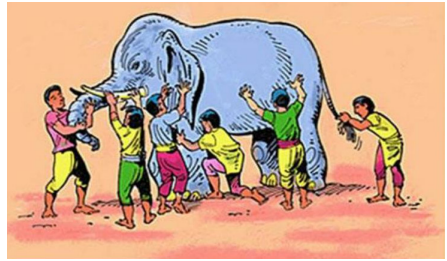
Intro to Blockchain

Bo Waggoner, CU Boulder

IAFCI Rocky Mountain Crypto Forum, Jan. 27, 2026



Intro to Blockchain: Goals

Mental model $\Longrightarrow$ **Shared, secure cloud computer**

Some nuts and bolts $\Longrightarrow$ **How do they work?**

Uses and industry $\Longrightarrow$ **How are they used today?**

Agenda:

Part 1: What's a blockchain? (50 min)

Pause (5 min)

Part 2: Nuts and bolts (30 min)

Pause (5 min)

Part 3: The industry (20 min)

Q&A (10 min)

Part 1: What's a blockchain?

- Mental model: "shared, secure cloud computers"
- Applications: cryptocurrency, stablecoins, NFTs, ...

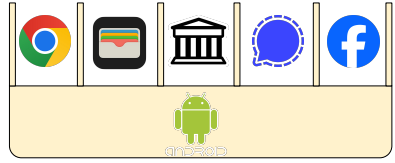
What is a computer? (phone, etc)

What is a computer? (phone, etc)

User

Apps

Operating System



Hardware

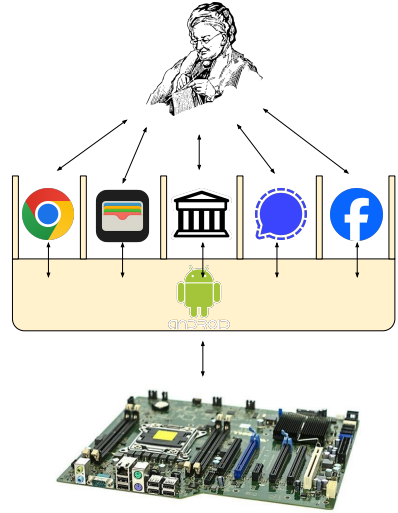
What is a computer? (phone, etc)

User

Apps

Operating System

Hardware



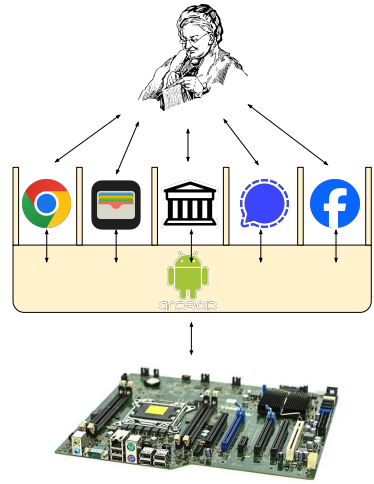
What is a computer? (phone, etc)

User

Apps

Enforces security rules on apps → Operating System

Hardware

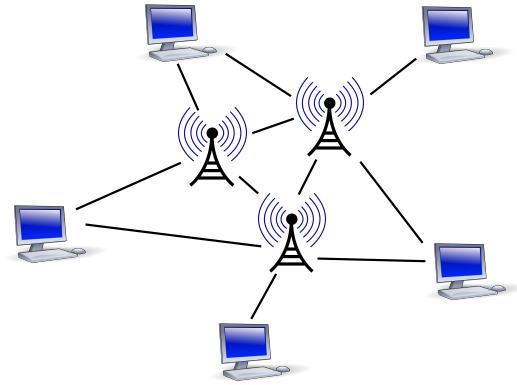


What is the Internet?

What is the Internet?

A hardware network allowing communication protocols on top.

Protocols: webpages (http/https), email (imap/smtp/pop3), ftp, vpn, voip, video streaming, apps, ...

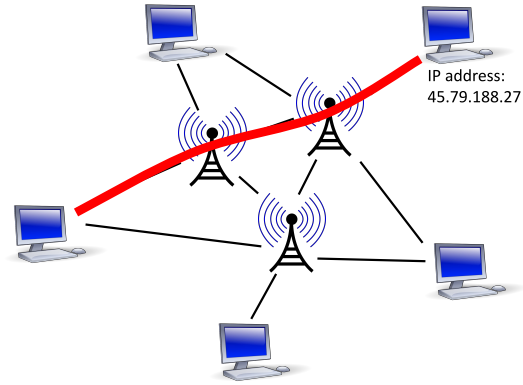


What is the Internet?

A hardware network allowing communication protocols on top.

Protocols: webpages (http/https), email (imap/smtp/pop3), ftp, vpn, voip, video streaming, apps, ...

Generally encrypted: routers see source/destination, not content



What is “the cloud”?

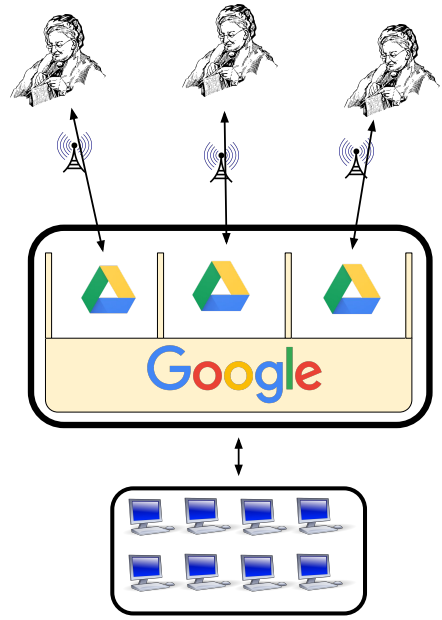
What is "the cloud"?

Users

Apps and accounts

Cloud provider

Hardware



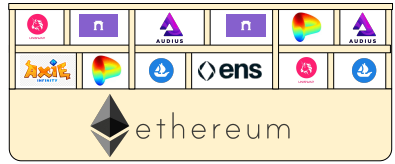
What is a blockchain (functionally)?

What is a blockchain (functionally)?

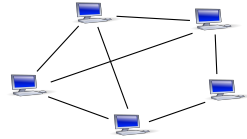
Users

Apps and accounts

“Virtual machine”



Network of nodes



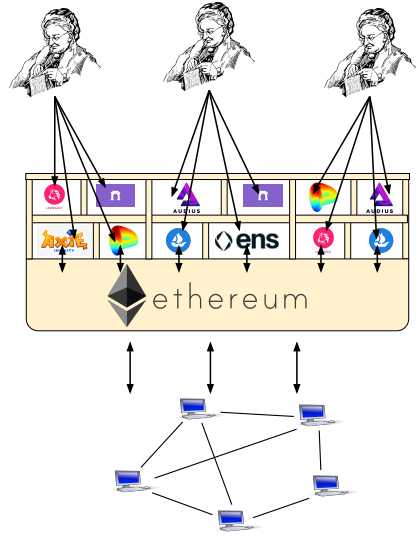
What is a blockchain (functionally)?

Users

Apps and accounts

“Virtual machine”

Network of nodes



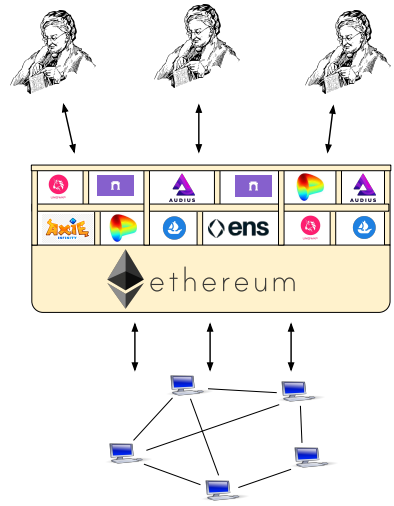
What is a blockchain (functionally)?

Use cryptographic keys to access → **Users**

Can be deployed by anyone → **Apps and accounts**

Enforces access rules → **“Virtual machine”**

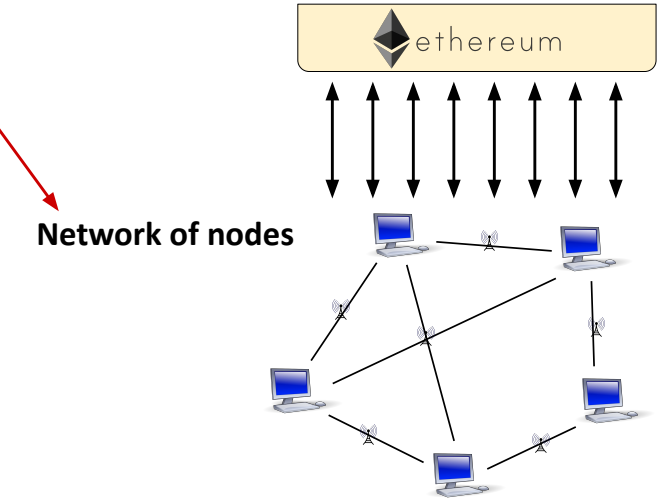
Can be anyone; incentives to particpate → **Network of nodes**



More about the “nodes”

More about the “nodes”

Can be anyone;
incentives to particpate

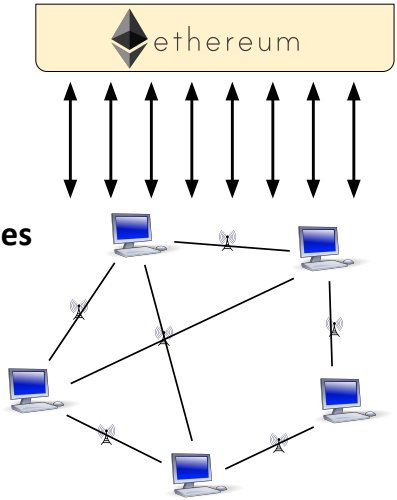


More about the "nodes"

Can be anyone; incentives to particpate

Each maintain a copy of the "virtual machine" state

Network of nodes



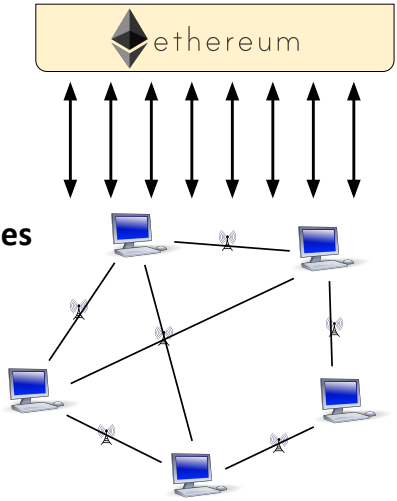
More about the "nodes"

Can be anyone;
incentives to particpate

Each maintain a copy of the
"virtual machine" state

Listen for requested updates
from users over the Internet

Network of nodes



More about the "nodes"

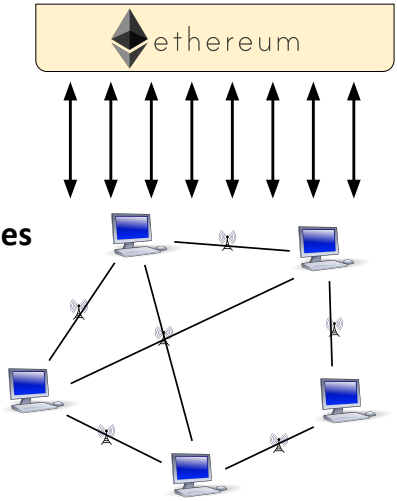
Can be anyone;
incentives to particpate

Each maintain a copy of the
"virtual machine" state

Listen for requested updates
from users over the Internet

Agree on a new set of
updates (a "block")

