Distributed Trust and Blockchains	Date: *10 September 2019*
Instructor: *Sujit Prakash Gujar*	Scribes: Ankit Pant, Tarpit Sahu

Lecture 4: Bitcoin as a Platform

1 Recap

The following subsections briefly covers the contents covered in the precious class.

1.1 Bitcoin Consensus

Bitcoin overcomes the impossibility of achieving consensus in a distributed system (Fisher et al., 1985) by providing incentives. To achieve consensus, the transactions are broadcast to all the nodes and each node collects the new transactions into a block. The three kinds of consensus (Narayanan et al., 2016) required for Bitcoin to be successful are:

1. Consensus about rules.
2. Consensus about history.
3. Consensus that coins are valuable.

1.2 Selecting Random Node

The node/miner that adds the next block to the blockchain needs to be selected randomly. Each miner needs to solve a *crypto-puzzle* and the one who solves it first gets the chance to append it to the ledger.

1.3 Proof-of-Work

A Proof-of-Work (PoW) system (or protocol, or function) is a consensus mechanism (Wikipedia, 2019). It requires some work from the service requester, usually meaning processing time by a computer. Proof-of-work is a consensus algorithm in a Blockchain network. One disadvantage of Proof-of-work is that it is vulnerable to 51% *attack* Tar (2018).

1.4 Bitcoin Puzzle

The puzzle needed to be solved in order to present *proof-of-work* is basically of the form:

Find a *nonce* such that:

$$H(nonce \,||\, prev\_hash \,||\, transaction\_1 \,||\, transaction\_2 \,||\, \ldots \,||\, transaction\_n) < target$$

$$Where : target = 2^{256-k}$$

1.5 Incentive Engineering

- The longest chain is deemed as correct
- Appending to the longest chain is rewarded
- Appending elsewhere is penalised

2 Introduction

Apart from cryptocurrency, Bitcoin can be used for a variety of other application as well. Some of the applications do not require any changes to the Bitcoin architecture while some require small modifications. The following sections (and their subsections) have been largely referenced from (Narayanan et al., 2016). The following sections provide brief information on some applications of Bitcoin as a platform:

3 Bitcoin for Secure Timestamping

One of the fundamental parts of the Bitcoin architecture is the *Append-only* property of the ledger. It ensures that once the information has been written on the blockchain it is practically largely unalterable. Another useful property that Bitcoin provides is a secure notion of ordering. This ordering arises from the block hash pointers.

3.1 Secure Timestamping

Secure Timestamping with respect to *blockchain* can be described as follows:

Definition 1 (Secure Timestamping)**.** *The application of using* hash functions *and publishing* $H(r \mid x)$ {*where* r *is random nonce and* x *is the value we want to commit*} *at time* T *on the blockchain so that* r *and* x *can be revealed later on* {*and verified*} *thus convincing anyone looking at the blockchain later on that the value of* x *was known at time* T*.*

The notion can be further understood by considering the following example:
Suppose we want to prove that we know some value x at some specific time T. However we may not want to reveal x at time T but actually reveal it when we make the proof. However we want to ensure that once we've made the proof, the evidence that we knew the value of x all along to be permanent. We can do that by publishing the *hash* $H(r \mid x)$ at time T and then at a later time reveal r and x. Now anyone can look into the append-only ledger and be convinced that we must have known x at the time when we published $H(r \mid x)$, since there is no other feasible way of generating the data (Hash functions have the property of both *pre-image resistance* and *second pre-image resistance* and being append only $H(r \mid x)$ that was published earlier cannot be changed either).

3.2 Applications of Secure Timestamping

Secure Timestamping can be used for:

- Knowledge Proofs (as in the example in the previous subsection)
- Designing *public key signature scheme* (Guy Fawkes signature scheme)

3.3 Secure Timestamping – Old (traditional) way

In order to achieve secure timestamping, one may publish the hash of data in a newspaper or some other media which is widely seen by the public, by purchasing an advertisement. Since archives of old newspapers issues are maintained at libraries, it can be used for secure timestamping as the issue in which the hash was published can be later referred to when the proof is published.

