Blockchain Technology Fundamentals

Prof. Neeraj Kumar, SMIEEE,

Professor, CSED

Thapar Institute of Engineering and Technology, Patiala, Punjab, India

Email: Neeraj.kumar@thapar.edu

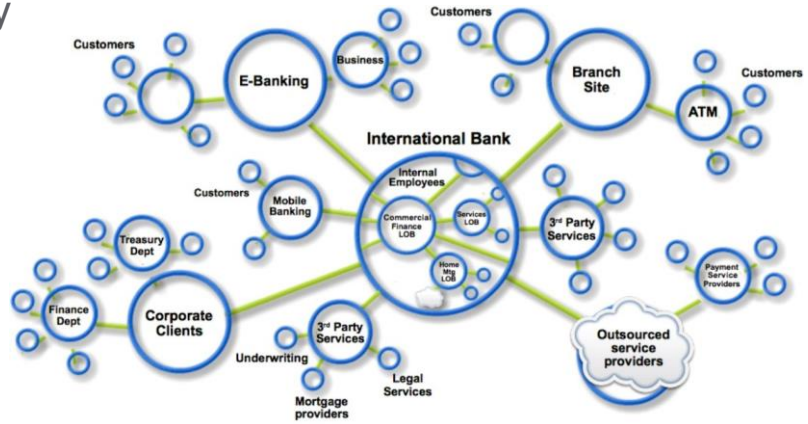
Contents of the presentation

- Basics of Blockchain
- Key components and terminologies used
- Blockchain Structure
- Consensus Algorithms
- Implementation and Challenges

Business Networks, Markets & Wealth

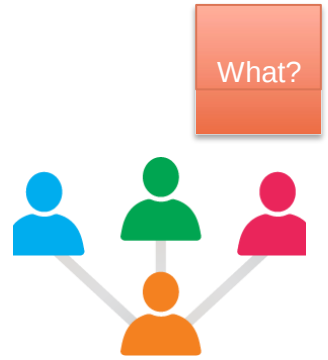
What?

- Business Networks benefit from connectivity
  - Connected customers, suppliers, banks, partners
  - Cross geography & regulatory boundary
- Wealth is generated by the flow of goods & services across business network
- Markets are central to this process:
  - Public (fruit market, car auction), or
  - Private (supply chain financing, bonds)



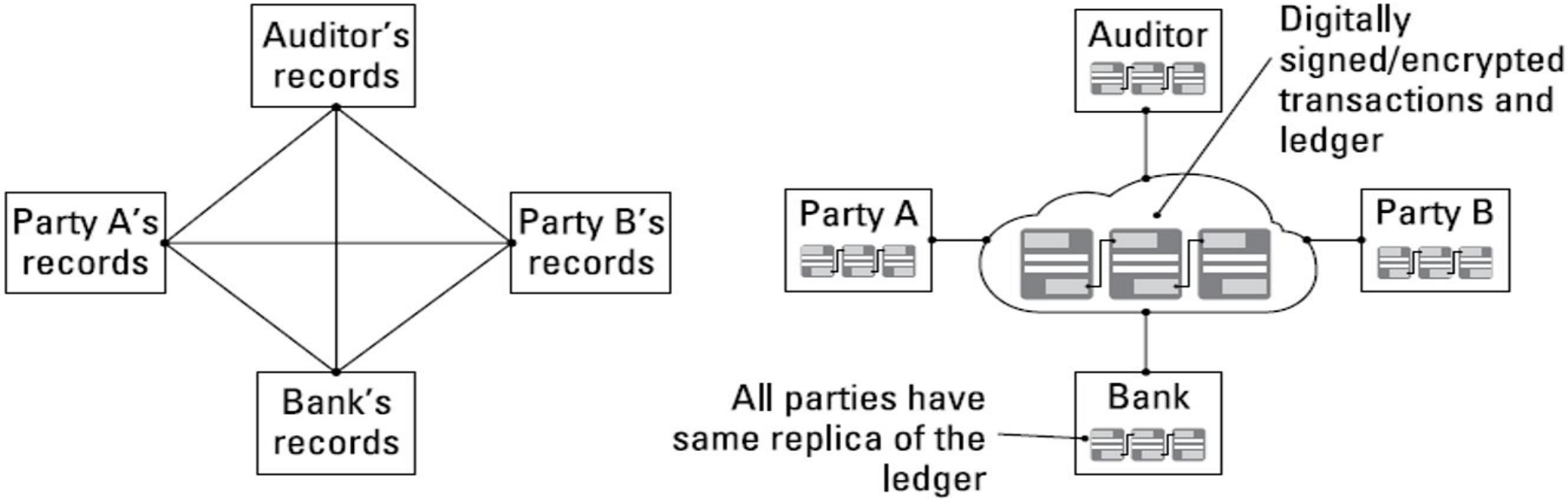
Participants, Transactions & Contracts

- Participants - members of a business network
  - Customer, Supplier, Government, Regulator
  - Usually resides in an organization
  - Has specific identities and roles
- Transaction - an asset transfer
  - John gives a car to Anthony (simple)
- Contract - conditions for transaction to occur
  - If Anthony pays John money, then car passes from John to Anthony (simple)
  - If car won't start, funds do not pass to John (as decided by third party arbitrator) (more complex)



Blockchain's Origin

- The shortcomings of current transaction systems
  - During 2000's financial crisis



Blockchain Benefits

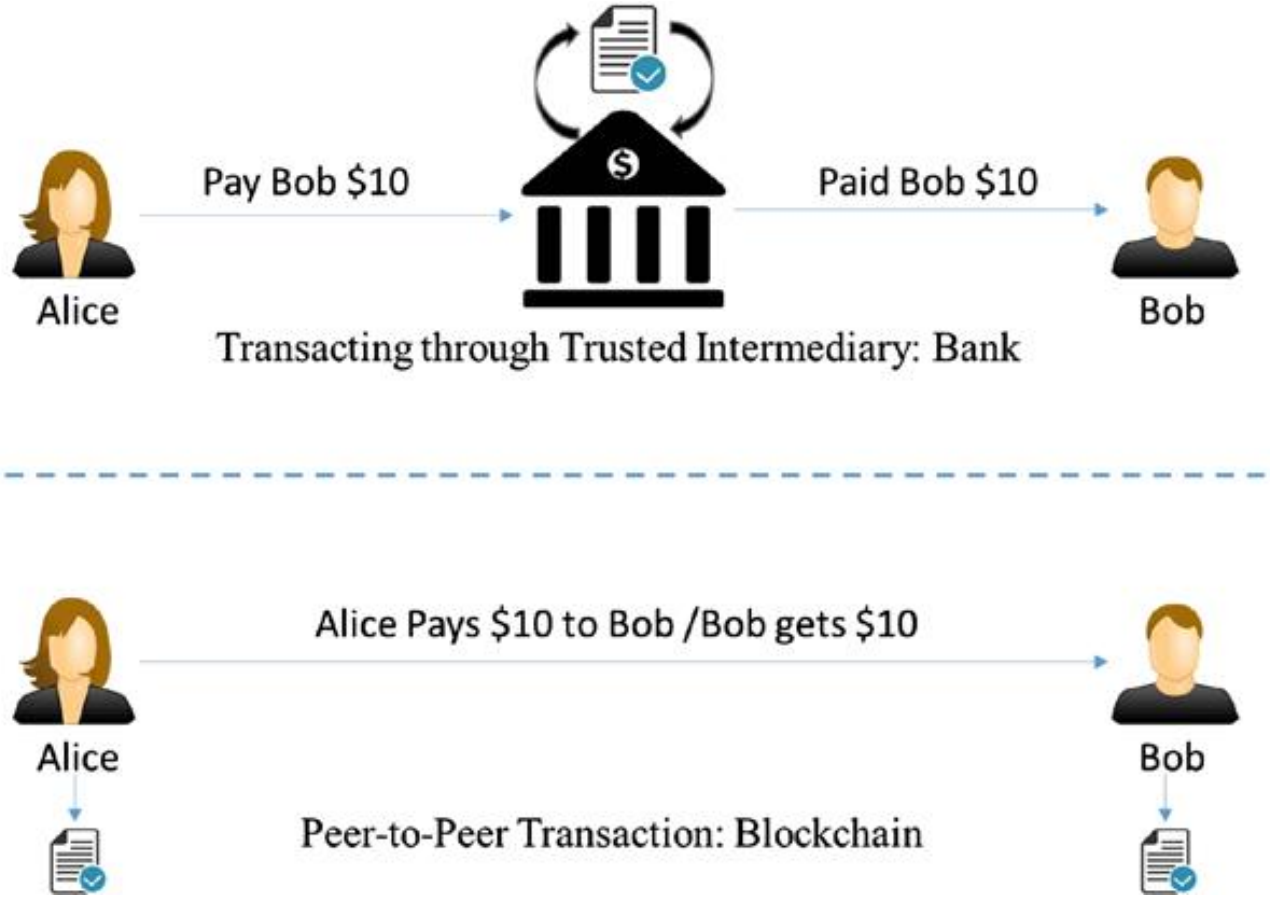
Reduce costs and complexity

Improve discoverability

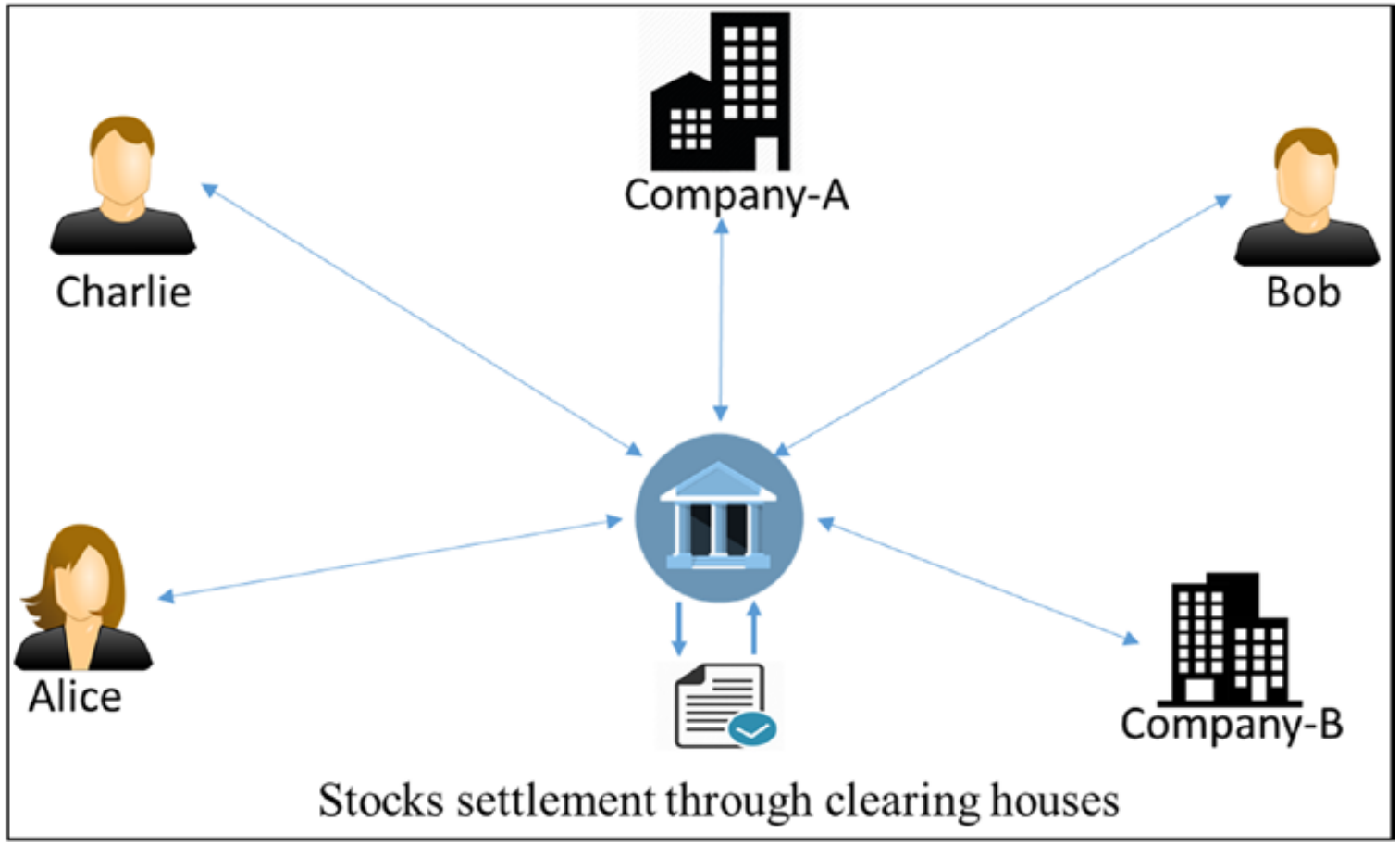
Trusted recordkeeping

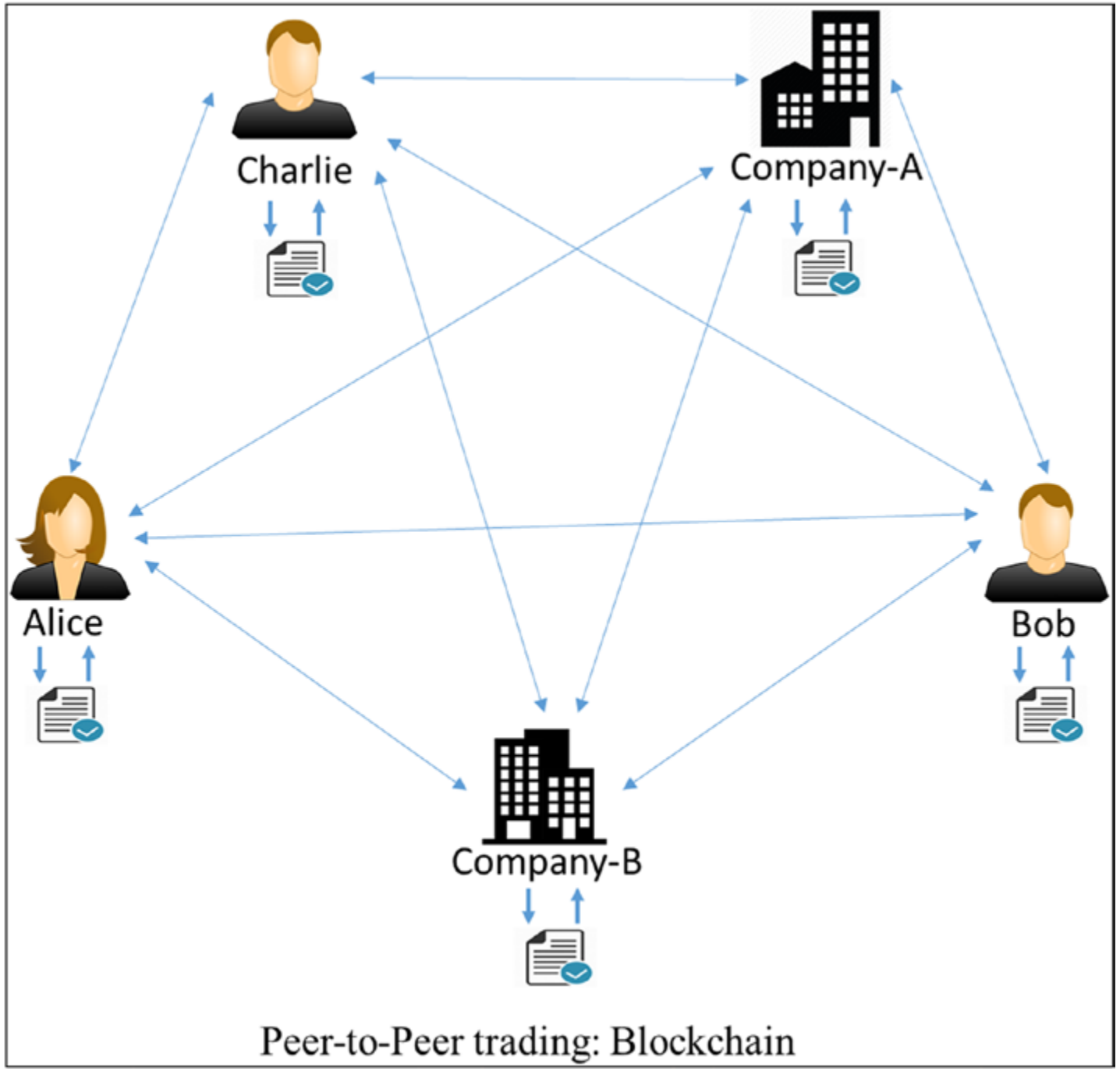
Shared trusted processes

Transactions with and without blockchain



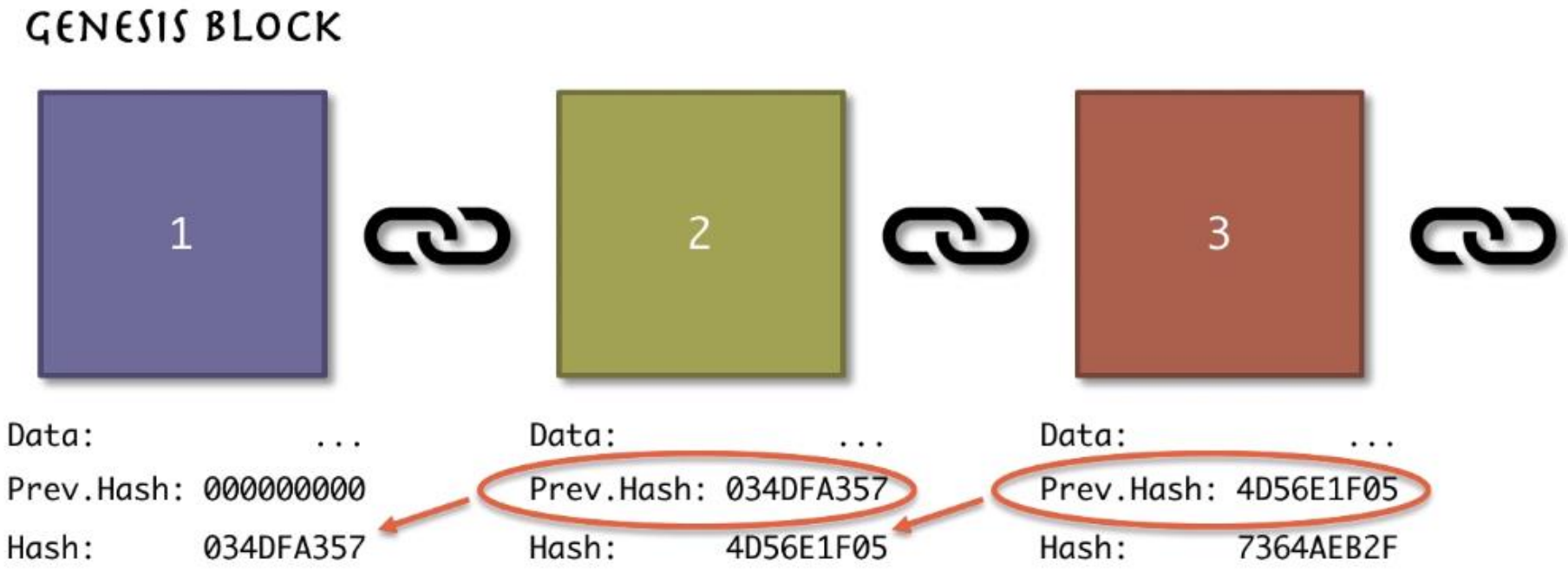
B. Singhal et. al “Beginning Blockchain”, Apress publications


