CSE446: Blockchain & Cryptocurrencies

Lecture – 21: Blockchain Feasibility, Security & Governance

Inspiring Excellence

Agenda

- Blockchain Governance
- Advanced concepts

Blockchain Governance

- Governance is a structure through which a participant or user of a system uses and participates in the system
- Almost every social structure has some sort of governance
- Governments are a prime example of how governance functions
- There are different types of governments and modes of governance
- There are three entities that dictate governance
  - Rulers
  - Rules
  - Participants

https://101blockchains.com/blockchain-governance/

Blockchain Governance

- Simply, the ruler set the rules based on the participant's goals and needs
- For any governance system to work properly, all the three elements need to work together and play nicely without interrupting the other
- You can look at big countries, for example, to understand the different governance models
- China's approach is different as they have a one-party governance system
- Other countries deploy a democratic approach where people decide their government

https://101blockchains.com/blockchain-governance/

Blockchain Governance

- There are two types of Governance in Blockchain:
  - Off-chain governance
  - On-chain governance

https://101blockchains.com/blockchain-governance/

Off-chain Governance

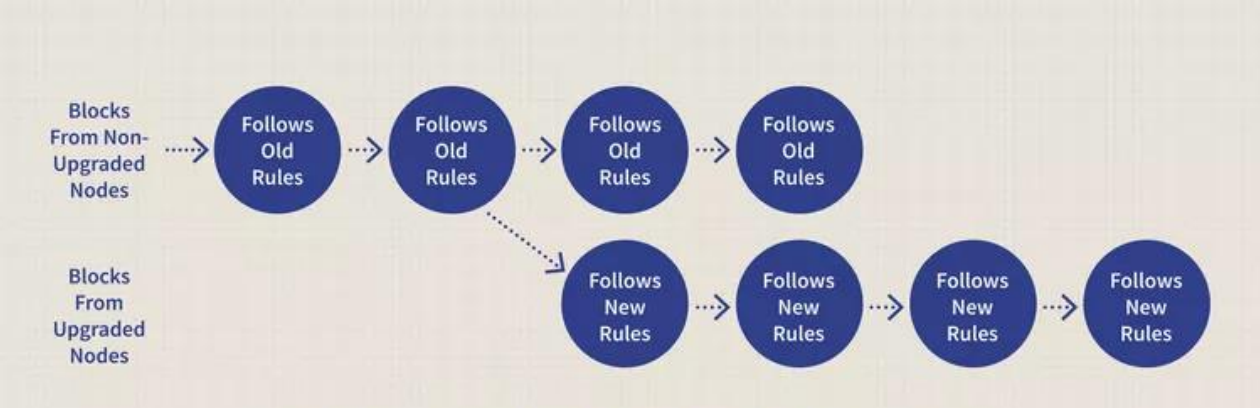
- In an off-chain Governance model, all the major changes proposed to a blockchain system are thoroughly discussed online by key stakeholders
- The key stakeholders include the core development team, other developers, miners/stakers, researchers, and the end-user community
- Bitcoin and Ethereum use this model
- In this model, major changes are proposed as improvement proposals known as Bitcoin Improvement Proposal (BIP) or Ethereum Improvement Proposal (EIP)
- The core development team of the blockchain system holds regular online meetings where anyone is welcome to participate
- As per their discussion, a particular BIP or EIP is chosen

Off-chain Governance

- The corresponding proposal is then developed in the core code base of the blockchain system
- Now then question is: how to introduce this in the live blockchain system?
- In a traditional system, the software/server is placed under maintenance and becomes offline
- However, a live blockchain can never be down for a single moment
- Everyone is requested to update the core software
- The requested change is set to be activated in future from a certain block onwards

