Microsoft

Beginners Series to: Blockchain

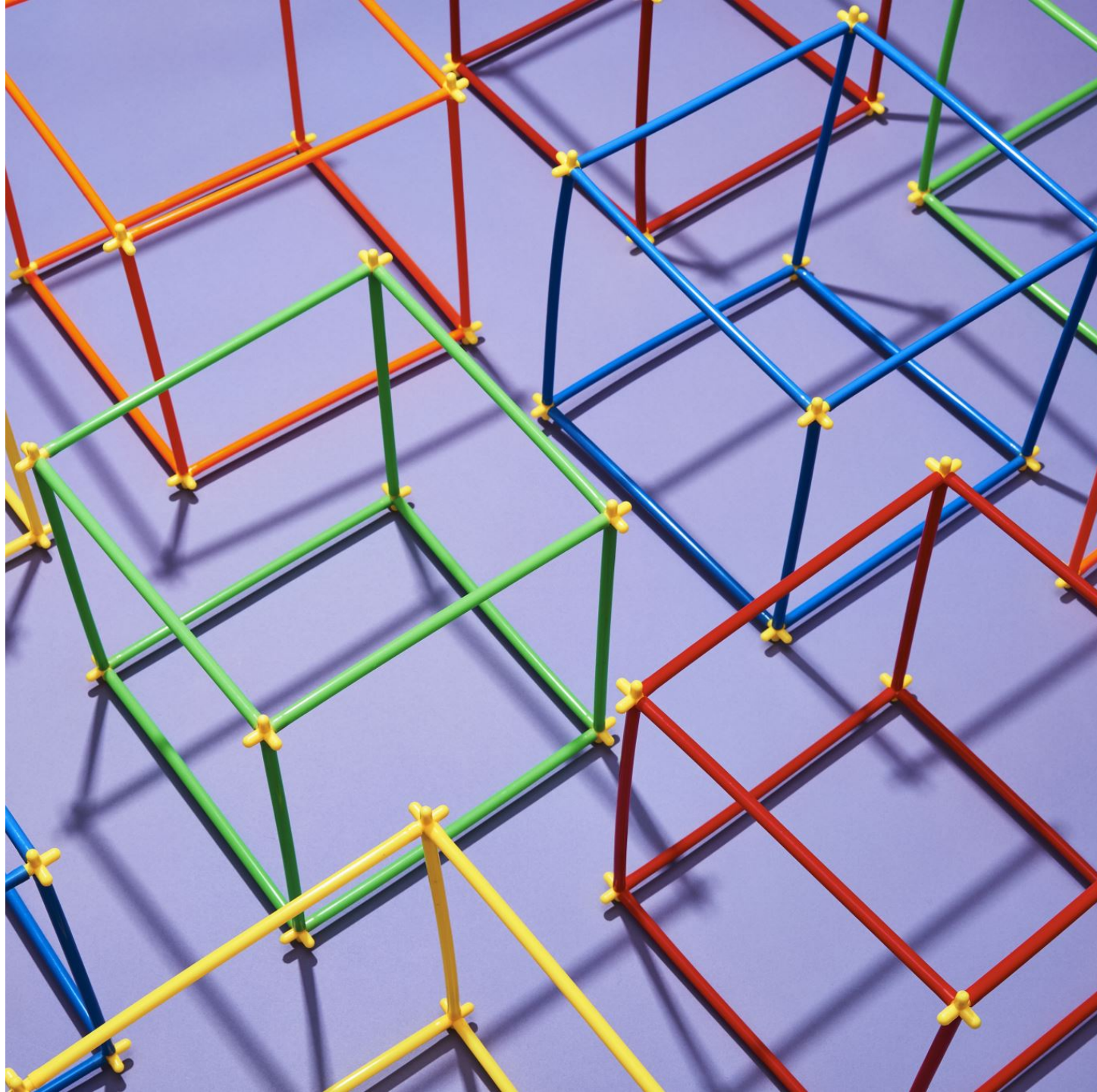
Meaghan Lewis

Topics covered

- History of blockchain
- Evolution of cryptocurrency
- Blockchain nodes
- Mining
- Consensus algorithms
- Blockchain use cases
- Bitcoin
- Ethereum
- Smart contracts
- Crypto tokes

Goals:
To provide a strong foundation for those not familiar with blockchain.

Gain an understanding of blockchain technology, how it's been used, and see how you can participate in and build blockchain networks.



About me

Meaghan Lewis

Senior Program Manager

- Focus on creating and delivering learning experiences centered around emerging technology for Microsoft Reactors worldwide.
- Previously worked in the QA field for nearly a decade.
- Have a passion for teaching lifelong learners and has spent years speaking at conferences and delivering online courses.
- Lives in the San Francisco Bay Area with my husband and two dogs

Microsoft

History of Blockchain

Distributed ledger technology

- What blockchain is built on
- Decentralized
- Records spread across multiple locations or participants
- Enforce security

Blockchain networks

- Public or private
- Participants from around the world
- Trust built into system
- Consensus algorithms
- Verified transactions

History

- Created in 1991
- Others built off this idea
  - Bit gold
  - Ecash
  - Proof of work
  - Hashcash
- Bitcoin was the first major application

