Handout 7 (Bitcoins)

In my opinion Bitcoins are a Ponzi scheme[1]—still the ideas behind them are really beautiful and not too difficult to understand. Since many colourful claims about Bitcoins float around in the mainstream media, it will be instructive to re-examine such claims from a more technically informed vantage point. For example, it is often claimed that Bitcoins are anonymous and free from any potential government meddling. It turns out that the first claim ignores a lot of research in de-anonymising social networks, and the second underestimates the persuasive means a government has at their disposal. Below I will follow the very readable explanations about Bitcoins from

http://www.michaelnielsen.org/ddi/
how-the-bitcoin-protocol-actually-works/

http://www.imponderablethings.com/2013/07/
how-bitcoin-works-under-hood.html

Let us start with the question who invented Bitcoins? You could not make up the answer, but we actually do not know who is the inventor. All we know is that the first paper

https://bitcoin.org/bitcoin.pdf

is signed by Satoshi Nakamoto, which however is likely only a pen name. There is a lot of speculation who could be the inventor, or inventors, but we simply do not know. This part of Bitcoins is definitely anonymous. The first Bitcoin transaction was made in January 2009. The rules in Bitcoin are set up so that there will only be 21 Million Bitcoins with the maximum reached around year 2140. Contrast this with other fiat currencies where money can be printed almost at will. The smallest unit of a Bitcoin is called a Satoshi which is the 10^{-8} part of a Bitcoin. Remember a Penny is the 10^{-2} part of a Pound.

The two main cryptographic building blocks of Bitcoins are cryptographic hashing (SHA-256) and public-private keys using elliptic-curve encryption for digital signatures. Hashes are used to generate 'fingerprints' of data that ensures its integrity. Public-private keys are used for signatures. For example sending a message, say *msg*, together with the encrypted version

$$msg, \{msg\}_{Kpriv}$$

allows everybody with access to the public key to verify the message came from the person who knew the private key. Signatures are used in Bitcoins for verifying the addresses where the Bitcoins come from. Addresses in Bitcoins are essentially the public keys. There are 2^{160} possible addresses, which is such a vast amount that there is not test for duplicates…or already used addresses.

Traditional banking involves a central ledger which specifies the current balance in each account, for example

[1] http://en.wikipedia.org/wiki/Ponzi_scheme

account	balance
Alice	£10.01
Bob	£4.99
Charlie	-£1.23
Eve	£0.00

Bitcoins work differently in that there is no central ledger, but a public record of all transactions. This means spending money corresponds to sending messages of the very rough form

$$\{\text{I, Alice, am giving Bob one Bitcoin.}\}_{K^{priv}_{Alice}}$$

They are encrypted with Alice's private key such that everybody, including Bob, can use Alice's public key K^{pub}_{ALice} in order to verify the message came really from Alice, or more precisely from the person who knows K^{priv}_{Alice}. The problem with such messages in a distributed system is what happens if Bob receives 10, say, of these messages. Did Alice intend to send him 10 Bitcoins, or did the message by Alice get duplicated by for example an attacker re-playing a sniffed message. What is needed is a kind of serial number for such messages. Meaning transaction messages look more like

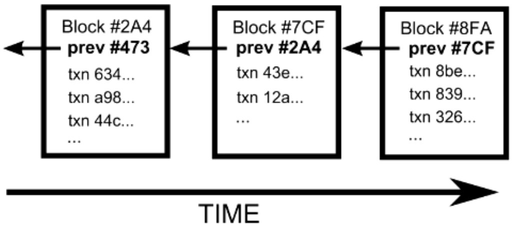
$$\{\text{I, Alice, am giving Bob Bitcoin \#1234567.}\}_{K^{priv}_{Alice}}$$

There are two problems that need to be solved. One is who is assigning serial numbers to bitcoins and also how can Bob verify that Alice actually owns this Bitcoin to pay him? In a system with a bank as trusted third-party, Bob could do the following:

- Bob asks the bank whether the Bitcoin with that serial number belongs to Alice and Alice hasn't already spent this Bitcoin.
- If yes, then Bob tells the bank he accepts this Bitcoin. The bank updates the records to show that the Bitcoin with that serial number is now in Bob's possession and no longer belongs to Alice.

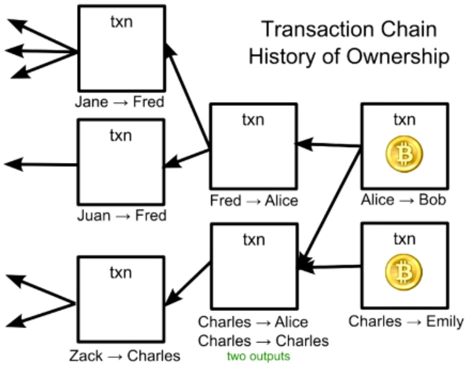
But banks would need to be trusted and would also be an easy target for any government interference, for example. Think of the early days of music sharing where the company Napster was the single point of "failure" which was taken offline by law enforcement.

Bitcoin solves the problem of not being able to rely on a bank by making everybody the bank. Everybody who cares can have the entire transaction history starting with the first transaction made in January 2009. This history of transactions is called *blockchain*. Bob can use his copy of the blockchain for determining whether Alice owned the Bitcoin and if yes transmits the message to every other participant on the Bitcoin network. The blockchain looks roughly like a very long chain of individual blocks



Each block contains a list of individual transactions. They are hashed so that the data in the transactions cannot be tampered with. This hash is the unique serial number of each block. Each block also contains a reference of the previous block. Since this previous-block-reference is also hashed, the whole chain is robust against tampering. We can check this by checking the entire blockchain whether the references and hashes are correctly recorded. I have not tried it myself, but it is said that with the current amount of data in the blockchain it takes roughly a day to check the consistency of the blockchain on a “normal” computer. Fortunately this consistency test from the beginning usually only needs to be done once.

Recall I wrote earlier Bitcoins that do not maintain a ledger listing all the current balances in each account.


Transaction Chain
History of Ownership
txn
Jane → Fred
txn
Juan → Fred
txn
Zack → Charles
txn
Fred → Alice
txn
Charles → Alice
Charles → Charles
two outputs
txn
Alice → Bob
txn
Charles → Emily