CS 5594: BLOCKCHAIN TECHNOLOGIES

Spring 2024

THANG HOANG, PhD

BLOCKCHAIN OVERVIEW

Outline

- Traditional Transactions
- Traditional Trust Models and Issues
- Why Blockchain? What is Blockchain?
- Blockchain Components and Useful Terminologies

Traditional Transaction Model

$10,000

send(Alice, $10K)

notify TX received

TRUSTED THIRD PARTIES

Account #	Name	Balance
2136544	Bob	$100,000
32136545	Doge	$500,000
32136546	Eve	$1,000,000

A

$10,000

B

Account #	Name	Balance
32136521	Alice	$100,000
32136522	Carol	$500,000
32136523	Dave	$1,000,000

Ledger A

Account #	Destination	Amount
32136544	32136521	- $60,000
32136544	32136521	+ $200,000
32136544	32136521	- $10,000

Transaction records

Ledger B

Account #	Destination	Amount
32136521	32136544	+ $60,000
32136521	32136544	- $200,000
32136521	32136544	+ $10,000

Traditional Transaction Issues

Pros

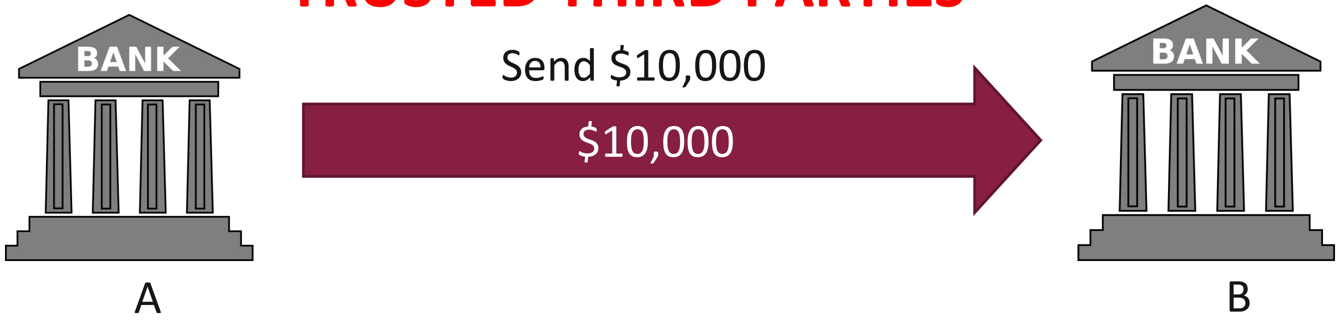
- **Trust** & Integrity
- Centralized
- Standardized processes & procedures

Cons

- Security, Privacy, **Trust**
- Intermediation
  - Expensive, efficiency
- Centralized
  - Counterparty risk/fraud
  - Single point of failure

TRUSTED THIRD PARTIES

Account #	Name	Balance
2136544	Bob	$100,000
32136545	Doge	$500,000
32136546	Eve	$1,000,000



Account #	Name	Balance
32136521	Alice	$100,000
32136522	Carol	$500,000
32136523	Dave	$1,000,000

Ledger A

Account #	Destination	Amount
32136544	32136521	- $60,000
32136544	32136521	+ $200,000
32136544	32136521	- $10,000

Ledger B

Account #	Destination	Amount
32136521	32136544	+ $60,000
32136521	32136544	- $200,000
32136521	32136544	+ $10,000

Traditional Transaction Issues

- Centralized systems suffer from many factors
  - **Trust**
  - Security and Privacy
  - Fraud, single point of failure
  - Operational cost to maintain trusted entities

What is Trust?

- All decisions we make everyday are based on a degree of trust
  - Driving car
  - Buying groceries
  - Online purchase
- Trust reduces operational cost
  - Without trust, one must verify the reliability of everything
  - Impossible to verify everything

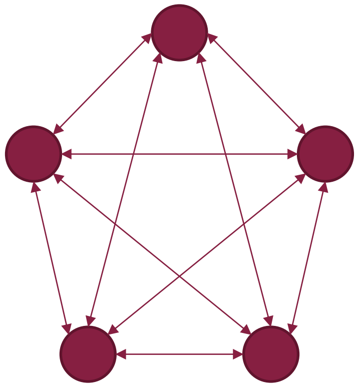
What is Trust?

- Trust is gray-scale. There are different degrees of trust
  - Full trust
  - Semi-trust
  - Weak trust
- Trust is a two-sided coin
  - A complex psychological state combined of rational and emotional factors
  - Acceptance of uncontrolled and unquantified risk
  - “Trust begins where prediction ends.” – David Lewis and Andrew Weigert

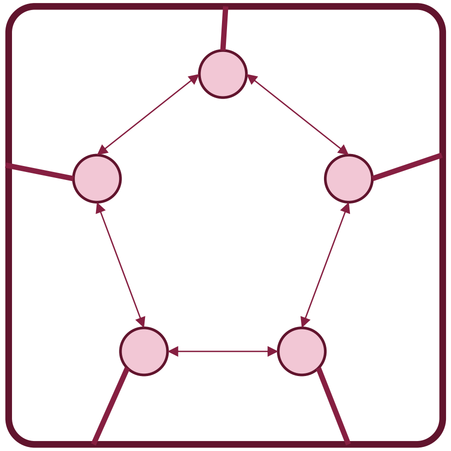
Conventional Trust Models

Three trust architectural models:

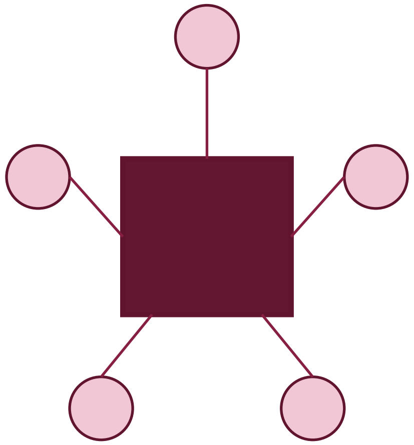
- **P2P**: I trust you because of *you*
- **Leviathan**: I trust you because of legal contracts established by trusted authorities
- **Intermediary**: I trust you because of trusted platform we both operate on



