Course II:

DeFi Primitives

4. Joining the World of DeFi

(ii) Blockchain Tech Big Picture

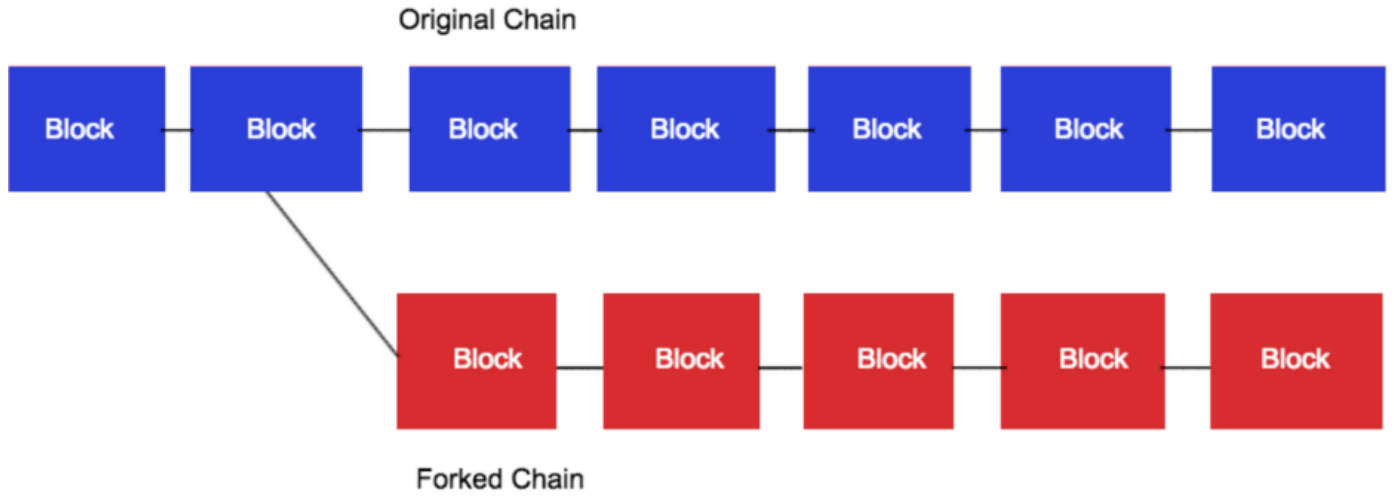
e) Cross-chain, Immutability, Oracles, Privacy

Tech Big Picture

- **Connection**: Are we headed to a world of millions if not billions of blockchains – or will there be one Masterchain?

Tech Big Picture

- **Immutability**: This is a crucial characteristic of a blockchain. What are the guarantees on my transaction?
  - Block confirmations
  - The issue of forks
    - Bitcoin Cash 1 Aug 2017
    - Bitcoin Gold 24 Oct 2017
    - Bitcoin SV 15 Nov 2018



https://hackernoon.com/blockchain-forks-b0dca84db0b0 https://www.investopedia.com/tech/history-bitcoin-hard-forks/

Tech Big Picture

- **Real world verification**: How do we verify events in the real world trustlessly on a digital and siloed blockchain?
  - Much work needs to be done on oracles (software, hardware, inbound, outbound, and consensus based). How do we trust the oracle?
  - RFID tags?

By KufoletoAntonio De Lorenzo and Marina Ventayol - Own work, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=3314736

https://blockchainhub.net/blockchain-oracles/

Tech Big Picture

- **Governance**: We are only now thi… go…e. This is very much related to consensus mechanisms – but broader in that the computer programs that generate current blockchains will surely need improvement and enhancements in the future. Who will do this? (BIP/EIP for example.)
  - Much research on consensus mechanisms.
  - What will the world look like with potentially millions of DAOs?

Tech Big Picture

- **Privacy**: Delicate balance needs to be achieved. No one has worked it out yet.
  - This is not just a blockchain issue!




Tech Big Picture: Zero Knowledge Proof

How is a voting blockchain feasible if the government can see how everyone votes?

- The answer is a **zero knowledge proof**
- This means that you provide cryptographic proof that you are a valid owner of a voting token – yet you do not have to reveal who you are.

Tech Big Picture: Zero Knowledge Proof

- Imagine your friend is color-blind.
- You have two billiard balls; one is red, one is yellow, but they are otherwise identical.

- To your friend, they seem completely identical, and he is skeptical that they are actually distinguishable. You want to prove to him that they are in fact differently-colored. On the other hand, <u>you do not want him to learn which is red and which is yellow</u>.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Tech Big Picture: Zero Knowledge Proof

Proof system:

- You give the two balls to your friend so that he is holding one in each hand.
- You can see the balls at this point, but you don't tell him which is which.
- Your friend then puts both hands behind his back. Next, he either switches the balls between his hands, or leaves them be.
- Finally, he brings them out from behind his back. You now have to "guess" whether or not he switched the balls.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Tech Big Picture: Zero Knowledge Proof

Proof system:

- By looking at their colors, you can determine whether or not he switched them. If they were the same color, there is no way you could guess correctly with probability higher than 1/2.
- If you and your friend repeats this T times (for large T), your friend should become convinced that the balls are indeed differently colored; otherwise, the probability that you would have succeeded at identifying all the switch/non-switches is at most $(1/2)^T$
- Furthermore, the proof is "zero-knowledge" because your friend never learns which ball is yellow and which is red; indeed, he gains no knowledge about how to distinguish the balls.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Tech Big Picture: Zero Knowledge Proof

Key idea:

- Zero knowledge proof is the ability to prove a secret without revealing what the secret is
- Sometimes called zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge)

https://medium.com/coinmonks/blockchain-zero-knowledge-proof-in-a-nutshell-f0684a669a68


Asymmetric-key-cryptography
Scaling-risk
AMM
Proof-of-stake
Yield-farming
Vertical-scaling
DEX
Nonce
Sharding
Slashing
KYC
Address
Vampirism
Mint
Invariant
Schelling-point-oracle
Direct-incentive
DAO
Halting-problem
Testnet
ERC
Optimistic-rollup
EOA
Airdrop
Fork
Keeper
Smart-contract
Oracle
Double-spend
Gas
Hexadecimal
Burn
Miner
Mainnet
PoS
Defi-Legos
Consensus-protocol
Layer
Utility-token
Flash-swap
Horizontal-scaling
Miner-extractable-value
Flash-loan
PoW
IDO
Contract-account
dApp
Node
Vault
Stablecoin
Router-contracts
Symmetric-key-cryptography
Digest
Impermanent-loss
Bonding-curve
Governance-token
Hash
Proof-of-work
DeFi
Staking


Asymmetric-key-cryptography
Scaling-risk
AMM
Proof-of-stake
Yield-farming
Vertical-scaling
DEX
Nonce
Sharding
Slashing
KYC
Address
Vampirism
Mint
nvariant
Schelling-point-oracle
DAO
Optimistic-rollup
ERC
EOA
Airdrop
Fork
Oracle
Keeper
Smart-contract
Double-spend
Gas
Hexadecimal
Burn
Miner
PoS
Mainnet
Defi-Legos
Consensus-protocol
Layer
Utility-token
Flash-swap
Horizontal-scaling
Miner-extractable-value
Flash-loan
PoW
IDO
Contract-account
dApp
Node
Router-contracts
Symmetric-key-cryptography
Digest
Impermanent-loss
Governance-token
Hash
Proof-of-work
DeFi

Course III: DeFi Deep Dive

Next

- We will do a **DeFi Deep Dive** looking at specific applications including: Credit/Lending, Decentralized Exchange, Derivatives and Tokenization