Bitcoin

Lecturer: Dr. Joseph Doyle

Some slides based on material found at https://blockchain.berkeley.edu/decal/fa18/fund/

Introduction

- Bitcoin is a cryptocurrency created in 2008 by Satoshi Nakamoto
- A cryptocurrency can be defined as “a currency built upon computer science, cryptography, and economics”
- Essentially the idea is that it is not controlled by a central authority and is purely digital
- The data structure known as blockchain is used to implement bitcoin and this was its original use

Blockchain Introduction

- There are a lot of miscon about blockchain but it can be defined as “a method of storing d ngst multiple parties that ensures data integrity”
- It is a distributed ledger or shared database where every participant holds a copy
- It is useful as data committed to the blockchain cannot be changed
- It is also useful for ensuring transparency as all transaction are recorded in the ledger

Blockchain Misconceptions

- Enterprise blockchains are always useful
- Blockchains are more efficient
- Blockchains are cheap
- Building your own blockchain is easy
- Essentially results in glorified public key cryptography

Bitcoin Components

- There are four principal components to Bitcoin namely:
  - Identity
  - Transactions
  - Record-Keeping (Blockchain)
  - Consensus (Proof-of-Work)

Bitcoin Identity

- Identities in Bitcoin are used to:
  - Receive money
  - Spend/Claim Money
  - Blame
- In Bitcoin public and private keys are used to as identities

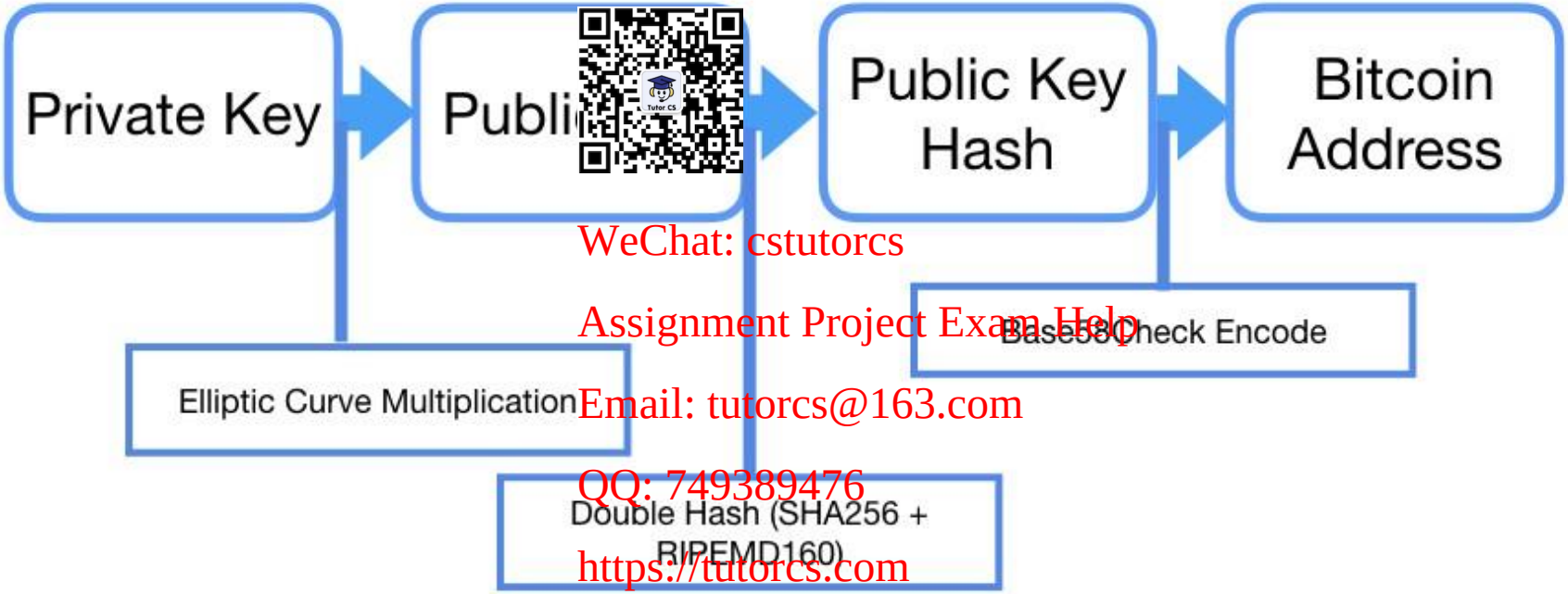
Bitcoin Identity

- The private key acts as a key to unlock the public key and the money associated with it
- The public key is for receiving Bitcoin
- The private key is chosen at random and the public key is generated from this private key
- Bitcoin is hidden in a large amount of public keys 2^{160}
- Practically impossible for anyone to overlap assuming the random generation of a public key