Network of nodes



More about the "nodes"

Can be anyone;
incentives to particpate

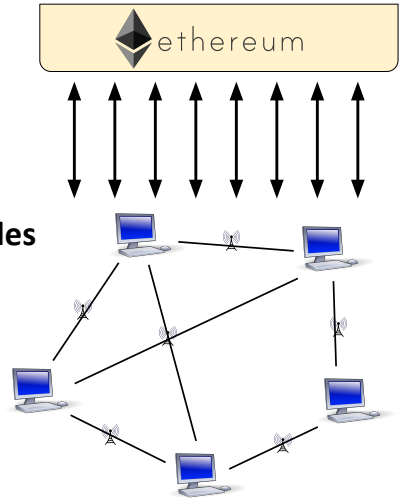
Each maintain a copy of the
"virtual machine" state

Listen for requested updates
from users over the Internet

Agree on a new set of
updates (a "block")

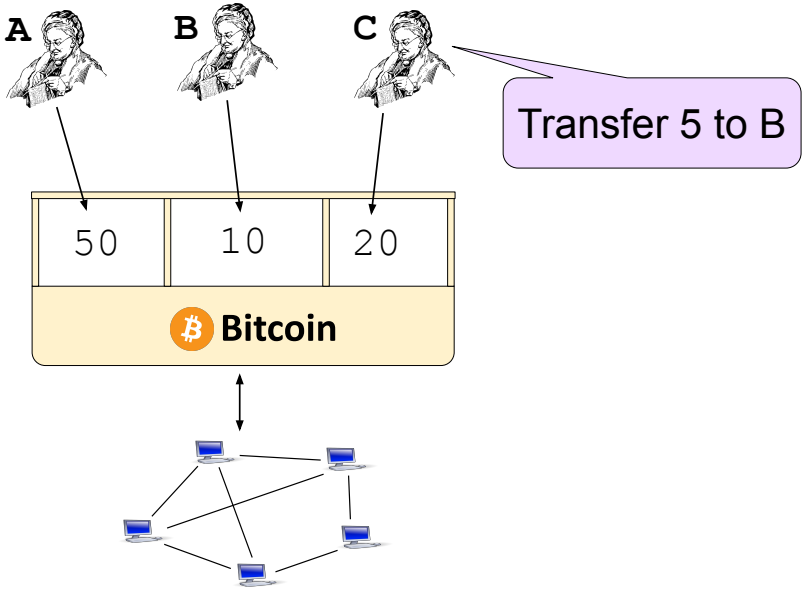
Apply the update to their
copy of the virtual machine

