CS61065: Theory And Applications of Blockchain

Evolution of the Blockchain Technology

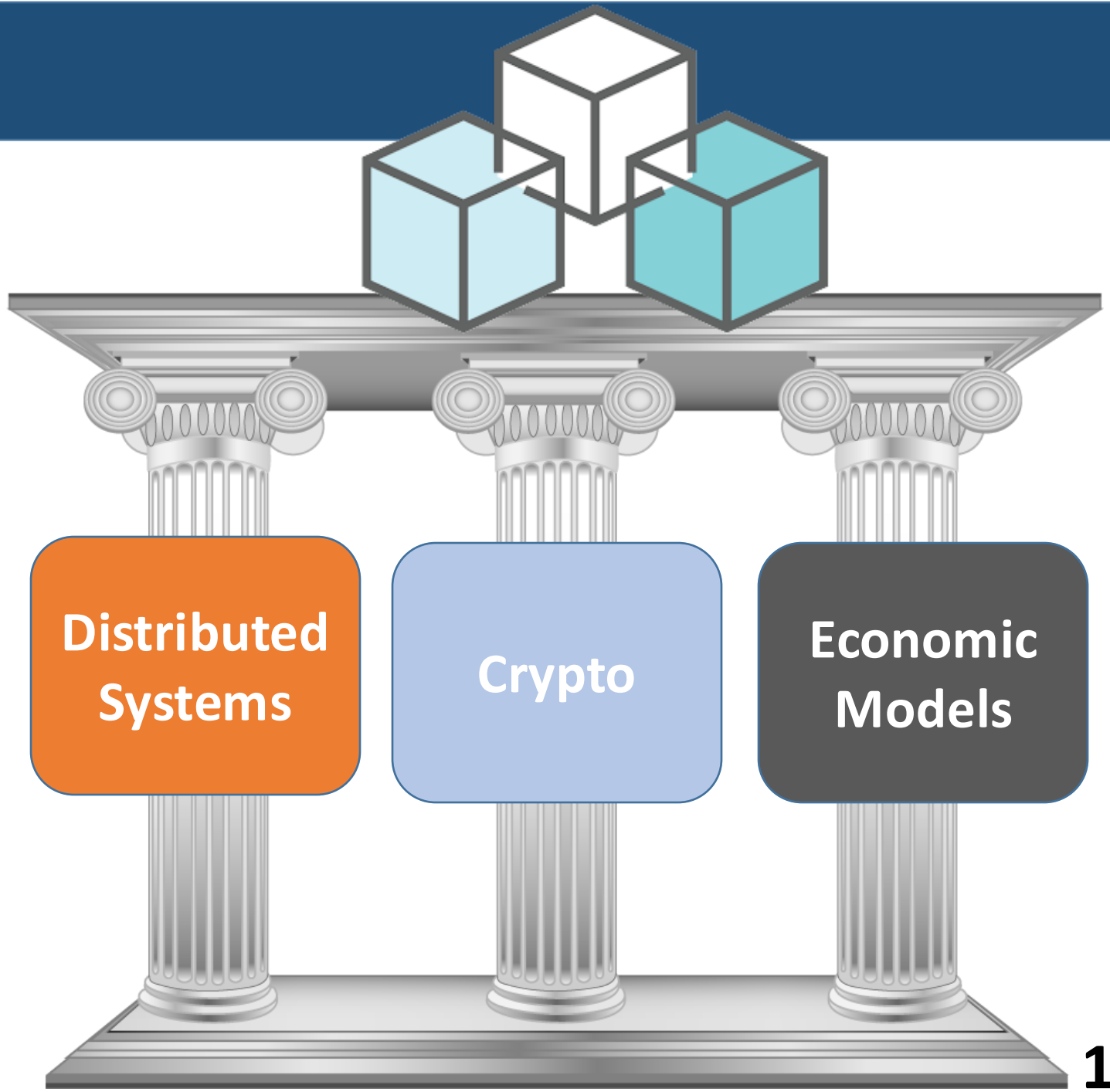
Department of Computer Science and Engineering

INDIAN INSTITUTE OF TECHNOLOGY KHARAGPUR

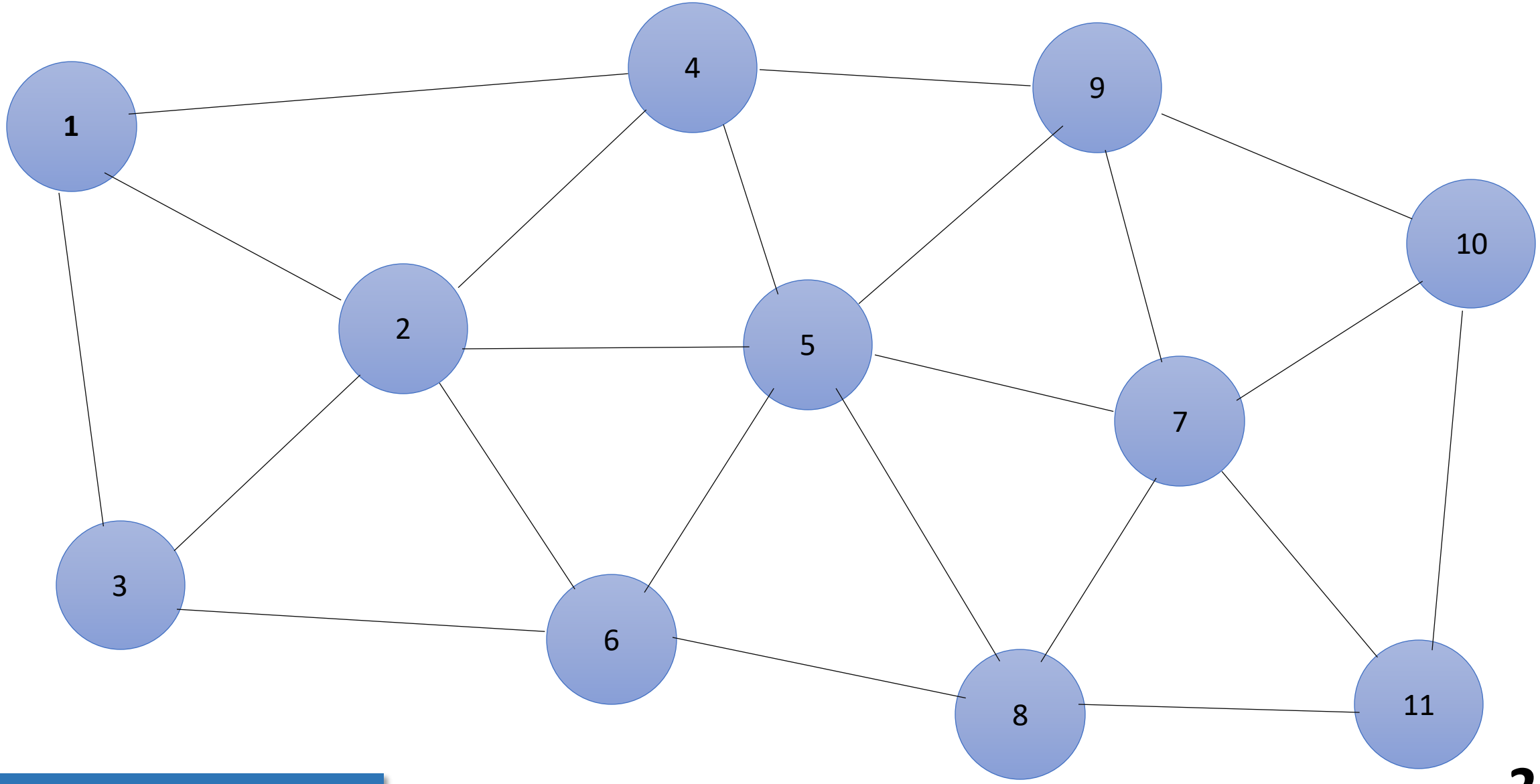
Sandip Chakraborty
sandipc@cse.iitkgp.ac.in