Company-A
Charlie
Bob
Alice
Company-B
Stocks settlement through clearing houses

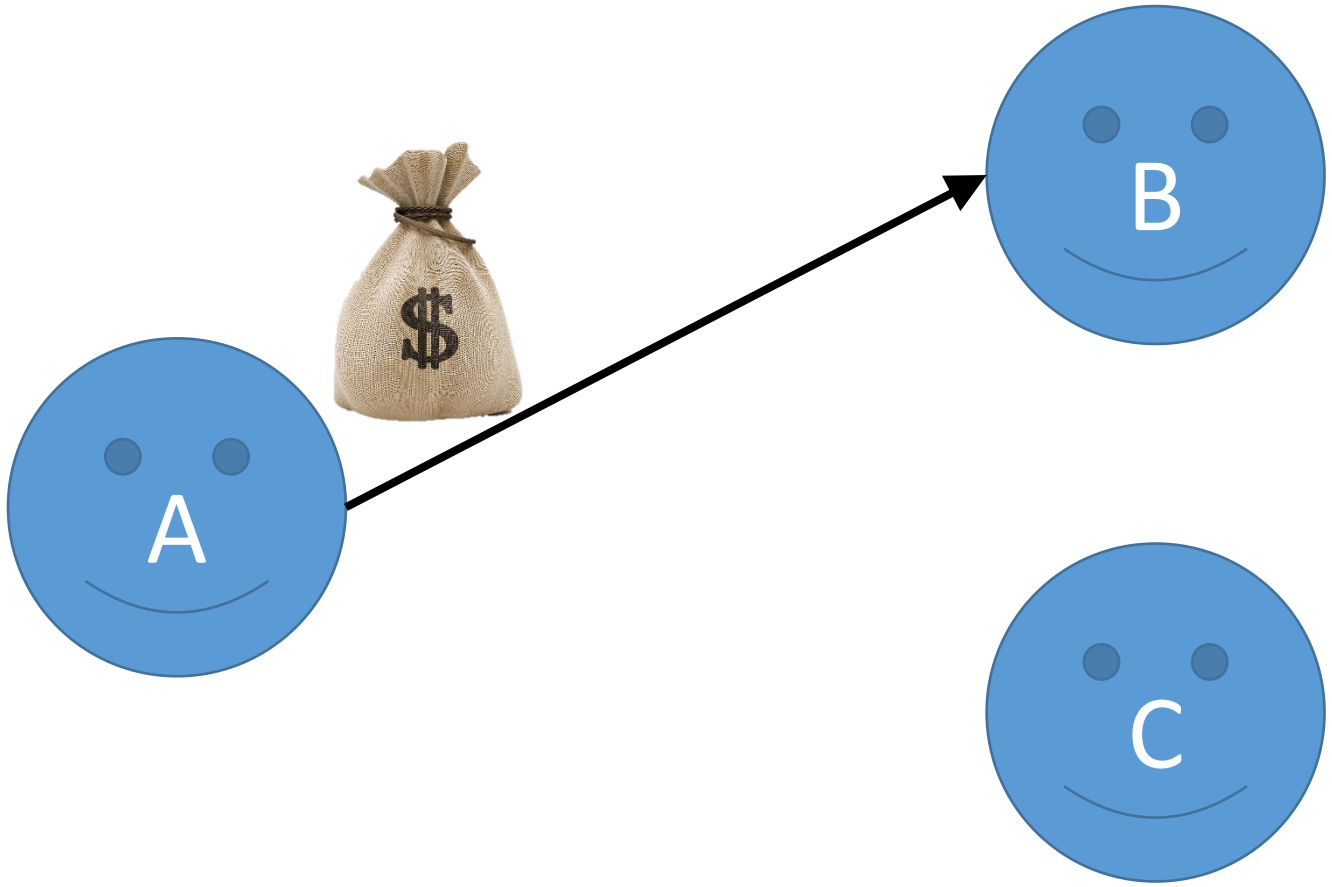


Peer-to-Peer trading: Blockchain

Blockchain


GENESIS BLOCK
1
2
3
Data: ...
Prev.Hash: 000000000
Hash: 034DFA357
Data: ...
Prev.Hash: 034DFA357
Hash: 4D56E1F05
Data: ...
Prev.Hash: 4D56E1F05
Hash: 7364AEB2F

Key Challenges



1. **No stealing: Only Alice can move her money**
2. Minting: Fair money creation
3. No double-spending: Alice cannot duplicate her money

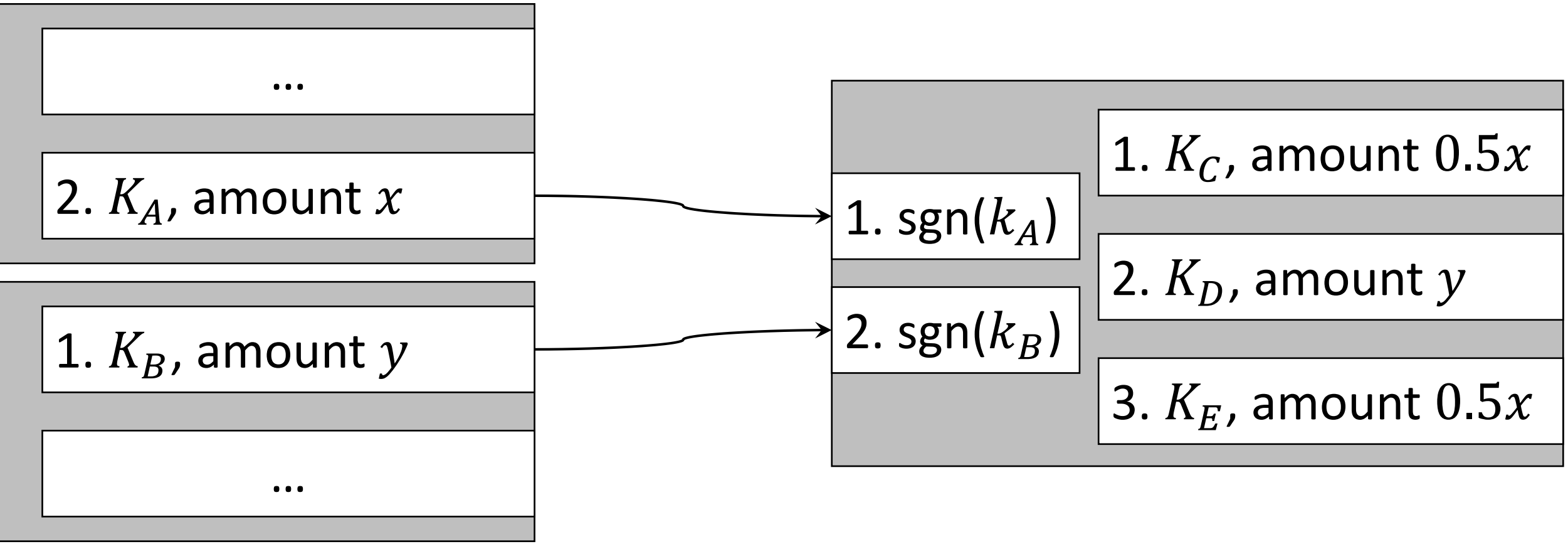
60 Seconds on Public Key Signatures

Alice generates key pair

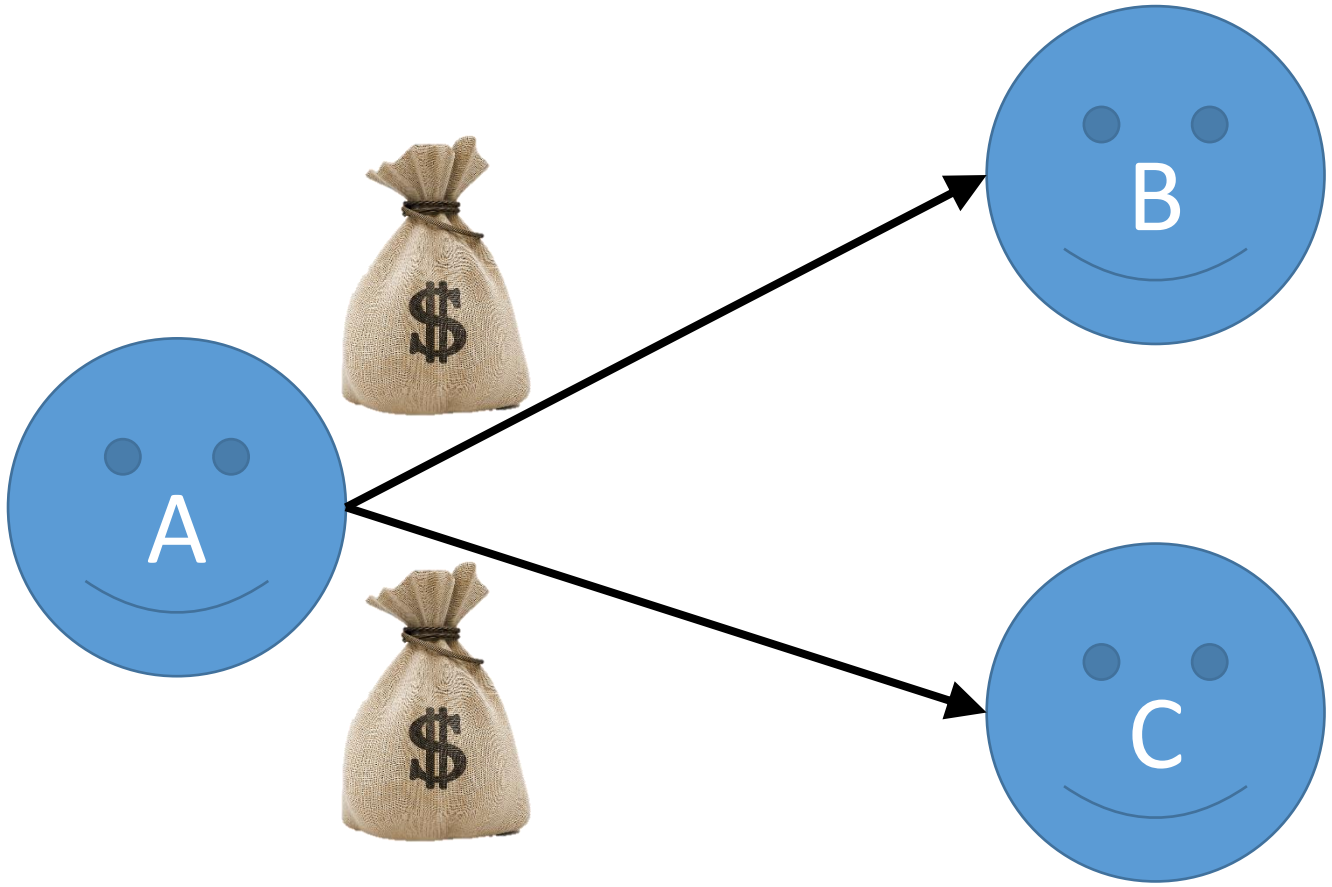
1. private key k_A, kept secret
2. public key K_A, published with ***public key infrastructure***

- Alice signs a message m with private key k_A, generating a signature s.
- Anyone can verify that s is a signature of m with key k_A given m and K_A.

Addresses and Transactions

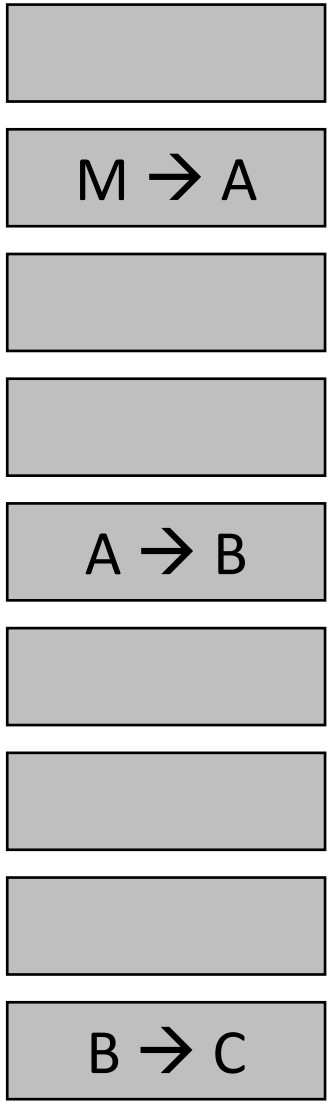


Key Challenges

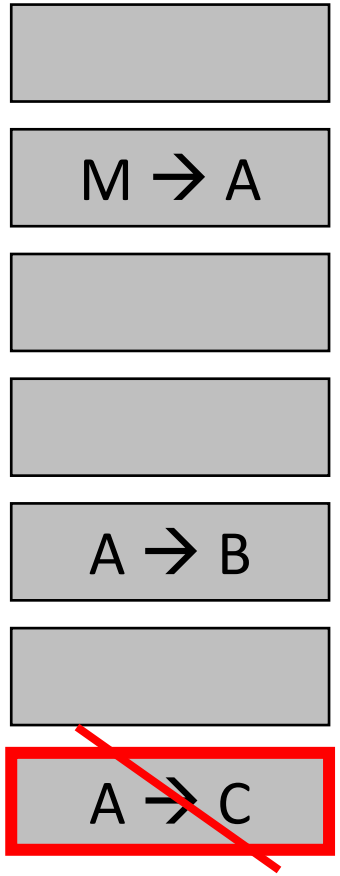


1. No stealing: Only Alice can move her money
2. **No double-spending: Alice cannot duplicate her money**
3. Minting: Fair money creation