Network of nodes

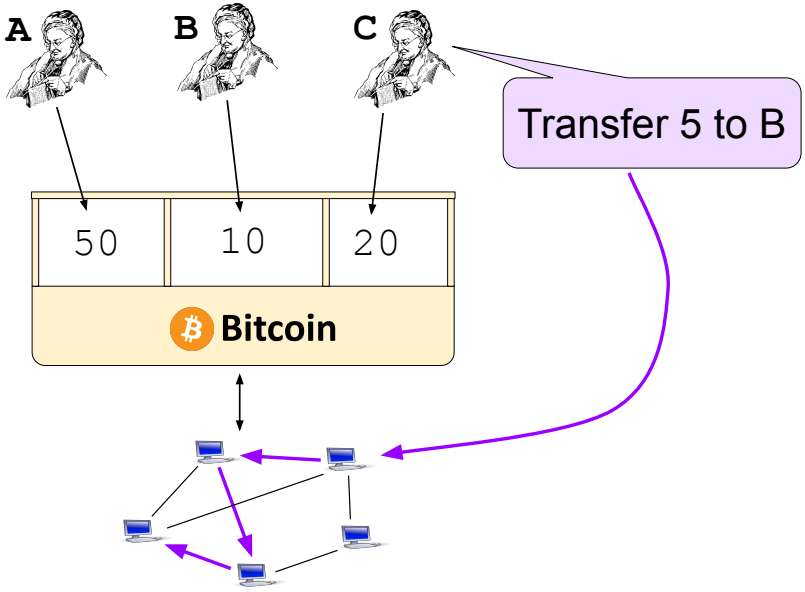


Example: Bitcoin

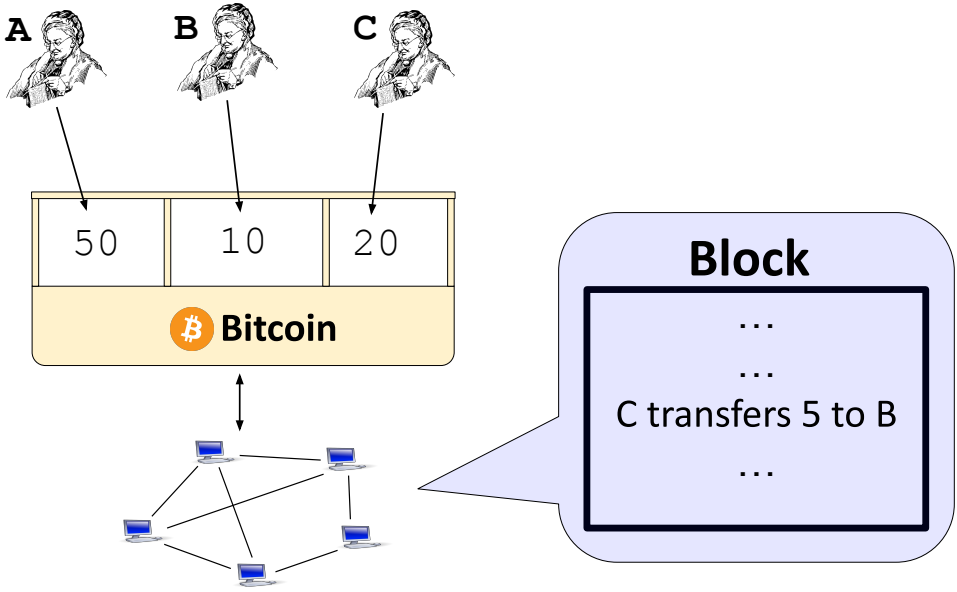
Example: Bitcoin



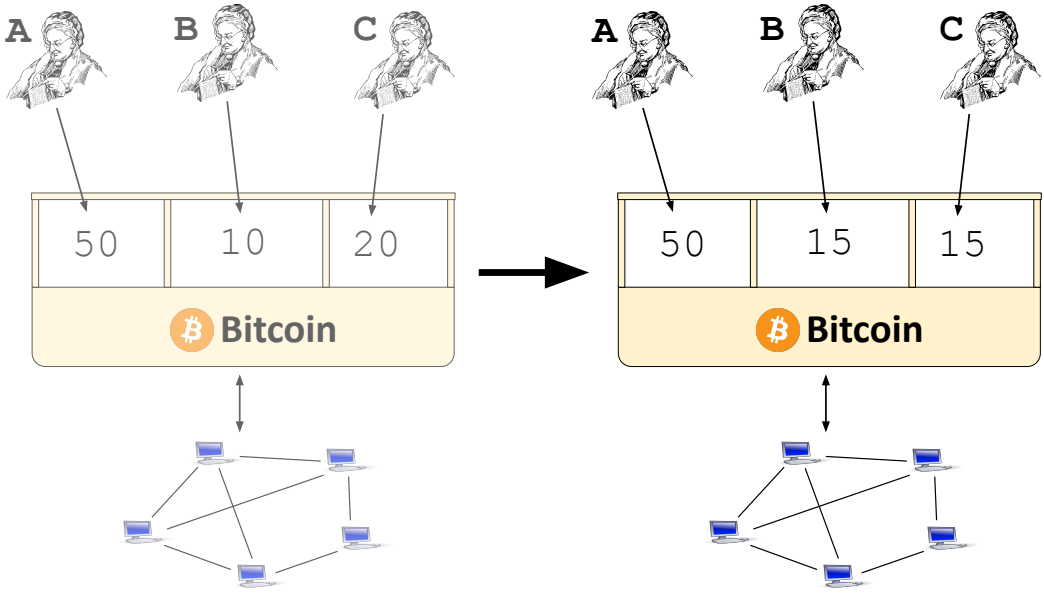
Example: Bitcoin



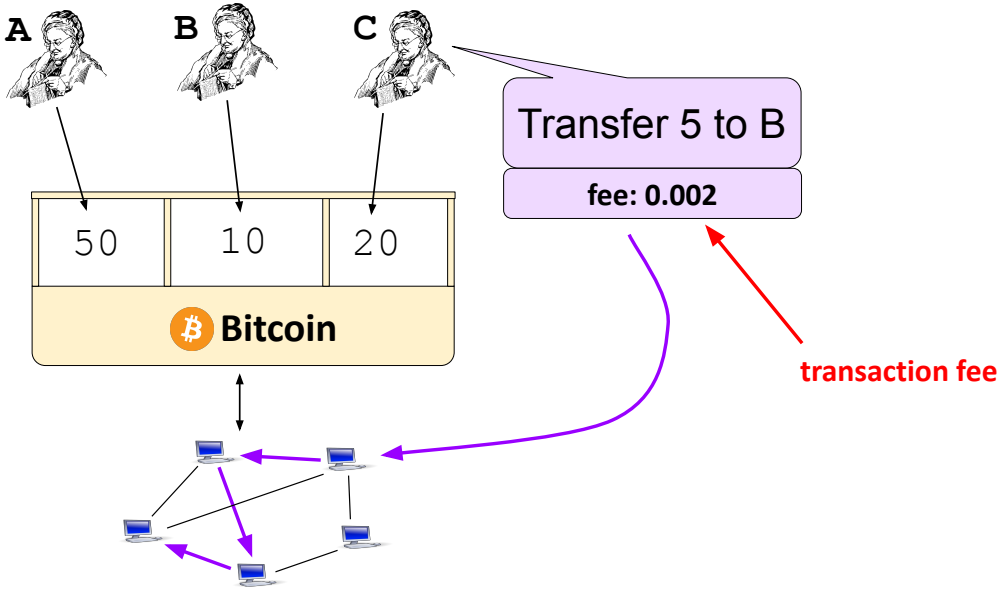
Example: Bitcoin



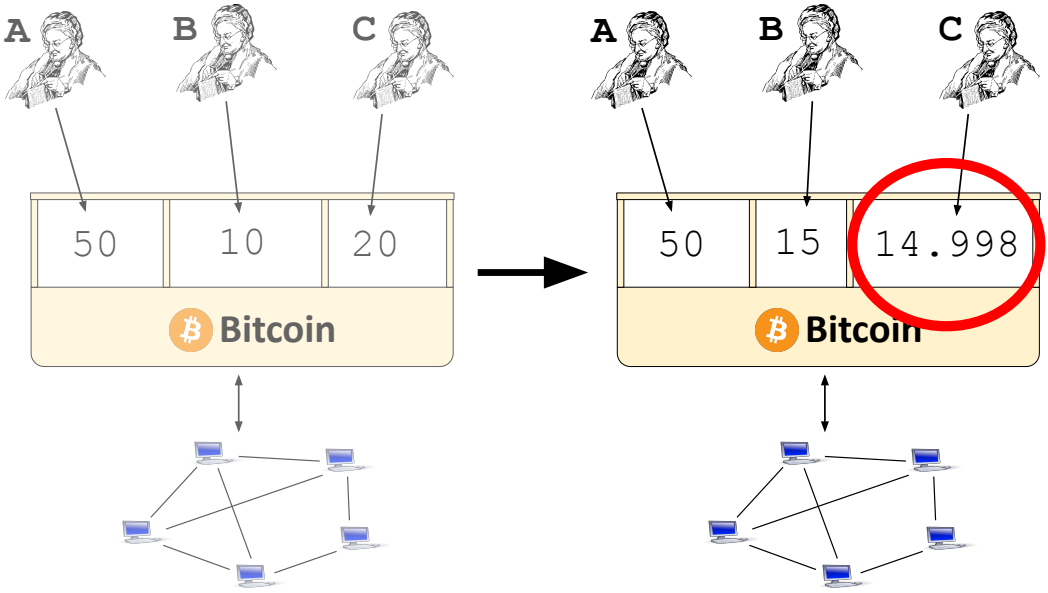
Example: Bitcoin



Actually: pay fees to nodes

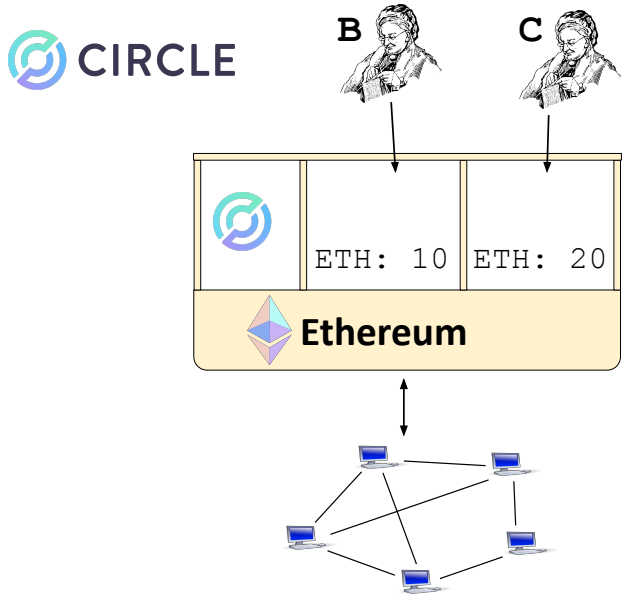


Actually: pay fees to nodes

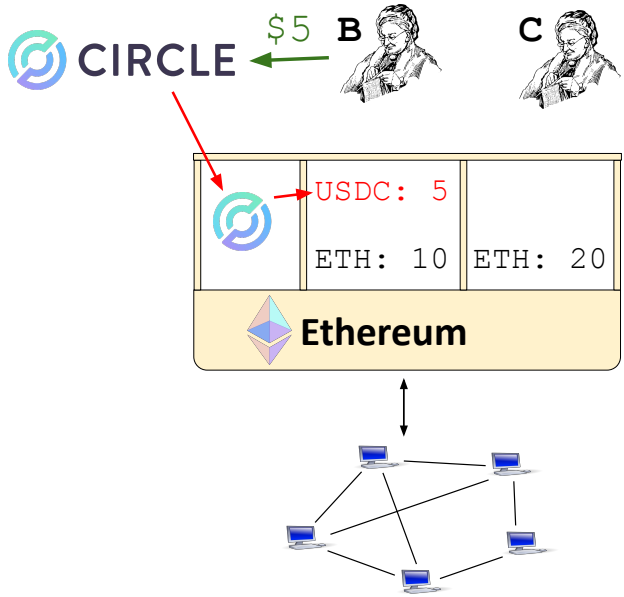


Example: stablecoin, exchange

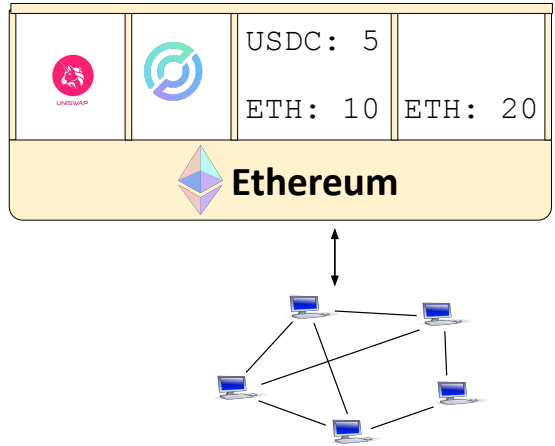
Example: stablecoin, exchange



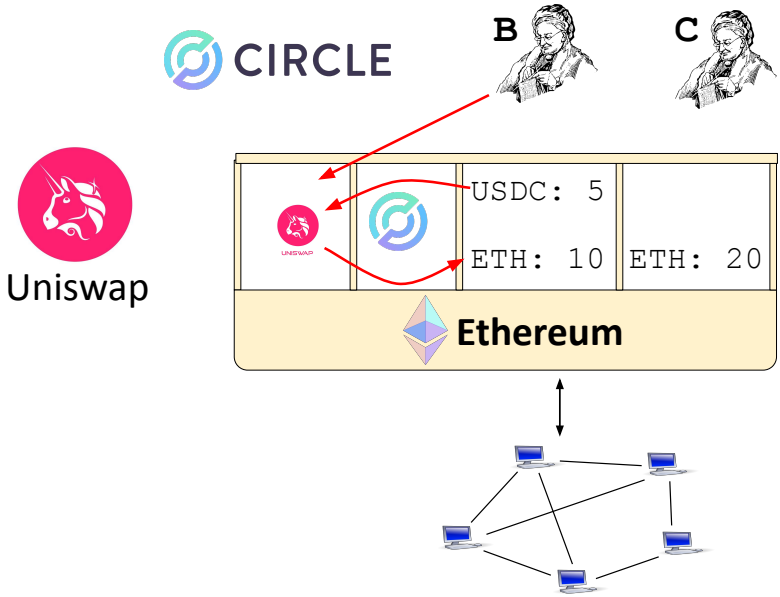
Example: stablecoin, exchange



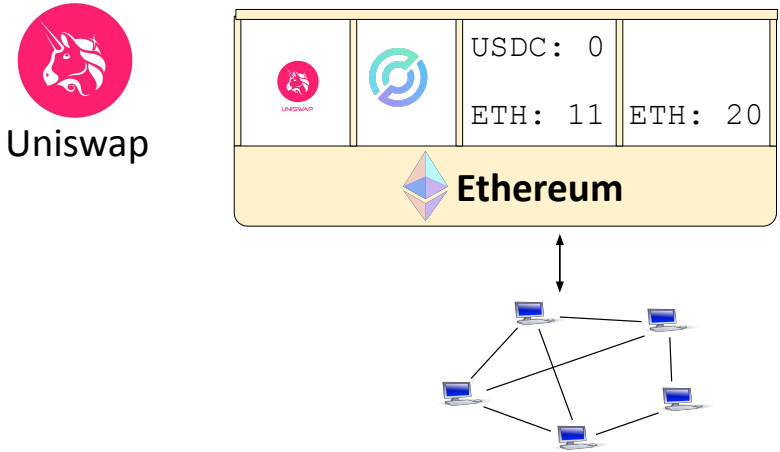
Example: stablecoin, exchange



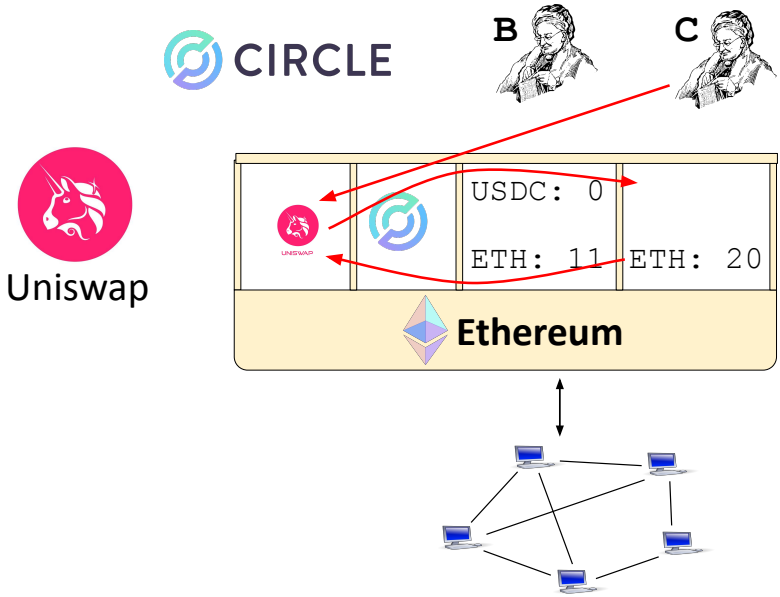
Example: stablecoin, exchange



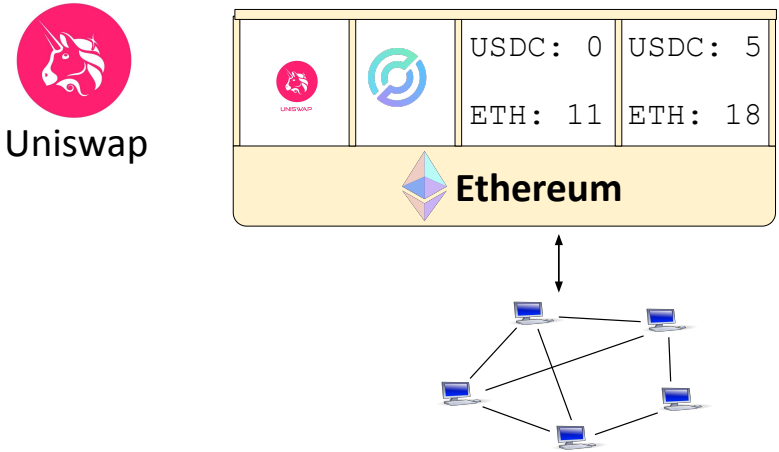
Example: stablecoin, exchange