Bitcoin principles

Accessible

Decentralized

Secure

Private

Consensus mechanisms

Encourages participation

Phases


Cryptocurrencies
Smart contracts
Applications
Industry adoption

Microsoft

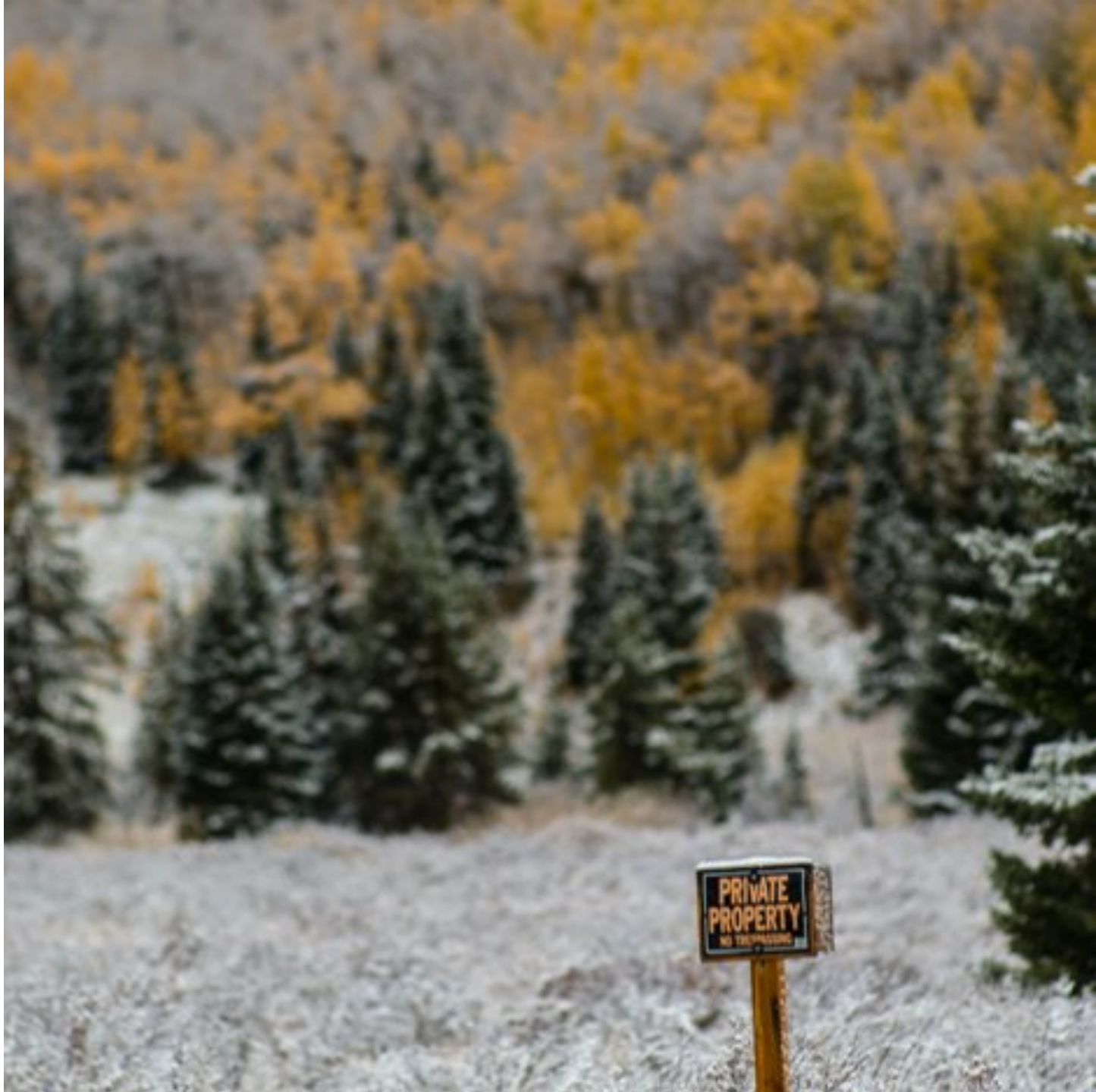
Types of blockchains

Public

- Transparent
- Decentralized
- Require consensus
- Incentivize participation
- High security
- Protected identity
- Censorship resistant
- Accessible

