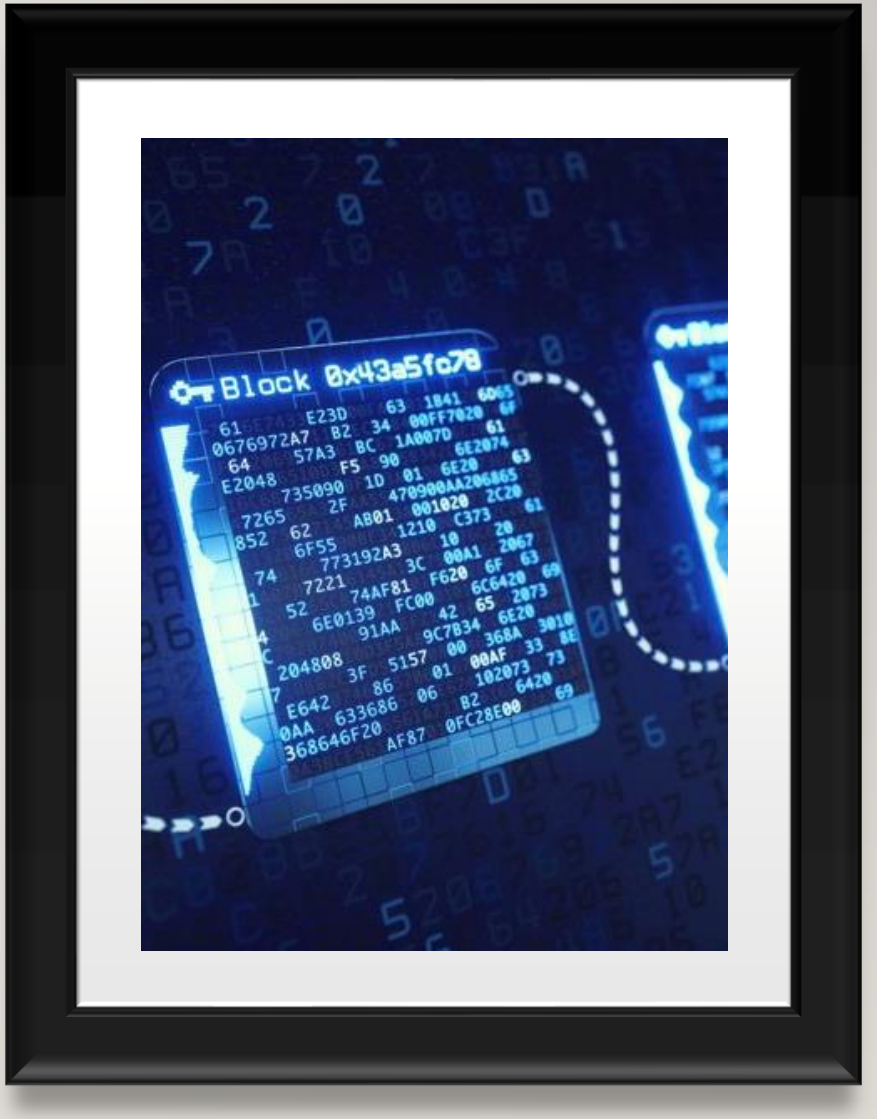
THE BLOCKCHAIN EVOLUTION – PART I

Sept 2021



2 PART AGENDA

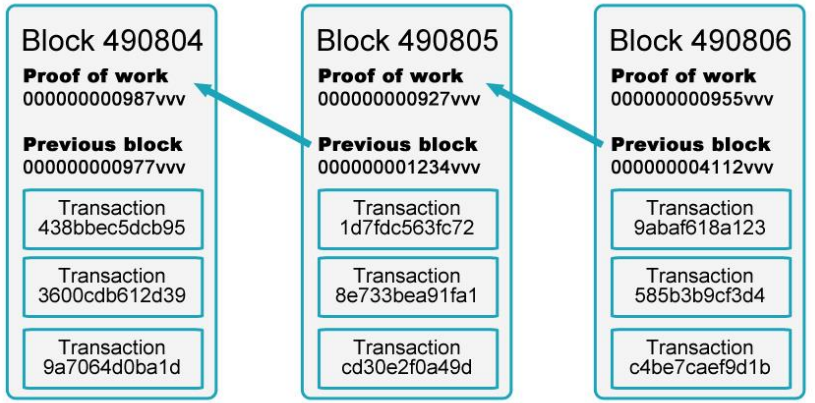
Part I

- Intro: What is a Blockchain? Crypto ‘currencies’
- Understanding Bitcoin
- Understanding Ethereum

Part II

- Smart Contracts
- Ethereum for Enterprise

WHAT IS A BLOCKCHAIN?



- Distributed Ledger Technology(DLT): a decentralized database
  - Managed by various participants. No central authority that acts as arbitrator or monitor.
  - As a distributed log of records, there is greater transparency - manipulation more difficult.
- Blockchain is a DLT– a log of records, written as blocks that form a chain.
  - A chain of transactions, where the output of one transaction is the input of the next transaction. - Each block has a hash; the next block begins with that same ‘hash’.
  - The hashes allow verification that the encrypted information has not been manipulated, and that it can’t be manipulated.

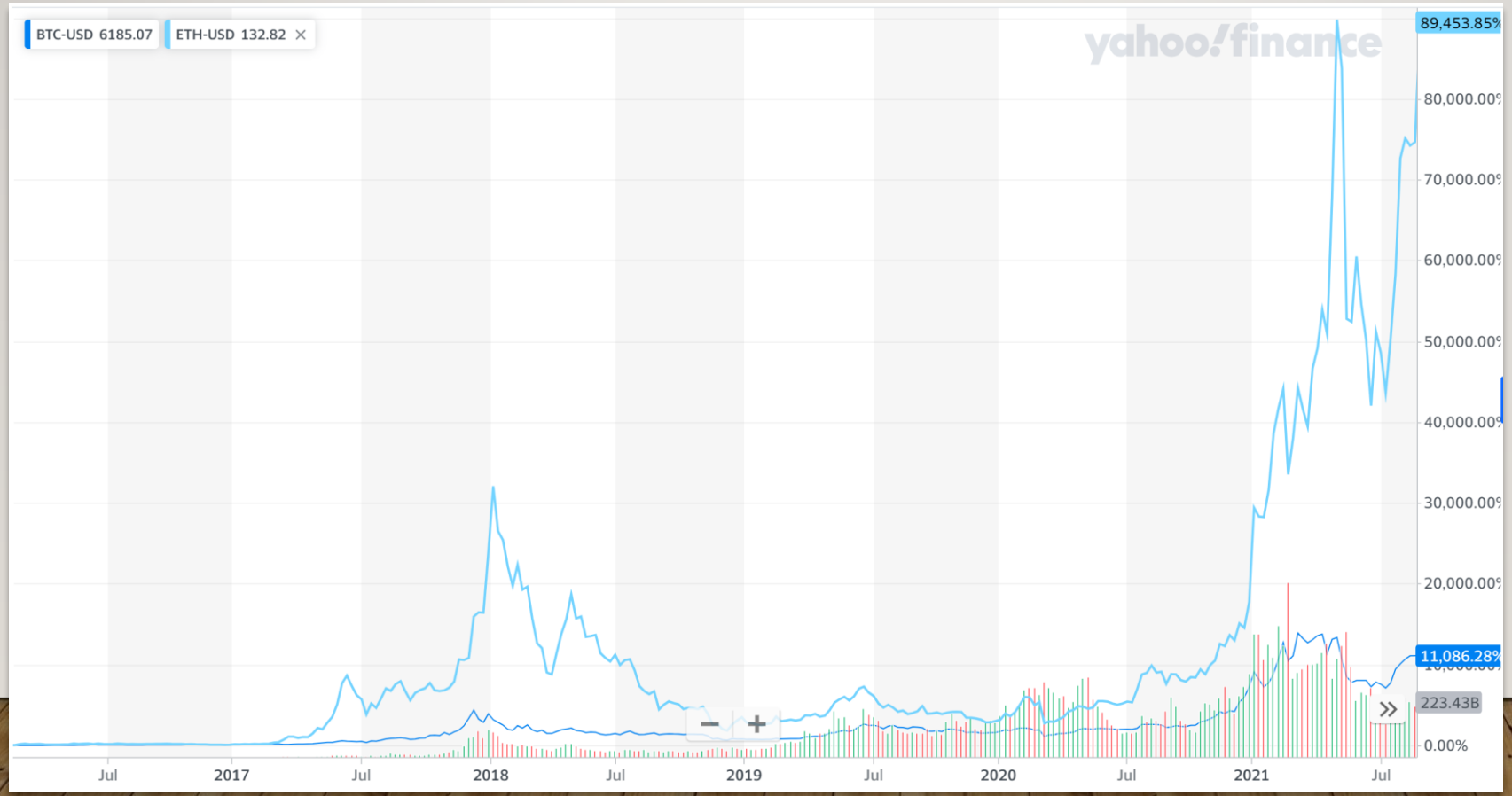
CRYPTO 'CURRENCY' GROWTH – 5YRS

BTC:12th Sept 2021 - $851bln

Eth:12th Sept 2021 - $294bln

BTC VS ETH

Largest bitcoin transaction was $1.1 billion, transmitted instantly. For a fee of only $0.68.



EU: BITCOIN IS NOT A CURRENCY

Bitcoin has been labelled a crypto-asset, Not a currency. [ECB ref]

- No one is backing it - no guarantees on your right to pay with it
- No legal protection if it is stolen
- Very volatile

BITCOIN

"BITCOIN IS A **CONSENSUS NETWORK** THAT ENABLES A NEW PAYMENT SYSTEM AND A COMPLETELY DIGITAL MONEY.

BITCOIN: ORIGINS

- 2008 Satoshi Nakamoto published "Bitcoin: A Peer-to-Peer Electronic Cash System"
- Goal: to allow online payments to be sent directly from one party to another without going through a financial institution. - Became the first decentralized **peer-to-peer** payment network. Nobody owns the network.
- "Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network."
- Software downloadable from https://bitcoin.org/en/download

BITCOIN

Money Challenges

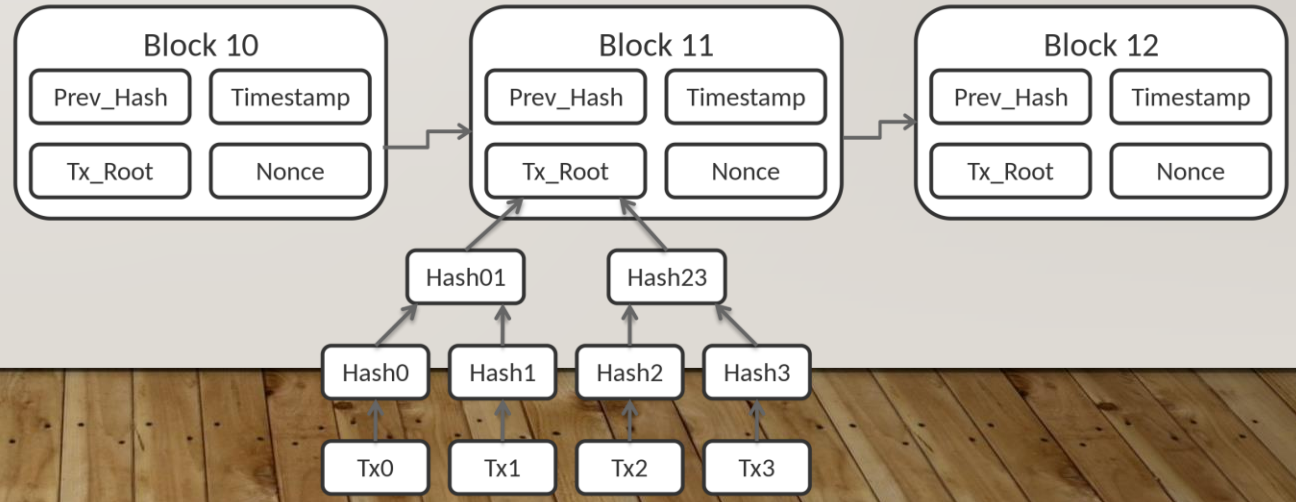
- Can I trust that the money is authentic and not counterfeit?
- Can I trust that the digital money can only be spent once (known as the "double-spend" problem)?
- Can I be sure that no one else can claim this money belongs to them and not me?

Bitcoin consists of:

- A decentralized peer-to-peer network (the bitcoin protocol)
- A public transaction ledger (the blockchain)
- A set of rules for independent transaction validation and currency issuance (consensus rules)
- A mechanism for reaching global decentralized consensus on the valid blockchain (Proof-of-Work algorithm)

BITCOIN: IN ITS OWN WORDS ..

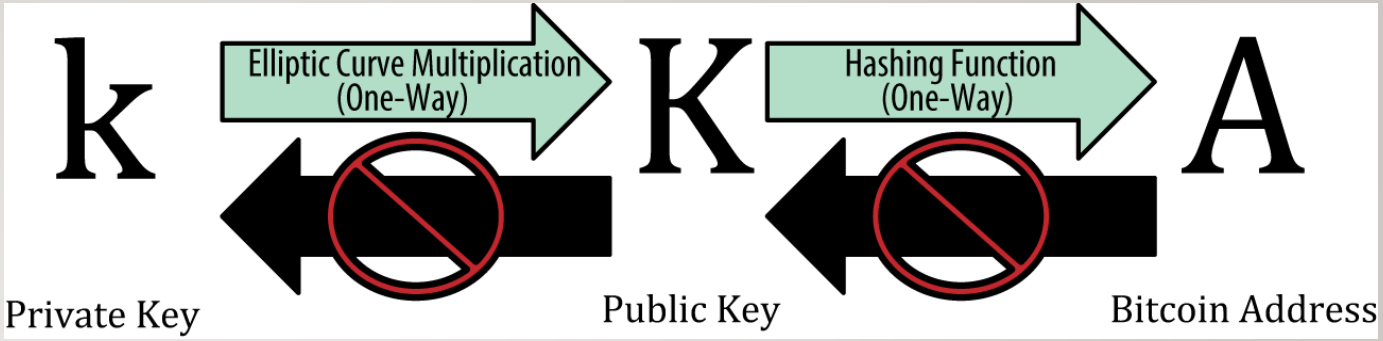
- Bitcoin network is sharing a public ledger called the "block chain". This ledger contains every transaction ever processed, allowing a user's computer to verify the validity of each transaction. The authenticity of each transaction is protected by digital signatures corresponding to the sending addresses, allowing all users to have full control over sending bitcoins from their own Bitcoin addresses. [Bitcoin FAQ]
- nodes can leave and re-join the network at will.



