ECE 595: Foundations of Blockchain Systems **October 14, 2020**

Lecture 2: Bitcoin

Lecturer: Sreeram Kannan *Scribe: Senjuti Dutta*

This lecture mainly highlights the definition and one specific use case of blockchain, the cryptocurrecy Bitcoin. Applications of blockchain beyond cryptocurrencies are also mentioned here. To begin the discussion on Bitcoin, this lecture explains about some cryptographic primitives like hash and digital signatures to carefully understand the structure of a Bitcoin.

2.1 What is Blockchain?

The high level view point of blockchain is that it is a mechanism to coordinate between multiple parties without a trusted intermediary.

2.1.1 Core Properties of Blockchain

- Immutability : The ability of blockchain ledger to remain unchanged.
- Fault-Tolerant : The property of blockchain where the entire system does not fail even when a certain percentage of nodes are faulty or malicious (given that the percentage is not too high).

Note: The distributed ledger can be considered as an account book which keeps all the transaction details.

2.1.2 Application-level properties

- Censorship Resistant: This property implies that any party wishing to transact on the network can do so as long as they follow the rules of the network protocol.
- Transparency: It provides a fully auditable and valid ledger of transactions. By this property whoever join the property view all information on that network.
- Truly Permissionless: This means that anyone can join the network.
- Privacy: It means that if anyone in the network are doing transaction other nodes in the network will not able to see it.

It is important to mention that currently it is possible to achieve some amount of transparency and privacy both using zero-knowledge proof.

2.2 When not to use a blockchain

People use blockchain for many different purposes. There are categories where the use of blockchain seems logical and useful, but can in fact create problems. These are the following examples where it is not a good and efficient solution to use blockchain.

- Presence of high trust intermediary: In this case there is somebody who is uniquely entrusted doing some aspects of functionality.

Scenario: The FCC is responsible for managing and licensing the electromagnetic spectrum for commercial users and for non-commercial users including: state, county and local governments. FCC is highly trusted in this case. In this situation using blockchain is not a cost effective way. **Instead running a server will be more efficient.**

- Presence of physical aspects to coordination: This means that there physical aspects related to coordination. This also makes blockchain an ineffective solution.
  Scenario: Let's say eBay decides they want to use blockchain. On top of being a highly trusted intermediary as mentioned above, their platform has various physical aspects (shipping, receiving, etc.). For example, pretend a customer ordered a phone on eBay. On eBay's blockchain, the customer may have ordered a blue iPhone 12 64GB, but there is nothing to ensure that the seller sends the appropriate phone and that the user receives it and that there is no problems. In this case the physical system interacts with the blockchain through user input which introduces uncertainty. **Physical aspects cannot be inherently assured by blockchain.**
- Certifying physical provenance: Provenance means tracking a value or object. **Blockchain cannot ensure *correct* data entered into blockchain**.
  Scenario: We want to track an object in the supply chain. If we use blockchain it can certify that somebody actually signed or something happened, but whether it actually happened physically is not something that can be satisfied.
- Efficiency is the primary determinant: There are cases where efficiency is the primary goal, in these cases, using blockchain is not a smart choice. **No decentralized system can be more efficient than a centralized system**.
  Scenario: Let's consider there is a manufacturing company which wants to produce products efficiently, blockchain in this case will not be helpful.

2.3 Applications of Blockchain

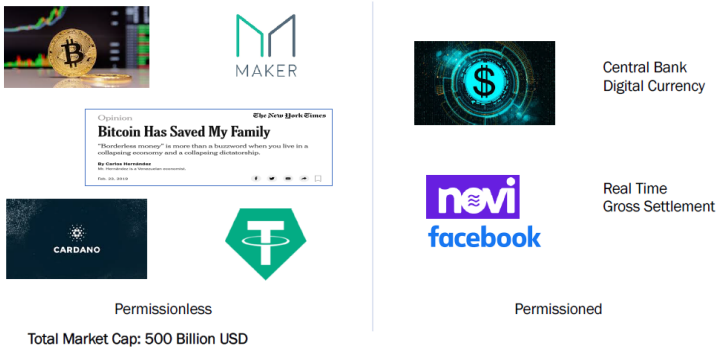

Figure 2.1: Applications of Blockchain : Cryptocurrencies

2.3.1 Cryptocurrencies

A cryptocurrency is a digital token designed to work as a medium of exchange. Many cryptocurrencies are based on decentralized systems based on blockchains like Bitcoin, Corando and so on. These are all based on permissionless blockchain. That means anyone can join and leave the

blockchain network. On the other hand there are applications like Central bank digital currency (CBDC), based on permissioned blockchain. In case of permissioned blockchain, blocks need permission from the creator to participate.