Bitcoin Identity

- Bitcoin uses the Elliptic C[illegible]ital Signature Algorithm (ECDSA) to generate its public and p[illegible]ys
- Essentially this algorithm uses a trapdoor function which is a mathematical function that is difficult to invert but easy to calculate initially
- The hashing function SHA-256 (more on this later) and the RACE Integrity Primitives Evaluation Message Digest (RIPEMD) are then used along with base 58 encoding to generate the Bitcoin address along with a prefix and a checksum to make it evident if there has been tampering

Bitcoin Identity



https://medium.com/coinmonks/what-is-a-bitcoin-address-6c822c857004

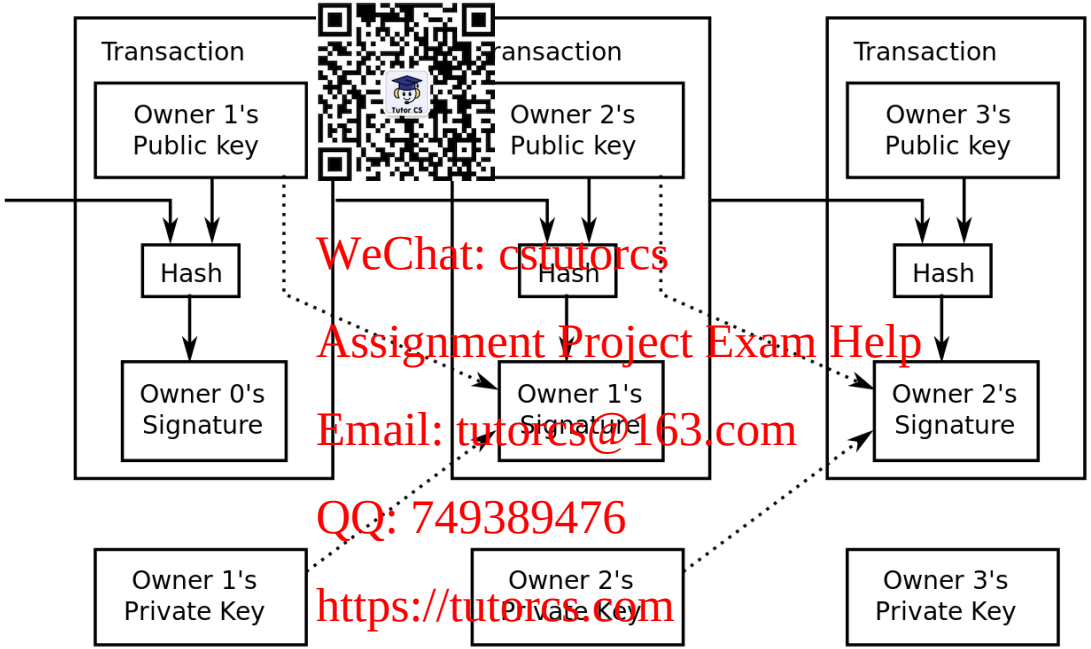
Bitcoin Transactions

- In Bitcoin each account holds a set of unspent Transaction Outputs (UTXOs)
- A UTXO can contain any amount of Bitcoin and is spend in its entirety
- A UTXO can be redeemed only once
- Transactions contain a signature of the owner of the funds

Bitcoin Transactions

- Each transaction consists of one or more inputs and one or more outputs
- To prevent double spend, an input must refer to a UTXO
- If the sum of the inputs exceeds the sum of the outputs and additional output is used to return the change to the owner of the UTXO
- If the private key is lost the Bitcoin network will not recognize any other form of ownership
- Interestingly, about 20% of Bitcoins are believed to be lost ~ £8 billion as of December 2018