BITCOIN FUNDAMENTALS

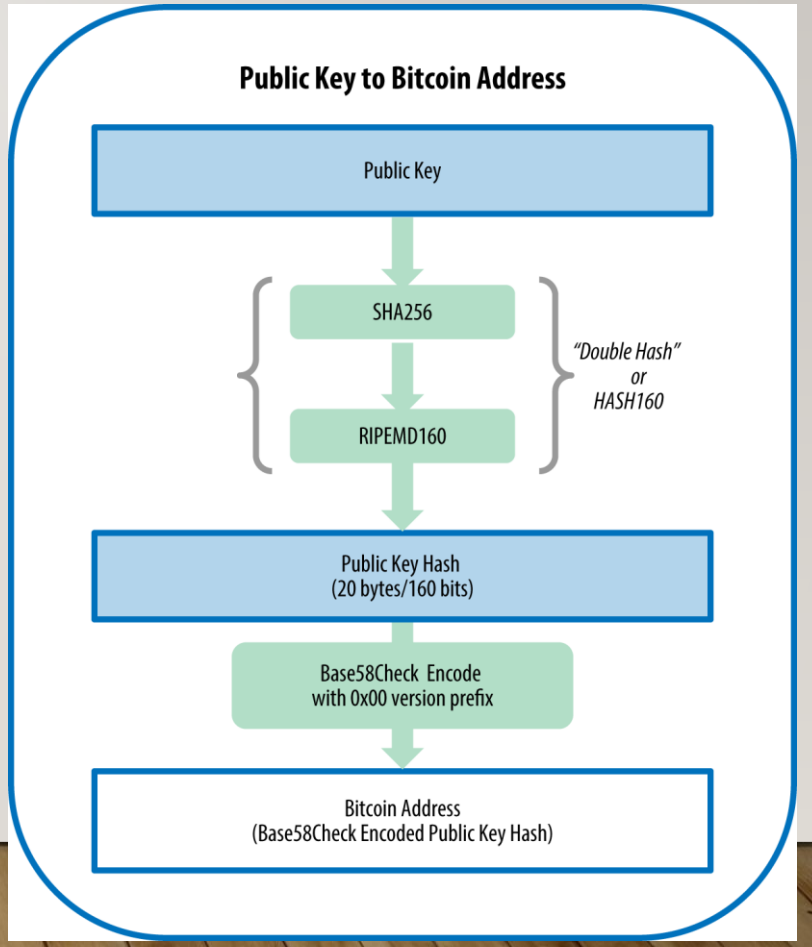
- Bitcoin users communicate with each other using the bitcoin protocol via the internet
- ‘coins’ are implied in transactions that transfer value from sender to recipient: the transaction tells the network that the owner of some bitcoin value authorized the transfer of that value to another owner.
- Bitcoin users own keys that allow them to prove ownership of bitcoin in the bitcoin network. They can sign transactions to unlock the value and spend it by transferring it to a new owner.
- Possession of the key that can sign a transaction is the only prerequisite to spending bitcoin, putting the control entirely in the hands of each user.

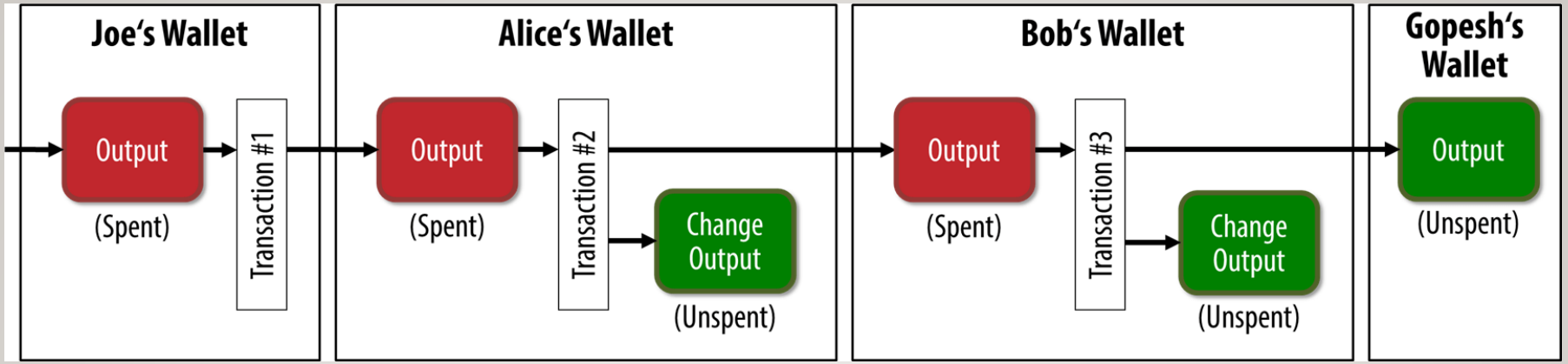
GETTING STARTED



The Public key is used to receive funds, the private key is used to sign transactions to spend the funds.

- Generate Private Key (a random number)
- Generate Public Key: Asymmetric transformation of the private key using elliptical curve multiplication (secp256k1 curve) to generate public key
- Address = RIPEMD160(SHA256(K)). Address encoded with Base58Check
- Decide on Wallet: Hot Wallets / Cold Wallets



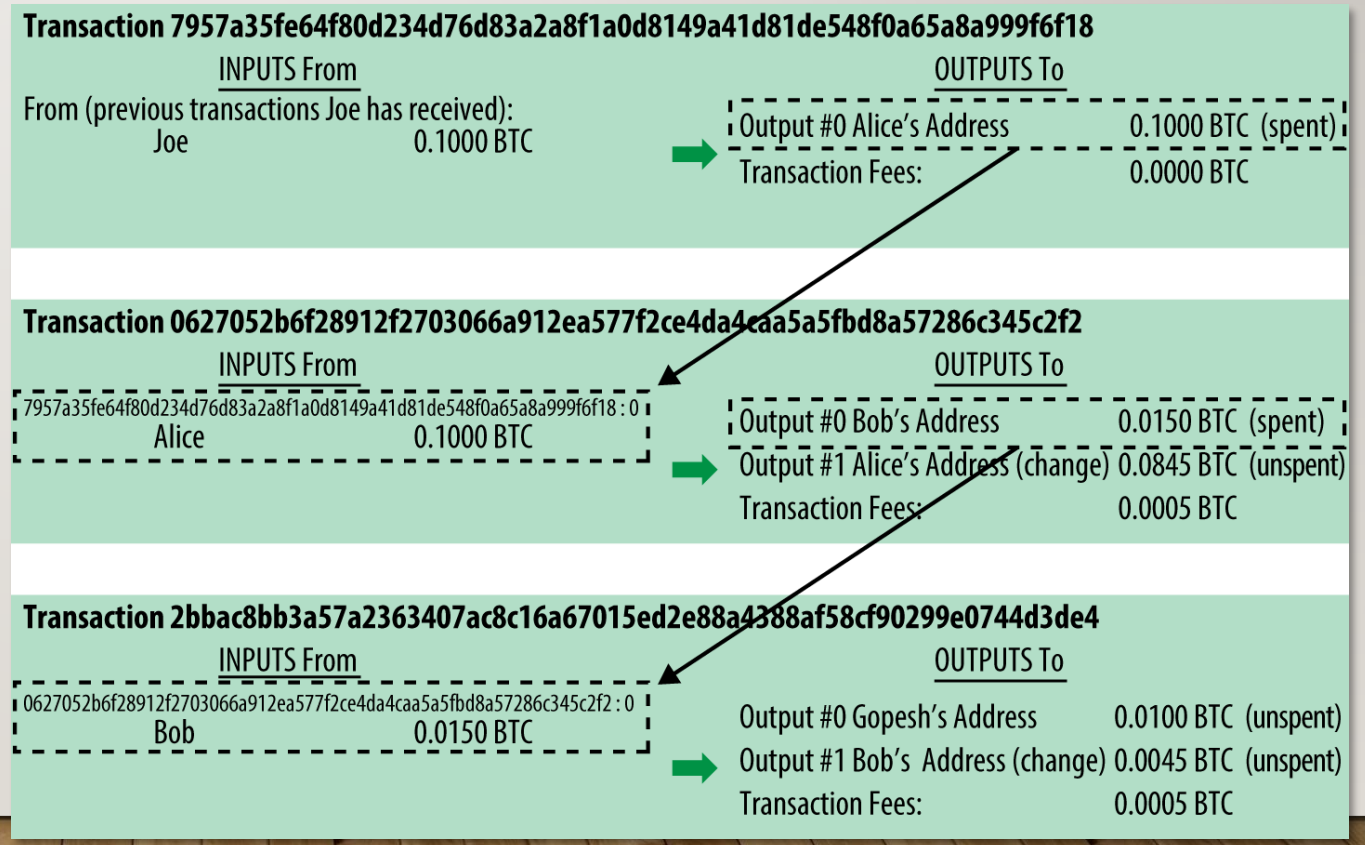


UXTO – unspent transaction output / SXTO – spent...

Each transaction has one or more inputs - transaction IDs referencing previous transactions that contains the UTXO being spent

When we say that a user's wallet has "received" bitcoin, what we mean is that the wallet has detected on the blockchain an UTXO that can be spent with one of the keys controlled by that wallet.

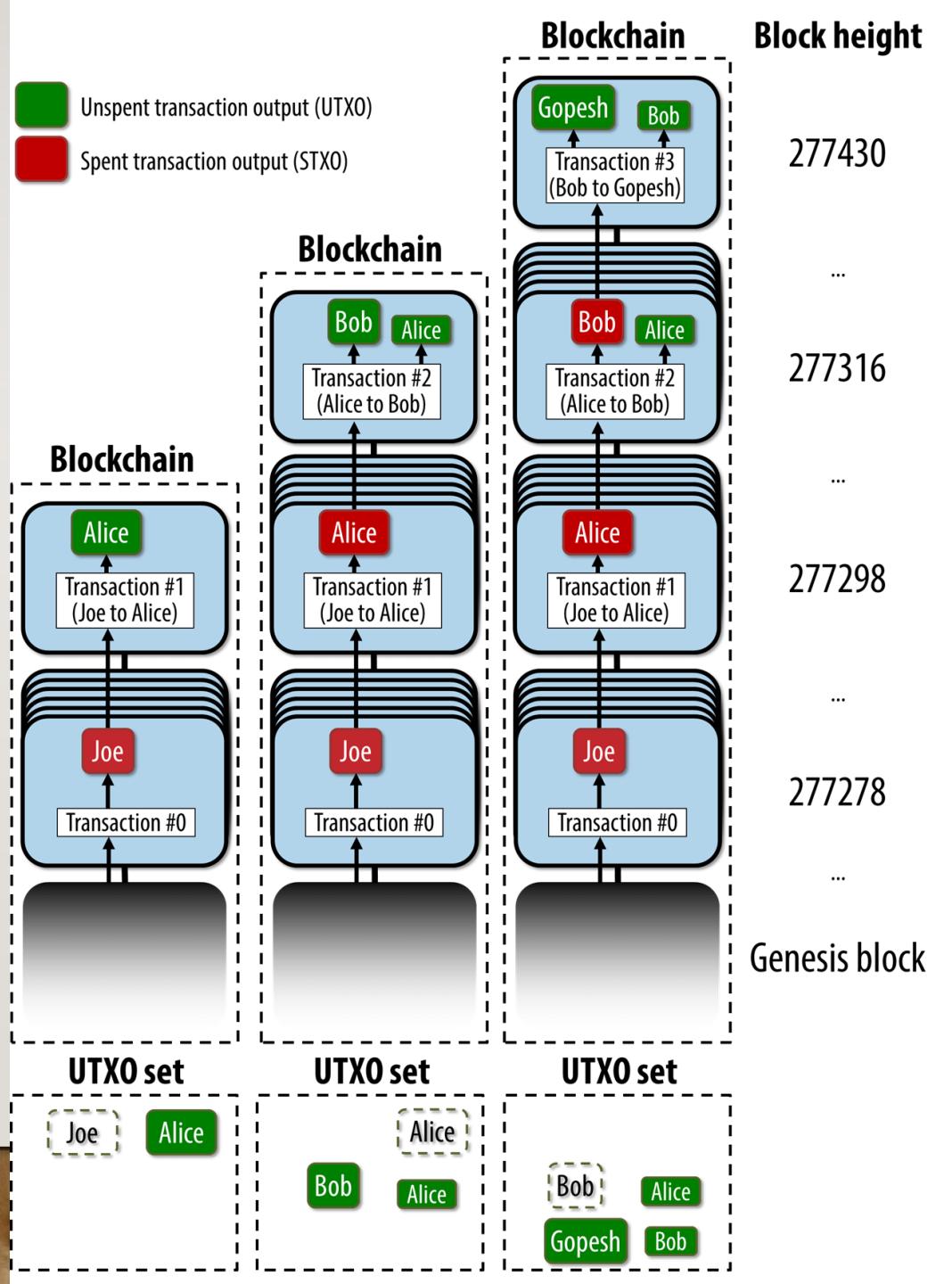
A user's bitcoin "balance" is the sum of all UTXO that user's wallet can spend and which may be scattered among hundreds of transactions and hundreds of blocks.