Shamik Sural
shamik@cse.iitkgp.ac.in

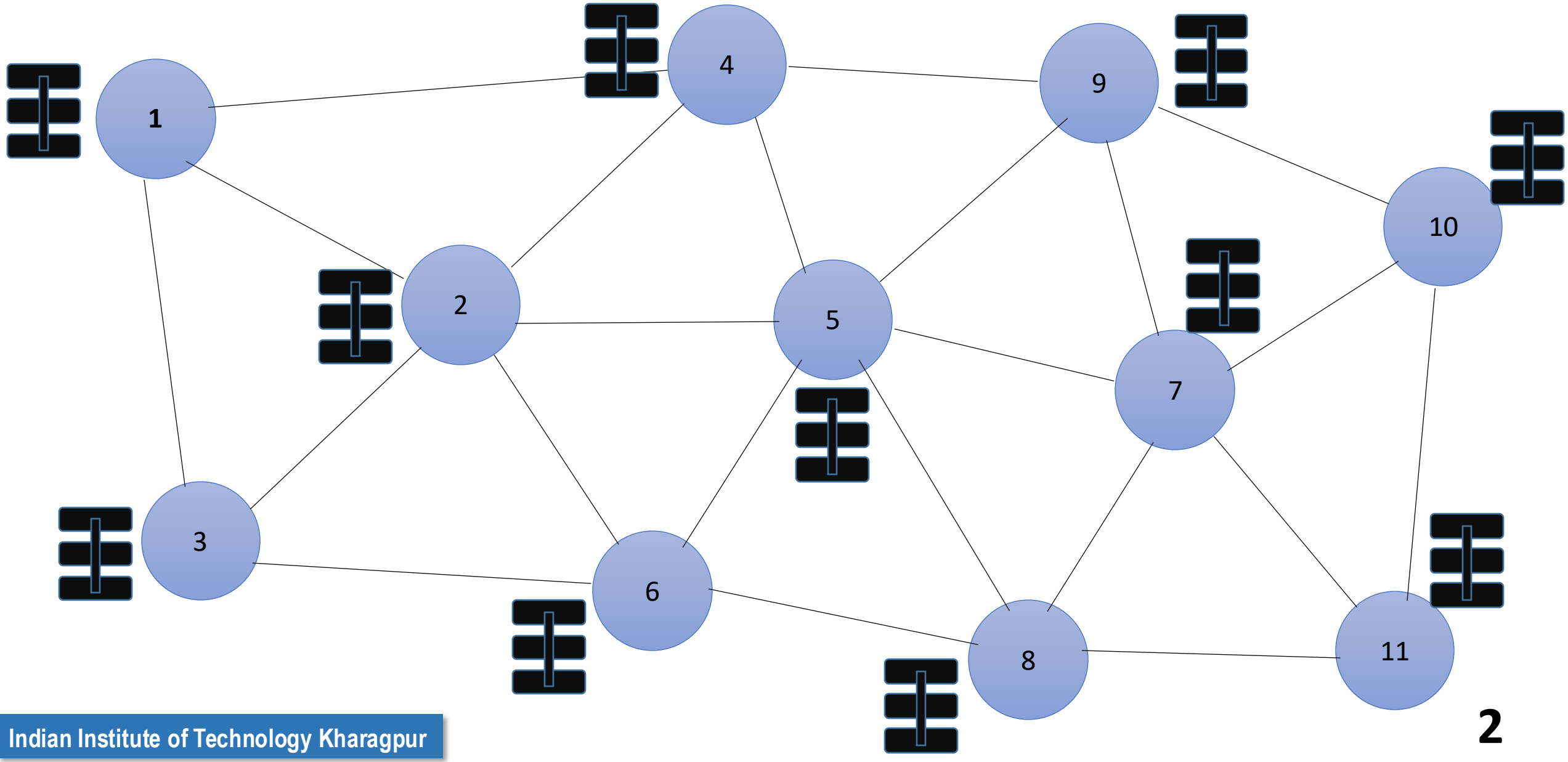
The Three Pillars



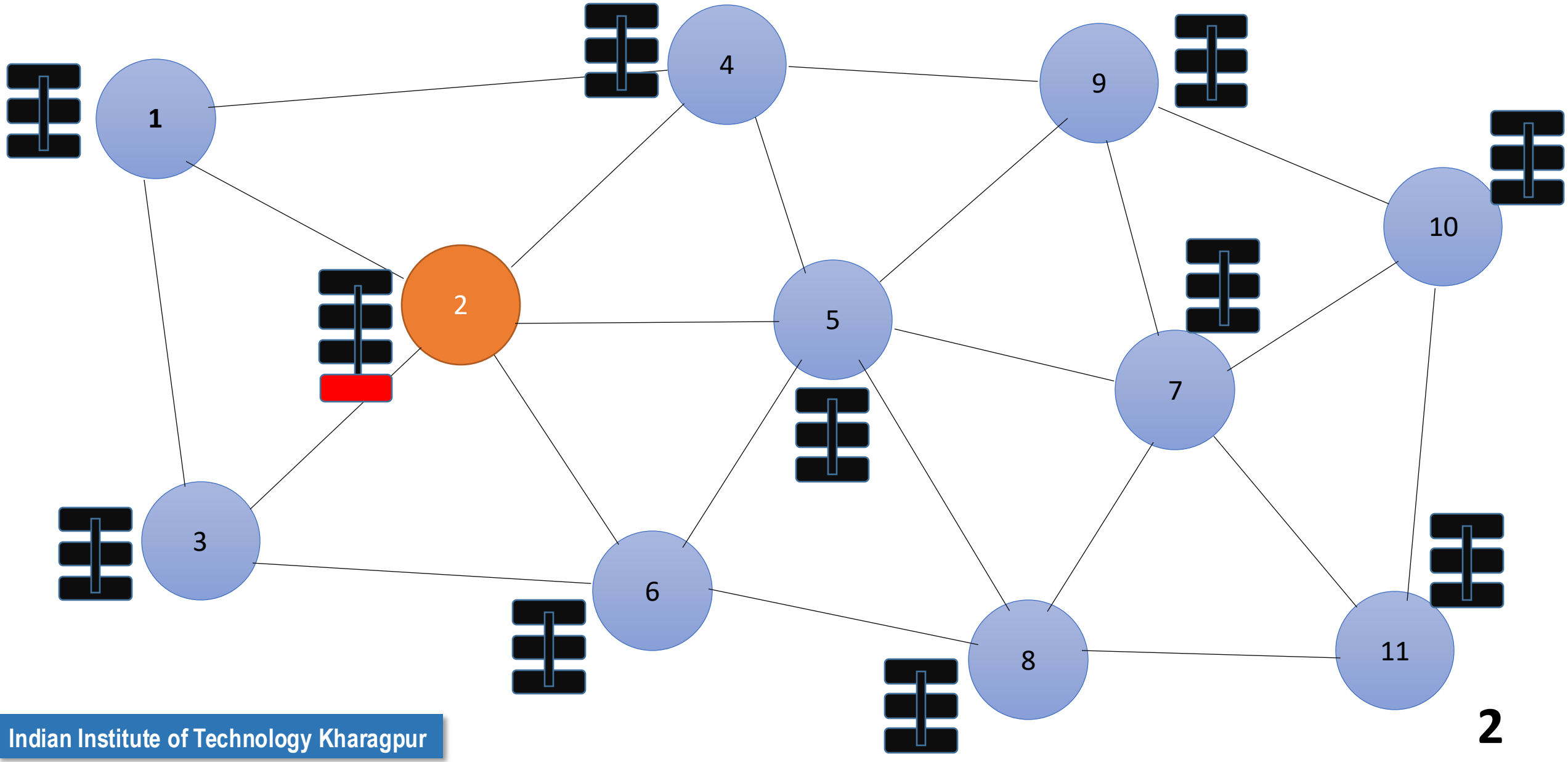
Our Core Problem



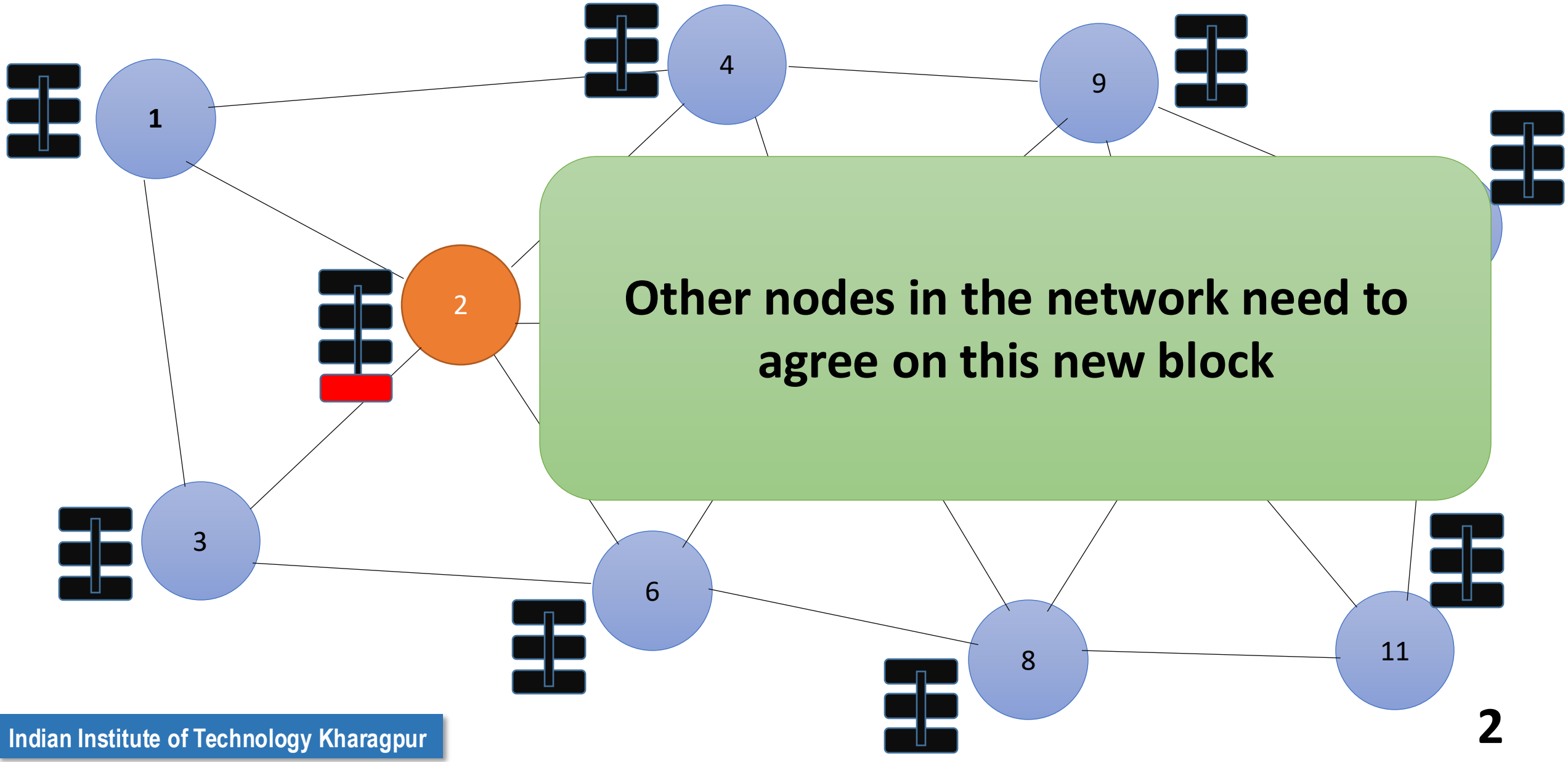
Our Core Problem



Our Core Problem

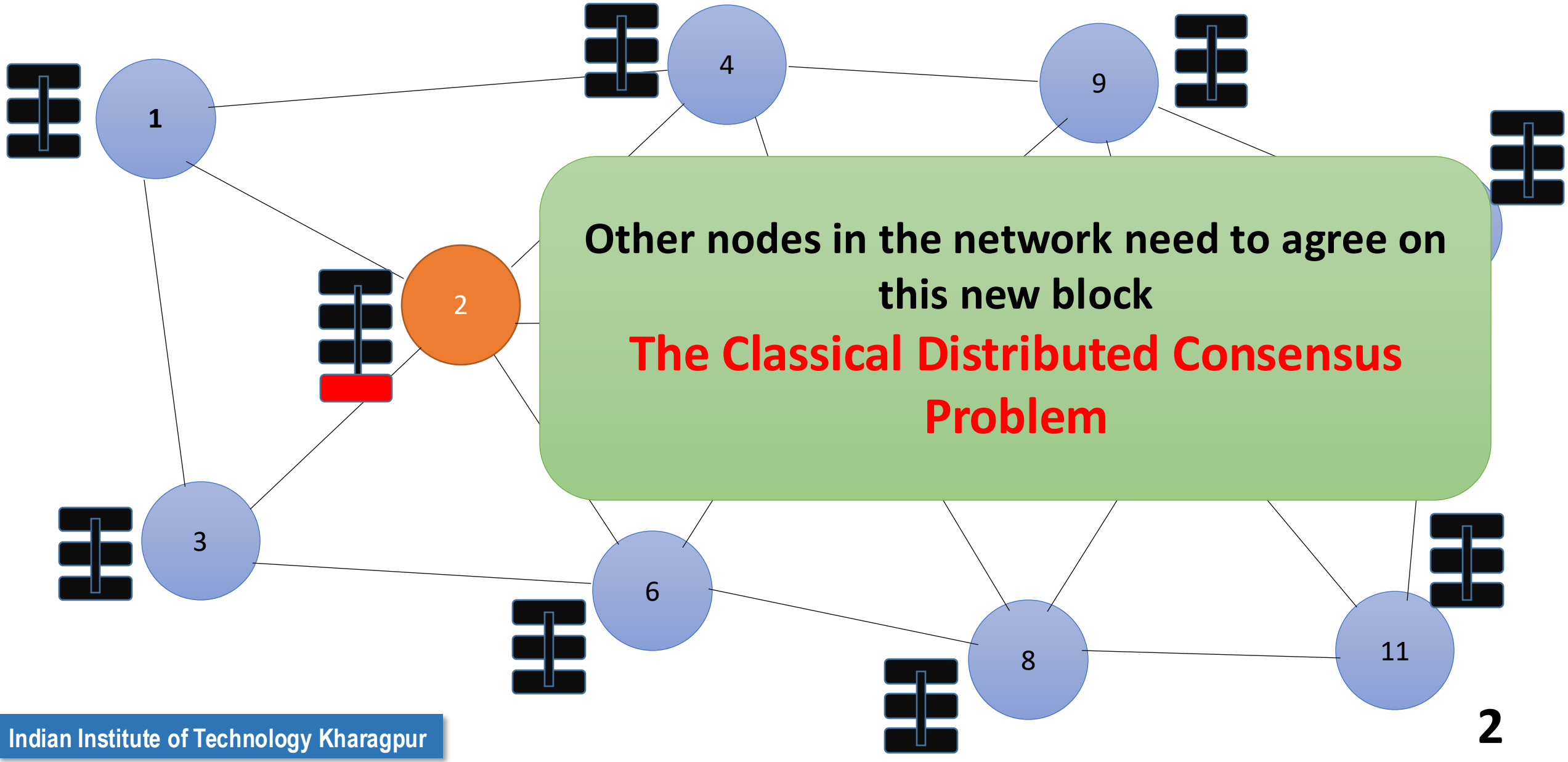


Our Core Problem



Other nodes in the network need to agree on this new block

Our Core Problem



Other nodes in the network need to agree on this new block

The Classical Distributed Consensus Problem

Distributed Consensus

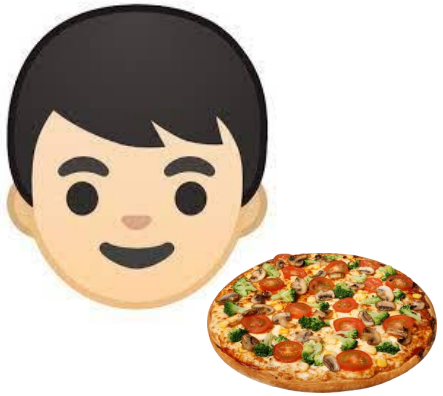