Bitcoin Transactions

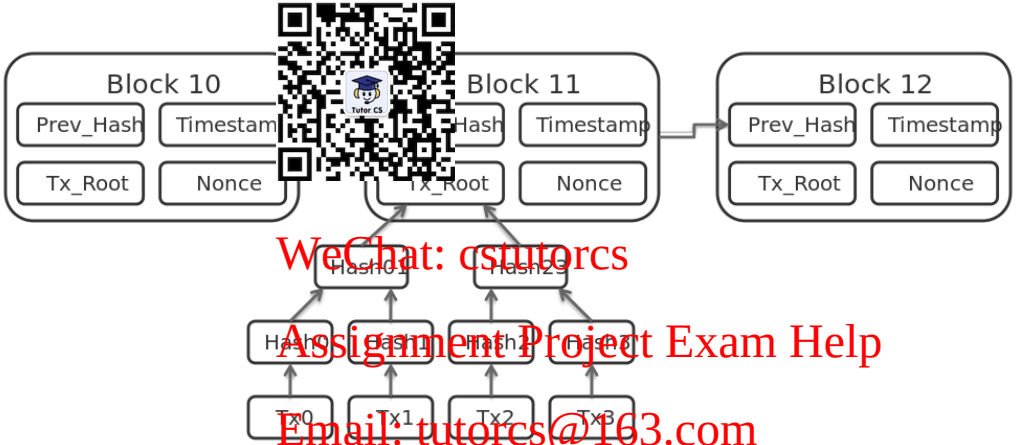


https://en.wikipedia.org/wiki/Bitcoin

Bitcoin Blockchain

- These transactions are stored in a distributed database known as a Blockchain
- The transactions are compiled into blocks and stored in a Blockchain
- Each participant in the network maintains a copy of the Blockchain
- New blocks need to be validated before they can be added to the Blockchain

Bitcoin Blockchain



https://en.wikipedia.org/wiki/Blockchain

Blockchain Security Concerns

- Double Spend: A user attempts to send the same Bitcoins to different users
  - In principal, we could prevent this by asking participants to vote to determine if a transaction is valid but as it is inexpensive to create a Bitcoin identity it is still vulnerable
- Sybil Attack: A user attempts subvert a reputation system by forging identities
  - To prevent this attack a mechanism which requires significant resources must be utilised to validate transactions. A user with multiple identities will still have resource constraints which prevent Sybil attacks. In Bitcoin the mechanism is known as proof-of-work

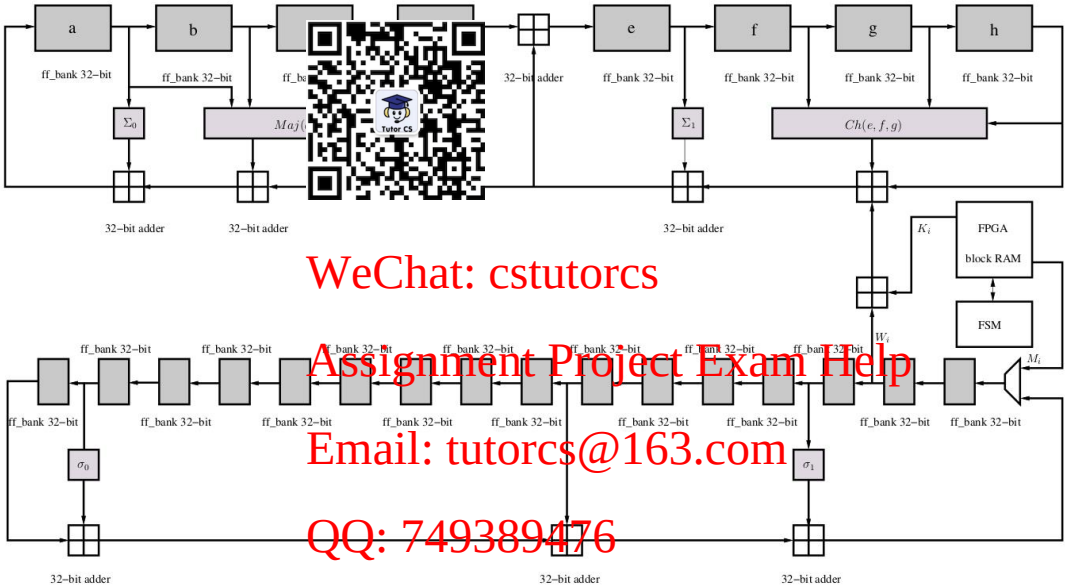
Bitcoin Blockchain proof-of-work

- Transactions are grouped together into block which contains a hash of the previous
- The hashing function used is SHA-256
- For the new block to be accepted by the distributed Bitcoin network a node needs to find a nonce which can be combined with the block to produce a hash that is smaller than the networks difficulty target

SHA-256

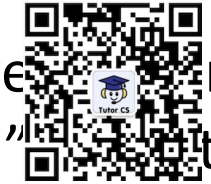
- This hashing function is designed by the NSA
- It has three properties which make it useful for securing the Bitcoin network namely
  - If a user has the hash it is computationally difficult to determine the input of the hashing function
  - If a user has the hash it is computationally difficult to determine an input that would produce the same hash
  - It is computationally difficult to find two inputs which will produce the same hash

SHA-256



https://opencores.org/usercontent/img/1375985843

Bitcoin Blockchain proof-of-work (example)



- For example if we we mpting to find a nonce for the String “Hello World!” the SHA-256 hash that was smaller than a difficult target e.g. Need to have four leading zeros
- The nonce can be determined to be 4250 on this case

Bitcoin Blockchain proof-of-work (example)