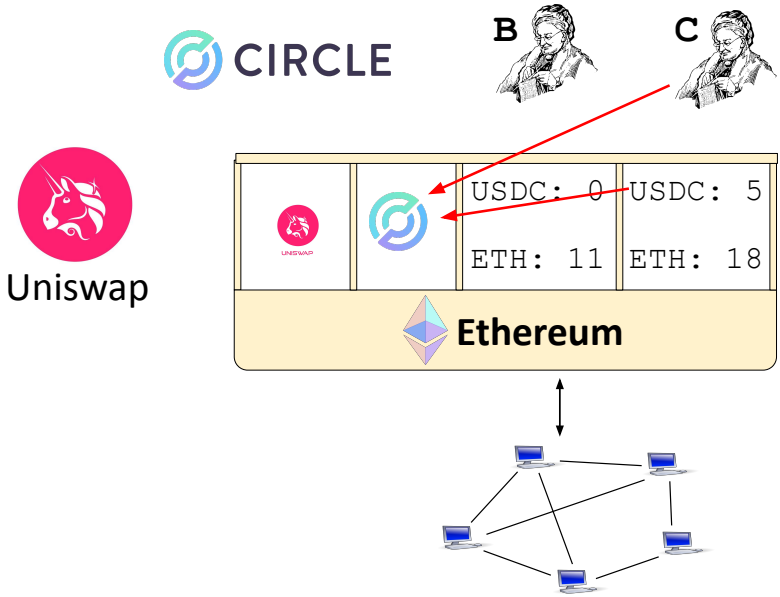
Example: stablecoin, exchange



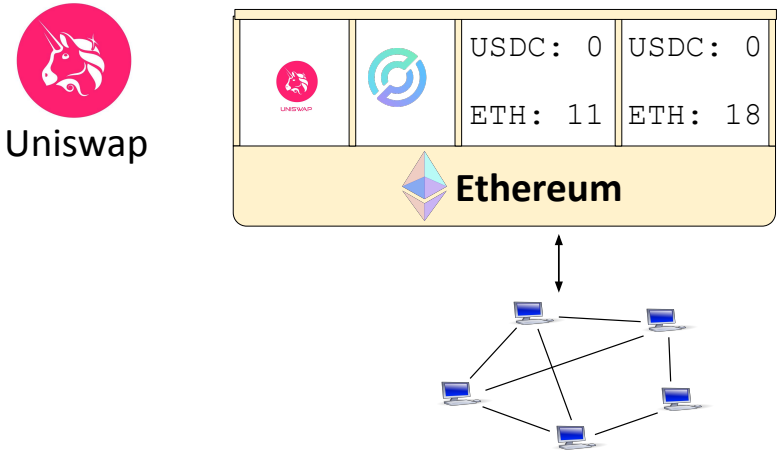
Example: stablecoin, exchange



Example: stablecoin, exchange

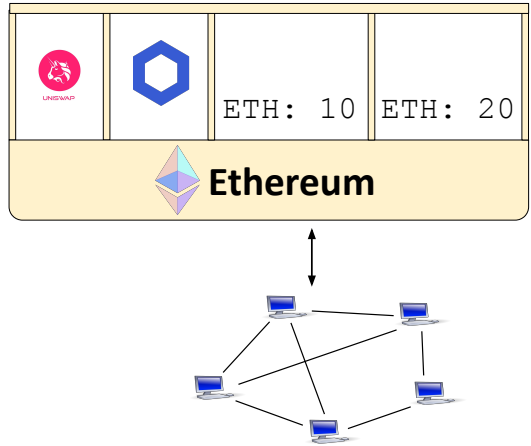


Example: stablecoin, exchange

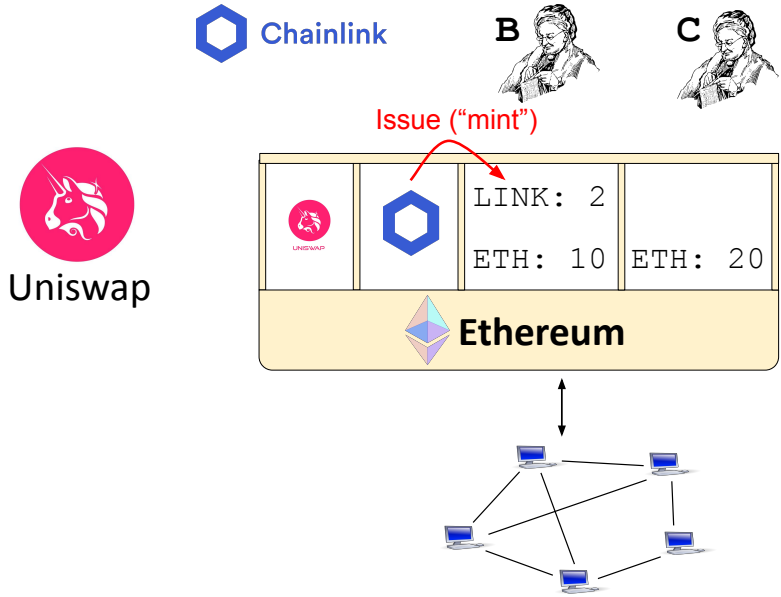


Example: tokens

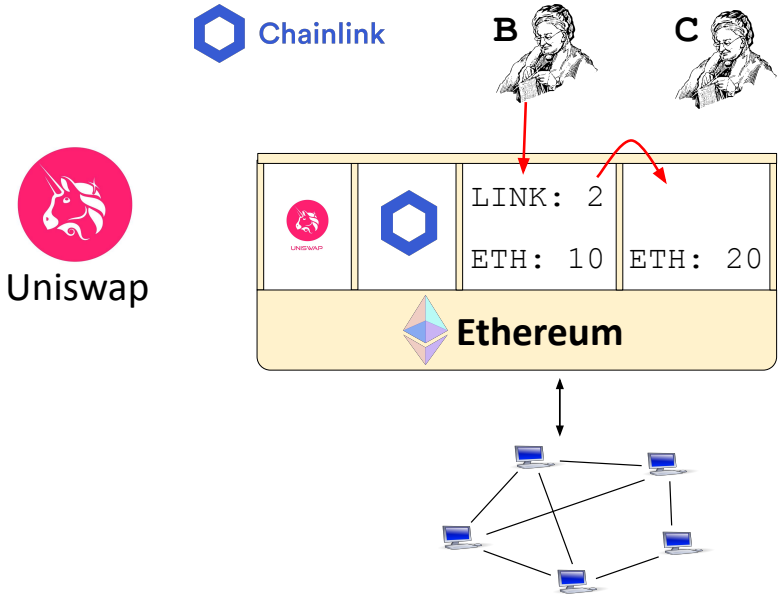
Example: tokens



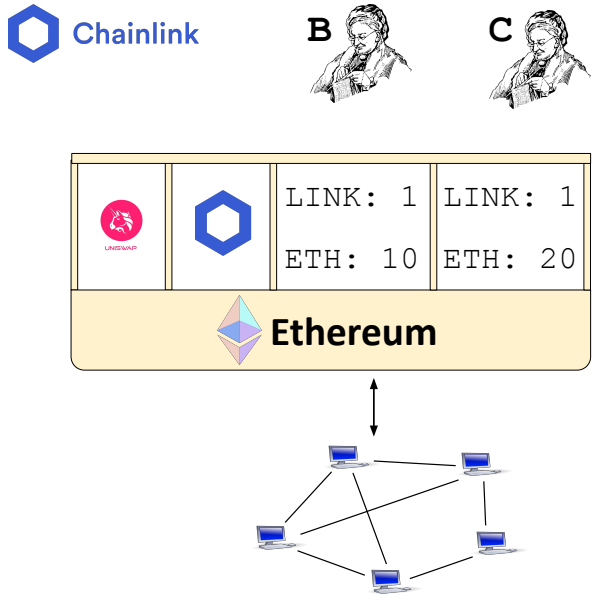
Example: tokens



Example: tokens



Example: tokens

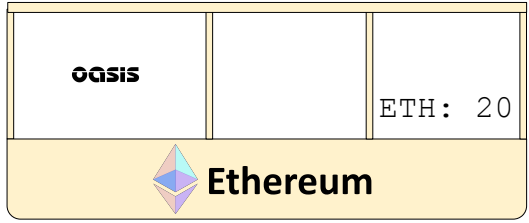


Example: Non-Fungible Token (NFT)

Example: Non-Fungible Token (NFT)

*

$100



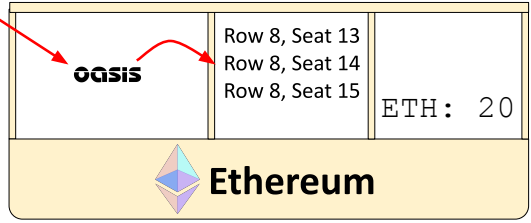
*hypothetical

Example: Non-Fungible Token (NFT)

*

B

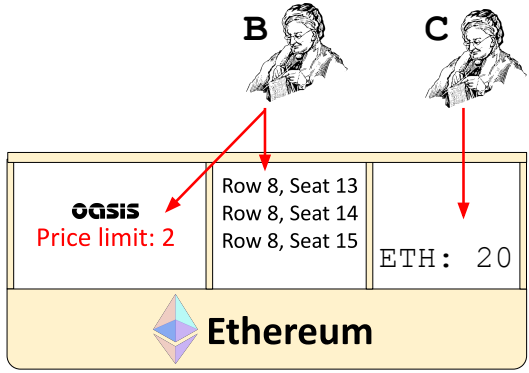
C



*hypothetical

Example: Non-Fungible Token (NFT)

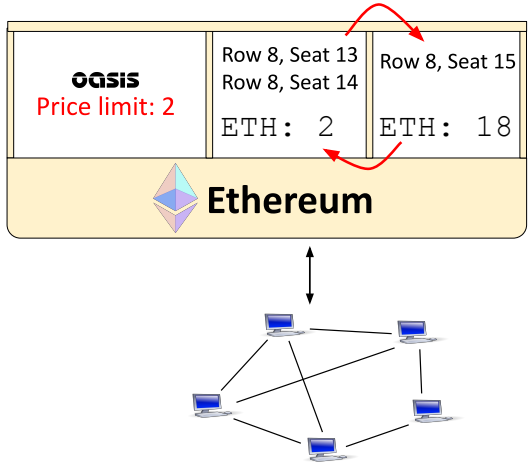
*



*hypothetical

Example: Non-Fungible Token (NFT)