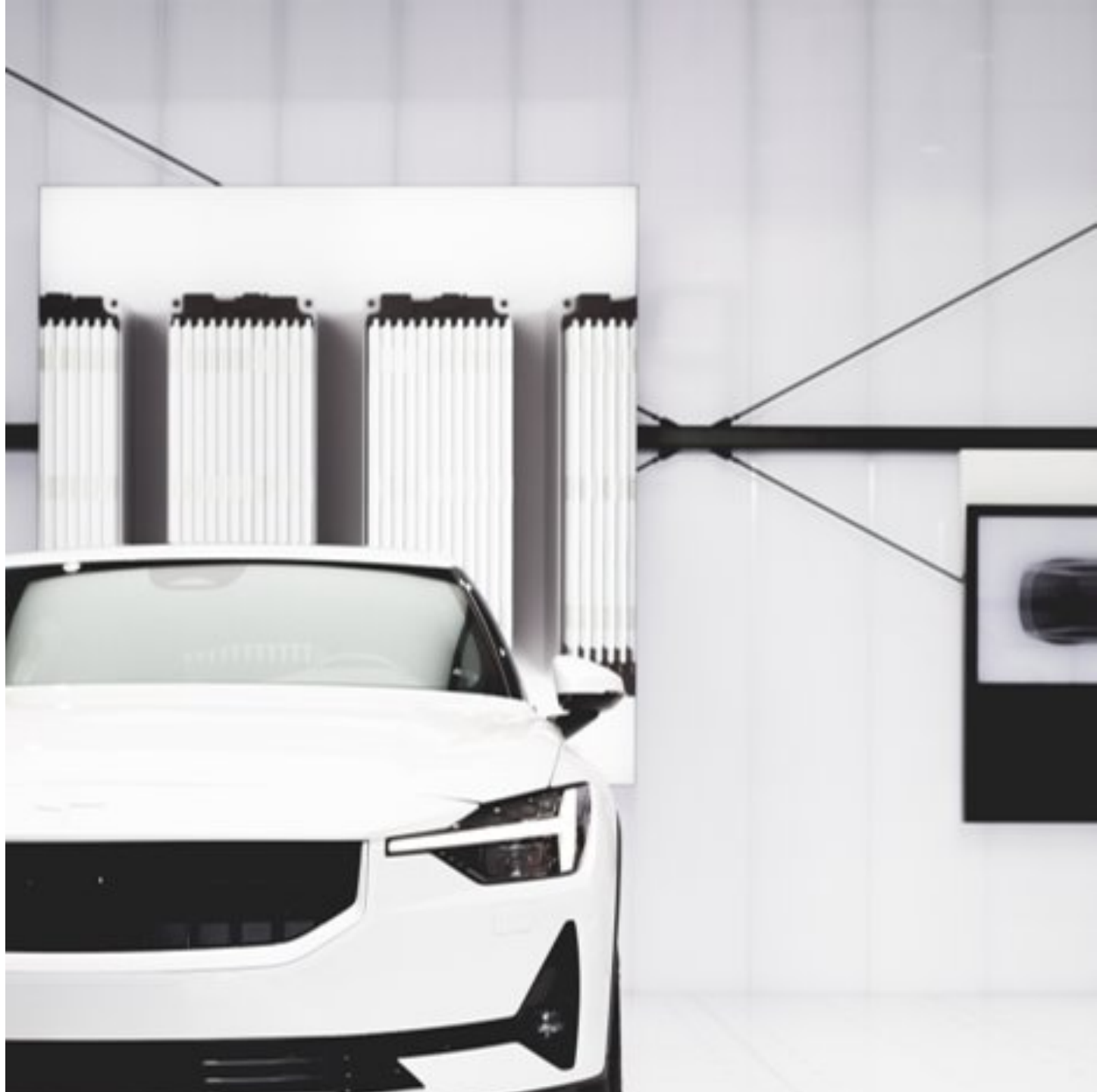
Private

- Invite only
- Permissioned
- Known identity
- High trust
- Centralized
- Faster transactions
- Better scalability
- No incentives



Hybrid

- Some private data, some public
- Mixed permissions
- Parties have different needs
- Optimize processes



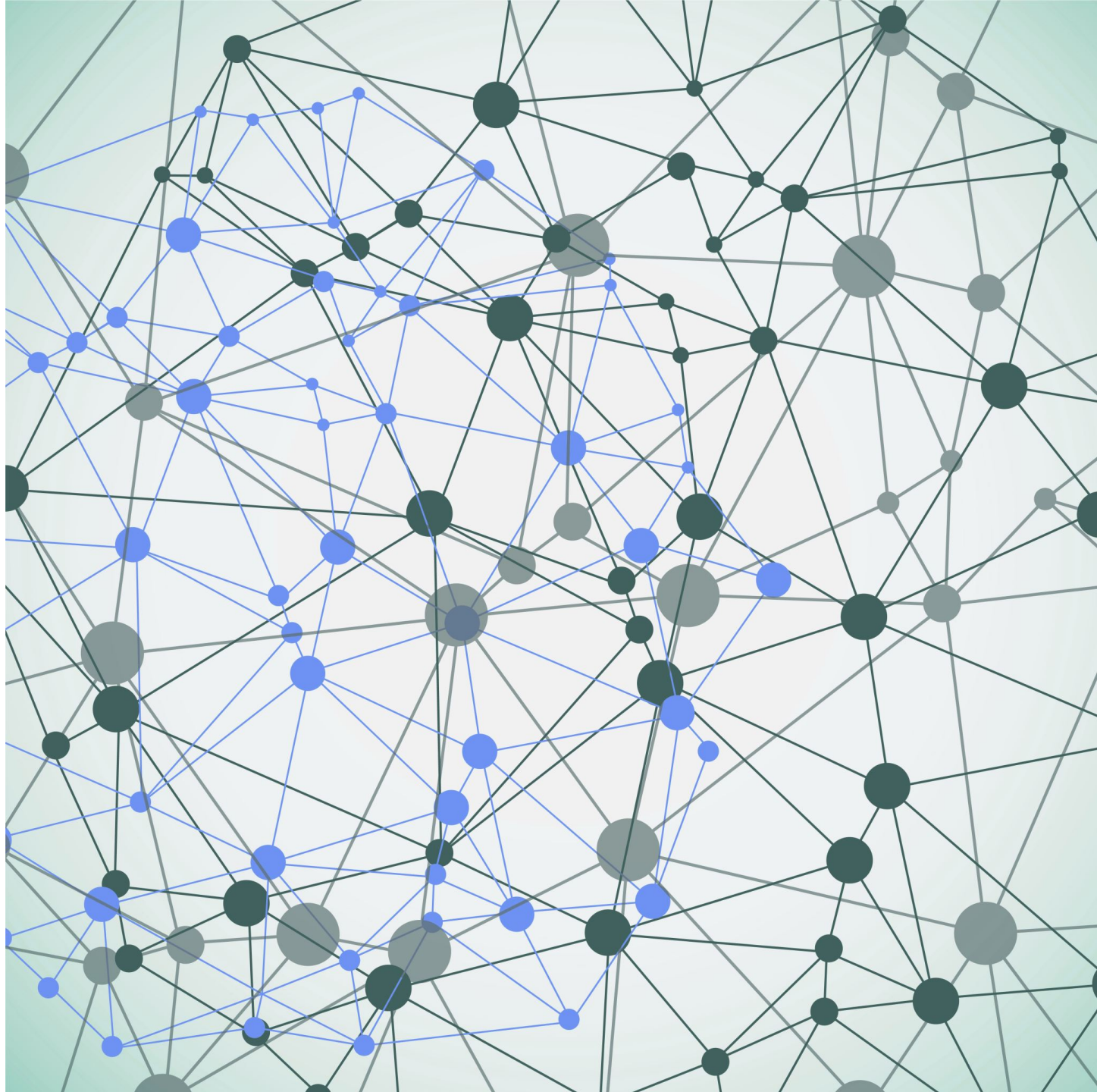
Microsoft

Byzantine Generals Problem

Byzantine Generals Problem

- No trust in each other
- Attack will succeed if they work together
- Many points of failure

A computer system will catastrophically fail if the systems are not working together strategically.



How blockchain helps

Nodes work together

Trust built in

Transactions are secure

Tamper proof system

Microsoft

Evolution of cryptocurrency


THE UNITED STATES OF AMERICA
ONE DOLLAR
L 95112039 R
WASHINGTON, D.C.
FEDERAL RESERVE NOTE
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE

3 questions to ask with fiat currency

How is it dispensed?