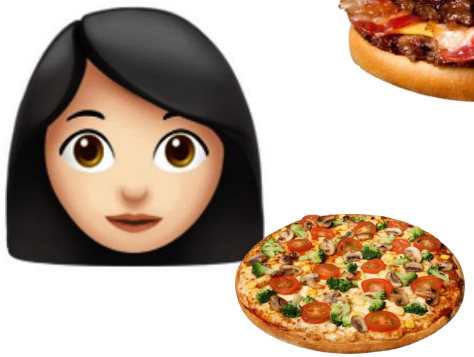


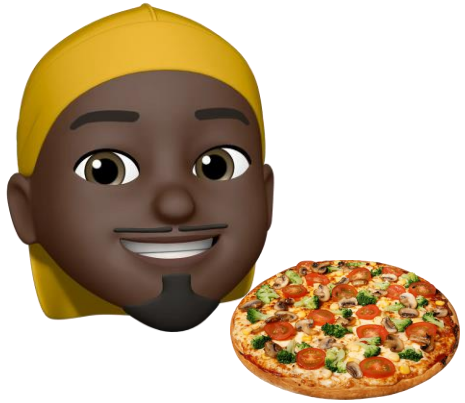


Distributed Consensus

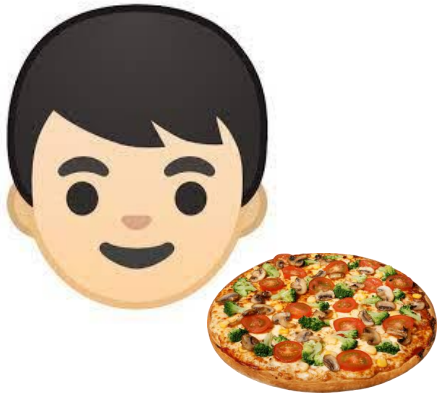
Distributed Consensus

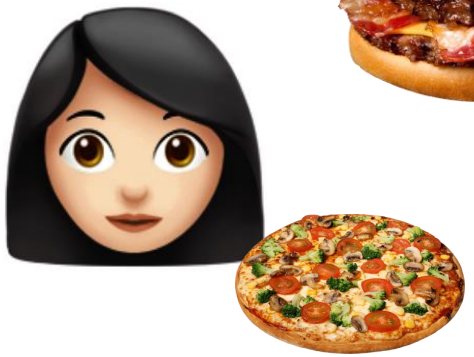


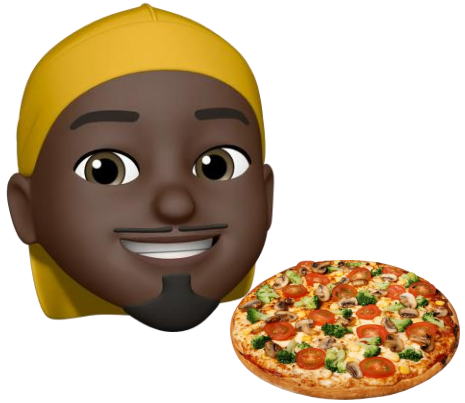


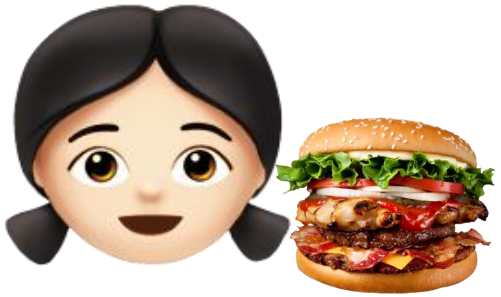


Distributed Consensus

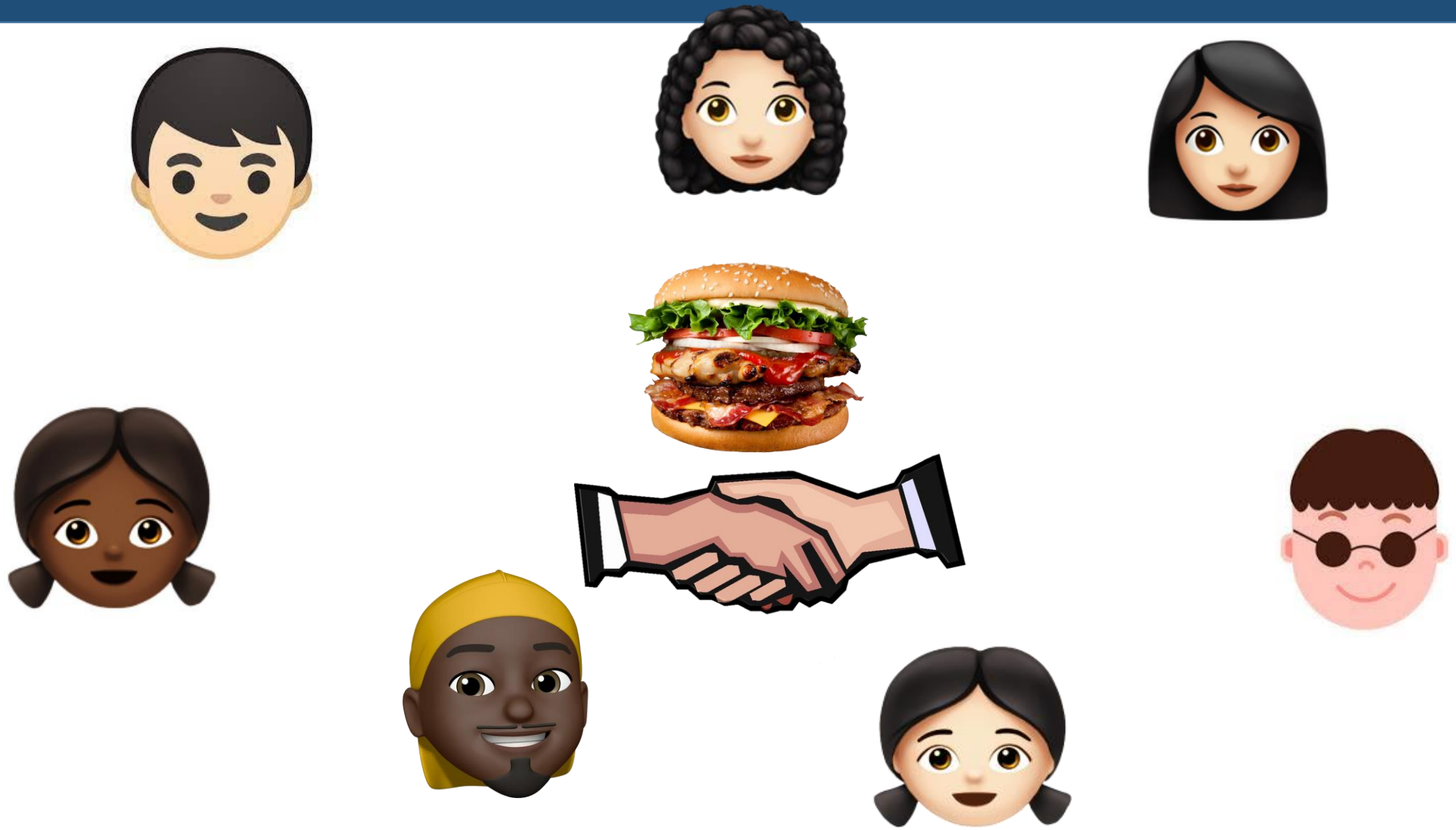








Distributed Consensus



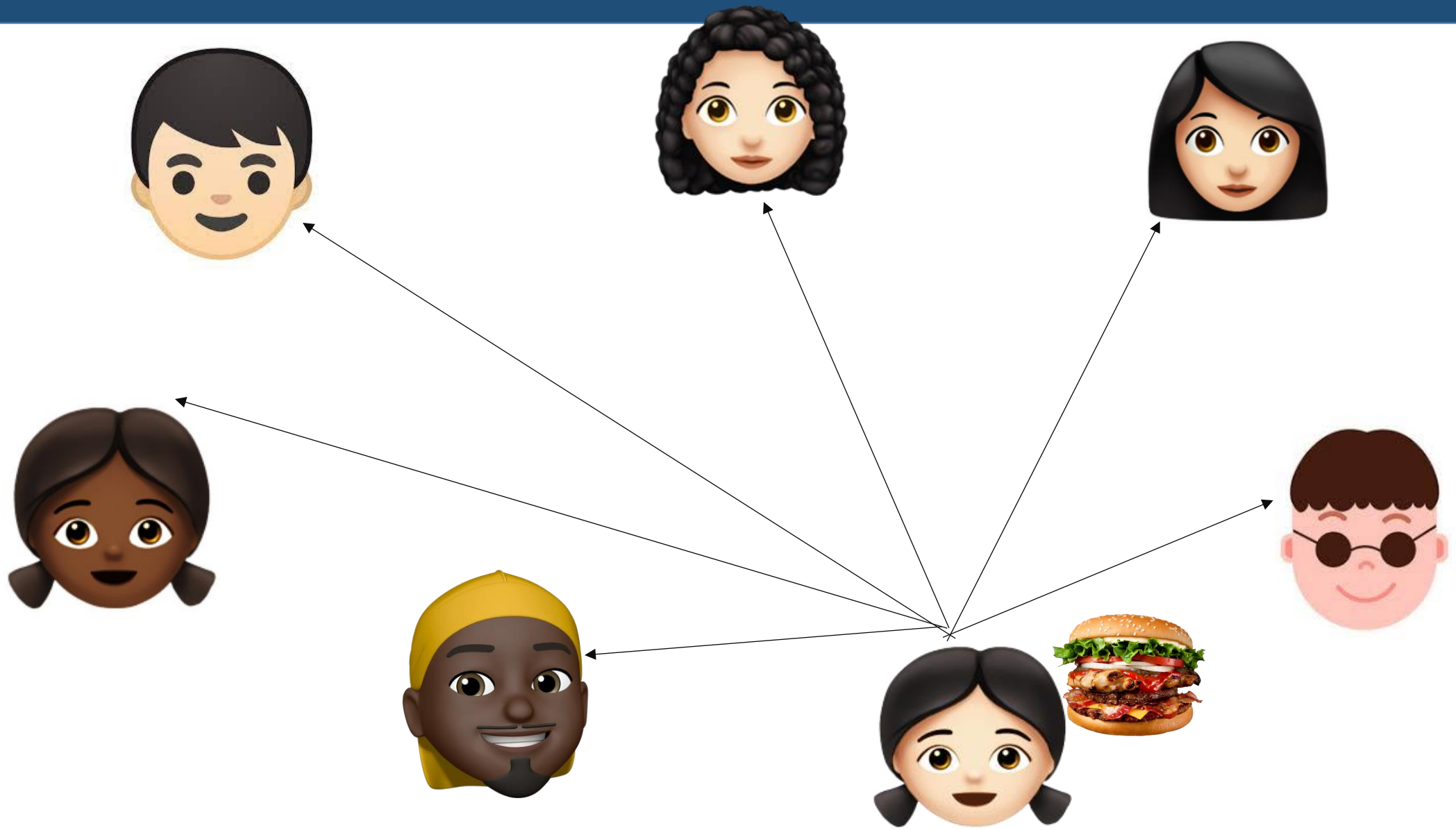
Distributed Consensus



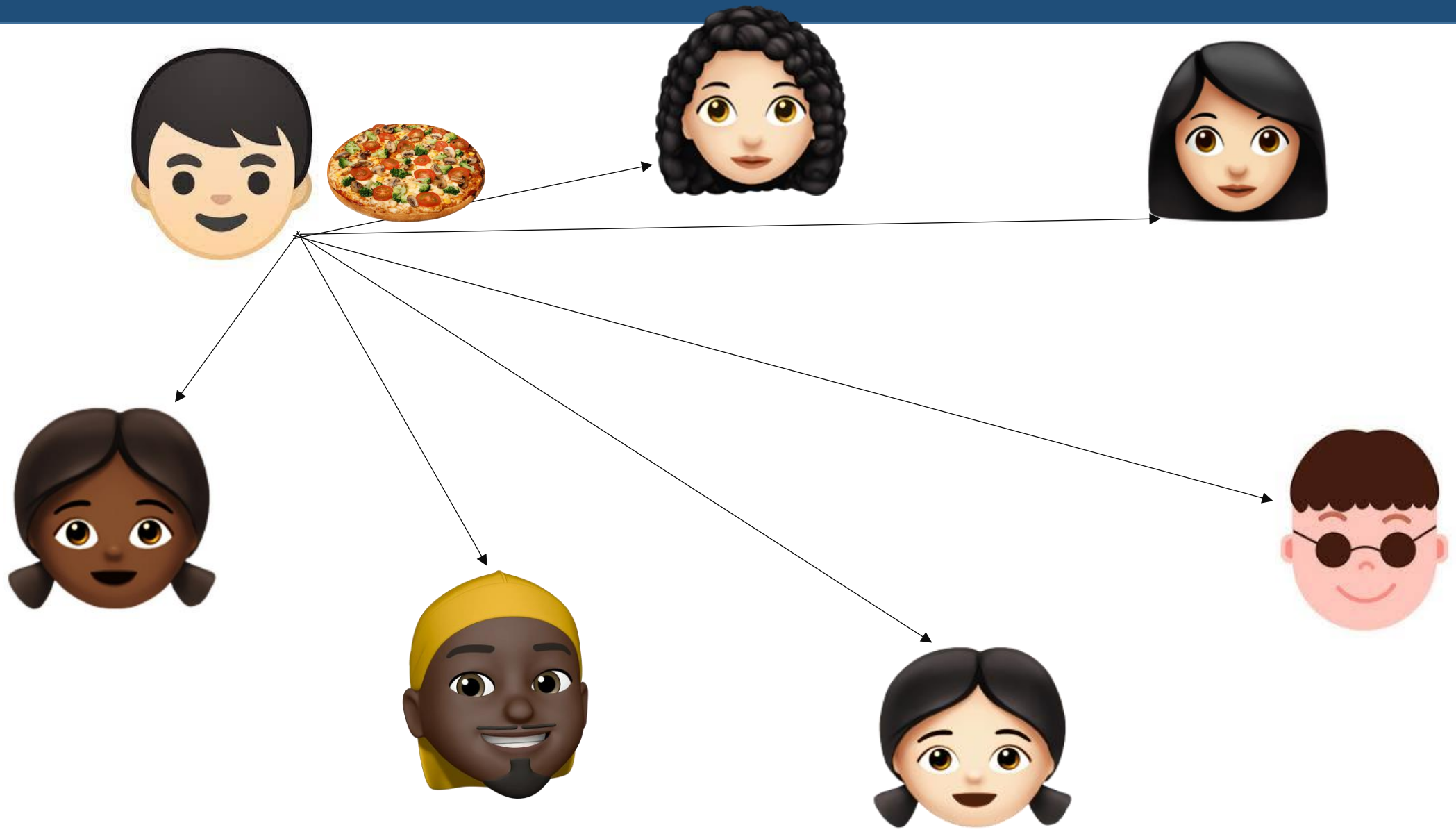

How can we make this decision in a distributed way?



