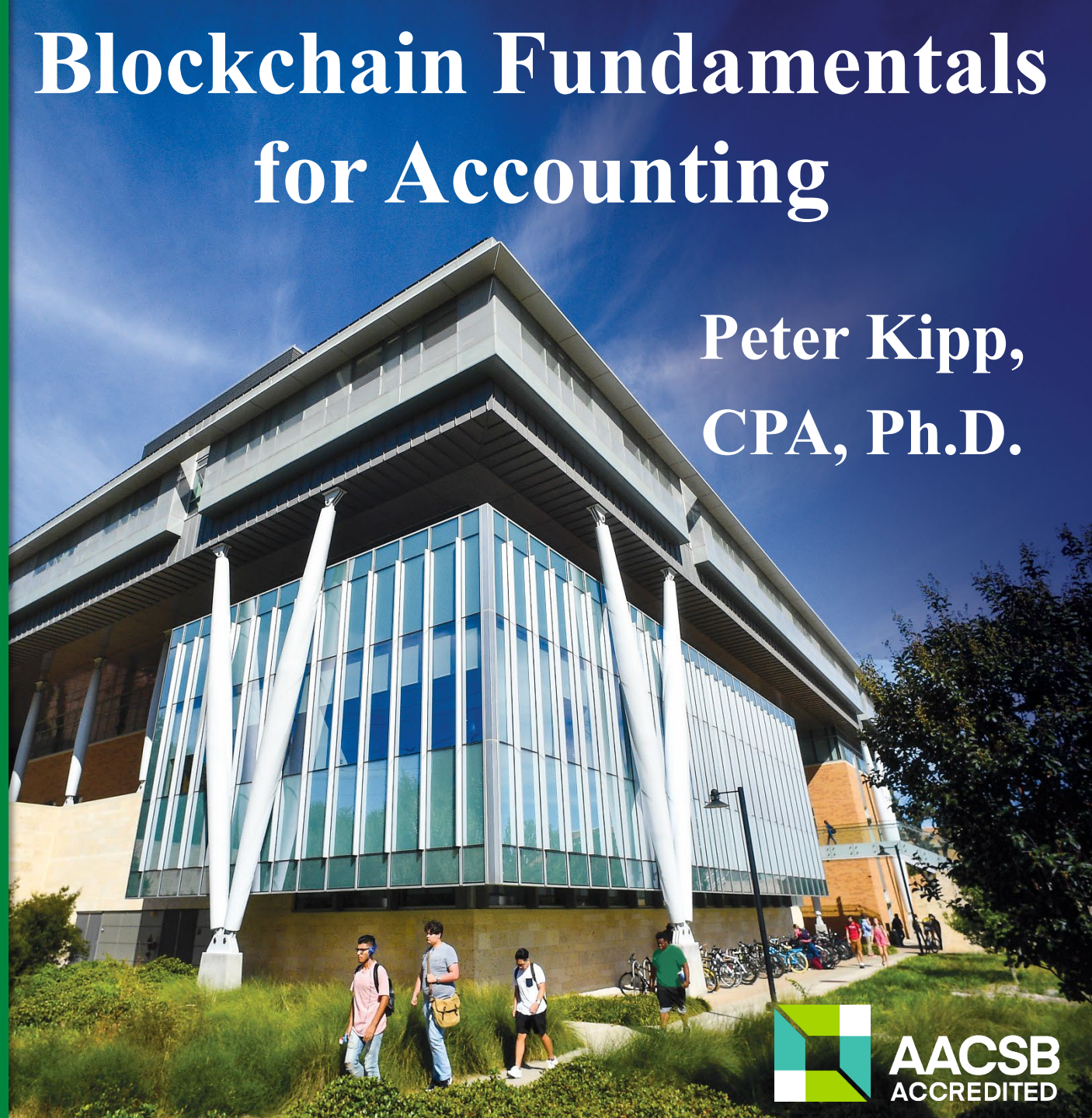
Blockchain Fundamentals for Accounting

Peter Kipp,
CPA, Ph.D.