- Difficulty target => 0001000000000[illegible]0000000000000000000000000000000000000000
- "Hello, world!0" => 1312af178c253f[illegible]a6adc1e25e81caa44c749ec81976192e2ec934c64
- "Hello, world!1" => e9afc424b79e4f[illegible]31156d3a17228d6e1eef4139be78e948a9332a7d8
- "Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
- ...
- "Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
- "Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
- "Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9

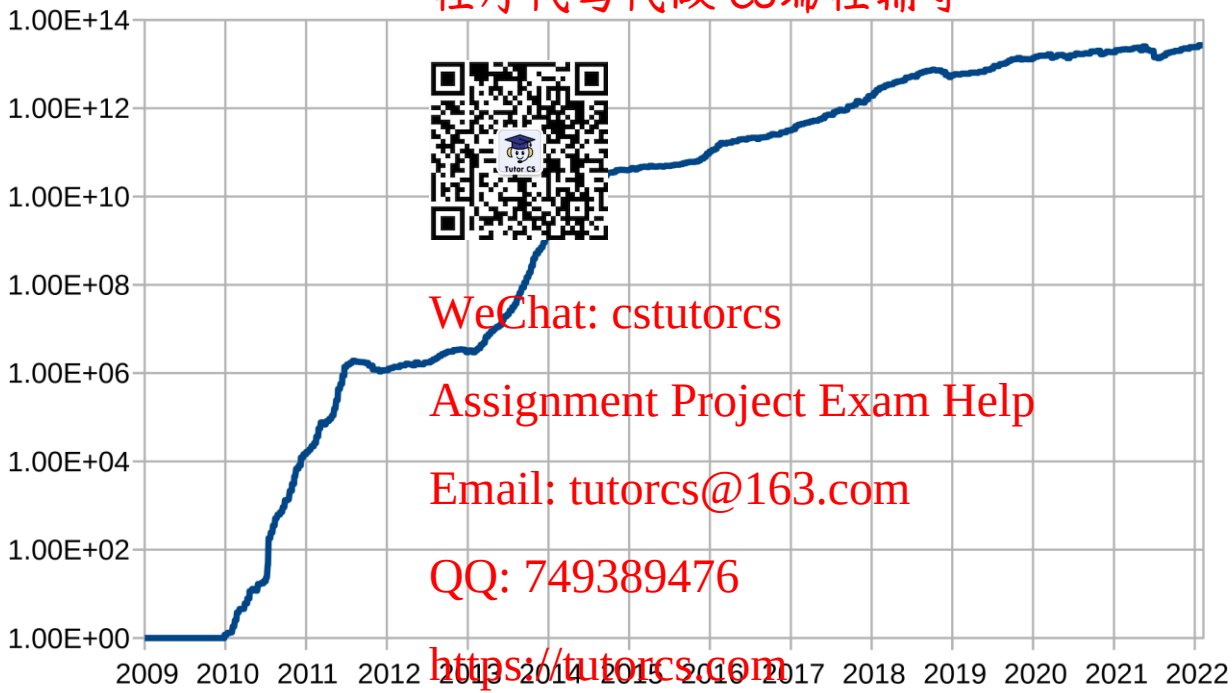
Blockchain Validation

- Once the nonce is calculated it is easy to achieve consensus as it only requires one use of the hash function to verify the new block.
- Thus consensus in the network can be achieved rapidly

Blockchain Miners

- In order to encourage the ca[illegible] of nonces and the validation of transaction Bitcoin is offered as a rewar[illegible]icipants who discover the nonce for a block of transactions
- Difficulty target is adjusted every 2016 blocks with the goal of keeping the average time between new blocks at approximately 10 minutes
- Unfortunately this means that the difficulty has been increasing exponentially as Bitcoin becomes more popular
- Transaction fees can be used to encourage miners to process a particular block
- This also discourages the use of micro transactions which negatively effect the network

Blockchain Difficulty



https://en.wikipedia.org/wiki/Bitcoin

Blockchain Miners

- As of May 2020 6.25 Bitc[illegible] the reward for successfully adding a blockchain
- This reward is designed to half every 210,000 blocks (approximately every 4 years) until it eventually drops to zero when the limit of 21 million Bitcoins is reached
- At this point miners will only receive transaction fees when processing new blocks
- This is expected to occur circa 2140

Bitcoin Numbers

https://en.wikipedia.org/wiki/Bitcoin

Blockchain Hardware

- Different hardware can be used to find nonces namely
  - CPU
  - GPU
  - FPGA
  - ASIC