2.3.2 Applications beyond Cryptocurrencies

There are many other applications of blockchain beyond cryptocurrencies. These are some examples:

Figure 2.2: Applications beyond Cryptocurrencies

2.3.3 Projected Application

There are some following projected applications of blockchain in different areas like food safety and origin registration tracking, voting, new music release, drug supply chain and so on. Many companies in the food industry are using blockchain to prevent agricultural fraud and improve food safety. Security of the digital voting is always a big question. With the utilization of blockchain a safe and robust framework for digital voting can be devised. In today's music industry, blockchain has created a whole new level of inter-mediation between artists and fans. It also provides cost effective and user friendly alternatives to piracy, giving royalties to artists. Blockchain technology is used in pharmaceutical industry to fix supply chain vulnerabilities in a cheaper, easier and faster way.

2.4 Big Gap

Many intermediaries which are purely digital could be potentially utilize blockchain if there was enough throughput. Throughput refers to the ability to process transaction at which valid transactions are committed by the blockchain. Today's blockchain infrastructure does not have enough throughput. For example Etherum has a throughput 20 Tx/ sec but some the digital applications need 10K Tx/sec. So we can see there is a huge gap between our desired and current level of throughput.

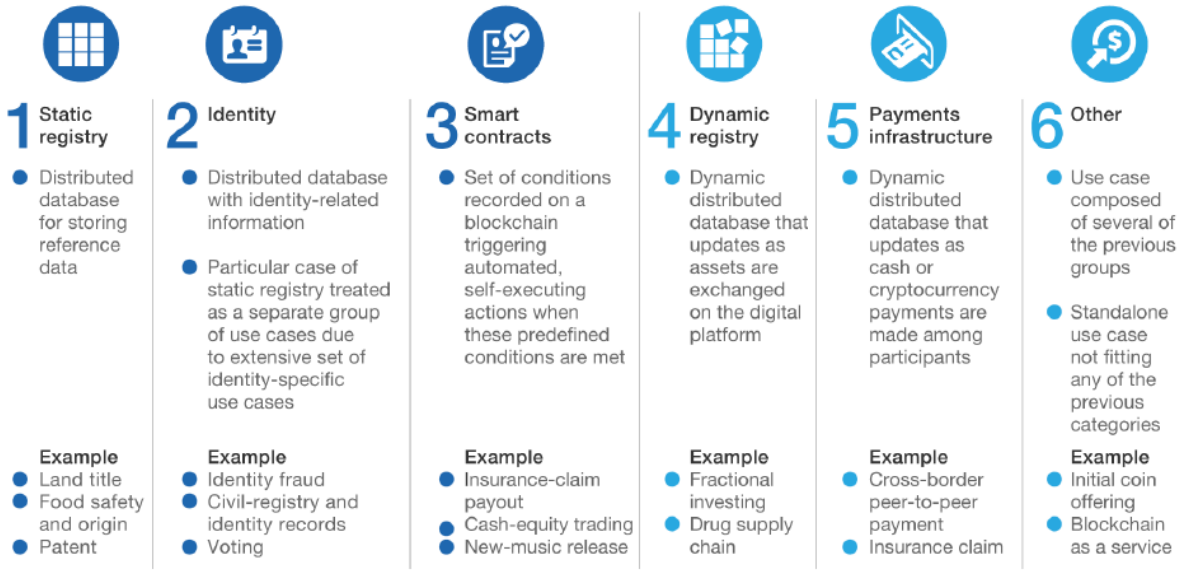

Figure 2.3: Projected Applications

2.5 Cryptographic Primitives

2.5.1 Collision Resistance Hash Function

- Hash Function: The hash function takes a big message space (long file or string) and maps it to a small set of bits.

$$H : M \to T \text{ is a hash function where } |M| \gg |T|$$

  It is easy to compute $H(x)$ given x but given $H(x)$ it is "hard" to find x.
- Collision Resistance: A collision for H is a pair $m_0 \neq m_1 \in M$ such that: $H(m_0) = H(m_1)$.