G. BRINT RYAN
COLLEGE
OF BUSINESS

UNT®

EST. 1890



AACSB
ACCREDITED

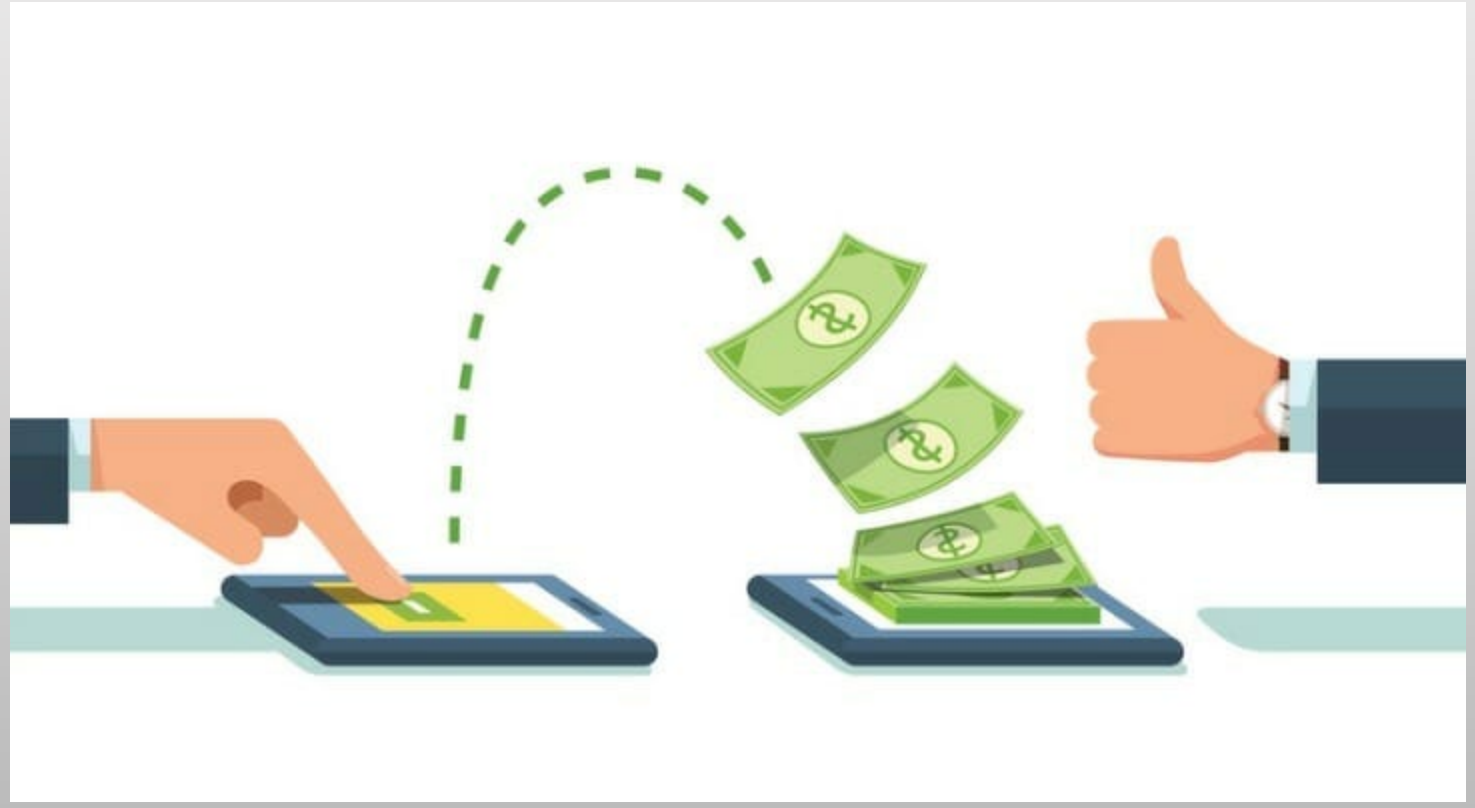
Objectives

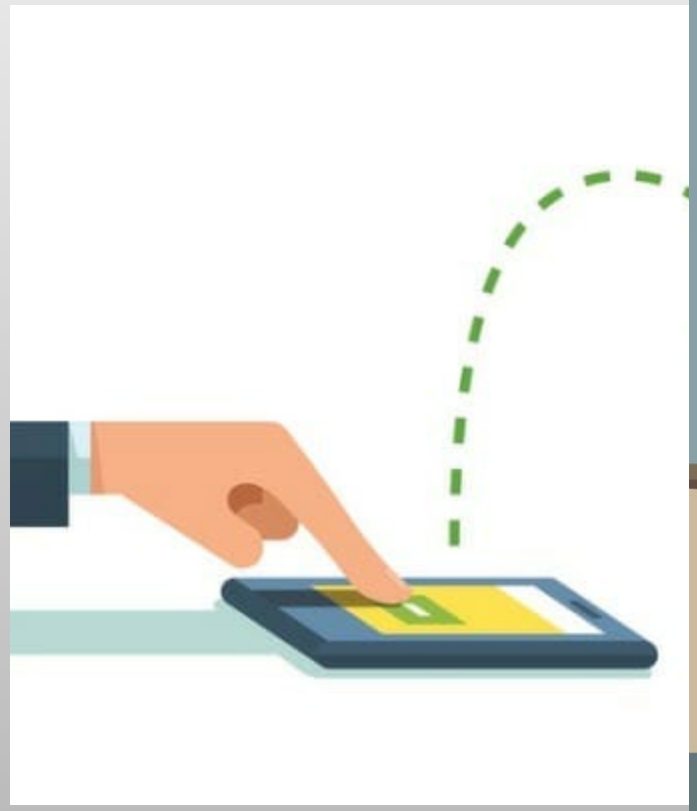
- Define and describe the underlying technologies of blockchain
- Describe some shortcomings of blockchain
- Examples of current and early adoption
- Considerations for adoption within your organization

What is Blockchain?

- “What is a Blockchain? Is It Hype?” (NYT 2021)
- “Blockchain Data Is The Next Big Thing…” (Forbes 2022)
- “…[blockchain] offers a sweeping vista of opportunity to reimagine how the financial system can and should work in the Internet era…” (Marc Andreesen 2014)
- “Blockchain technology will revolutionise far more than money: it will change your life.” (Dominic Frisby 2016)
- “Blockchain technology is the most significant invention since the internet and electricity” (Mark Metry 2017)
- “There are no good uses for blockchain” (Kai Stinchcombe 2018)
- “[O]ne of the most overhyped technologies ever” (Nouriel Robini 2018)