Blockchain Hardware

	Ha[illegible]	Time to block (years)
CPU	20[illegible]	7,620,101
GPU	200 million	762,010
FPGA	1 billion	152,357
ASIC	14 trillion	10.88

https://blockchain.berkeley.edu/decal/fa18/fund/

Blockchain Hardware

- CPU
  - Only used in the early days of Blockchain
  - Complicated instruction set which is not really suitable for Blockchain
- GPU
  - Most common in 2012
  - An order of magnitude faster than CPU
  - Consumes a lot of power and has other components which are not useful for mining

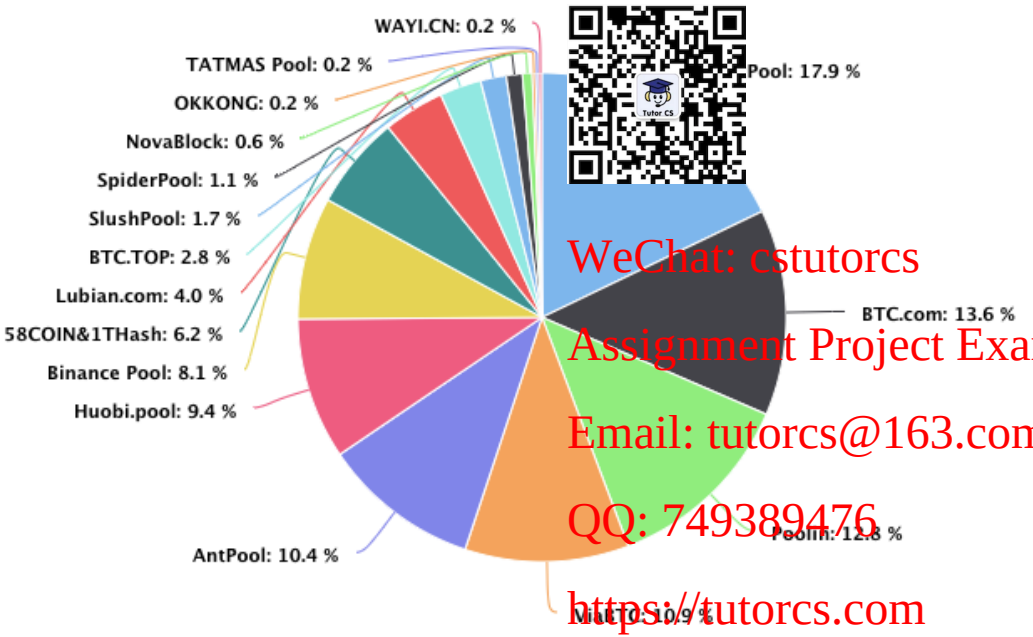
Blockchain Hardware

- FPGA
  - Niche technology but can be programmed to do other things
  - Last piece of technology that is not completely useless if Bitcoin fails
- ASIC
  - Only performs SHA-256
  - This requires a large upfront cost
  - Antminer S9 (14 TH/s): $3000

Mining Pools

- Being an individual miner is considered quite risky so miner tend to join pools to manage the risks
- This reduces the variance in mining rewards
- Run by a pool manager or pool operator
- The manager usually takes a cut of the mining rewards

Mining Pools



https://changelly.com/blog/bitcoin-mining-pools/

Mining Pools

- Miners in a pool s shares which are “near-valid” blocks to the pool manager
- The number of shares is proportional to the computational power being expended
- The pool operator pays for valid shares
- Valid blocks are shares as well and the individual who finds the valid block is not awarded additional coins

Mining Pools

- Different payment schemes:
  - Pay-per-share. Pool pays out for every share submitted
  - Proportional. Pool pays out when blocks are found, proportional to the work miners submitted for the block
  - Pay Per Last N Shares. Similar to proportional, but instead of looking at the number of shares in the round, instead looks at the last N shares, regardless of round boundaries.
  - Many others

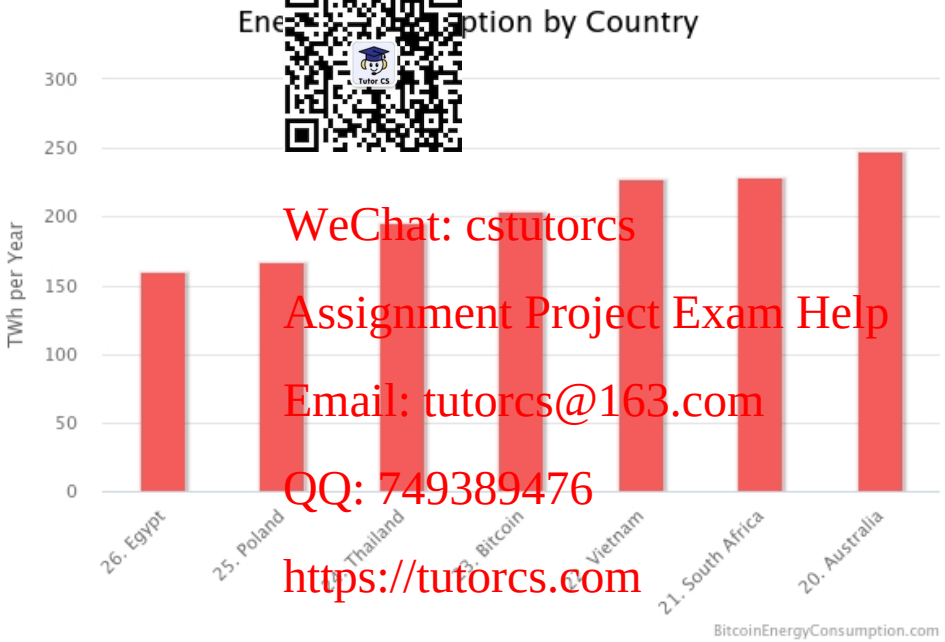
Advantages/Disadvantages of Mining Pools