P2P



Leviathan

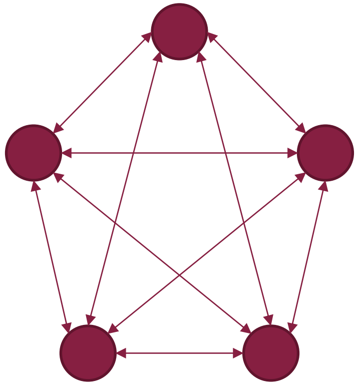


Intermediary

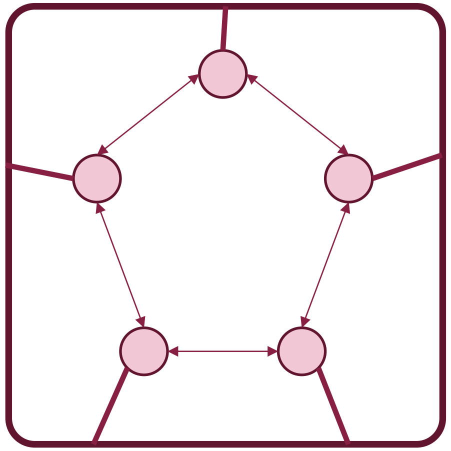
Conventional Trust Models

Three trust components per transaction

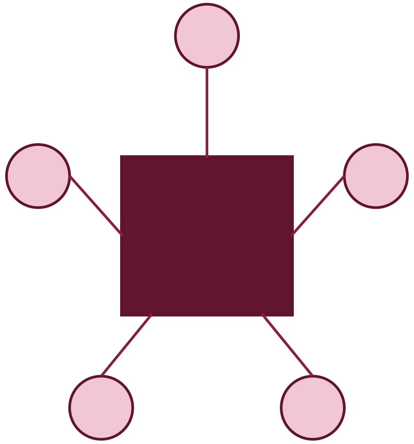
- Counterparty (P2P)
- Dispute resolution mechanism (CA)
- Intermediary



P2P



Leviathan



Intermediary

A Crisis of Trust

- Trust forms the ways we interact and behave
  - High-trust societies are powerful and outperform low-trust societies
- **However, trust is in crisis!!!**
  - Trust level is decreasing over recent years
  - 80% of Americans do not trust government, 67% of them do not trust each other

A Crisis of Trust

“The root problem with conventional currency is all the trust that’s required to make it work. The central bank must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust.”

- Satoshi Nakamoto

A Crisis of Trust

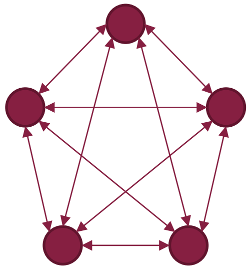
Trust fails because of

- **Direct violation:** non-reputed organization
  - Lend somebody money
- **Opportunistic behavior**: When benefits outweigh trust factors
  - Facebook–Cambridge Analytica scandal
- **Systemic collapse**: Unwanted behaviors (compromised, corrupted)
  - Equifax data breach, Apple iCloud, Sony PlayStation Network

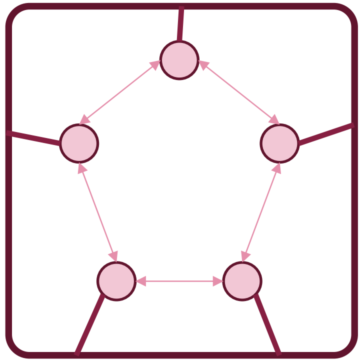
Extremely hard to restore/recover trust when it fails

Blockchain: A Revolution of Trust

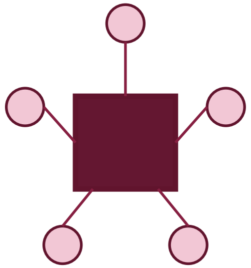
- **Blockchain**: a revolution of trust
  - “Trustless trust” – Reid Hoffman (LinkedIn founder)
  - A trusted network without trusting anyone



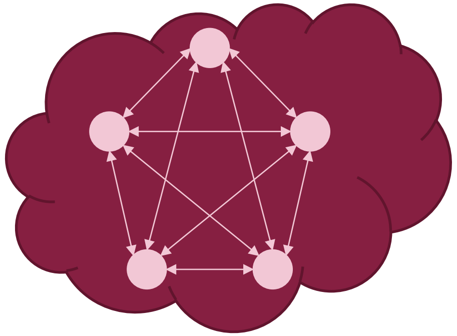
P2P



Leviathan



Intermediary



Blockchain

Blockchain

An open network where everybody can establish trust themselves

- **Decentralized**: Trust distributed across multiple entities
- **Open**: Anyone can participate and verify the integrity and trustworthiness
- **Anonymity**: Everybody identity remains hidden
- **Enhanced confidentiality, integrity & privacy**
- **Eliminate centralized party**: Reduced operational cost

Blockchain

Blockchain establish trust via software programs

- **Anonymity**
  - Everybody is equal and anonymous
  - Eliminate impacts of counterparty identify in justifying the trustworthiness
- **Decentralized** platform with reward incentive mechanisms
  - Encourage honest and trustworthy behavior of many participants
- **Smart contract** with predefined algorithms
  - Dispute resolution

Blockchain

- In blockchain network, nothing to be trustworthy except its output
- All transactions validated via rigorous mathematical proofs
  - Anybody can verify proofs publicly

In Proof We Trust

Why Blockchain?

- **Enhanced Security and Reliability**
  - via decentralization model and cryptography
  - Centralization more vulnerable to corruptions, errors, mistakes
- **Tamper-Proof**
  - Data alteration remains extremely difficult

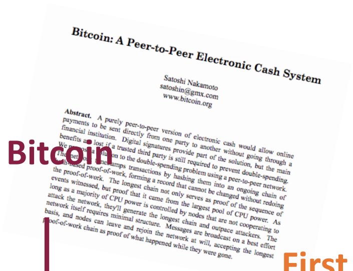
Why Blockchain?

- **Digital Freedom**
  - Complete anonymity and transaction security and confidentiality
  - Transactions direct to recipients without routed to a trusted entity (e.g., bank)
  - Trusted entity always comes with risk and cost
- **Improved Transparency**
  - Everyone can verify and track transactions
  - Nobody can modify transactions on their own

Why Blockchain?

- **Better Efficiency and Reduced Cost**
  - Automated process
  - Minimal transaction cost
  - No need of maintaining central authority

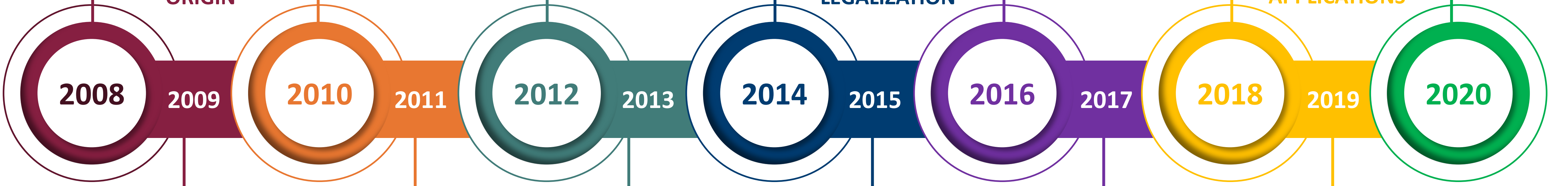
Blockchain Evolution



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. 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. 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. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.