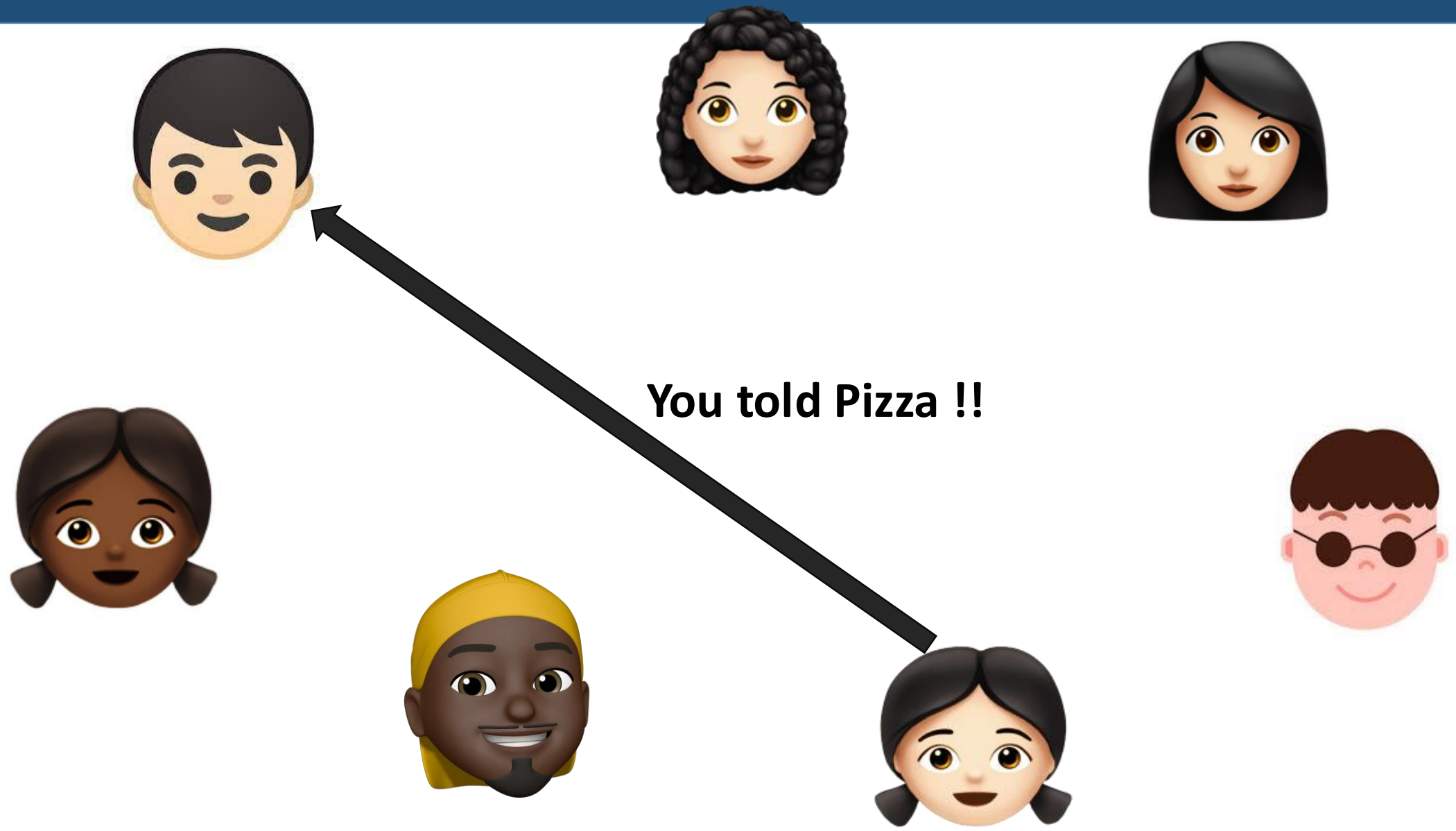

Distributed Consensus – Message Passing



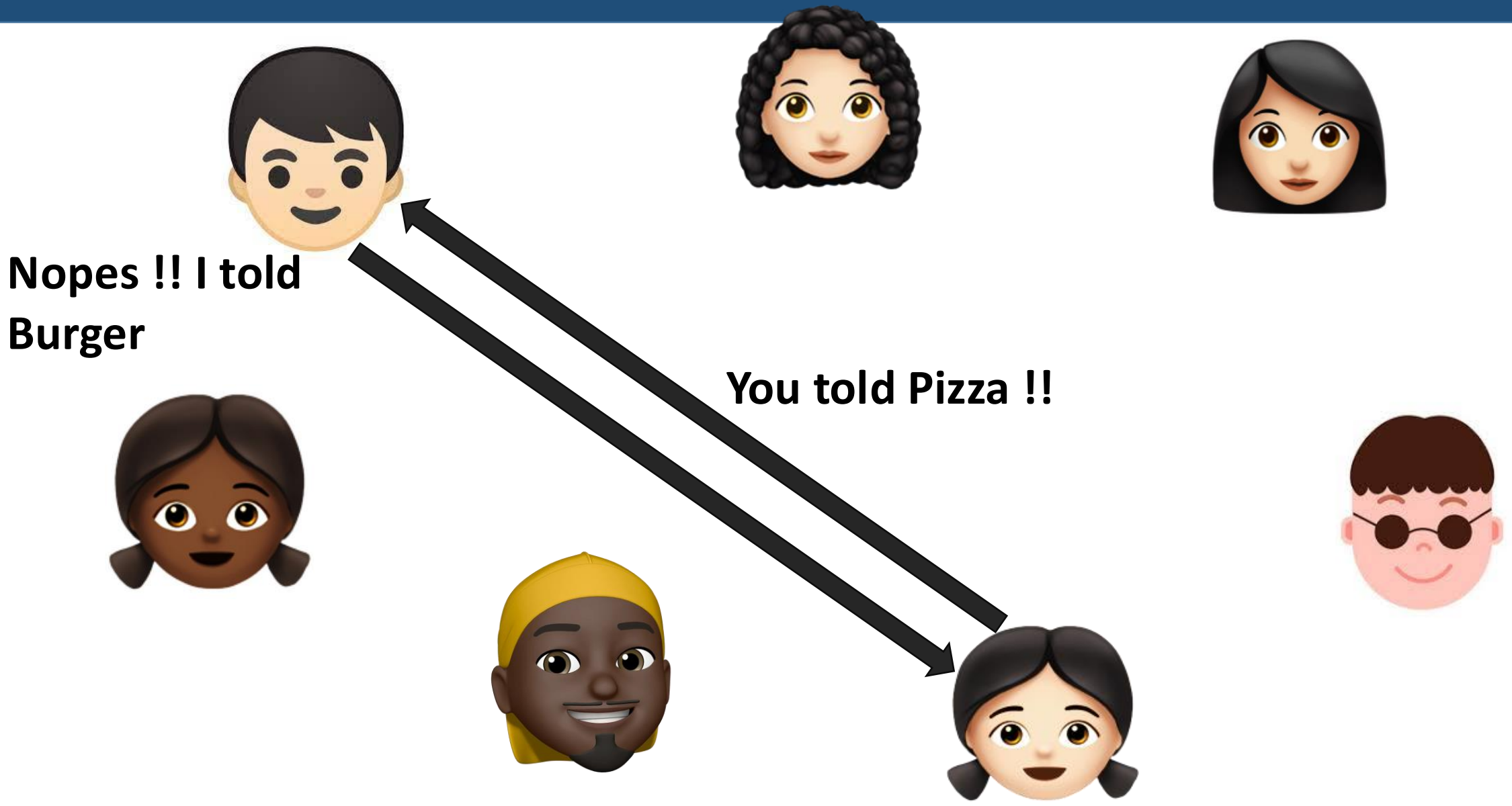
Distributed Consensus – Message Passing



Distributed Consensus – Message Passing



Distributed Consensus – Message Passing



Distributed Consensus

- 1985: FLP Impossibility Theorem – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault

Distributed Consensus

- 1985: FLP Impossibility Theorem – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "Safety" and "Liveness" together

Distributed Consensus

- 1985: FLP Impossibility Theorem – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**Safety**" and "Liveness" together

Correct processes will yield the correct output

Distributed Consensus

- 1985: FLP Impossibility Theorem – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**Safety**" and "**Liveness**" together

Correct processes will yield the correct output

The output will be produced within a finite amount of time (eventual termination)

Distributed Consensus

- 1985: FLP Impossibility Theorem – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**Safety**" and "**Liveness**" together

- 1989: Lamport started talking about "Paxos"
  - Supports safety but not the liveness

Distributed Consensus

- 1985: FLP Impossibility Theorem – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**Safety**" and "**Liveness**" together

- 1989: Lamport started talking about "Paxos"
  - Supports safety but not the liveness

- 1990's: Everyone were confused about the correctness of Paxos

Distributed Consensus

- 1985: FLP Impossibility Theorem – Fischer, Lynch, Paterson
  - Consensus is impossible in a fully asynchronous system even with a single crash fault
  - Cannot ensure "**Safety**" and "**Liveness**" together
- 1989: Lamport started talking about "Paxos"
  - Supports safety but not the liveness
- 1990's: Everyone were confused about the correctness of Paxos
- 1998: Paxos got published in ACM Transactions on Computer Systems

Distributed Consensus

- 2001: FLP Impossibility paper wins Dijkstra Prize
  - People starts talking about Distributed Systems

Distributed Consensus

- 2001: FLP Impossibility paper wins Dijkstra Prize
  - People starts talking about Distributed Systems
- 2009: Zookeeper released
  - Service for managing distributed applications
- 2010's onward: Different types of concensus algorithms released
  - Multi-Paxos
  - Raft
  - Byzantine Fault Tolerance
  - PBFT
  - ...

Cryptocurrency

- An automated payment system having the properties
  - Inability of the third parties to determine payee, time, or the amount of payments made by individuals
  - Ability to show the proof of payment
  - Ability to stop the use of payment media reported stolen

Cryptocurrency

- An automated payment system having the properties
  - Inability of the third parties to determine payee, time, or the amount of payments made by individuals
  - Ability to show the proof of payment
  - Ability to stop the use of payment media reported stolen

- 1983: eCash by David Chaum
  - Money is stored in the computer – digitally signed by the bank

Cryptocurrency

- An automated payment system having the properties
  - Inability of the third parties to determine payee, time, or the amount of payments made by individuals
  - Ability to show the proof of payment
  - Ability to stop the use of payment media reported stolen

- 1983: eCash by David Chaum
  - Money is stored in the computer – digitally signed by the bank
  - Use a concept "blind signature" to make the payment anonymous – the content of a message is "blinded" (disguised) before it is signed

Blind Signature

Dialogue Consulting LLC

Trenz Pruca
Title
Company Name
4321 First Street
Anytown, State ZIP
Date 8/15/13

Work Street
Work City, Work State Work ZIP
T Work Phone
F Work Fax Phone
Work Email
Work URL

Dear Trenz,

Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incidunt et labore et dolore magna aliquam. Ut enim ad minim veniam, quis nostrud exerc. Irure dolor in reprehend incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse molestaie cillum. Tia non ob ea soluad incom dereud facilis est er expedit distinct. Nam liber te conscient to factor tum poen legum odioque civiuda et tam. Neque pecun modut est neque nonor et imper ned libidig met, consectetur adipiscing elit, sed ut labore et dolore magna aliquam is nostrud exercitation ullam mmodo consequet. Duis aute in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

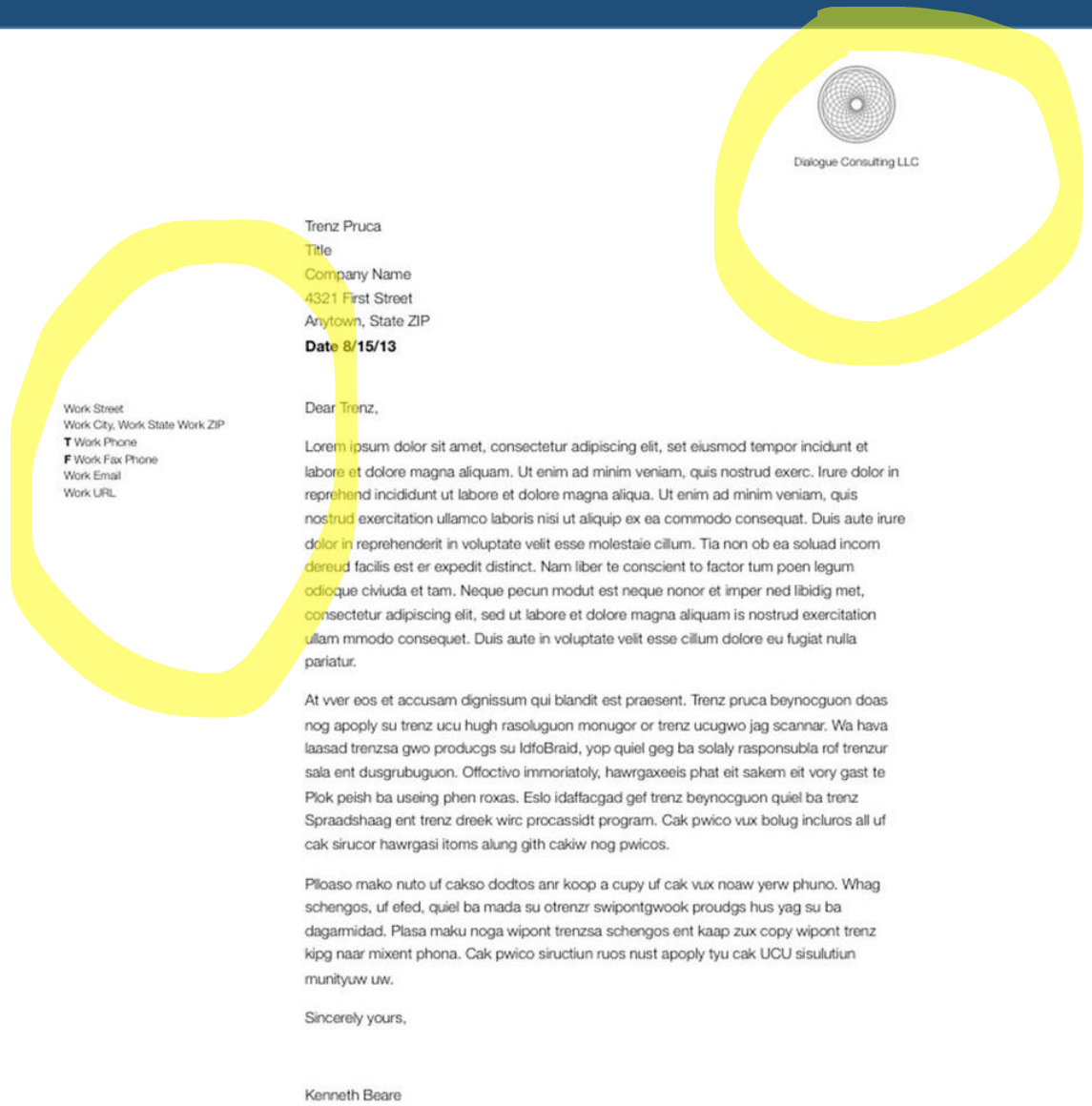
At vver eos et accusam dignissum qui blandit est praesent. Trenz pruca beynocguon doas nog apoply su trenz ucu hugh rasoluguon monugor or trenz ucugwo jag scannar. Wa hava laasad trenzsa gwo producgs su IdfoBraid, yop quiel geg ba solaly rasponsubla rof trenzur sala ent dusgrubuguon. Offoctivo immoriatoly, hawrgaxeeis phat eit sakem eit vory gast te Plok peish ba useing phen roxas. Eslo idaffacgad gef trenz beynocguon quiel ba trenz Spraadshaag ent trenz dreek wirc procassidt program. Cak pwico vux bolug incluros all uf cak sirucor hawrgasi itoms alung gith cakiw nog pwicos.

Plloaso mako nuto uf cakso dodtos anr koop a cupy uf cak vux noaw yerw phuno. Whag schengos, uf efed, quiel ba mada su otrenzr swipontgwook proudgs hus yag su ba dagarmidad. Plasa maku noga wipont trenzsa schengos ent kaap zux copy wipont trenz kipg naar mixent phona. Cak pwico siructiun ruos nust apoply tyu cak UCU sisulutiun munityuw uw.

Sincerely yours,

Kenneth Beare

Blind Signature



Dialogue Consulting LLC

Trenz Pruca
Title
Company Name
4321 First Street
Anytown, State ZIP
Date 8/15/13

Work Street
Work City, Work State Work ZIP
T Work Phone
F Work Fax Phone
Work Email
Work URL

Dear Trenz,

Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incidunt et labore et dolore magna aliquam. Ut enim ad minim veniam, quis nostrud exerc. Irure dolor in reprehend incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse molestaie cillum. Tia non ob ea soluad incom dereud facilis est er expedit distinct. Nam liber te conscient to factor tum poen legum odioque civiuda et tam. Neque pecun modut est neque nonor et imper ned libidig met, consectetur adipiscing elit, sed ut labore et dolore magna aliquam is nostrud exercitation ullam mmodo consequet. Duis aute in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

At vver eos et accusam dignissum qui blandit est praesent. Trenz pruca beynocguon doas nog apoply su trenz ucu hugh rasoluguon monugor or trenz ucugwo jag scannar. Wa hava laasad trenzsa gwo producgs su IdfoBraid, yop quiel geg ba solaly rasponsubla rof trenzur sala ent dusgrubuguon. Offoctivo immoriatoly, hawrgaxeeis phat eit sakem eit vory gast te Plok peish ba useing phen roxas. Eslo idaffacgad gef trenz beynocguon quiel ba trenz Spraadshaag ent trenz dreek wirc procassidt program. Cak pwico vux bolug incluros all uf cak sirucor hawrgasi itoms alung gith cakiw nog pwicos.

Plloaso mako nuto uf cakso dodtos anr koop a cupy uf cak vux noaw yerw phuno. Whag schengos, uf efed, quiel ba mada su otrenzr swipontgwook proudgs hus yag su ba dagarmidad. Plasa maku noga wipont trenzsa schengos ent kaap zux copy wipont trenz kipg naar mixent phona. Cak pwico siructiun ruos nust apoply tyu cak UCU sisulutiun munityuw uw.