BITCOIN DIGITAL DECENTRALIZED PEER TO PEER



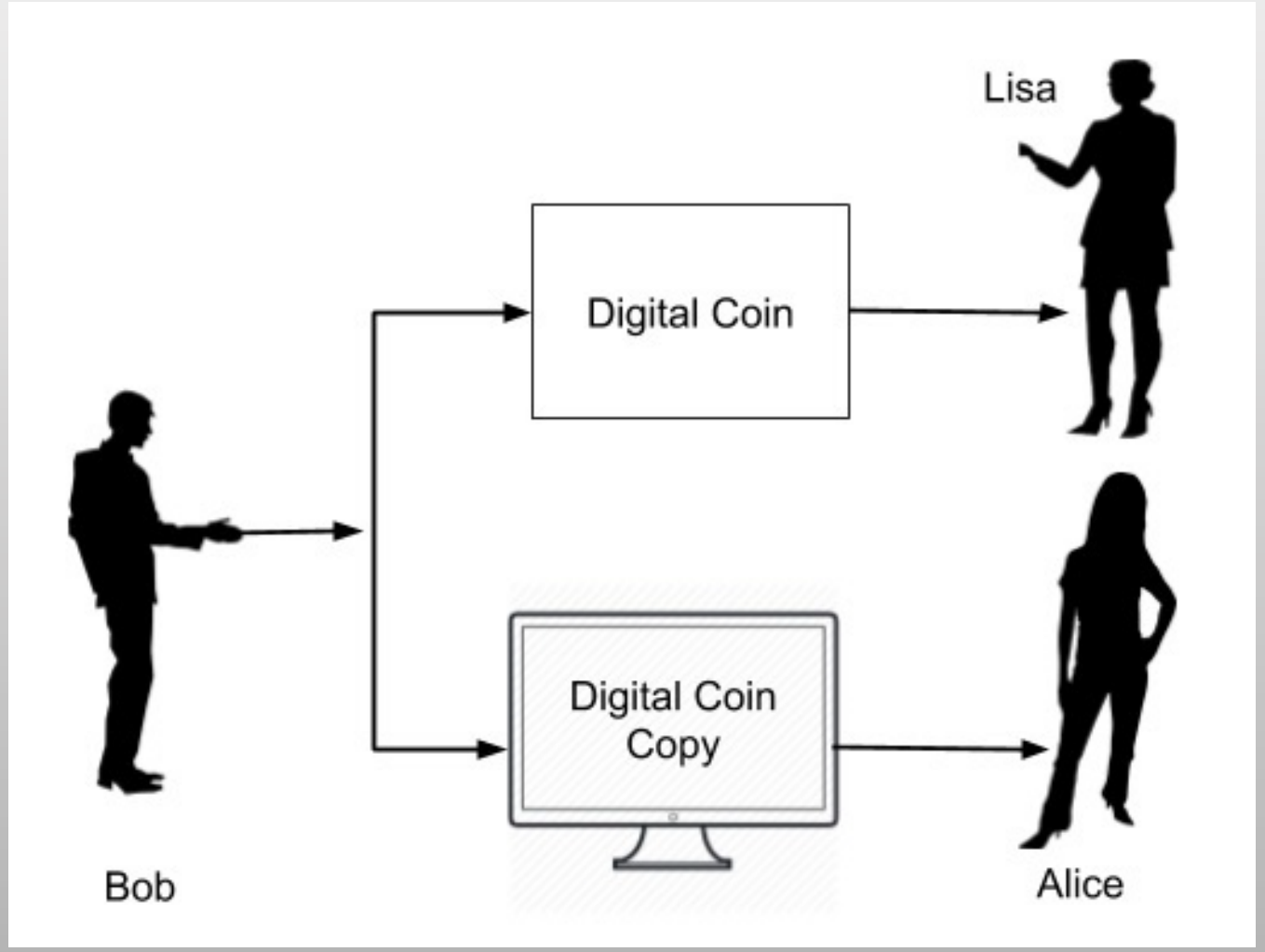



SOLUTION

PayPal

PayPal

venmo


Lisa
Digital Coin
Digital Coin
Copy
Bob
Alice


Nous connaîtrions-nous
seulement un peu nous-mêmes,
sans les arts!
Gabrielle Roy (1909-1983)
Could we ever know
each other in the slightest
without the arts!
EYU0661660
EYU0661660
20
IMPRIMÉ EN 2005 / PRINTED IN 2005
© 2004 BANK OF CANADA © 2004 BANQUE DU CANADA

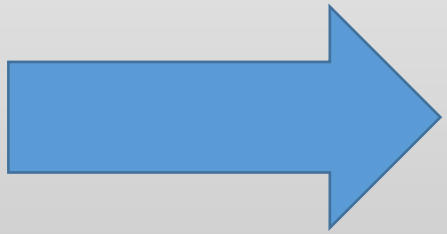

BANK
OF
CANADA


BLOCKCHAIN

How does Blockchain Work?

- Bitcoin blockchain: aggregates transactions into blocks and chains them together.
- Original idea from Haber and Stornetta (1991) – Secure timestamping of digital documents.
  - Each certificate ensures the validity of the transaction
- Sophisticated application of several existing technologies.
  - Public key – private key (asymmetric) encryption
  - Cryptographic hashing
  - Distributed ledger
  - Peer-to-peer consensus

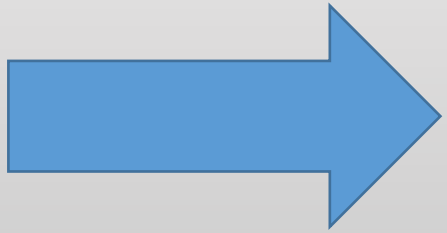
Asymmetric Encryption

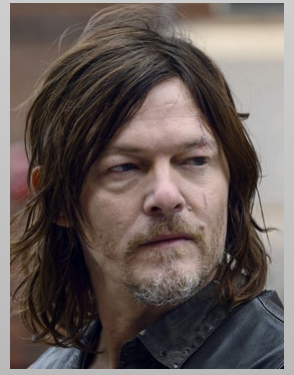


Public

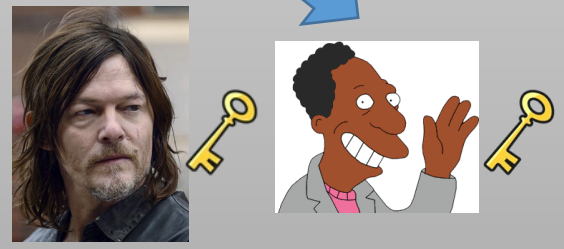
Private

Asymmetric Encryption





Asymmetric Encryption

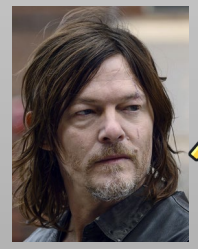


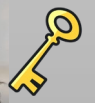
Four Necessary Conditions

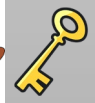
- 1) The asset is valid (i.e., the cash exists)
- 2) The asset has not been consumed/used in a previous transaction (i.e., double-spending)
- 3) Total value that comes in is the same that went out (i.e., not creating or destroying value)
- 4) The transaction is validly signed by the owner's private key