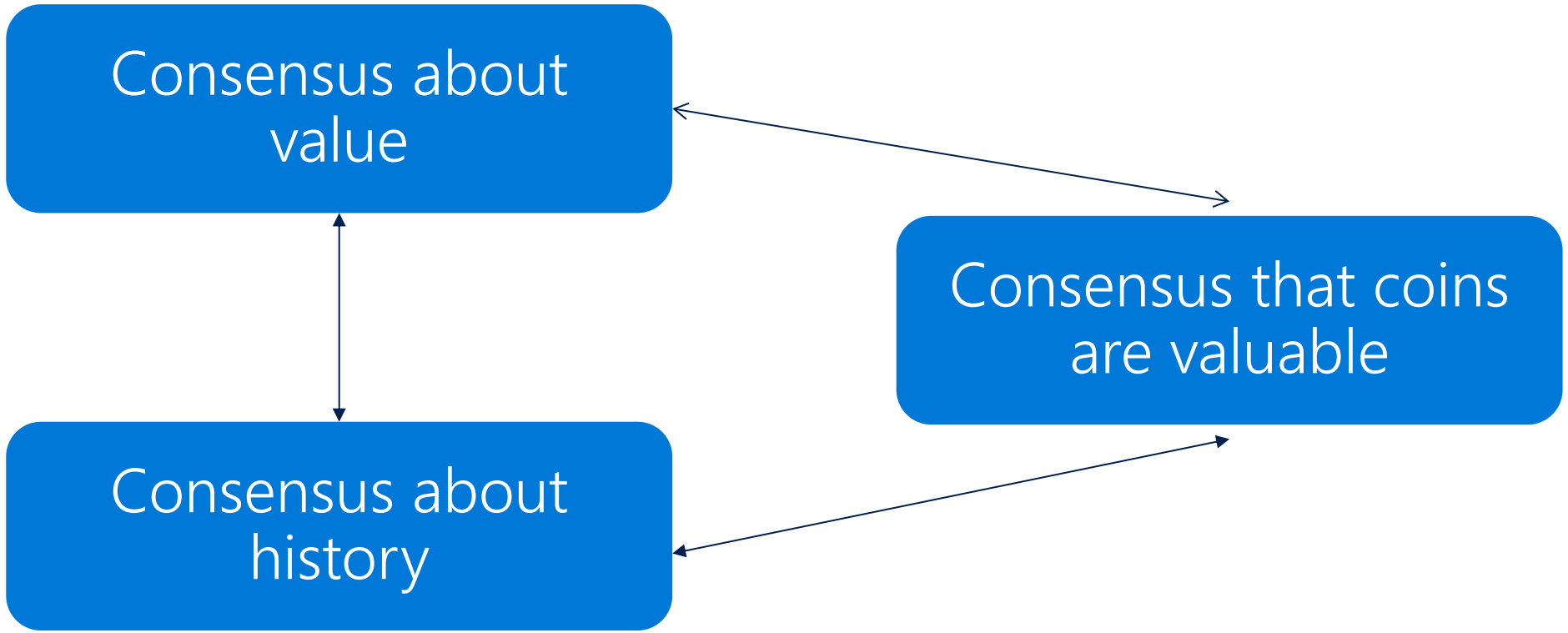
How do we give it a value?

How do we use it?


4111 0166 1329 5787
MONTH / YEAR
VALID THRU 12/18
VISA
Business
JAMES ESCAFE


THIS NOTE IS LEGAL TENDER
FOR ALL DEBTS, PUBLIC AND PRIVATE
JULY 4, 1776.