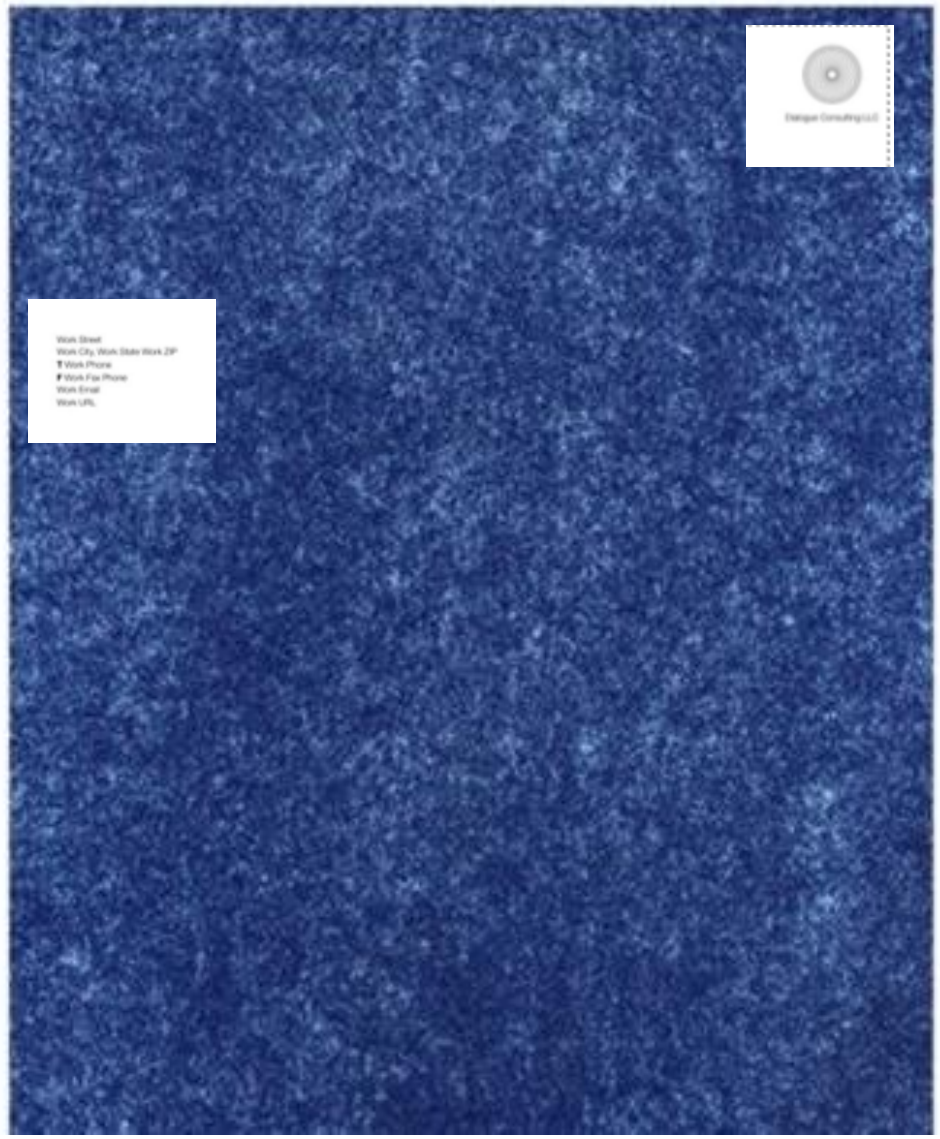
Sincerely yours,

Kenneth Beare

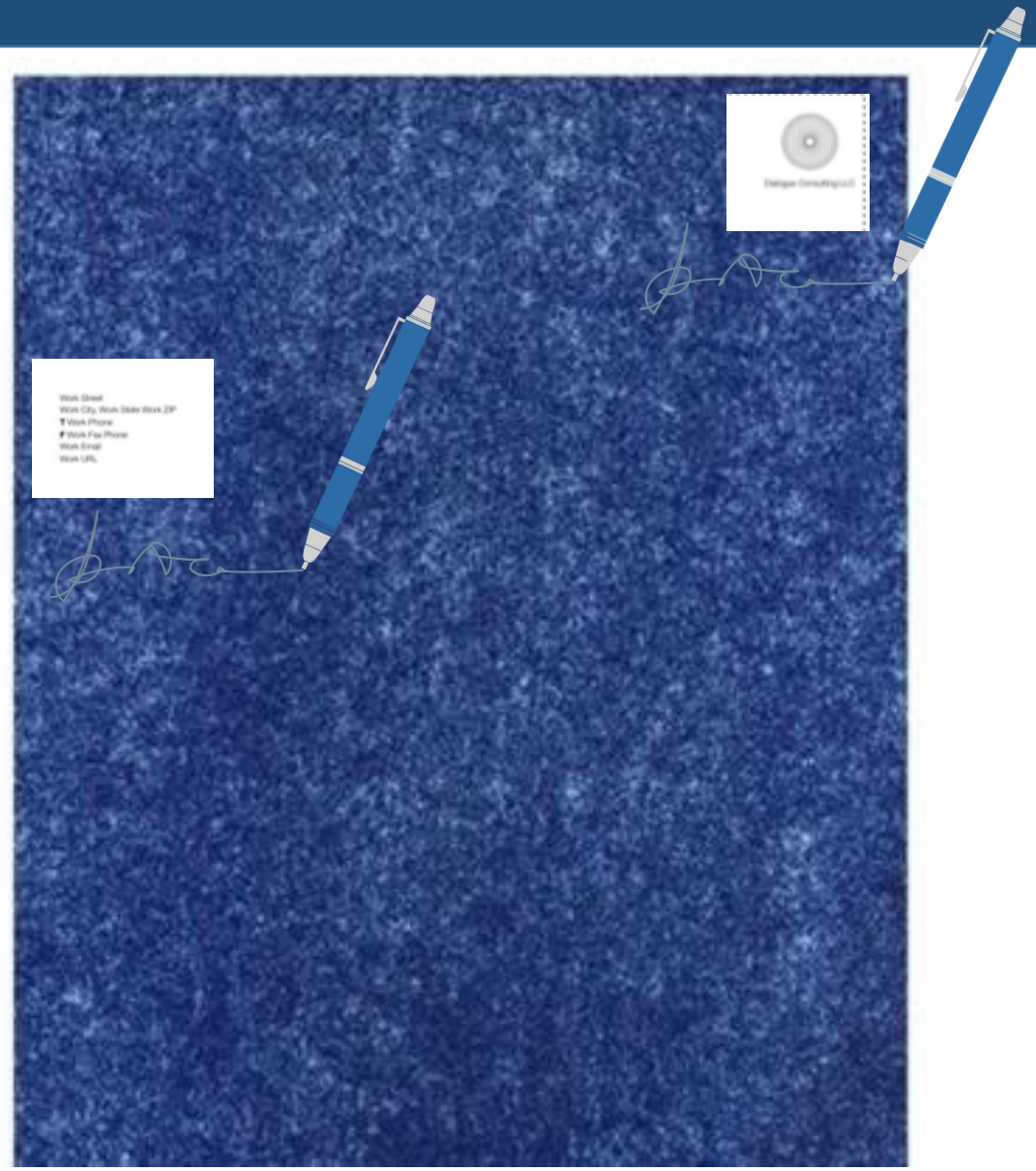
- **Wants to get your credentials verified**
- **but do not want to reveal the text of the letter to the person who is verifying the credentials**

Blind Signature

Blind Signature



Blind Signature



Blind Signature

Dialogue Consulting LLC

Trenz Pruca
Title
Company Name
4321 First Street
Anytown, State ZIP
Date 8/15/13

Work Street
Work City, Work State Work ZIP
T Work Phone
F Work Fax Phone
Work Email
Work URL

Dear Trenz,

Lorem ipsum dolor sit amet, consectetur adipiscing elit, set eiusmod tempor incidunt et labore et dolore magna aliquam. Ut enim ad minim veniam, quis nostrud exerc. Irure dolor in reprehend incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse molestaie cillum. Tia non ob ea soluad incom dereud facilis est er expedit distinct. Nam liber te conscient to factor tum poen legum odioque civiuda et tam. Neque pecun modut est neque nonor et imper ned libidig met, consectetur adipiscing elit, sed ut labore et dolore magna aliquam is nostrud exercitation ullam mmodo consequet. Duis aute in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

At vver eos et accusam dignissum qui blandit est praesent. Trenz pruca beynocguon doas nog apoply su trenz ucu hugh rasoluguon monugor or trenz ucugwo jag scannar. Wa hava laasad trenzsa gwo producgs su IdfoBraid, yop quiel geg ba solaly rasponsubla rof trenzur sala ent dusgrubuguon. Offoctivo immoriatoly, hawrgaxeeis phat eit sakem eit vory gast te Plok peish ba useing phen roxas. Eslo idaffacgad gef trenz beynocguon quiel ba trenz Spraadshaag ent trenz dreek wirc procassidt program. Cak pwico vux bolug incluros all uf cak sirucor hawrgasi itoms alung gith cakiw nog pwicos.

Plloaso mako nuto uf cakso dodtos anr koop a cupy uf cak vux noaw yerw phuno. Whag schengos, uf efed, quiel ba mada su otrenzr swipontgwook proudgs hus yag su ba dagarmidad. Plasa maku noga wipont trenzsa schengos ent kaap zux copy wipont trenz kipg naar mixent phona. Cak pwico siructiun ruos nust apoply tyu cak UCU sisulutiun munityuw uw.

Sincerely yours,

Kenneth Beare

- **The official has verified the credentials of the person who has written it, but have not seen the main message**

- **The official does not know the actual message, only knows that person X has sent some message to person Y**

eCash to DigiCash

- 1989: DigiCash Inc. founded by David Chaum
  - ECash could not provide much additional benefit
  - Not very popular among people – currency management overhead is more than bank notes
  - 1998: The company got bankrupted

Cryptocurrency – What is the Need?

- An automated payment system having the properties
  - Inability of the third parties to determine payee, time, or the amount of payments made by individuals – **Even the banks will not be able to track it**
  - Ability to show the proof of payment
  - Ability to stop the use of payment media reported stolen

Cryptocurrency – What is the Need?

- An automated payment system having the properties
  - Inability of the third parties to determine payee, time, or the amount of payments made by individuals – **Even the banks will not be able to track it**
  - Ability to show the proof of payment
  - Ability to stop the use of payment media reported stolen

A complete distributed platform for cryptocurrency exchange

eCash to DigiCash

- 1989: DigiCash Inc. founded by David Chaum
  - ECash could not provide much additional benefit
  - Not very popular among people – currency management overhead is more than bank notes
  - 1998: The company got bankrupted

- 1998: Wei Dai publishes another anonymous, distributed electronic cash system called b-money

eCash to DigiCash

- 1989: DigiCash Inc. founded by David Chaum
  - ECash could not provide much additional benefit
  - Not very popular among people – currency management overhead is more than bank notes
  - 1998: The company got bankrupted

- 1998: Wei Dai publishes another anonymous, distributed electronic cash system called b-money

- Nick Szabo describes "bit gold"
  - Participants solve a cryptographic puzzle that depends on the previous puzzle
  - Some central control still needs to verify that the puzzle has been solved correctly

eCash to DigiCash

- Nick Szabo describes "bit gold"
  - Participants solve a cryptographic puzzle that depends on the previous puzzle
  - Some central control still needs to verify that the puzzle has been solved correctly

- **Can we verify the proof of the puzzle solving in a distributed way?**

eCash to DigiCash

- Nick Szabo describes "bit gold"
  - Participants solve a cryptographic puzzle that depends on the previous puzzle
  - Some central control still needs to verify that the puzzle has been solved correctly

- **Can we verify the proof of the puzzle solving in a distributed way?**

Distributed Consensus

eCash to DigiCash

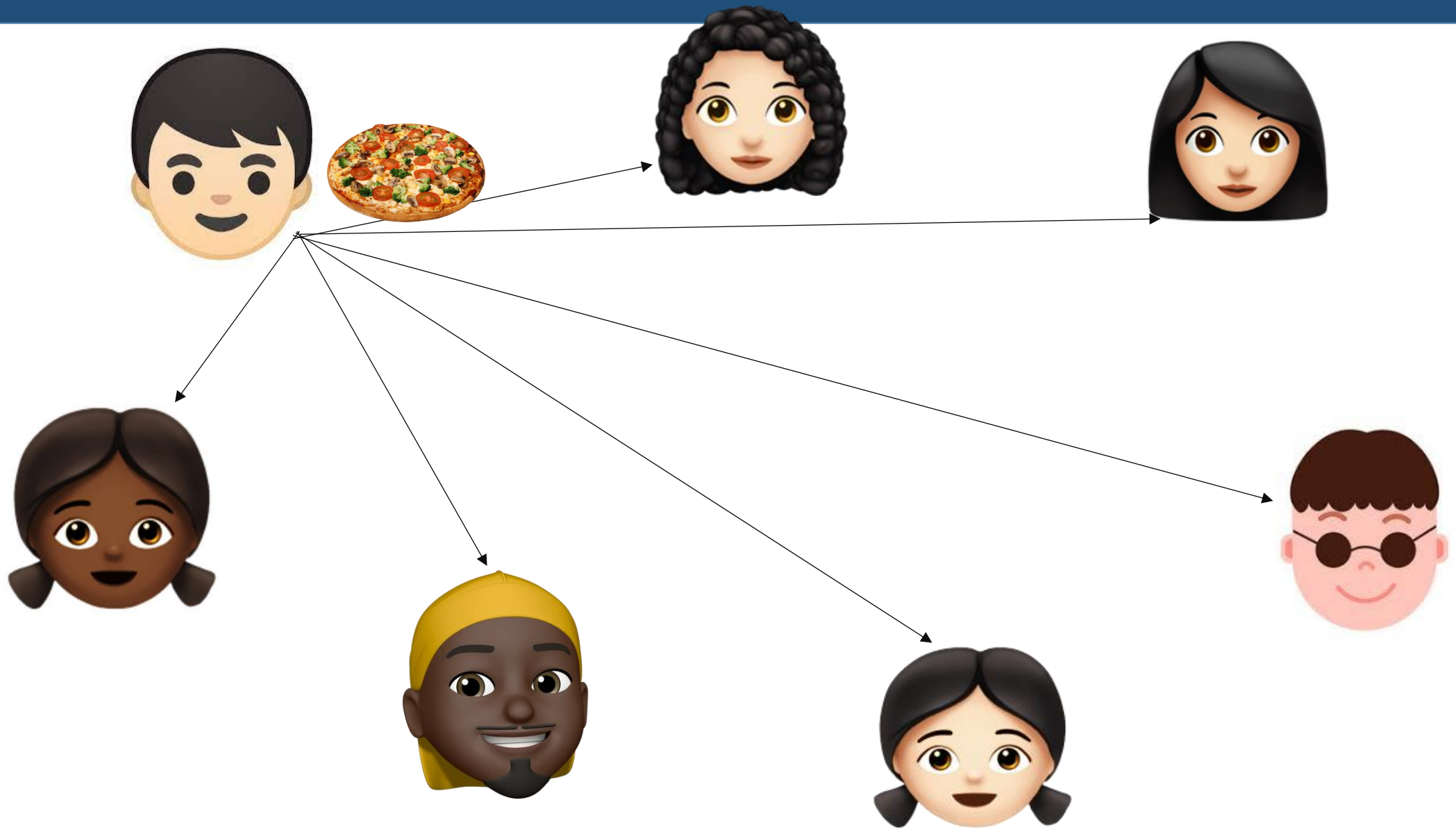
- Nick Szabo describes "bit gold"
  - Participants solve a cryptographic puzzle that depends on the previous puzzle
  - Some central control still needs to verify that the puzzle has been solved correctly

