`

STATE BAR OF WISCONSIN
PINNACLE
Your Practice. Our Purpose.

WSSFC 2022

Technology Track – Session 2

Cryptocurrency and Blockchain 101

Aaron Brooks, Jeffrey M. Glazer

About the Presenters…

Aaron Brooks, Brooks Law and Consulting LLC, Naperville, IL.

Jeffrey M. Glazer is a partner at Ogden Glazer + Schaefer where he manages the firm's food and beverage practice. He has worked with alcohol beverage companies for the past 15+ years and his practice encompasses all 4 tiers of the 3-tier system (don't forget the farmers that make the ingredients!!); OG+S represents a wide array of (farmers), manufacturers, wholesalers, and retailers. He has spoken at numerous events across the country on food and beverage issues and published frequently on topics relevant to the industry. Jeff was the founder of Madison Beer Review and Madison Craft Beer Week.

The Basic Elements of Blockchain

Aaron W. Brooks

When trying to understand what blockchain is and how it works, it's helpful to begin by considering the specific problem that blockchain was invented to solve, and the historical context within which it arose. The first blockchain was the Nakamoto Blockchain (more commonly known as Bitcoin). Bitcoin was launched on January 3, 2009, and the first Bitcoin transaction occurred on January 11, 2009.[1] At this time, the World was consumed by the Global Financial Crisis of 2008. In the United States, many felt outrage and fear at the ideas of "too big to fail" and a governmental bailout of the global banking system.[2] Similarly, this period began a renewed examination of the systemic impact on government control and creation of money, and specifically who tends to benefit from governmental policies relating to the money supply.[3] These dynamics came together to severely undermine confidence in banking institutions acting as the gatekeepers of most financial transactions. So too, these events are the direct and immediate inspiration for the very first sentence of the original Bitcoin whitepaper: "A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution."[4]

Core Blockchain Technology

For Bitcoin to be a fully electronic form of money, and for it to avoid all forms of centralized control, the system needed to be inherently secure and functional. In other words, it needed to work on its own and without the need for a central administrator. It needed to ensure that money could not be double-spent, and it needed everyone who used the system to simultaneously agree that all transactions recorded in the system were valid and irreversible. To accomplish these goals, Satoshi Nakamoto (the pseudonym for the person or group who invented Bitcoin) drew upon several pre-existing technologies. The most important of these building blocks were: Asymmetric cryptography and hash functions, peer-to-peer networking, consensus algorithms, and proof of investment. Thus, rather than thinking of blockchain as a new and never-before-seen technology, we should instead think of blockchain as a new and unique combination of existing tools that were brought together to solve a very specific problem.

[1] Blackburn, Huber, Eliaz, et.al. "Cooperation Among an Anonymous Group Protected Bitcoin During Failures of Decentralization." arXiv:2206.02871, 2022.

[2] Weinstein, Adam. "'We Are the 99 Percent' Creators Revealed." Mother Jones, October 7, 2011. https://www.motherjones.com/politics/2011/10/we-are-the-99-percent-creators. Accessed October 1, 2022.

[3] Stoller, Matt. "The Cantillon Effect: Why Wall Street Gets a Bailout and You Don't." Promarket, April 13, 2020, https://www.promarket.org/2020/04/13/the-cantillon-effect-why-wall-street-gets-a-bailout-and-you-dont. Accessed October 1, 2022.

[4] Nakamoto, Satishi. "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin.org, October 31, 2008. https://bitcoin.org/bitcoin.pdf. Accessed October 1, 2022.

Asymmetric Cryptography and Hash Functions

Asymmetric cryptography is a system whereby people can exchange encrypted messages without knowing one another's private decryption key.[5] The core idea behind asymmetric cryptography is that of a public/private key pair. Everyone can know your public key, but your private key is like a secret password. If something is encrypted using your public key, it can only be decrypted using your private key. The reverse is true as well: If something is encrypted using your private key, it can only be decrypted using your public key.

Asymmetric cryptography plays a major role in blockchain; it's the foundation for how blockchain accounts are created and how blockchain transactions are conducted. A blockchain account is little more than a public/private key pair. The public key in a blockchain account is the wallet address. The private key for that wallet is necessary to authorize transactions from that wallet.

One major benefit of public/private key pairs in blockchain is the fact that one can send and receive money without ever disclosing the password for their blockchain account. For example, Bitcoin transactions work by the payor sending Bitcoin to the payee's public wallet address, and that is the only information the payee needs to send that money. By contrast, in a credit card transaction, the payor typically provides the payee with all the information necessary for the payee to conduct future fraudulent transactions. Similarly, bank account checks disclose the account number and routing number of the payee, which is again enough information to conduct future fraudulent transactions.[6]

The second cryptographic function that makes blockchain work is that of a hash function. Hash functions are computer algorithms that take a random data input and convert it into a standard 256-bit unique output. The following are examples of hash functions produced using the SHA-256 algorithm:

A	559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd
Apple	f223faa96f22916294922b171a2696d868fd1f9129302eb41a45b2a2ea2ebbfd
APPLE	55562347f437d65829303cf6307e71acf8b84a020989dd218f31586eeafd01a9

For any given input, regardless of the length or characters used, the output is always a standard 256-bit code (represented in 64 hexadecimal characters). For any specific input, the SHA-256 output is always the same. Thus, "A" is always equal to the 256-bit code shown in the first row above. However, if one is only given the 256-bit code, it is impossible to reverse engineer the

[5] This differs from *symmetric cryptography* systems, where all participants share the private key; for example, a Zoom meeting can be encrypted, but all participants must know the same passkey to join the meeting.

[6] ARK Invest. "The ₿ Word | Live with Cathie Wood, Jack Dorsey, & Elon Musk." YouTube, July 21, 2021. https://youtu.be/Zwx_7XAJ3p0?t=252. Accessed October 1, 2022.

input and figure out that the code stands for “A” – so hash functions are nonreversible one-way transactions.

Blockchain systems use hash functions is to create an entity called a *Merkle Tree*. The end result of a blockchain-based Merkle Tree is called a *root hash*, and it is the root hash which creates the “chain” in blockchain. The following table attempts to illustrate how the hashes of each individual transaction are hierarchically combined to create a single hash for the entire set of transactions:

Hash of Each Transaction	Hash of Hashes	Root Hash
Transaction One Hash	*Hash of One and Two Hashes*	*Hash of (1+2) and (3+4)*
Transaction Two Hash		
Transaction Three Hash	*Hash of Three and Four Hashes*	
Transaction Four Hash		

Think of the table above as a block of individual transactions. The root hash is the penultimate hash of all the transactions within that block. This root hash is then used as the input to encrypt the block that comes after it. The root hash of the next block then becomes the input to encrypt the block that comes after that. This encryption process continues block after block after block; and, in this way, the transaction blocks are chained together by each of their root hash values.

Because the transaction blocks are chained together by each of their root hash values, it becomes harder and harder to alter any one of the transactions as more and more blocks get added to the chain. The reason is that the root hash of each block is calculated from the exact contents of the transactions in that block. Altering any one of these transactions would produce a vastly and unpredictably different root hash (which would then alter the hash values of every block that comes after that, because every block value is calculated from the exact hash of the previous block). Thus, an attacker seeking to alter blockchain transactions would need to alter all the transactions in every block that comes after the transaction they are trying to attack. Since blockchain miners around the world are in constant competition to produce the next block in the chain, the attacker would need to alter all these transactions and hashes at a rate that is consistently faster than every other miner on Earth combined. In short, it isn’t practically conceivable that anyone could alter a blockchain transaction after it is locked into the chain.

Peer-to-Peer Networking

A network is any system that allows two or more computing devices to communicate with each other. Often, networks follow the client/server model in which many end user devices all use a central server to store data and provide resources. However, some networks remove the server and allow each of the clients to function as equals. All computers on such a network are *peers*, and transactions on such a network happen from one *peer* to another without any intermediary servers.

Peer-to-peer networking is critical to blockchain functionality, because one of the main points of blockchain was to eliminate the idea of a central processor of transactions. On any given blockchain, therefore, all transactions are processed by every node on that blockchain. For this to work, all the nodes on the blockchain must be connected on a common network (that network typically being the Internet). Each node must also be running the appropriate software for that blockchain. A blockchain's software provides the essential communication protocols and the core transaction validation rules that are associated with that blockchain.

When a blockchain transaction gets authorized by a wallet holder's private key, that transaction is then broadcast to all nodes on the blockchain. The blockchain's communication protocols and designated network ports coordinate and facilitate this broadcast. Each node operator then races to put that transaction into a block and then validate all the transactions in that block. The first node to assemble and validate a new block will earn the right to publish that block to the public chain, and that node typically then earns a reward for this effort. All of this happens according to the consensus algorithms and investment proofing mechanisms discussed below.

Consensus Algorithms

Blockchains are designed to be decentralized. Therefore, no central authority should be required to determine whether any given blockchain transaction is valid. For a decentralized system to work, all nodes on the blockchain must simultaneously agree that every transaction on the chain is valid. Blockchain processors are not related, coordinated, or publicly known; thus, they cannot rely on trust or legal enforcement to ensure they each process transactions according to a given set of rules. For all these reasons, each blockchain must have a built-in system, known as a consensus algorithm, to ensure that every node processes and validates transactions the same way.

Blockchain consensus algorithms are built into the software that forms the blockchain itself. Since all nodes must run the same blockchain software in order to communicate with each other, they must all run the same consensus algorithm. The consensus algorithm requires each node to process transactions according to a list of very specific criteria,[7] and they must reject any transaction or block of transactions that fails any of these criteria. For example, blockchain transaction criteria might include things like:

- The transaction is formatted correctly and contains all information necessary to form a complete transaction
- The payor account has the necessary funds to perform the transaction
- There is no duplicate or conflicting transaction in the pool of unprocessed transactions
- The payee public wallet key is valid and existing

[7] For a detailed list of the validation criteria used in Bitcoin, See: Antonopoulos, Andreas. "Mastering Bitcoin, 2nd Edition." O'Reilly Media, Inc., 2017, Ch. 10.

Any blockchain can create its own consensus algorithm. The speed and security of a blockchain's consensus algorithm can be an important factor that determines whether the blockchain becomes widely adopted.

Investment Proofing Mechanisms

Investment proofing mechanisms are a close relative to the consensus algorithm. The purpose of an investment proofing mechanism is to create some kind of test to ensure that anyone who wants to process transactions on a blockchain has made an investment of some kind, and therefore has a financial stake in the security and stability of the network itself.

The first investment proofing mechanism for blockchain was implemented in Bitcoin and called *proof of work*. This mechanism was taken directly from a previous system called *Hashcash* by Adam Back.[8] Hashcash was designed to limit email spam by requiring any computer that sends an email to solve a math problem in order to push the email onto the network. By solving the math problem, the sender proves that they have expended a certain amount of computational power. The more email that a sender sends, the more computational power they must expend. Theoretically, the amount of power required to send mass email spam would outweigh the benefit of doing it.

Similarly, to process a block of transactions on a proof of work based blockchain, a processor must solve a math problem[9] that requires it to expend computational power. Not only does this require all processors to make a fairly substantial investment prior to processing transactions, but it also makes altering valid transactions exponentially more difficult as more and more blocks are added to the chain, because the person seeking to alter the transaction would need to repeat the proof of work for every block that comes after the transaction they seek to alter.

Proof of work is frequently criticized for consuming inordinate amounts of electricity.[10] This happens because every processing node in the blockchain must separately and simultaneously compete to solve the same math problem in order to earn the right to publish the next block. Since Bitcoin was first introduced a second major investment proofing mechanism has evolved: *Proof of stake*.

[8] Back, Adam. "A Partial Hash Collision Based Postage Scheme." Hashcash.org, March 28, 1997. http://www.hashcash.org/papers/announce.txt. Accessed October 1, 2022.