Asymmetric Encryption

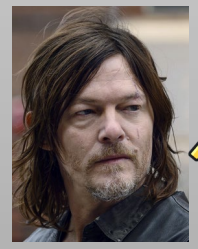
Asymmetric Encryption



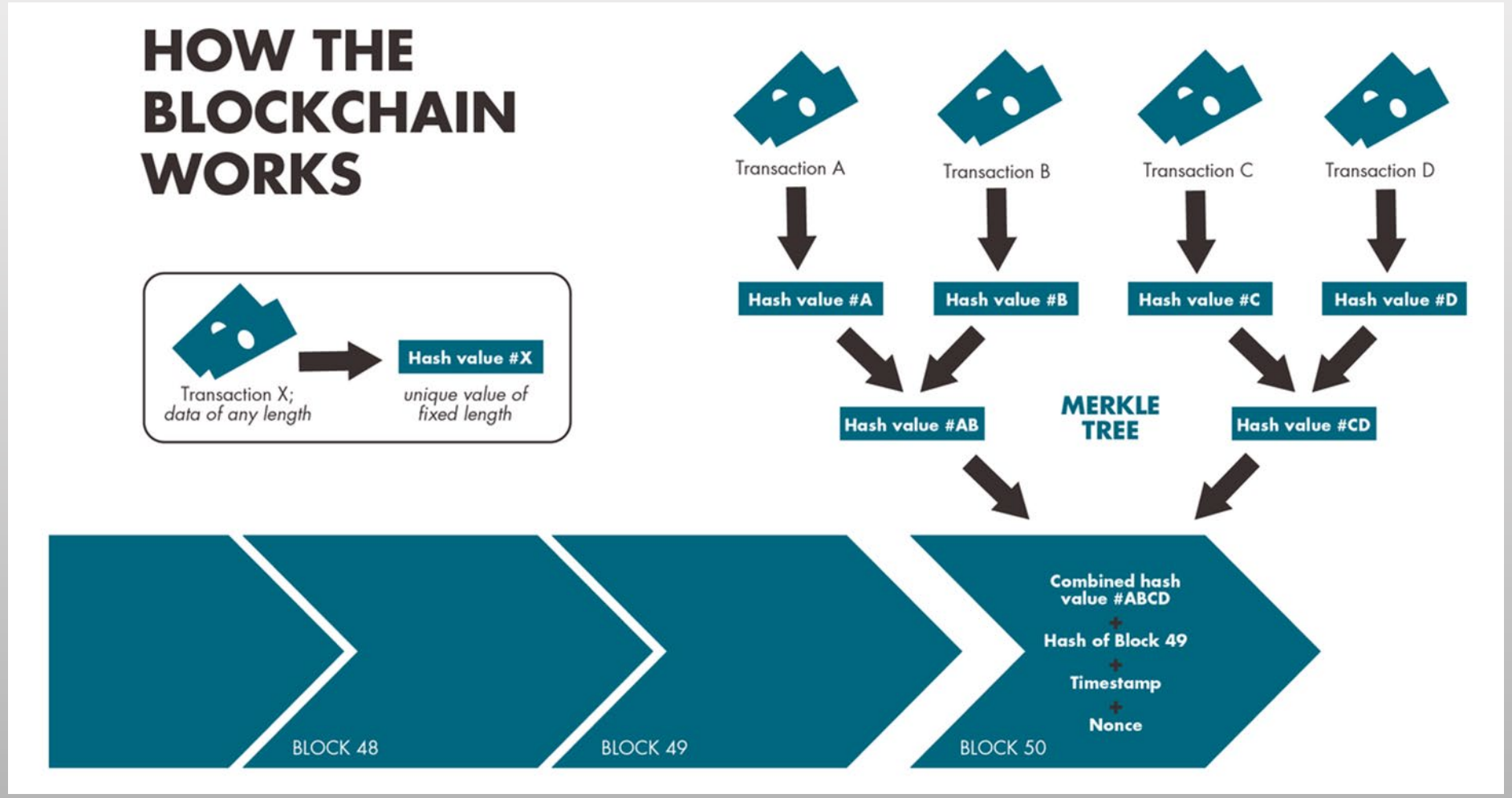




Asymmetric Encryption



Cryptographic Hash Function



Cryptographic Hash Function

- Transaction A
  - Alice sent $100.00 to Bob at 14:25 10-02-2023.
  - Hash: 2f6248f57ab21845db5bb03935b884308c6f66fb62d980f56ed76a06261fc7d8

Cryptographic Hash Function

- Transaction A
  - Alice sent $100.00 to Bob at 14:25 10-02-2023.
  - Hash: 2f6248f57ab21845db5bb03935b884308c6f66fb62d980f56ed76a06261fc7d8
- Transaction B
  - Carl sent $200.00 to Daryl 15:10 10-02-2023.
  - Hash: ff10756385dbc6d127da28202f2eb027b231a95a8751a2c0b182487a9ab86dff

Cryptographic Hash Function

- Concatenate # Transaction A and # Transaction B
  - 2f6248f57ab21845db5bb03935b884308c6f66fb62d980f56ed76a06261fc7d8ff10756385dbc6d127da28202f2eb027b231a95a8751a2c0b182487a9ab86dff
- Concatenated Hash: 6c5daa11004ed417d329dda7f5d231ecbac372280fcace4e305f6926ef5bf86c

Cryptographic Hash Function

- Now, what if I change the original transaction?
- Alice sent $100.00 to Carl at 14:25 10-02-2023.
  - Hash: 0c02e8848b996c978b37ea84dedc688bdbe463daf7ed0a45563ac147c7f737f3
- Updated Concatenated AB Hash:
  - a1bacf8ef5dcc0364b65076f36893a6e3300f3c27ae7c037077c7c072b60bb72
- Original Concatenated AB Hash:
  - 6c5daa11004ed417d329dda7f5d231ecbac372280fcace4e305f6926ef5bf86c

Cryptographic Hash Function

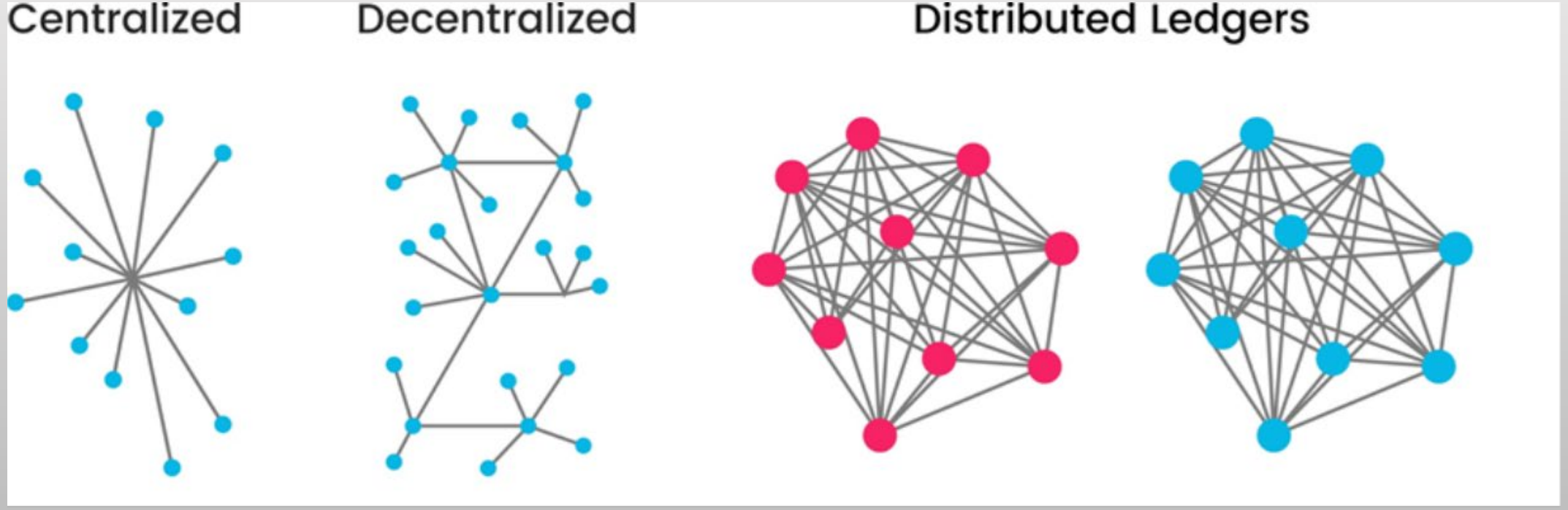
- Now, what if I change the original transaction?
- Alice sent $100.00 to Carl at 14:25 10-02-2023.
  - Hash: 0c02e8848b996c978b37ea84dedc688bdbe463daf7ed0a45563ac147c7f737f3
- Updated Concatenated AB Hash:
  - a1bacf8ef5dcc0364b65076f36893a6e3300f3c27ae7c037077c7c072b60bb72
- Original Concatenated AB Hash:
  - 6c5daa11004ed417d329dda7f5d231ecbac372280fcace4e305f6926ef5bf86c
- Change is “tamper evident”