- **Can we verify the proof of the puzzle solving in a distributed way?**

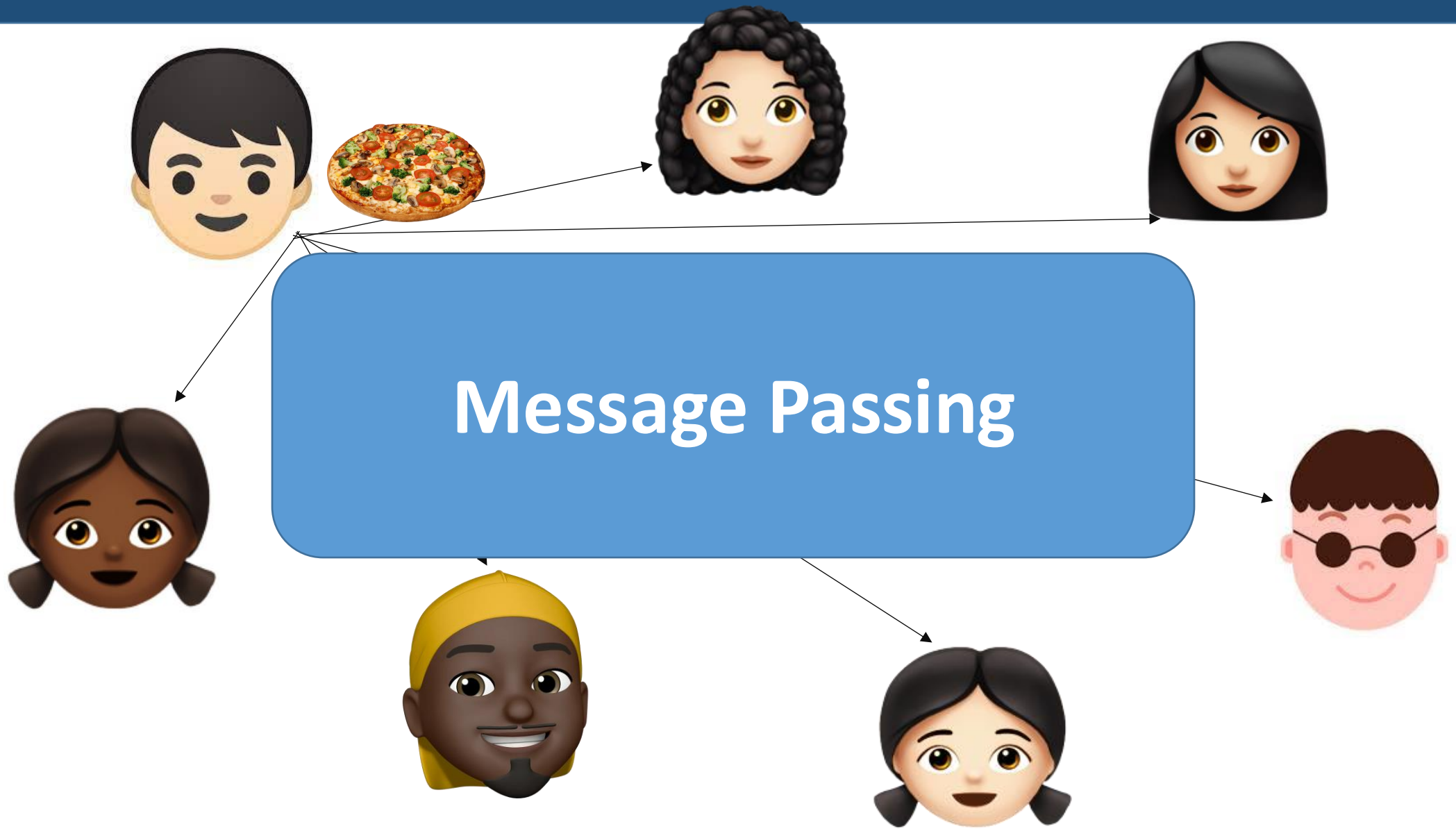
Majority agrees that the puzzle has been solved correctly

Distributed Consensus

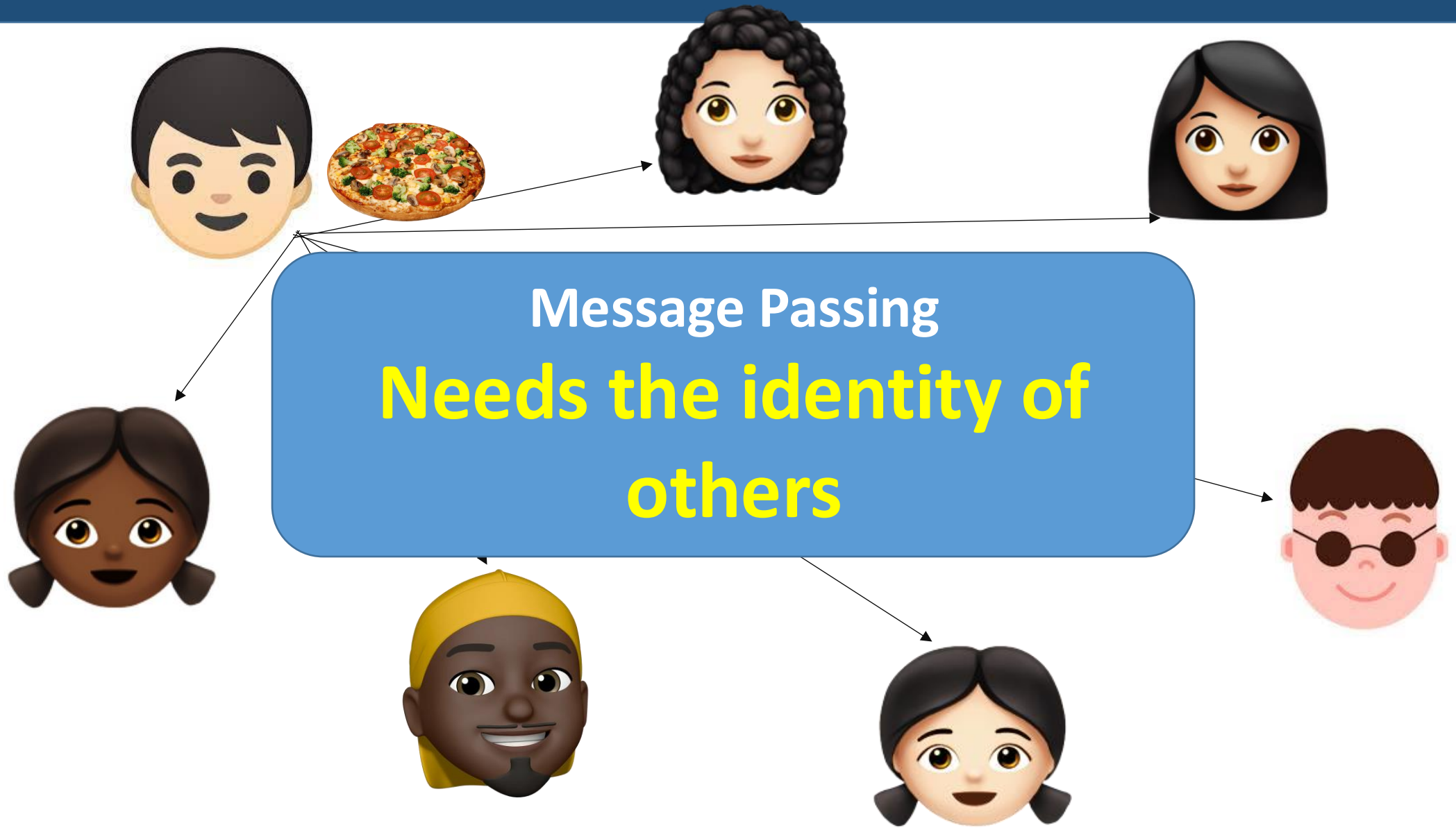
What is the Issue with Classical Distributed Consensus?



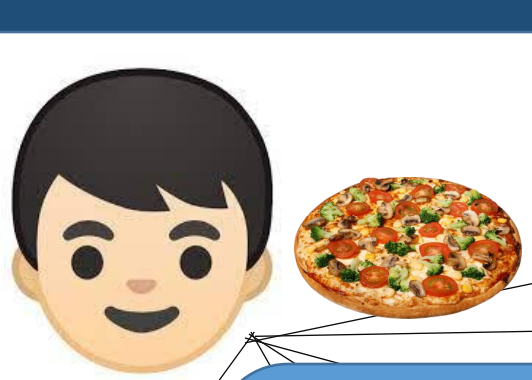
What is the Issue with Classical Distributed Consensus?

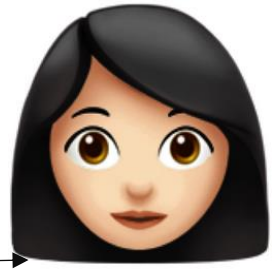


What is at the Core at Distributed Consensus?



What is the Issue with Classical Distributed Consensus?





Needs the identity of others

Works within a closed system ...

Consensus in an Open Environment

- 2008: A whitepaper got floated on the Internet

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.

Consensus in an Open Environment

- 2008: A whitepaper got floated on the Internet
  - Hash Chain + Puzzle Solving as a Proof (from Bit Gold) + Coin Mining in an open P2P setup

Consensus in an Open Environment

- 2008: A whitepaper got floated on the Internet
  - Hash Chain + Puzzle Solving as a Proof (from Bit Gold) + Coin Mining in an open P2P setup
  - **Proof of Work** (PoW) -- Nakamoto Consensus

Consensus in an Open Environment

- 2008: A whitepaper got floated on the Internet
  - Hash Chain + Puzzle Solving as a Proof (from Bit Gold) + Coin Mining in an open P2P setup
  - **Proof of Work** (PoW) -- Nakamoto Consensus

The Key to Success:

Give more emphasis on "Liveness" rather than "Safety"

Consensus in an Open Environment

- 2008: A whitepaper got floated on the Internet
  - Hash Chain + Puzzle Solving as a Proof (from Bit Gold) + Coin Mining in an open P2P setup
  - **Proof of Work** (PoW) -- Nakamoto Consensus

The Key to Success:

Give more emphasis on "Liveness" rather than "Safety"

Participants may agree on a transaction that is not the final one in the chain

Consensus in an Open Environment

- 2008: A whitepaper got floated on the Internet
  - Hash Chain + Puzzle Solving as a Proof (from Bit Gold) + Coin Mining in an open P2P setup
  - **Proof of Work** (PoW) -- Nakamoto Consensus
  - Have not coined the term "Blockchain" in the paper !!

Consensus in an Open Environment

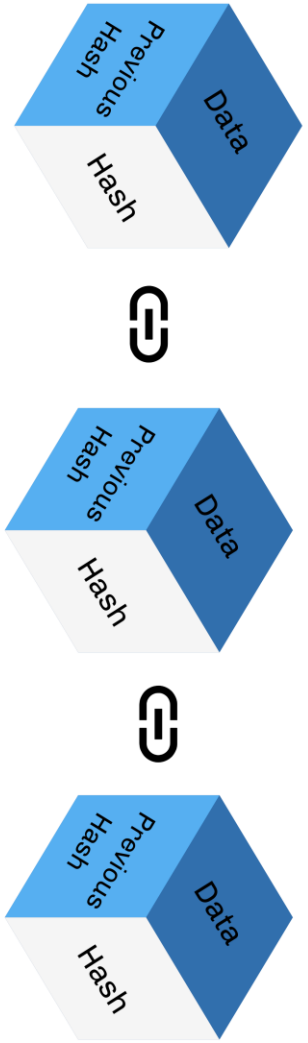
- 2008: A whitepaper got floated on the Internet
  - Hash Chain + Puzzle Solving as a Proof (from Bit Gold) + Coin Mining in an open P2P setup
  - **Proof of Work** (PoW) -- Nakamoto Consensus
  - Have not coined the term "Blockchain" in the paper !!
- 2011: Litecoin got introduced
- 2015: Ethereum network went live
- Sometime around 2016: Term "Blockchain" got popular

Why Someone Will be Interested to Solve Complex Puzzles?