A successful cryptocurrency has…



Microsoft

Bitcoin

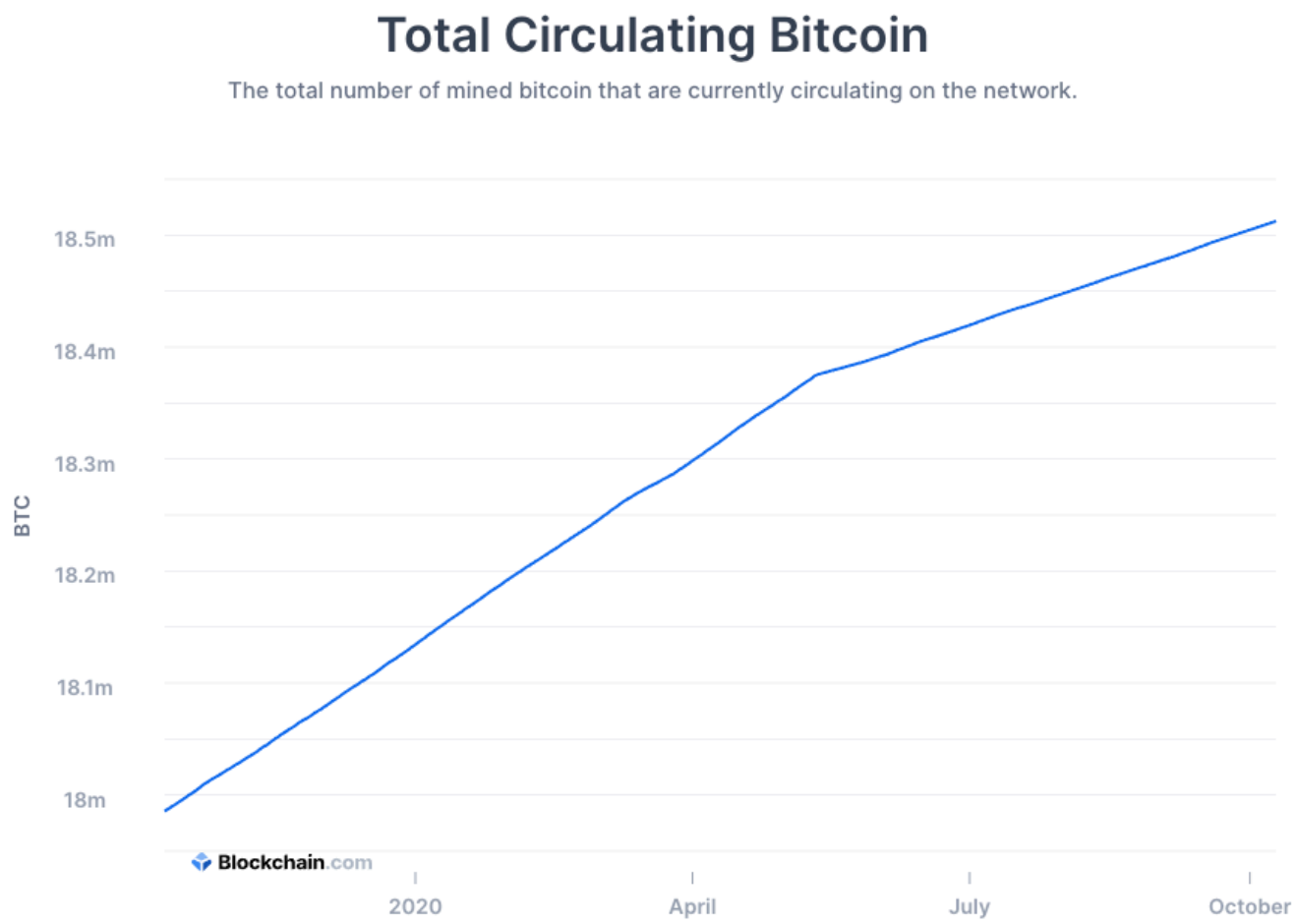
Bitcoin

- Introduced in 2008 by Satoshi Nakamoto
- Provided a white paper and working code
- Built on previous cryptocurrency ideas with several clever new tweaks
- Solves problems of centralization, double-spending, identity, scarcity, consensus and more
- An economic system that rewards participation
- A public transaction ledger

How to participate

- Buy: https://bitcoin.org/en/buy
- Choose your wallet: https://bitcoin.org/en/choose-your-wallet
- Anyone can buy or sell
- Allows user-to-user payment

www.blockchain.com/charts/total-bitcoins



www.blockchain.com/charts/market-price

Bitcoin transactions

- Rule base for verifying using the proof of work algorithm
- Transactions take roughly 10 minutes to verify
- Current block problem becomes more difficult to solve

Double spending problem

- Users try to spend money twice
- Mining process creates consensus about valid transactions

Securing your identity

- Public and private keys
- Use cryptographic signature to sign transactions
- Keys cannot be traced back to your identity

Microsoft

Ethereum

Ethereum

- Vitalik Buterin wanted to evolve the Bitcoin platform
- Programmable, smart-contract-based public blockchain
- Global and open-sourced platform

Ethereum

- Accessible for all
- Decentralized peer-to-peer network
- Censorship-resistant
- Has a currency called Ether (ETH)

Get started with Ethereum

- Buy: https://ethereum.org/eth/
- Wallet: https://ethereum.org/wallets/
- Apps: https://ethereum.org/dapps/

Ethereum transactions

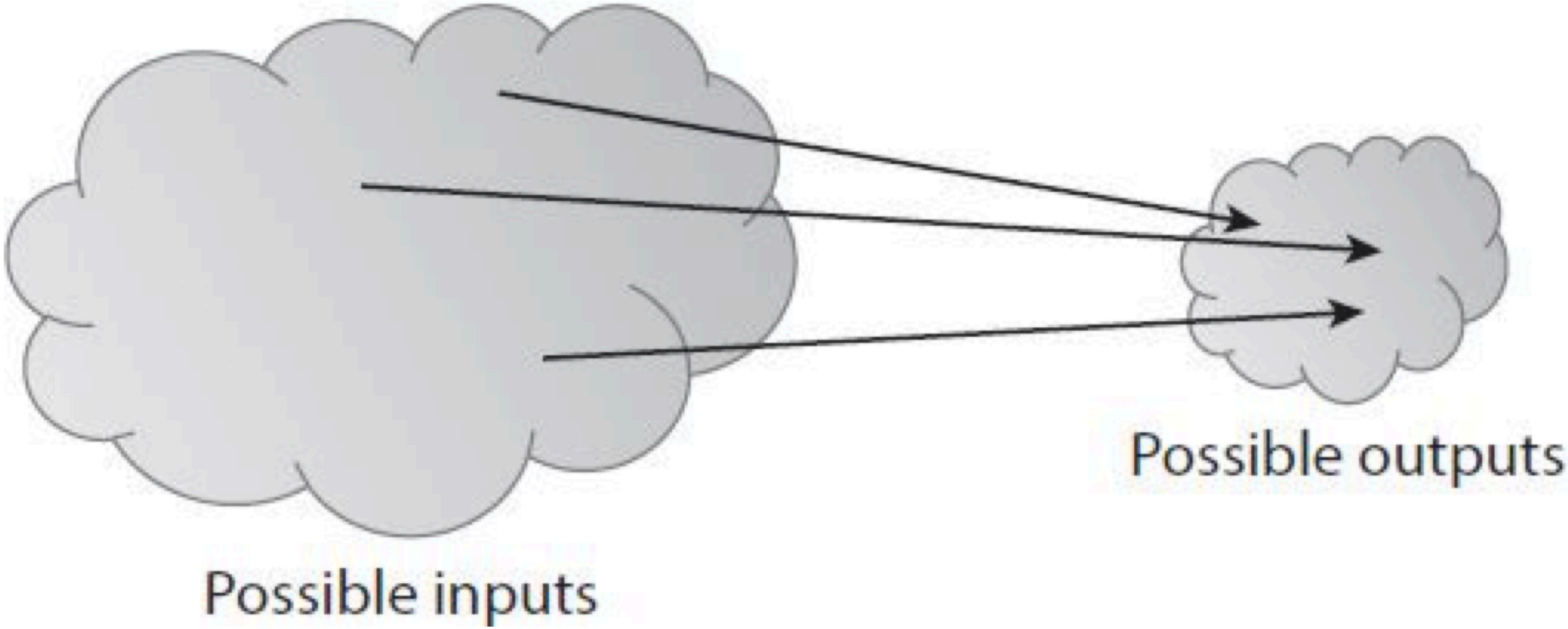
- Currently uses proof of work algorithm to verify
- Miners rewarded with a certain amount of Ether
- Transaction times 10-15 seconds

“The key component is this idea of a Turing-complete blockchain. … As a data structure, it works kind of the same way that Bitcoin works, except the difference in Ethereum is, it has this built-in programming language.”