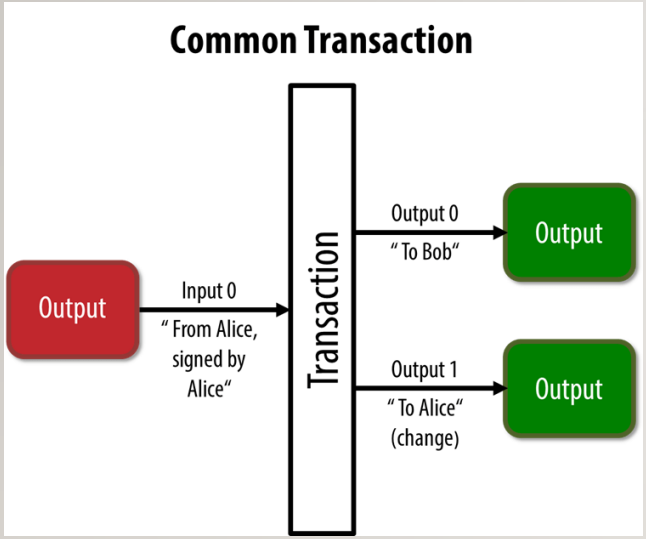


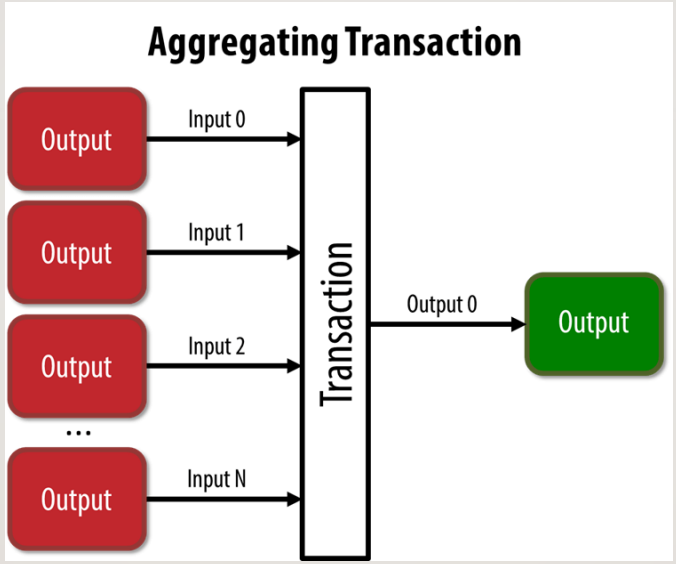
Transaction as Double-Entry Bookkeeping

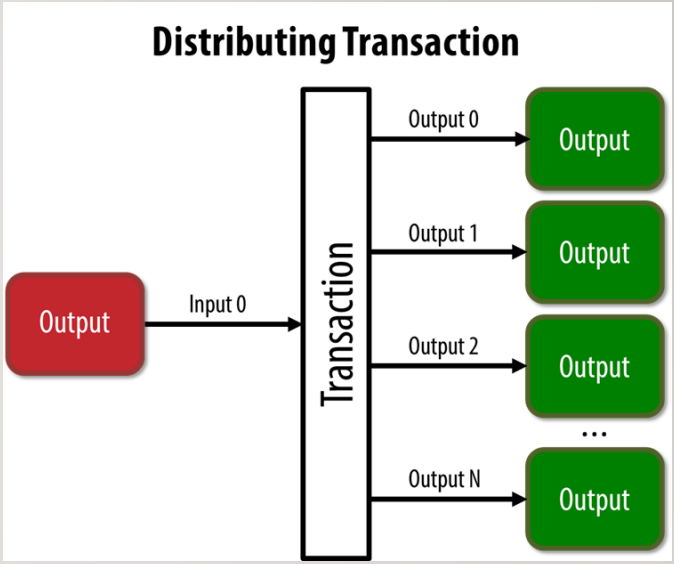
Inputs	Value	Outputs	Value
Input 1	0.10 BTC	Output 1	0.10 BTC
Input 2	0.20 BTC	Output 2	0.20 BTC
Input 3	0.10 BTC	Output 3	0.20 BTC
Input 4	0.15 BTC		
Total Inputs:	0.55 BTC	Total Outputs:	0.50 BTC

	Inputs	*0.55 BTC*
-	*Outputs*	*0.50 BTC*
	Difference	*0.05 BTC (implied transaction fee)*









Network needs to be able to track unspent transaction outputs, or *UTXO*

PAYING TRANSACTION FEES

- Transaction fees are used as a protection against users sending transactions to overload the network and as a way to pay miners for their work helping to secure the network.
- The precise manner in which fees work is still being developed and will change over time. Because the fee is not related to the amount of bitcoins being sent, it may seem extremely low or unfairly high.

BITCOIN: MINING / CONSENSUS

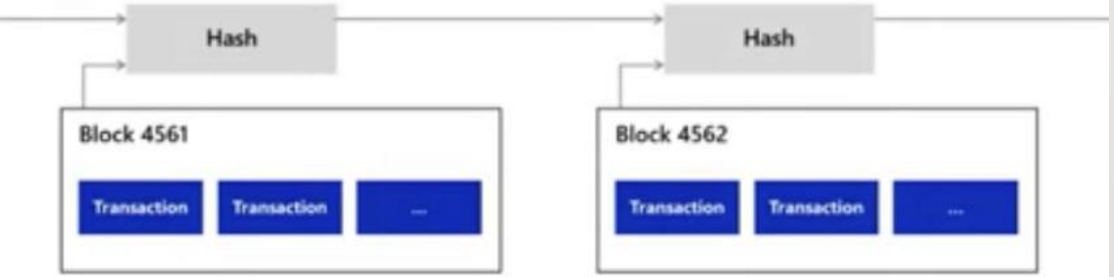
- Satoshi Nakamoto's solution to achieve consensus without a central trusted authority uses the concept of **Proof-of-Work**
- Bitcoins are created through a process called "mining" involves competing to find solutions to a mathematical problem while processing bitcoin transactions.
- Any participant in the bitcoin network may operate as a miner, using their computer's processing power to verify and record transactions.
- Every 10 minutes, on average, a bitcoin miner can validate the transactions of the past 10 minutes and is rewarded with brand new bitcoin.
- bitcoin mining decentralizes the currency-issuance and clearing functions of a central bank and replaces the need for any central bank.

