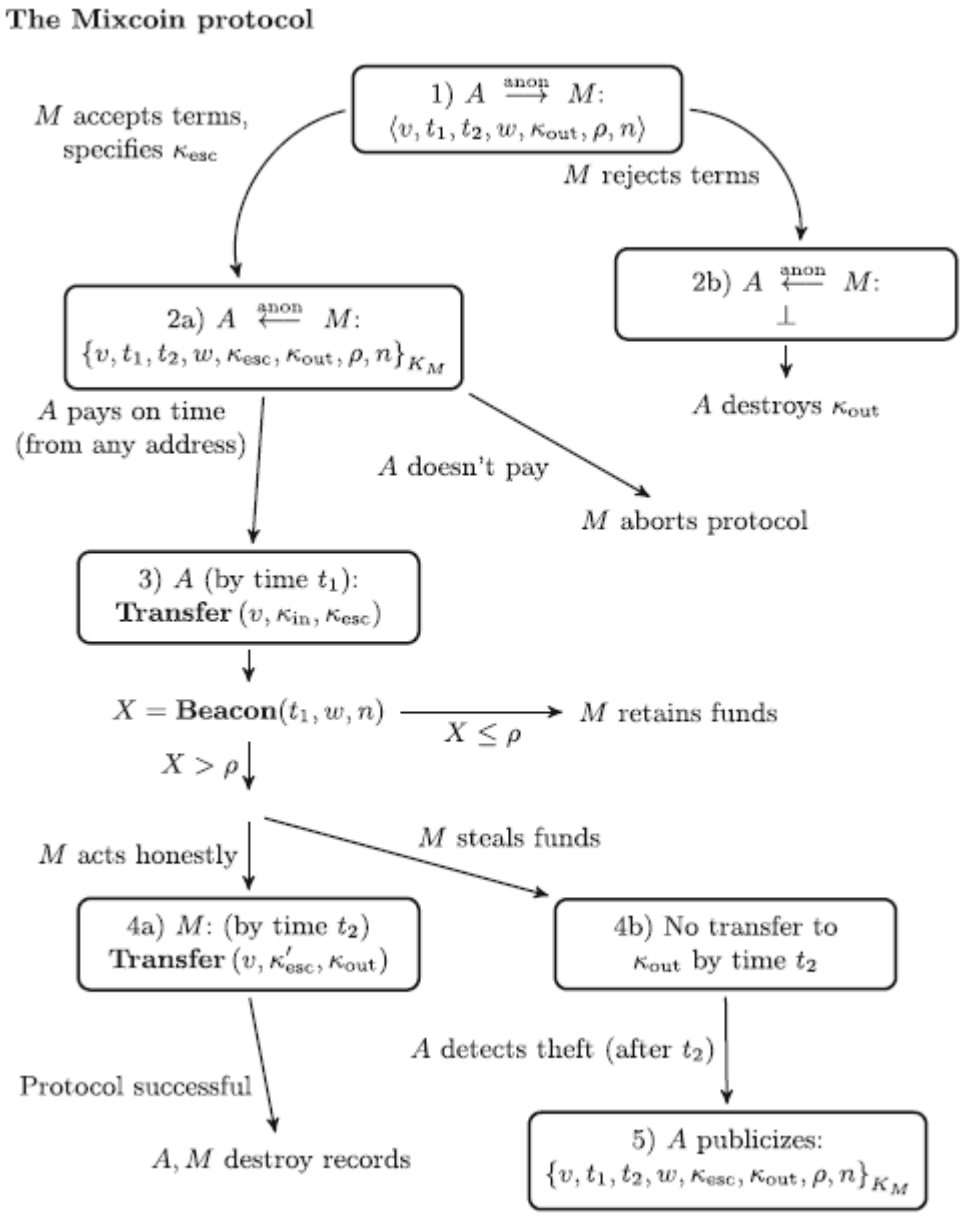
Step 1: Alice contacts the mix over an anonymous channel and sends the following information:

v the value (chunk size) to be mixed
*t*1 the deadline by which Alice must send funds to the mix
*t*2 the deadline by which the mix must return funds to Alice
K_{out} the address where Alice wishes to transfer her funds
ρ the mixing fee rate Alice will pay
n a nonce, used to determine payment of randomized mixing fees
w the number of blocks the mix requires to confirm Alice's payment

Step 2a:

(If the mix accepts these terms): It generates a fresh escrow address Kesc and sends back a warranty containing all of Alice's parameters plus K_{esc}, signed using KM.