3.4 Secure Timestamping in Bitcoin

The simplest solution proposed was to send coins (money) to the hash of the data instead of the hash of public key. However with this approach, the coins (money) sent to the data become un-spendable and hence are lost forever.
Another approach called *CommitCoin* can be used that allows the data to be encoded into a private key. Compared to encoding commitments in the public key, this *CommitCoin* avoids the need to burn (spend) coins and for miners to track an un-spendable output forever. However, it is quite complex (based on Elliptic Curve Digital Signature Algorithm (ECDSA) having the property that bad source of randomness can leak the private key).
The more preferred way of Bitcoin timestamping is by using *OP_RETURN* transaction which results in a provably un-spendable output. The *OP_RETURN* instruction returns immediately with an error and hence that script does not run successfully and the data included in it is ignored.

3.5 Attacks on Proof of Clairvoyance

The idea behind *proof of clairvoyance* is the proof that one has the ability to predict the future. It may seem that using Secure Timestamping, we can make proofs of clairvoyance. However using secure timestamping alone cannot be use to prove clairvoyance. A simple attack on such an attempt is to commit a variety of possible outcomes and only reveal the commitments that turn out to be true. Hence in order to prove that one actually has the ability to predict the future, one must be able to prove that one is timestamping one specific prediction rather than multiple predictions. This is difficult in Bitcoin as in Bitcoin's secure timestamping does not tie commitments to any individual's public identity.

4 Bitcoin as "Smart" Property

4.1 Non Fungibility

In economics, fungibility is the property of a good or a commodity whose individual units are essentially interchangeable, and each of its parts is indistinguishable from another part.

For example, since one kilogram of pure gold is equivalent to any other kilogram of pure gold, whether in the form of coins, ingots, or in other states, gold is fungible. Other fungible commodities include sweet crude oil, company shares, bonds, other precious metals, and currencies.

"The fact that bitcoins have histories means that bitcoins aren't fungible."
Fungibility matters in cryptocurrencies because coins previously used by someone else for nefarious purposes, can be purchased or acquired through legit means by innocent individuals, who may then be labeled as criminals for using the tainted coins. Taking another example, just as coin collectors value old coins, someday bitcoin collectors might place special value on coins originating int the genesis block or some other early block in Bitcoin's history.

4.2 Coinbase Transaction

A coinbase transaction is a unique type of bitcoin transaction that can only be created by a miner. This type of transaction has no inputs, and there is one created with each new block that is mined on the network. In other words, this is the transaction that rewards a miner with the

block reward for their work. Any transaction fees collected by the miner are also sent in this transaction.

4.3 UTXOs

An UTXO defines an output of a blockchain transaction that has not been spent, i.e. used as an input in a new transaction. Bitcoin is the most famous example of a cryptocurrency that uses the UTXO model.

In the case of a valid blockchain transaction, unspent outputs (and only unspent outputs) may be used to effect further transactions. The requirement that only unspent outputs may be used in further transactions is necessary to prevent double spending and fraud. For this reason, inputs on a blockchain are deleted when a transaction occurs, whilst at the same time, outputs are created in the form of UTXOs. These unspent transaction outputs may be used (by the holders of private keys; for example, persons with cryptocurrency wallets) for the purpose of future transactions.

4.4 Metadata in Currency

Some people add metadata to offline currency. They write various messages on banknotes, often as a joke or political protest. This generally doesn't affect the value of the banknote and is just a novelty.

Similarly we can have authenticated metadata attached to our currency -metadata that cannot easily be duplicated. One way to achieve this is to include a cryptographic signature in the metadata and ties this metadata to the serial number of this banknote.

$$sign(metadata + serial) \tag{1}$$

What could this be used for? Say a baseball team wants to use dollar bills as tickets, as shown in Figure 1.

Figure 1: Adding useful metadata to ordinary banknotes.

- This way they no longer have to go through the hassle of printing their own tickets and making sure that no one can print counterfeit tickets.
- The New York Yankees could simply assert that the dollar bill with a specific serial number now represents a ticket to a specific game and a specific seat.

- These dollar bills would be distributed in the same ways that paper tickets are normally distributed, such as by being mailed to fans when they buy tickets online.
- Whoever is holding that note has the right to enter the stadium, sit in the assigned seat, and watch the game, with no other questions asked.
- The banknote itself is the ticket!

Now currency can represent many things. Also the underlying currency value of bank note is maintained.

4.5 Non Fungibility & Metadata : Results

- Currency can now represent anything.
- Anti-counterfeiting properties are inherited.
- Underlying value also maintained.
- New meaning relies on trust in issuer.