Cryptographic Hash Function

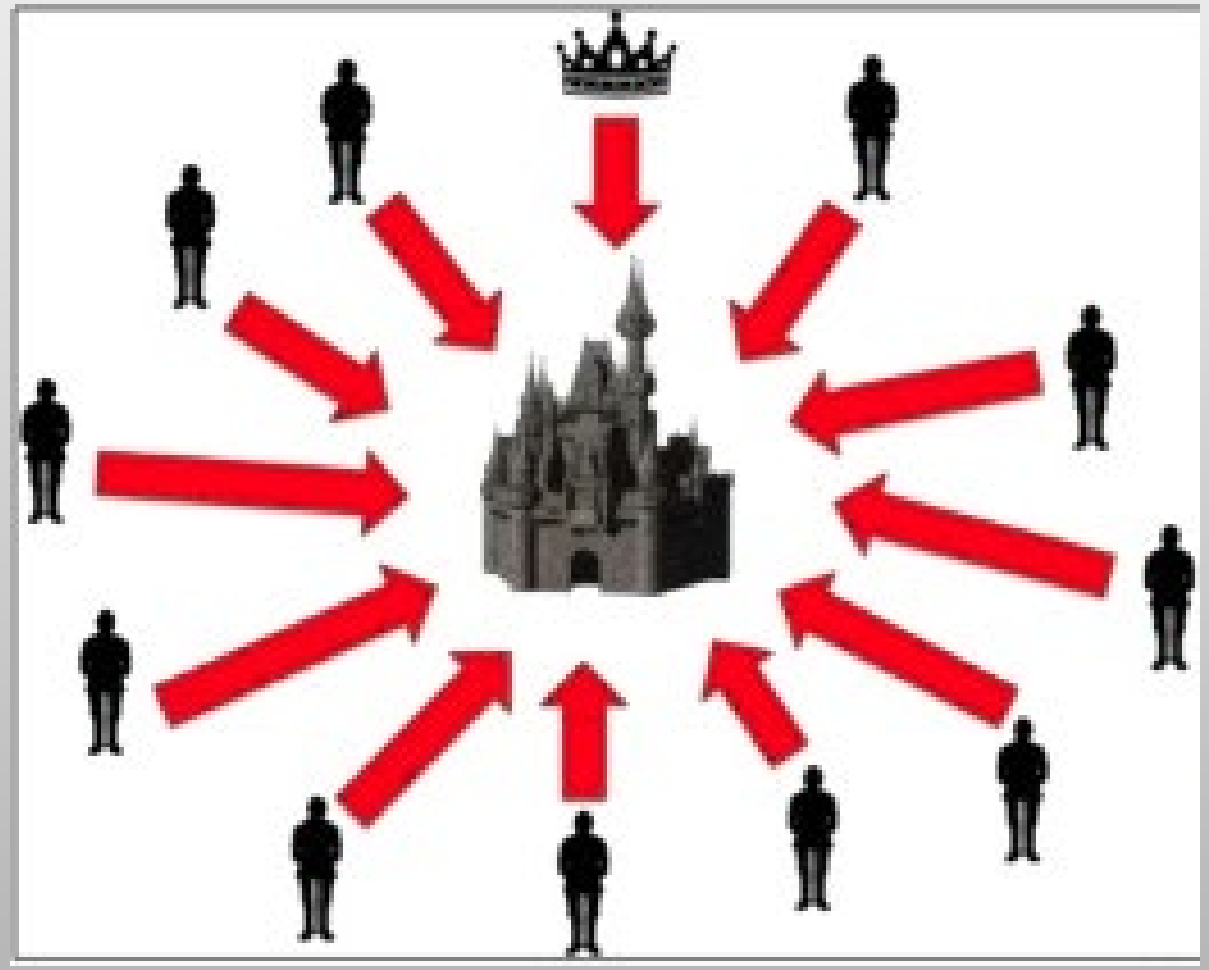
Cryptographic Hash Function

- Three necessary conditions:
- 1) Collision resistant – it is infeasible to find two values that result in the same hash
  - If $x \neq y$ and $H(x) = H(y)$, not collision resistant
- 2) Hiding – given the hash of a nonce and a message, it is infeasible to determine the message.
  - Nonce is a "number used only once"
  - E.g., cannot "decrypt" the hash
- 3) Puzzle friendliness – there is no strategy better than trying random values to solve for the nonce.