- Advantages
  - Individual miners can participate in the network
  - Software changes can be upgraded easily
- Disadvantages
  - Centralized
  - Vulnerable to a number of attacks
  - Requires the pool manager to be trusted

Proof of Work Problems

- As the value of mining increases with time the difficulty associated has tended to increase (due to increased competition)
- This has resulted in some unfortunate environmental consequences
- As of March 2022 Bitcoin consumes more energy than Thailand which is listed as 24th of the 200 hundred or so countries in the world in terms of energy consumption

Proof of Work Problems



Proof of Work Problems

Proof of Work Problems

Proof of Work Problems

- This is clearly not a good
- Even ignoring the enviror costs the economical ones are huge
- As of December 2018 the mining costs for Bitcoin are estimated at $2.2 billion
- Alternative methods have been proposed to lower this cost the most famous of which is Proof of Stake which is used in other cryptocurrencies
- The Casper protocol of the Ethereum cryptocurrency is an example of this (supposed to be released in 2023 but it was originally planned for 2019 so some scepticism is warranted)

Proof of Work Problems

- The essential problem with proof of work is that it assumes there are more honest participants than dishonest participants
- There is no advantage to honest participation in the network
- Proof of Stake purposes introducing advantages to honest participants by
  - Introducing Penalties
  - Assigning voting privileges based upon the currency associated with a participant

Proof of Stake

- In proof of work 51% computational power of the network is required for malicious transactions
- In proof of stake 51% of the cryptocurrency of the network is required for malicious transactions
- Discourages malicious transactions as it is likely to damage the value of the cryptocurrency and hence the participants assets
- Potentially good solution but there are potential problems with liquidity as participants may be reluctant to sell

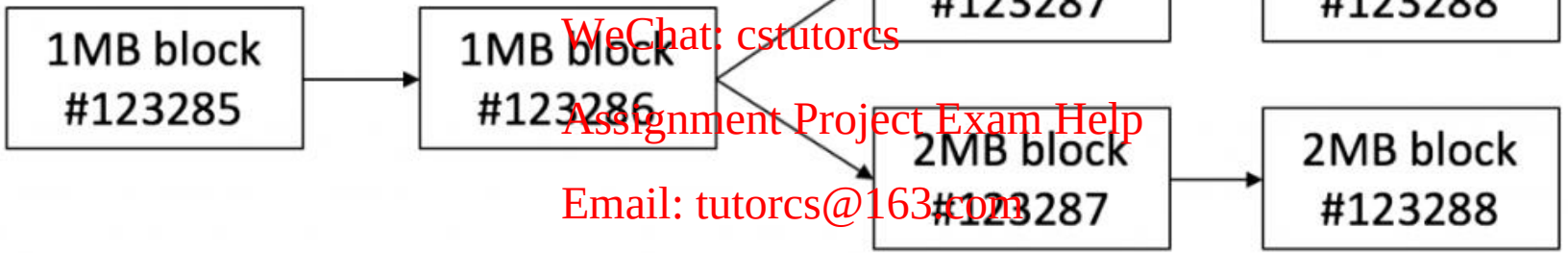
Proof of Stake

- In proof of stake user join[illegible]ator pool
- Forgers who validate tran[illegible]are selected through a deterministic process which may or may not involve their “stake”
- Stake in this case is defined as their level of cryptocurrency wealth or how long they have been a part of the validator pool
- Once the forgers have been selected they reach a consensus on which is the next valid block in the chain

Proof of Stake Problems

- Nothing at Stake: If there are two competing block which are being validated a participant could attempt to validate both blocks at the same time as it increases their chance of a reward
- This can be prevented in two ways known as slashing
  - Punishing participants who vote for the wrong fork (through a reduction in their voting stake)
  - Punishing participants who vote for multiple forks