A function $H : M \to T$ is collision resistant if it is "hard" to find even a single collision for H.

2.5.2 Digital Signature

In the digital world, it is easy to copy a signature which leads to a binding problem. The signing algorithm takes as input the secret key (i.e the signing key) and message, and outputs the digital signature. There is an entity called a verifier which takes as input signer's public key, digital signature and the message. It outputs "accept" or "reject" based on the match. This signature scheme consists of the following three algorithms:

- Gen(): This outputs a public key and secret key pair (pk, sk).
- Sign(sk, msg): This algorithm takes as input a secret key and message. It outputs signature σ.
- Verify(pk, msg, σ): This algorithm is run by the verifier. It takes as input pk, msg and signature σ. It outputs "accept" and "reject".

Secure signatures: Adversaries who see signatures on many messages of his/her choice, cannot forge a signature on a new message.

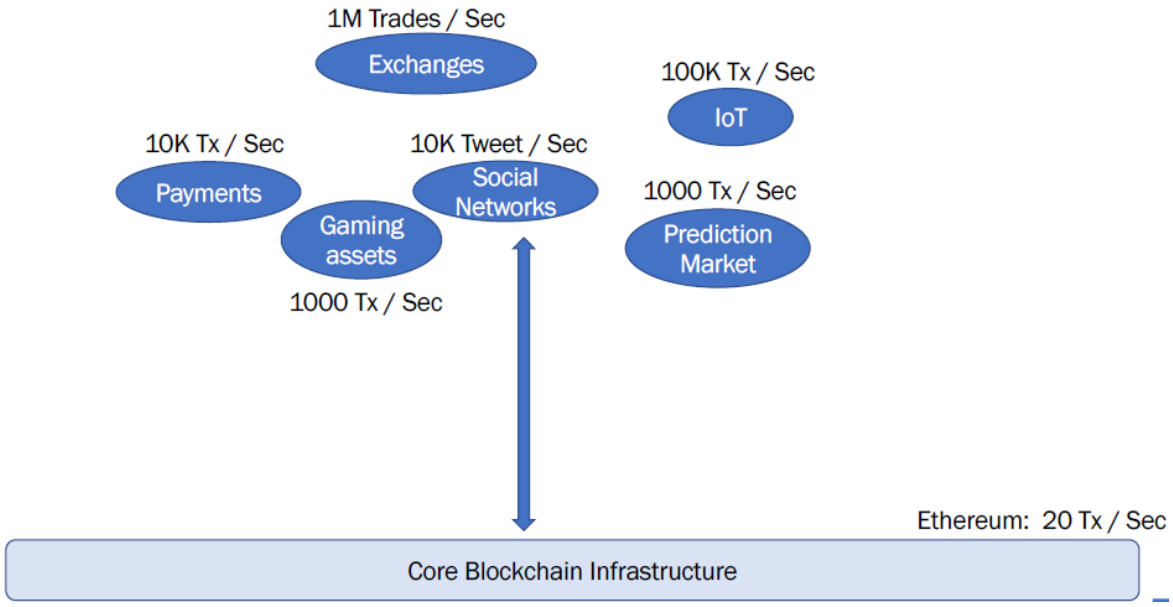

Figure 2.4: Projected Applications

Figure 2.5: Hash Function

2.6 Bitcoin: Case Study

Bitcoin is a purely peer-to-peer version of electronic cash that allows online payments to be sent directly from one party to another without going through a financial institution. It was launched in January 2009 by a person or a group of people under the pseudo-name Satoshi Nakamoto.

2.6.1 How does Bitcoin work?

There is a sequence of blocks in the chain. The ledger is recorded over this sequence of blocks. The ledger is maintained by group of nodes in the blockchain network. Firstly there is a root block called the genesis block and this block is broadcast to all other nodes. We can think of this chain as a tree where each node keeps track of the previous all nodes. The goal in the network is to work together and continue growing the chain.
Mining is the process which generates new blocks and keeps adding the block to the chain if the mining succeeds. Each node in the network gets this newly mined block through broadcasting. When miners receive this block then each miner check if the mining procedure is correct. If all the miners verify that the mining process is correct then they attach the block to the local version of the blockchain. Therefore all the nodes eventually keep up the same sequence of blocks.

2.6.2 Bitcoin Primer - Mining

Each block stores a bunch of transactions and they are connected by an arrow called pointer. A miner checks a bunch of transactions and adds the block to the chain.