Bitcoin

BTC Genesis block created

First BTC **transaction** (10,000 BTC for a pizza!)

1 BTC = 1 USD

Frauds and attacks explored

Silk Road opened

1 BTC = 100 USD

BTC ATM debuted

Ethereum (ETH)

Ethereum White Paper
A NEXT GENERATION SMART CONTRACT & DECENTRALIZED APPLICATION PLATFORM
By Vitalik Buterin

When Satoshi Nakamoto first set the Bitcoin blockchain into motion in January 2009, he was simultaneously introducing two radical and untested concepts. The first is the "bitcoin", a decentralized peer-to-peer online currency that maintains a value without any backing, intrinsic value or central issuer. So far, the "bitcoin" as a currency unit has taken up the bulk of the public attention, both in terms of the political aspects of a currency without a central bank and its extreme upward and downward volatility in price. However, there is also another, equally important, part to Satoshi's grand experiment: the concept of a proof of work-based blockchain to allow for public agreement on the order of transactions. Bitcoin as an application can be described as a first-to-file system: if one entity has 50 BTC, and simultaneously sends the same 50 BTC to A and to B, only the transaction that gets confirmed first will process. There is no intrinsic way of determining from two transactions which came earlier, and for decades this stymied the development of decent digital currency. Satoshi's blockchain was the first credible decentralized solution. And n rapidly starting to shift toward this second part of Bitcoin's technology, and how the bl used for more than just money.

Commonly cited applications include using on-blockchain digi financial instruments ("colored coins"), the owners non-fungible assets such as domain name decentralized exchange, financia reputation systems. Anot

Paypal, MS accept BTC payment

Devastating attacks on Mt.Gox. BTC price cratered

ETH Genesis block created

Linux unveils **Hyperledger,** BC protocol for decentralized apps

Bugs in **ETH DAO** code exploited

1 BTC = 10,000 USD

Block.one unveils **EOS**: new BC protocol for decentralized apps

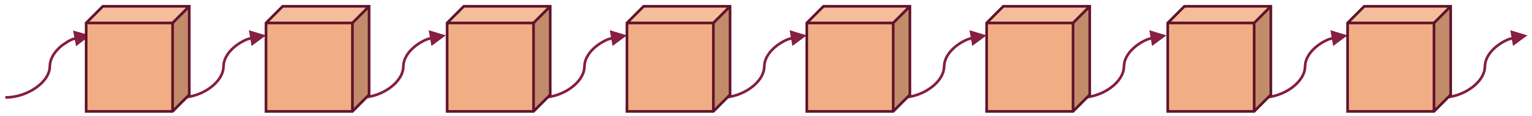
Dapps

Mainstream Adoption
Government
Central Banks

Widescale Adoption
Life Sciences
Healthcare
Supply chains
Energy resources

What is Blockchain?

- First, Bitcoin is not Blockchain
  - Bitcoin is a digital currency that uses blockchain as the underlying data structure
- Blockchain is a data structure where data blocks are linked together
- Data blocks in the chain cannot be deleted or altered (**Immutability**)

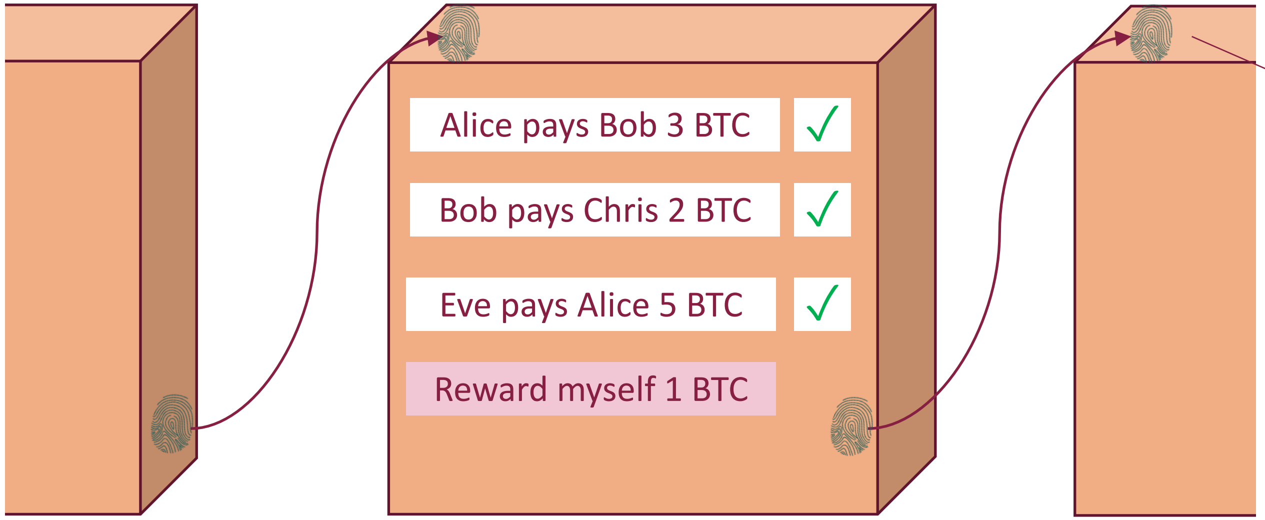


What is Blockchain?

- Blockchain is a <u>comprehensive system</u> consisting of
  - Transactions
  - Immutable ledgers
  - Decentralized network
  - Data encryption/decryption
  - Consensus mechanisms
  - Smart contracts

What is Blockchain?

- Blockchain permits transactions to be gathered and recorded in the block
- Blocks are chained in chronological order via cryptographic hash

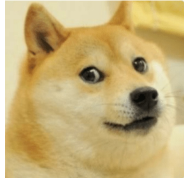


Block header contains a unique crypto hash

How Blockchain Works?