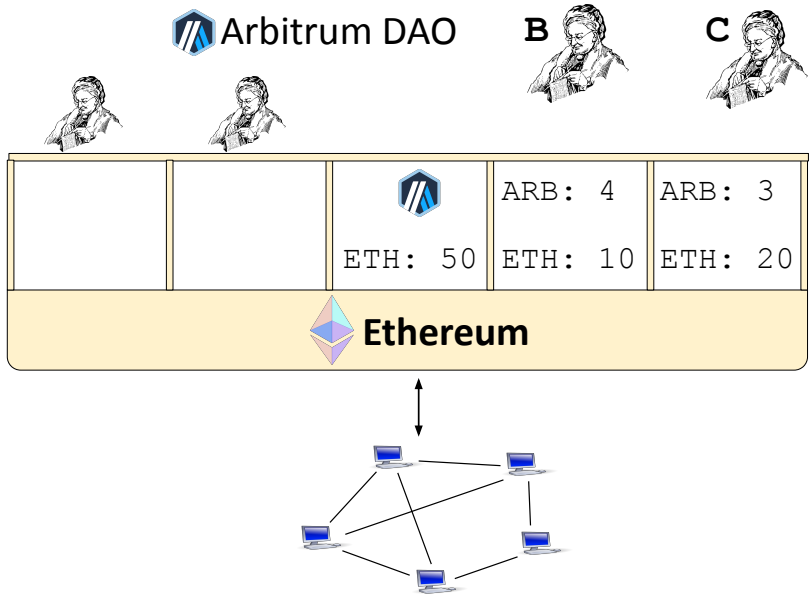
*



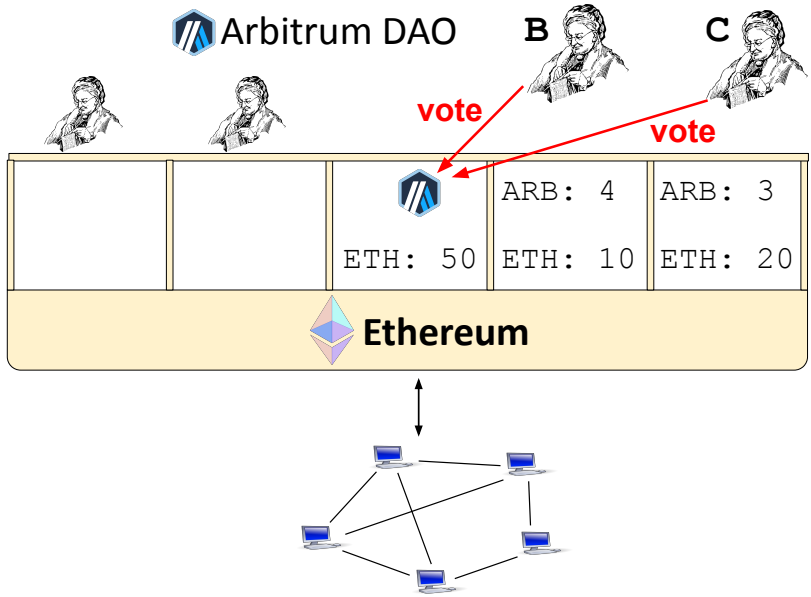
*hypothetical

Example: voting

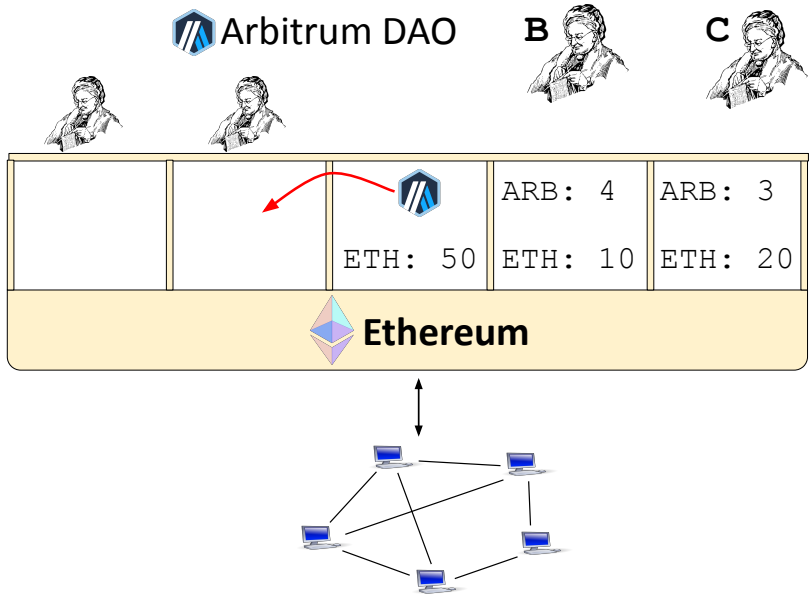
Example: voting



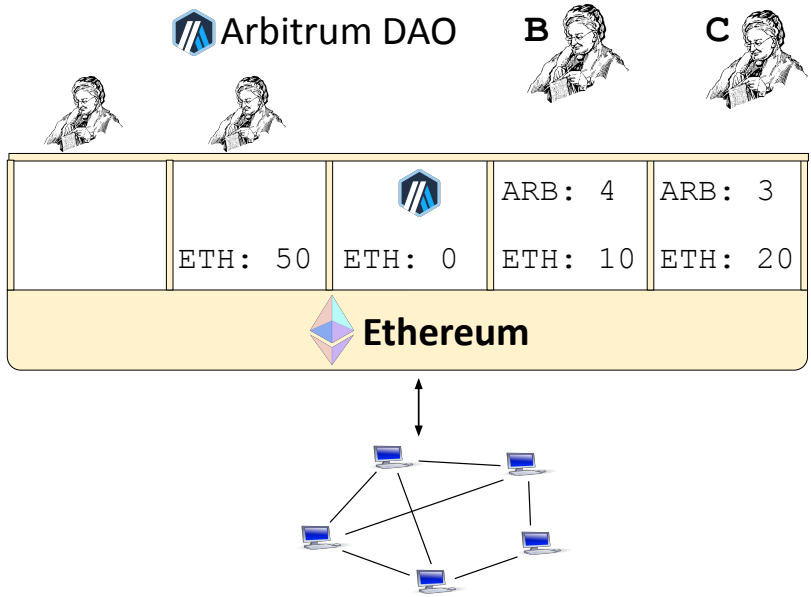
Example: voting



Example: voting



Example: voting



History and uses of blockchains

Bitcoin (2009) introduced cryptocurrency, Ethereum (2014) general-purpose blockchains. Many others exist; they do not directly interoperate.

History and uses of blockchains

Bitcoin (2009) introduced cryptocurrency, Ethereum (2014) general-purpose blockchains. Many others exist; they do not directly interoperate.

Main types of blockchain assets:

- **Native currency** of a blockchain: BTC (Bitcoin), SOL (Solana), etc.
- **Tokens** as "blockchain apps": stablecoins, memecoins, voting tokens.
- **Non-fungible tokens (NFTs)** that represent a unique asset, also "blockchain apps": art, concert tickets, Real-World-Assets.

History and uses of blockchains

Bitcoin (2009) introduced cryptocurrency, Ethereum (2014) general-purpose blockchains. Many others exist; they do not directly interoperate.

Main types of blockchain assets:

- **Native currency** of a blockchain: BTC (Bitcoin), SOL (Solana), etc.
- **Tokens** as "blockchain apps": stablecoins, memecoins, voting tokens.
- **Non-fungible tokens (NFTs)** that represent a unique asset, also "blockchain apps": art, concert tickets, Real-World-Assets.

Common blockchain apps:

- **Decentralized Finance ("DeFi")**: trading, lending, prediction markets
- **NFTs:** representing digital (or real-world) assets
- **Video games**, social networks

Potentially useful properties

Potentially useful properties

- Neutral, reliable clearinghouse – reduce counterparty risk
- Convenience, low fees – in some cases
- Stability, resilience, reliability - particularly in non-U.S. contexts
- Open source platform to build apps/businesses/co-ops on
  - customized organizations and rules/bylaws
  - low "take rates" and chance of capture
  - compare: Apple, Facebook, Spotify, Strava, ...

Summary of Part 1: What's a blockchain?

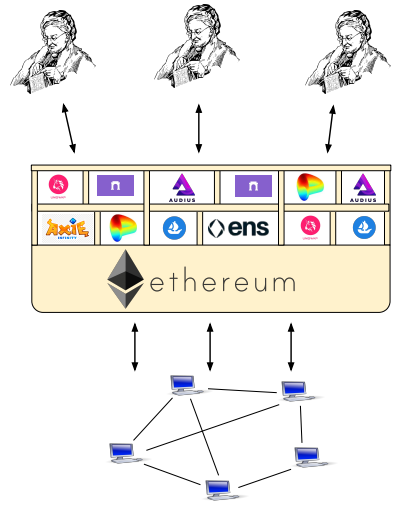
Summary of Part 1: What's a blockchain?

Use cryptographic keys to access → **Users**

Can be deployed by anyone → **Apps and accounts**

Enforces access rules → **"Virtual machine"**

Can be anyone; incentives to particpate → **Network of nodes**

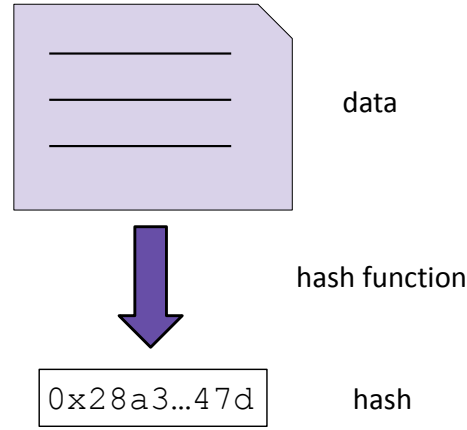


Part 2: Nuts and bolts

- Cryptography, under the hood
- Broad takeaways

Hashes

A hash is a "summary" of some data computed by a specific function.

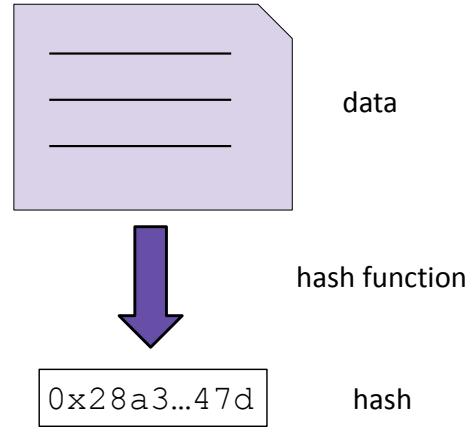


Hashes

A hash is a "summary" of some data computed by a specific function.

Properties:

- Short
- Unique* (no two have the same hash)
- Not reversible* (hides the data)



Hashes

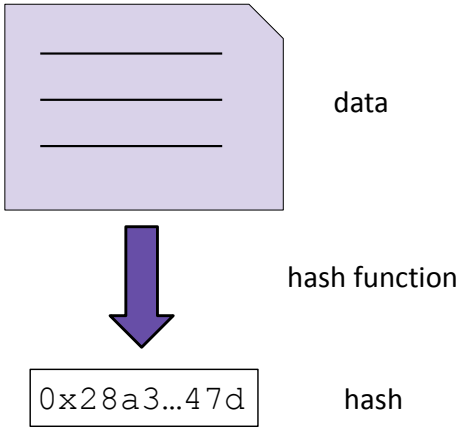
A hash is a "summary" of some data computed by a specific function.

Properties:

- Short
- Unique* (no two have the same hash)
- Not reversible* (hides the data)

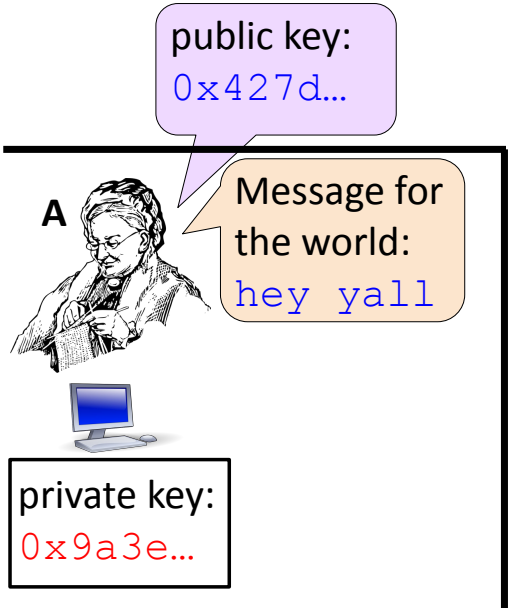
Applications:

- Identifiers (transaction `0x28a3...`)
- Commitments

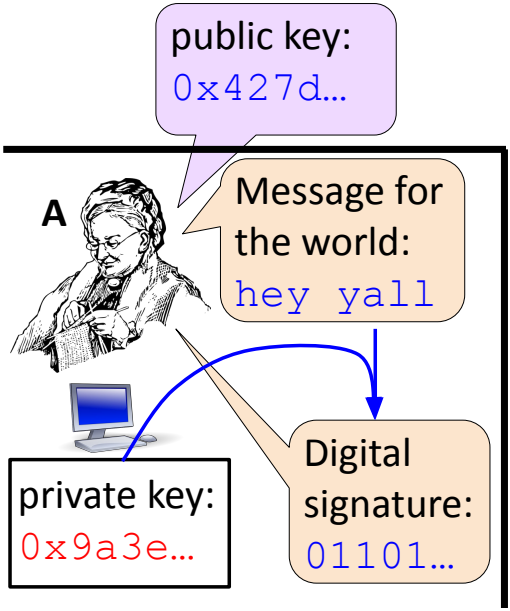


Digital signatures

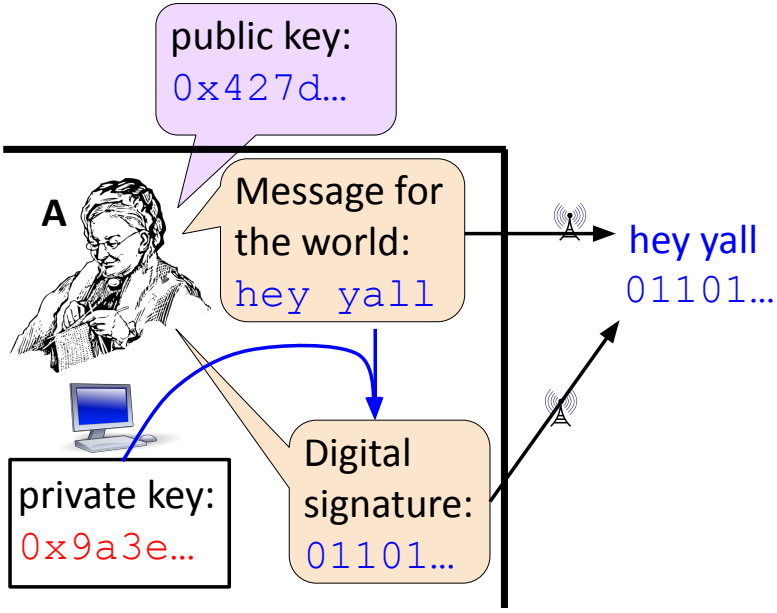
Digital signatures



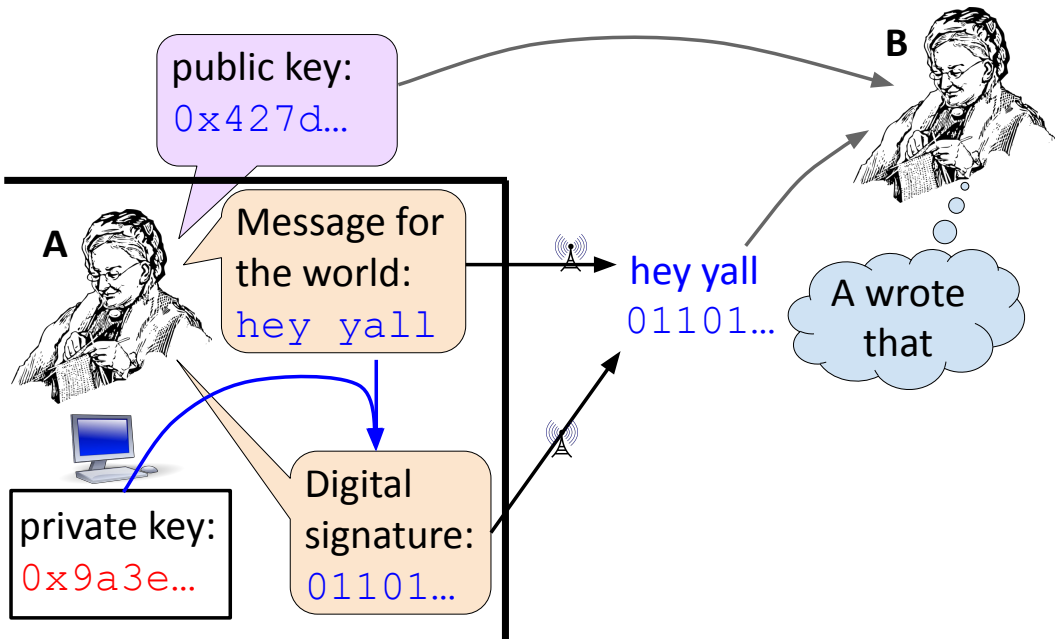
Digital signatures



Digital signatures

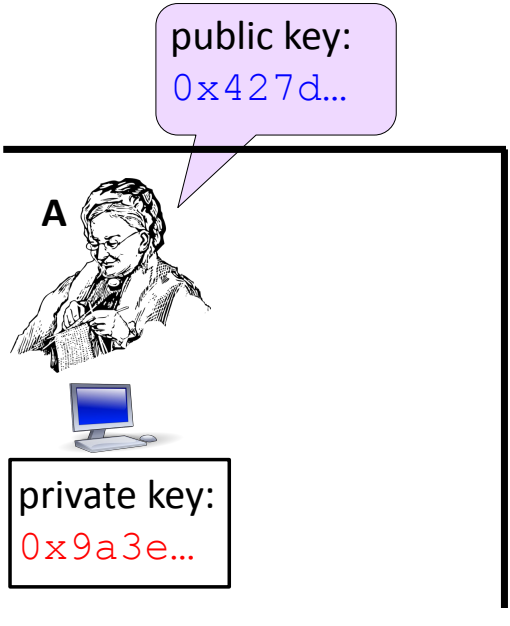


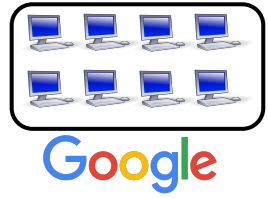
Digital signatures



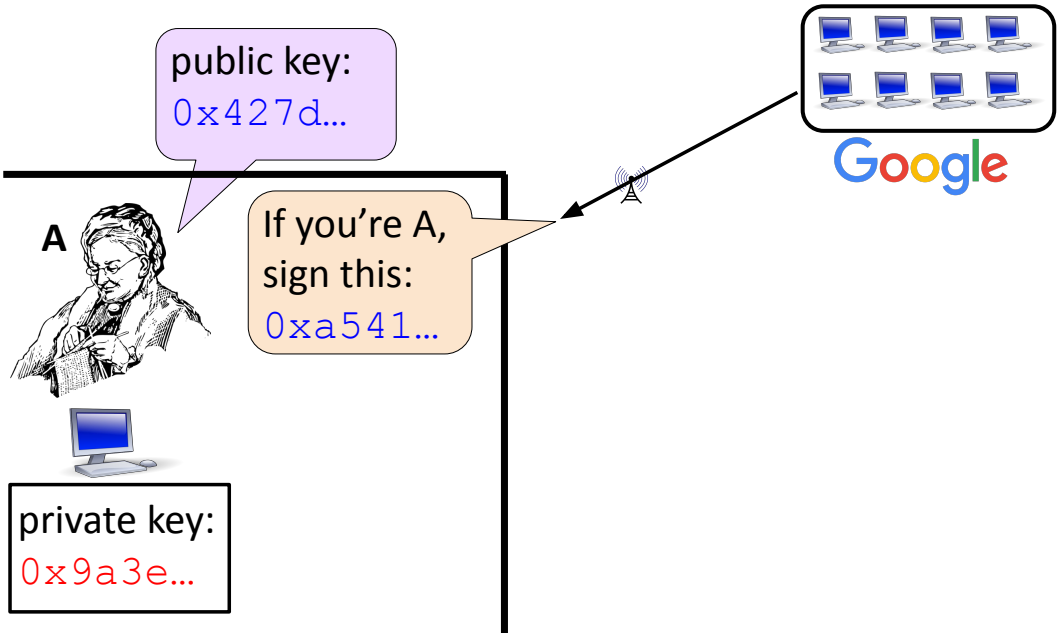
Digital signatures: for authenticating (passkeys)

Digital signatures: for authenticating (passkeys)

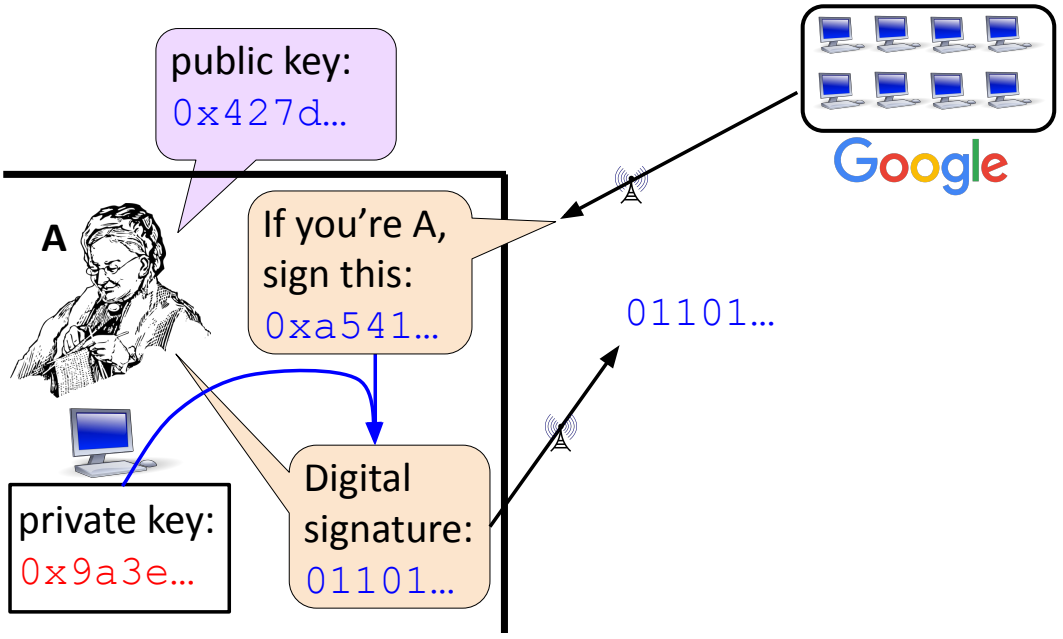




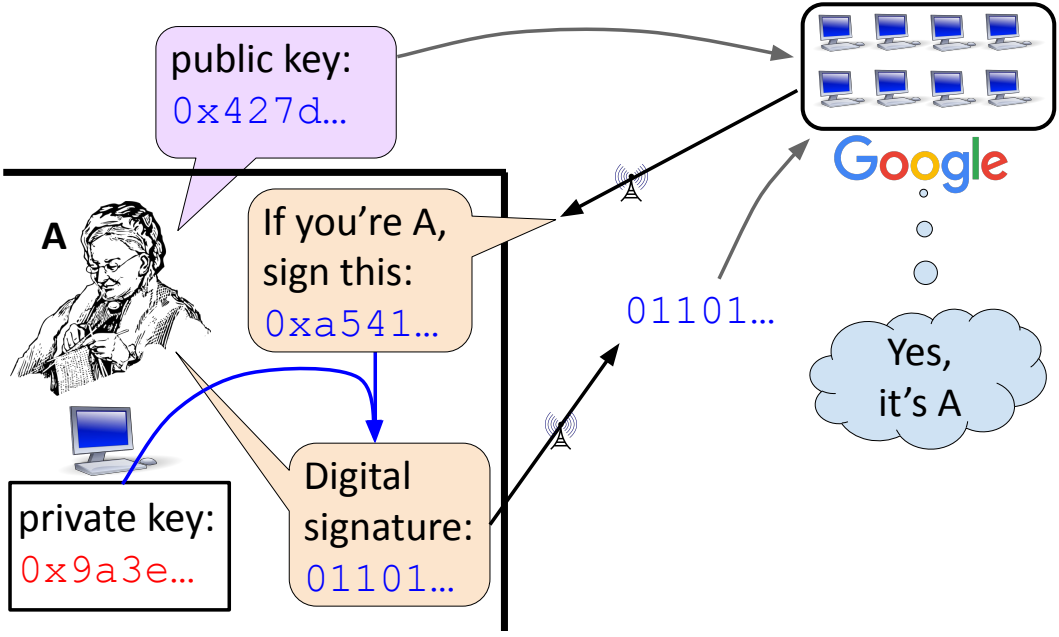
Digital signatures: for authenticating (passkeys)



Digital signatures: for authenticating (passkeys)

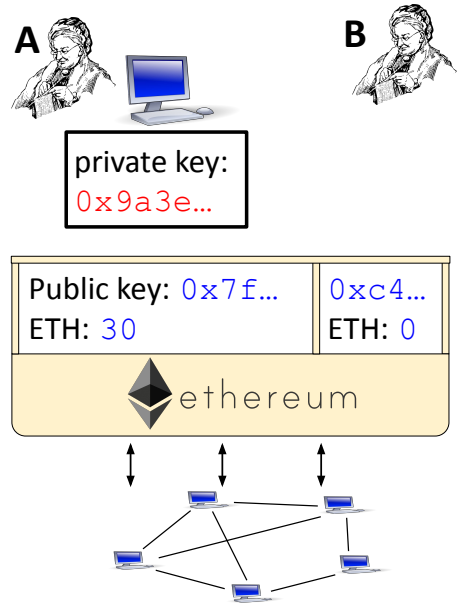


Digital signatures: for authenticating (passkeys)