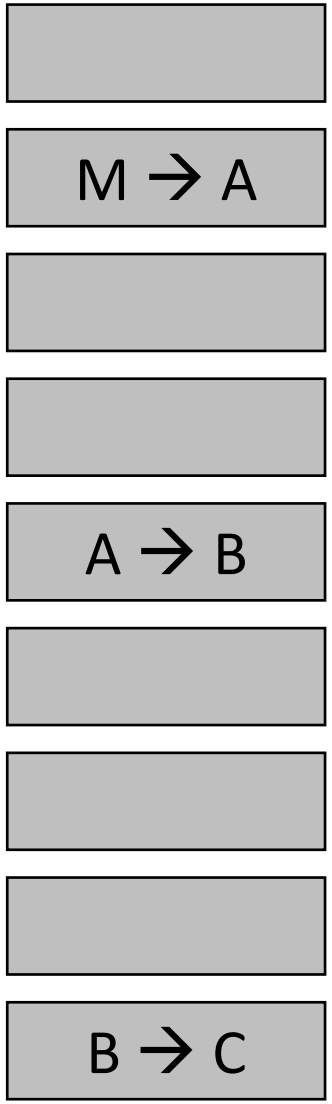
Global Ledger



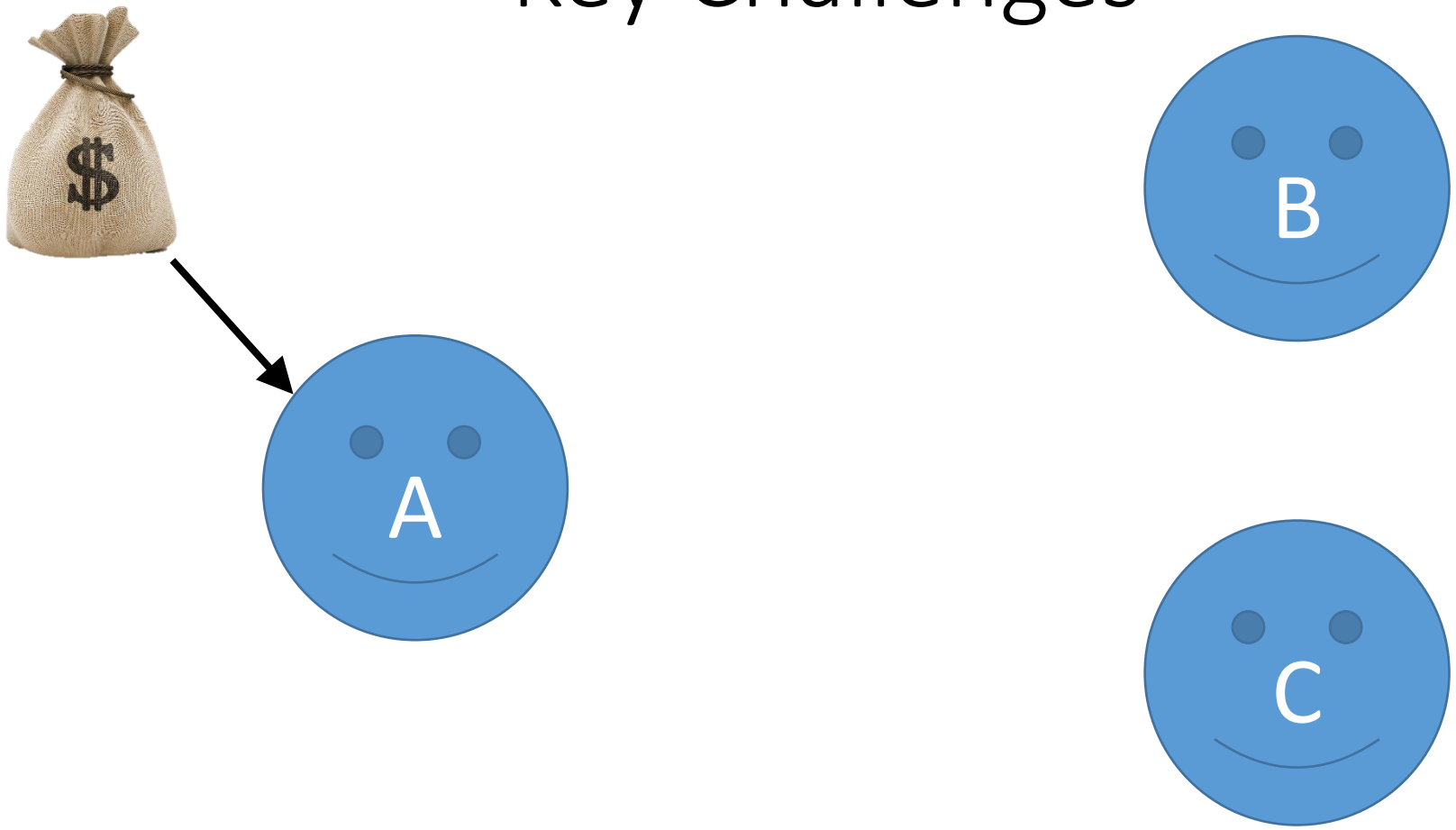
Global Ledger



Global Ledger

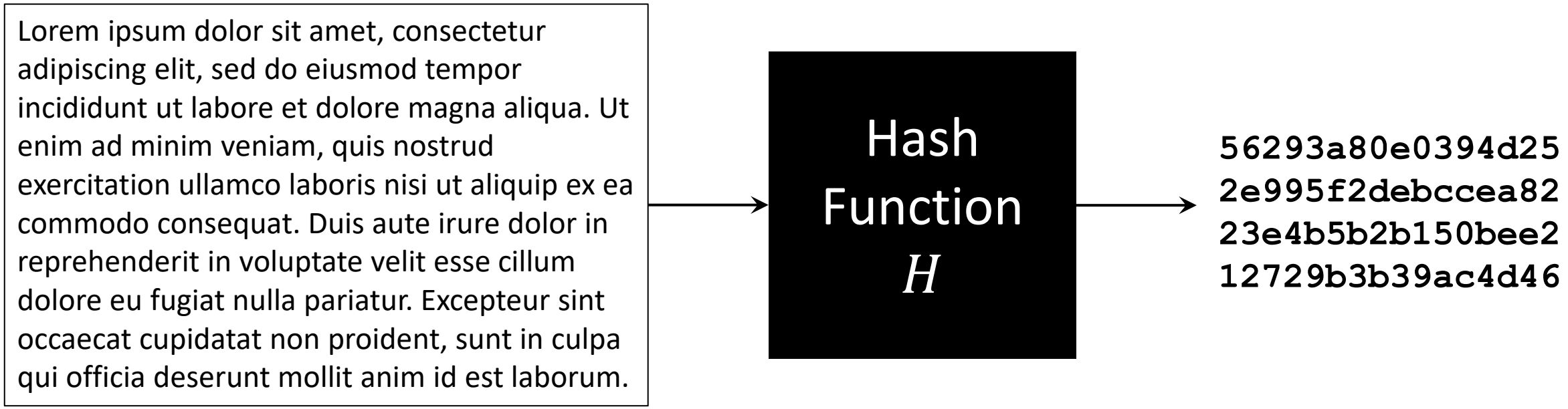


Key Challenges



1. No stealing: Only Alice can move her money
2. No double-spending: Alice cannot duplicate her money
3. **Minting: Fair money creation**

60 Seconds on Cryptographic Hashing



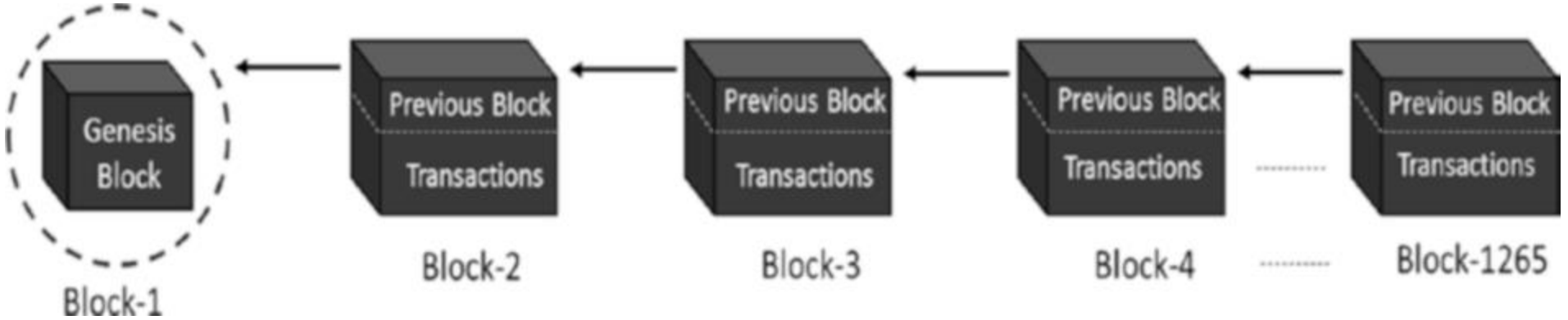
String input

256 bit number (for example)

Given a 256bit number h, one cannot find an input string that results in h faster than repeatedly guessing inputs x and calculating $H(x)$.

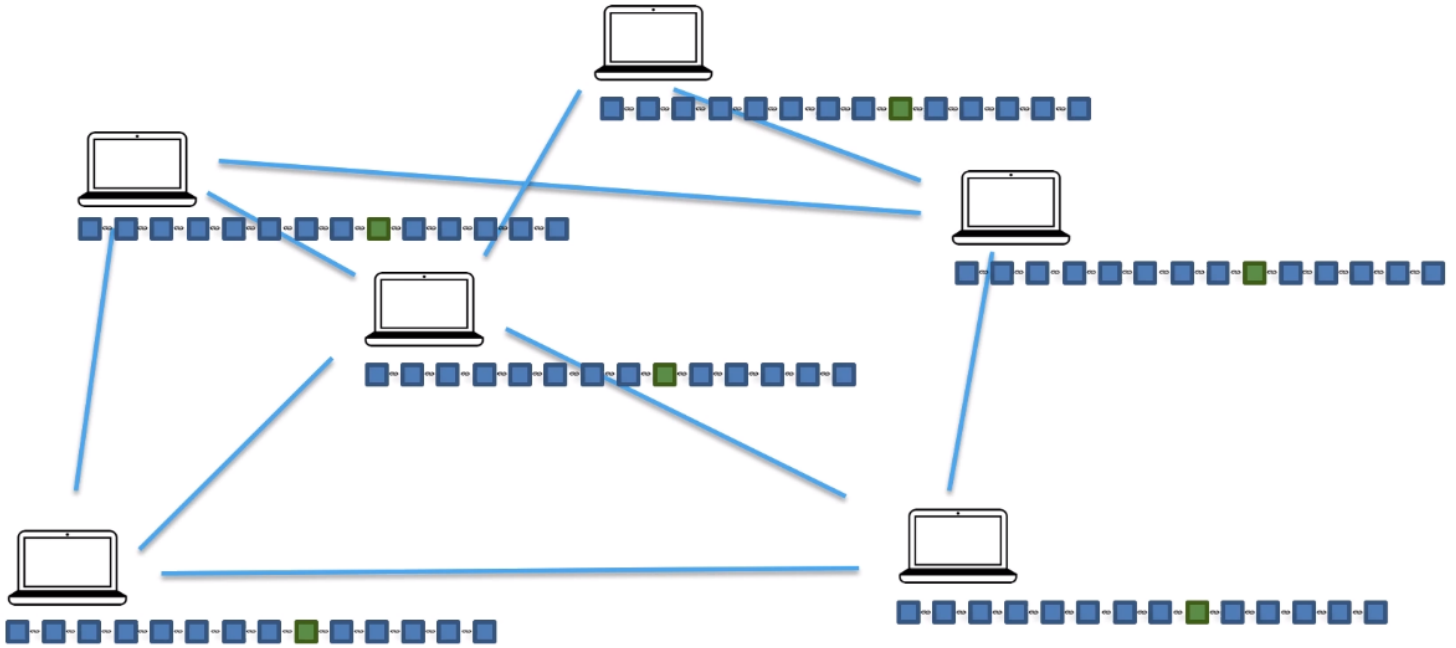
How the data is tamper proof

- Cryptographic hash chain linking



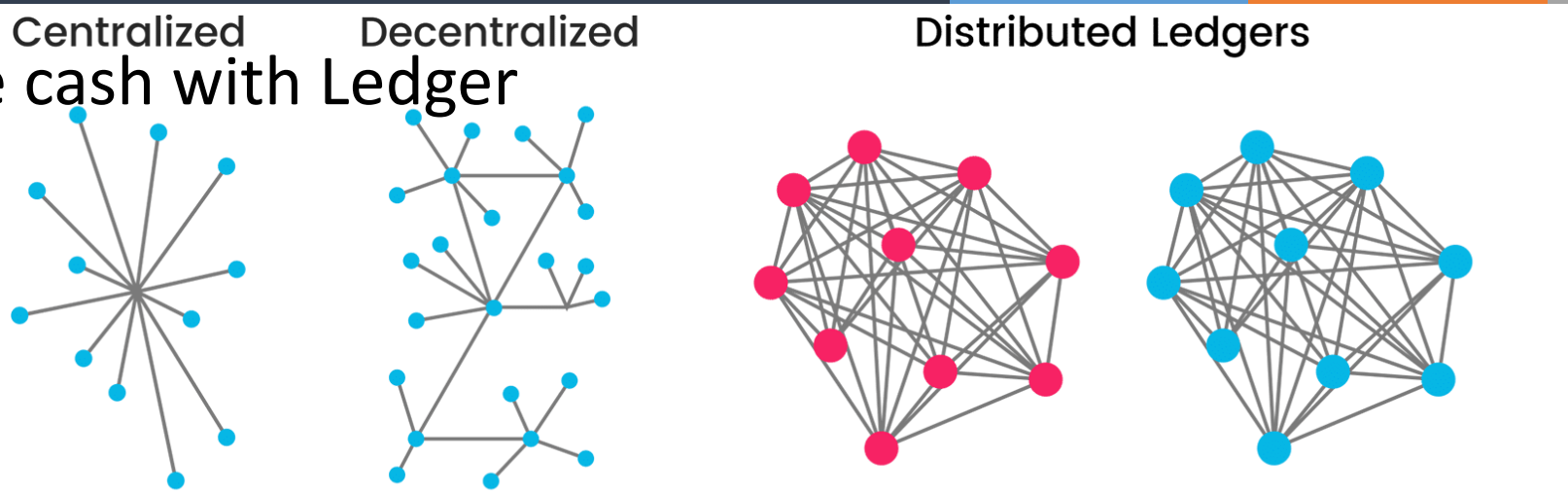
Adding Trust and security

- Chain is replicated across multiple locations
- In a Distributed fashion



Decentralization

- Replace cash with Ledger



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

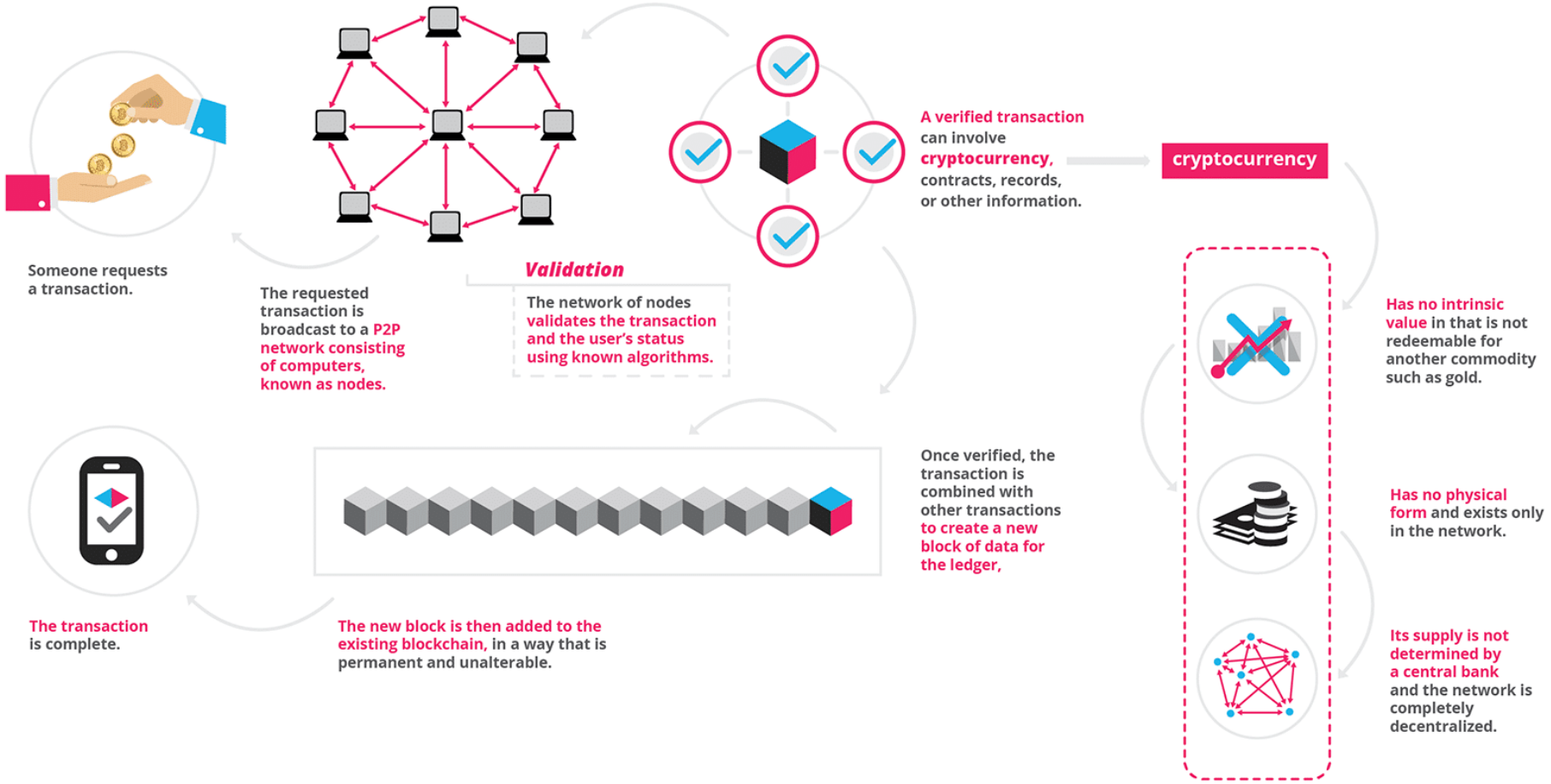
- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

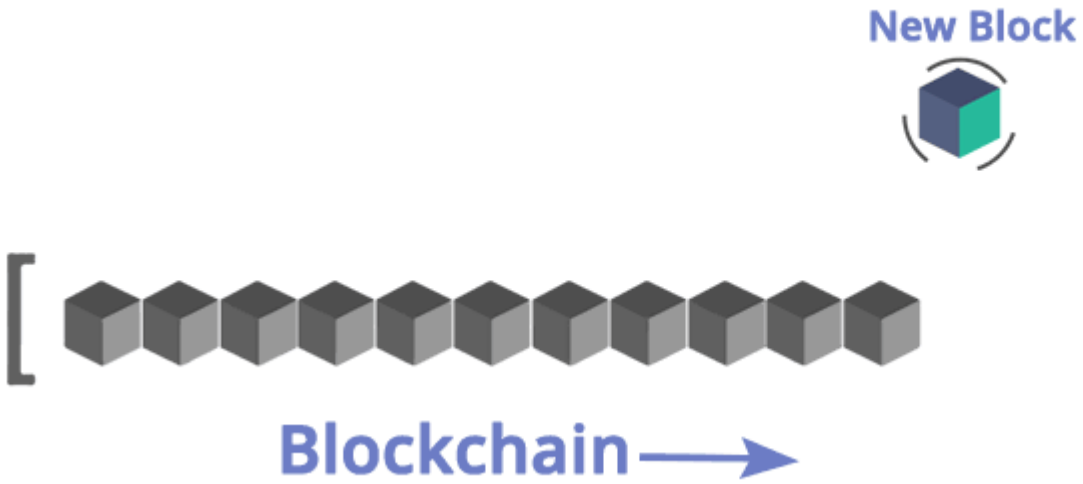
- Permision is required for users to have a copy of the legder and participate in confirming transactions