[9] Although most people refer to this as a "math problem" it's really just a guessing game. Put simply, a proof of work blockchain processor must guess a number that, when incorporated into the root hash, results in an output that begins with a series of zeros. There is no pattern to how these guesses should be plotted; a miner must simply use a computer that is fast enough to guess so many numbers over and over that they have a reasonable chance of getting the right output before any other competing miner does the same thing. Computers with enough power to do that will draw a large amount of electricity.

[10] Hinsdale, Jeremy. "Cryptocurrency's Dirty Secret: Energy Consumption." News from the Columbia Climate School, May 4, 2022. https://news.climate.columbia.edu/2022/05/04/cryptocurrency-energy. Accessed October 1, 2022.

In a proof of stake paradigm, blockchain transaction processors must possess a certain quantity of the blockchain's coins in order to qualify as a processor. This addresses the same concern that proof of work mechanisms seek to address, which is to prove that a blockchain processor has made a substantial investment in the network. However, unlike proof of work, a proof of stake investment needs only be made once (as opposed to every time a new block is processed). In this way, proof of stake blockchains consume significantly less energy than their proof of work counterparts.

Blockchain Use Cases

Money

As described above, the initial use case for blockchain was to serve as a new digital currency. Bitcoin was intended to function the same way that any other money functions. Unlike traditional money, however, Bitcoin is resistant to manipulation and centralized control. Thus, while a government can increase the supply of its own fiat currency by printing more, Bitcoin has a finite supply and a rate of production that cannot be altered.

Bitcoin is designed to act like money and be sought after for the same reasons people try to acquire traditional money. The following are some key elements of Bitcoin that, in my view, cause it to be valued like money:

- Rarity. Bitcoin cannot be randomly found or created. As a hypothetical, if a basic rock was commonly scattered around the planet and anyone could easily collect a bag full of basic rocks, then nobody would regard that rock as money because the effort to collect more rocks will always be less than the effort needed to produce goods and services for which that rock could be traded. If, however, that rock were difficult and expensive to find (like gold), then people are more likely to trade goods and services in exchange for pieces of that rare rock.
- Known or Predictable Market Capitalization. Bitcoin has a fixed total production limit of 21 million, and it has an algorithmically determined rate of production. Continuing with the gold analogy, if we thought there was a vast new supply of gold that might soon be discovered, we would not place as much value on gold. The value of gold is based on our reasonable belief that we know about how much exists and how quickly more gold will be mined.
- Identifiable/Verifiable. Bitcoin cannot be counterfeited, and it is very easy to determine whether a unit of Bitcoin is real or not. Similarly, people can easily determine whether a unit of gold is real and calculate its level of purity. If it became easy to produce synthetic gold that is indistinguishable from traditional gold, then the value of gold would drop.
- Attractive or Interesting. Many people find Bitcoin to be fascinating, and they are very taken with the idea of how the system functions and the joy of participating in Bitcoin transactions. Similarly, gold is inherently attractive to people. The look and feel of gold contributes to the valuation people attribute to gold. On the other hand, if a substance had

all the aforementioned traits, but it was slimy, smelly, and rancid, it seems unlikely that it could function as money (unless it could be encapsulated in something that shields these unpleasant qualities while preserving all the other traits).

Smart Contracts

Blockchain systems can be more than simple ledgers of financial transactions. They can also be global decentralized computers that run distributed computer programs called smart contracts. Like any blockchain account, a smart contract has a public address and a private key. However, smart contracts also contain computer code that can be invoked when it receives special transactions through its native blockchain. Some popular implementations of smart contracts are summarized as follows:

- Nonfungible Tokens. A nonfungible token (or "NFT") is a special type of blockchain asset that is created and controlled by a smart contract that follows a well-defined token standard. The most popular NFT standard is ERC-721, which is defined within the Ethereum blockchain protocols. NFTs could evolve into the first bona fide way of truly owning digital assets. Currently, most digital assets (such as music, movies, and books) are stored in a centralized system like Amazon or Netflix and simply licensed to the end user. They typically cannot be loaned, sold, gifted or bequeathed. However, if a digital song, movie, or book were implemented as an NFT and transferred on a blockchain, the wallet owner associated with those digital assets would have true ownership and the ability to loan or sell those assets without any control or permission from a centralized authority.
- Decentralized Finance. Another important use of blockchain based smart contracts is decentralized finance systems (or "DeFi"). For example, a person could borrow money by staking one or more blockchain based assets in a smart contract. If the money were not repaid as provided in the smart contract, then the staked asset would be automatically liquidated. On the other side of these transactions, individual lenders can invest their resources into the liquidity pool that funds DeFi loans. These DeFi loans are secured by the staked assets, and they earn interest by virtue of the smart contract that enforces the repayment terms. In this way, loans and interest-bearing investments can be established, coordinated, and enforced without any central authority managing the transactions.
- Tokenized Real Estate. Another popular use of smart contracts is to create investment tools whereby fractional interests of real estate projects can be bought and sold on an open market without any centralized authority. For example, consider that a condominium complex could be transferred into a legal entity, and the ownership of that legal entity can be represented by tokens on a blockchain. Those tokens can then be sold to investors who wish to participate in the potential appreciation and profits of the condominium's operations. Those token holders now have a market through which they can exchange these tokens in a way that is like stock.

Conclusion

Blockchain is certainly a new and exciting invention. It is, however, essentially just a new and unique combination of existing technology, and not so much a new technology itself. The overall level of blockchain investment and development has grown every year since the initial release of the Nakamoto Blockchain. Thus, our current understanding of blockchain is that of a new and rapidly changing system. Still, while we can expect future blockchains to be more sophisticated and capable, it seems likely that the fundamental elements of blockchain that are described in this paper will always be the core of any future blockchain system. They are the essence of what makes blockchain different from other computer networks.

The Essential Concept

Hash Functions and Asymmetric Cryptography

Hash Function Examples (SHA256)

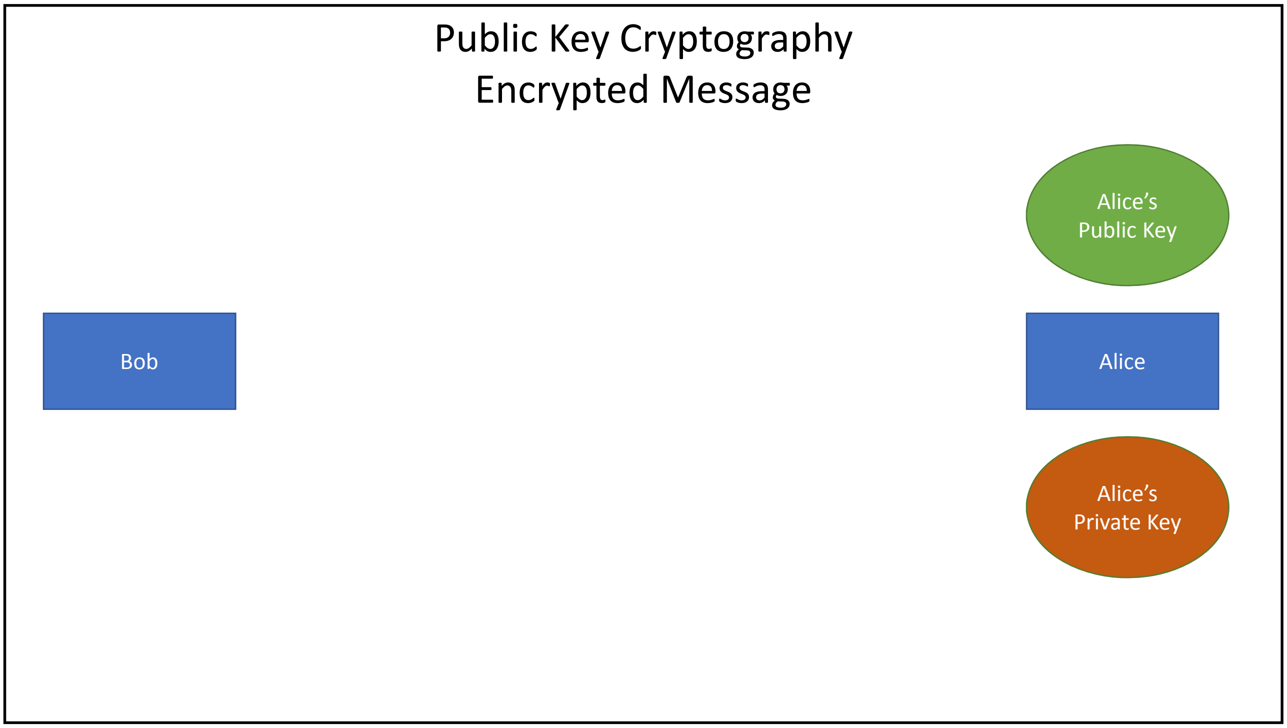
A → 559aead08264d5795d3909718cdd05abd49572e84fe55590eef31a88a08fdffd

Apple → f223faa96f22916294922b171a2696d868fd1f9129302eb41a45b2a2ea2ebbfd

APPLE → 55562347f437d65829303cf6307e71acf8b84a020989dd218f31586eeafd01a9

Lw#zdv#wkh#ehvw#ri#wlphv/#lw#zdv#wkh#zruvw#ri#wlphv/#lw#zdv#
wkh#djh#ri#zlvgrp/#lw#zdv#wkh#djh#ri#irrolvkqhvv/#lw#zdv#
wkh#hsrfk#ri#eholhi/#lw#zdv#wkh#hsrfk#ri#lqfuhgxolw|/#lw#zdv#
wkh#vhdvrq#ri#Oljkw/#lw#zdv#wkh#vhdvrq#ri#Gdunqhvv/#lw#
zdv#wkh#vsulqj#ri#krsh/#lw#zdv#wkh#zlqwhu#ri#ghvsdlu/#zh#
kdg#hyhu|wklqj#ehiruh#xv/#zh#kdg#qrwklqj#ehiruh#xv/#zh#
zhuh#doo#jrlqj#gluhfw#wr#Khdyhq/#zh#zhuh#doo#jrlqj#gluhfw#
wkh#rwkhu#zd|00lq#vkruw/#wkh#shulrg#zdv#vr#idu#olnh#wkh#
suhvhqw#shulrg#wkdw#vrph#ri#lwv#qrlvlhvw#dxwkrulwlhv#
lqvlvwhg#rq#lwv#ehlqj#uhfhlyhg/#iru#jrrg#ru#iru#hylo/#lq#wkh#
vxshuodwlyh#ghjuhh#ri#frpsdulvrq#rqo|1