Off-chain Governance

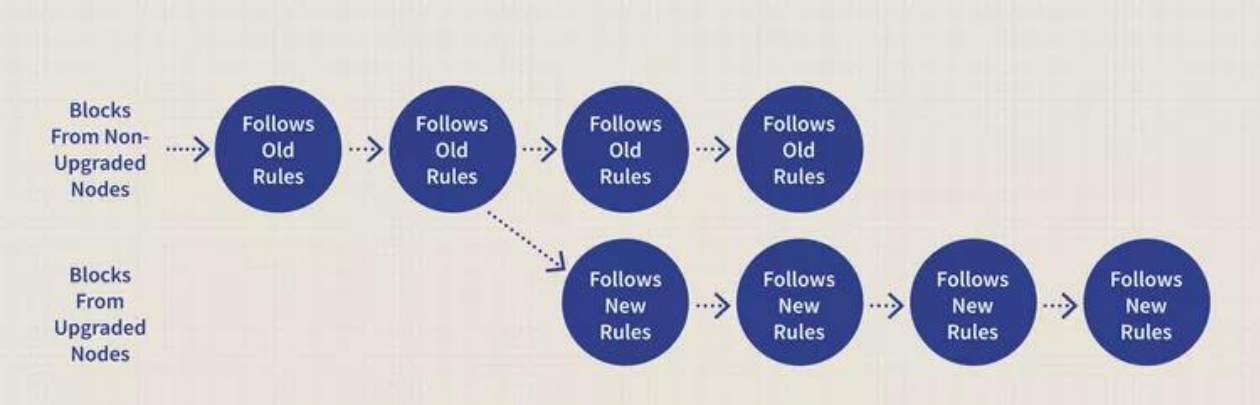
- Adopting a particular proposal essentially creates a fork in the system
- There could be two such forks: hard fork and soft fork



https://www.investopedia.com/thmb/Wo9jkeb4IULyAk1TrgOQRtmwUMQ=/750x0/filters:no_upscale():max_bytes(150000):strip_icc():format(webp)/HardForkBlockchain3-6f5d8ce52f8a4dcba1137264e0d6c2d6.png

Off-chain Governance

- A hard fork refers to a radical change to the protocol of a blockchain network that effectively results in two branches, one that follows the previous protocol and one that follows the new version
- In a hard fork, miners must choose which blockchain to continue verifying
- With a soft fork, only one blockchain will remain valid as users adopt the update



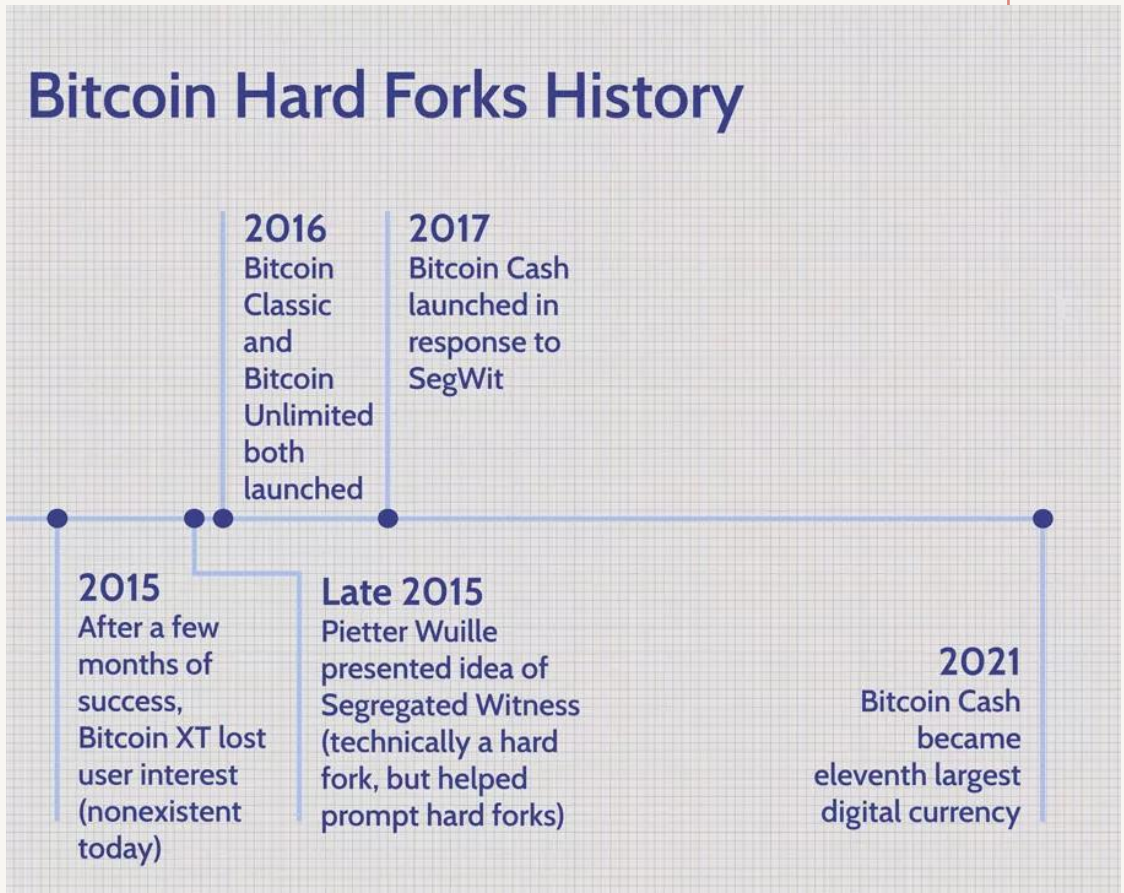
https://www.investopedia.com/thmb/Wo9jkeb4IULyAk1TrgOQRtmwUMQ=/750x0/filters:no_upscale():max_bytes(150000):strip_icc():format(webp)/HardForkBlockchain3-6f5d8ce52f8a4dcba1137264e0d6c2d6.png