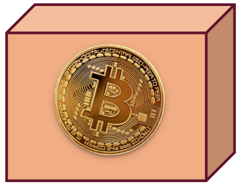
In digital transaction…

D wants to send money to C



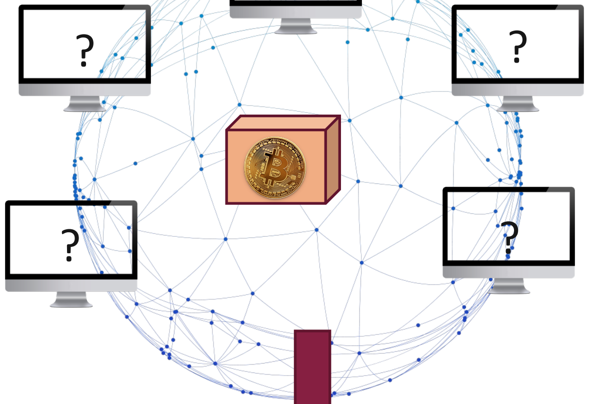
D

The **transaction** Tx is represented as a block

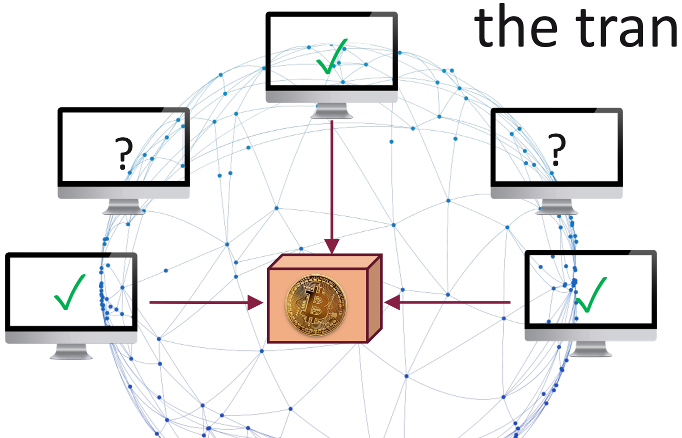


BC block

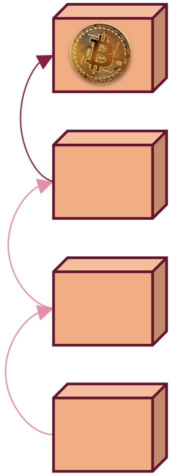
The block is broadcast to all the **distributed nodes** in the network



Sufficient nodes **verify and approve** the transaction



Tx is appended to Blockchain



BC

C receives the money

C

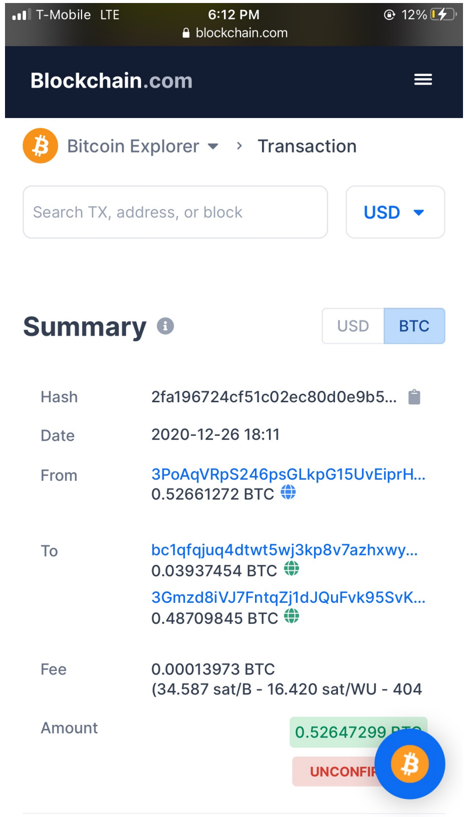
Types of Blockchain

- **Public** and **private**
- Many mechanisms in public BC are not needed in private BC (handled by legal contracts)

Characteristic	Public blockchain	Private blockchain
Access	Anyone can read/write	Only private group can read/write
Authority	Decentralized	Partially Decentralized
Tx Speed	Slow	Fast
Consensus	Permissionless	Permissioned
Identity	Anonymous	Known
Efficiency	Low	High
Immutability	Full	Partial
Examples	₿ ⟠	ripple Quorum HYPERLEDGER

Blockchain Transactions

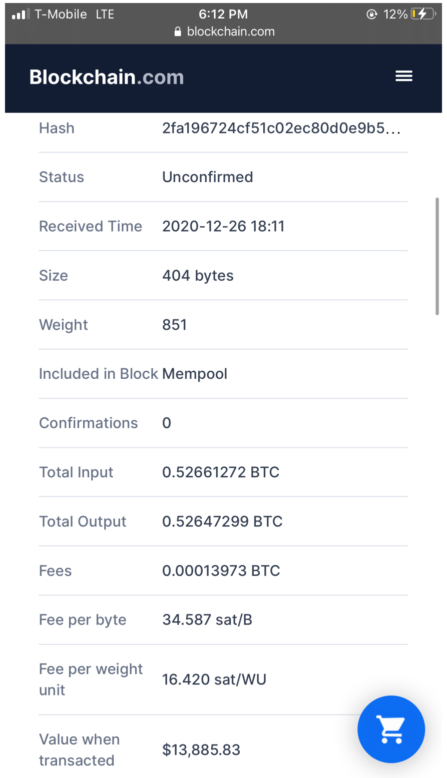
- Smallest element
- Record every decision and action taken
- Proof of history, provides provenance