Step 2b:
(If the mix rejects these terms): The mix may also reject Alice's request for any reason. Alice similarly has no obligation to transfer funds after receiving a warranty. If Alice declines (or forgets) to do so by the deadline t1 the mix deletes its records and move on.



Step 3:

If Alice does transfer the agreed value v to κesc by the deadline t1 then the mix is obligated to transfer an equal value to K_{out} by time t2. If Alice doesn't pay, the Mix aborts the protocol.

Step 4a:

If the mix does so faithfully, then both parties destroy their records to ensure forward anonymity against future data breaches.

Step 4b:

If the mix fails to transfer the value v to K_{out} by time t2, then go to step 5.

Step 5:

Alice publishes her warranty. Because the warranty is signed by the mix's long-term key KM and all Bitcoin transactions are publicly logged, anybody can verify that the mix cheated.

Mixing Fees:

Mixing fees are randomized whereby with probability p, the mix retains the entire value as v as a fee and with probability 1-p takes no fee at all. This produces an expected mixing rate fee of p and leaves K_{out} with either nothing or full v. The mix uses a publicly verifiable mechanism to randomly choose which chunks to retain as mixing fees. Specifically, the mix generates a (p, 1-p) random bit which neither party can predict for fairness. This can be done with a public source of randomness called a beacon.

Sequential Mixing:

Alice chooses N mixes M1, M2…, Mn and executes the mixcoin protocol with each one of them in reverse order instructing each mix Mi to forward her funds to the escrow address *Kesc+1* which she previously received from mix Mi+1. After obtaining N signed warranties, Alice then transfers her chunk to *Kesc1* and if any mix in the sequence fails to transfer it she can prove it with the appropriate warranty.

Advantages of Mixcoin Protocol:

Mix Indistinguishability: Single-use mix addresses ensure that passive adversaries can't determine which mix a user is interacting with. The anonymity set in this case is then the set of all users interacting with *any* mix at the same time.

Accountability: Mixcoin mixes issue signed warranties to users. A user can then confidently send funds to the mix, knowing that if the mix misbehaves she can publish this warranty, damaging the mix's reputation and its business model.

Threat Model

Due to the double spending prevention in Bitcoin, replay attacks are impossible in Mixcoin.

The Passive Adversary's View with Mix Indistinguishability:

It is assumed that this adversary can reliably determine with high probability which Bitcoin transactions are mix traffic, given their size v and their use of one-time escrow addresses. However, due to their one-time nature, this adversary is unable to link escrow addresses to specific mixes. In this case, the adversary is left to observe a sea of apparently identical escrow addresses and the system appears to function as one universal mix consisting of all participants using the chunk size v.

Active Adversaries and Distinguishable Mixes:

When Alice sends a chunk from K_{in} to M via K_{esc}, the client who ultimately receives this chunk will learn that K_{in} interacted with M. Similarly, the client who sends the chunk to K_{esc} which is eventually sent to K_{out} will also learn that Alice interacted with M. An active adversary can exploit this in a flooding attack, learning up to two other addresses interacting with the same mix for each chunk sent through that mix. Against such a strong active attacker who can link every escrow address to its originating mix, the system appears similar to be a traditional communication mix network with mixes behaving as stop-and-go mixes with limited pooling due to the block size.

Conclusion:

The Mixcoin protocol addresses most of the privacy issues of the Bitcoin network. It seems to be a very robust layer of privacy which could be added to the Bitcoin network. It uses the already existing infrastructure of the Bitcoin network and hence is backward compatible with it. It is a simple scheme which provides strong anonymity and can be deployed quickly.

References:

https://en.wikipedia.org/wiki/Bitcoin

Nakamoto, S. (2008) Bitcoin: A peer-to-peer electronic cash system," p.2012.

http://en.bitcoinwiki.org/Main_Page

Bonneau, Narayanan, Miller, Clark, Kroll and Felten (2014), "Mixcoin: Anonymity for Bitcoin with Accountable Mixes"

https://www.youtube.com/watch?v=JQzepQoZYi0

Koshy and McDaniel, "An Analysis of Anonymity in Bitcoin Using P2P Network Transactions"

Nicolas Christi, Reihaneh Safavi-Naini, "Financial Cryptography and Data Security"