Off-chain Governance

- How this change is adopted entirely depends on the miners/stakers adopting this particular change
- Miners update their software to signal that they agree to this particular change
- If there are some miners who do not agree to a particular proposal, they might continue mining on the previous branch
- An interesting case is the Bitcoin fork

Off-chain Governance

- In order to scale Bitcoin, many argued to increase the block size
- This resulted in a number of Bitcoin forks
- Notable is the Bitcoin Cash launched in 2017, created in response to SegWit
- SegWit (Segregated Witness): reducing transaction size so that more transactions could be accommodated without modifying bitcoin block size
- Bitcoin Cash introduced 8MB block size



https://www.investopedia.com/thmb/b7njmOEAD2GyTjzW3-vXVpOqUGc=/750x0/filters:no_upscale():max_bytes(150000):strip_icc():format(webp)/dotdash-history-bitcoin-hard-forks-Final-038926240447463 08f36e9002031f830.jpg

On-chain Governance

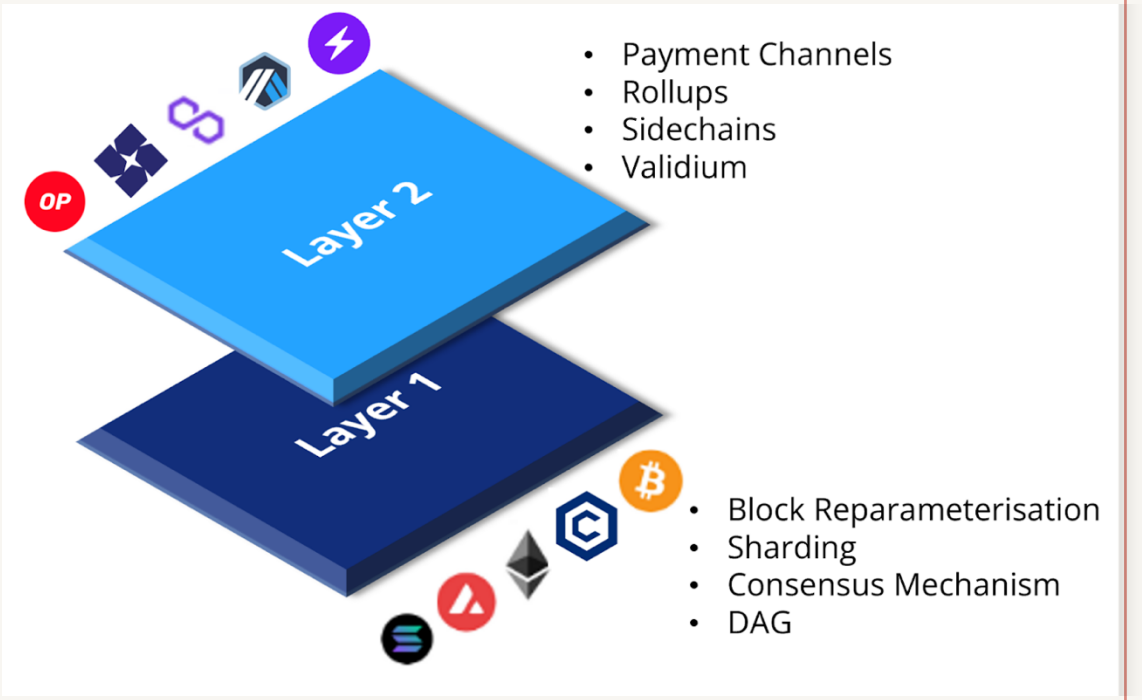
- On-chain governance is a system for managing and implementing changes via blockchain systems
- Developers propose changes through code updates and each node or participant votes on whether to accept or reject the proposed change
  - These votes are stored on-chain
- Typically, on-chain governance involves the following stakeholders: Miners, Developers and Users
- Stakeholders in the process are provided economic incentives to participate
- For example, each node can earn a cut of overall transaction fees for voting, while developers are rewarded through alternate funding mechanisms