BITCOIN:MINING

Mining

Miners collect transactions into *blocks*

Then submit a proposal for a block after solving a cryptographic puzzle



Proof of Work example

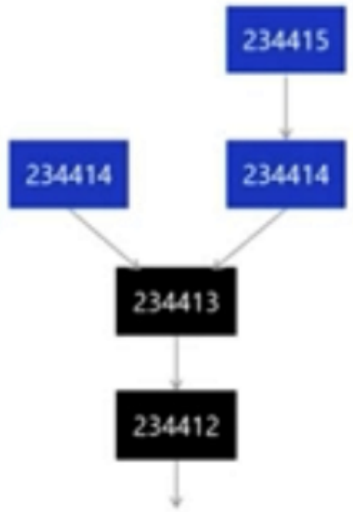
Goal

Find a hash that starts with 0000 of "hello, world!" plus a *nonce*

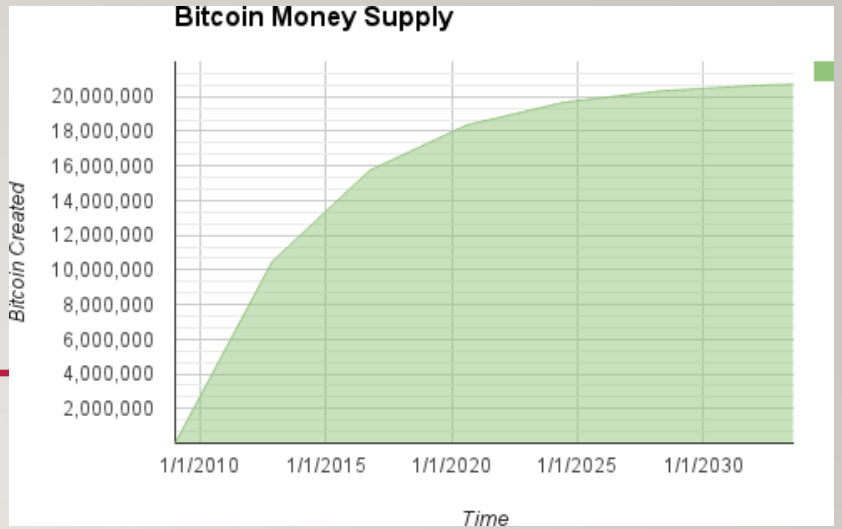
```
✖ "Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
✖ "Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
✖ "Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
  ...
✖ "Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
✖ "Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
✔ "Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

Forks

Forks occur when miners mine blocks at about the same time



BITCOIN: MINING / ISSUANCE



- bitcoin protocol includes built-in algorithms that regulate the mining function across the network. The difficulty of the processing task that miners must perform is adjusted dynamically so that someone succeeds ~every 10 minutes regardless of how many miners are competing.
- The protocol halves the rate at which new bitcoin is created every 4 years; limits the total number of bitcoin that will be created to a fixed total just below 21 million coins (2140)
- bitcoin cannot be inflated by "printing" new money beyond the expected issuance rate.

HOW DOES MINING HELP SECURE BITCOIN?

- Mining creates the equivalent of a competitive lottery that makes it very difficult for anyone to consecutively add new blocks of transactions into the block chain. This protects the neutrality of the network by preventing any individual from gaining the power to block certain transactions. This also prevents any individual from replacing parts of the block chain to roll back their own spends, which could be used to defraud other users. Mining makes it exponentially more difficult to reverse a past transaction by requiring the rewriting of all blocks following this transaction.
- [Bitcoin FAQ ref]

BITCOIN: SOLVING DOUBLE SPENDING

- Time takes to validate a transaction against double spend attacks – for each input nodes check every other transaction ever made to validate the input hasn't been spent
- A full blockchain node verifies a transaction by checking the entire chain of thousands of blocks below it in order to guarantee that the UTXO is not spent, whereas an SPV (simplified payment verification) node checks how deep the block is buried by a handful of blocks above it.
- For most practical purposes, well-connected SPV nodes are secure enough, striking a balance between resource needs, practicality, and security. For infallible security, however, nothing beats running a full blockchain node.

WAITING FOR TRANSACTION CONFIRMATION

HOW LONG TO WAIT?

Confirmations	Lightweight wallets	Bitcoin Core
0	Only safe if you trust the person paying you	
1	Somewhat reliable	Mostly reliable
3	Mostly reliable	Highly reliable
6	Minimum recommendation for high-value bitcoin transfers	
30	Recommendation during emergencies to allow human intervention	

- Each confirmation takes between a few seconds and 90 minutes, with 10 minutes being the average.
- If the transaction pays too low getting the first confirmation can take much longer.
- Every user is free to determine at what point they consider a transaction sufficiently confirmed, but 6 confirmations is recommended. [Bitcoin FAQ ref]

BITCOIN: CRYPTO USE

- Bitcoin communications and transaction data are not encrypted and do not need to be.
- User's digital keys are not actually stored in the network, are created and stored by users (in a wallet).
  - If you lose your keys – there is no recourse!
- A bitcoin address is a string of digits and characters to share with anyone who wants to send you money.
- Hashes:
  - SHA-256 (transaction hashes) & RIPEMD-160 (address creation)
- Transaction signing
  - Bitcoin uses Elliptic Curve Digital Signature Algorithm (ECDSA) to sign transactions.
    - ECDSA uses secp256k1 curve from http://www.secg.org/sec2-v2.pdf is used.

BITCOIN CRYPTO USE

Node to Node Interactions

- The original implementation of bitcoin communicates entirely in the clear. While this is not a major privacy concern for full nodes, it is a big problem for SPV nodes.
- Two solutions that provide encryption of the communications:
  - Tor Transport and P2P Authentication and Encryption with BIP-150/151.
  - Bitcoin Improvement Proposals, BIP-150 and BIP-151, add support for P2P authentication and encryption
- BIP-151 enables negotiated encryption for all communications between two nodes that support BIP-151.
- BIP-150 offers optional peer authentication that allows nodes to authenticate each other's identity using ECDSA and private keys.
  - BIP-150 requires that prior to authentication the two nodes have established encrypted communications as per BIP-151.
- As of February 2021, BIP-150 and BIP-151 are not implemented in Bitcoin Core.

IS LIMITING THE ISSUANCE A PROBLEM?

- that there will only ever be 21 million Bitcoin in existence.
- miners, who secure the network, will have less incentive to stick around.
- The current circulating supply of Bitcoin is around 18.8 million BTC, which accounts for close to 90% of all the tokens that will ever exist. [ref]
- current rate, a 6.25 BTC block reward is issued every ten minutes. This equates to 900 new BTC entering circulation each day. This rate halves every four years
- In eight halvings time (the year 2052), the issuance rate will be 3.5 BTC per year, which will yield just 0.0243 BTC for each block reward. - is this rate sufficient to secure the Bitcoin blockchain?

PRIVACY? BITCOIN IS NOT ANONYMOUS

- All Bitcoin transactions are stored publicly and permanently on the network, which means anyone can see the balance and transactions of any Bitcoin address.
- The identity of the user behind an address remains unknown until information is revealed during a purchase or in other circumstances. This is one reason why Bitcoin addresses should only be used once. [Bitcoin FAQ ref]

Blockchain.com Wallet Exchange Explorer Buy Bitcoin Trade

Address

USD BTC

This address has transacted 3 times on the Bitcoin blockchain. It has received a total of 75.50844354 BTC ($2,534,217.40) and has sent a total of 75.50844354 BTC ($2,534,217.40). The current value of this address is 0.00000000 BTC ($0.00).

Address	bc1qq2euq8pw950klpjcawuy4uj39y...
Format	BECH32 (P2WPKH)
Transactions	3
Total Received	75.50844354 BTC
Total Sent	75.50844354 BTC
Final Balance	0.00000000 BTC

Transactions

Hash 280c5f96397b9502b99703842712b... 2021-06-07 18:48

bc1qq2euq8pw9... 5.90422177 BTC → bc1qvjh9cq6qlj4f... 5.90419482 BTC

Fee 0.00002695 BTC (14.110 sat/B - 6.167 sat/WU - 191 bytes (24.500 sat/vByte - 110 virtual bytes)) -5.90422177 BTC

Hash 943f2d576ed8d9f388ba75eb82fe35... 2021-06-07 18:40

bc1qq2euq8pw... 69.60422177 BTC → bc1qq2euq8pw9... 5.90422177 BTC, bc1qpx7vyv5tp... 63.69996546 BTC

Fee 0.00003454 BTC (15.559 sat/B - 6.157 sat/WU - 222 byte (24.496 sat/vByte - 141 virtual bytes)) -63.70000000 BTC

Blockchain.com Wallet Exchange Explorer Buy Bitcoin Trade

Hash daf38c7b38eb0a587cf843f47000d5... 2021-05-28 04:01

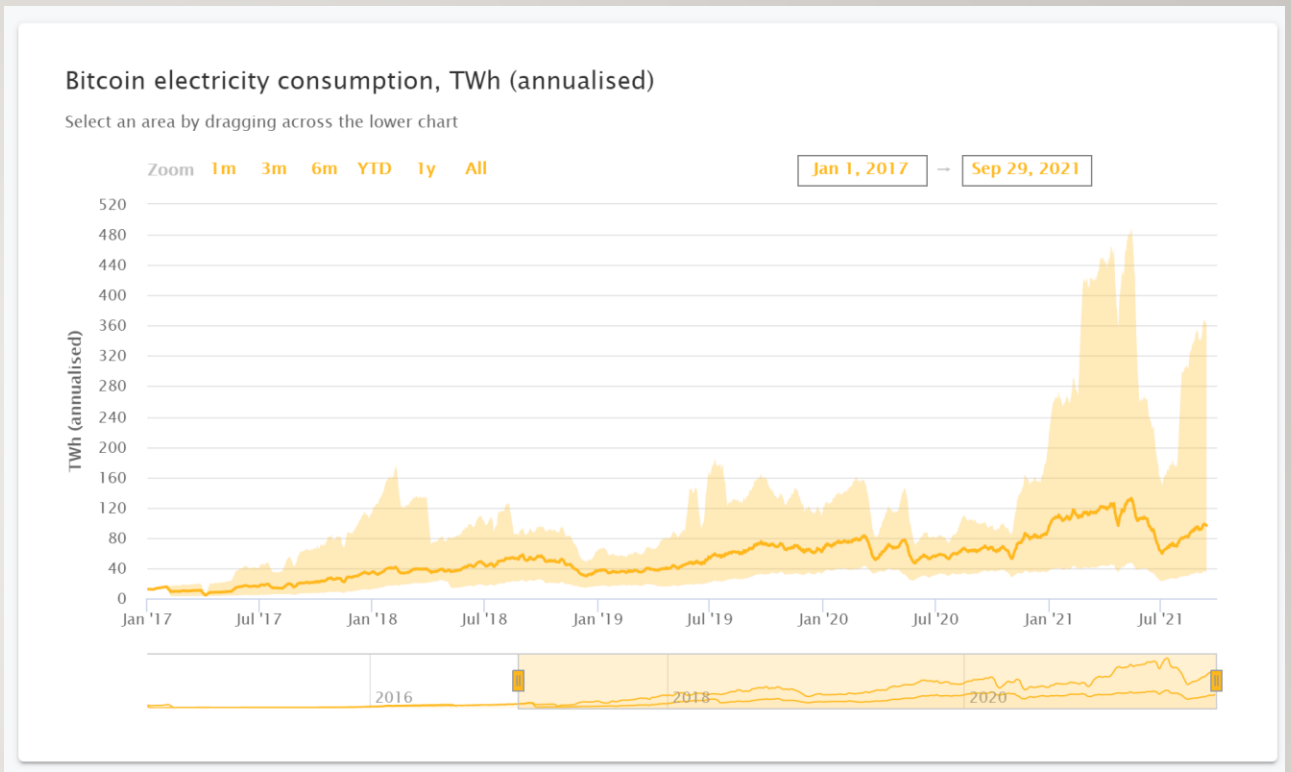
378JHJCpWgSK...	0.00164331 BTC	→ bc1qq2euq8pw...	69.60422177 BTC
3E71mBDDXxkk1...	0.00002104 BTC		
33EPYRGgMjEs1...	0.00000547 BTC		
3QP3qPJqTHvX...	0.00000547 BTC		
3FfgyWERGVxtg...	0.00055095 BTC		
3GvGJXyDg59J...	0.00001200 BTC		
34T2Jm9ZzQgw...	0.00002138 BTC		
3Kgona229L78R...	0.00006469 BTC		
3F61Aj9SCDwiuz...	0.00019160 BTC		
3QP3qPJqTHvXd...	0.00132300 BTC		
35nnRBcz6BWP...	0.00001205 BTC		
38gE7V2Sp5Gh...	3.66843600 BTC		
3QiJWsCXt6xAF...	0.00010100 BTC		
3EYkxQSUv2K...	63.70000000 BTC		
3ESP4jp7nfQNrK...	1.42099200 BTC		
3B1eo6x9AnFj6J...	0.47521100 BTC		
3HceXRtFgSFeA...	0.00015371 BTC		
3CUFbhj4ftvUE7...	0.33870000 BTC		
36cnexG5eSDsz...	0.00398799 BTC		
3AGSews8AK4T...	0.00179782 BTC		
39fjQ4d91LrtyH...	0.00001604 BTC		
34Lz9Rf5gxBfrX...	0.00063500 BTC		
38DfXrnLxmiLxs...	0.00022800 BTC		
3FJncYBuKH76...	0.00000547 BTC		

Fee 0.00989322 BTC (139.873 sat/B - 34.968 sat/WU - 7073 +69.60422177 BTC

reference; account

Theoretical lower bound	Estimated	Theoretical upper bound
4.02 GW	11.75 GW	41.69 GW
34.93 TWh	Annualised consumption: 96.20 TWh	360.62 TWh

Source: https://cbeci.org/



Ireland

Average monthly hashrate share, Apr'21:

2.27%

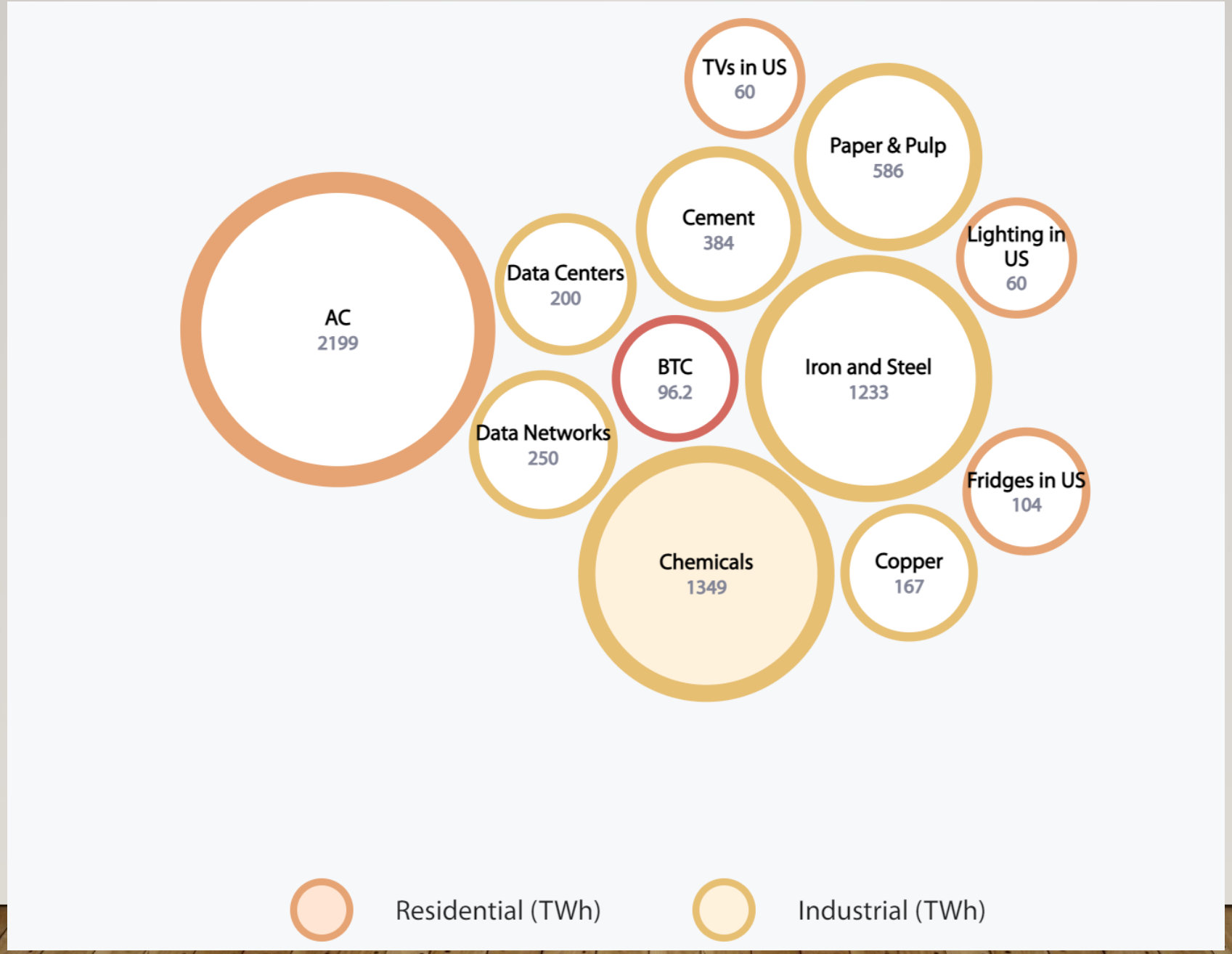
Kazakhstan	Philippines	Bitcoin	Netherlands	United Arab Emirates
91.7 TWh per year	93.4 TWh per year	96.2 TWh per year	110.7 TWh per year	119.5 TWh per year

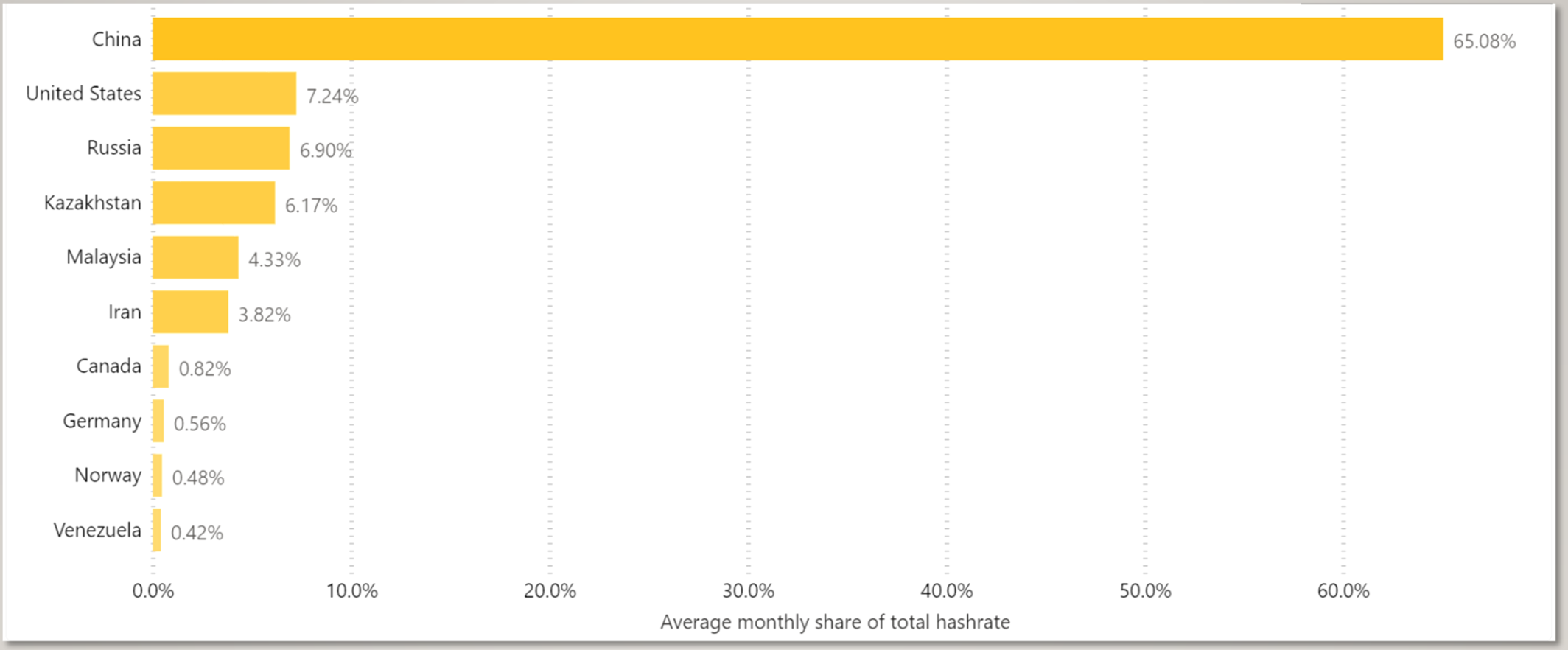
Electricity

Production
26 730 TWh

Consumption
22 315 TWh

Bitcoin share
0.43%


TVs in US
60
Paper & Pulp
586
Cement
384
Lighting in US
60
Data Centers
200
AC
2199
BTC
96.2
Iron and Steel
1233
Data Networks
250
Fridges in US
104
Chemicals
1349
Copper
167
Residential (TWh)
Industrial (TWh)



- More than 150 quintillion attempts at guessing the number are now carried every second of the day
- ‘mining’ happens where power is cheapest, most notably north-western China’s Xinjiang Province where coal is abundant and accounts for two-thirds of the country’s energy use.
- Power demand from crypto farms in Abkhazia in north western Georgia has been so high in recent years that rolling blackouts became the norm and equipment had to be confiscated by the state.

BLOCKCHAIN: RISKS / ATTACK CATEGORIES

- Consensus Manipulation: 51%
- Replay attacks
- Double Spending
- Key Theft
- Possible future Environmental / Regulatory clampdown that would impact cost
- Bitcoin Core software vulnerability (Inability to force upgrade network node software)

ETHEREUM

WHAT IS ETHEREUM?

- Bitcoin's blockchain, tracks the state of units of bitcoin and their ownership.
  - distributed consensus state machine where transactions cause a global state transition, altering the ownership of coins.
- Ethereum: instead of tracking only the state of currency ownership, Ethereum stores both code and data
  - 'The worlds programmable blockchain' – introduces a cryptocurrency called ether to meter and constrain execution.