Introducing Ethereum and Solidity: Foundations of Cryptocurrency and Blockchain Programming for Beginners

Microsoft

Blockchain cryptography



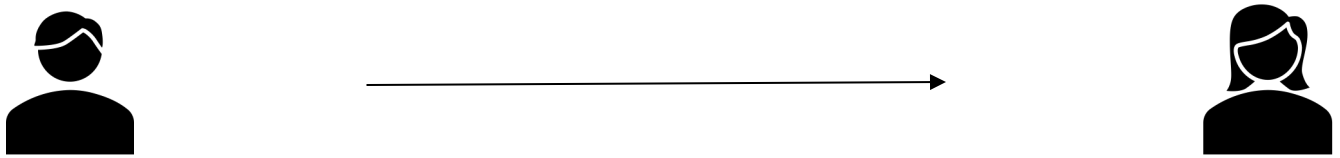
"Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction"

Main principles of hashing functions

- Unfeasible to reverse a hash
- Unfeasible to generate a message for a given hash
- Unfeasible to find two inputs that generate the same hash

```
> cat message.txt
Meet me tomorrow for dinner at Carpe Vino.

> shasum -a 256 message.txt
36f0b87161b4aa29c391b442ca33077eaa2978517ddc181867ff26a5453f6dff
message.txt


> echo "password" | hexdump
0000000 70 61 73 73 77 6f 72 64 0a
0000009


> echo "passwore" | hexdump
0000000 70 61 73 73 77 6f 72 65 0a
0000009



> echo "password" | shasum -a 256
6b3a55e0261b0304143f805a24924d0c1c44524821305f31d9277843b8a10f4e -



> echo "passwore" | shasum -a 256
c78e8a700401d1cded1ee2c8e89d9e1d772783bd2c29e8304bd9ead3cc46b5ca -
```

Hashing a blockchain transaction



- Create a transaction that contains receiver's public key
- Sign transaction with sender's private key

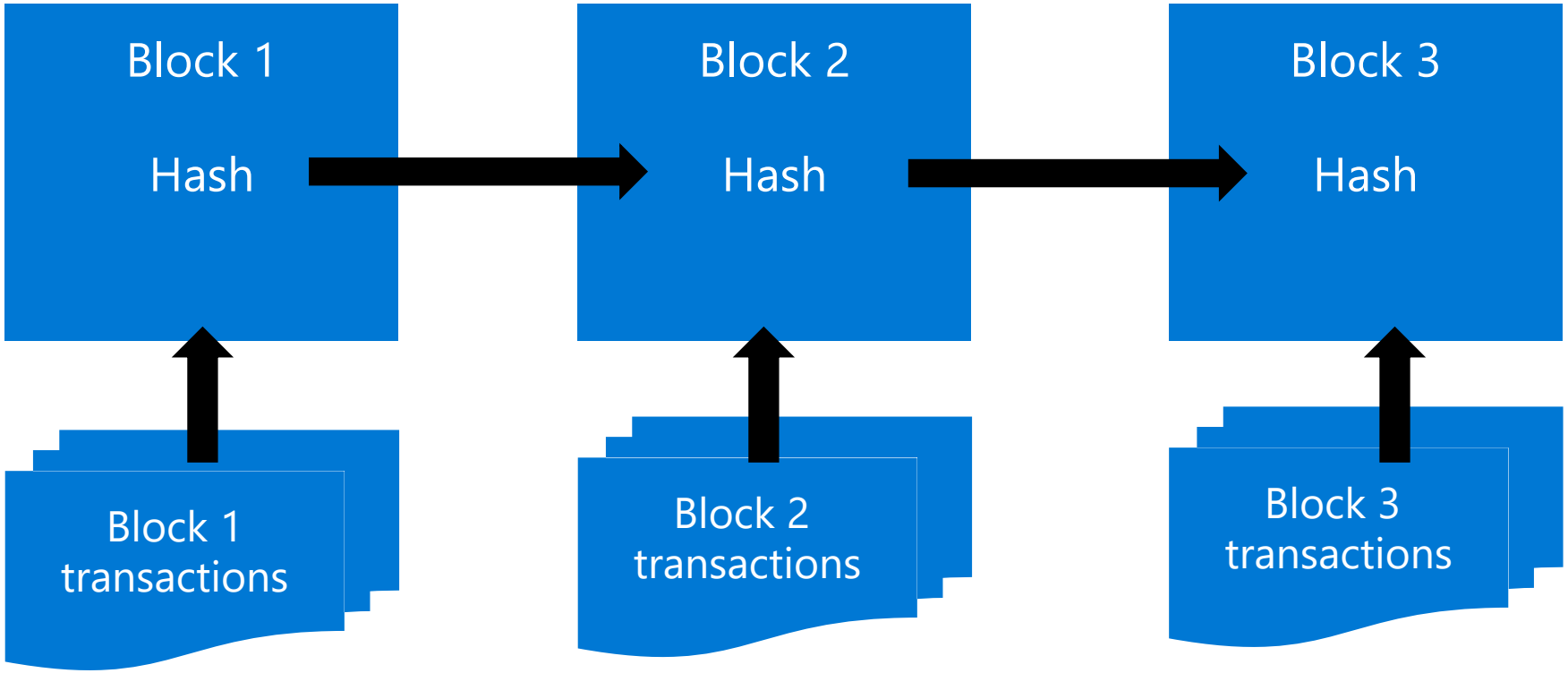
- Checks transactions digital signature with sender's public key
- If hash matches, then transaction is valid

Microsoft

Mining

Current block

- Current block includes the hash of a previous block, which creates a connection



Each block holds at least one transaction

Miners get to select which transactions make up a block

Miners receive a block reward

Bitcoin rewards

- Started at 50 BTC, currently 6.25 BTC
- Around 2140 all Bitcoin will be minted
- Only transaction fees will remain

Bitcoin mining

- Race to find a hash of a block that is less than the current difficulty level
- Block is constructed to include a CoinBase transaction
- Miners profit upon winning the round from CoinBase + Fees
- After all coins are mined, it will just be transaction fees
- Payment to miners is not the point
- Security and validation of the blockchain is the point