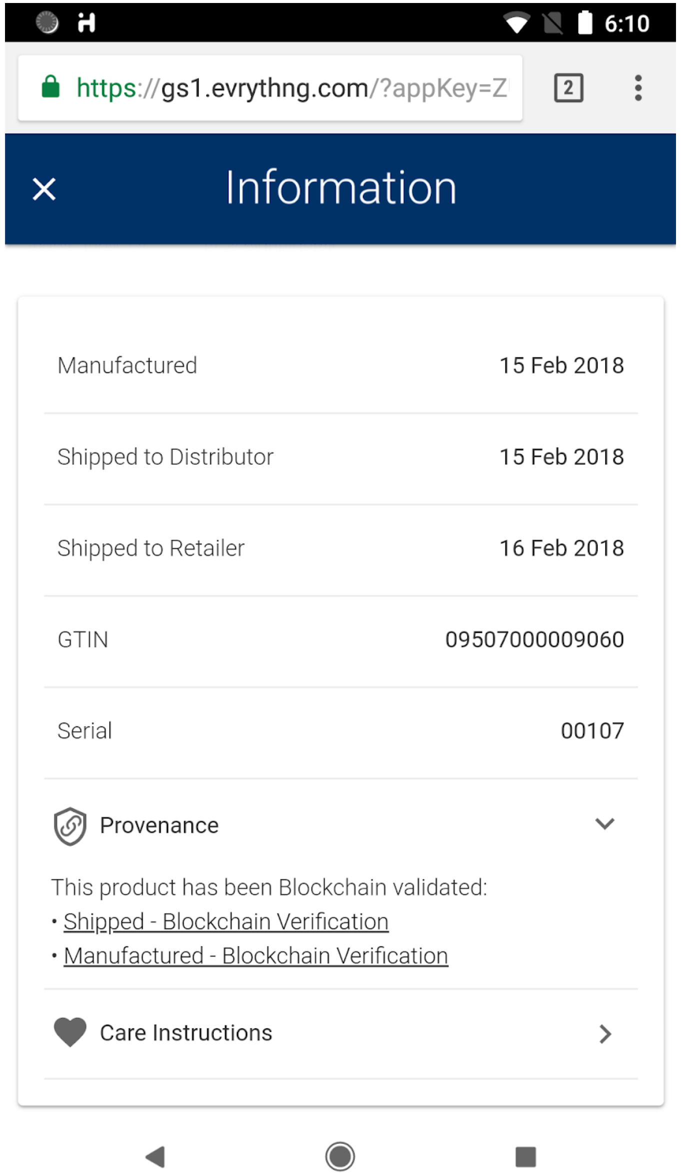
Summary

USD BTC

Hash	2fa196724cf51c02ec80d0e9b5...
Date	2020-12-26 18:11
From	3PoAqVRpS246psGLkpG15UvEiprH... 0.52661272 BTC
To	bc1qfqjuq4dtwt5wj3kp8v7azhxwy... 0.03937454 BTC 3Gmzd8iVJ7FntqZj1dJQuFvk95SvK... 0.48709845 BTC
Fee	0.00013973 BTC (34.587 sat/B - 16.420 sat/WU - 404
Amount	0.52647299 BTC UNCONFI



Hash	2fa196724cf51c02ec80d0e9b5...
Status	Unconfirmed
Received Time	2020-12-26 18:11
Size	404 bytes
Weight	851
Included in Block	Mempool
Confirmations	0
Total Input	0.52661272 BTC
Total Output	0.52647299 BTC
Fees	0.00013973 BTC
Fee per byte	34.587 sat/B
Fee per weight unit	16.420 sat/WU
Value when transacted	$13,885.83



Information

Manufactured	15 Feb 2018
Shipped to Distributor	15 Feb 2018
Shipped to Retailer	16 Feb 2018
GTIN	09507000009060
Serial	00107

Provenance

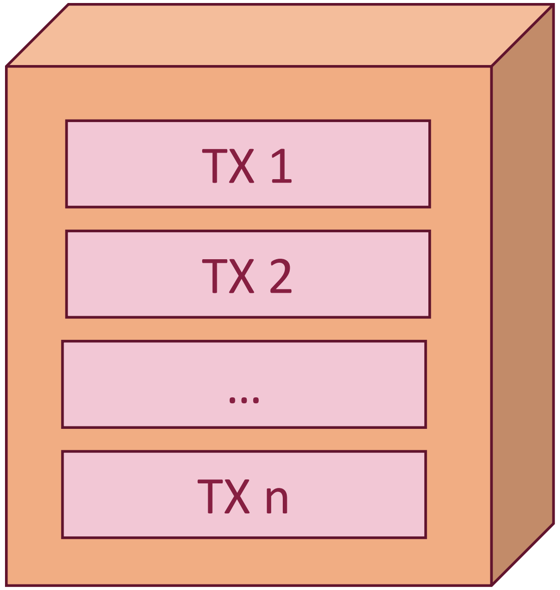
This product has been Blockchain validated:
- Shipped - Blockchain Verification
- Manufactured - Blockchain Verification

Care Instructions

Image from https://evrythng.com/

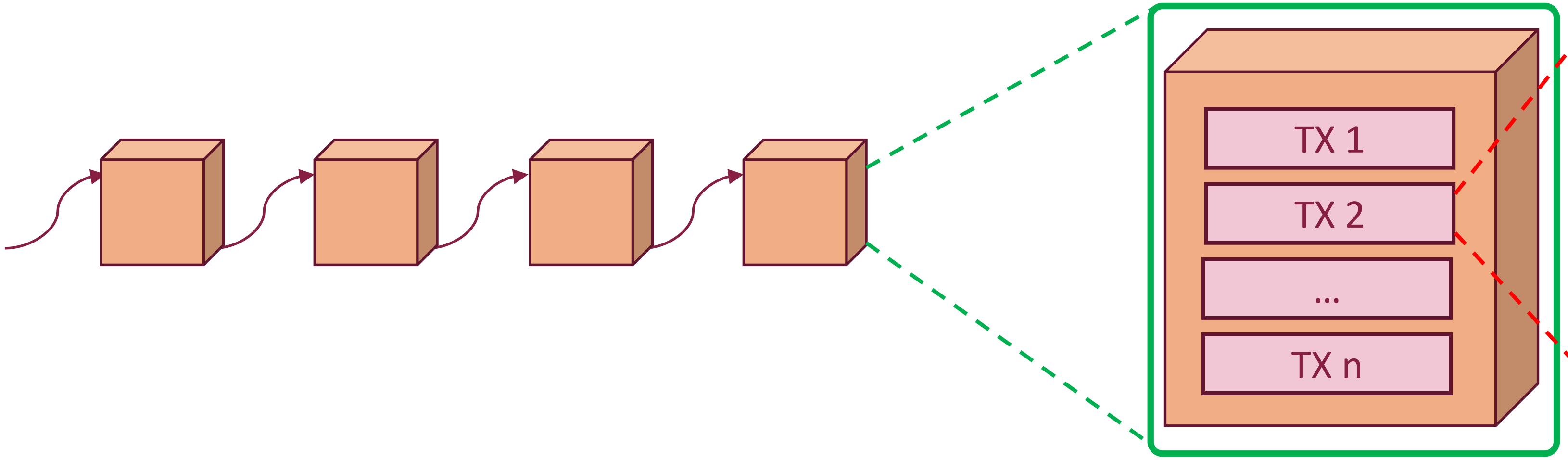
Blockchain “Block”