  - Ethereum Virtual Machine – where program's called smart contracts run. Every operations is executed in every node.
- Ethereum platform: a globally decentralized computing infrastructure that executes smart contracts.
  - The enables developers to build powerful decentralized applications (Dapps) with built-in economic functions.
  - Ethereum programs run "everywhere," yet produce a common state that is secured by the rules of consensus.

ETHEREUM FUNDAMENTALS

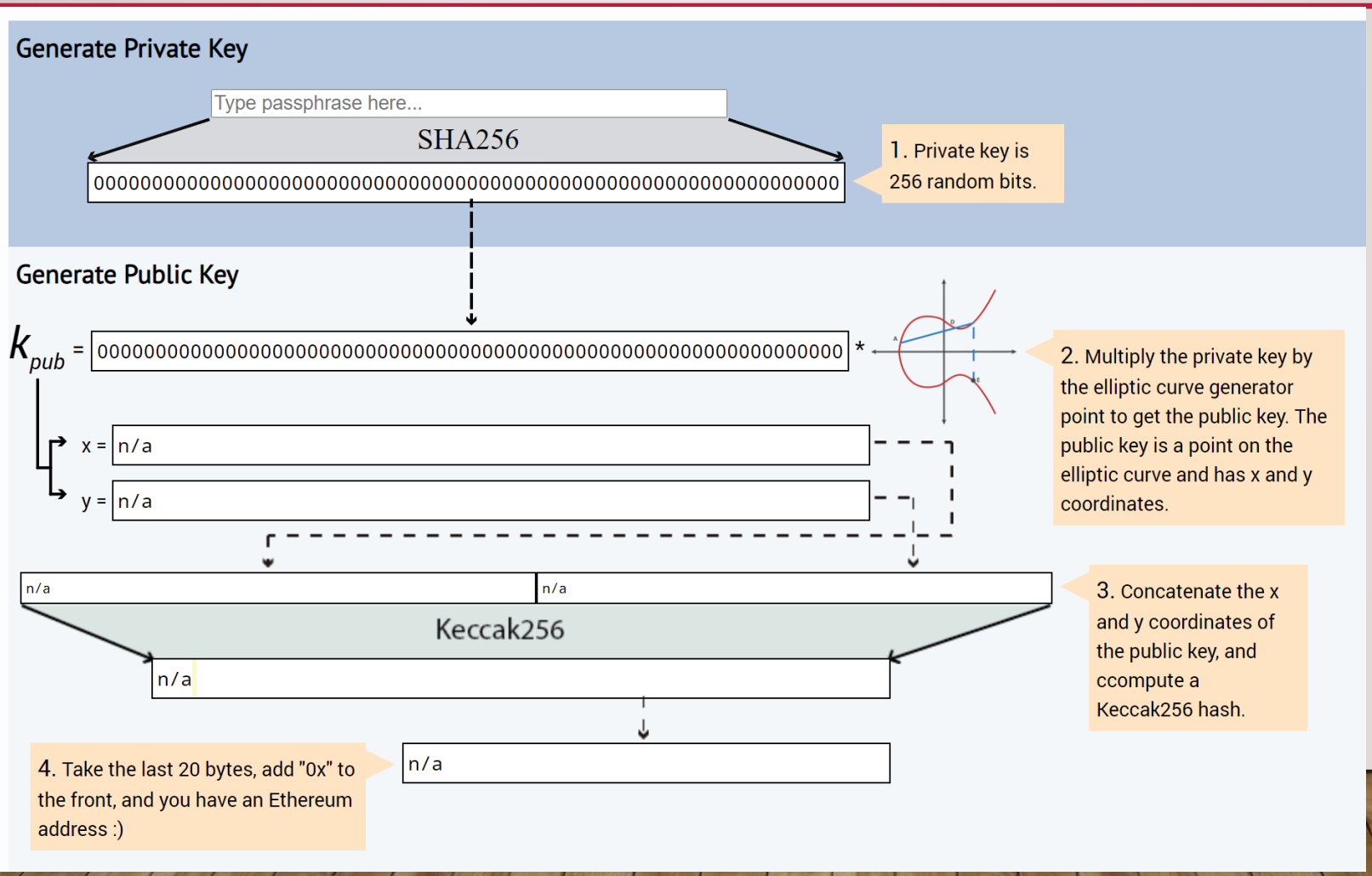
- Ethereum was initially described in a white paper by Vitalik Buterin.
- Ethereum is the system, Ether is the currency. Also identified also as "ETH" or with the symbols Ξ
- Ethereum blocks are validated approximately every 12 seconds on Ethereum (vs approximately every 10 minutes on Bitcoin.)
- Two accounts types on Ethereum:
  - User Accounts ("Externally-Owned Accounts / EOA")
  - Contracts.

FUNDAMENTALS: ETHER CURRENCY

- Bitcoin has a fixed supply of 21,000,000 coins; Ethereum has no supply cap.
- Identified also as "ETH" or with symbol Ξ
- Wallet holds your keys and can create and broadcast transactions on your behalf.
- If you lose your private keys, you lose access to your funds and contracts. No one can help you regain access

Value (in wei)	Exponent	Common name	SI name
1	1	wei	Wei
1,000	10^3	Babbage	Kilowei or femtoether
1,000,000	10^6	Lovelace	Megawei or picoether
1,000,000,000	10^9	Shannon	Gigawei or nanoether
1,000,000,000,000	10^{12}	Szabo	Microether or micro
1,000,000,000,000,000	10^{15}	Finney	Milliether or milli
1,000,000,000,000,000,000	*10^{18}*	*Ether*	*Ether*
1,000,000,000,000,000,000,000	10^{21}	Grand	Kiloether
1,000,000,000,000,000,000,000,000	10^{24}		Megaether

ETHEREUM ADDRESSES



- Base address format does not include checksum
- Source:[ref]

ETHEREUM CRYPTO USE

- Nodes authenticate using ECDSA based handshake using secp256k1curve
- Communications between nodes (including transaction data) are unencrypted
- Senders do not require authorisation to invoke a transaction.
- Transaction sender signs using ECDSA using secp256k1 curve
- Hashing algorithm used for block signing is Keccak-256
  - Keccak-256 was the SHA-3 winning nomination.
  - NIST proposed some adjustments after Keccak was adopted by Ethereum
  - Keccak256 != SHA-3

DIFFERENT NETWORKS

- Main Ethereum Network
  - The main public Ethereum blockchain. Real ETH, real value, and real consequences.
- Ropsten Test Network
  - Ethereum public test blockchain and network. ETH on this network has no value.
- Kovan Test Network
  - Ethereum public test blockchain and network using the Aura consensus protocol with proof of authority (federated signing). ETH on this network has no value. The Kovan test network is supported by Parity only. Other Ethereum clients use the Clique consensus protocol, which was proposed later, for proof of authority–based verification.
- Rinkeby Test Network
  - Ethereum public test blockchain and network, using the Clique consensus protocol with proof of authority (federated signing). ETH on this network has no value.

SMART CONTRACTS

- Smart contracts are a type of Ethereum account
  - A collection of code (its functions) and data (its state)
  - resides at a specific address on the Ethereum blockchain.
  - they have a balance, do not have a private key, cannot initiate a transactions over the network.
  - deployed to the network and run as programmed when called by a user account.
- User accounts can interact with a smart contract by submitting transactions that execute a function defined on the smart contract.
- Smart contracts define rules and enforce them via the code.
- Smart contracts can not be deleted by default, and interactions with them are irreversible.

SMART CONTRACTS: GAS

- a smart contract can be created such that it runs forever when a node attempts to validate it. (a DoS attack.)
- How does Ethereum constrain the resources used by a smart contract if it cannot predict resource use in advance? A metering mechanism called gas
  - As the EVM executes a smart contract it accounts for every instruction (computation, data access..)
  - Each instruction has a predetermined cost in units of gas. Gas is purchased for the transaction, paid in ether..
  - When a transaction triggers the execution of a smart contract, it must include an amount of gas that sets the upper limit of what can be consumed running the smart contract. any unused gas is refunded back to the sender
  - The EVM terminates execution if the gas consumed by computation exceeds the gas available in the transaction.
- Gas is the amount of ETH a transaction's sender must pay to the miner who includes the transaction in the blockchain. Protects against resource-consumption attacks by compromised/malfunctioning nodes.

DECENTRALISED APPS (ĐAPPS)

- Ethereum's vision expanded to become a platform for programming ĐApps
- A ĐApps is composed of at least:
  - Smart contracts on a blockchain
  - A web frontend user interface
- Ethereum web3.js JavaScript library
  - bridges JavaScript applications that run in your browser with the Ethereum blockchain.
  - includes an interface to a P2P storage network called Swarm and a P2P messaging service called Whisper.
- With these three components included in a JavaScript library running in your web browser, developers have a full application development suite that allows them to build web3 DApps.

UPGRADES & HARD FORKS

- With Bitcoin changes are only implemented if they are backward compatible. Existing clients are allowed to opt-in, but will continue to operate if they decide not to upgrade.
- In Ethereum, by comparison, the community's development culture is focused on the future. The mantra is "move fast and break things." If a change is needed, it is implemented, even if breaking compatibility, or forcing clients to update.
- be prepared to rebuild your infrastructure as some of the underlying assumptions change.
- contradiction between deploying code to an immutable system and a development platform that is still evolving.
- You can't simply "upgrade" your smart contracts. be prepared to deploy new ones, migrate users, apps, and funds, and start over.
- In order to "evolve" the platform, you have to be ready to scrap and restart your smart contracts
- Ethereum is a developer's blockchain, built by developers for developers.

FORKING

- Soft fork – no change to protocol structure. Miners can reject & continue mining older coin.
- Hard fork - changes the cryptocurrency protocol, renders older versions invalid. (split)
- DAO fork (2016):
  - 'The DAO' (A Decentralised Autonomous Organisation) raised over $150m from more than 11,000 members - the largest crowdfunding in history. An attacker discovered a contract flaw and drained of 3.6 million Eth.
  - Moved funds to a new contract - goal to restore coins stolen by DAO. Some Ethereum supporters (15%) disagreed with the proposed fork. Resulted in the cryptocurrency split into two: Ethereum and Ethereum Classic
- Tangerine Whistle Fork (2016) – to protect against DOS attacks
- [Source: Full history of releases and forks– Ethereum History, The DAO attack]

https://blog.ethereum.org/2016/10/13/announcement-imminent-hard-fork-eip150-gas-cost-changes/

Announcement of imminent hard fork for EIP150 gas cost changes

Posted by Martin Swende on October 13, 2016

Research & Development

During the last couple of weeks, the Ethereum network has been the target of a sustained attack. The attacker(s) have been very crafty in locating vulnerabilities in the client implementations as well as the protocol specification.

While the recent patches have led to an overall increased resiliency in the client implementations, the attacks have also demonstrated that a lower-level change to the EVM pricing model is needed.

For many users, the most visible consequence is probably that they are having difficulties getting transactions included in blocks, and full nodes are facing memory limitations in managing the bloated state.

This is our strategy to address these issues:

- As a temporary measure to minimize the effects of the most recent attack, we recommend all miners to lower the gaslimit to 500K gas.
- A hard-fork based on EIP 150 version 1c will be put into effect at block ~~2457000~~ [see below]. This will reprice certain operations to correspond better to the underlying computational complexity.
- A second hard-fork will follow shortly after, aimed at reverting the current "state-bloat" introduced by the attacks. This second fork will serve to remove accounts which are empty; lacking code, balance, storage and nonce == 0.

We have implemented the changes required in the clients and are currently extending and adding tests in an effort to prevent the introduction of consensus-breaking vulnerabilities.

And as a reminder, the Ethereum Bug Bounty is open and includes the new hardfork-implementations.

EDIT: Fork block has been moved to **2463000** in order to accommodate even more testing.

Ethereum protocol upgrades

Code name	Release date	Release block
Frontier	30 July 2015[28]	0
Ice Age	8 September 2015	200,000
Homestead	15 March 2016	1,150,000
DAO Fork	20 July 2016	1,920,000
Tangerine Whistle	18 October 2016	2,463,000
Spurious Dragon	23 November 2016	2,675,000
Byzantium	16 October 2017	4,370,000
Constantinople	28 February 2019[29]	7,280,000
Petersburg	28 February 2019[*citation needed*]	7,280,000
Istanbul	8 December 2019	9,069,000
Muir Glacier	2 January 2020[30]	9,200,000
Berlin	15 April 2021[31]	12,244,000
London	5 August 2021[32]	12,965,000

ETHEREUM BASED ERC20 TOKENS

- Tokens represent any tradable goods such as coins, loyalty points etc.
- You can create your own crypto-currencies based on Ethereum.
- By using the ERC20 standard your tokens will be compatible with other client or wallets that use the same standards - can also be sent to any Ethereum address.
- Solidity: A language for writing smart contracts.
- Tether on the Ethereum blockchain is an ERC20 token - makes tether available in Ethereum smart contracts or decentralized applications.

ETHEREUM BASED ERC20 TOKENS

- ERC20 standard defines a set of functions to be implemented by all ERC20 tokens [ref: tutorial]