→ ed633af0c65541c5f02ab7bb2dc922832ac7f91071497991096c32e8905246b4



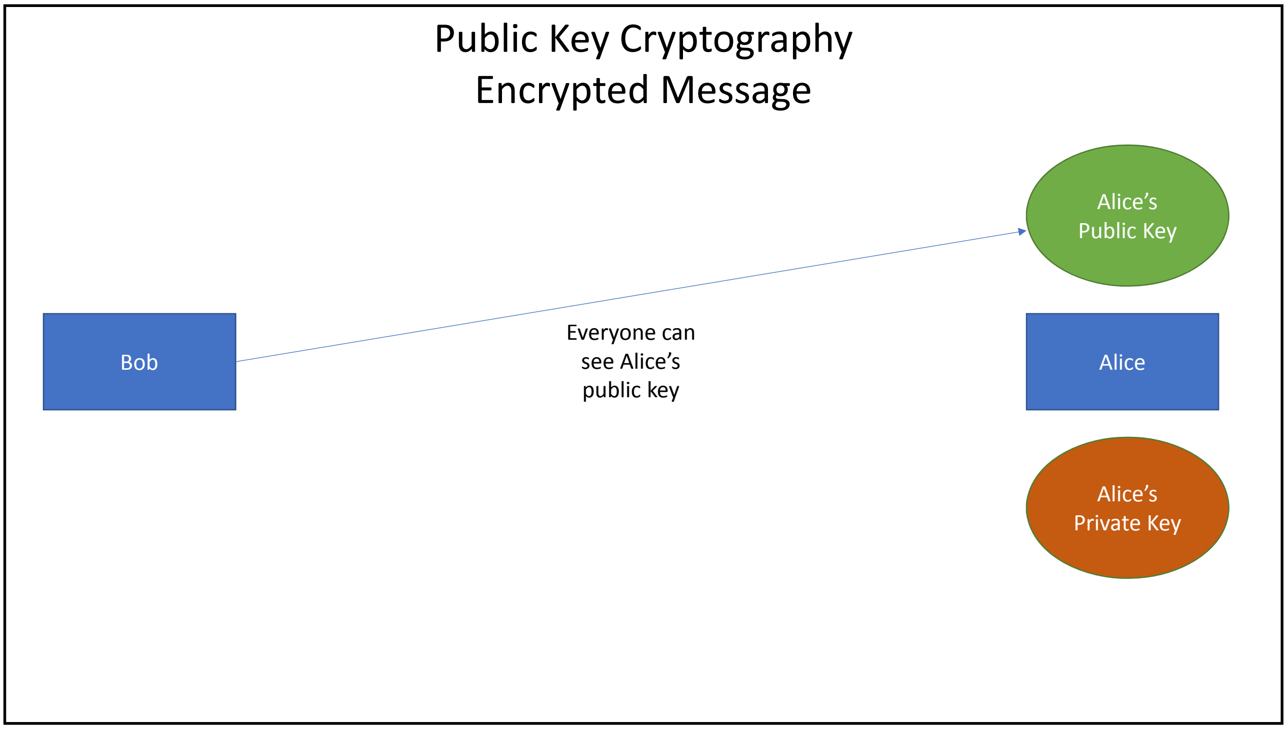
Public Key Cryptography
Encrypted Message