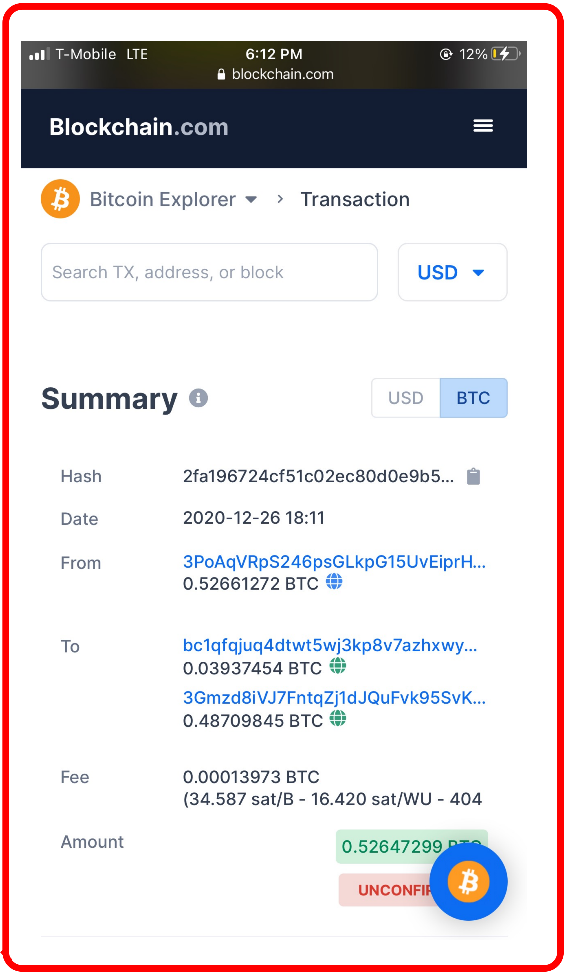
- Contain multiple transactions
  - The transaction is immutable/indelible
- Write and Read-Only
- Once a block is chained, it is extremely difficult to change
  - Modification possible
  - Rework on all the subsequent blocks and consensus for each block



Chain of Blocks

- Contain multiple blocks
- Blocks linked using cryptography
- An instance of distributed ledger





Summary

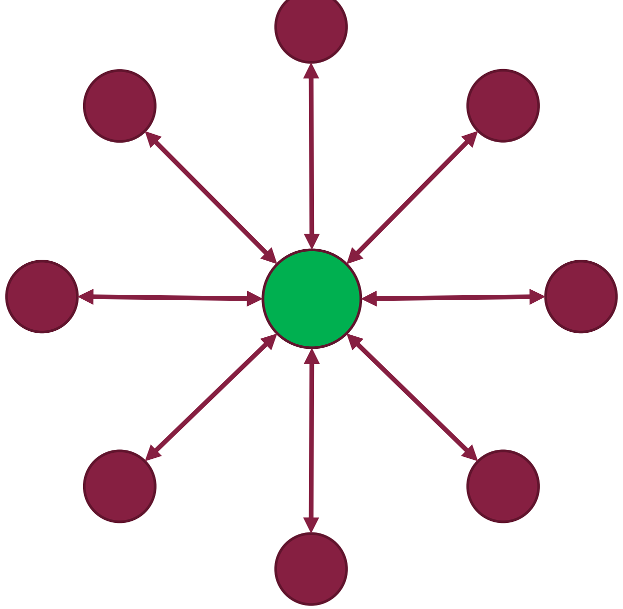
USD BTC

Hash	2fa196724cf51c02ec80d0e9b5...
Date	2020-12-26 18:11
From	3PoAqVRpS246psGLkpG15UvEiprH... 0.52661272 BTC
To	bc1qfqjuq4dtwt5wj3kp8v7azhxwy... 0.03937454 BTC 3Gmzd8iVJ7FntqZj1dJQuFvk95SvK... 0.48709845 BTC
Fee	0.00013973 BTC (34.587 sat/B - 16.420 sat/WU - 404
Amount	0.52647299 BTC UNCONFI

Distributed Network

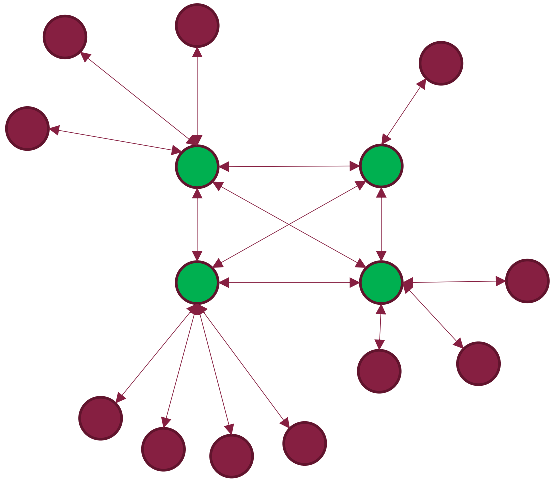
- Blockchain operates on a decentralized/distributed P2P network
- Each node stores a copy of the ledger
  - Distributed Ledger

Centralized Network



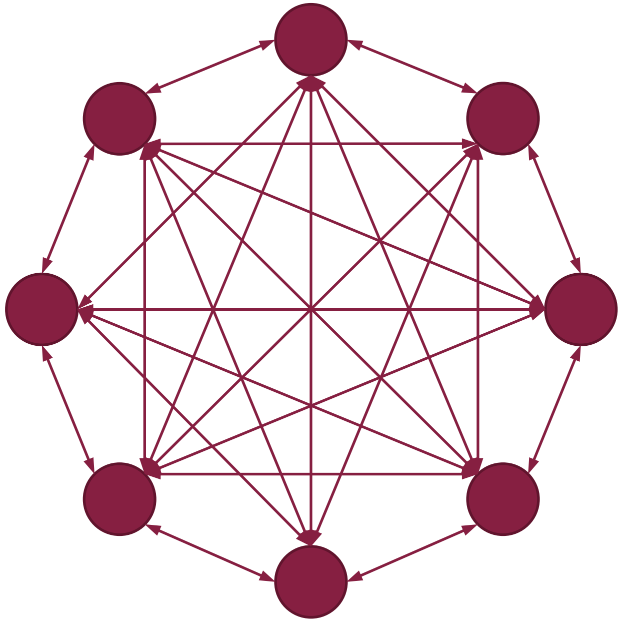
nodes interact with a single central node