Blockgeeks

Highlights

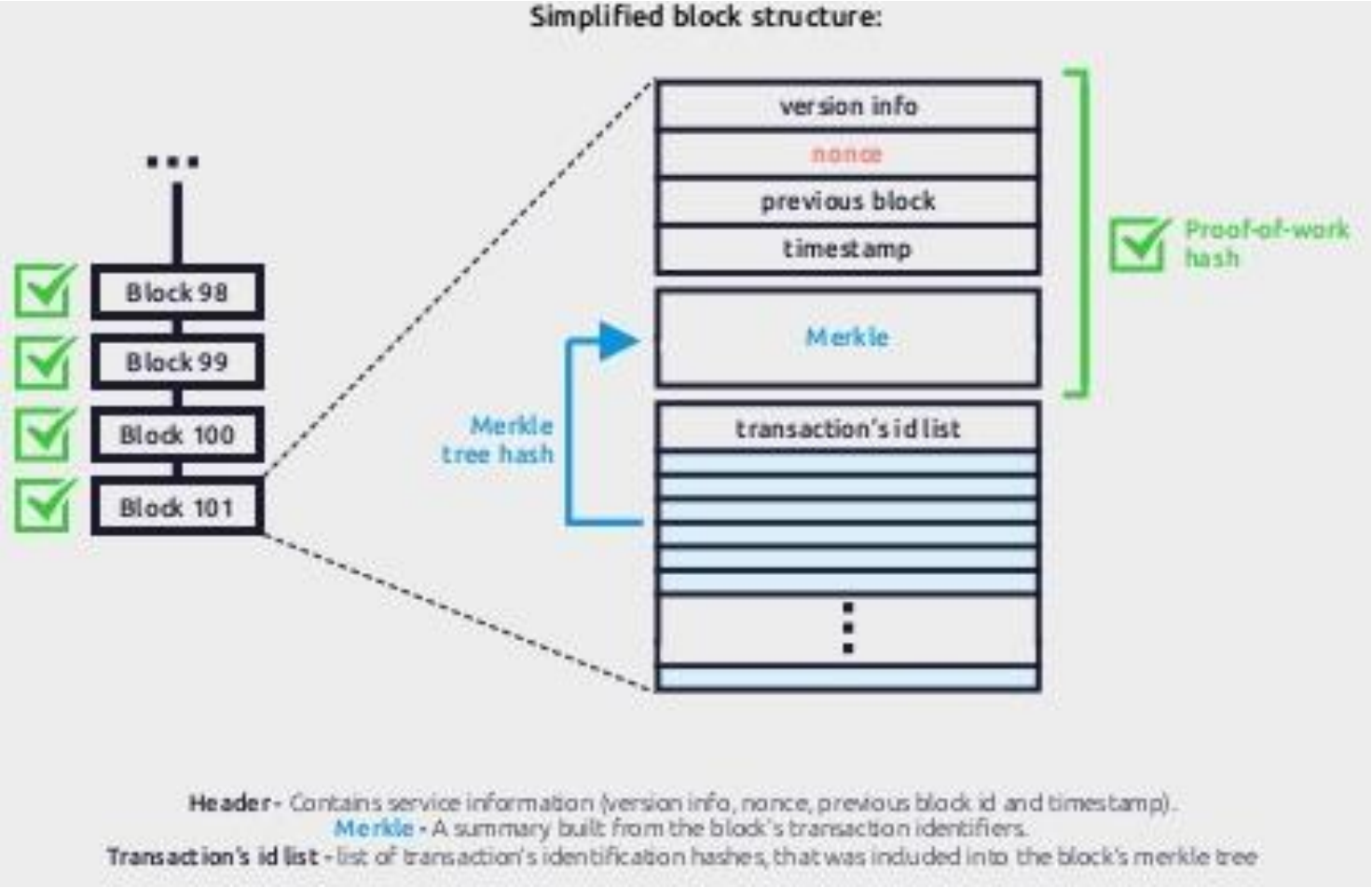

Someone requests a transaction.
The requested transaction is broadcast to a P2P network consisting of computers, known as nodes.
Validation
The network of nodes validates the transaction and the user's status using known algorithms.
A verified transaction can involve cryptocurrency, contracts, records, or other information.
cryptocurrency
Has no intrinsic value in that is not redeemable for another commodity such as gold.
Has no physical form and exists only in the network.
Its supply is not determined by a central bank and the network is completely decentralized.
Once verified, the transaction is combined with other transactions to create a new block of data for the ledger,
The new block is then added to the existing blockchain, in a way that is permanent and unalterable.
The transaction is complete.

Blockchain Structure



Source: https://www.edureka.co/blog/blockchain-tutorial/

What does a block look like?



Mining – Minting for Proof of Work

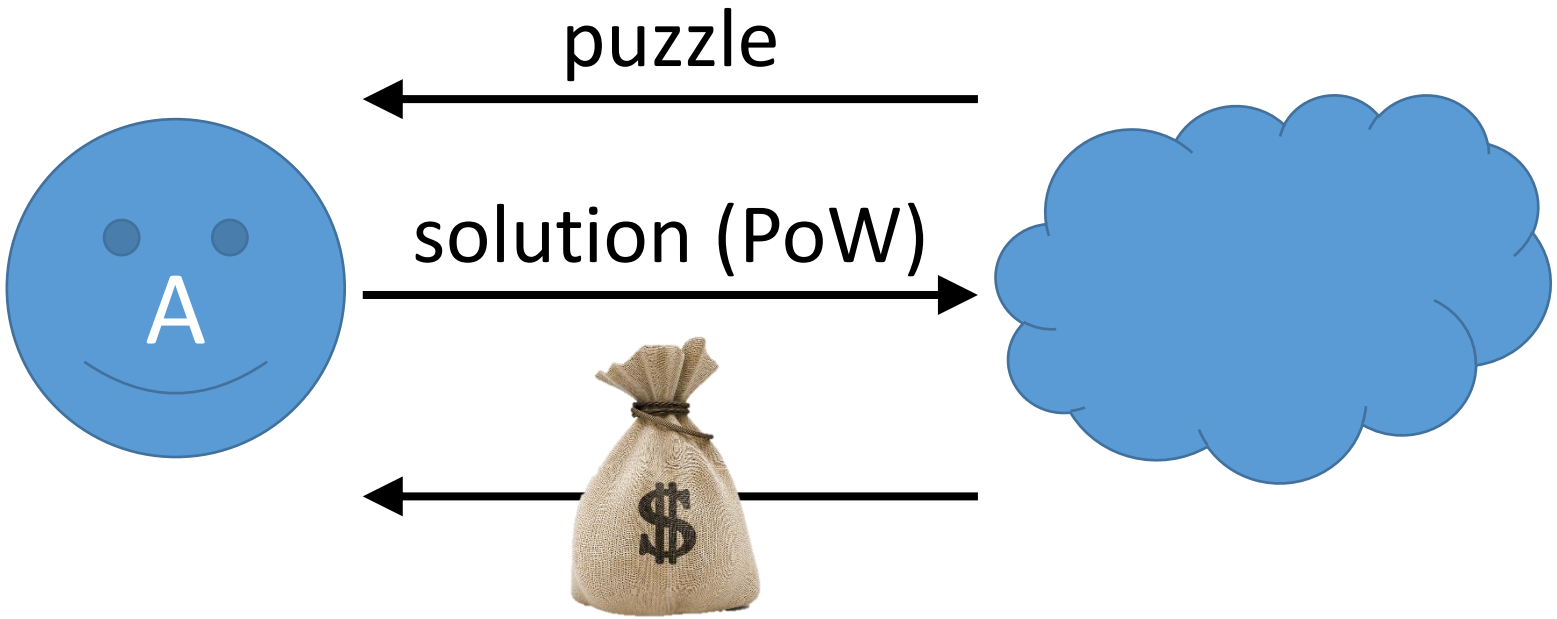
Computationally difficult puzzle:

$$\text{Find } x \text{ such that } H(x|y) < t$$

Solver guesses values for x until finding a valid one

- Different strings y for different puzzles
- The target t determines the difficulty, average time to solve

Mining – Minting for Proof of Work



Key Challenges

1. No stealing: Only Alice can move her money

   Cryptographic signatures
2. No double-spending: Alice cannot duplicate her money

   Global ledger
3. Minting: Fair money creation

   Mint for proof of work

Key Challenges

1. No stealing: Only Alice can move her money

   Cryptographic signatures
2. No double-spending: Alice cannot duplicate her money

   Global ledger
3. Minting: Fair money creation

   Mint for proof of work

Who runs the public key infrastructure?

Who maintains the public ledger?

Who gives money for puzzles?

Can this be decentralized?

Slide courtesy of Ittay Eyal

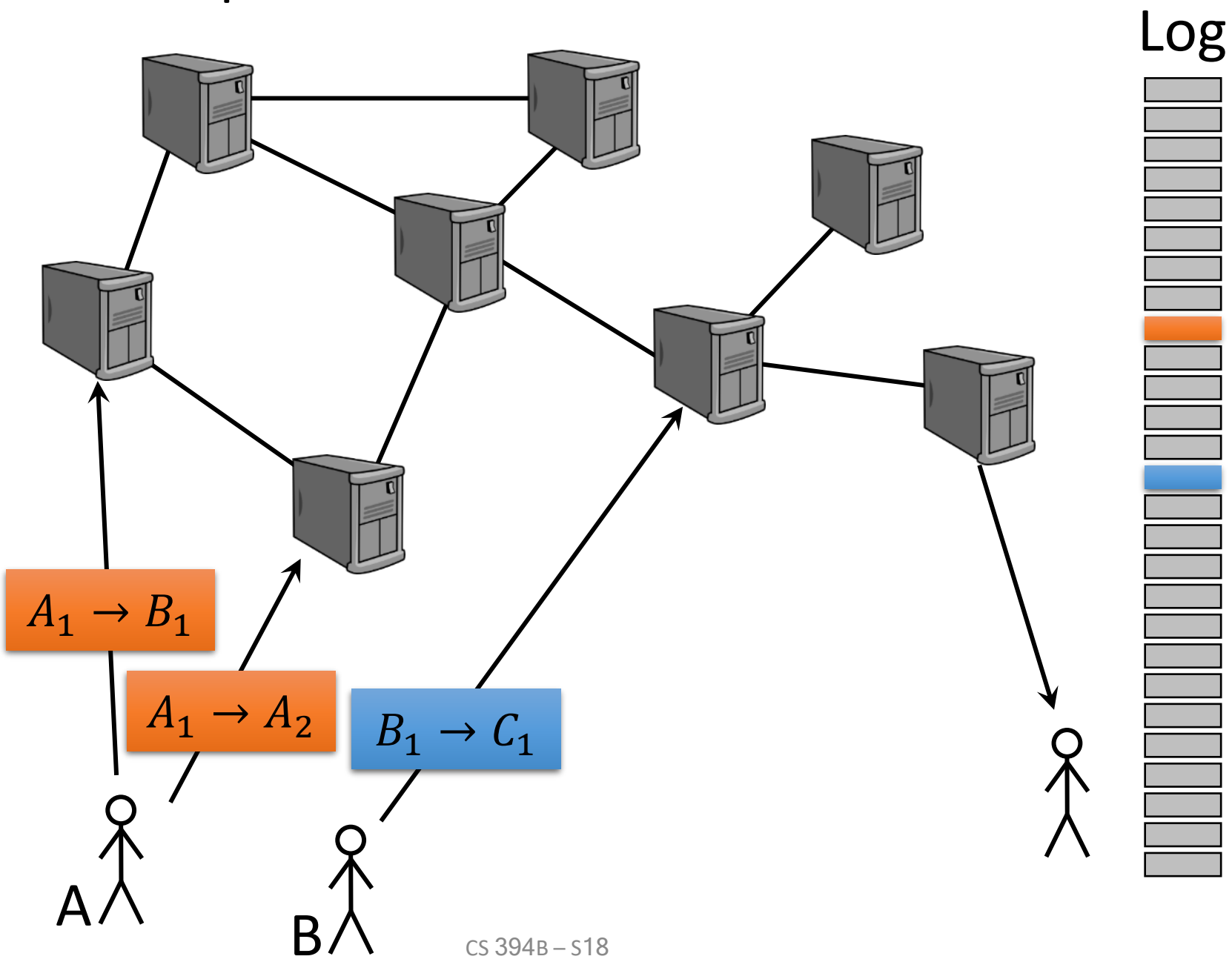
Replicated State Machine

- Instead of one machine, use a ***replicated state machine***
- Multiple machines operate a single ledger, PKI, and mint fairly
- A subset can behave arbitrarily – aka ***Byzantine***

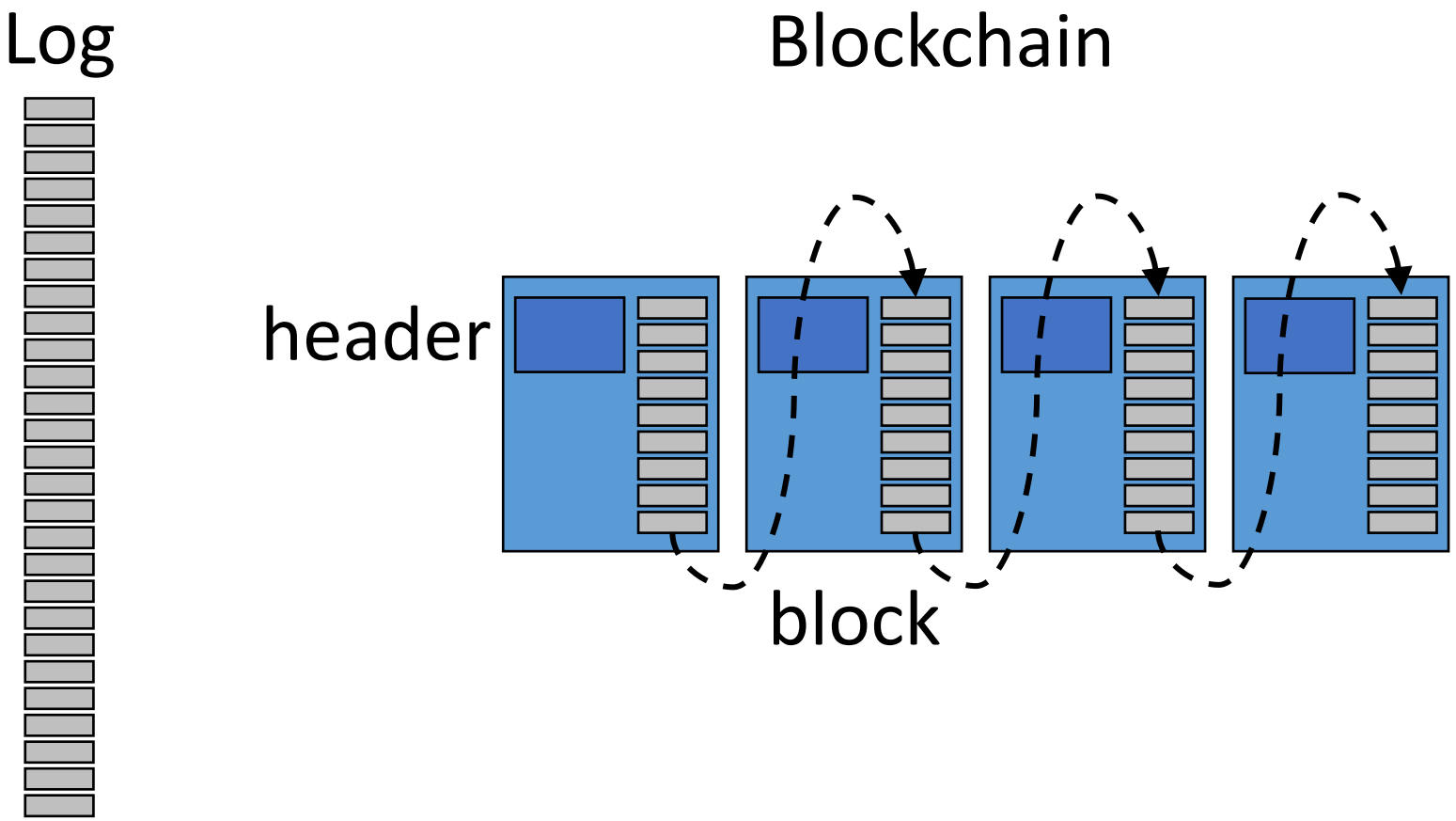
But who chooses the participating machines?