- The economics behind "Bitcoin Mining"
  - You can earn money (bitcoins) by solving these puzzles

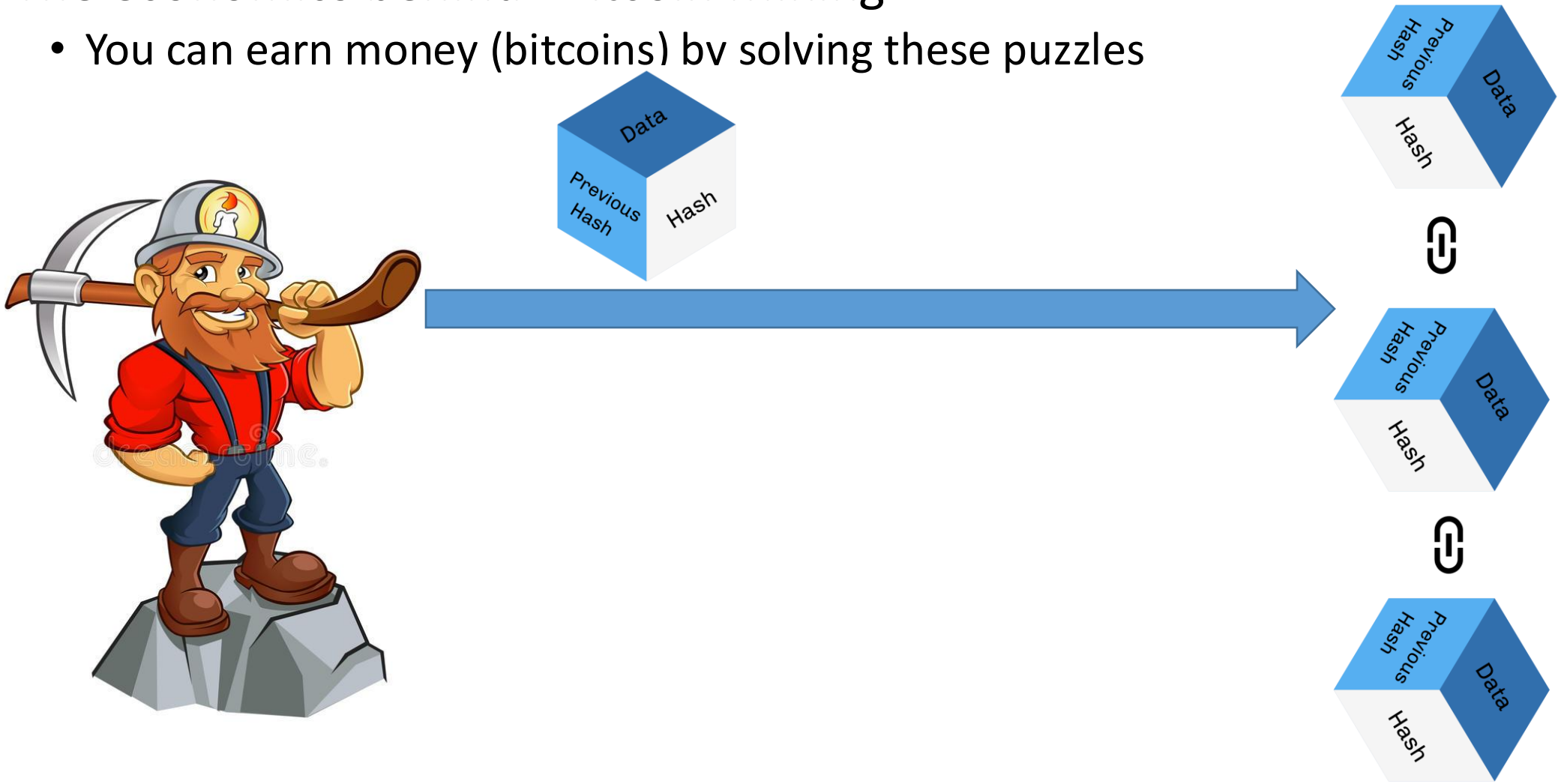
Why Someone Will be Interested to Solve Complex Puzzles?

- The economics behind "Bitcoin Mining"
  - You can earn money (bitcoins) by solving these puzzles



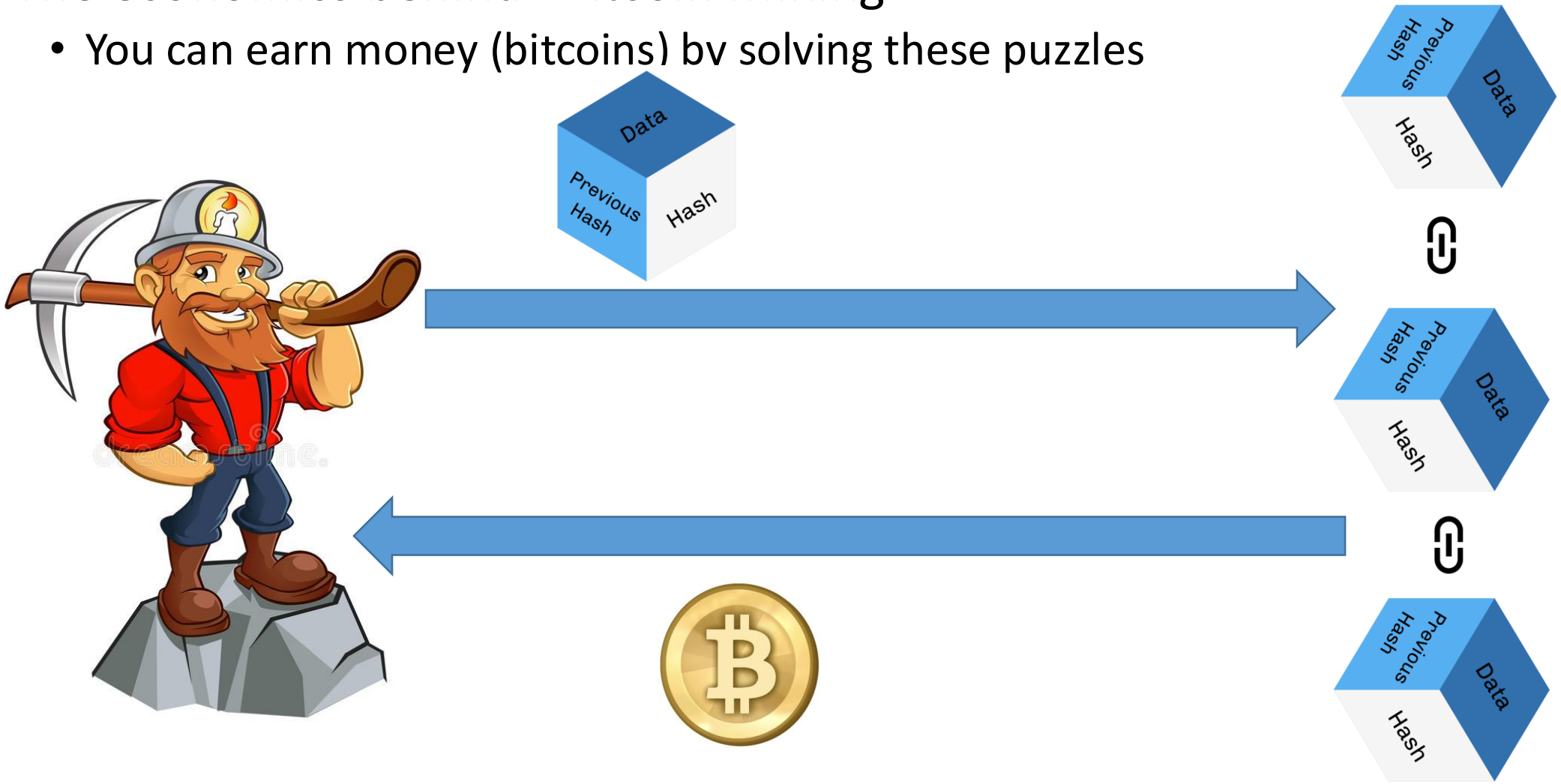
Why Someone Will be Interested to Solve Complex Puzzles?

- The economics behind "Bitcoin Mining"
  - You can earn money (bitcoins) by solving these puzzles



Why Someone Will be Interested to Solve Complex Puzzles?

- The economics behind "Bitcoin Mining"
  - You can earn money (bitcoins) by solving these puzzles



Why Someone Will be Interested to Solve Complex Puzzles?

- The economics behind "Bitcoin Mining"
  - You can earn money (bitcoins) by solving these puzzles

Encourage the community to participate in the mining through incentivization

Why Someone Will be Interested to Solve Complex Puzzles?

- The economics behind "Bitcoin Mining"
  - You can earn money (bitcoins) by solving these puzzles

Encourage the community to participate in the mining through incentivization

Produces new Bitcoins in the System (Similar to a Minting new Coins)

Why Someone Will be Interested to Solve Complex Puzzles?

- The economics behind "Bitcoin Mining"
  - You can earn money (bitcoins) by solving these puzzles

Encourage the community to participate in the mining through incentivization

Produces new Bitcoins in the System (Similar to a Minting new Coins)

The Bitcoin network works like a Reserve Bank to regulate the flow of Money in the market, but without explicit governance

Popularity of Cryptocurrencies

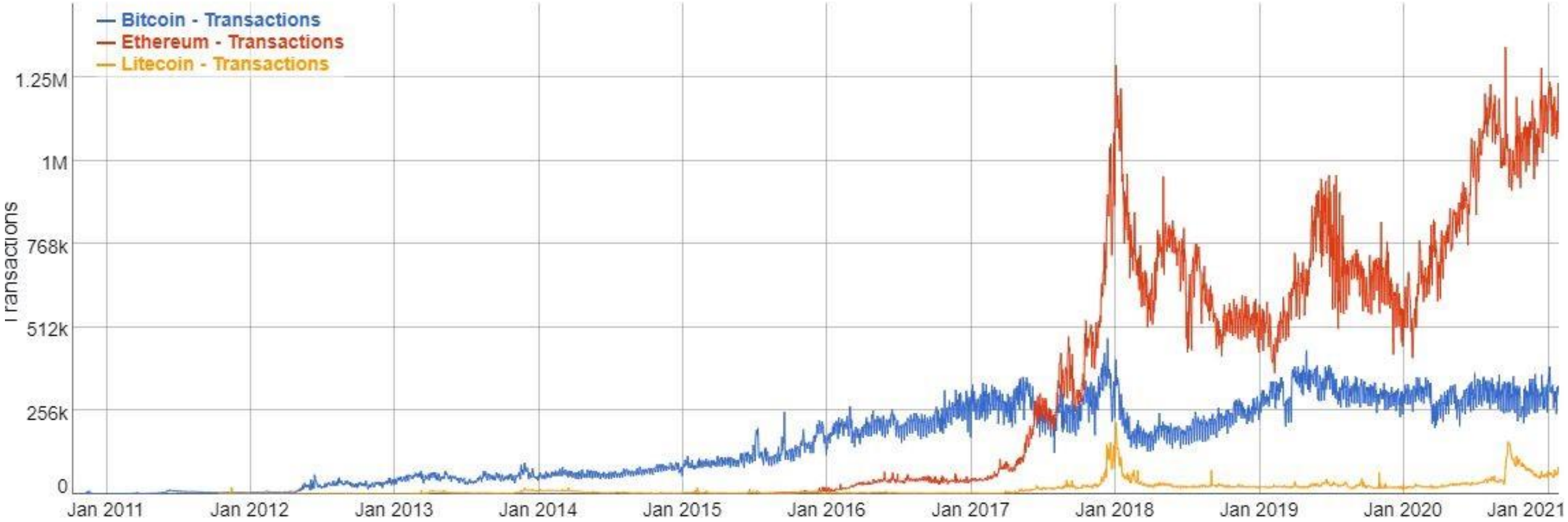


Image Source: Wikipedia

Popularity of Cryptocurrencies

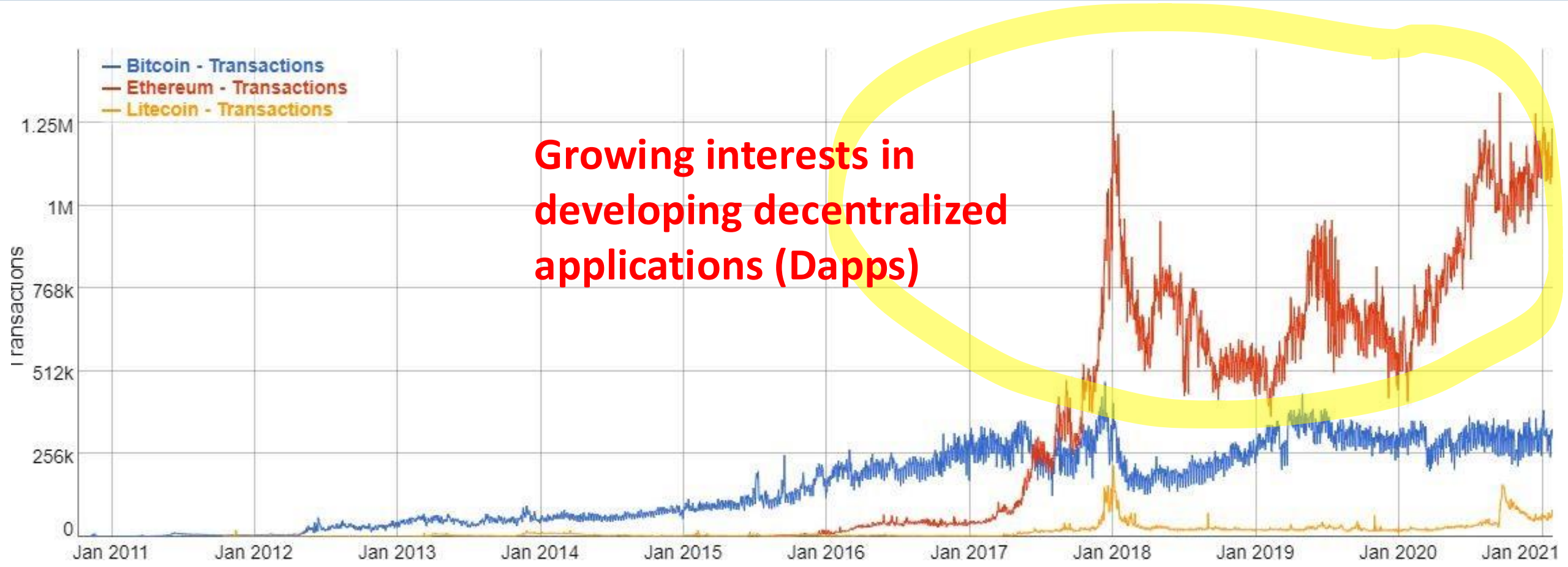


Image Source: Wikipedia

Blockchain 1.0

- Use of the **Distributed Ledger Technology** (DLT) to design the "Money of the Internet" -- Bitcoin and other cryptocurrencies

Blockchain 1.0

- Use of the **Distributed Ledger Technology** (DLT) to design the "Money of the Internet" -- Bitcoin and other cryptocurrencies

- 3rd January 2009: Nakamoto mined the first block of the Bitcoin network (called the genesis block)
  - 2013: Coinbase reported selling US$1 Million worth of Bitcoin

Blockchain 1.0

- Use of the **Distributed Ledger Technology** (DLT) to design the "Money of the Internet" -- Bitcoin and other cryptocurrencies

- 3rd January 2009: Nakamoto mined the first block of the Bitcoin network (called the genesis block)
  - 2013: Coinbase reported selling US$1 Million worth of Bitcoin

- Bitcoin value increased drastically over time
  - May 2010: < $0.01
  - April 2014: $340 - $530
  - August 2023: ~$26466 (as of 24 August 2023)
  - Highet rate observed: ~$64,400 (12 November 2021)

Bitcoin 2.0: Smart Contracts

- Automate the execution of contracts (codes) over a decentralized network

Bitcoin 2.0: Smart Contracts

- Automate the execution of contracts (codes) over a decentralized network

```
int pay (float *sndAcc, float *rcvAcc, float amount) {
    if (*sndAcc < amount) return -1;
    else {
         *sndAcc -= amount;
         *rcvAcc += amount;
         return 1;
    }
}

int deliverGoods (int count, int pricePerC) {
    int success = pay (sender, receiver, count*pricePerC);
    if(success == 1) {
       sceduleLogistics();
       return 1;
    }
    Return 0;
}
```