Alice’s
Public Key

Bob

Alice

Alice’s
Private Key



Public Key Cryptography
Encrypted Message

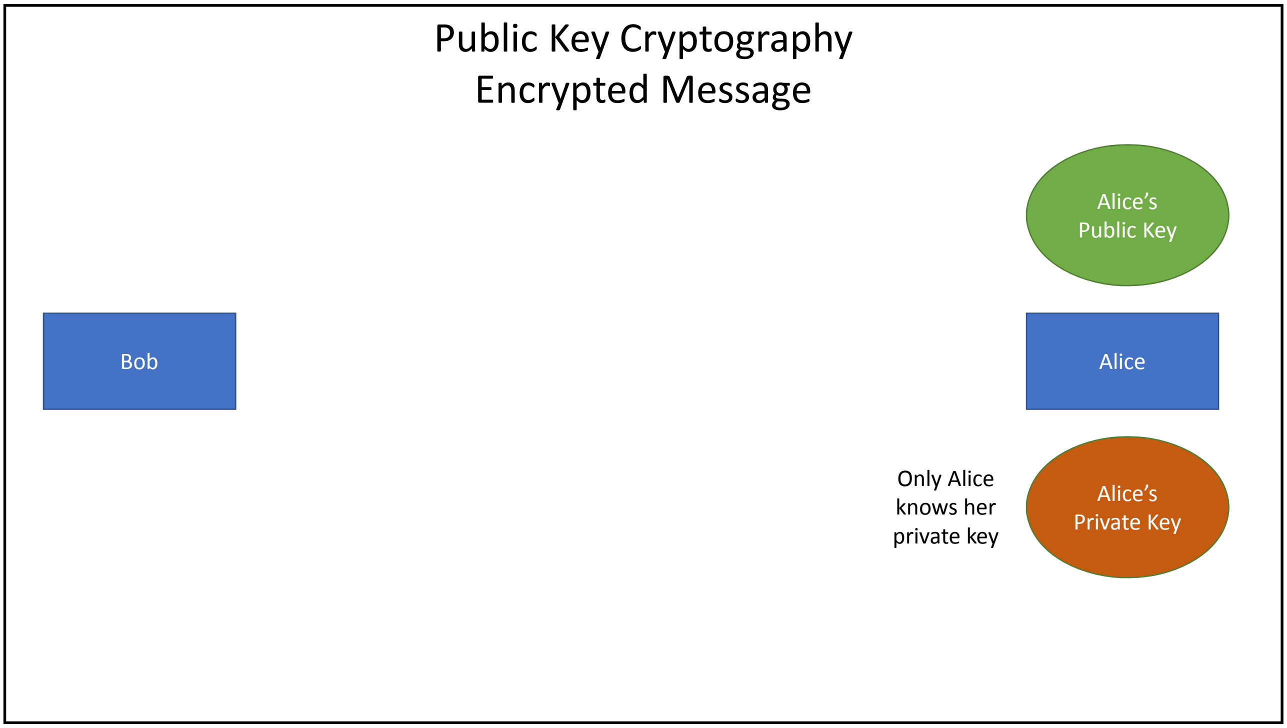
Alice’s
Public Key

Bob

Everyone can
see Alice’s
public key

Alice

Alice’s
Private Key



Public Key Cryptography
Encrypted Message

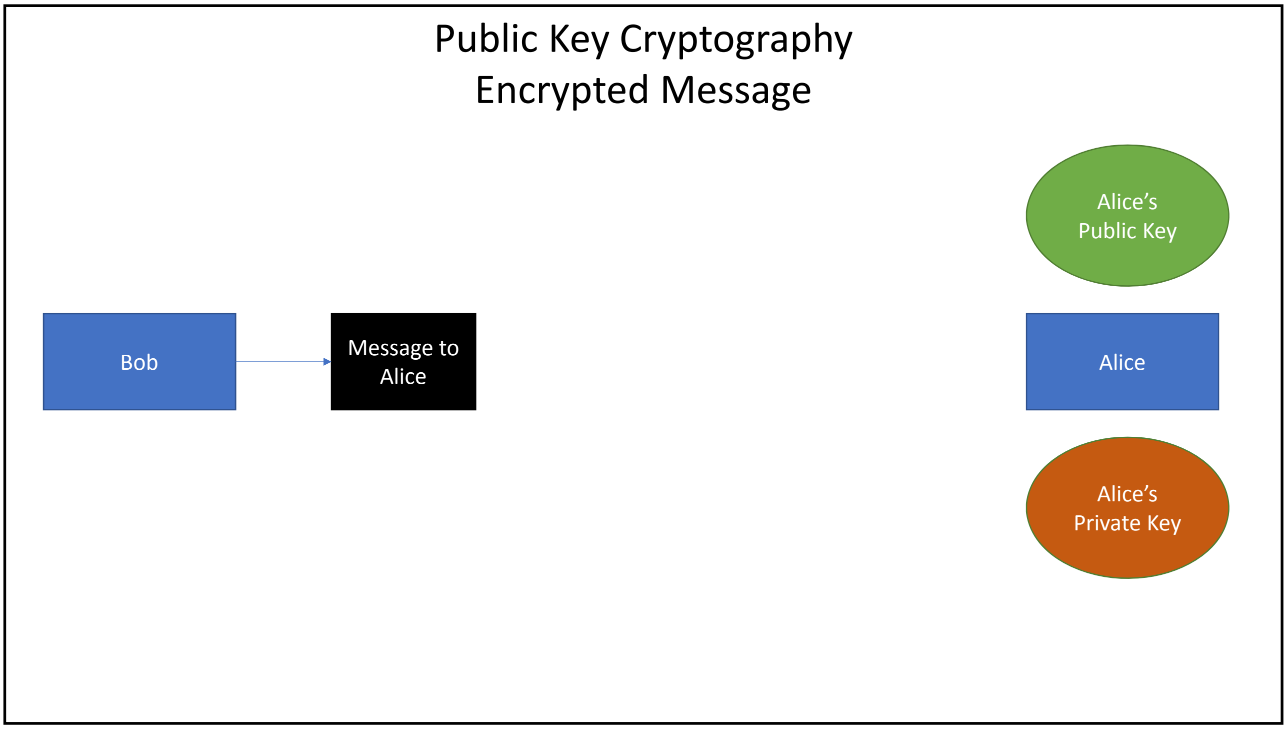
Alice's Public Key

Bob

Alice

Only Alice knows her private key

Alice's Private Key



Public Key Cryptography
Encrypted Message

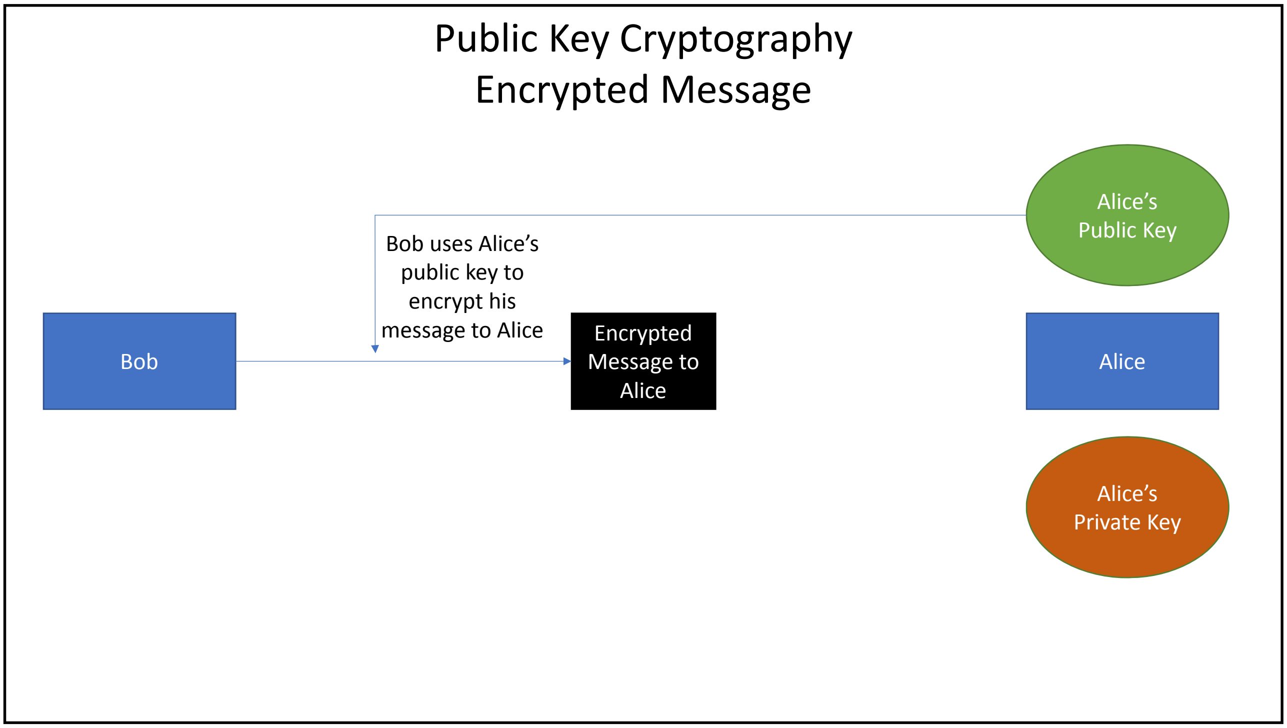
Alice's Public Key

Bob

Message to Alice

Alice

Alice's Private Key



Public Key Cryptography
Encrypted Message

Alice's
Public Key

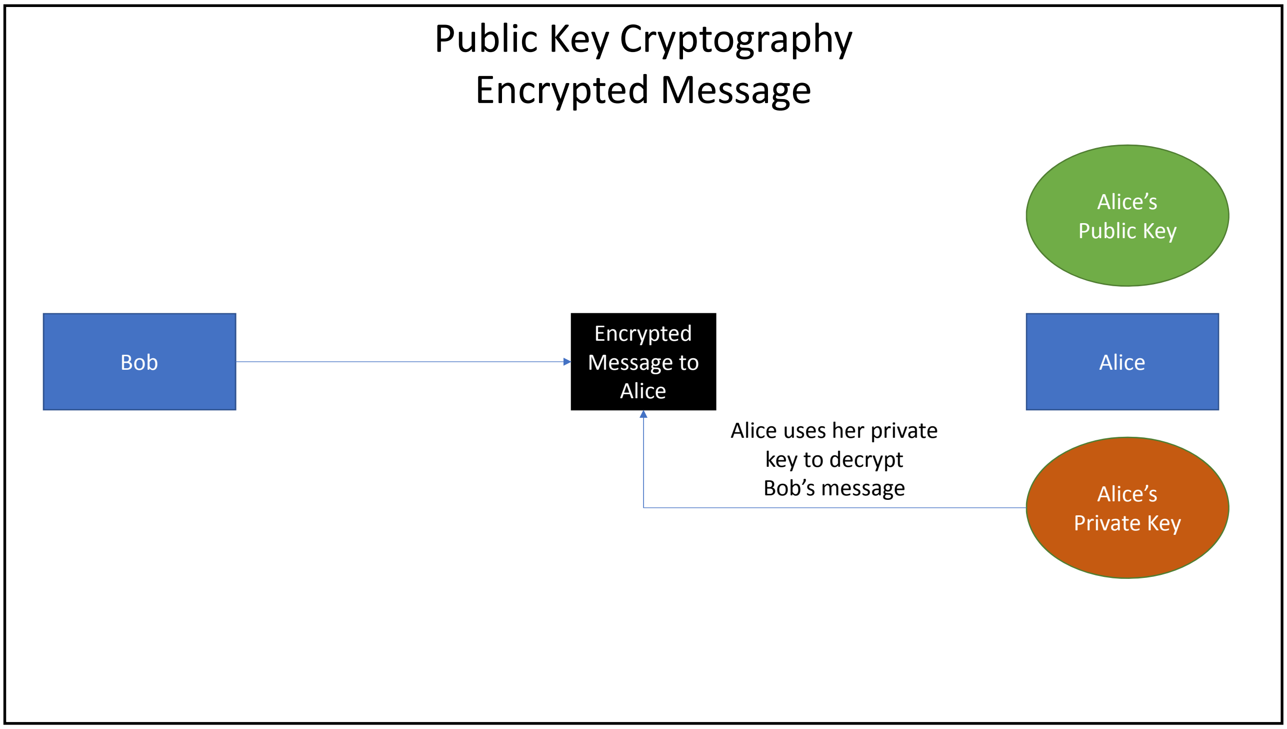
Bob uses Alice's
public key to
encrypt his
message to Alice