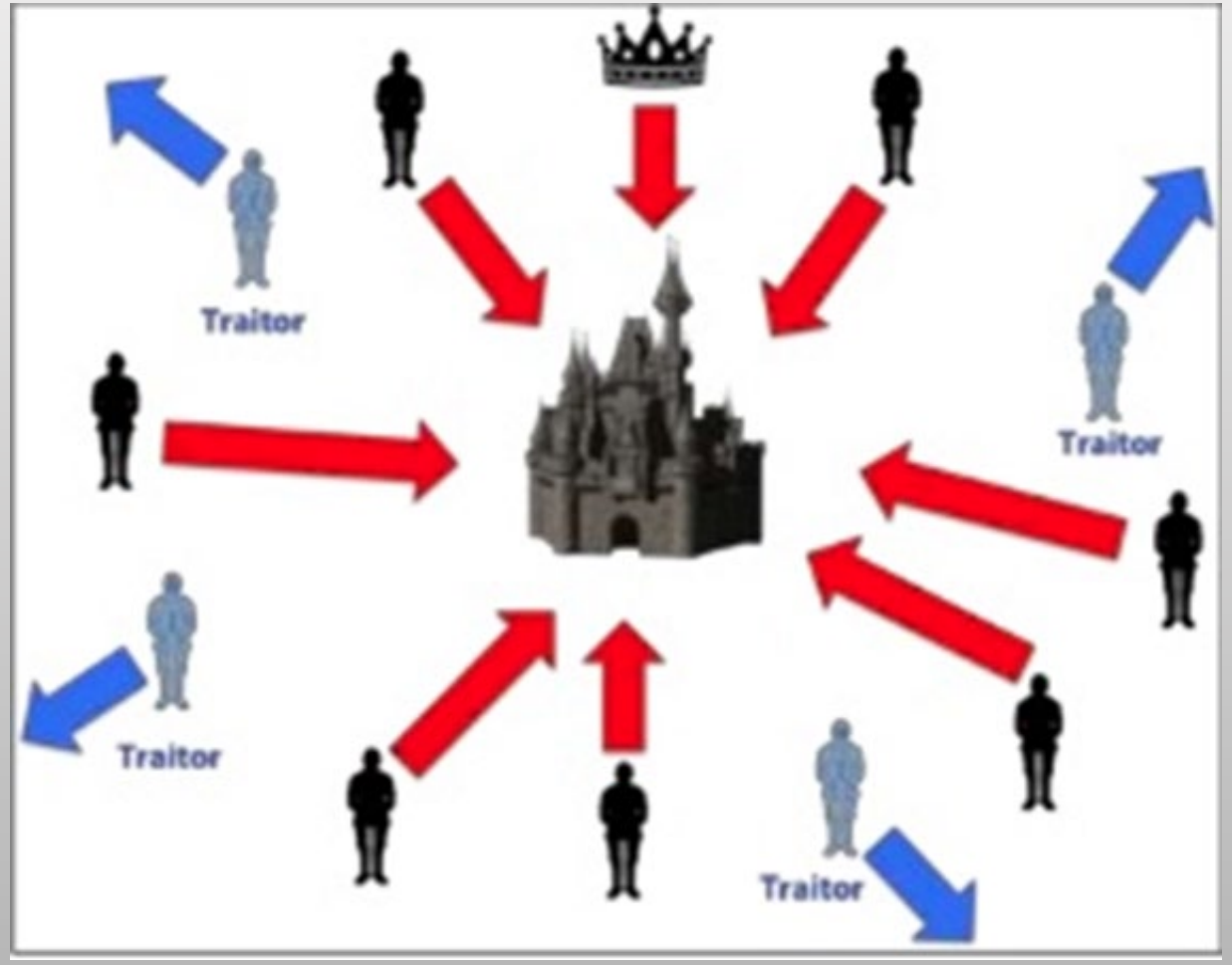
Distributed Consensus Protocol



Distributed Consensus Protocol



Distributed Consensus Protocol

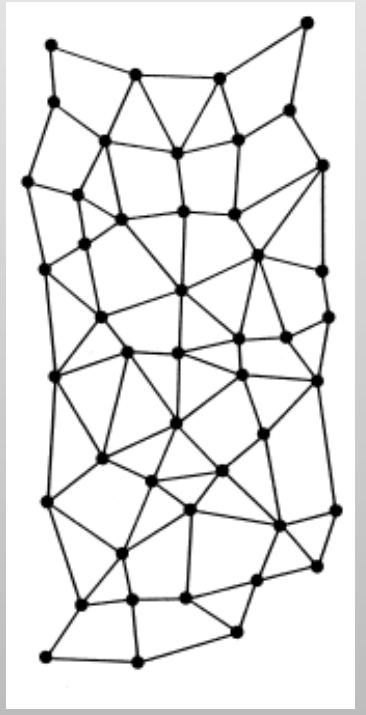


Distributed Consensus Protocol

- The protocol must have two properties:
  - It must terminate with all honest nodes in agreement on a value.
  - The value must have been generated by an honest node.
- But what does “honesty” mean when we don’t have perfect information?
  - Impossible to know which transactions are morally legitimate.
  - How do we incentivize “honest” behavior?

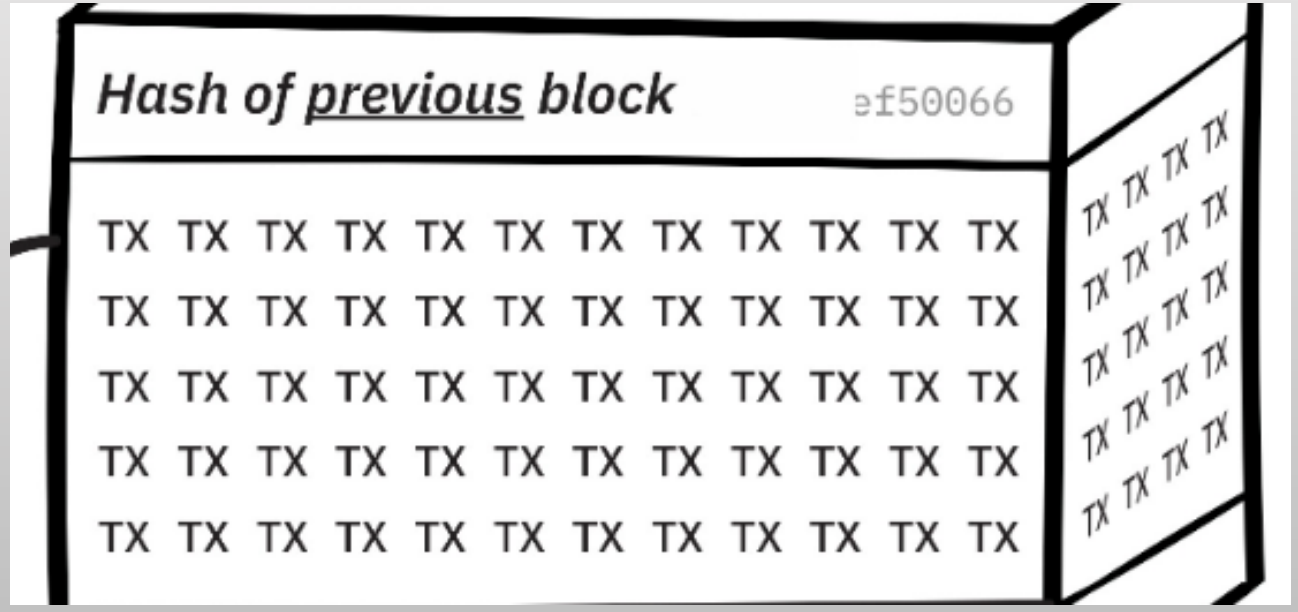
Distributed Consensus Protocol

- 1) New transactions are broadcast to all nodes
  - *But*, not yet formally added to the blockchain. They are "unconfirmed" and stored in nodes memory.



Distributed Consensus Protocol

- 1) New transactions are broadcast to all nodes.
- 2) Each node collects new transactions into a block



Distributed Consensus Protocol

- 3) In each round, a *random* node gets to broadcast its block
  - Probability is proportional to some scarce resource in a Proof of Work system.
  - Bitcoin blockchain uses a hash puzzle to proxy for computing power
    - Must find a nonce that generates a certain amount of leading 0's in the hash
    - Example: 19 leading zeroes