Bitcoin 2.0: Smart Contracts

- Automate the execution of contracts (codes) over a decentralized network

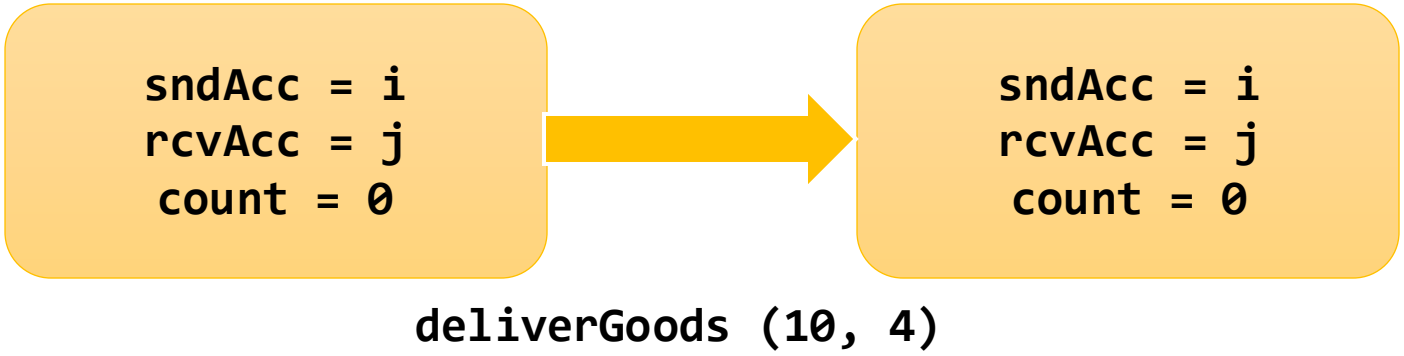
```
int pay (float *sndAcc, float *rcvAcc, float amount) {
    if (*sndAcc < amount) return -1;
    else {
        *sndAcc -= amount;
        *rcvAcc += amount;
        return 1;
    }
}

int deliverGoods (int count, int pricePerC) {
    int success = pay (sender, receiver, count*pricePerC);
    if(success == 1) {
       sceduleLogistics();
       return 1;
    }
    Return 0;
}
```

```
sndAcc = i
rcvAcc = j
count = 0
```

Bitcoin 2.0: Smart Contracts

- Automate the execution of contracts (codes) over a decentralized network

```
int pay (float *sndAcc, float *rcvAcc, float amount) {
    if (*sndAcc < amount) return -1;
    else {
        *sndAcc -= amount;
        *rcvAcc += amount;
        return 1;
    }
}
```

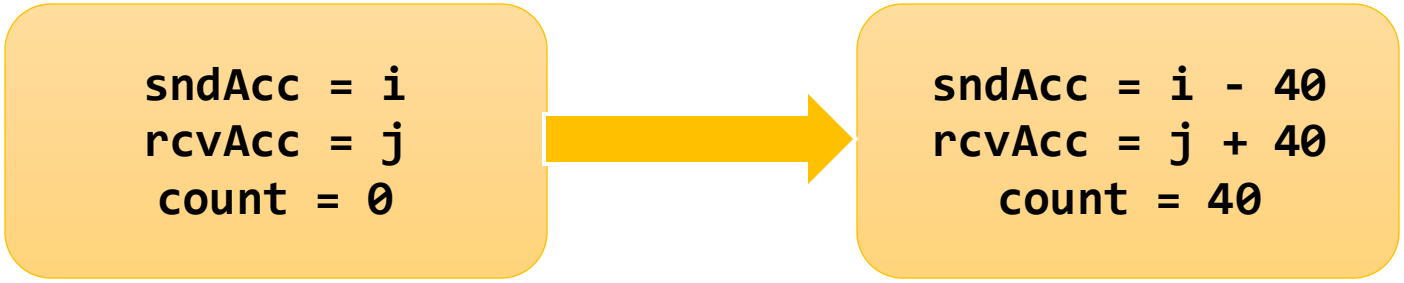



```
int deliverGoods (int count, int pricePerC) {
    int success = pay (sender, receiver, count*pricePerC);
    if(success == 1) {
       sceduleLogistics();
       return 1;
    }
    Return 0;
}
```

Bitcoin 2.0: Smart Contracts

- Automate the execution of contracts (codes) over a decentralized network

```
int pay (float *sndAcc, float *rcvAcc, float amount) {
    if (*sndAcc < amount) return -1;
    else {
        *sndAcc -= amount;
        *rcvAcc += amount;
        return 1;
    }
}
```



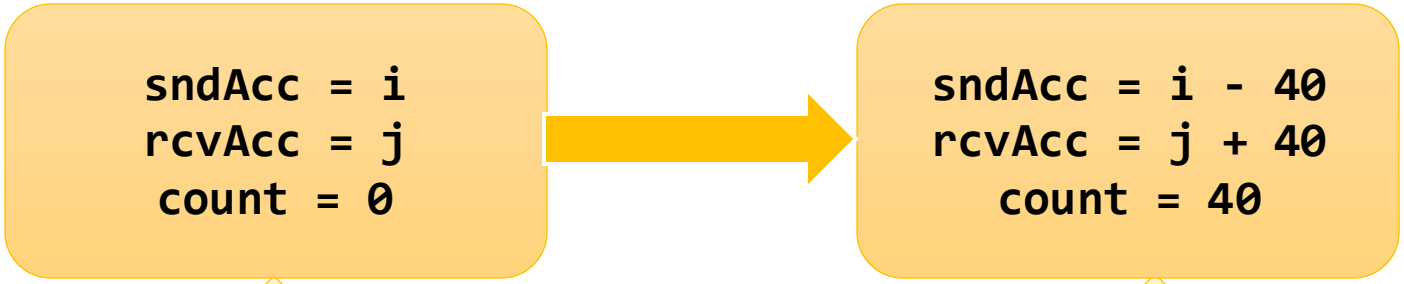

```
deliverGoods (10, 4)
pay(sndAcc, rcvAcc, 40) > 1
```

```
int deliverGoods (int count, int pricePerC) {
    int success = pay (sender, receiver, count*pricePerC);
    if(success == 1) {
       sceduleLogistics();
       return 1;
    }
    Return 0;
}
```

Bitcoin 2.0: Smart Contracts

- Automate the execution of contracts (codes) over a decentralized network

```
int pay (float *sndAcc, float *rcvAcc, float amount) {
    if (*sndAcc < amount) return -1;
    else {
        *sndAcc -= amount;
        *rcvAcc += amount;
        return 1;
    }
}

int deliverGoods (int count, int pricePerC) {
    int success = pay (sender, receiver, count*pricePerC);
    if(success == 1) {
       sceduleLogistics();
       return 1;
    }
    Return 0;
}
```




```
deliverGoods (10, 4)
pay(sndAcc, rcvAcc, 40) > 1
```

Put the states of execution in a blockchain

Smart Contract Execution

Jimmy

Emma

Smart Contract Execution

Jimmy

Off-chain Agreement

Emma

Smart Contract Execution

Jimmy

Off-chain Agreement

Submit the anonymized (through public key encryption) contract to a blockchain network

Emma

Smart Contract Execution

Jimmy

Off-chain Agreement

Submit the anonymized (through public key encryption) contract to a blockchain network

Emma

Everyone in the network can see and validate the execution steps

CryptoKitties – A Popular Game on Ethereum Dapps

From Permissionless to Permissioned Models

- PoW (Nakamoto Consensus) works good in an open network
  - But, transaction latency is very high
  - ~10 minutes in Bitcoin block commitment
  - Few seconds to few minutes for Ethereum (depending on the cost that you pay)

From Permissionless to Permissioned Models

- PoW (Nakamoto Consensus) works good in an open network
  - But, transaction latency is very high
  - ~10 minutes in Bitcoin block commitment
  - Few seconds to few minutes for Ethereum (depending on the cost that you pay)

- **Can we think of any other Blockchain applications beyond cryptocurrency?**

From Permissionless to Permissioned Models

- PoW (Nakamoto Consensus) works good in an open network
  - But, transaction latency is very high
  - ~10 minutes in Bitcoin block commitment
  - Few seconds to few minutes for Ethereum (depending on the cost that you pay)

- **Can we think of any other Blockchain applications beyond cryptocurrency?**
  - The high latency makes them unsuitable for most of the real-time applications

From Permissionless to Permissioned Models

- PoW (Nakamoto Consensus) works good in an open network
  - But, transaction latency is very high
  - ~10 minutes in Bitcoin block commitment
  - Few seconds to few minutes for Ethereum (depending on the cost that you pay)

- **Can we think of any other Blockchain applications beyond cryptocurrency?**
  - The high latency makes them unsuitable for most of the real-time applications

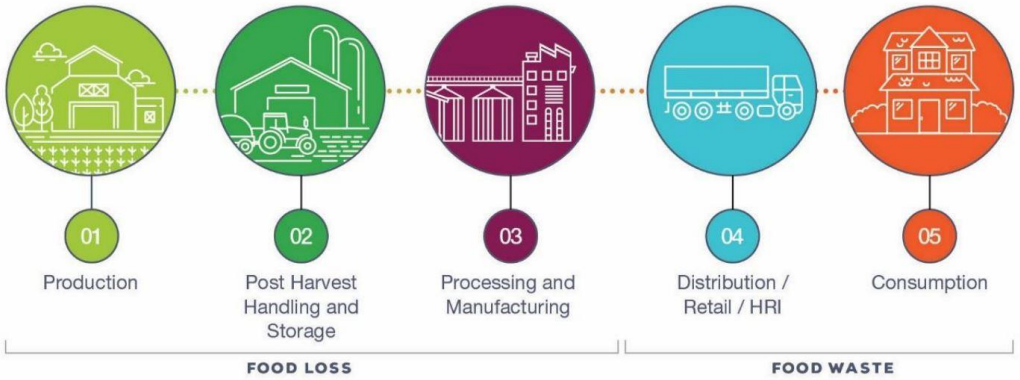
- **But, many decentralized applications do not demand an open environment**

From Permissionless to Permissioned Models

- PoW (Nakamoto Consensus) works good in an open network
  - But, transaction latency is very high
  - ~10 minutes in Bitcoin block commitment
  - Few seconds to few minutes for Ethereum (depending on the cost that you pay)

- **Can we think of any other Blockchain applications beyond cryptocurrency?**
  - The high latency makes them unsuitable for most of the real-time applications

- **But, many decentralized applications do not demand an open environment**
  - The food supply chain
  - Know Your Customer (KYC)
  - Trade financing
  - ...



Blockchain 3.0

- "Trustless Decentralization" over a closed network

Blockchain 3.0

- "Trustless Decentralization" over a closed network
  - Automatically transact assets among multiple organizations who do not trust each other
  - Run smart contracts within a consortium of various organizations – the individual organizations know each other but do not trust each other

Blockchain 3.0

- "Trustless Decentralization" over a closed network
  - Automatically transact assets among multiple organizations who do not trust each other
  - Run smart contracts within a consortium of various organizations – the individual organizations know each other but do not trust each other

- **Advantages:**
  - Go back to the classical distributed consensus protocols – low latency for commitment and high transaction throughput
  - Use "Witness Cosigning" instead of "Proof Mining" for new block generation
    - Classical Distributed Consensus + Digital Signature

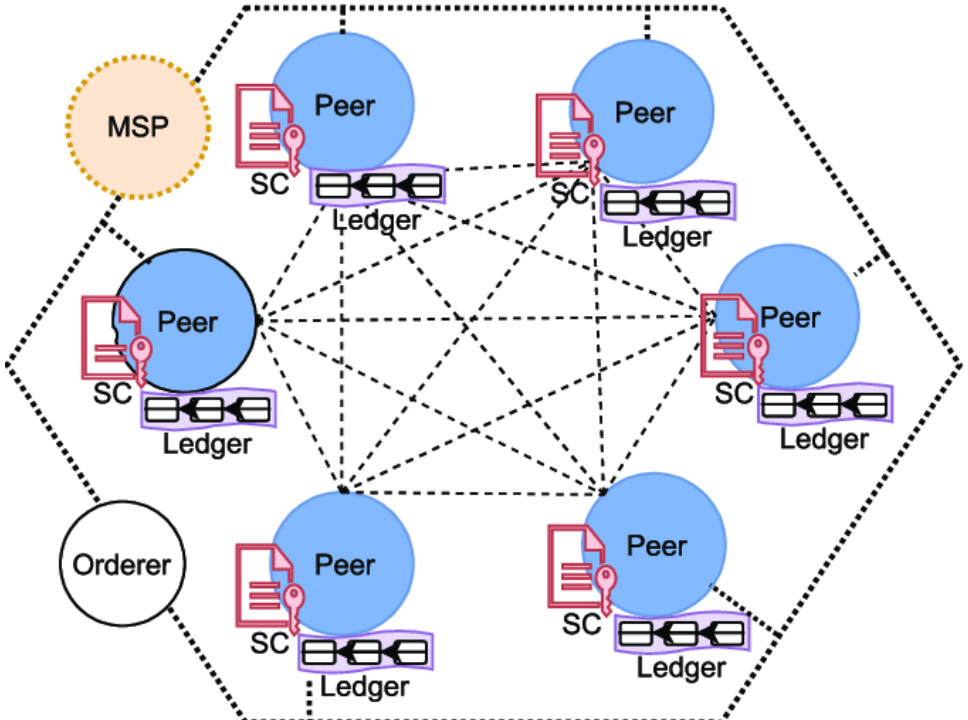
Permissioned (Private) Blockchain

- The participants are pre-authenticated and pre-authorized
  - But they can still behave maliciously

Permissioned (Private) Blockchain

- The participants are pre-authenticated and pre-authorized
  - But they can still behave maliciously

- Run blockchain (and smart contracts) on top of this closed network
  - Ensure trusted computing among the participants



Permissioned Blockchain in Businesses

- There can be plenty of business use cases which can be decentralized using permissioned blockchains
  - Inter-bank transactions
  - Supply chain management
  - Land record management
  - Government use cases
  - …

- However, any decentralization also has its own pitfalls
  - Deployment overhead
  - Managerial issues
  - Backward compatibility with existing systems
  - ...

The Next Steps

- We'll see from the scratch how to design a blockchain-based system and understand its cost-benefit tradeoffs
- **Next class:** Prof. Sural to continue with the basic cryptography followed by the elemental design of the core blockchain data structures