Bob

Encrypted
Message to
Alice

Alice

Alice's
Private Key



Public Key Cryptography
Encrypted Message

Alice's
Public Key

Bob

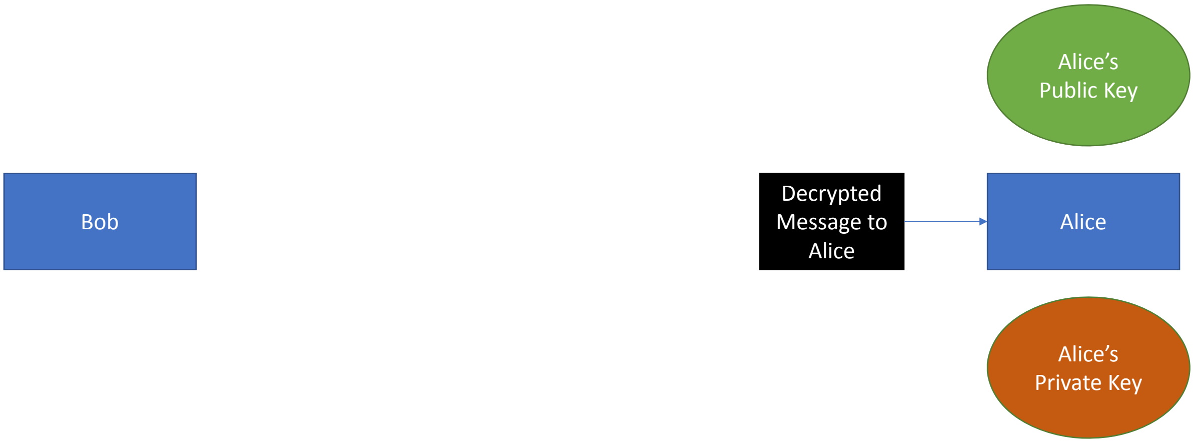
Encrypted
Message to
Alice

Alice

Alice uses her private
key to decrypt
Bob's message

Alice's
Private Key

Public Key Cryptography
Encrypted Message



Alice's
Public Key

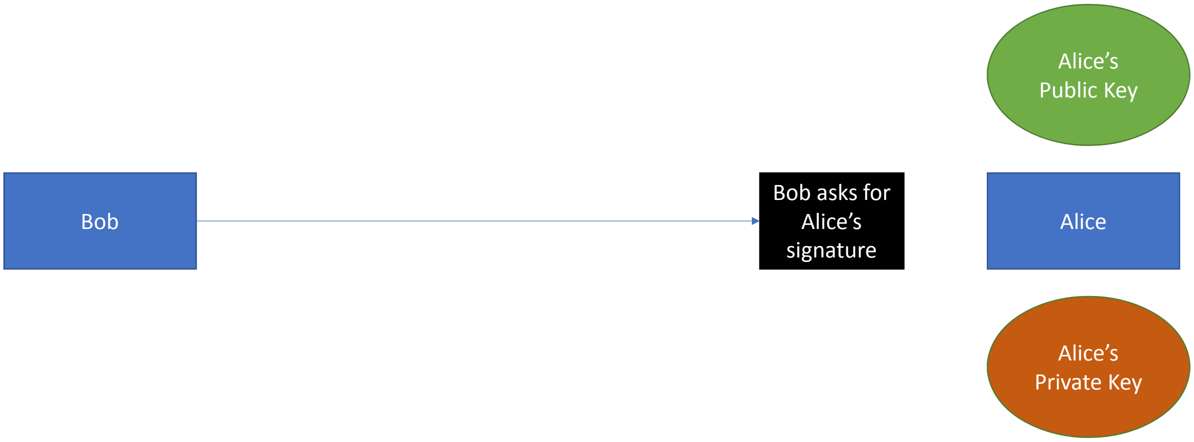
Bob

Decrypted
Message to
Alice

Alice

Alice's
Private Key

Public Key Cryptography
Digital Signature



Alice's
Public Key

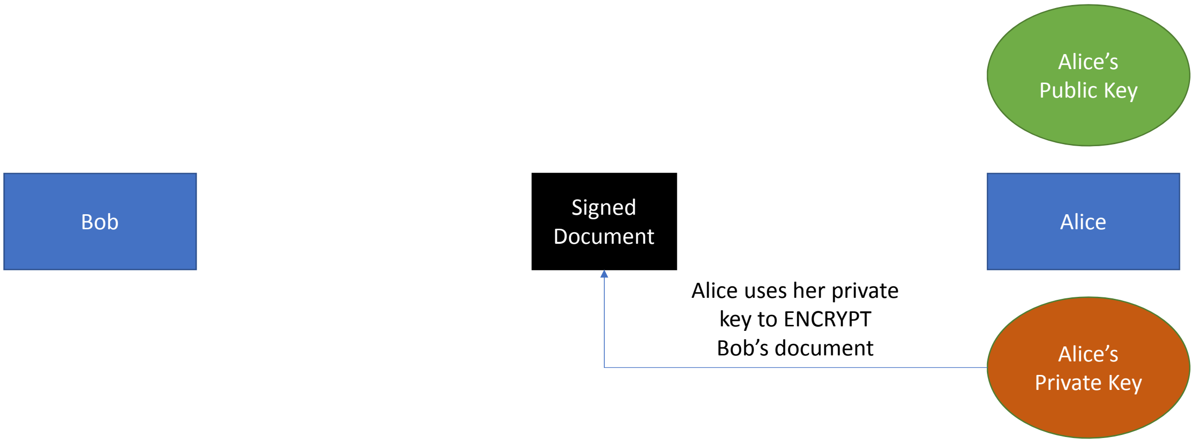
Bob

Bob asks for
Alice's
signature

Alice

Alice's
Private Key

Public Key Cryptography
Digital Signature



Alice's Public Key

Bob

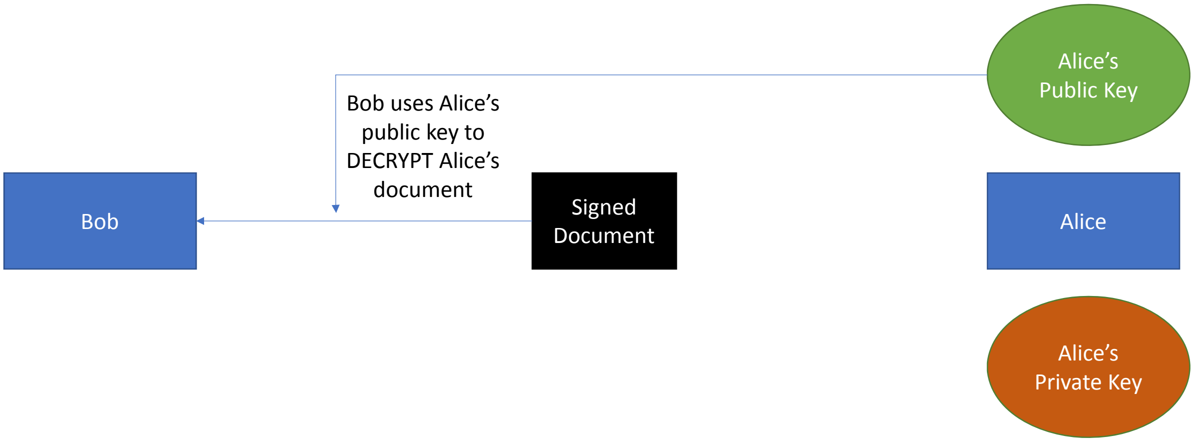
Signed Document

Alice

Alice uses her private key to ENCRYPT Bob's document

Alice's Private Key

Public Key Cryptography
Digital Signature



Alice's Public Key

Bob uses Alice's public key to DECRYPT Alice's document

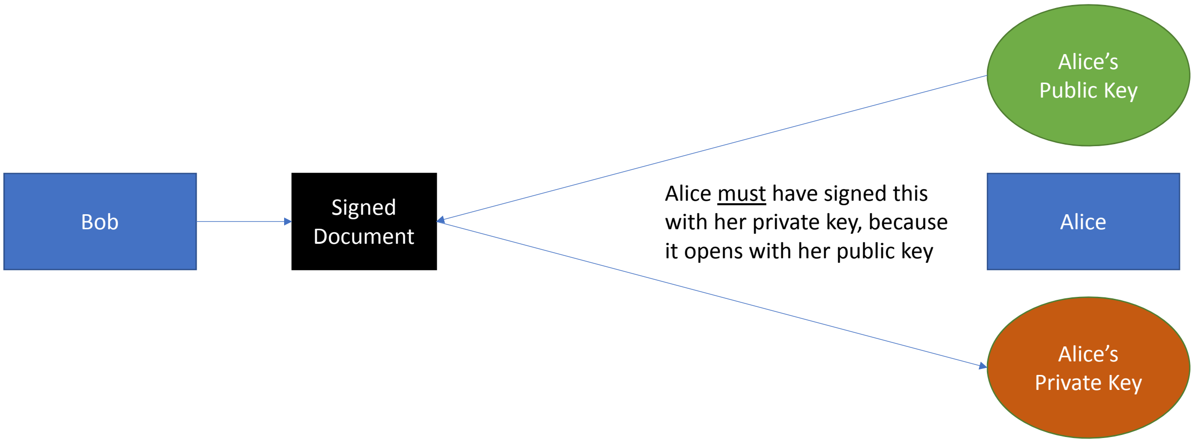
Bob

Signed Document

Alice

Alice's Private Key

Public Key Cryptography
Digital Signature



Alice's Public Key

Bob

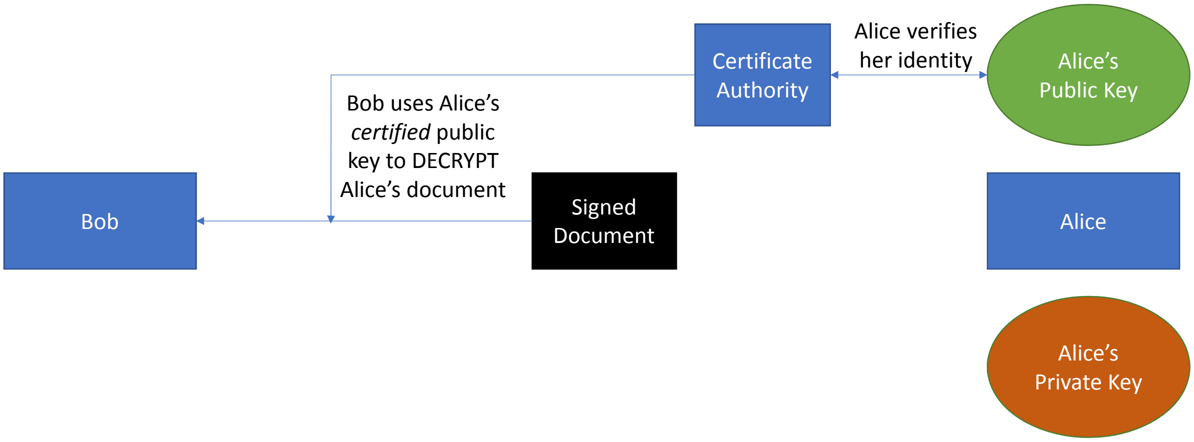
Signed Document

Alice <u>must</u> have signed this with her private key, because it opens with her public key

Alice

Alice's Private Key

Public Key Cryptography
***Verified* Digital Signature**



Certificate Authority

Alice verifies her identity

Alice's Public Key

Bob uses Alice's *certified* public key to DECRYPT Alice's document

Bob

Signed Document

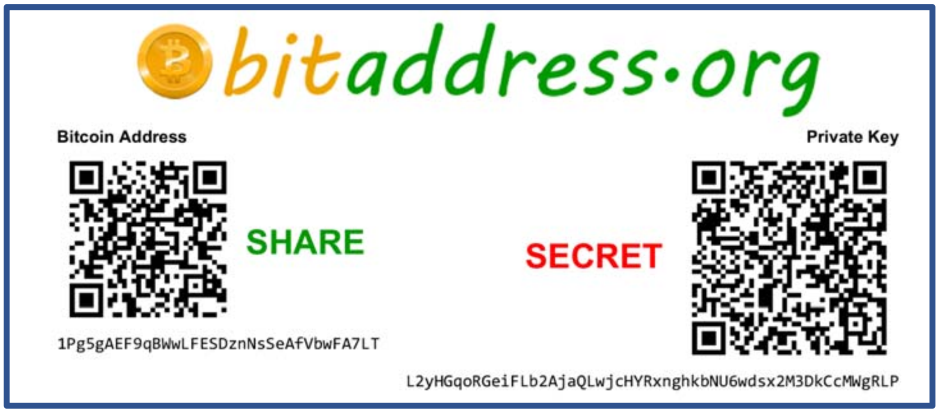
Alice

Alice's Private Key

The Essential Containers

Key Pairs and Wallets

Paper Wallet Example



Bitcoin Address

SHARE

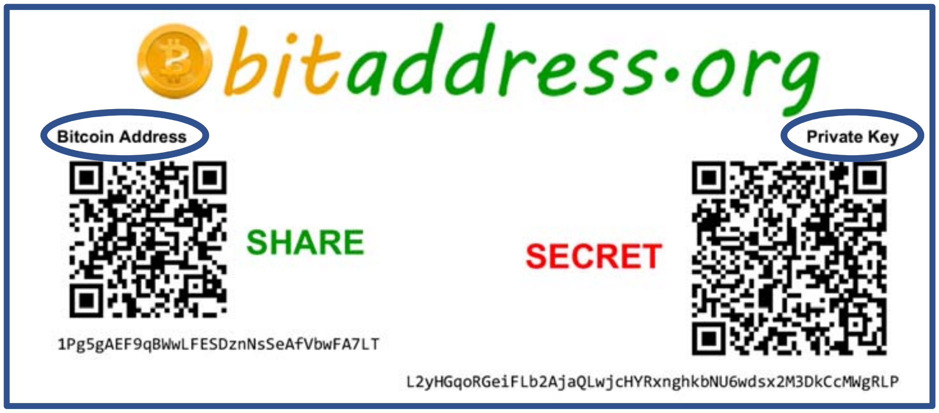
1Pg5gAEF9qBWwLFESDznNsSeAfVbwFA7LT

Private Key

SECRET

L2yHGqoRGeiFLb2AjaQLwjcHYRxnghkbNU6wdsx2M3DkCcMWgRLP

Paper Wallet Example



bitaddress.org

Bitcoin Address

SHARE

1Pg5gAEF9qBWwLFESDznNsSeAfVbwFA7LT

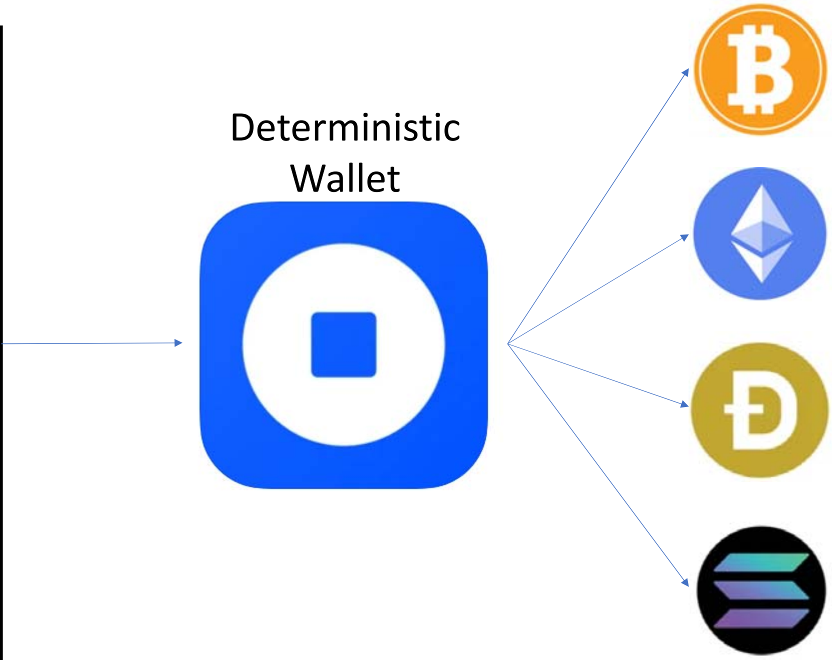
Private Key

SECRET

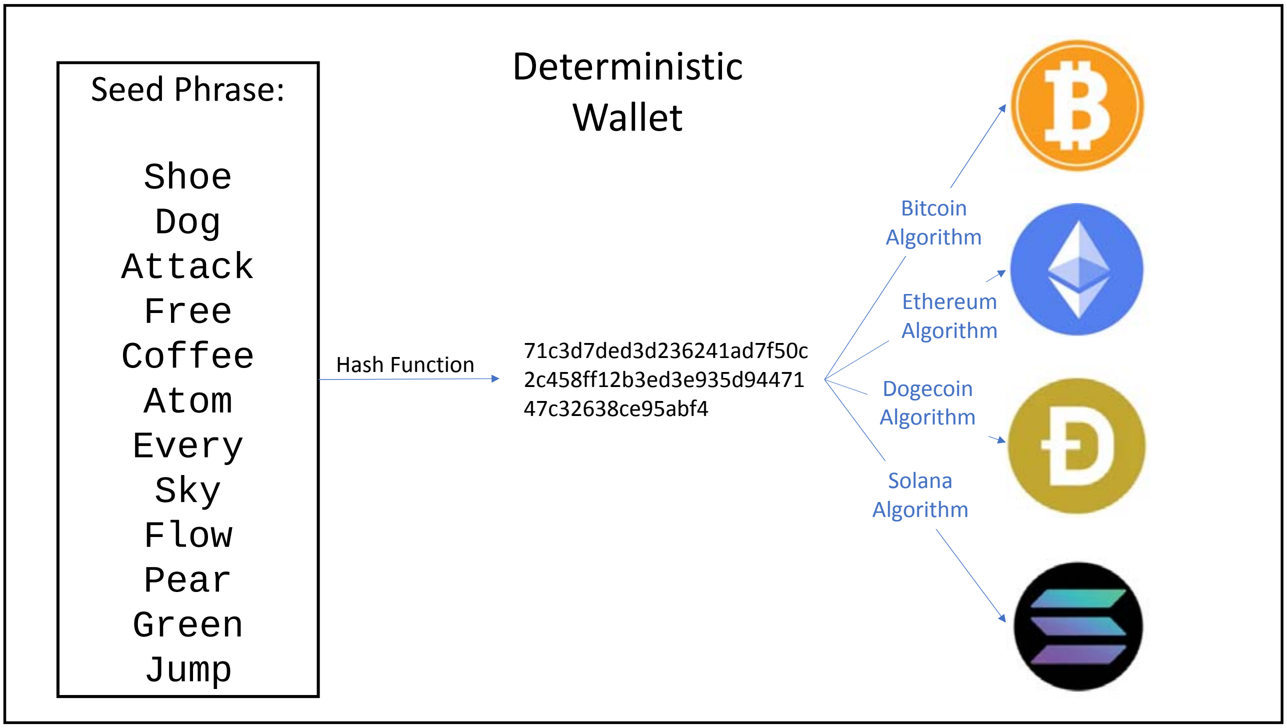
L2yHGqoRGeiFLb2AjaQLwjcHYRxnghkbNU6wdsx2M3DkCcMWgRLP

Seed Phrase:

Shoe
Dog
Attack
Free
Coffee
Atom
Every
Sky
Flow
Pear
Green
Jump



Deterministic Wallet



Deterministic Wallet

Seed Phrase:

Shoe
Dog
Attack
Free
Coffee
Atom
Every
Sky
Flow
Pear
Green
Jump

Hash Function

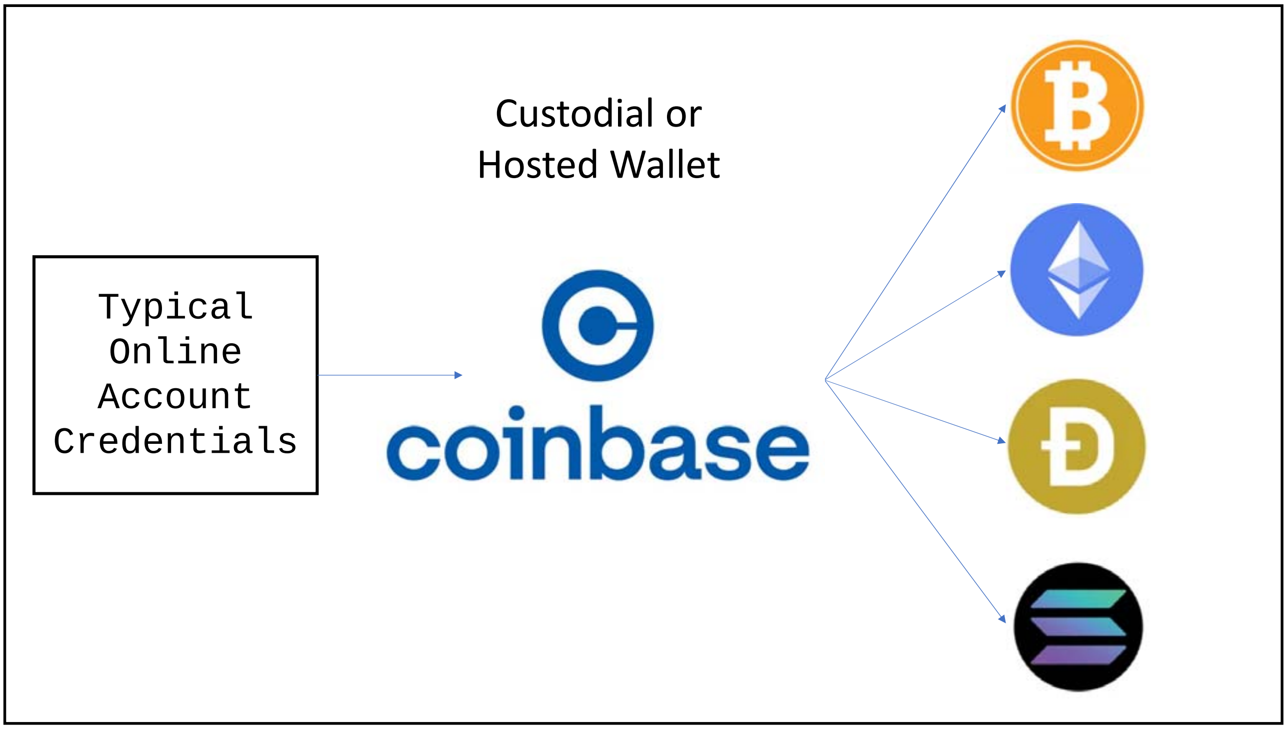
71c3d7ded3d236241ad7f50c
2c458ff12b3ed3e935d94471
47c32638ce95abf4