Slide courtesy of Ittay Eyal

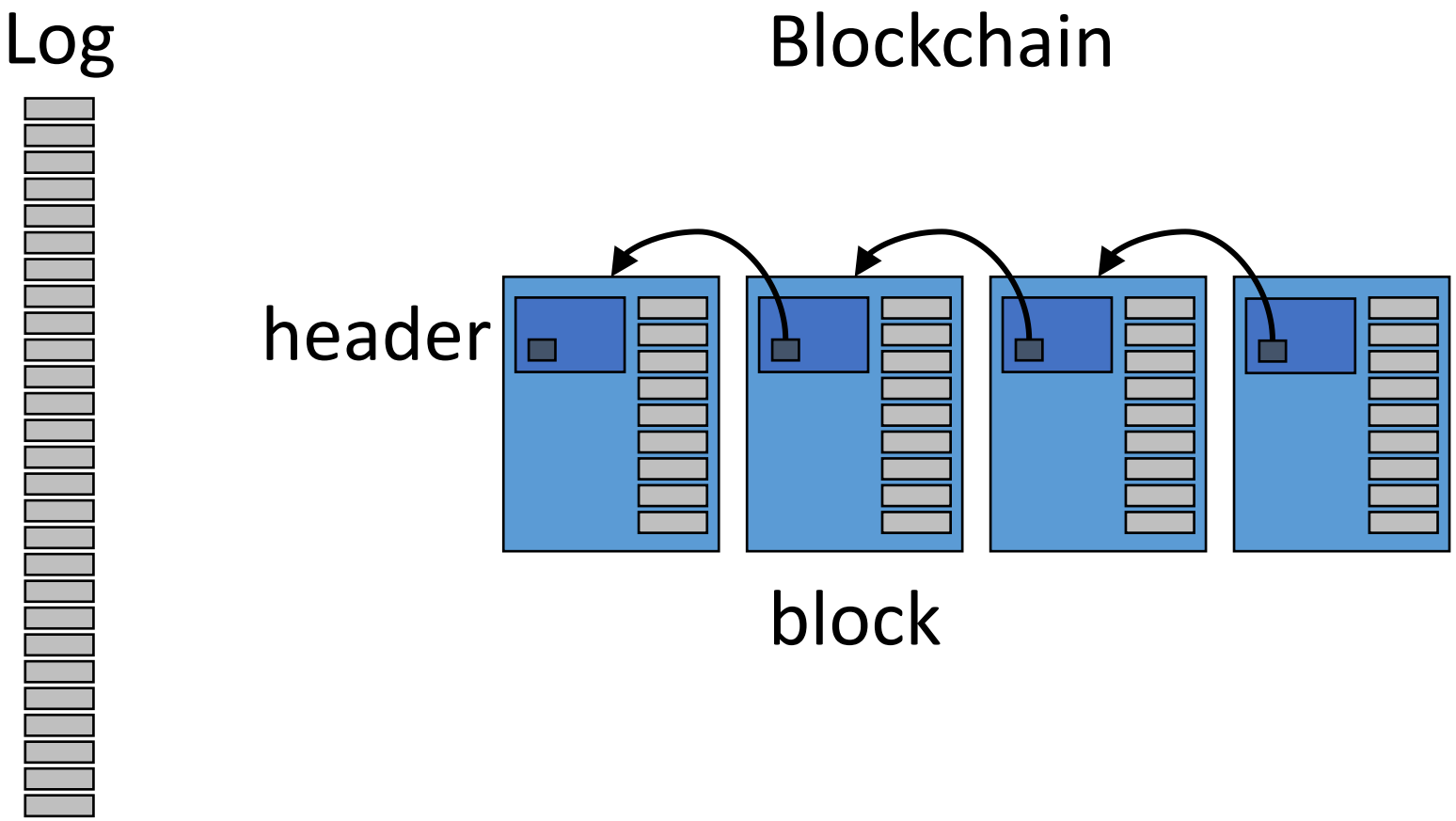
A Replicated State Machine



Nakamoto's Blockchain

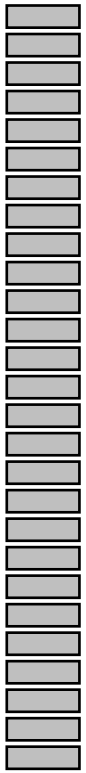


Nakamoto's Blockchain

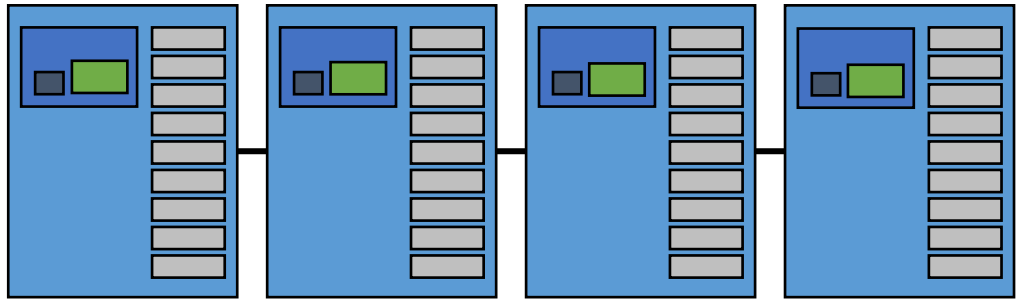


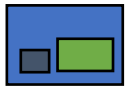
Nakamoto's Blockchain

Log



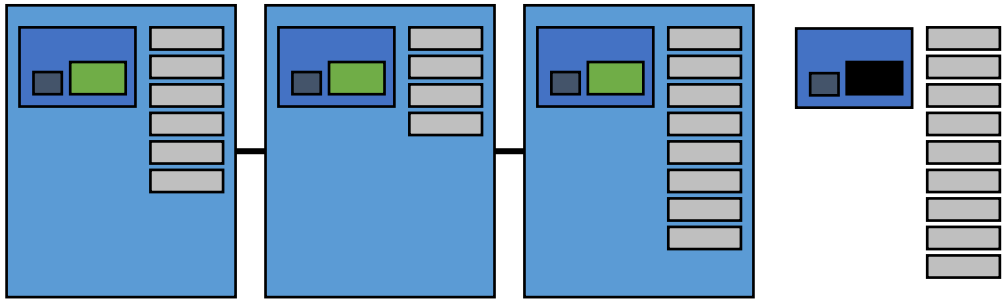
Blockchain



hash() < target*

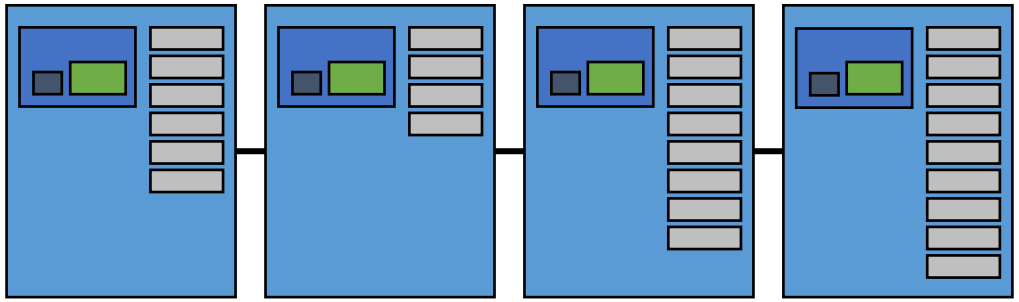
* *target*: a deterministic function of previous blocks

Nakamoto's Blockchain



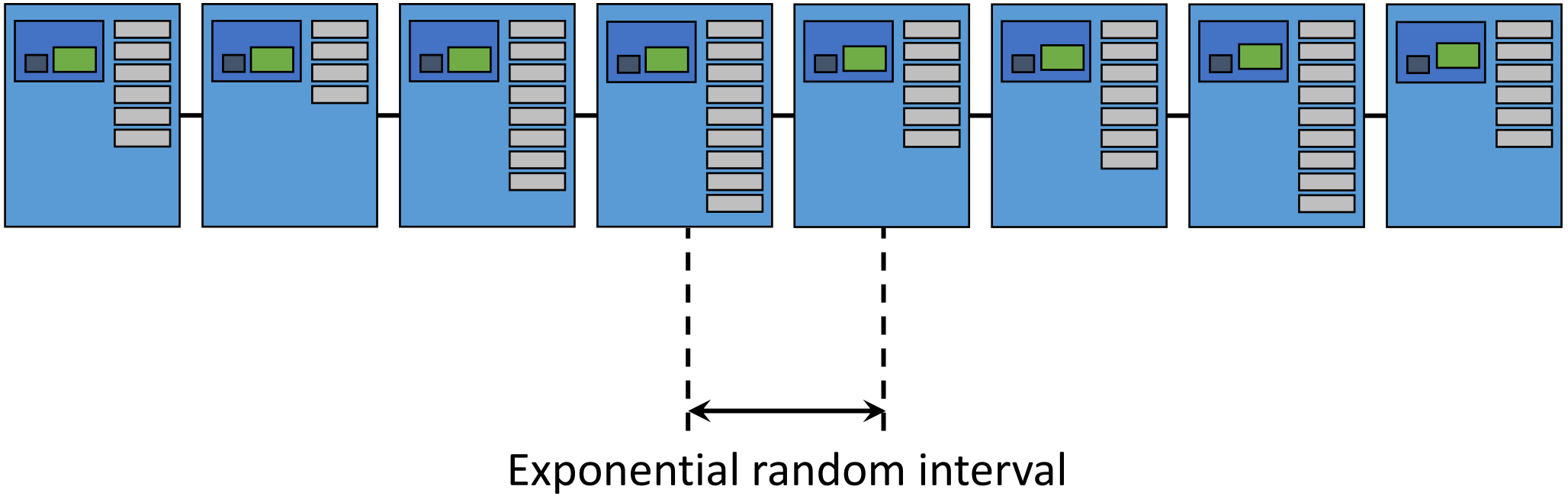
Slide courtesy of Ittay Eyal

Nakamoto's Blockchain



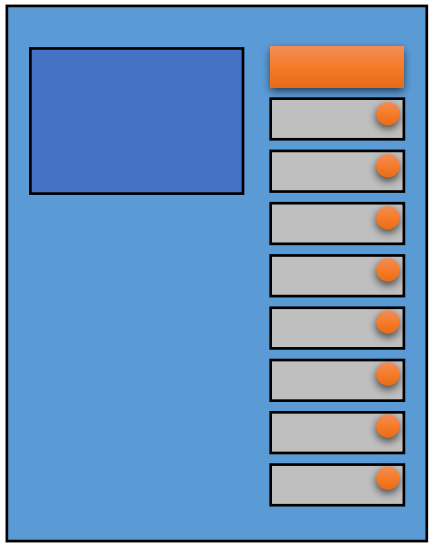
Slide courtesy of Ittay Eyal

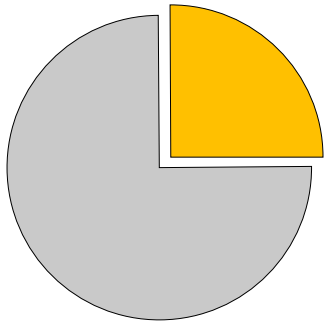
Nakamoto's Blockchain

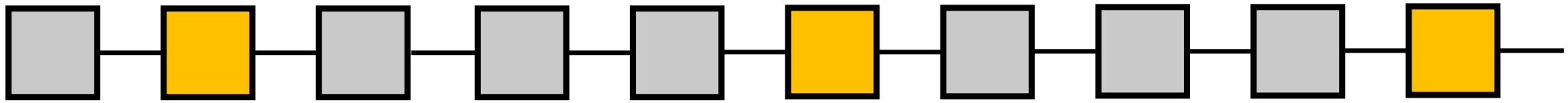


Incentive for Mining

- **Internal** Prize:
  - **Minting**
  - **Fees**







Wins proportional to computation power

4 Key Concepts of Blockchain

Distributed shared ledger

Cryptography

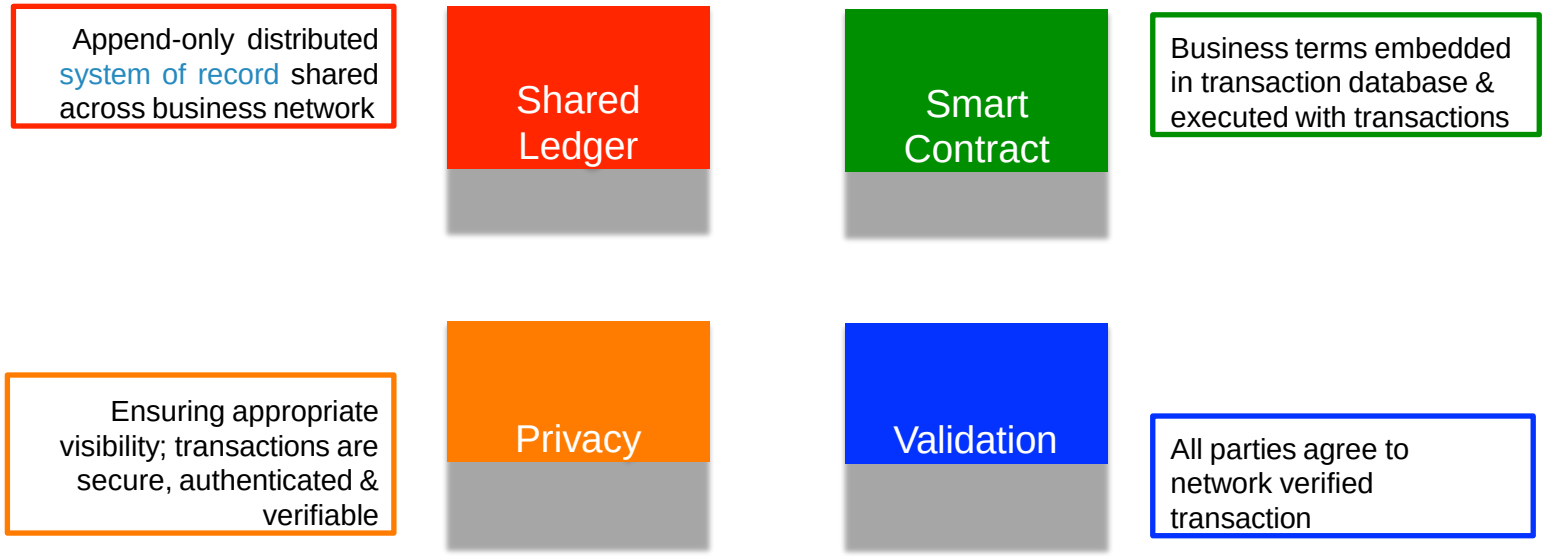
Consensus

Smart contracts

Source: IBM, A new disruption in financial services

Blockchain for Business

What?



Broader participation, lower cost, increased efficiency

Blockchain terminologies

- **Bitcoin**
  - How the money transfer works

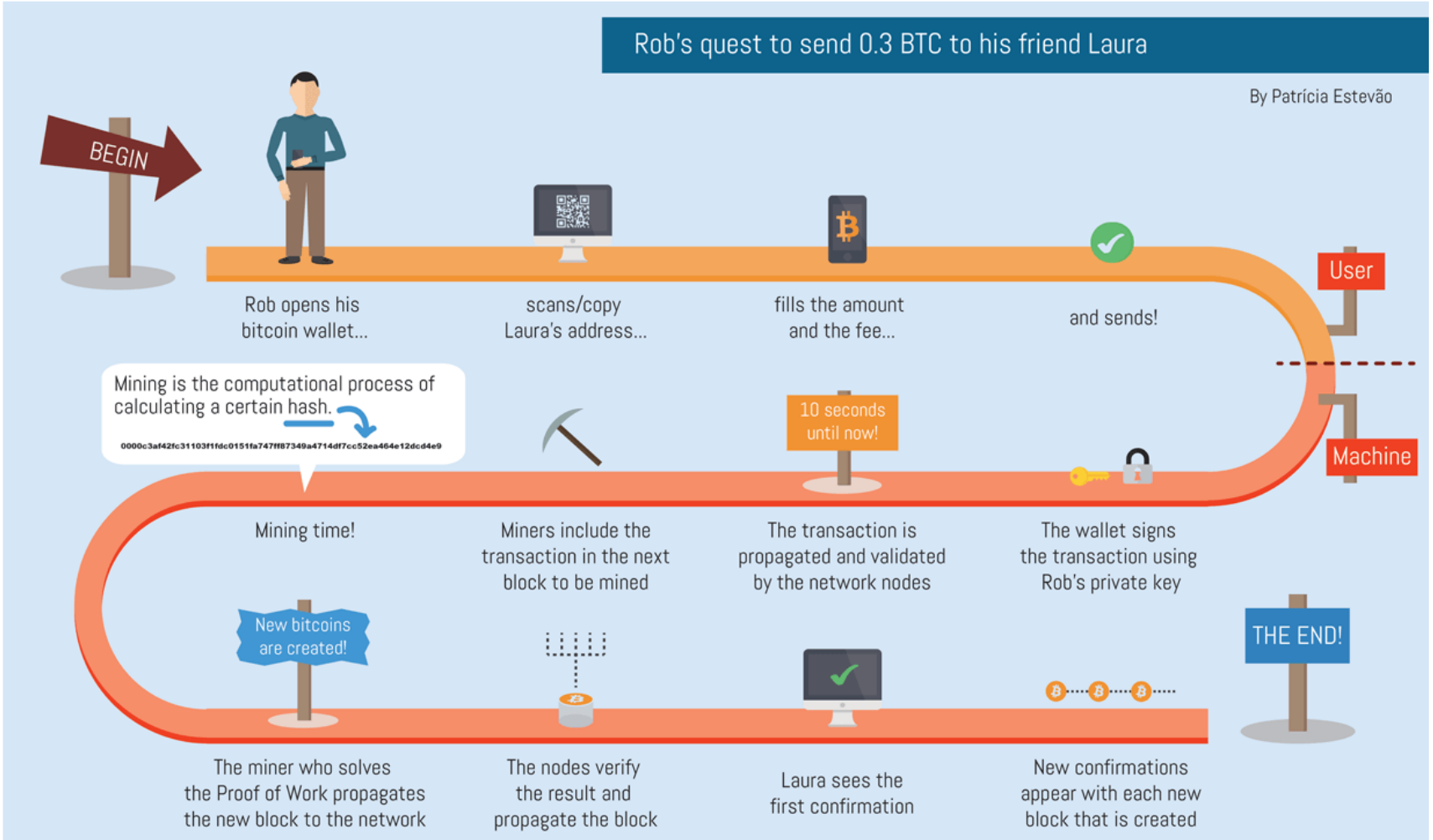


Image source: https://www.weusecoins.com/images/bitcoin-transaction-life-cycle-

Comparing Bitcoin and Ethereum

VS	Bitcoin	Ethereum
Founder	Satoshi Nakamoto	Vitalik Buterin
Release Date	9 Jan 2008	30 July 2015
Release Method	Genesis Block Mined	Presale
Blockchain	Proof of work	Proof of work (Planning for POS)
Useage	Digital Currency	Smart Contracts Digital Currency
Cryptocurrency Used	Bitcoin(Satoshi)	Ether
Algorithm	SHA-256	Ethash
Blocks Time	10 Mintues	12-14 Seconds
Mining	ASIC miners	GPUs
Scalable	Not now	Yes

Distinction between databases and blockchain ledgers

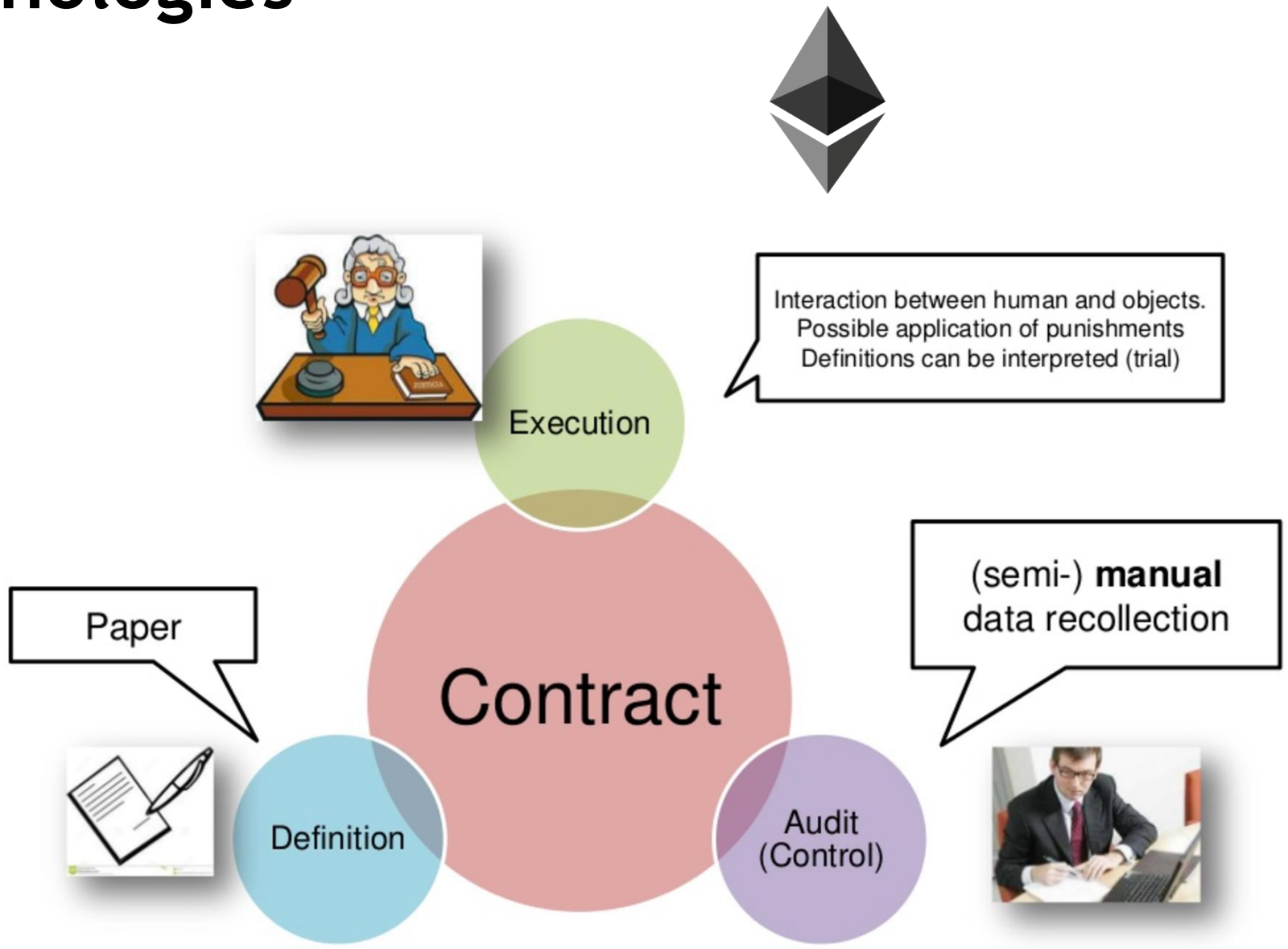
Databases 	VS	Blockchains 
Databases have admins & centralized control		No on is the admin or in-charge
Only entities with rights can access database		Anyone can access (public) blockchain
Only entities entitled to read or write can do so		Anyone with right proof of work can write on the blockchain
Databases are fast		Blockchains are slow
No history of records & ownership of digital records		History of records & ownership of digital records