Distributed Network



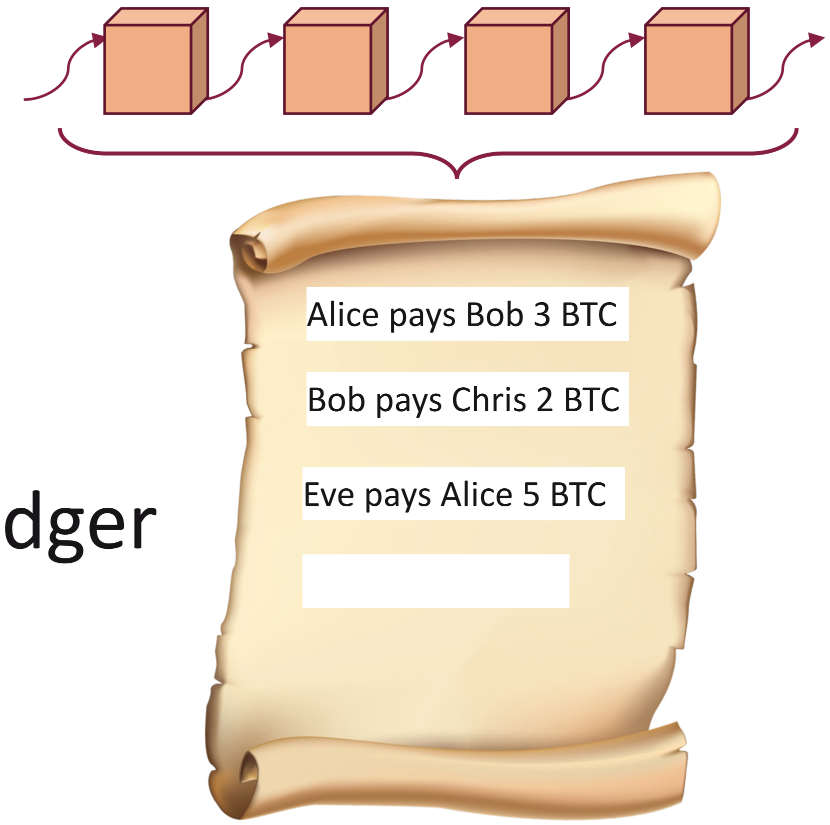
nodes interact with some central nodes

Decentralized Network



Nodes interact with each other directly

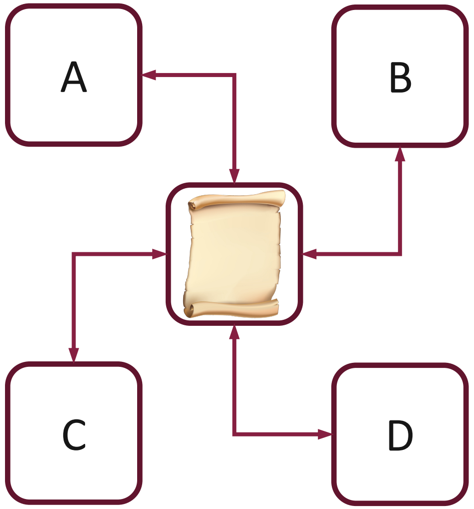
Distributed Ledger



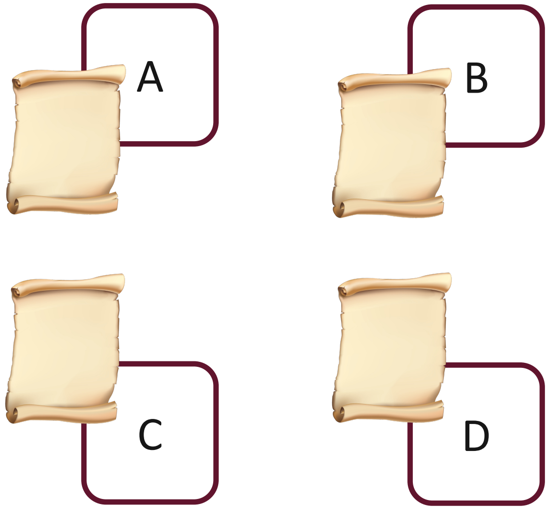
Blockchain is a <u>distributed ledger</u>

- **Centralized ledger:** stored by a central node
- **Distributed ledger**: stored in every node
  - All nodes agree on the true state of the ledger (via a consensus protocol)

Centralized ledger



Distributed ledger



Distributed Ledger

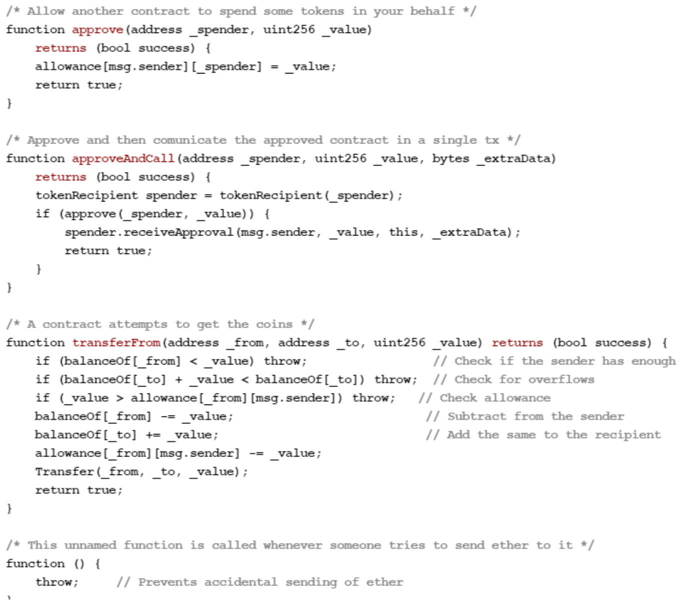
- Keep track of all transactions performed in the network
- Can be encrypted for confidentiality
- Can be used without by individuals without a central authority
- **Immutable:** Ledger records are very difficult to be altered
  - Changing a record in the ledger requires a consensus from all participants
  - Rework on all subsequent records

Distributed Consensus

- Ensure the blocks in blockchain are valid and truthful
- Prevent malicious adversaries from system compromise and chain-forking
- Many consensus protocols, each with different pros and cons
  - Proof of Work (PoW), Proof of Stake (PoS), Proof of Elapsed Time (PoET), Proof of Activity (PoA), Proof of Burn (PoB)
  - Paxos, BFT, Streamlet
- We will explore many of blockchain consensus protocols throughout this course

Smart Contract

- A program running in a secure environment that controls the transfer of digital assets between parties under certain conditions
- Contract encoded into blockchain
- Enable broader blockchain applications beyond cryptocurrencies