Bitcoin Algorithm

Ethereum Algorithm

Dogecoin Algorithm

Solana Algorithm

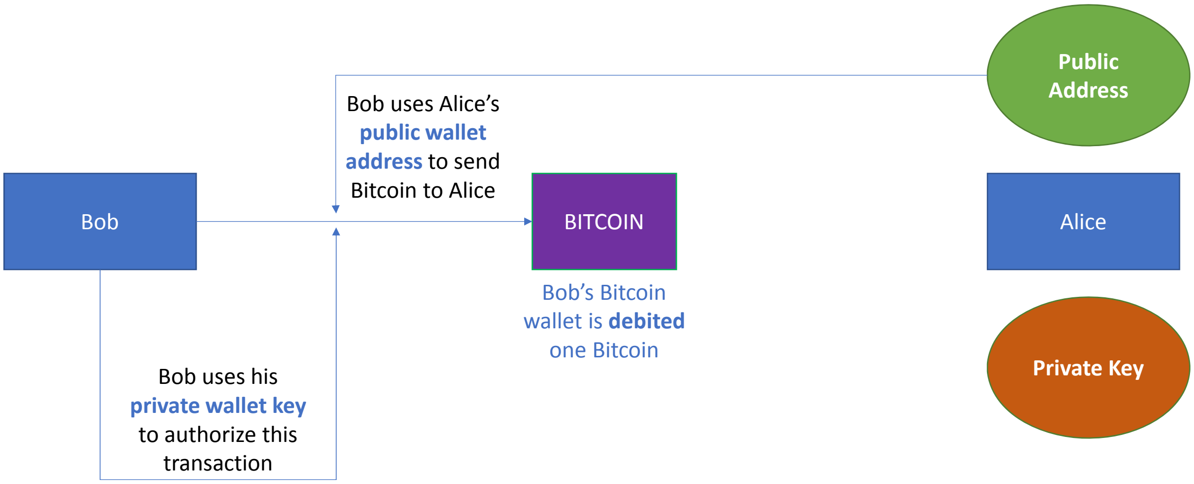


Custodial or Hosted Wallet

Typical
Online
Account
Credentials

coinbase

Bitcoin Transaction

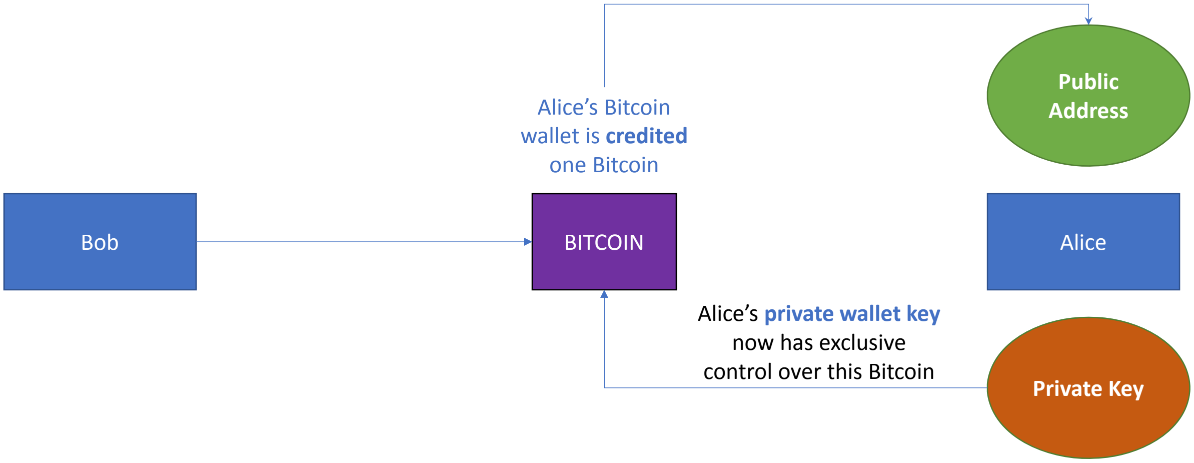


Bob uses Alice's **public wallet address** to send Bitcoin to Alice

Bob's Bitcoin wallet is **debited** one Bitcoin

Bob uses his **private wallet key** to authorize this transaction

Bitcoin Transaction



Alice's Bitcoin wallet is **credited** one Bitcoin

Alice's **private wallet key** now has exclusive control over this Bitcoin

Core Blockchain Security Features

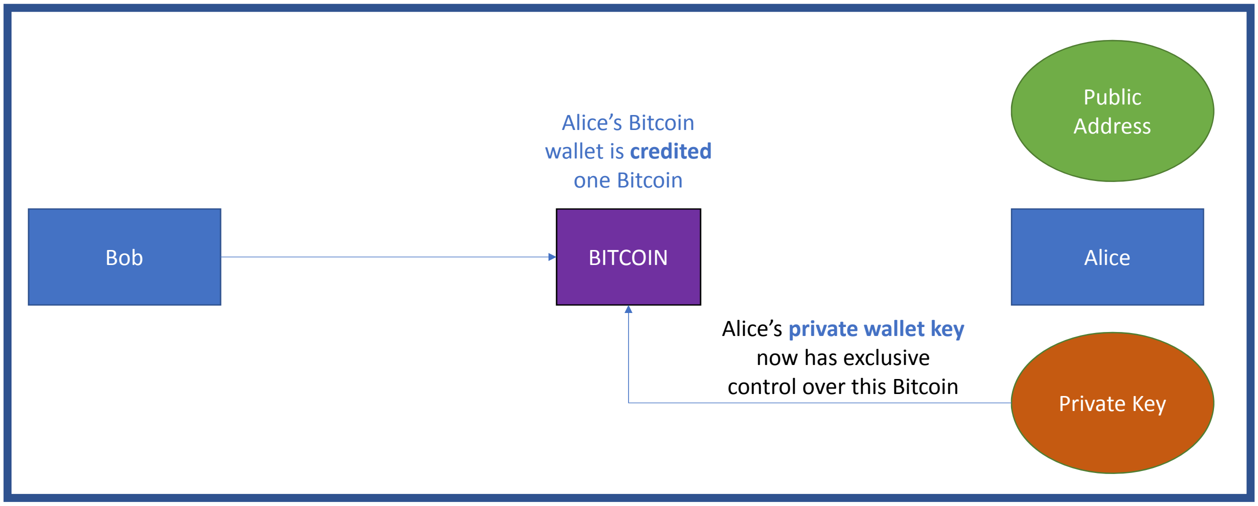
Cryptographic Links

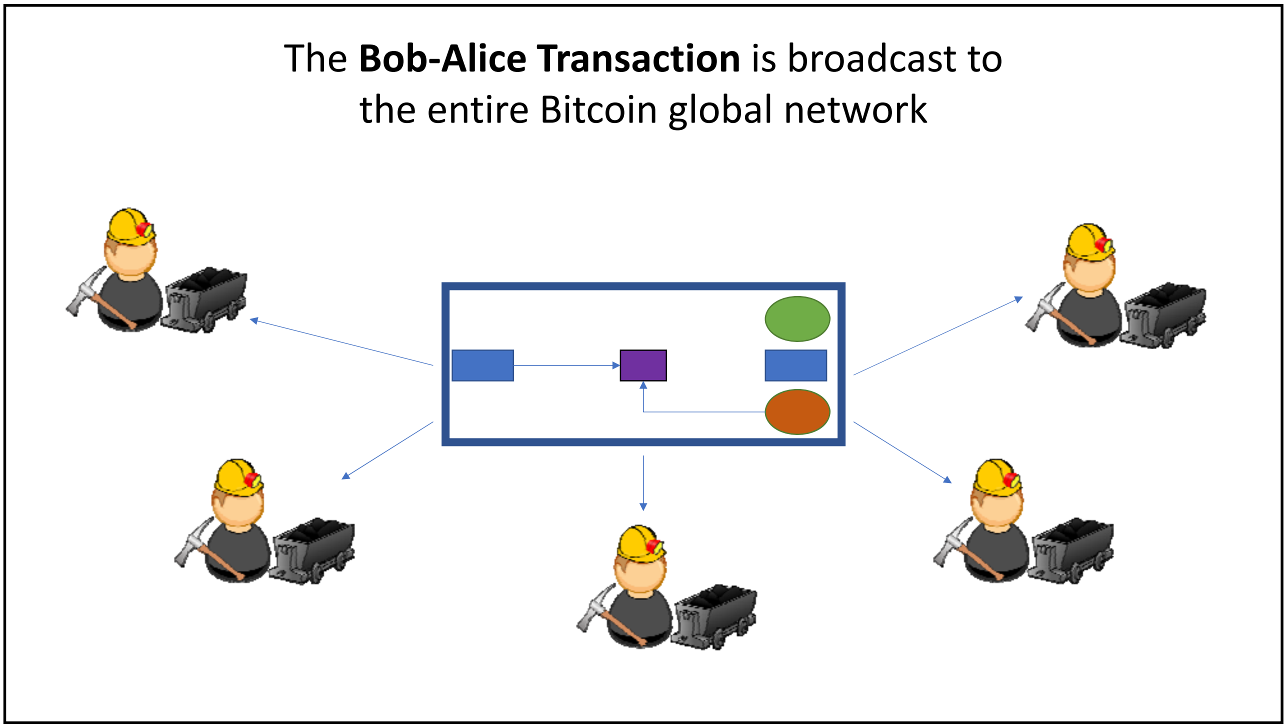
Immutability

Decentralization

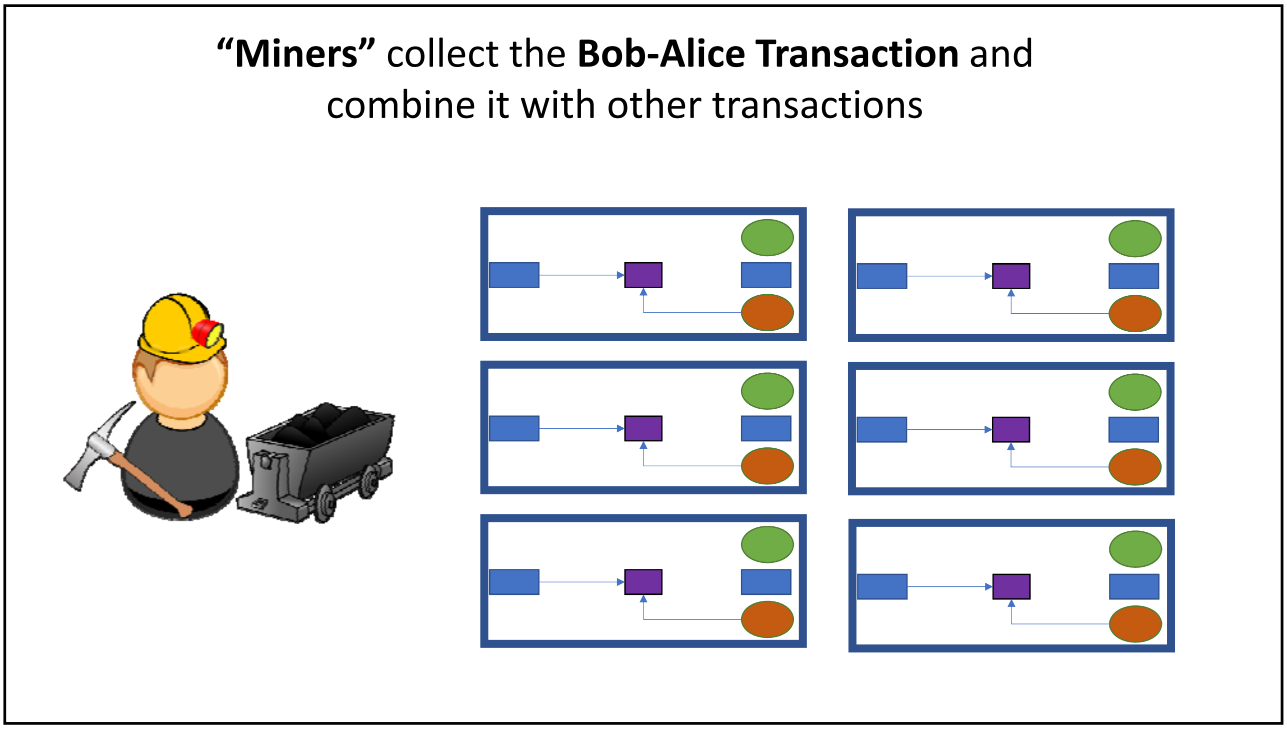
Public Key Addressing

This is a Single Bitcoin Transaction


Public Address
Alice's Bitcoin wallet is **credited** one Bitcoin
Bob
BITCOIN
Alice
Alice's **private wallet key** now has exclusive control over this Bitcoin
Private Key



The **Bob-Alice Transaction** is broadcast to the entire Bitcoin global network

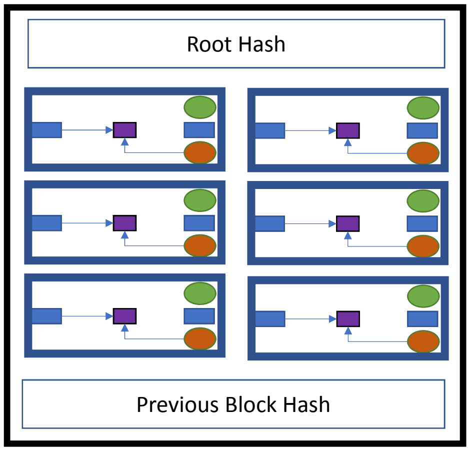


"Miners" collect the **Bob-Alice Transaction** and combine it with other transactions

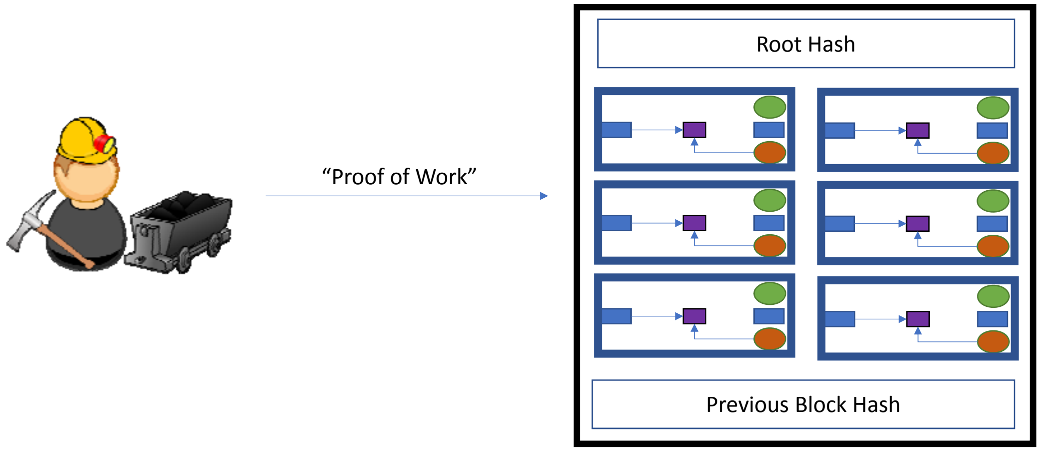
Transactions Get Summarized as a “Root Hash”

Hash of Each Transaction	Hash of Hashes	Root Hash
Transaction One Hash	*Hash of One and Two Hashes*	*Hash of (1+2) and (3+4)*
Transaction Two Hash		
Transaction Three Hash	*Hash of Three and Four Hashes*	
Transaction Four Hash		

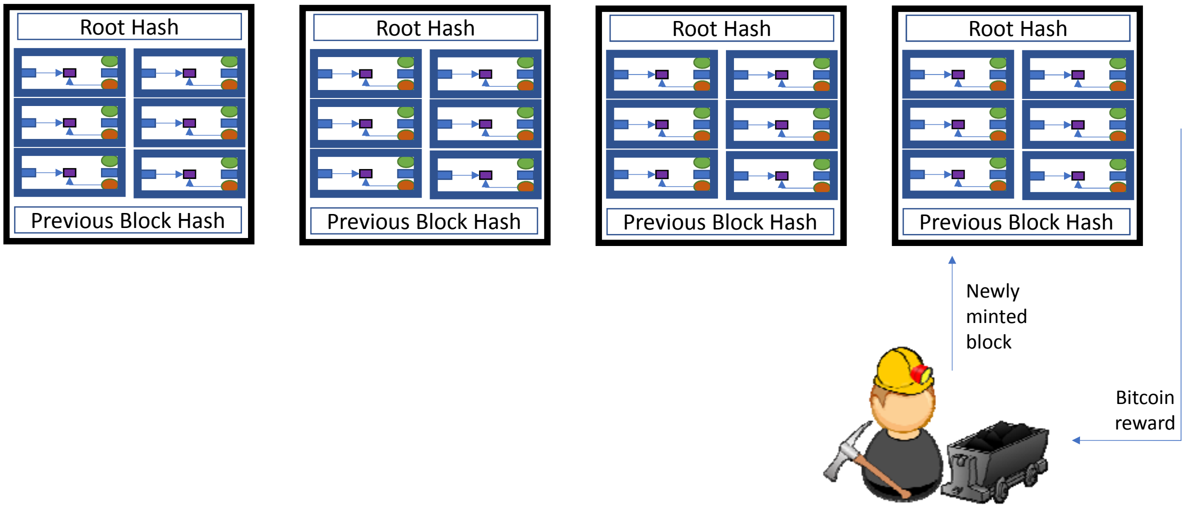
Transaction Groups Become Hashed Blocks



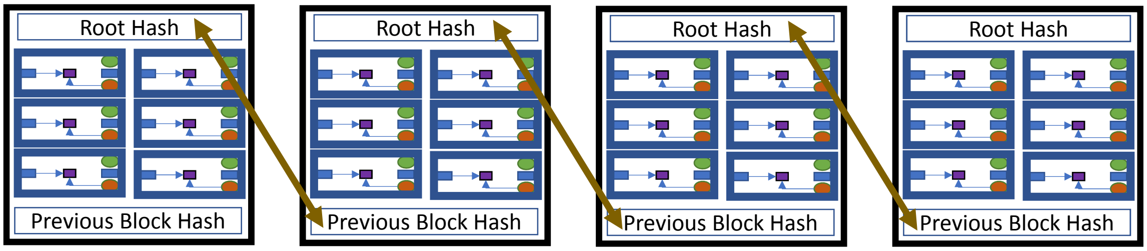
Miners then race to **validate the transactions** and satisfy a **proof of investment** requirement



The winning miner then adds his block to the chain of previous blocks and gets a reward

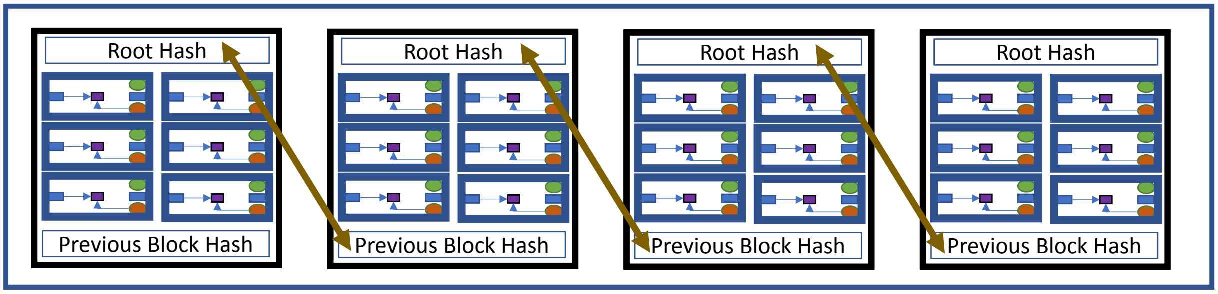


The Root Hash of All Blocks are Cryptographically Locked

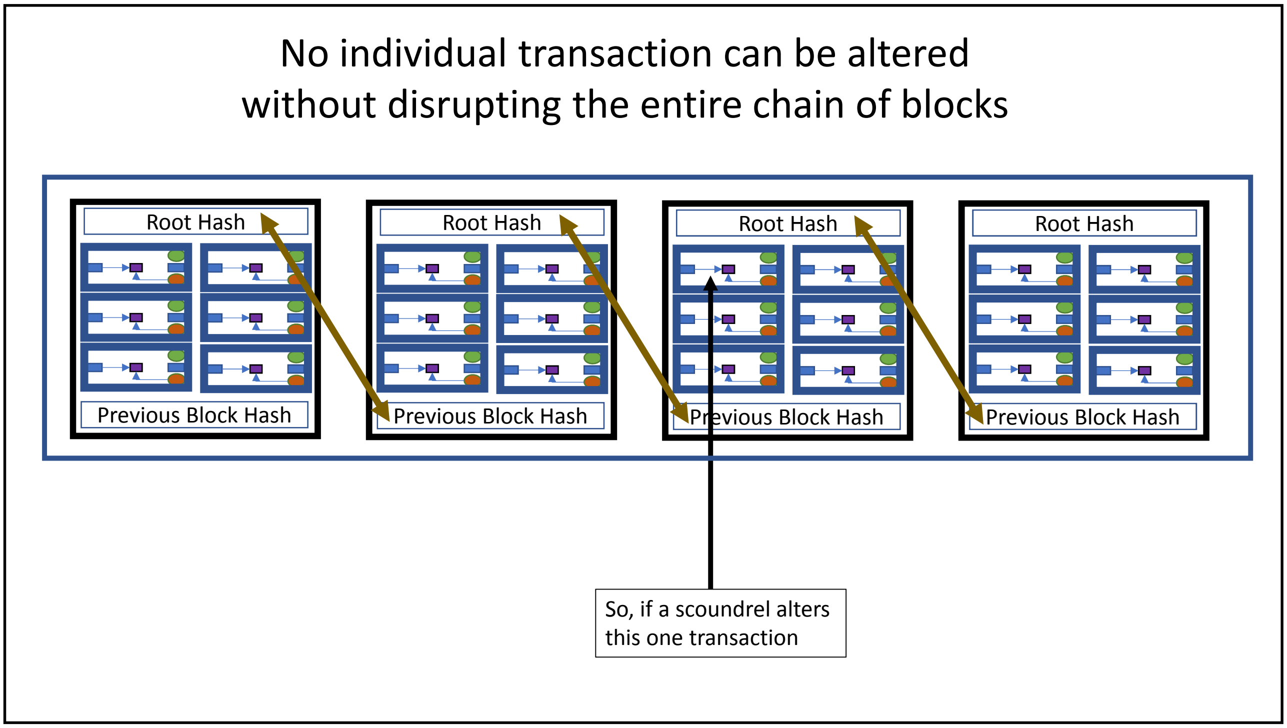


Root Hash
Previous Block Hash
Root Hash
Previous Block Hash
Root Hash
Previous Block Hash
Root Hash
Previous Block Hash