Source: https://coinsutra.com/blockchain-v

Blockchain terminologies

- **Ethereum**
  - *Smart Contract*

How a “Traditional” contract works:



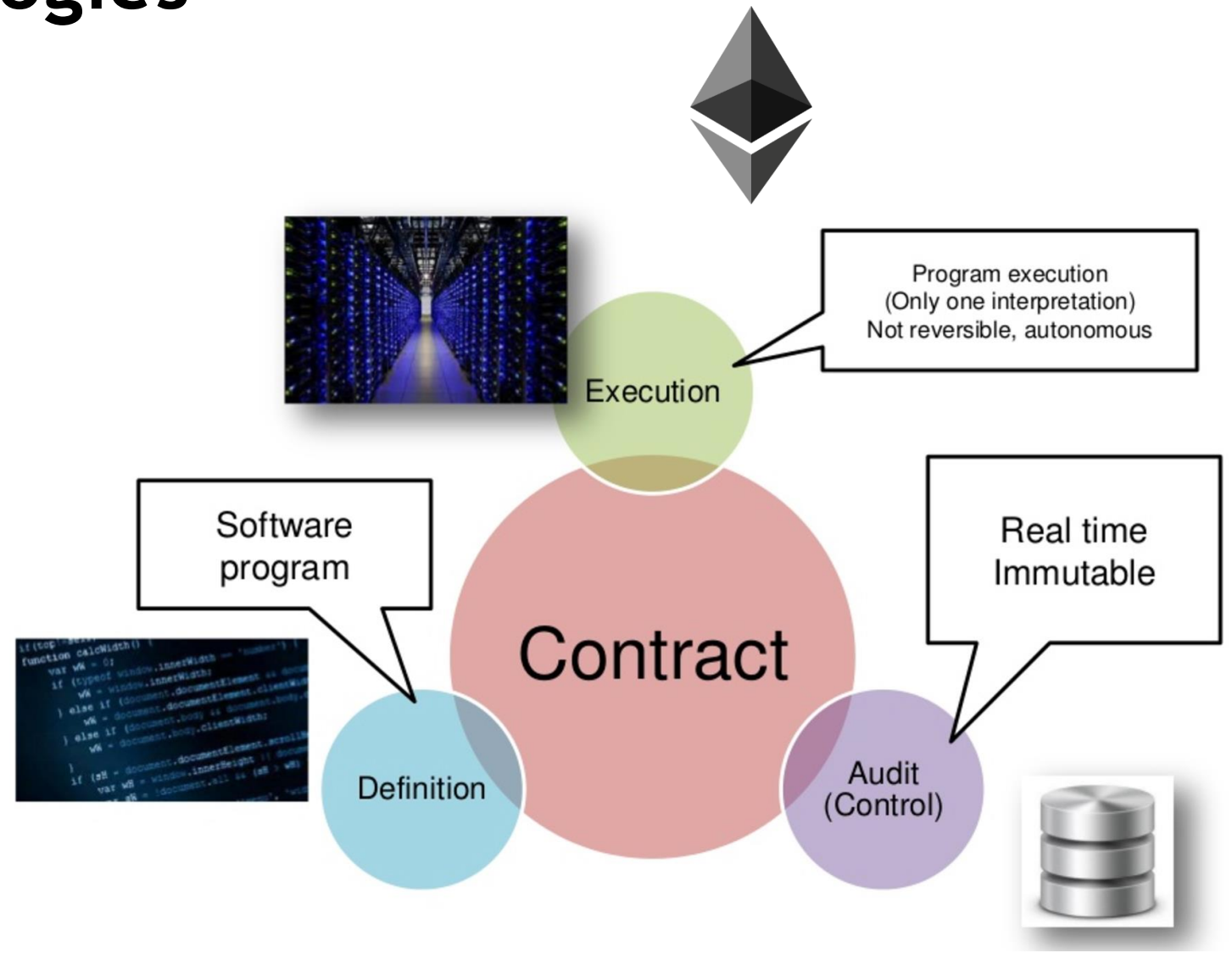
Source: https://www.investopedia.com/terms/s/smart-contracts.asp

Image source: https://image.slidesharecdn.com/smart-contracts-150925125224-lva1-app6892/95/smart

Blockchain terminologies

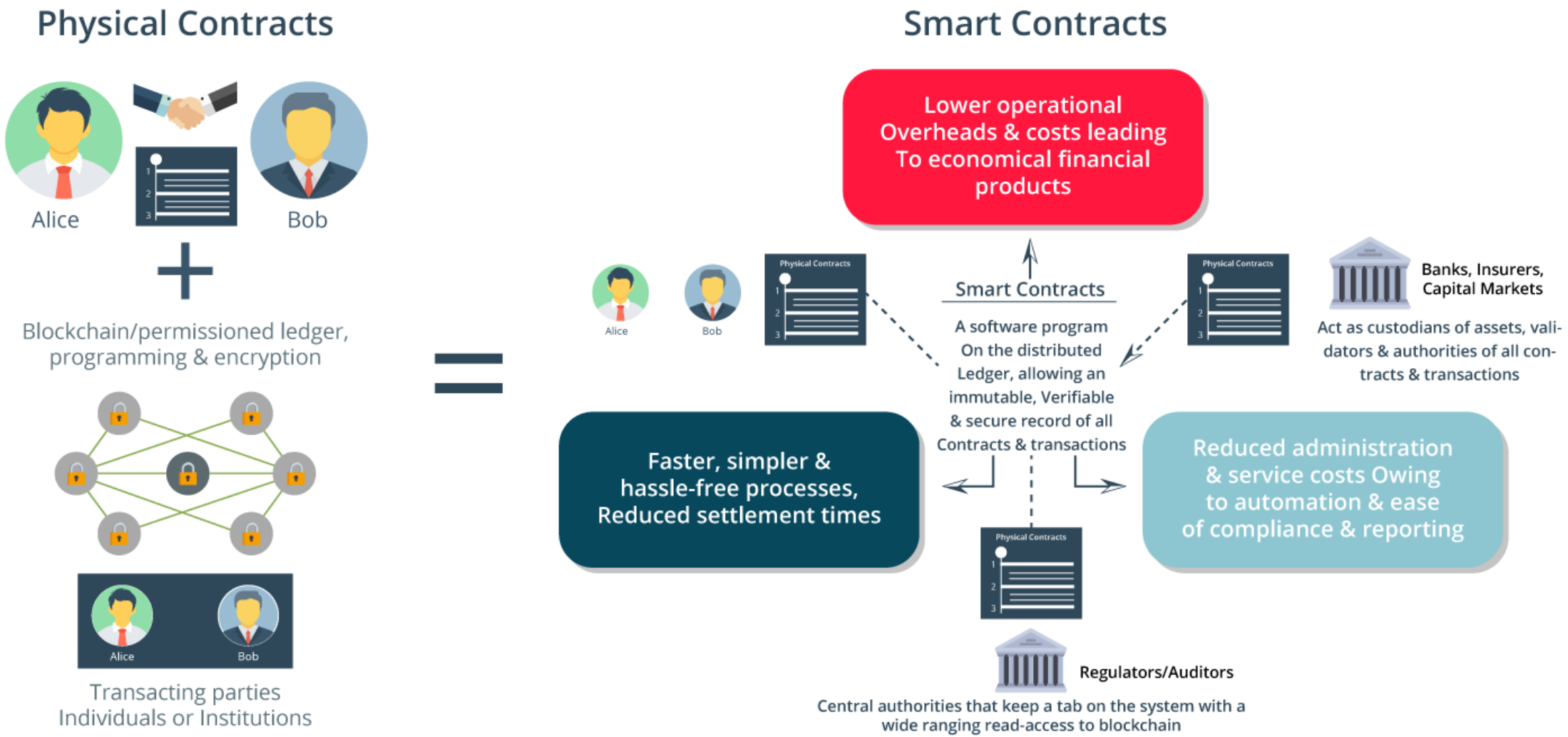
- **Ethereum**
  - *Smart Contract*

How a "*Smart Contract*" contract works:



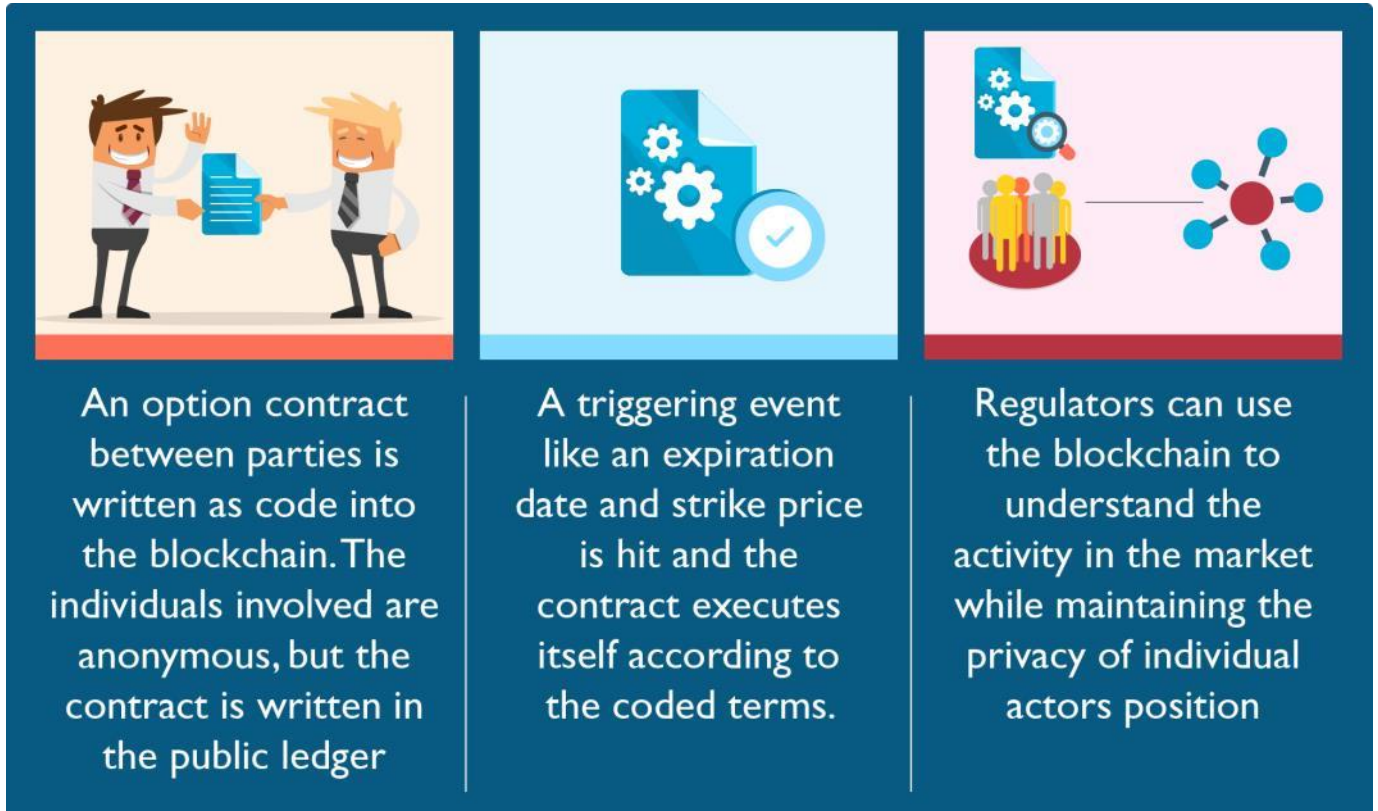
Source: https://www.investopedia.com/terms/s/smart-contracts.asp/

How Smart Contracts Work in a Permission Blockchain



Smart Contracts

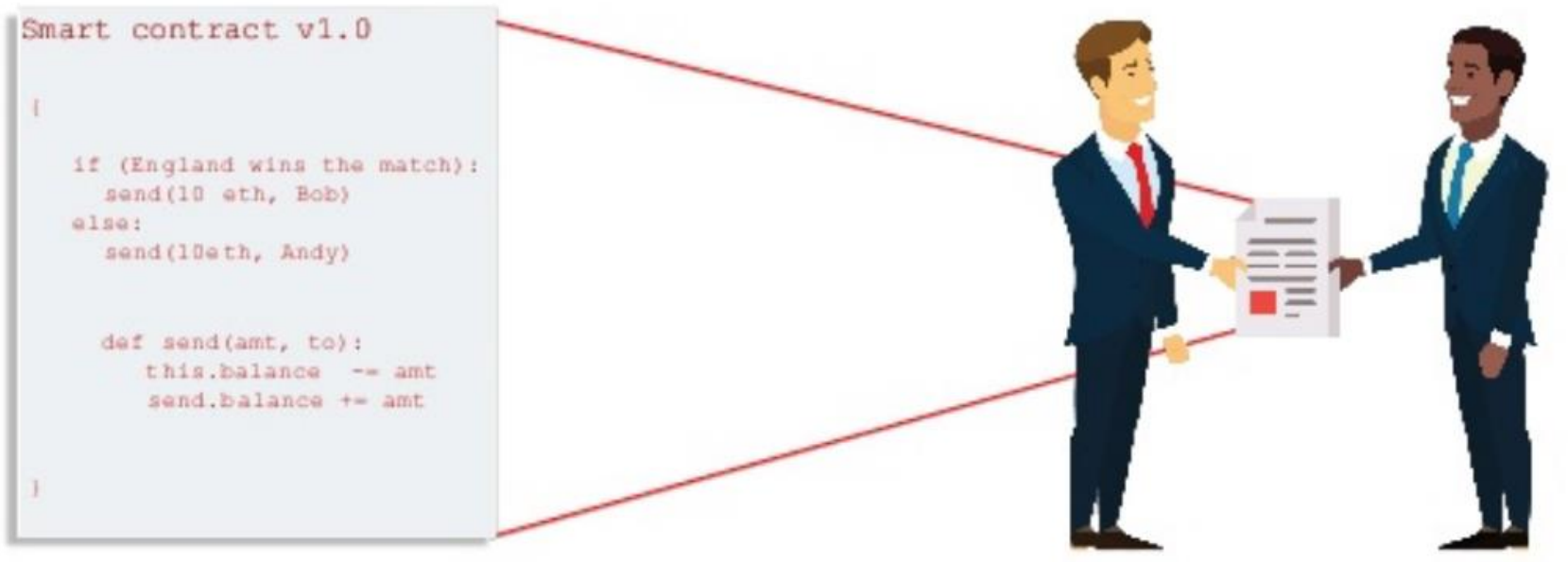
- A smart contract is a computerized transaction protocol that executes the terms of a contract
- When running on the blockchain a smart contract becomes like a self-operating computer program that automatically executes when specific conditions are met
- Smart contracts are majorly If This Then That Statements which run on the conditions provided