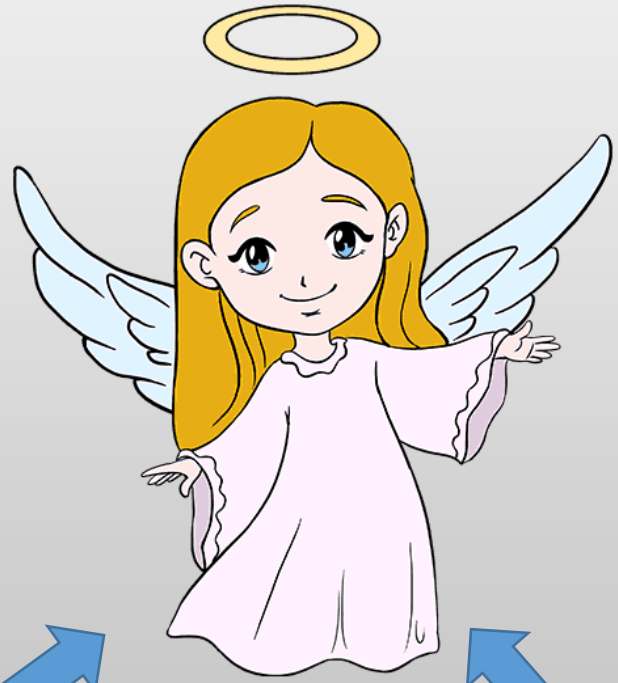
Distributed Consensus Protocol

- 00000000000000000369ae2244f8178d555d9c33a722b165f2538f3b0c5b3a
- Nonce: 2,825,505,042
- *h*(Previous Hash + Merkle Root + Nonce) = Current Hash

Distributed Consensus Protocol

- 4) Other nodes accept the block only if all transaction in it are valid (e.g., unspent bitcoin, valid signatures)
- 5) Nodes express their acceptance of the block by including its hash in the next block they create

Distributed Consensus Protocol



Distributed Consensus Protocol

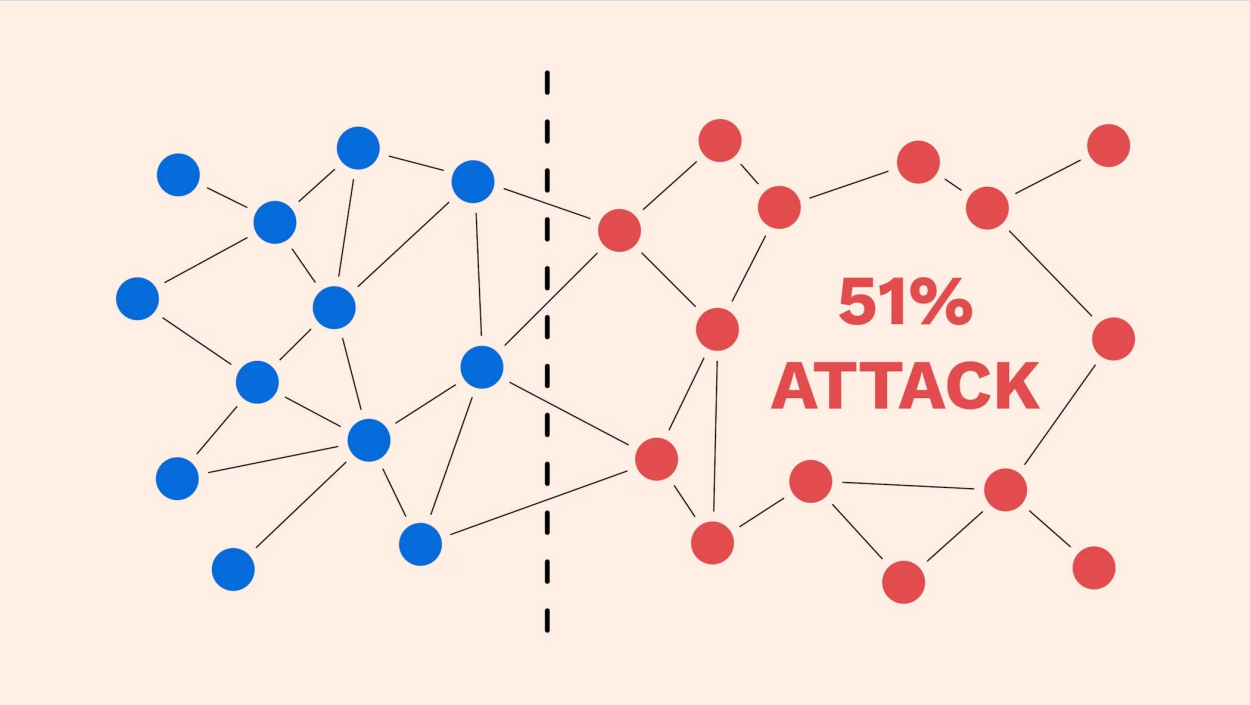
- 1) Must be difficult to compute (e.g., puzzle friendliness)
  - Approximately 269 exahashes/second
  - 269 quintillion hashes generated by all miners on the bitcoin blockchain/second
- (2) Parametizable
  - i.e., recalculates the difficulty of the hash puzzle every 2,016 blocks to keep the rate of block generation one block/10 minutes
- (3) Trivial to verify
  - i.e., easy to confirm the hash with the nonce

Distributed Consensus Protocol

- Other consensus protocols include:
  - Proof of Stake
    - Avoids energy expenditure of PoW
    - Randomly assigns block leadership to participants proportional to their stake in the system
    - Vulnerable to gaming through forking
  - Proof of Elapsed Time
    - Nodes are required to wait for a randomly determined time period (determined by a trusted code), and the first one to complete the designated waiting period wins the new block.
  - Proof of Importance
    - Similar to PoS, but attempts to discourage gaming by randomly assigning block leadership to participants proportional to their activity (e.g., number of transactions, amount spent, etc.).
  - Proof of Activity
    - Hybrid of PoW and PoS

Is Blockchain Invincible?

- 51% attacks
  - Targets smaller cryptocurrency
  - Usually requires a “hard fork”



Is Blockchain Invincible?

- Transactional Malleability
  - Input address (where is it coming from), output address (where is it going), the asset being sent, and the cryptographic signature of the sender
    - Can't change the transaction semantics without subverting the cryptography
    - However, can make amendments that change the transaction ID or the hash
  - If the amended transaction is accepted by the network first, the original transaction will not be accepted
- Compromised private keys and code vulnerability
  - Ethereum Decentralized Autonomous Organization (DAO)
  - Mt. Gox
  - Bitfinex

Why are Accountants Interested?