```
function totalSupply() public view returns (uint256);
function balanceOf(address tokenOwner) public view returns (uint);
function allowance(address tokenOwner, address spender)
public view returns (uint);
function transfer(address to, uint tokens) public returns (bool);
function approve(address spender, uint tokens)  public returns (bool);
function transferFrom(address from, address to, uint tokens) public returns (bool);
```

- ERC20 functions allow an external user, (e.g. a crypto-wallet app) to find out a user's balance and transfer funds from one user to another.
- A constructor is a special function automatically called by Ethereum right after the contract is deployed. -initializes the token's state
- The smart contract defines two specifically defined events. These events will be invoked or emitted when a user is granted rights to withdraw tokens from an account, and after the tokens are actually transferred.

```
event Approval(address indexed tokenOwner, address indexed spender,
 uint tokens);
event Transfer(address indexed from, address indexed to,
 uint tokens);
```

ERC20 TOKENS

- Transaction sending ether to an address changes the state of an address. A transaction transferring a token to an address only changes the state of the token contract, not the state of the recipient address
- ERC20 token standard only tracks the final balance of each account and does not (explicitly) track the provenance of any token.
- hundreds of Ethereum users who accidentally transferred various tokens to contracts that didn't have any ERC20 capability. According to some estimates, tokens worth more than roughly $2.5 million USD (at the time of writing) have gotten "stuck" like this

STABLECOIN CONCEPT

- ...A digital currency that is pegged to a "stable" reserve asset like the U.S. dollar (fiat currency) or gold. Designed to be less volatile relative to unpegged cryptocurrencies like Bitcoin. [ref]
- Can be traded for the U.S. dollar on a one-to-one ratio (e.g. using platforms Coinbase, Circle.)
- Stablecoins are open, global, and accessible to anyone on the internet, 24/7
  - They're fast, cheap and secure to transmit
  - They're digitally native to the Internet and programmable
- Intention is to have the value as close as possible to $1. Backed by actual dollars at financial institutions.

STABLECOIN EXAMPLES

- Examples of popular crypto coins that have a value equivalent to that of a single U.S. dollar and are backed by dollar deposits.
  - USD Coin (USDC) [Aug 2021 there are 27 billion USDC in circulation.]
    - runs on the Ethereum, Stellar, Algorand, and Solana blockchains. Founded by Circle
    - USDC reserves regularly attested (!= audited) by Grant Thornton, (E.g. April 2021, Late Attestations)
  - Tether (USDT) [As of August 2021, there are approx 63.2 billion USDT tokens in existence.]
    - Available on Ethereum
  - TrueUSD
    - Available on Ethereum, TRON, BSC, Avalanche, Signature

STABLECOIN: TETHER

- originally designed to always be worth $1.00, maintaining $1.00 in reserves for each tether issued. Owners of tethers have no contractual right/ legal claims/ guarantee that tethers can be redeemed or exchanged for dollars. Controlled by owners of Bitfinex. [Whitepaper]
- Mar 2019 - changed the backing to include loans to affiliate companies.
- In May 2021, Tether published a report showing that only 2.9% of Tether was backed by cash, with over 65% backed by commercial paper.
- Bitfinex exchange was the subject of a lawsuit by the New York Attorney General for using Tether's funds to cover up $850 million in funds missing since mid-2018
- As of August 2021, there are approximately 63.2 billion USDT tokens in existence.

NFTS - NON-FUNGIBLE TOKENS

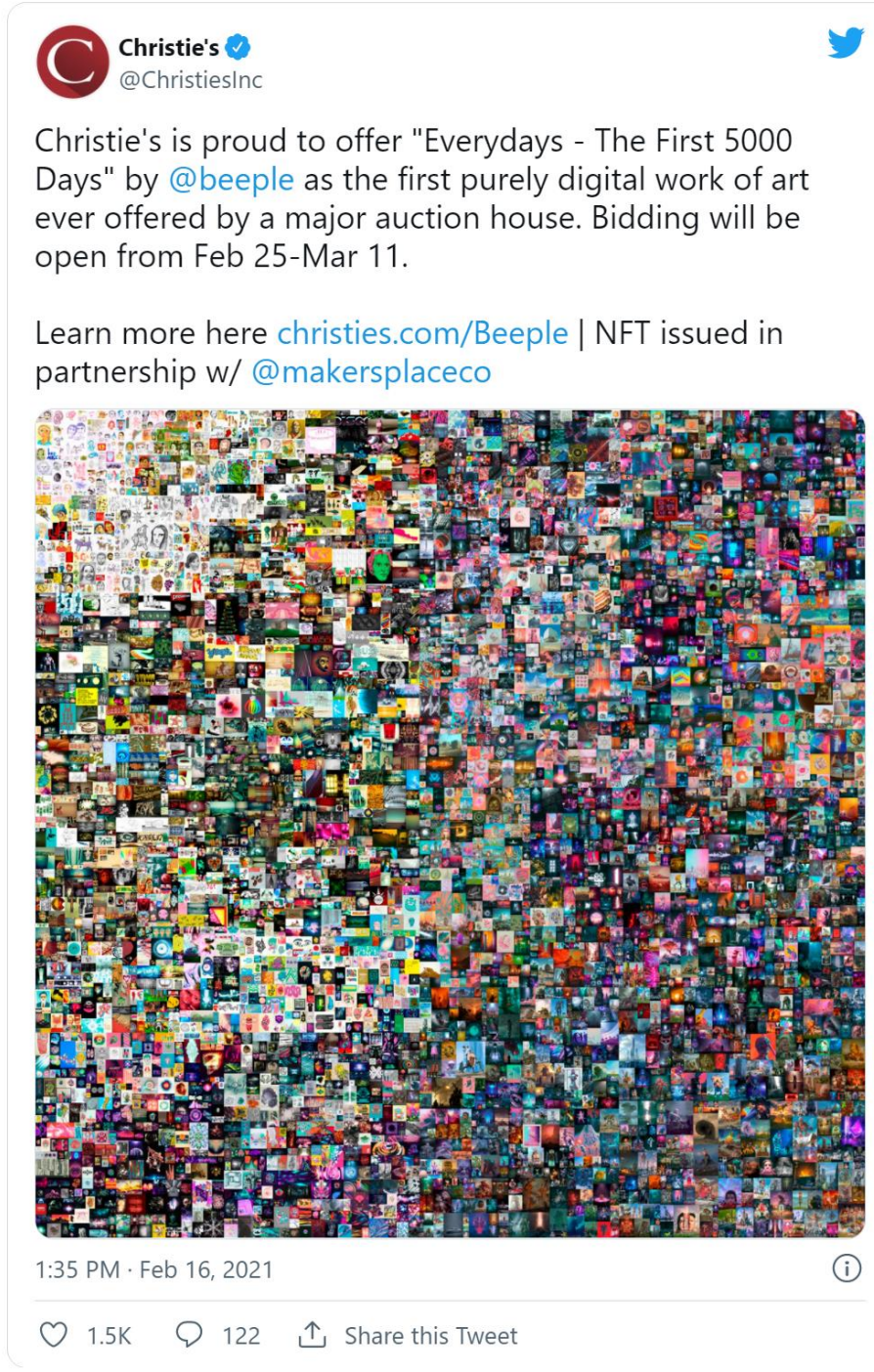
- Fungible tokens are indistinguishable from each other (e.g. dollar or USDC).
- Non-Fungible Tokens (NFTs) Supported by Ethereum to be unique, indivisible, can only have one owner.
  - used to represent ownership of rare items (digital art, cryptokitties, virtual real estate …).
  - Instead of getting an actual oil painting to hang on the wall, the buyer gets a digital file instead.
  - Ownership allows for items to be verified and transferred. Can be sold on the Ethereum blockchain through various digital auction websites.
  - Twitter's Jack Dorsey sold his first ever tweet as an NFT for more than $2.9 million
- ERC20 is a standard for fungible tokens; Tracks each token owner's balance. (Owner is the primary key).
- NFT based on ERC 721: Non-Fungible 'deed' tokens. Tracks each deed ID and who owns it. (primary key=deed)
- The owner or creator can also store specific information inside the NFT. For instance, artists can sign their artwork by including their signature in an NFT's metadata.

FAN TOKENS

- Fan tokens allow holders to vote on mostly minor decisions related to their clubs
- Existing: Barcelona, PSG. .. Planned for 2021: Man Utd, AC Milan, Inter Milan, Leeds Utd, Aston Villa, Man City, Arsenal … (Socios.com)
- Messi's PSG sign-on fee included a "welcome package," estimated at 25-30 million€
- PSG's tokens have a market capitalisation of about $52 million

NFTS FOR ART SALES

- NFTs afford artists and content creators a unique opportunity to monetize their wares.
  - the artist can sell it directly to the consumer as an NFT, lets them keep more of the profits.
  - artists can program in royalties so they'll receive a percentage of sales whenever their art is sold to a new owner.
- March 2021: Mike Winkelmann — (digital artist known as Beeple) sold an NFT of his work for $69 million at Christies