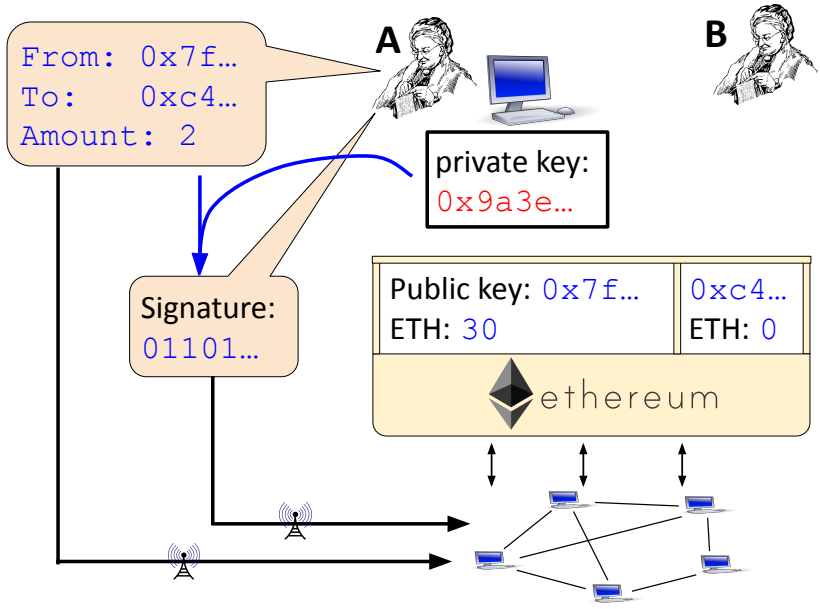


Digital signatures: sending transactions

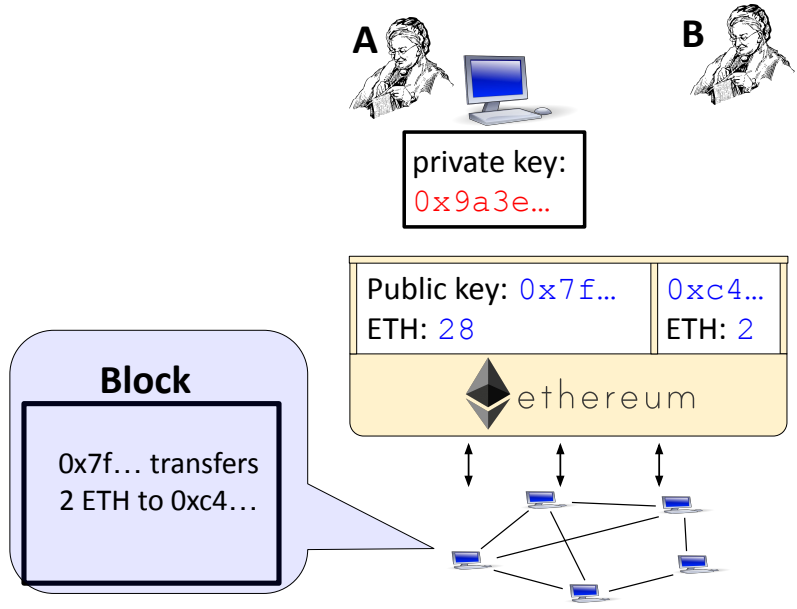
Digital signatures: sending transactions



Digital signatures: sending transactions

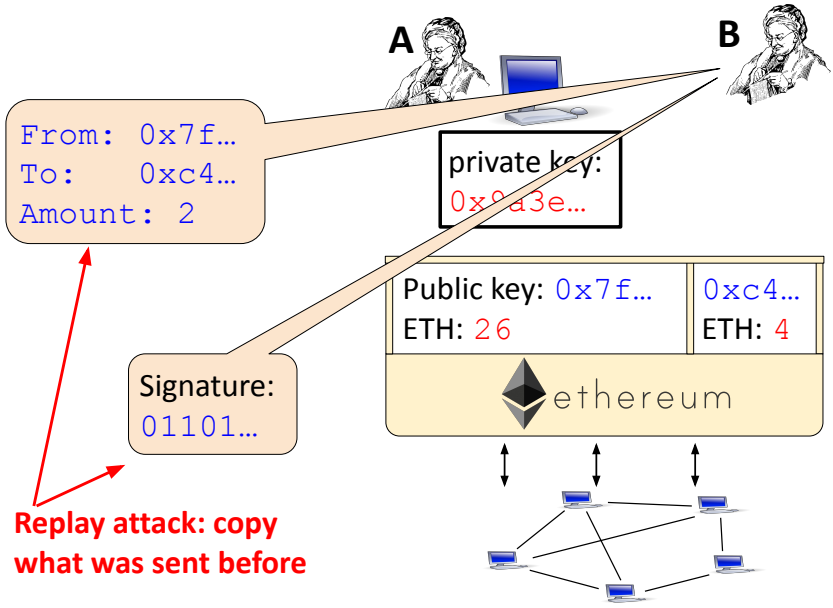


Digital signatures: sending transactions

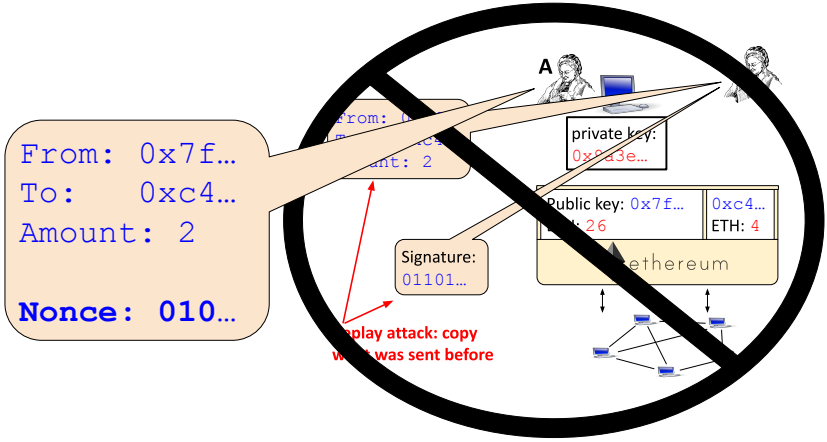


Digital signatures: replay attacks

Digital signatures: replay attacks



Digital signatures: replay attacks



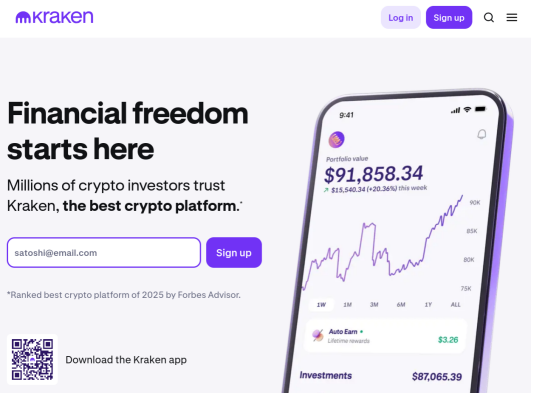
Prevented by including a unique transaction identifier (“nonce”).

Key management: cryptocurrency or tokens

Key management: cryptocurrency or tokens

(1) Buying on an exchange

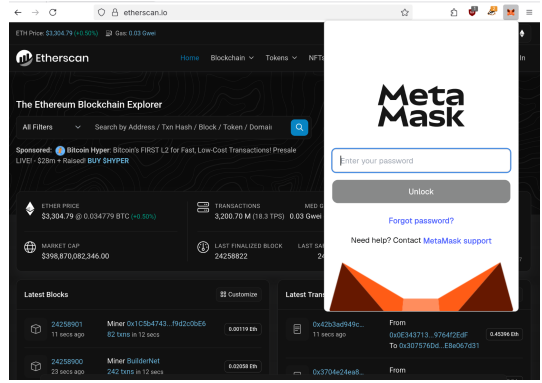
- Exchange custodies the assets (brokerage)
- May transfer to user-owned wallet



Key management: cryptocurrency or tokens

(1) Buying on an exchange

- Exchange custodies the assets (brokerage)
- May transfer to user-owned wallet

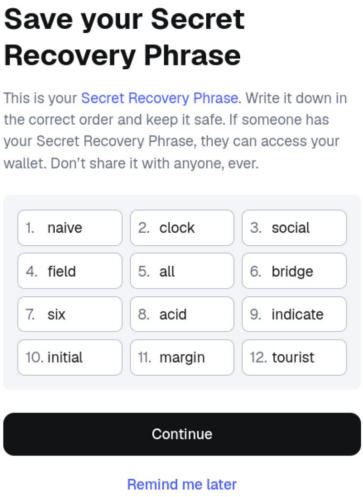


(2) Keeping keys on your device

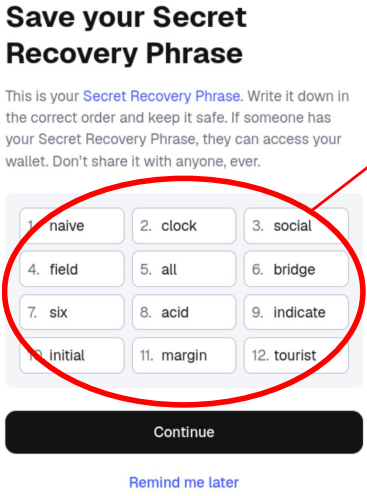
- Use "wallet" on phone or browser
- Generate 12-word recovery mnemonic
- Mnemonic determines keys
  - Can generate a sequence of keys

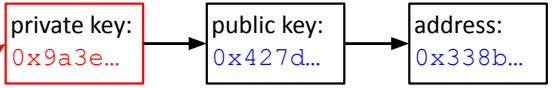
Mnemonics and keys

Mnemonics and keys

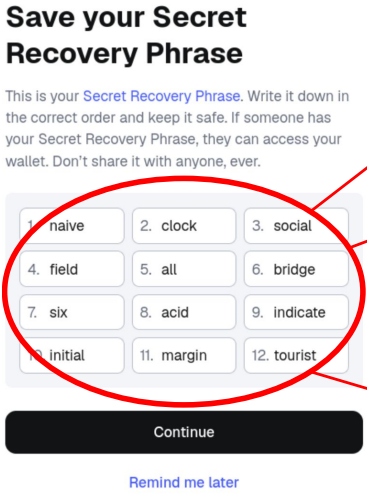


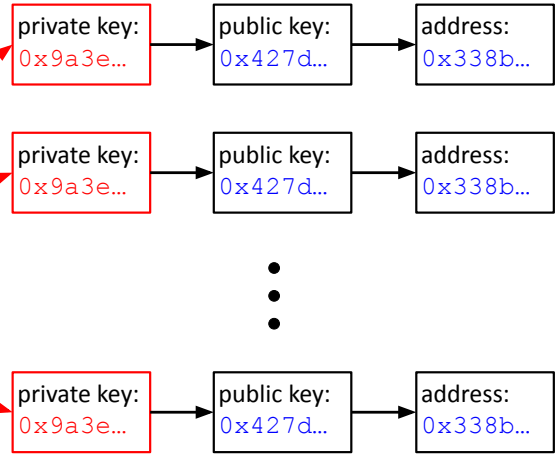
Mnemonics and keys



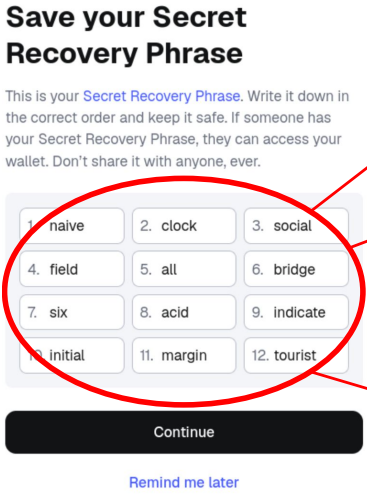


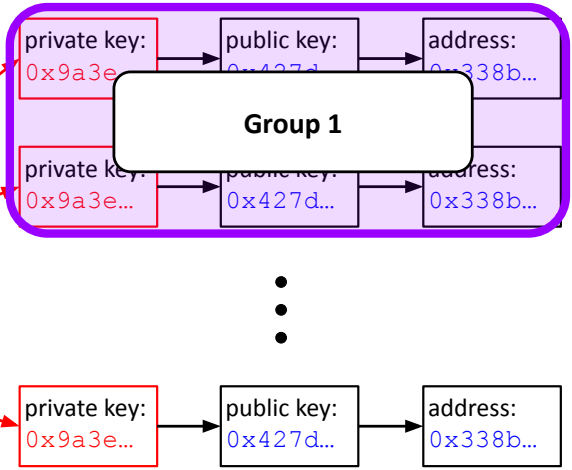
Mnemonics and keys





Mnemonics and keys





Zero-knowledge

On blockchains, everything is generally publicly visible.

