# Building Software Systems

Lecture 6.3

## Blockchain Applications

SAURABH SRIVASTAVA

ASSISTANT PROFESSOR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

IIT (ISM) DHANBAD

# Recap ...

Till now, we have discussed the fundamental concepts and the technologies behind a blockchain

- For instance, we discussed the concepts of Digital Signatures and Merkle Trees

Now, we will discuss how Blockchains are usually used in a real-world scenario

# The concept of Proof-of-Work

The credit for the blockchain data structure, in its current form, goes to *Satoshi Nakamoto*

- The person (whose identity is still a mystery) defined blockchains to be used for a decentralised currency …
- … called the bitcoin (we have been seeing its examples all this while)
- One of the problems that was tackled successfully in the paper, was that about *trust* in a decentralised system
- In the absence of a central authority, there is no way to differentiate between the good and the evil
- By evil, we mean people who wish to spend the same money twice – or manipulate the ledger illegally
- The provided solution is called Proof-of-work – the idea was to "incentivise" the good nodes for their work

To do so, two fields were introduced in the block header

- The *Nonce* field is a counter that is incremented by one after each iteration of a process called *mining*
- The idea is to find the hash of the block header, with different Nonce values, until we achieve a "suitable hash"
- The suitability may be defined in different ways – e.g., the hash must start with *n* zeros on the left
- If we increase the value of n, the problem becomes harder – this value becomes the *difficulty target* to achieve
- If a node solved this hard problem – the node gets some currency or credit in the system (the incentive) !!

# Demo of Mining Process

HTTPS://ANDERSBROWNWORTH.COM/BLOCKCHAIN/BLOCKCHAIN

# Need for a “blockchain-like” solution

In January 2010, Haiti was devastated by an earthquake

- Around 2,50,000 residences and 30,000 commercial buildings were estimated to have collapsed
- However, reconstruction activities were hampered due to a lack of undisputable land records
- In fact, only about 5% people had proof of their land ownership even before the earthquake

Even in places where land records are maintained, a centralised control may not be trusted

- This is true especially for the countries where corruption is rampant
- Officials may manipulate records – possibly created decades ago “on paper” – for malicious benefits

This provides a strong need for a digital storage solution which …

- … is tamper-proof, or at least, resistant to changes, and …
- … is decentralised, i.e., not under the control of a single, centralised entity

A solution based on Blockchains can provide both these features

- The chain of hashed headers, coupled with a distributed structure, fulfils both the above criteria

# Applications of Blockchains (1/3)

The initial applications of Blockchains were in the field of Payments

- Bitcoin – the digital currency we have been discussing all this while – was the first on the scene
- Since then, multiple currencies, colloquially called “cryptocurrencies” have propped up
- Although there are many such currencies, the lion’s share is between Bitcoin and *Ethereum*

Blockchains are also being used in the field of Digital Arts

- A novel concept, called a Non-Fungible Token or NFT is a blockchain-based solution for selling digital arts
- An NFT creates a digital identity for a digital art such as a painting …
- … whose ownership can be transferred from one owner to another
- These transactions are stored on a blockchain (more often on Ethereum) which can be verified publicly

Blockchains have a great future in building voting systems

- Voting – either physical or digital – has the same challenges as we discussed for the land records example
- Blockchains – along with smart contracts (code to enforce voting protocols) – can be used to do the same

# Applications of Blockchains (2/3)

Another major field where Blockchains are being used is Healthcare

- One of the major challenges in the field of healthcare is trustworthy and secure patient data
- Kept in the form of Electronic Health Records, they are stored with central (usually government) agencies
- Blockchain-based solutions are being adopted to decentralise the same for better availability
- Well-sequenced, trustworthy electronic health records are also being used to build inferencing solutions …
- … through the application of Machine Learning models using smart contracts

Blockchains are also revolutionising the supply chain

- A major issue with supply chains is assuring that a product's quality and quantity be tracked as it travels
- The product may go through multiple independent businesses across multiple geographic locations
- Decentralised solutions built over permissioned blockchains are proving to be a good option for businesses
- The resistance to change also makes these solutions provide guarantees ….
- … that an entity cannot change its reported states of the product later with a malicious intent

# Applications of Blockchains (3/3)

A typical example of Applications of Blockchain in supply chain is one built by RCS global

- They built a global blockchain-based solution called the Responsible Sourcing Blockchain Network (RSBN)
- Built over the IBM Blockchain Platform, the project was initiated in the Democratic Republic of Congo (DRC) …
- … to ensure traceability of minerals from mines to the end product

Anyone in the supply chain of the Lithium-ion (Li-ion) batteries could join RSBN

- The idea is to track the mined elements for the same such as Lithium, Nickel, Cobalt and Copper
- If a participating organization produces some raw material of interest in some mine in DRC …
- … it can be traced from a smelter, a cathode plant, a battery-production plant, and even …
- … till to the appliance in which the battery was finally installed