Ethereum mining

- Process is similar to Bitcoin where miners solve the current block problem
- Transaction rounds 10-15 seconds
- Number of transactions limited by gas
- Miner receives 2 ETH as a reward
- Over 100 million Ether in circulation

Microsoft

Consensus algorithms

Solving the block problem

No complex math involved

Search **for a 64-digit hex number**

When the computer finds the right hash you win

Proof of work

- Initially, one in 16 hashes would have worked
- Hashing throughput continues to grow
- Set a target of finding a hash less than:
  - 0x1000000000000000000000000000000000000000000000000000000000000000
- Increase the difficulty by setting a new target of:
  - 0x0100000000000000000000000000000000000000000000000000000000000000

Proof of stake

- Achieve consensus from those who put some stake in the ecosystem as a deposit
- No competition to solve block problem
- Validators choose next block
- Validators selected based on an algorithm
- Validator receives a transaction fee

Microsoft

Blockchain transactions

Exploring transactions

Visit: https://www.blockchain.com/explorer to explore helpful information about Bitcoin and Ethereum including the latest blocks and transactions.

Validating transactions

- Check syntax and data structure
- No empty inputs and outputs
- Transaction size (bytes) < maximum block size
- Output value is reasonable range and outputs don't already exist elsewhere (already spent)
- Inputs are valid and >= outputs
- Lock times are reasonable
- Number of signature operations are reasonable
- Locking/unlocking scripts are safe, standard and validating
- Transaction references match to the block or pools

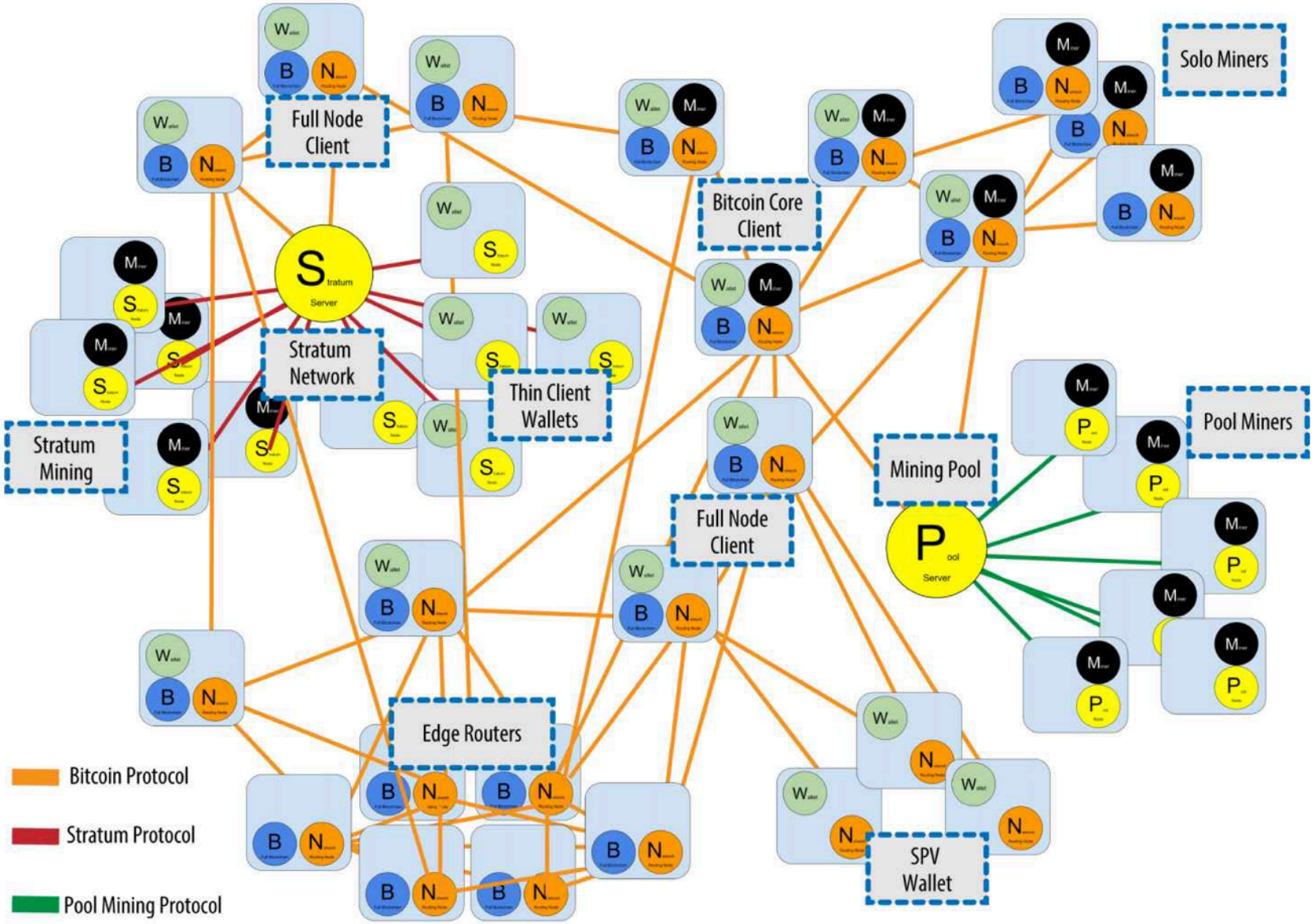
https://blockchain.info/block/000000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f

Microsoft

Blockchain nodes

Nodes

- Represents participants on the network and serve specific purposes
- Nodes come and go
- Anyone can run a node
- There are many different types of nodes