Proof of Stake Problems

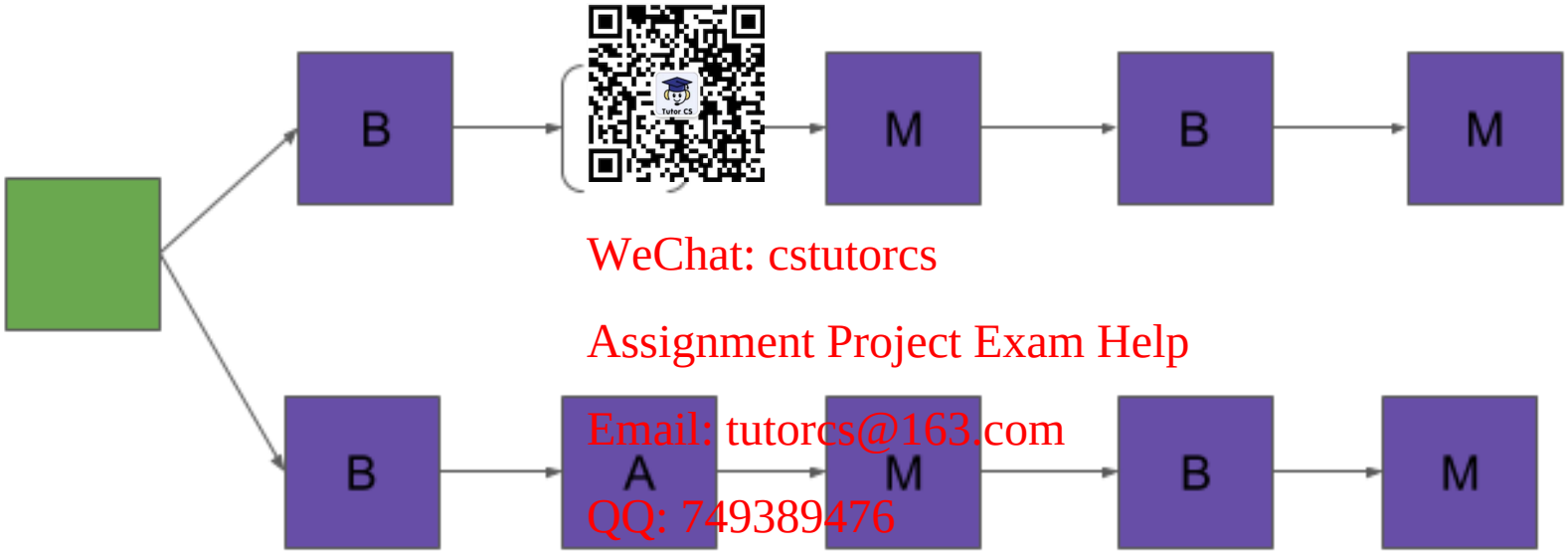


https://coinify.com/news/what-is-a-blockchain-fork/

Proof of Stake Problems

- Long Range Attack: P[illegible]ant creates a new fork starting at the genesis block and [illegible]pts to take over the main chain
- It can be difficult to identify the main chain
- This is a particular problem if slashing is not used
- In general it is assumed that the longest chain is the correct chain (This makes sense for Proof of Work but not Proof of Stake)