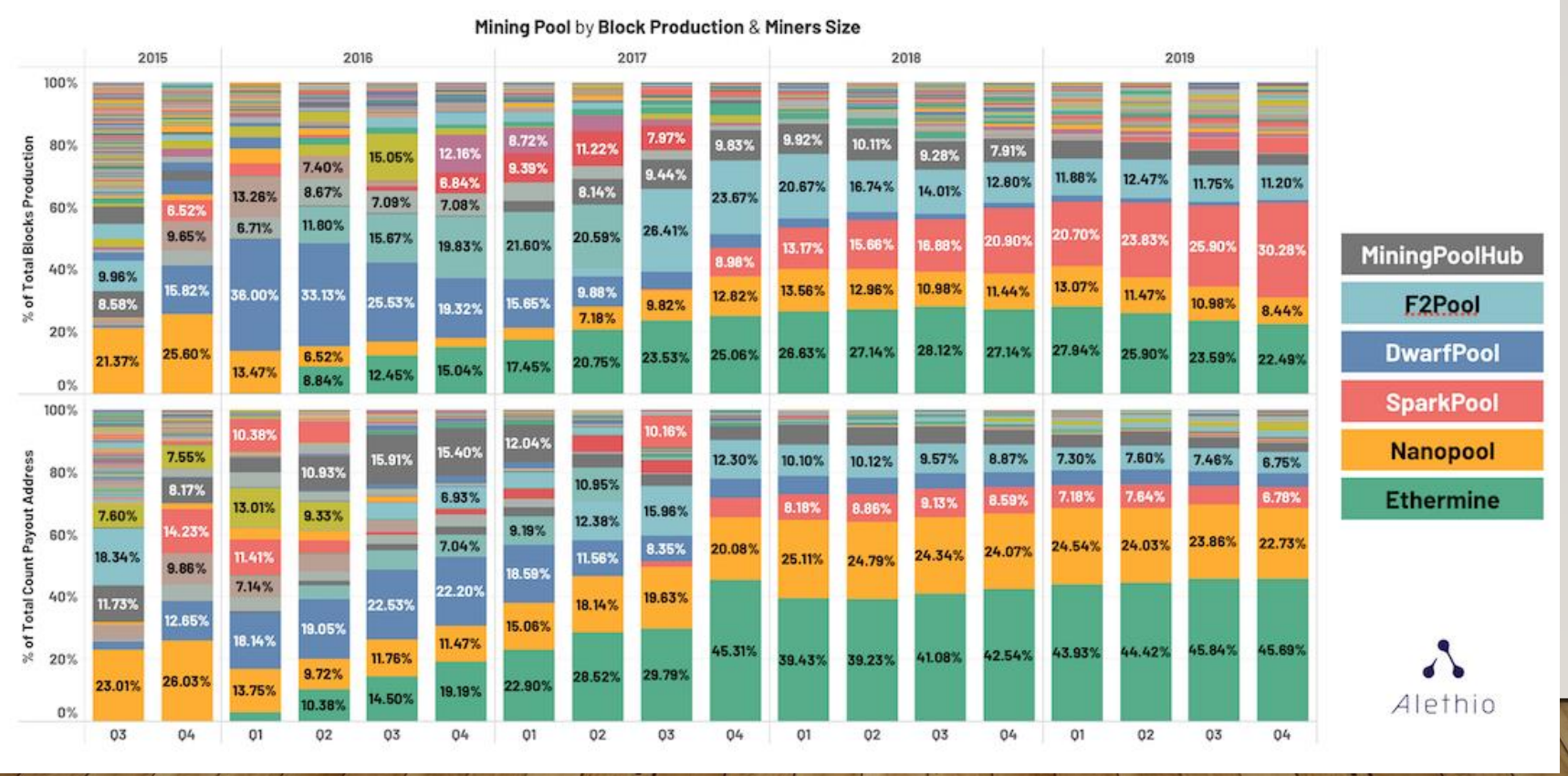
SMART CONTRACT SECURITY CONSIDERATIONS

- Everything you use in a smart contract is publicly visible, even local variables and state variables marked private.
- Front Running - transactions are visible in the mempool for a short while before being executed
- Anyone can send ether to any other account.
- Favour Pull over Push payments
- Re-entrancy [contract A-> contract B] gives control of an Ether transfer to B. B can call back into A before it completes.
- Gas Limit and Loops – DOS scenarios if a loops that do not have a fixed number of iterations – but can only consume as much as the limit - can leave the contact to be stalled.
- Never use tx.origin for contract authorization checks
- Underflows / Overflows

Sources: [Consensys Smart Contract Security Guidance; Solidity Smart Contract Guidance]

MINING POOLS

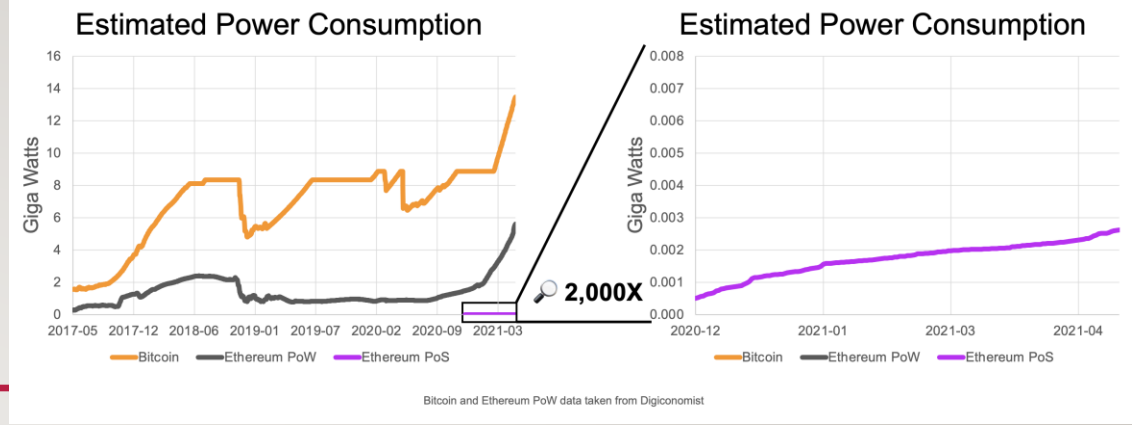
- After 2019 over 50% of blocks on Ethereum were mined by just two mining pools. [ref]



ETHEREUM 2.0

- Development underway for a major upgrade to Ethereum known as Ethereum 2.0 (Eth2)
- purpose is to increase transaction throughput for the network by splitting up the workload into many blockchains running in parallel (referred to as sharding)
  - The shard chains upgrade will spread the load of the network into 64 new chains.
  - reduce congestion and improving speeds beyond the current 15-45 transactions per second limit
  - Introduces **proof-of-stake** consensus
- **Beacon** Chain will randomly assign validators to different shards
  - this makes it virtually impossible for validators to ever collude by attacking a specific shard.
  - cost the attacker far more than they could ever gain from an attack.
- Staking: you don't need to invest in elite hardware to 'run' an Ethereum node. Encourage more people to become a validator

PROOF OF STAKE



- Proof of Stake (POS) is an alternative to the 'proof-of-work' model (POW) that Ethereum currently uses to generate new 'Ether'. Remove the need to utilize power-hungry mining equipment or consumer large amounts of electricity.
- The Ethereum Foundation announced its move to a Proof Of Stake system by end of 2021.
- Ethereum, users will need to stake 32 ETH to become a validator into the official Ethereum 2.0 deposit contract
- Validators are chosen at random to create blocks; responsible for checking and confirming all blocks.
- After other validators then "attest" that they have seen the block the block is added to the blockchain.
- Validators receive rewards both for successfully proposing blocks (just as they do in PoW) and for making attestations about blocks that they have seen.
- A user can lose a portion of their stake for things like going offline (failing to validate) or their entire stake for deliberate collusion.

ETRHEREUM DISTRIBUTIONS

An Ethereum client is a software application that implements the Ethereum specification and communicates over the peer-to-peer network with other Ethereum clients.

Currently, there are six main implementations of the Ethereum protocol:

- Parity, written in Rust
- Geth, written in Go
- cpp-ethereum, written in C++
- pyethereum, written in Python
- Mantis, written in Scala
- Harmony, written in Java

NCC: ETHEREUM IMPLEMENTATION VULNERABILITY CATEGORIES

NCC ref – coinbugs – Analysis / attack methodology against Ethereum implementations

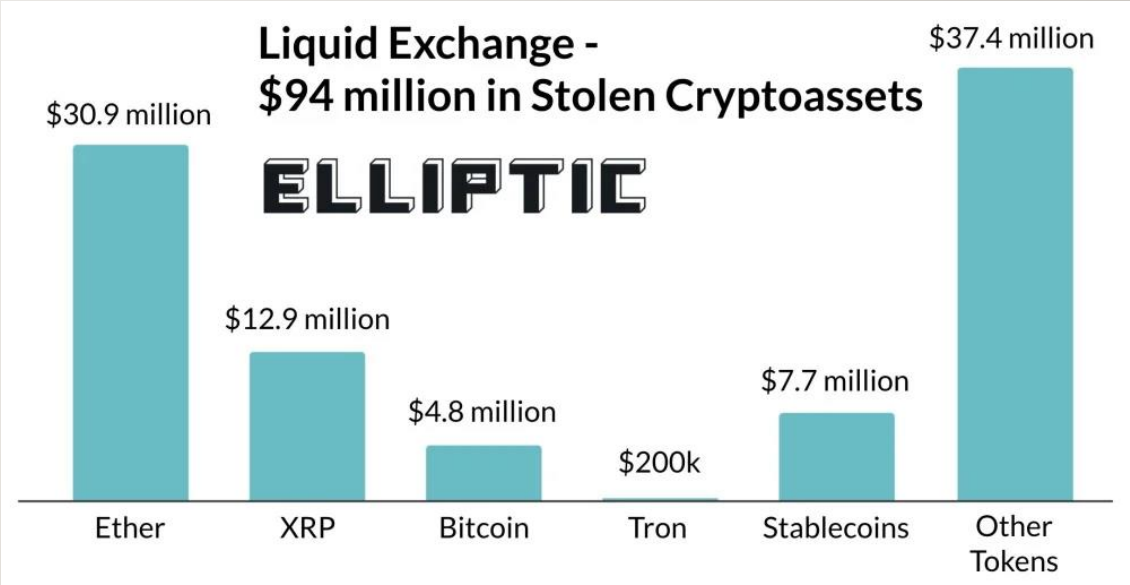
- 1. Netsplit due to multiple client implementations
- 2. Netsplit due to execution environment discrepancies
- 3. Netsplit via block hash poisoning
- 4. Netsplit via unintended or pre-mature fork
- 5. Netsplit via branch confusion
- 6. Improper timestamp validation
- 7. Integer underflow/overflow
- 8. Merkle tree implementation issues
- 9. Storage exhaustion in block or transaction processing
- 10. CPU exhaustion in block or transaction processing

"DEFI" – DECENTRALISED FINANCE

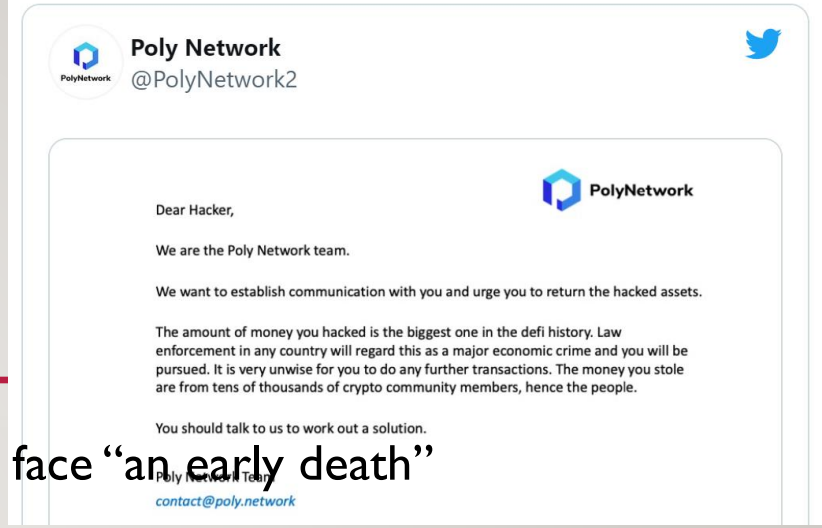
- Financial products available on a public decentralized blockchain network open to anyone to use, no middlemen or brokerages. No IDs or proof of address necessary to use DeFi.
- Designed to remove intermediaries between transacting parties, minimal or no regulation
- Software written on blockchains makes it possible for buyers, sellers, lenders, and borrowers to interact peer to peer. Smart contracts that automate agreement terms between buyers and sellers or lenders and borrowers. "Code is Law"
- Ref #1

LIQUID BREACH

- Aug 19th 2021: Liquid breach - $94m
- Japanese Crypto-currency exchange
- $45 million in Ethereum tokens, being converted into Ether using decentralised exchanges (DEXs) such as Uniswap and SushiSwap. - to avoid having these assets frozen
- ~$20m Ether laundered through Tornado Cash, a smart-contract based mixer used to obscure the blockchain money trail.



POLY $610M MULTI-CHAIN ATTACK



Blockchain-based systems face evolutionary pressure. Weak projects face "an early death"

Since the start of the year until July, DeFi-related hacks totalled $361 million

- Chinese Cross-Chain decentralised finance platform; sits on top of different blockchains, including Bitcoin, Ethereum and Elrond. A master wallet keeps a balance for each coin type.
- Aug 10th 2021: hacker exploited a vulnerability between contract calls effectively allowing the intruder to declare themselves as the owner of funds processed through the platform: $610m
- Flaws were due to a contract authorization weakness and allowing a user defined parameter. [Kudelski report of Poly hack]