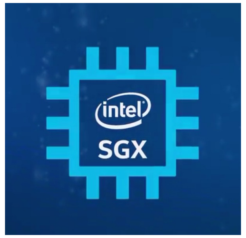
```
/* Allow another contract to spend some tokens in your behalf */
function approve(address _spender, uint256 _value)
    returns (bool success) {
    allowance[msg.sender][_spender] = _value;
    return true;
}

/* Approve and then comunicate the approved contract in a single tx */
function approveAndCall(address _spender, uint256 _value, bytes _extraData)
    returns (bool success) {
    tokenRecipient spender = tokenRecipient(_spender);
    if (approve(_spender, _value)) {
        spender.receiveApproval(msg.sender, _value, this, _extraData);
        return true;
    }
}

/* A contract attempts to get the coins */
function transferFrom(address _from, address _to, uint256 _value) returns (bool success) {
    if (balanceOf[_from] < _value) throw;                 // Check if the sender has enough
    if (balanceOf[_to] + _value < balanceOf[_to]) throw;  // Check for overflows
    if (_value > allowance[_from][msg.sender]) throw;   // Check allowance
    balanceOf[_from] -= _value;                          // Subtract from the sender
    balanceOf[_to] += _value;                            // Add the same to the recipient
    allowance[_from][msg.sender] -= _value;
    Transfer(_from, _to, _value);
    return true;
}

/* This unnamed function is called whenever someone tries to send ether to it */
function () {
    throw;     // Prevents accidental sending of ether
}
```

Source: https://blockgeeks.com/guides/smart-contracts/



Smart Contracts

- Smart contract is a computer program that
  - **Defines** rules
  - **Enforces** obligations and penalties
  - **Executes** actions required by clauses
  - **Autonomous** without ownership
  - **Secure**
- Written in a high-level programming language (e.g., Solidity)

Blockchain Techniques	Smart Contracts?	Language
Bitcoin	✗	C++
Ethereum	✓	**Solidity**
Hyperledger	✓	GoLang, C++, etc

Encryption

- Confidential transaction
- Prevent sensitive information to be leaked to malicious attacker
- Blocks can be partially or fully encrypted
  - Symmetric/asymmetric encryption
- Some (private) blockchains employ access control for visibility

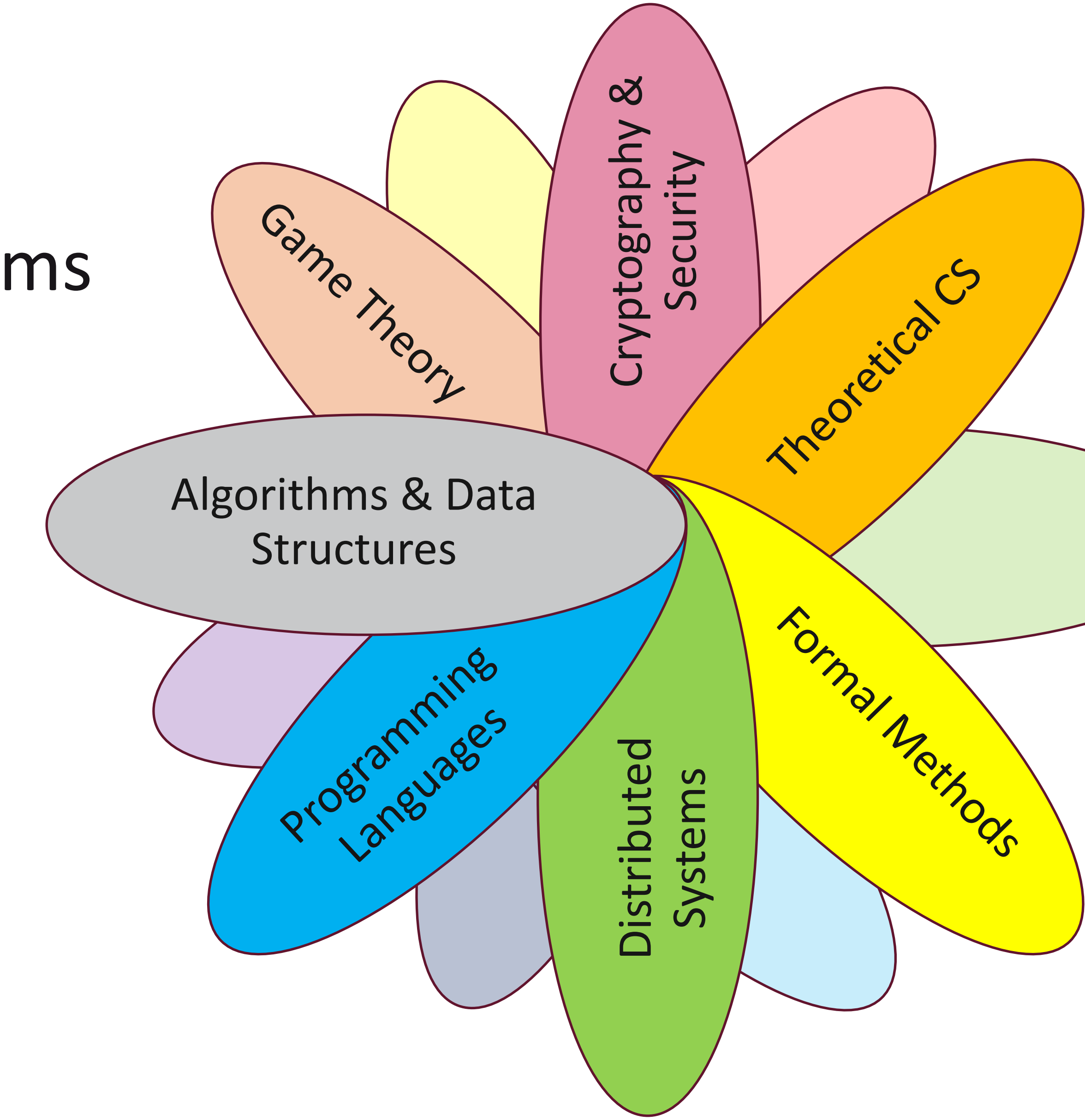
Challenges

- Energy consumption
- Resource-wasteful
- Immaturability
  - Scalability
  - Standardization
  - Awareness and Understanding
- Interaction with legacy infrastructure

Summary

- Blockchain is interdisciplinary
- Cryptography and Distributed Systems are fundamental building blocks

Operation	Crypto Techniques
Init & Broadcast Transactions	• Digital Signature • Private/Public Keys
Transaction Validation	• Proof-of-Work
Chaining blocks	• Hash Function


Game Theory
Cryptography & Security
Theoretical CS
Algorithms & Data Structures
Formal Methods
Programming Languages
Distributed Systems