Advanced concepts

- Three major advanced concepts to address the scalability and privacy issues of blockchain
  - Layer 2 solution
  - Sharding
  - ZKP (Zero-knowledge Proof)

Layer 2 solution

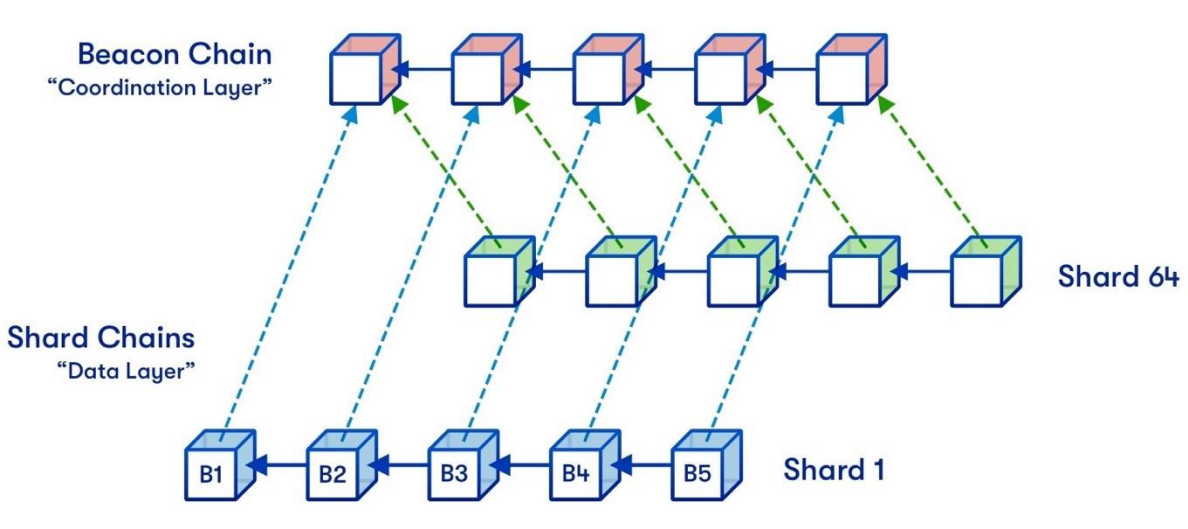
- Layer-1 refers to the main blockchain
- Layer-2, however, is an overlaying network that sits on top of the blockchain
- Lightning Network is the Layer-2 solution for Bitcoin
- Plasma, Polygon, Optimism, and Arbitrum are just a few of the Layer-2 networks built on Ethereum



https://lh4.googleusercontent.com/B1uC_R-1QjLjiUyluH8AsNvlypLA08KJhh4xKimpCIxzJscitYNgrsixZmcnhAj0Umq_bL7yghOzr9nyRQjAsL66uQjxGG8YQoMvNKRmVz1-g0nWxkh3OOl1BalAHgnmreXsLAmcRe7m1R_C6Q