4.6 Colored Coins

The term *Colored Coins* loosely describes a class of methods for representing and managing real world assets on top of the Bitcoin Blockchain. While originally designed to be a currency, Bitcoin's scripting language allows to store small amounts of metadata on the blockchain, which can be used to represent asset manipulation instructions.
The advantage of using Bitcoin's blockchain as the backbone leverages Bitcoin's strengths, such as immutability, non-counterfeitability, ease of transfer, robustness and transparency thus allowing asset manipulation with unprecedented security and ease. The *issuance and propagation* of *Colored Coins* can be seen in Figure 2.

4.6.1 Implementation : OpenAssets Protocol

- Assets are issued using a special Pay-to-Script-Hash address.
- If you want to issue colored coins, you first choose a Pay-to-Script-Hash address to use. Any coin that transfers through that address and comes in without a color will leave with the color designated by that address.
- There are various exchanges that track which addresses confer which colors onto coins. Since coins can sequentially pass through more than one color-issuing address, they can have more than one color.
- Every time you make a transaction that involves colored coins, you have to insert a special marker output.

4.6.2 Uses of Colored Coins

- Stock in a company
- Represent a claim to some real-world property
- Perform some functions of Domain Name System

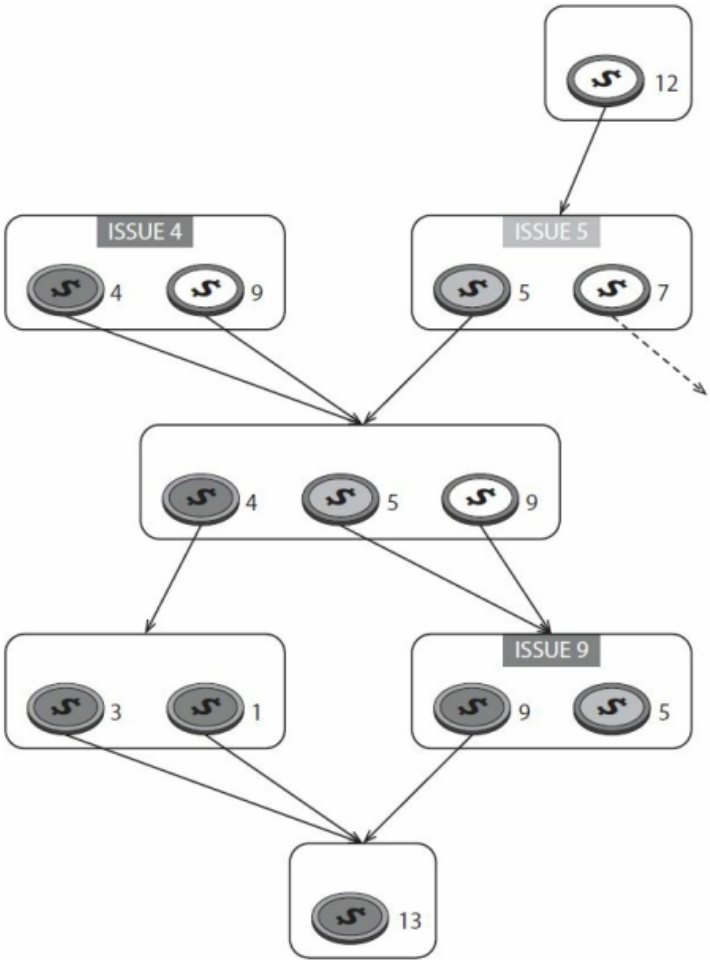

Figure 2: Colored coins. The transaction graph shown illustrates issuance and propagation of "color."

4.7 Pros & Cons of Bitcoin as "Smart" Property

4.7.1 Pros

1. compatible with BTC
2. ignored by community
3. flexible to represent any asset

4.7.2 Cons

1. small cost of unspendable markers.
2. must check every previous transaction.

References

Fisher, M. J., Lynch, N. A., and Paterson, M. S. (1985). Impossibility of distributed consensus with one faulty process. *Journal of the Asscktion for Computing Machinery*, 32:374–382. https://groups.csail.mit.edu/tds/papers/Lynch/jacm85.pdf.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton University Press. https://bitcoinbook.cs.princeton.edu/.

Tar, A. (2018). Proof-of-work, explained. *Cointelegraph.com*. https://cointelegraph.com/explained/proof-of-work-explained.

Wikipedia (2019). Proof of work. *Wikipedia the free encyclopedia*. https://en.wikipedia.org/wiki/Proof_of_work.