Proof of Stake Problems



https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9

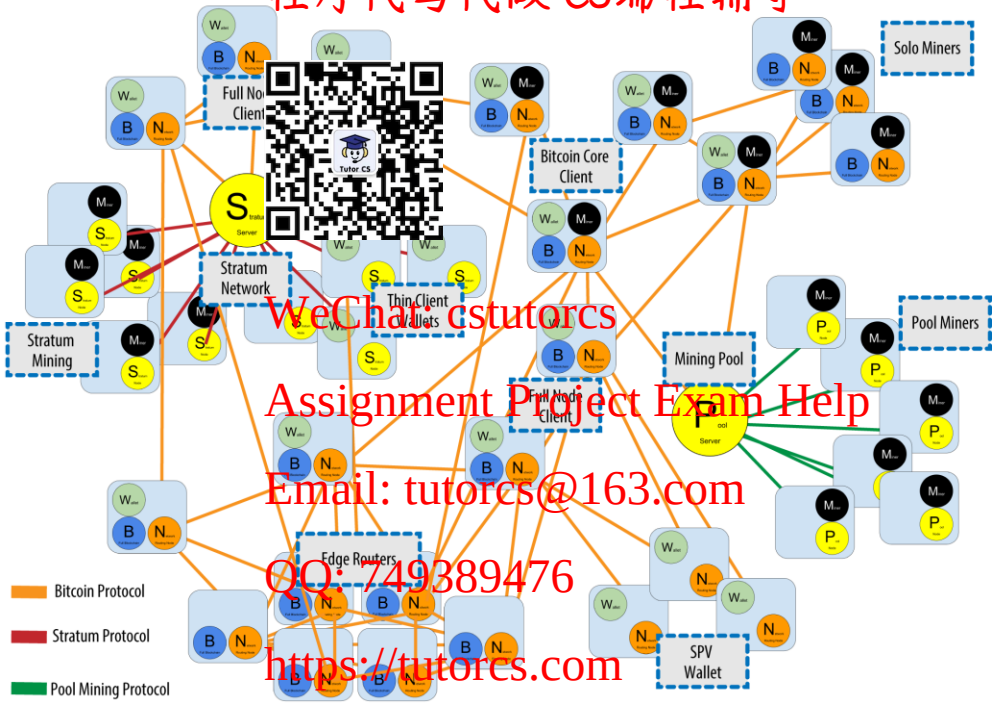
Proof of Stake Problems

- Stake Grinding: In proof of stake the system needs to determine the next validator randomly
- The next validator is determined by the signature of the block from the current validator
- The current validator can produce new signatures to improve their chances of being selected as a validator again
- This can be mitigated by using a proof of stake algorithm which does not use the previous signature to select the validator or some form of thresholding scheme

Bitcoin Participants

- There are a number of users in the Bitcoin network
- Not every participant wants to function as miner so different applications have been created to accommodate this
- The types of users include
  - Miners
  - Full Blockchain
  - Network
  - Wallet

Bitcoin Participants



https://github.com/bitcoinbook/bitcoinbook

Bitcoin Wallets

- Used when users do not want to participate in the validation network
- Store, send, list and receive transactions associated with an address
- Many different applications
- https://bitcoin.org/en/choose-your-wallet can be used to select an application
- Simple Payment Verification can be used to verify if a particular transaction is included in a block without downloading the entire chain

Bitcoin Wallets

- Assumes that incc chain is honest
- In the long term the chain is probably honest
- A user cannot really afford to put the entire blockchain on a phone
- The blockchain was 324 GB in April 2022
- Having a thin client is a reasonable trade-off

Bitcoin Size

https://blockchain.com

Blockchain Implementations

- Hyperledger
- Led by Linux Foundation, IBM
- Focused on finance healthcare, supply chain
- Consortium consists of 20+ corporate members, 120+ start-ups and ecosystem participants,20+ institutions to advance blockchain technologies
- https://www.hyperledger.org/

Blockchain Implementations

- Consensys
- Incubator for Ethereum-focused applications, startups and developer tools
- “Hub-and-spoke model with shared, central resources and “spoke” ventures
- Support adoption, ecosystem expansion and network effects for Ethereum
- *https://consensys.net/*

Blockchain Implementations

- R3CEV
- Tech companies and [illegible] consortium with 70+ members
- Focused on developing **Corda**, private open-source distributed ledger platform designed specifically for banks
- Designed for banks to record, manage, synchronise, support transactions and agreements
- https://www.r3.com/

Blockchain Implementations

- Enterprise Ethereum Alliance
- Consortium of 150+ Fortune 500 companies, start-ups, academic institutions and governments
- Goal is to innovate and align around enterprise applications of Ethereum blockchain
- https://entethalliance.org/

Other Blockchain Applications

- Vehicle and auto parts supply chain
  - Streamline and secure title and record management
  - Reduce prevalence of counterfeit parts
  - Keep tracks of vehicles post-manufacture
- Machine-to-Machine(“M2M”) Payments
  - Vehicles could pay to “platoon” or pass on motorway
  - Could also be used to pay external accounts such as tolls and electric vehicle charging stations

Other Blockchain Applications

- Lending platforms which allow users to put up crypto assets as collateral
  - SALT
  - Cred
- Insurance which uses existing reputation-based trust networks/communities
  - Wetrust

Other Blockchain Applications

- Identity Management
- Prevent the exploitation of personal information
- Personal information is encrypted and can be used for various web services
  - Civic
- Could also be used to access government services
  - uPort

Other Blockchain Applications

- Supply chain
- Unbroken record of a product's ownership history
  - Fair Trade
  - Sustainable agriculture
  - Organic Certification
  - Counterfeit Drug Prevention
  - Authentication of luxury goods

Other Blockchain Applications

- Energy
- Microgrid is used for (e.g. rooftop solar panels) energy generation and blockchain used to record transactions
- Energy can be distributed to neighbours and sold back to utility if not needed
- Could also include information on carbon emissions to encourage generators and users to lower carbon footprint
  - Swytch

Other Blockchain Applications

- Traceable donatio
- Large donations are used as part of a stake in PoS consensus and the block rewards are donated
  - Pinkcoin
- Traceability of micro-donations used to buy forest-based carbon credits
  - Poseidon