Sharding

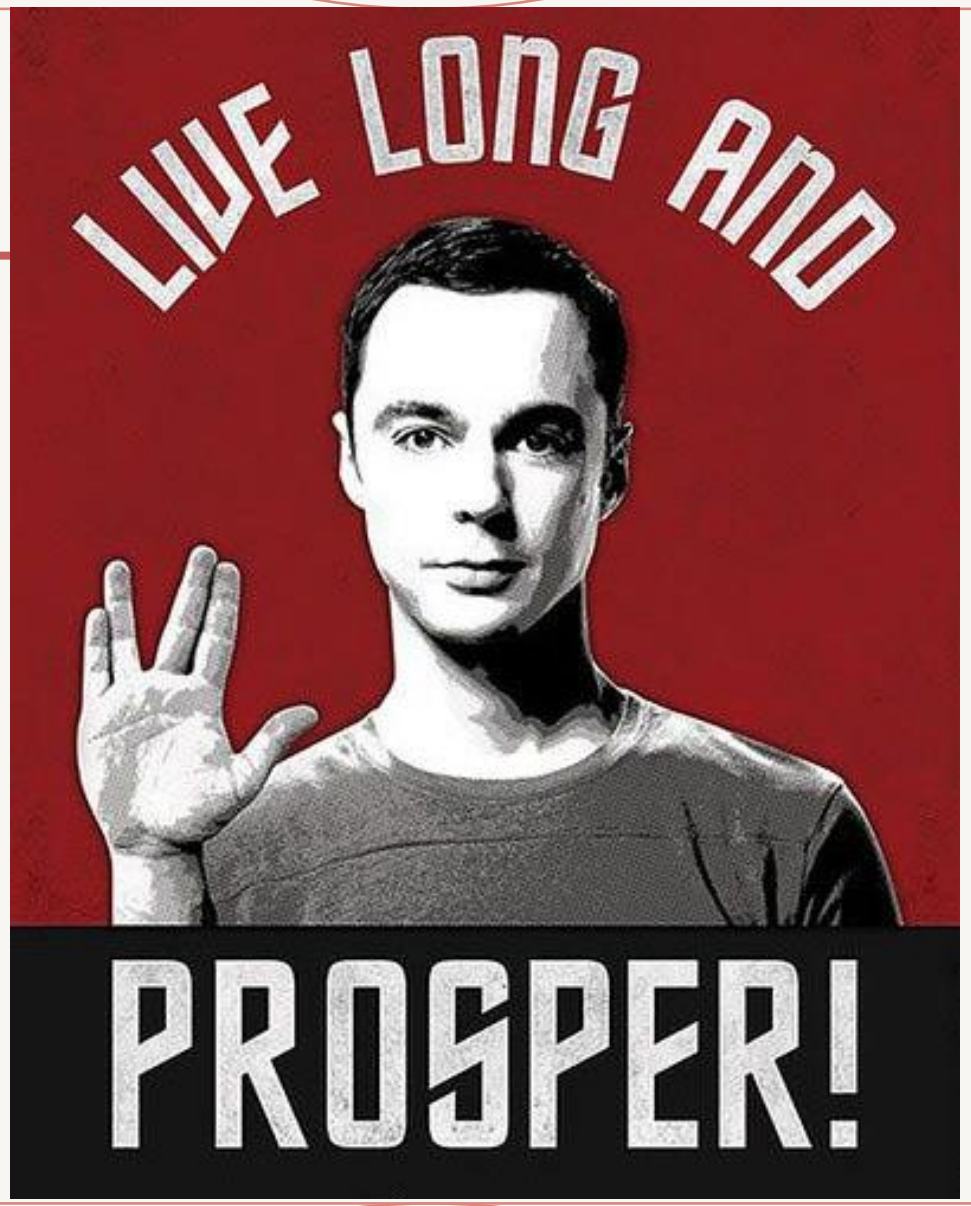
- Sharding is a method of database partitioning that is utilised by blockchain organisations to increase scalability
- This enables them to execute a greater number of transactions per second and store data across multiple nodes in a sustainable way



https://vitalik.ca/images/sharding-files/beacon_chain.jpg

ZKP (Zero-knowledge Proof) in blockchain

- ZKP is a method by which one party can interacts with another party and provides proof of knowledge without unveiling their confidential data
  - Say there are two millionaire and they would like to determine who is richer without revealing their total assets
  - Logging in to an online system without providing passwords
- ZKP facilitates this by using advanced cryptographic mechanisms
- In blockchain, ZKP facilitates private transactions and others
  - Nobody in the blockchain knows who is the sender and who is the receiver
- Example: ZCash


LIVE LONG AND
PROSPER!