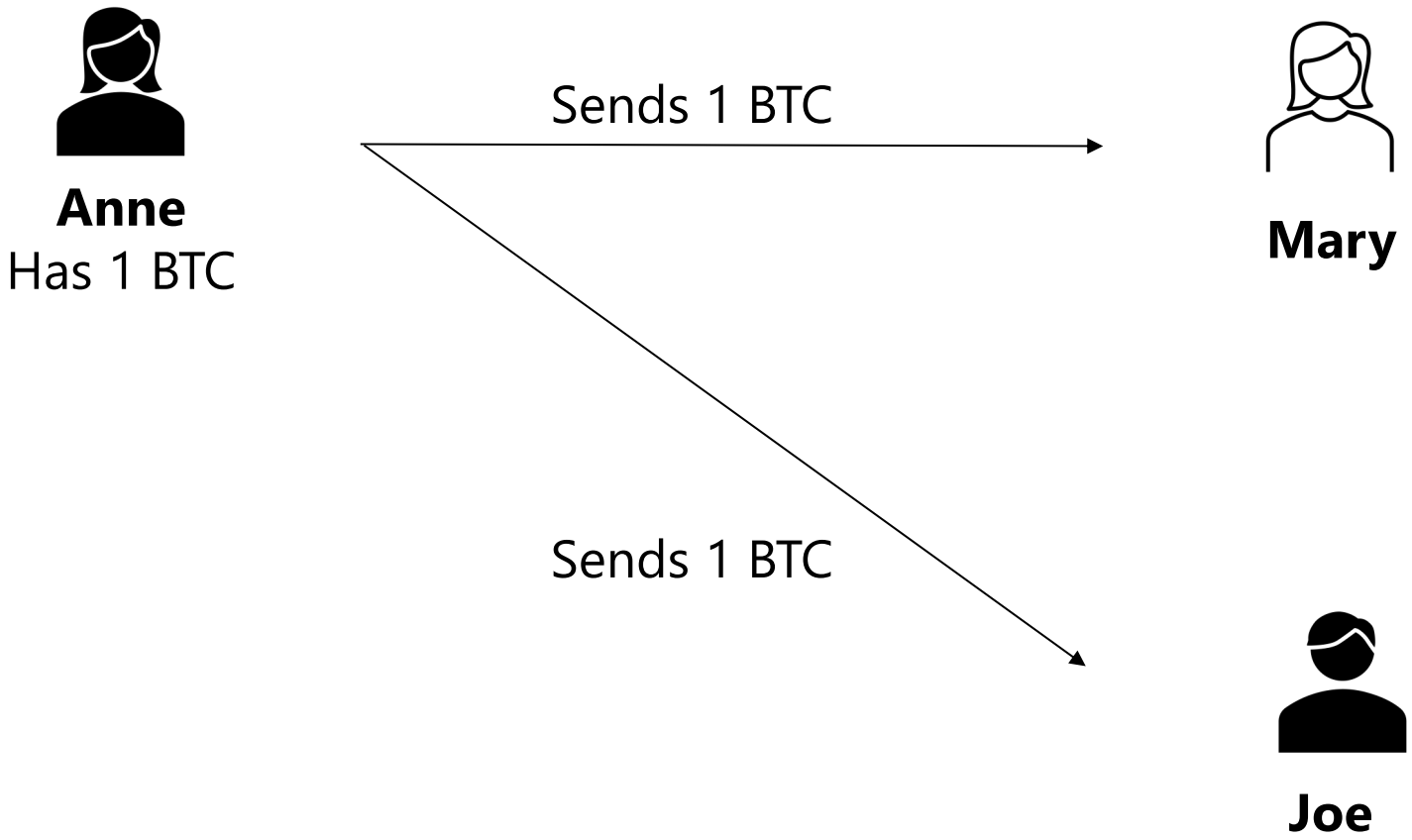
"Mastering Bitcoin"

Microsoft

Double spending

Double spending

- Currency that is spent twice
- Isn't a problem with cash
- Could possibly happen with credit
- This happens when bad actors try to exploit the network


Anne
Has 1 BTC
Sends 1 BTC
Sends 1 BTC
Mary
Joe

Solution to double spending

- Accept transactions in order and reward miners
- Mining and proof of work help prevent this
- Merchants wait for a number of transactions for confirmation

Microsoft

Blockchain use cases

Escrow

- Expedite escrow transactions
- Quickly verify finances
- Reduce fraud
- Provide transparency

Loyalty points

- Digital assets can represent tokens users earn and spend on a platform
- Singapore airlines allows users to convert miles into points that can be spent at major retailers

Voting

- Blockchain-based voting could improve engagement by providing a secure way to vote on mobile devices.
- Voatz is a mobile voting platform that runs on blockchain
- Follow My Vote is a secure online voting platform using an open-source virtual blockchain ballot box

Records

- There are some interesting things that local and state governments are looking into in regards to records
- Illinois is experimenting with blockchain to enhance the security of birth certificates, death certificates, voter registration cards, social security numbers and much more.
- The State of Delaware is archiving public documents and safely securing private records. The next step in Delaware’s initiative is to begin implementing smart contracts

Supply chain

- Blockchain is being used with supply chain to better understand the transaction of goods across each step of the process and track goods digitally.

- DHL is using it to keep a digital ledger of shipments and maintain integrity of transactions.

- Starbucks tracks the origins of their coffee beans and the transport of those beans from farm to store.

Microsoft

Solidity

About Solidity

- Object-oriented
- High-level
- Influenced by C++, Python, JavaScript
- Targets the Ethereum Virtual Machine
- Statically typed

Primary structures

- State variables
- Functions
- Function modifiers
- Events
- Struct Types
- Enum Types
- Mappings

Microsoft

Smart contracts

About smart contracts

- Programmatically defined
- Specify rules, requirements, and rewards
- Provide autonomy, trust, savings, safety, and efficiency
- Most prominently used with Ethereum

Microsoft

Truffle Suite

Truffle Suite

- Used to make blockchain development easier
- Provides the following tools:
  - Truffle Teams
  - Truffle
  - Ganache
  - Drizzle
- Visit: https://www.trufflesuite.com to learn more

Microsoft

OpenZeppelin

About OpenZeppelin

- OpenZeppelin provides tools to write, deploy and operate decentralized applications
- Provides two different products:
  - Contracts
  - SDK

Microsoft

Azure solutions

Solutions offered

- Azure Blockchain Development Kit for Etheruem
- Azure Blockchain Service
- Azure Blockchain Workbench

Microsoft