Zero-knowledge protocol (in theory): a proof that a fact is true, without revealing any other information.

Zero-knowledge

On blockchains, everything is generally publicly visible.

Zero-knowledge protocol (in theory): a proof that a fact is true, without revealing any other information.

Key example: transfer currency, hiding amount and recipient.

- Specialized cryptocurrencies: Monero, ZCash
- "Mixer" apps: Tornado Cash (on Ethereum, others)

Main takeaway: These technologies add privacy, but are also amenable to investigation.

Implications (1/3)

Implications (1/3)

- One mnemonic $\rightarrow$ multiple accounts on multiple blockchains
  cannot tell how it was used from the phrase itself

Implications (1/3)

- One mnemonic $\rightarrow$ multiple accounts on multiple blockchains
  cannot tell how it was used from the phrase itself

- Digital "assets" are stored on the blockchain;
  the user only stores their keys
  assets exist in public view; the keys prove ownership

Implications (1/3)

- One mnemonic $\rightarrow$ multiple accounts on multiple blockchains
  cannot tell how it was used from the phrase itself

- Digital "assets" are stored on the blockchain;
  the user only stores their keys
  assets exist in public view; the keys prove ownership

- Someone gets your private key or mnemonic
  $\Longrightarrow$ they can take all your stuff
  recommended: use "hot" and "cold" wallets
  watch out: vulnerability of phone and browser wallets
  modern remedies: multi-sig accounts, spending limits, ...

Implications (2/3)

Implications (2/3)

- Transactions aren't final 'till they're final
  time to finalize, if ever, depends on the chain

Implications (2/3)

- Transactions aren't final 'till they're final
  time to finalize, if ever, depends on the chain

- Transactions cannot be undone
  except with cooperation of recipient, if any
  modern remedies: undo can be built into the "app"

Implications (2/3)

- Transactions aren't final 'till they're final
  time to finalize, if ever, depends on the chain
- Transactions cannot be undone
  except with cooperation of recipient, if any
  modern remedies: undo can be built into the "app"
- You can't block people from sending you stuff
  anything sent to your address is "yours"

Implications (3/3)

Implications (3/3)

Cross-chain transfers ("bridges") and fiat exchanges are fraught:

- settlement in different denominations, ...
- different delivery mechanisms, ...
- different time scales.

Summary of Part 2: Nuts and bolts

- All data, assets, etc. are **stored on the blockchain**
- Control of assets = **possession of private key**
- Keys are managed by **software wallets**

Part 3: The Industry

- Major blockchains, their types
- Major uses of blockchains and cryptocurrency today

Timeline and stats

Timeline and stats

Major blockchains (*they do not interoperate!*):

Since	Chain	Native Currency	Features	Nodes	Transactions per day	Volume per day
2009	Bitcoin	BTC	first	100k+	400k	$50B
2012	"Ripple"	XRP	supports tokens	100's	2M	$3B
2013	Dogecoin	DOGE	intended as joke	500	40k	$1B
2014	Monero	XMR	privacy-focused	1k	25k	$300M
2014	Ethereum	ETH	general-purpose	10k	14M+	$40B+
2016	ZCash	ZEC	privacy-focused	100's	7k	$600M
2017	Cardano	ADA	proof of stake	3k	2M	$700M
2020	Solana	SOL	fast and cheap	1k	70M+	$10B+
1792	*NYSE*	*USD*	*NY Stock Exch.*	*1*	*10B*	*$500B*

Sources: CoinMarketCap.com, DefiLlama, various. Numbers very rough. Attempts to include volume traded in tokens on chain and in "Layer 2"s where applicable.

Types of blockchains and main examples

Types of blockchains and main examples

- **Just cryptocurrency:** Bitcoin, Dogecoin
- **Cryptocurrency + privacy:** Monero, ZCash
- **Tokens only:** XRPL ("Ripple")
- **General apps:** Ethereum, Cardano, Solana
- *"Layer 2 (rollups)" on Ethereum:* Base, Arbitrum, Optimism, Polygon, ...

NFTs

What is it: "non-fungible token" representing ownership of unique item, such as (digital) art or a ticket

NFTs

What is it: "non-fungible token" representing ownership of unique item, such as (digital) art or a ticket

Details:

- Made famous by digital "art" series such as "Bored Apes"
- Connection to legal ownership may be unclear
- Potentially important real financial use cases in near future

Memecoins

What is it: tokens bought/sold as part of a trend with no discernible purpose

Memecoins

What is it: tokens bought/sold as part of a trend with no discernible purpose

Details:

- Can be created as a token on top of a blockchain
- Creator can set properties (supply, initial price)
- Generally created as a meme with no real attempt to justify value

Initial Coin Offering (ICO)

What is it: new company raises money by selling tokens, often "governance tokens"

Initial Coin Offering (ICO)

What is it: new company raises money by selling tokens, often "governance tokens"

Details:

- Tokens may confer rights or access, e.g. voting
- Creator can set properties (supply, initial price)
- May raise legal questions in relation to securities

Important point: the creator can design the smart contract in different ways, e.g. may give the tokens no real uses, may be able to reclaim them or void them, etc.

Tokenization (Wrapped ____)

What is it: tradeable token that represents ownership of some frozen asset

Tokenization (Wrapped ____)

What is it: tradeable token that represents ownership of some frozen asset

Examples:

- Company owns 100 BTC and creates 100 "wrapped BTC" on a different blockchain (e.g. Ethereum); sells them, redeemable for BTC later
- Stablecoins are "wrapped USD"
- Liquid staking
  - In proof of stake, users "stake" (lock up) currency such as ETH and earn gradual rewards, similar to interest on a loan
  - Users can "wrap" the locked ETH into a tradeable token, weETH, representing ownership of the locked value

Decentralized Finance (DeFi)

What is it: large industry of financial products on-chain

Decentralized Finance (DeFi)

What is it: large industry of financial products on-chain

Examples:

- Lending/borrowing, often with digital assets as collateral
- Exchanges, e.g. Uniswap
- Derivatives, options, prediction markets
- Insurance

Glossary: wallets and sending transactions

Address: unique identifier (e.g. 0x62c1...) that can receive cryptocurrency.

Mnemonic, secret recovery phrase: 12-word (or more) phrase that determines private/public keys for an account(s).

Wallet: software, often a phone app or a web browser plugin, that manages accounts (public/private keys, addresses, cryptocurrency, other digital assets). **Hot wallet** means in active use; **cold wallet** means not Internet-connected.

Mempool: when a user sends a transaction request, the nodes add it to the blockchain's "mempool": transactions waiting to be included in a block.

Node, validator, miner: a computer syncing/updating the blockchain.

A satoshi: 0.000000001 Bitcoins. **A gwei, wei:** 0.000000001 Ether, 0.000000000000000001 Ether.

Custody, custodial: who controls an account's private keys, e.g. self-custody.

Ring signature: digital sig. that can come from any of an authorized group. Used in privacy-oriented blockchains (e.g. Monero) to obscure senders.

Multisig: actions require auth. from multiple private keys, e.g. at least 9 of 13.

Glossary: DeFi and d'apps

CEX, DEX: Centralized exchange (buy cryptocurrency, e.g. Coinbase, Kraken, Binance), Decentralized ex. (app on a blockchain, e.g. Uniswap, PancakeSwap).

dApp: decentralized app, deployed on a blockchain.

Smart contract: any program deployed to and running on a blockchain.

Confirmation, confirmed, final, finalized: with confirmation, it is known that the transaction has been processed by the blockchain; with finality, it is known the transaction can no longer be undone.

Bridge: a financial service for exchanging assets between multiple blockchains.

(Fungible) token: exchangeable digital asset, deployed as a blockchain app.

Non-fungible token (NFT): deployed as a blockchain app, a unique digital asset, perhaps tied to a real-world asset (RWA) or a copyright ownership.

Oracle: in a blockchain app depending on real-world outcomes, e.g. insurance or prediction markets, the oracle states what the true real-world outcome was.

Wrapped asset: a token on a blockchain that represents another asset, such as cryptocurrency from another blockchain. A stablecoin is a "wrapped dollar".

Glossary: DAOs and governance

Airdrop: when a project gives away free tokens to participants or supporters.

Initial Coin Offering (ICO): a project or company creates a token ("coin") and sells or distributes an amount to raise money and interest. May be for a DAO.

DAO: Decentralized Autonomous Organization, a group using blockchain apps to organize and make decisions. E.g. funds may be held by a smart contract and distributed according to votes cast on the blockchain.

Governance tokens: tokens that grant participation rights in e.g. a DAO, such as allowing the owner to cast votes.

Staking, liquid staking: in Proof of Stake chains, owners an "stake" the native cryptocurrency (such as Ether) to participate as a node and earn rewards. In liquid staking, users lend their currency to a pool that stakes it on their behalf and receive a tradeable token that represents the staked asset.

Fork: when a blockchain "splits" into two versions, becoming two different chains; nodes choose which chain to participate in. Very rare. The main examples are Bitcoin/Bitcoin Cash and Ethereum/Ethereum Classic.

Glossary: misc

EVM-compatible: Ethereum virtual machine compatible, a blockchain that can run apps written for Ethereum.

Layer 2, rollup: a "blockchain on a blockchain", a secondary blockchain, perhaps operated by a private company, that periodically syncs its updates back to a main blockchain. Examples on Ethereum are Base, Arbitrum, Optimism.

Block explorer, RPC Provider: Remote Procedure Call Providers are Internet services that allow one to query information about a blockchain or send transactions. A block explorer is a web interface for info about blocks, transactions, addresses and their assets, etc.

UTXO: Unspent transaction output. Each transaction creates new UTXOs for the receiver. To send a certain amount of funds on a blockchain, an account must reference the specific transaction(s) where it received that much funds and have not spent them: UTXOs.

Web3: nobody knows what this means.

Slides

https://bwag.prof/talks/2026/crypto-forum.pdf

Thanks to: Tim Roughgarden and Danny Ryan for suggestions and feedback.