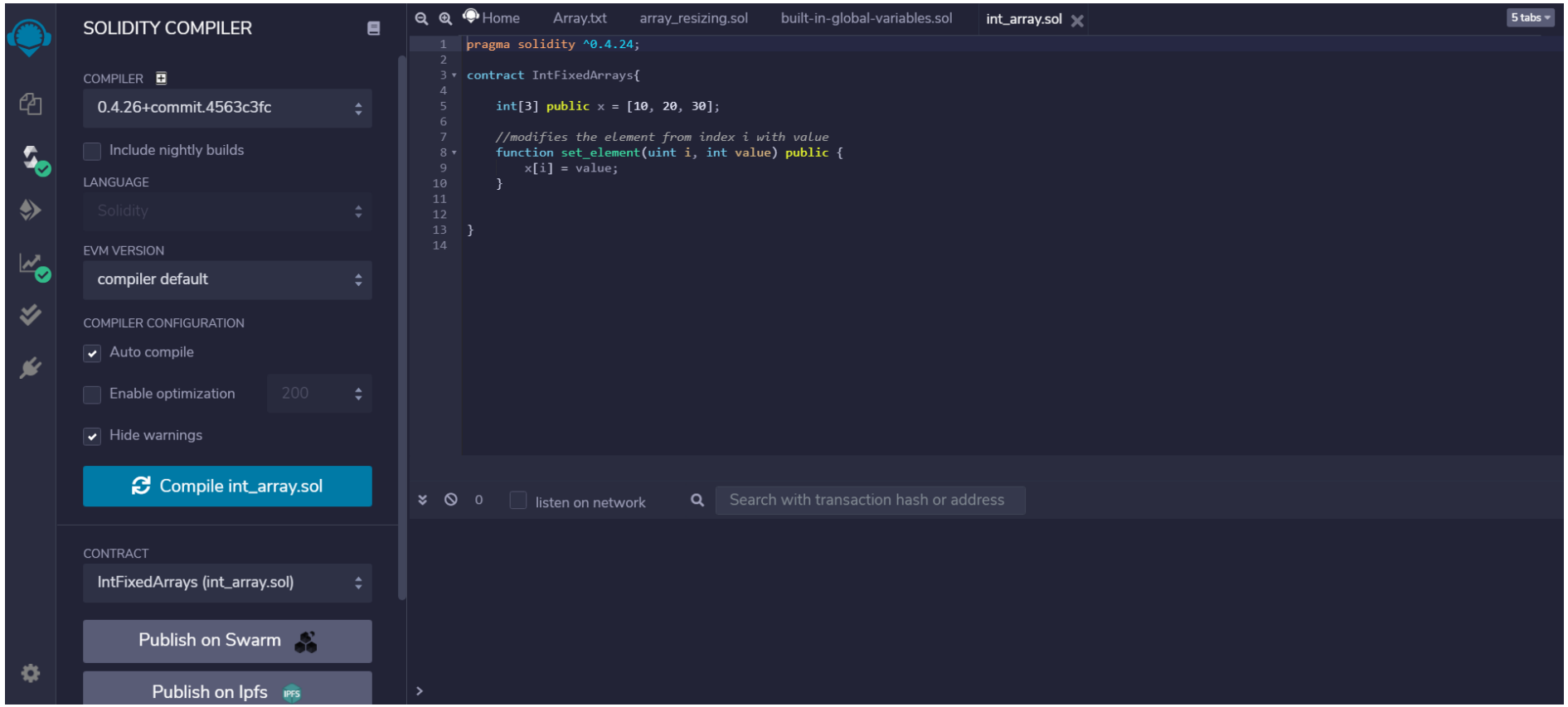
Types of Ethereum Accounts

Smart Contracts

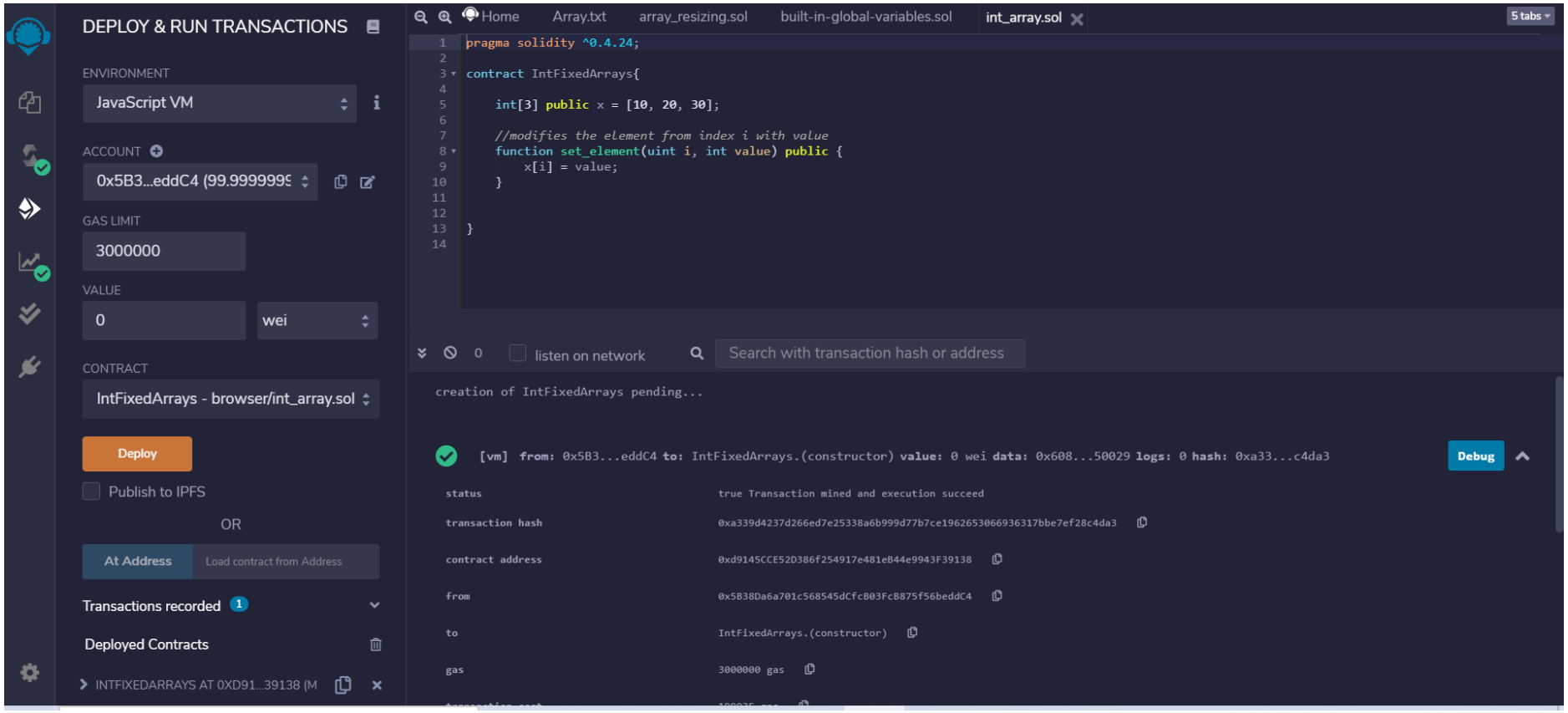
Smart contract is a computerized protocol wherein you write a standard contract rule that is tamper-proof.



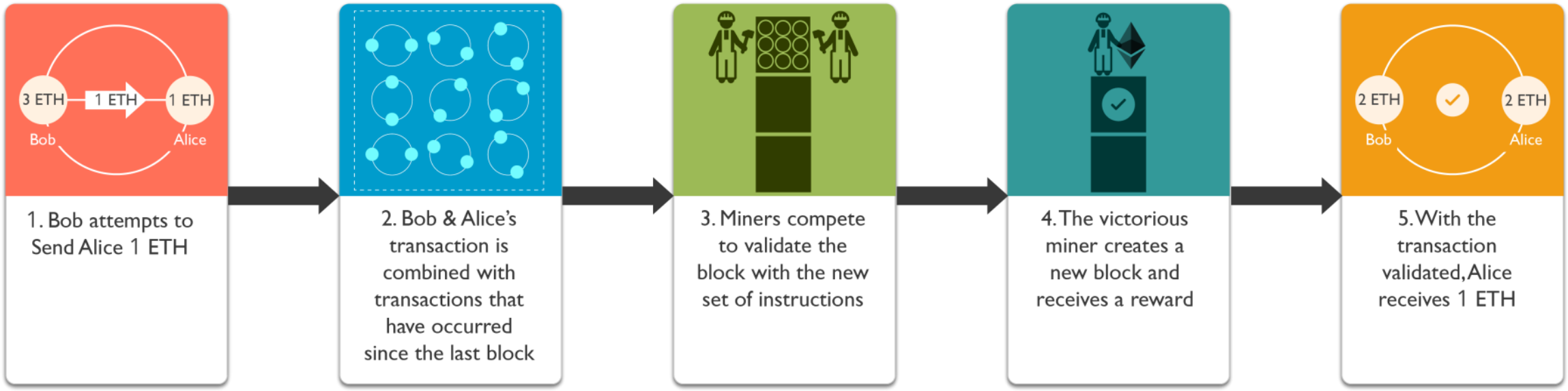
Compile in Remix IDE



Deployment in Remix IDE



Mining at a Glance



Mining a block in Blockchain

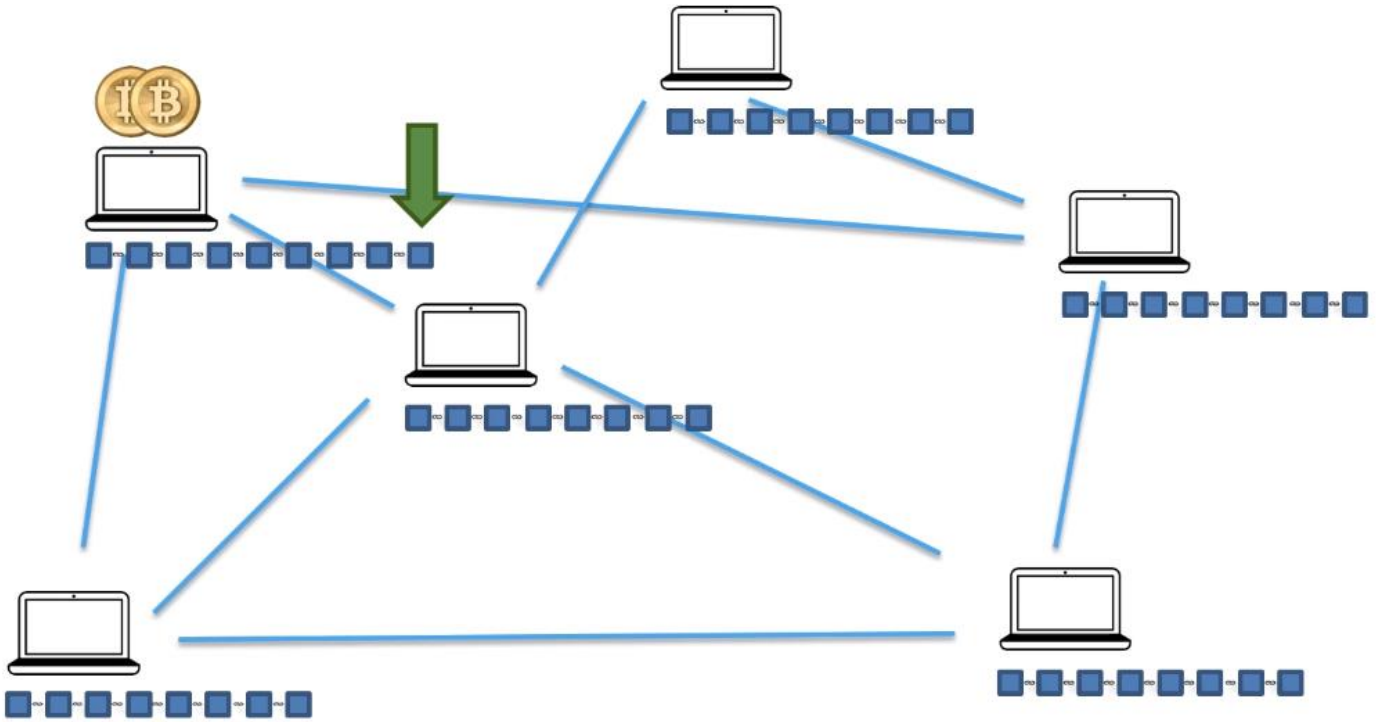
Block consists of

- Prev. block's hash — fixed
- Data (multiple transactions) — fixed
- Block Number — fixed
- Number used once (Nounce) — variable

- Cryptographic challenge: Adjust the nounce in such a was that current hash of the block is less than a threshold value.
- Using brute force. Why?
- Can't predict which nounce will give us the correct hash value of current block. Why?

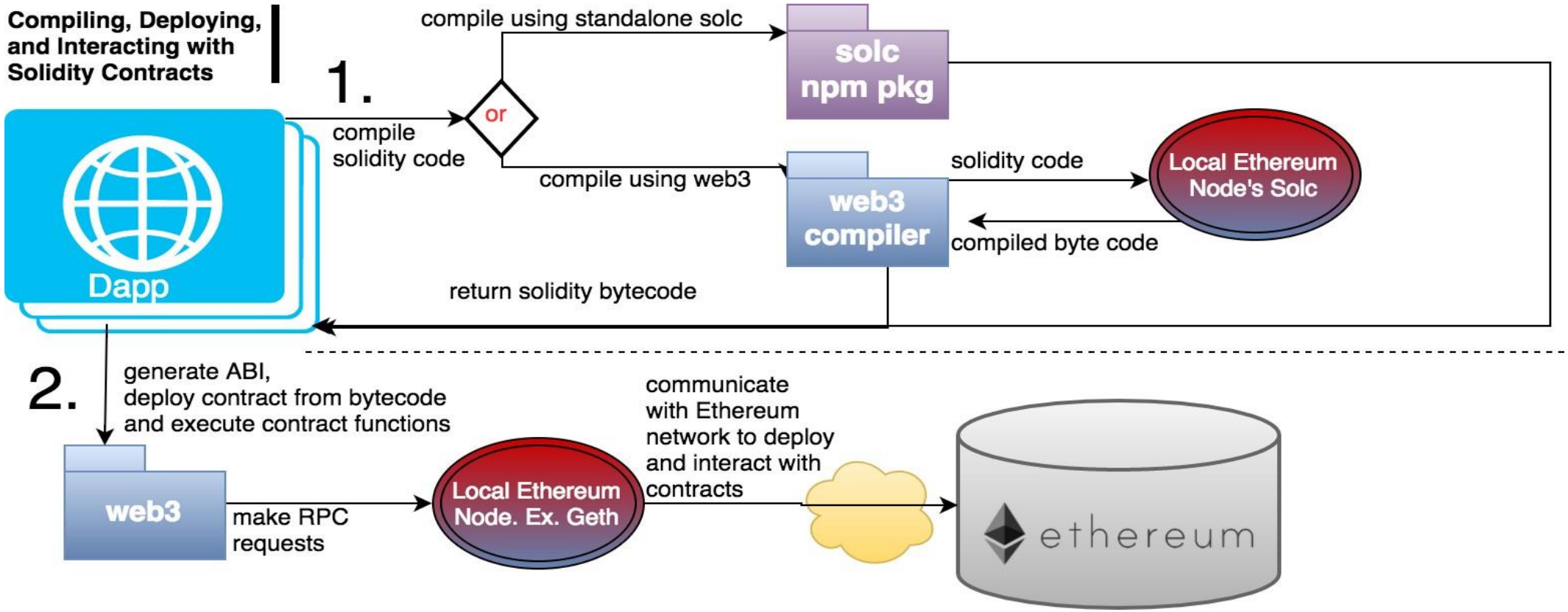
Mining

- cryptographic puzzle are hard to solve



Web3.js

- The key connection between the Ethereum network and your DApp
- Web3 allows you to compile, deploy, and interact with your smart contracts



Use Case – Business to Business Contracts

Why?

What?

- Buyer wants efficient way of converting a purchase order into validated, self executing contract updated to reflect the status of the supply.
- Agreement must be visible to the buyer, the seller, banks, logistics partners and other stakeholders.

How?

- Blockchain provides a shared record of the contract status which is updated as the contract progresses.
- Available to all parties to the agreement, their banks and partners.

Benefits

1. increased efficiency and transparency across the supply chain.
2. risk management improved through the near real time update of all contracts.

Use Case – Smart Refrigerator

What?

- Value of connected smart devices limited by ability to interact with business systems

How?

- Blockchain to manage automated interactions with the external world
- ordering and paying for food to arranging for its own software upgrades and tracking its warranty.

Benefits

1. business value from connected technology
2. efficiencies in network and supply chains.
3. status transparent to all network members

Why?

Use Case – Aircraft Maintenance

Why?

What?

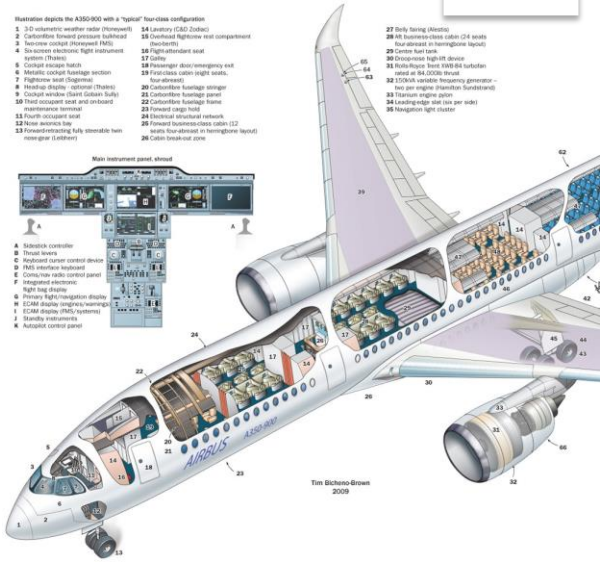
- Provenance of each component part in complex system hard to track
- Manufacturer, production date, batch and even the manufacturing machine program.

How?

- Blockchain holds complete provenance details of each component part
- Accessible by each manufacturer in the production process, the aircraft owners, maintainers and government regulators.

Benefits

1. trust increased no authority "owns" provenance
2. improvement in system utilization
3. recalls "specific" rather than cross fleet



ISSUE: SLOW CROSS-BORDER PAYMENTS

Solution: Introduces a faster and transparent payment gateways

ISSUE: COSTLY SUPPLY CHAIN MANAGEMENT

Solution: Gets rid of fraud with real-time view and increases revenue

ISSUE: ACCOUNTABILITY ISSUES IN TRADITIONAL CONTRACTS

Solution: Smart contracts offers transparency, and faster settlements

ISSUE: VULNERABLE IDENTITY MANAGEMENT AND THEFT

Solution: Digital identity offers safety and modularity to a person's identity

ISSUE: MISMANAGEMENT IN HEALTH CARE ORGANIZATIONS

Solution: Protects and stores patient data with full transparency

ISSUE: DIGITAL COPYRIGHT AND PIRACY

Solution: Offers decentralized copyright, piracy tracking and validation

ISSUE: SLOW GOVERNMENT SYSTEMS AND PUBLIC SECTORS

Solution: Provides faster, secured and cost-effective governmental systems

ISSUE: CORRUPTED CROWDFUNDING AND FUNDRAISING

Solution: Introduces real-time tracking, and immutable solutions

ISSUE: INADEQUATE REAL ESTATE ASSETS

Solution: Ensures liquidity and promotes fair buying and selling process

ISSUE: UNFAIRNESS IN SPORTS AND ESPORTS

Solution: Focuses on the well-being of players rather than companies

SUPPLY CHAIN MONITORING
Removes fraud, improves efficiency, and reduces cost.

BANKING
Faster money transfers, low fees, and better KYC.

DIGITAL IDENTITY
Unified digital system, paperless and trustable.

COPYRIGHT PROTECTION
Automated copyright management and royalty protection.

DIGITAL VOTING
Full transparency, hassle-less, and universal.

REAL ESTATE
Less paperwork, fractional ownership, and no mediator.

CHARITY
More transparency, no mediator cut, and global reach.

TRADING PHARMACEUTICALS
No counterfeit drugs, immutable supply chain, and cost-effective.

ASSET MANAGEMENT
Efficient trade processing and settlement.

CLAIMS PROCESS
Automated claims process with smart contracts.