- **Audit** – Immutable audit trail
- **Financial Services** – Decreased settlement times
- **Tax Authorities** – Immutable ledger
- **Supply Chain Management** – Record of asset provenance
- **Smart Contracts** – Boolean Logic

Examples of blockchain in practice

- Prototype blockchain to identify where food-borne illnesses originated in the supply chain
- Automated processing of invoices and payments to 70 carriers
  - 70% of invoices requiring reconciliation to less than 1%

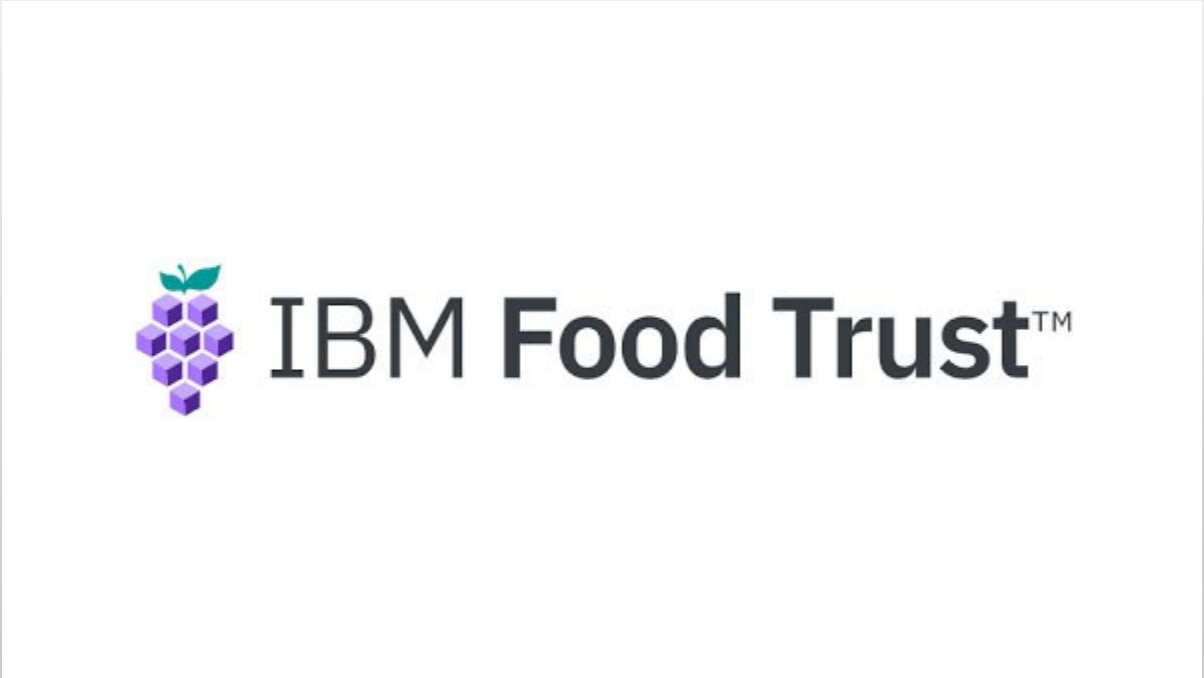
Examples of blockchain in practice

- LINQ – Pre-IPO trading on the private market

Examples of blockchain in practice

- Control and sell “inherent human data”

Examples of blockchain in practice



- Immutable and shared record of food provenance

Bitcoin Blockchain Shortcomings

- Inefficiency and scalability of the proof-of-work consensus protocol
  - Bitcoin blockchain allows 3.3 to 7 transactions a second
    - Visa processes 1,700 transactions a second and could process 24,000 transactions a second
  - Bitcoin blockchain consumes 150 terawatt hours annually.
    - The same energy consumed as the entire country of Argentina.
  - Several alternative cryptocurrencies are investigating different consensus mechanisms to address shortcomings of bitcoin.
- Private (permissioned) blockchains
  - Vulnerable to Byzantine General problem
- Side deals
  - No presence on the blockchain
- Regulatory requirements
  - Financial services industry needs to comply with anti-money laundering and know your customer laws/regulations

So… what if I want to start a blockchain?

- Bitcoin blockchain is designed to be…
  - Trustless
  - Record assets that are only “on-chain”
  - Pseudo-anonymous

So… what if I want to start a blockchain?

- Bitcoin blockchain is designed to be…
  - Trustless
  - Record assets that are only “on-chain”
  - Pseudo-anonymous

Smart Contracts

(solving the problem of trust)

- Agreement written directly into lines of code
  - Acts as an escrow account
  - Once condition(s) are met, the code executes
- Example: FOB Shipping Point
  - Once items are on-board, seller's obligation is complete, and the smart contract executes the code on the blockchain to release payment
- But… smart contracts cannot interact with data/systems outside their blockchain

Blockchain Oracle Problem

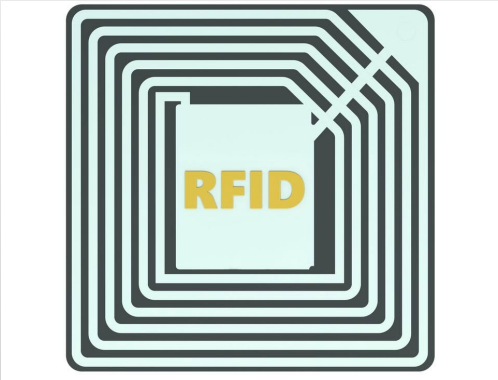
- Oracle: Facilitates communication between blockchains and any “off-chain” system
  - FOB Shipping Point: Oracle could read that RFIDs of associated product have been loaded on the truck
- Could be IoT sensors, APIs pulling data from the web, RPA processes, etc.
- Sheldon (2021) argues that oracles are analogous to service organizations
- **Considerations:** Does the oracle provide complete and accurate data? How do I gain assurance over the provenance of goods? How is appropriate consensus determined?

NFTs (solving the problem of physical assets)

- Bitcoin is only generated by the blockchain.
- How do I represent the physical world on a blockchain?

Blockchain in Practice

- How do I represent the physical world on a blockchain?



- **Considerations:** Who is responsible for minting new NFTs? How do I verify asset existence/ownership? How is consensus reached that an NFT should be added to the blockchain?

Four stages for blockchain implementation (Sheldon 2022)

- 1) Consortium Charter - Formally defines rights and privileges, such as:
  - 1) verify the occurrence of transactions
  - 2) submit transactions
  - 3) validate transactions and participate in consensus
  - 4) maintain a copy of the blockchain

Four stages for blockchain implementation (Sheldon 2022)

- 2) Asset Creation
  - 1) identification tag is attached to asset after creation
  - 2) asset creation is observed by participants/oracles
  - 3) attributes assigned to NFT and NFT minted
- 3) Asset Transfer
  - 1) validate transfer of the asset
  - 2) smart contract assisted transfer

4) Asset Retirement

- 1) When should token be “burned”

References for Future Reading

- Narayanan, A., J. Bonneau, E. Felten, A. Miller, S. Goldfeder. 2016. *Bitcoin and cryptocurrency technologies: a comprehensive introduction*. Princeton University Press.
- O'Dowd, A., V. Ramakrishna, P. Novotny, N. Gaur, L. Desrosiers, S. Baset. 2018. *Hand-On Blockchain with Hyperledger*. Packt Publishing.
- Sheldon, M. D. 2021. Auditing the blockchain oracle problem. *Journal of Information Systems* 35 (1): 121-133.
- Sheldon, M. D. 2022. Tracking tangible asset ownership and provenance with blockchain. *Journal of Information Systems* 36 (3): 153–175.

G. BRINT RYAN
COLLEGE
OF BUSINESS

UNT®

EST. 1890

Thank you.