The chain of all these blocks is called the "Blockchain"

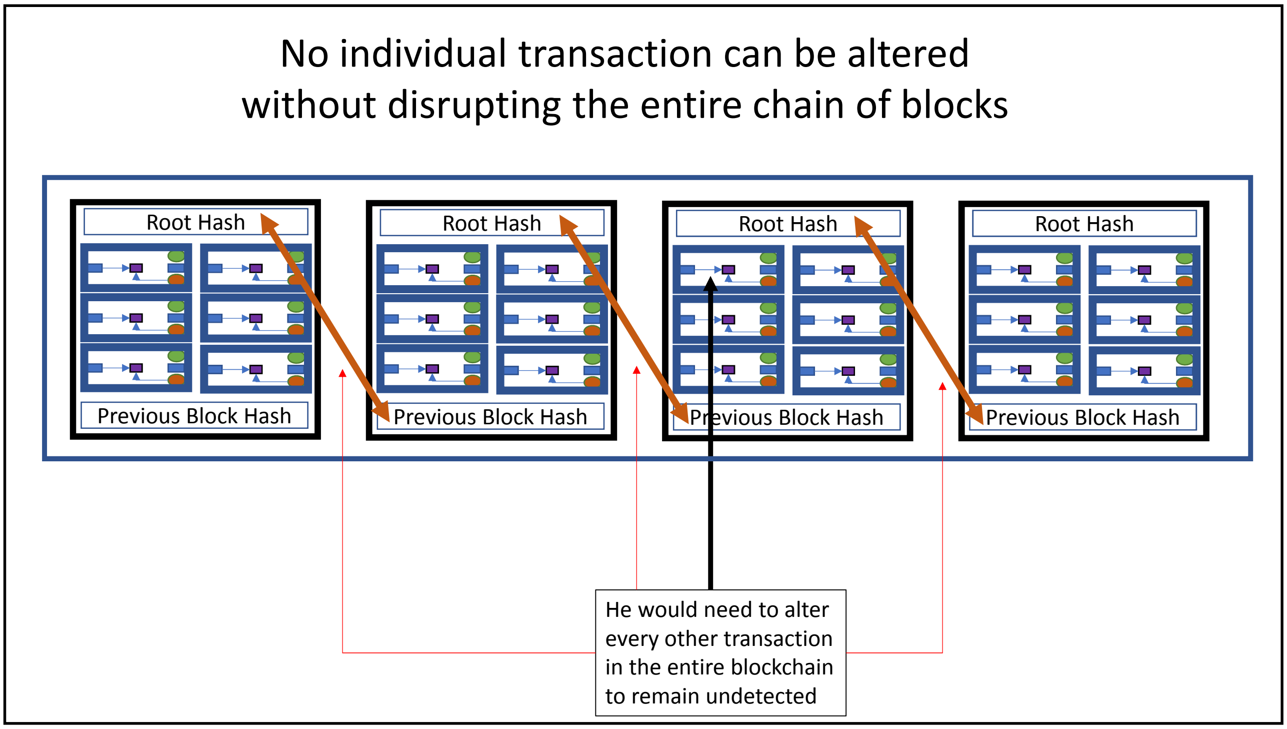


Root Hash
Previous Block Hash
Root Hash
Previous Block Hash
Root Hash
Previous Block Hash
Root Hash
Previous Block Hash



No individual transaction can be altered
without disrupting the entire chain of blocks

So, if a scoundrel alters
this one transaction



No individual transaction can be altered
without disrupting the entire chain of blocks

He would need to alter
every other transaction
in the entire blockchain
to remain undetected

Governance in Blockchain

Jeffrey M Glazer
jmglazer@ogs.law
www.ogs.law

Agenda

Protocol Tier	• ETH • BTC
Network Tier	• ERC20 • DOGE
Application Tier	• NFTs • Ripple
DAOs	

Governance

- The process of interactions through the laws, norms, power or language of an organized society over a social system (family, tribe, formal or informal organization, a territory or across territories). It is done by the government of a state, by a market, or by a network. It is the decision-making among the actors involved in a collective problem that leads to the creation, reinforcement, or reproduction of social norms and institutions

Or

- How do stakeholders within the tier negotiate disputes or resolve relevant questions amongst themselves

- On-chain v. Off-chain governance
  - On-Chain
    - Governance Tokens
    - Code/Business Rules
  - Off-Chain
    - Proposal/Discussion/Vote

Protocol Tier

- Protocol: a set of rules that governs the network of physical nodes and how they interact
- The rules define the interface of the network, interaction between the nodes/miners, incentives, kind of data, etc.
- Examples
  - Bitcoin/ETH/XRP
  - Hyperledger (IBM)/Azure Blockchain (Microsoft)
  - Most coins/currencies/NFTs/blockchain is some variant of Bitcoin or Ethereum; a lot of corporate development is done on Hyperledger or Azure

- Norms tend to be automated and decentralized (on-chain)
  - BTC: proof of work, syntax, data structures, resource usage limits, sanity checks, time locking, reconciliation with the memory pool and main branch, the coinbase reward and fee calculation, and block header verification.

- Decision-making tends to be manual and centralized (off-chain or hybrid)
  - BTC/ETH = open-source, but only changes approved through peer-review (bitcoin-dev email list, white paper, or Bitcoin Improvement Proposal) are accepted into protocol layer

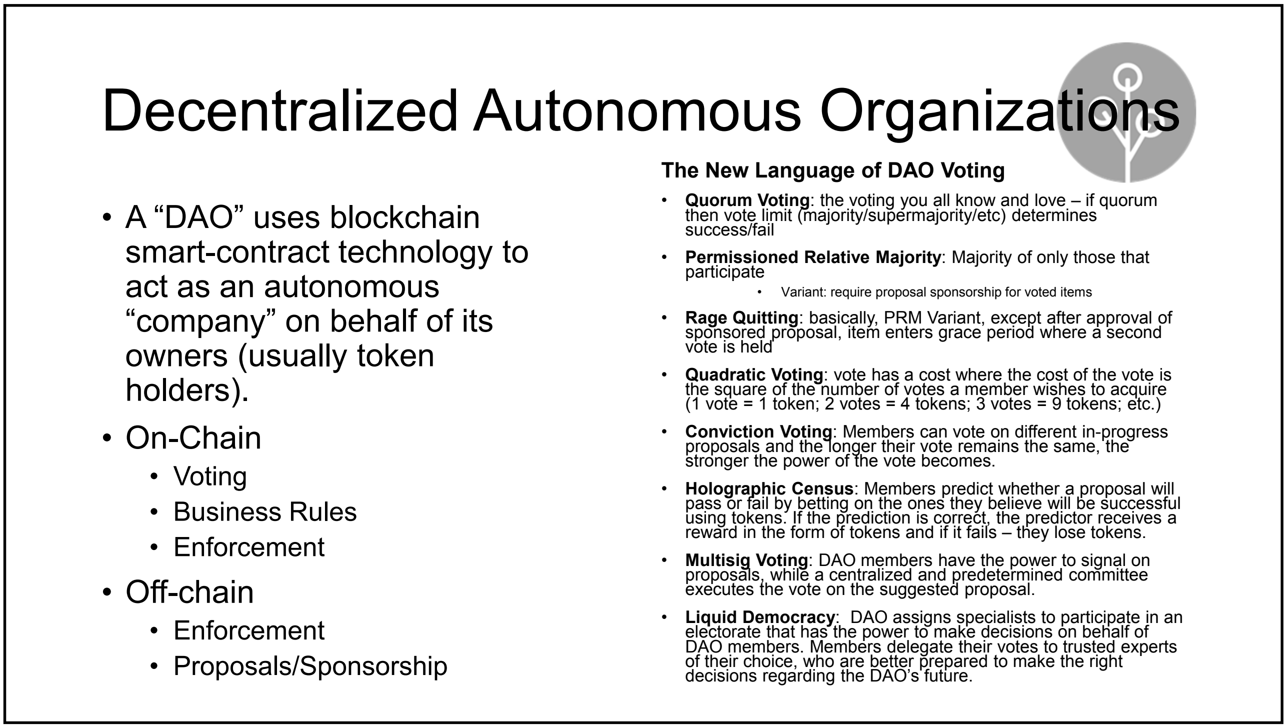
- Kinds of issues
  - Security (consensus)
    - ETH recently changed Security from Proof of Work -> Proof of Stake
  - Decentralization (node architecture)
  - Consistency (ledger replication)
  - Scalability

Network/Token Tier

- Network: any of the variant "coins" that are based on BTC or ETH (or others); often networks within a protocol rely on the shared protocol for security purposes*
- Tokens: A digital representation
- Examples:
  - Doge-coin (a network variant of BTC)
  - ERC-20 (the ETH token)
- On-chain: Usually adopt the business rules of the protocol and then may add specialized rules or functionality for network differentiation
  - Rules: Doge uses a different hashing encryption mechanism that is faster, but simpler (and lower energy) than BTC
- Functionality: Utility Tokens
  - Governance Tokens

Application Tier

- Applications: services that run on the Protocol and Network to individual users
- Examples
  - Bored Ape Yacht Club
  - Ripple
  - Decentralized Autonomous Organizations
- Hybrid
  - On-Chain: Governance Tokens
  - Off-Chain: Contracts or Underlying Organizational Structure (DAOs, LLCs, etc)



Decentralized Autonomous Organizations

- A “DAO” uses blockchain smart-contract technology to act as an autonomous “company” on behalf of its owners (usually token holders).
- On-Chain
  - Voting
  - Business Rules
  - Enforcement
- Off-chain
  - Enforcement
  - Proposals/Sponsorship

The New Language of DAO Voting

- **Quorum Voting**: the voting you all know and love – if quorum then vote limit (majority/supermajority/etc) determines success/fail
- **Permissioned Relative Majority**: Majority of only those that participate
  - Variant: require proposal sponsorship for voted items
- **Rage Quitting**: basically, PRM Variant, except after approval of sponsored proposal, item enters grace period where a second vote is held
- **Quadratic Voting**: vote has a cost where the cost of the vote is the square of the number of votes a member wishes to acquire (1 vote = 1 token; 2 votes = 4 tokens; 3 votes = 9 tokens; etc.)
- **Conviction Voting**: Members can vote on different in-progress proposals and the longer their vote remains the same, the stronger the power of the vote becomes.
- **Holographic Census**: Members predict whether a proposal will pass or fail by betting on the ones they believe will be successful using tokens. If the prediction is correct, the predictor receives a reward in the form of tokens and if it fails – they lose tokens.
- **Multisig Voting**: DAO members have the power to signal on proposals, while a centralized and predetermined committee executes the vote on the suggested proposal.
- **Liquid Democracy**: DAO assigns specialists to participate in an electorate that has the power to make decisions on behalf of DAO members. Members delegate their votes to trusted experts of their choice, who are better prepared to make the right decisions regarding the DAO’s future.