```
01;
bytes4(keccak256(abi.encodePacked(_method, "(bytes,bytes,uint64)"))),
```

PART II

OCT 21

ETHEREUM RECAP …

- Ethereum enables developers to build powerful decentralized applications (Dapps) with built-in economic functions.
- Different distributions: Parity(Rust),Geth(Go), cpp-ethereum, pyethereum, Mantis (Scala),Harmony (Java)
- Ethereum always developing new features. Protocol Updates can result in a Hard Fork.
- Two accounts types on Ethereum:
  - User Accounts ("Externally-Owned Accounts / EOA")
  - Contracts

ETHEREUM & SMART CONTRACTS

- Smart contracts are a type of Ethereum account - They are simply computer programs. (there is no “contract”)
- A collection of code (its functions) and data (its state). Resides at a specific address on the Ethereum blockchain. derived from the contract creation transaction and nonce
- Deployed to the network and run as programmed only when called by a user account. (never run on their own). They have a balance, do not have a private key - smart contract accounts own themselves.
- A contract can call another contract –but the chain of execution is always the result of a transaction from an EOA. Ethereum charges a Gas fee (Eth) to constrain the resources used by a smart contract (prevent DoS)

SMART CONTRACT PROPERTIES

- Immutable
  - Once deployed, the code of a smart contract cannot change.
  - Unlike with traditional software, the only way to modify a smart contract is to deploy a new instance. A contract can be "deleted," removing the code and its internal state (storage).
- Deterministic
  - The outcome of the execution of a smart contract is the same for everyone who runs it, given the context of the transaction that initiated its execution and the state of the Ethereum blockchain at the moment of execution.
- EVM context
  - Smart contracts operate with a very limited execution context. They can access their own state, the context of the transaction that called them, and some information about the most recent blocks.
- Decentralized world computer
  - The EVM runs as a local instance on every Ethereum node, but because all instances of the EVM operate on the same initial state and produce the same final state, the system as a whole operates as a single threaded "world computer."

OPCODES AND THEIR GAS COST

Smart contracts are typically written in a high-level language, such as Solidity.
In order to run, they must be compiled to the low-level bytecode that runs in the EVM.
Once compiled, they are deployed on the Ethereum platform

Gas

Command	Code	Description	Gas
ADD	0x01	Add two numbers	3
MUL	0x02	Multiply two numbers	5
LT	0x10	Less-then comparison	3
EQ	0x14	Equality comparison	3
SHA3	0x20	Compute SHA3 hash	30
CREATE	0xf0	Create a new contract	32000
SSTORE	0x55	Save word to storage	up to 20000

SMART CONTRACT FEEDBACK

Error Handling

- When a contract terminates with an error, all the state changes (changes to variables, balances, etc.) are reverted, all the way up the chain of contract calls if more than one contract was called.
- This ensures that transactions are atomic, meaning they either complete successfully or have no effect on state and are reverted entirely.

Events – useful to get feedback / Dapp can 'watch' for events

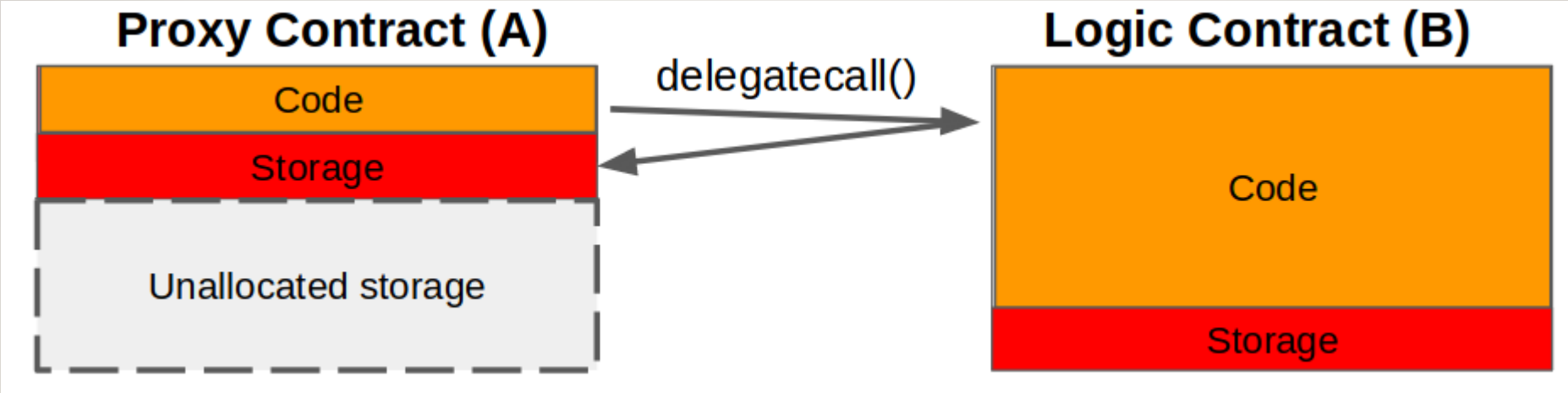
- useful for intra-contract communication, but also for debugging during development

SMART CONTRACT CHAINS

- Smart Contracts calling other smart contacts …
  - a **delegatecall**() is different from a **call**() in that the msg context does not change.
    - Call() changes the value of msg.sender to be the calling contract
    - Delegatecall() keeps the same msg.sender (msg.sender is not the address of caller)
  - delegatecall runs the code of another contract inside the context of the execution of the current contract.
  - The delegate call should be used with great caution.

PROPOSAL TO ALLOW CONTRACT UPDATES

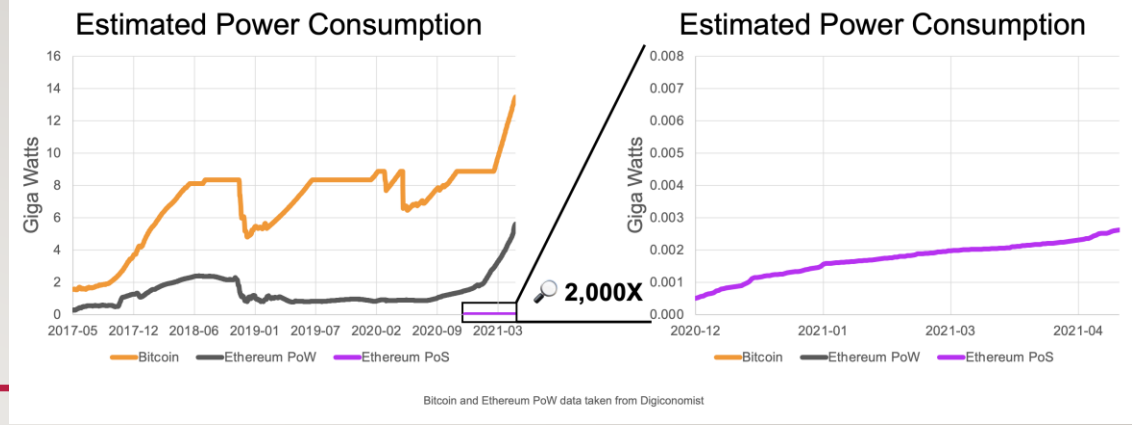
- Contract Proxy Proposal – EIP-1822



RECAP: ETHEREUM 2.0

- Development underway for a major upgrade to Ethereum known as Ethereum 2.0 (Eth2)
- purpose is to increase transaction throughput for the network by splitting up the workload into many blockchains running in parallel (referred to as sharding)
  - The shard chains upgrade will spread the load of the network into 64 new chains.
  - reduce congestion and improving speeds beyond the current 15-45 transactions per second limit
  - Introduces **proof-of-stake** consensus
- **Beacon** Chain will randomly assign validators to different shards
  - this makes it virtually impossible for validators to ever collude by attacking a specific shard.
  - cost the attacker far more than they could ever gain from an attack.
- Staking: you don't need to invest in elite hardware to 'run' an Ethereum node. Encourage more people to become a validator

RECAP: PROOF OF STAKE



- Proof of Stake (POS) is an alternative to the 'proof-of-work' model (POW) that Ethereum currently uses to generate new 'Ether'. Remove the need to utilize power-hungry mining equipment or consumer large amounts of electricity.
- The Ethereum Foundation announced its move to a Proof Of Stake system by end of 2021.
- Ethereum, users will need to stake 32 ETH to become a validator into the official Ethereum 2.0 deposit contract
- Validators are chosen at random to create blocks; responsible for checking and confirming all blocks.
- After other validators then "attest" that they have seen the block the block is added to the blockchain.
- Validators receive rewards both for successfully proposing blocks (just as they do in PoW) and for making attestations about blocks that they have seen.
- A user can lose a portion of their stake for things like going offline (failing to validate) or their entire stake for deliberate collusion.

ETHEREUM FOR ENTERPRISE

ON PRIVATE NETWORKS

BLOCKCHAIN ENTERPRISE CHALLENGES

Common Security Requirements	Public Ethereum Default
Strong identification / key rotations	Anonymous Identities / perpetual keys
Authentication / Authorization controls	Open access to Blockchain
NIST approved crypto	Crypto predefined
Forward Secrecy	Crypto predefined
Encryption in Transit	Unencrypted
Encryption at Rest	Unencrypted
HSMs for high value keys	Local storage for Node & transaction Keys
Run my own code /3rd party code untrusted	Execute all smart contracts submitted by others
Optimise compute / minimise costs	Mining???

ENTERPRISE USE QUESTIONS

- Use Mainnet?
  - public blockchain network for business interactions.
- Private Network:
  - May or may not include a 'GAS' transaction fee (constrain resource consumption)
  - Transactions not necessarily to transfer funds.
  - Transactions might not be intended to be viewed by everyone
  - Decide on your own consensus and identity strategy
  - Do we need to support Ether payments? Can we use the Eth in a private network?
  - Scalability: How often are we expecting to write a new block
    - Ethereum blocks are validated approximately every 12 seconds on Ethereum (vs approximately every 10 minutes on Bitcoin.)
  - How do we manage updates to code?
  - Multiparty signatures

OPEN-SOURCE ETHEREUM PROJECTS

- Hyperledger Community:
  - an open source community focused on developing frameworks, tools and libraries for enterprise-grade blockchain deployments.
- Hyperledger BESU:
  - an open source Ethereum client maintained by the Hyperledger community.
  - Besu is Mainnet compatible, Java-based, Apache 2.0 licensed.
- GoQuorum:
  - an open-source Ethereum client maintained by ConsenSys.
  - GoQuorum is Go-based and GPL licensed.

HYPERLEDGER BESU

- Used to develop enterprise applications requiring transaction processing in a private network.
- Runs on the Ethereum public network (mainnet), private networks, and test networks such as Rinkeby, Ropsten, and Görli.
- Consensus options: Proof of Work (Ethash) and Proof of Authority (IBFT 2.0 and Clique)
- Besu includes a CLI and JSON-RPC API for running, maintaining, debugging, and monitoring nodes in an Ethereum network. The API supports HTTP or via WebSockets or using Pub/Sub. Supports typical Ethereum functionalities such as:
  - Ether mining
  - Smart contract development
  - Decentralized application (Dapp) development.

HYPERLEDGER BESU NODE TYPES

- Validators (for Proof of Authority consensus protocol)
  - take turns to create new blocks.
  - Validators can vote to add or remove validators. Need > 50% of validator votes
  - In IBFT2 networks >66% of the validators must sign each block
  - In IBFT2 networks 4 validators are required to be fault tolerant
- Boot nodes - if you don't have a static address list of peers.
- Observer nodes
  - read only, to react to certain transactions and execute certain smart contracts
- Tessera nodes

CONSENSUS OPTIONS

- IBFT 2.0 (Proof of Authority) - grants immediate finality for enterprise use cases. - we will use this, we want pruning - to cut off transactions.
- QBFT - next version .. ..
- Ethash (Proof of Work)
- Clique (Proof of Authority) - fast, high fault tolerance, does not provide immediate finality.
- Proof of Stake includes the Casper protocol to achieve finality. Casper, a finality protocol, gets validators to agree on the state of a block at certain checkpoints. So long as 2/3 of the validators agree, the block is finalised. Validators will lose their entire stake if they try and revert this later on via a 51% attack.

ACCESS MANAGEMENT

- Permissioned Network vs On-Chain Permissioning
- On-Chain: Permissioning Management Dapp will facilitate managing permissioning rules and maintaining the list of admin accounts that can edit rules.
  - Account Ingress Contract
  - Nodes Ingress Contract
  - Host Allow Lists
- Ref #Consensys,

CRYPTO SCENARIOS

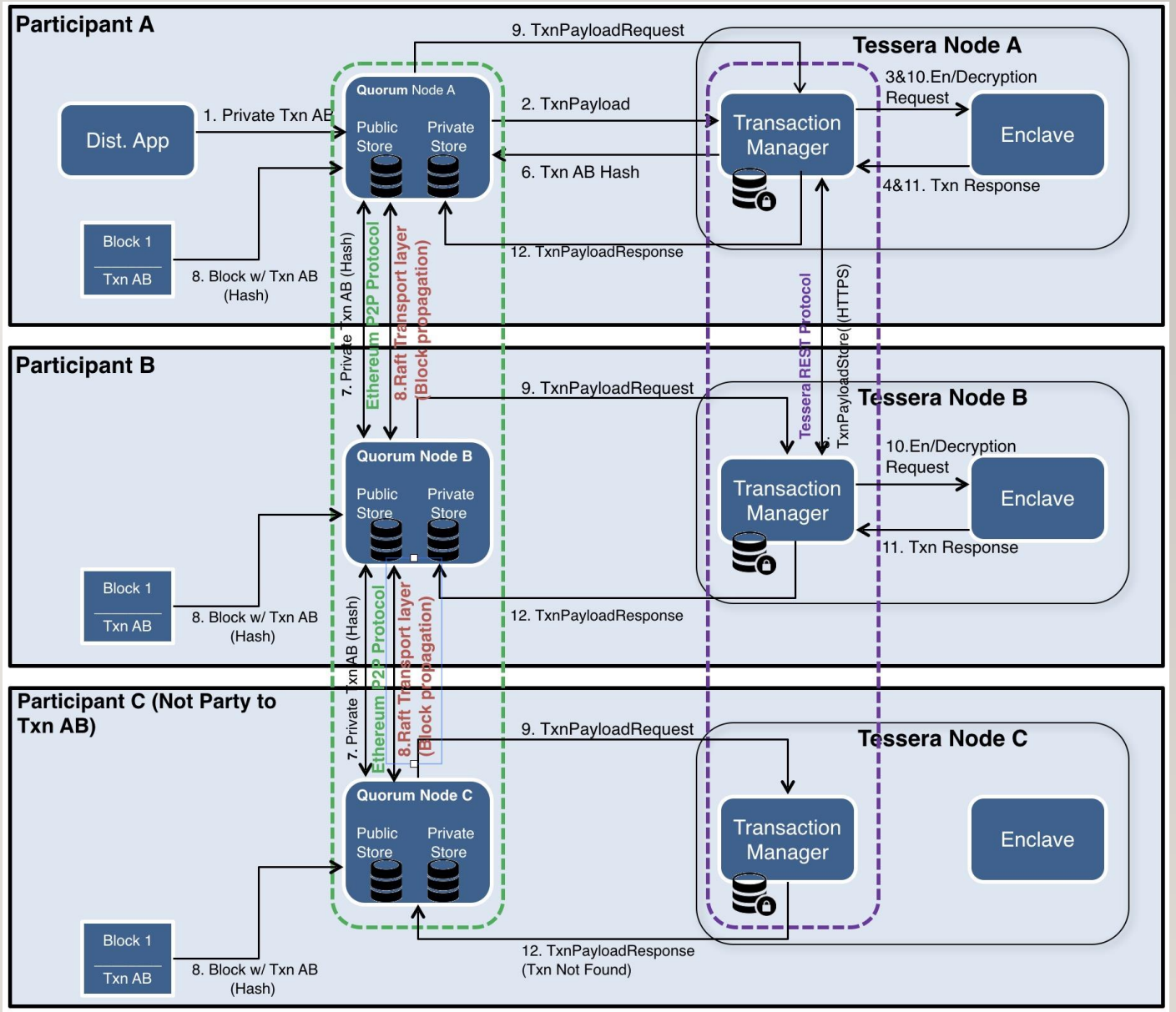
- Application – Blockchain Node -- Terrera
  - Application Key creation (private key)
  - Application Transaction signing
- Ethereum Node
  - Local storage (data@rest) / Smart Contracts
  - Ethereum Node to Ethereum Node
- Ethereum Node to Orion / Tessera Node (data in transit)
- Tessera to Enclave (data in transit)
  - Tessera Enclave data@rest
  - Tessera Enclave data in transit – Curve 25519 Diffie Hellman key exchange function, Salsa20 stream cipher, poly1305 MAC authenticates the
- Ethereum to Rollup Node .. ..

HYPERLEDGER + TESSERA

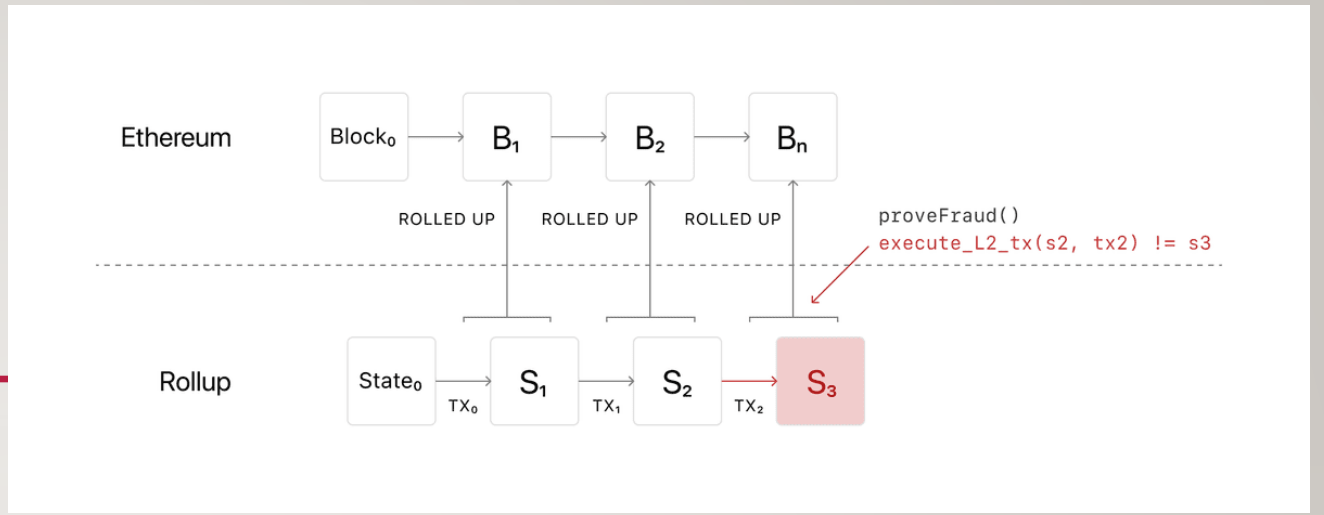
Tessera Transaction manager

the privacy manager for privacy-enabled Ethereum clients

[Ref]



ROLLUPS



- Off-chain processing of transactions
- Optimistic rollups use a side chain that sits in parallel to the main Ethereum chain.
- They can offer improvements in scalability because they don't do any computation by default. Instead, after a transaction they propose the new state to mainnet. Or "notarise" the transaction.
- Implementation is not standard, but interface is standard
- Publish Zero knowledge proof (merkle root)

PRIVACY – ZETHER

Zero Knowledge Proof protocol for Ethereum

- Provides transaction confidentiality which requires hiding investors' account balances and transaction amounts, while enforcing compliance rules and performing validity checks on all activities. [ref1] [ref2]
- Possible Scenario: Sealed bids – submit a bit – want to prove you have at least funds to cover bid, don't want to reveal bid to others
- uses ElGamal public key encryption to hide transaction amounts and utilizes zero-knowledge proofs to demonstrates the validity of a transaction to stakeholders, namely network validators, investors, and auditors.
- bidders can simply lock their accounts to the auction contract, thus getting full bid confidentiality.
- When the network validators receive the transaction, they verify the zero-knowledge proofs, and if successful, subtract CiphertextAlice(x) from Alice's balance and add CiphertextBob(x) to Bob's balance

ETHEREUM REFERENCES

- GitHub - ethereumbook/ethereumbook: Mastering Ethereum, by Andreas M. Antonopoulos, Gavin Wood
- https://takenobu-hs.github.io/downloads/ethereum_evm_illustrated.pdf
- https://entethalliance.org/wp-content/uploads/2020/11/EEA_Enterprise_Ethereum_Client_Specification_v6.pdf
- NCC-Group-Whitepaper-Coinbugs.pdf (nccgroup.com)
- https://www.forbes.com/advisor/investing/nft-non-fungible-token/

QUESTIONS

- ?