CERTIFICATE VERIFICATION
Global degree verification, paperless certificates.

MEDICAL RECORDKEEPING
Less paperwork, more accurate record-keeping.

On Line Gaming

- What?
- Game player wants to trade “gold” earned in current game for the currency or assets of another game
- Use experience with the current game to put me ahead and not have to start cold in the new game
- How?
- Blockchain holds tokens of value shared across on line gaming platform
- Benefits
- Transparency to game player, game owners & infrastructure providers
- Efficiencies through elimination of intermediaries
- Increased trust for all involved parties.

Other Potential Use Cases include . .

Why?

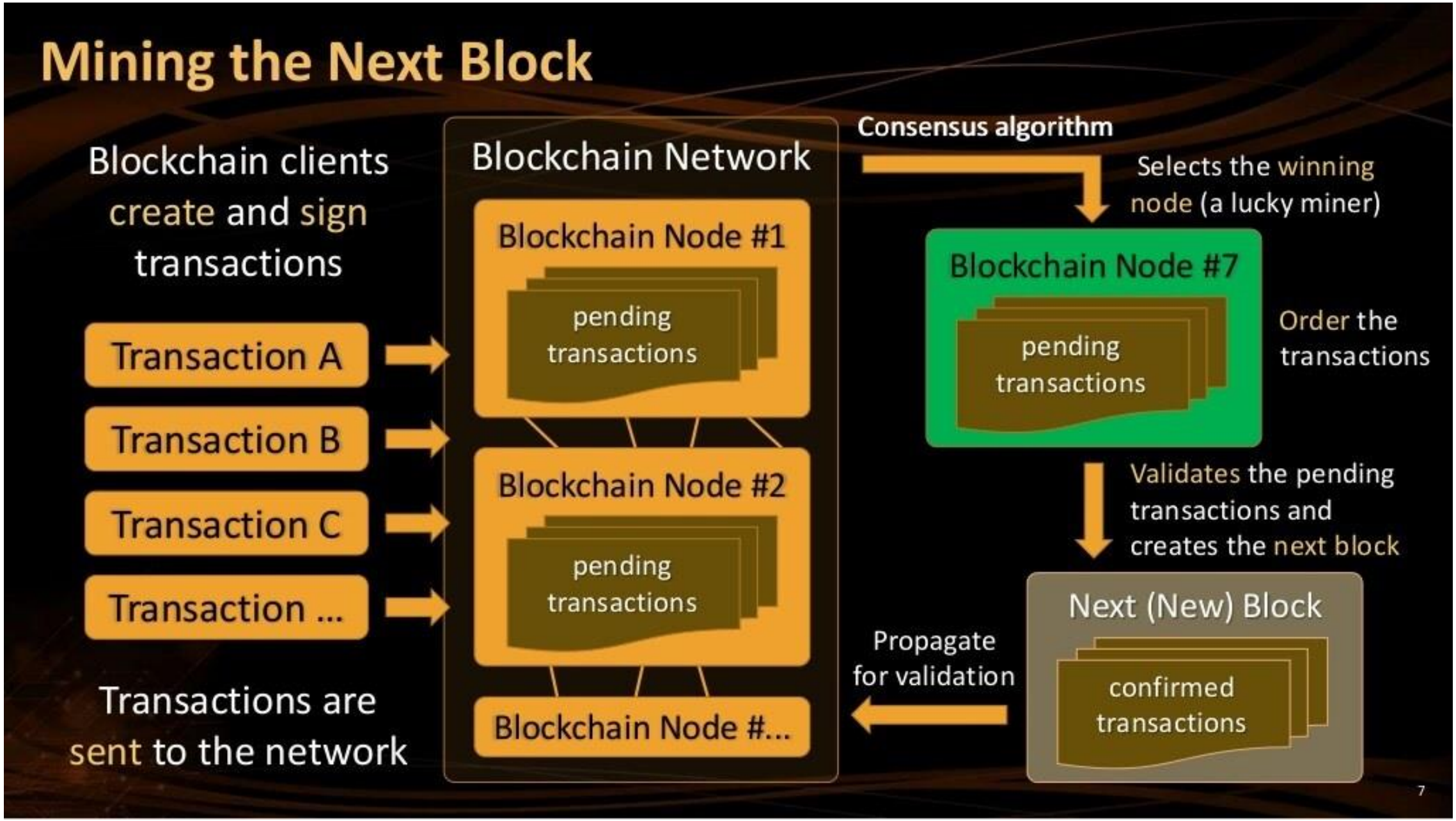
- **Securities**
  - Post-trade settlement
  - Derivative contracts
  - Securities issuance
  - Collateral management
- **Trade Finance**
  - Bill of Lading
  - Cross-currency payment
- **Syndicated Loans**
- **Intra-bank settlement**

- **Retail Banking**
  - Cross border remittances
  - Mortgage verification
  - Mortgage contracts (smart contract)
- **Public Records**
  - Real estate records
  - Vehicle registrations
  - Business license and ownership records

Consensus Algorithms: Basics

- What is mining ???

Mining the Next Block



What is Consensus Algorithm?

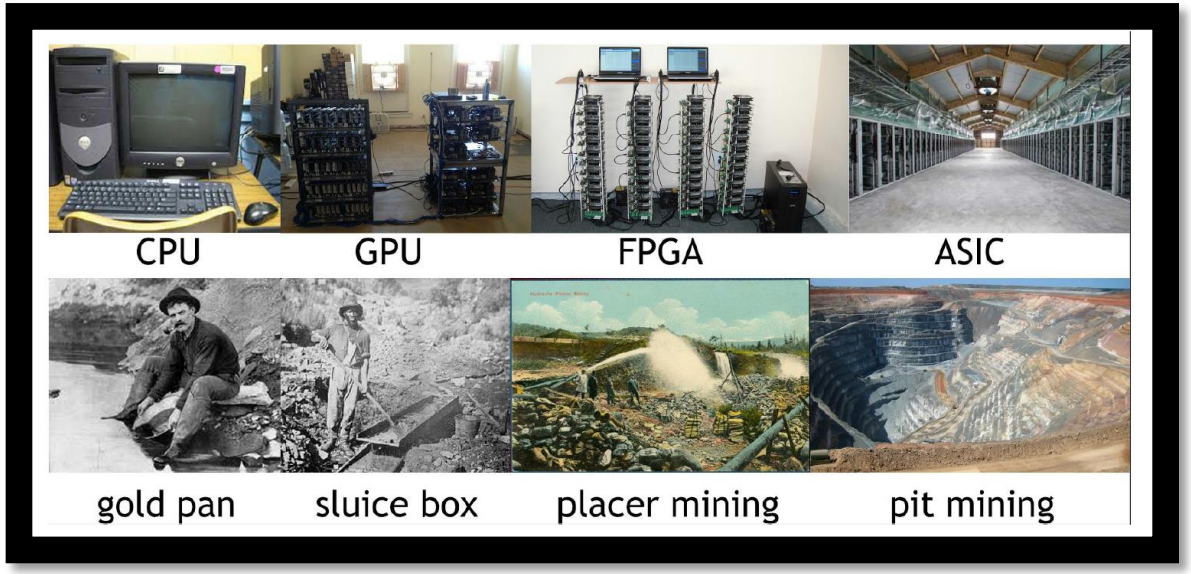
- **Consensus algorithm** (consensus protocol / consensus mechanism)
  - Algorithm to reach agreement among the blockchain nodes
  - All nodes should agree about the changes in the distributed ledger
- Proof-of-work (PoW), Proof-of-stake (PoS), other algorithms

Proof of Work
vs
Proof of Stake

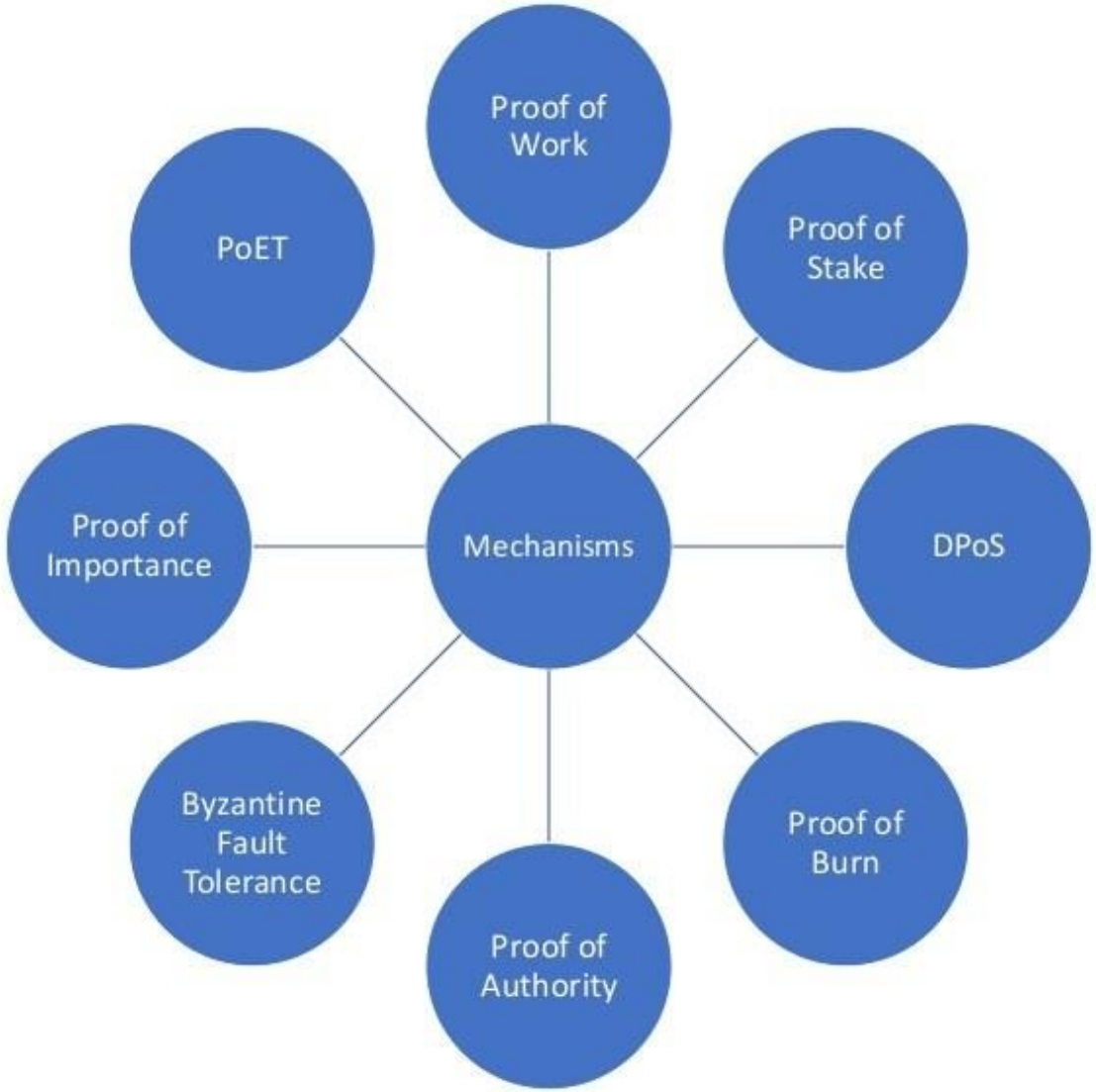
Consensus Algorithm – Requirements

- Fault-tolerance
  - Some nodes will be unavailable when the ledger is changed
  - Consensus should be reached by part of the nodes (e.g. majority)
- Attack-resistance
  - Some nodes will intentionally behave incorrectly
  - Honest nodes should win in the consensus process
  - Everyone on the network can verify the next block's correctness
  - Too much resources should be required for a successful attack

Professional mining



Consensus Mechanisms



Proof-of-Work (PoW)

- A "proof-of-work" (PoW) is a piece of data which is:
  - Difficult to produce
  - Easy for others to verify

- Producing a proof-of-work can be a random guessing process
  - Or can be organized in mining pools (joint PoW production)
- Example:
  - Find a number ***x***, such that **SHA256(*text* + *x*)** has 10 leading zeroes
  - 10 zeroes == network difficulty

Proof-of-Work: Problems

- Needs computing power
  - Computationally expensive
  - Energy intensive

- 51% attack
  - Attackers holding more than 50% of the power could potentially reverse-back transactions (double-spend money) / deny service
- Hashing algorithm types for PoW consensus
  - ASIC mineable (e.g. SHA256), CPU mineable (e.g. CryptoNight), GPU mineable (e.g. ETHash), CPU + GPU mineable (e.g. Equihash)

Proof-of-Work: Problems (2)

- Transactions speed – average wait time
  - Bitcoin: new block mined in ~ 9-10 minutes
  - Ethereum: new block mined in ~ 10-15 seconds
  - Business needs real-time transactions (milliseconds)
- Transactions throughput – transactions per second (tps)
  - Bitcoin: 2000-3000 / transactions per block → 3-5 tps (up to 7 tps)
  - Ethereum: 200-300 / transactions per block → 10-15 tps
  - Business needs thousands tps (e.g. VISA performs 2000 tps)

Originated in 1993 by Cynthia Dwork and Moni Naor

Why initially created?: Discourage DDoS but after 2009 was adopted for "trustless and distributed consensus"

Trustless and distributed consensus: Send/Receive money without a third party (bank)

Validation: Prove that you have spent a lot of computing power in making a block

Rewards: Given to the first miner who solves each blocks problem

How it works?

Transactions are bundled together into what we call a block

↓

Miners verify that transactions within each block are legitimate

↓

To do so, miners should solve a mathematical puzzle known as proof-of-work problem

↓

A reward is given to the first miner who solves each blocks problem

↓

Verified transactions are stored in the public blockchain

Understanding Mining

Mining process is an operation of inverse hashing.

1. Determine a number (nonce)
2. Cryptographic Hash Algorithm of block data results in less than a given threshold (Difficulty)

If more computing power is added to the network can result in:

1. "Difficulty" parameter to increase
2. Increasing the average number of calculations needed to create a new block.
3. Increases the cost of the block creation.
4. This parameter update should occur every 14 days and new block is generated every 10 minutes.

Proof-of-Work Cryptocurrencies

- Different cryptocurrencies use different hashing algorithms
  - Bitcoin, Bitcoin Cash – SHA256 – ASIC mineable
  - Ethereum, Ethereum Classic – ETHash – GPU mineable
  - ZCash, Bitcoin Gold – Equihash – CPU and GPU mineable
  - Monero – CryptoNight – CPU and GPU mineable
  - Litecoin, Dogecoin – SCrypt – GPU mineable
  - Dash – X11 – ASIC, CPU and GPU mineable
  - Stratis – X13 – ASIC, CPU and GPU mineable

See bitinfocharts.com

Proof of Capacity (PoC)

- Similar to PoW, but based on HDD, not CPU / GPU
  - Pay for mining with hard drive space
  - More hard drive space → better chance of mining the next block
- Calculating hashes is slow, so hashes are stored in the HDD for faster access
  - Plots – large data files holding of precomputed hashes
  - More plots → better your chance of finding the next block
  - Plot size is similar to hash rate in PoW

burst-coin.org

Proof of Stake (PoS)

- PoS is designed to increase network security and reduce resource wasting
- The creator of the next block is chosen in
  - Combinations of random selection and wealth
  - E.g. holding 1% of the coins gives the chance to verify (mine) 1% of the "Proof of Stake blocks“

- The "Monopoly Problem": a monopolist (holder of the most coins) could double spend or deny / filter other's transactions
  - Executing a monopoly attack is much more expensive than in PoW

From PoW to PoS Consensus

- Proof-of-stake (PoS) blockchains either
  - Start from a PoW algorithm to mine initial amounts of currency
    - Then switch to proof-of-stake, relying on the mined stakes
    - Example: BitConnect (bitconnect.co)
  - Or fork existing PoW blockchain with all its transactions, then switch to PoS-based consensus
    - Example: PIVX (pivx.org) forked from Dash
  - Or run a hybrid PoW + PoS consensus mechanism

Popular PoS Cryptocurrencies

- Cardano – cardanohub.org
- Qtum – qtum.org
- PIVX – pivx.org
- BitConnect – bitconnect.co
- Stratis – stratisplatform.com

Delegated Proof of Stake (DPoS)

- Stakeholders vote for delegates in democratic way
  - Every wallet holding coins can vote for delegates
  - Votes weight is proportional to the wallet's stake in the network
- Delegates generate new blocks (like miners in PoW)
  - Validate transactions and take the fees as profit
  - Maintain the blockchain, e.g. vote for changing the network parameters like block intervals, transaction fees, others
  - Very fast confirmation of transactions (< 1 sec)

Popular DPoS Cryptocurrencies

- Lisk – lisk.io
- EOS – eos.io
- BitShares – bitshares.org
- Ark – ark.io
- Steem – steem.io

Leased Proof of Stake (LPoS)

- In Leased PoS users can choose:
  - To be a full node or lease their stake
- Full nodes maintain the network
  - Process transactions and generate new blocks
  - PoS based on: own stake + leased stake
  - Serve as mining pools (collect fees and distribute the profits)
- Most users lease their stake to full nodes
  - Take a portion from the full node's profits, just like in pool mining

wavesplatform.com

Proof of Burn (PoB)

- PoB is similar to PoS, where stakes are based on burned coins
- Burning coins gives the privilege to mine
  - Burn coins by sending them to a burning address (where they are irretrievable)
  - More coins you burn = better chance to be selected to mine the next block
  - Random selection process (weighted)

http://slimco.in

- Like traditional mining → invest money to get mining power
  - PoW → invest in hardware; PoB → invest in burning coins

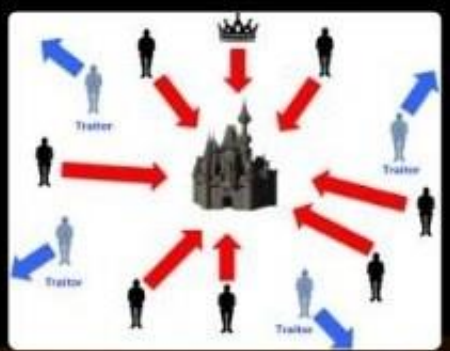
Proof of Importance (PoI)

- PoI is similar to PoS, where stakes are based on coins + activity
- The mining power calculated by the importance in the network
  - More coins hold for long time → bigger importance (like a stake)
  - More transactions / activities → bigger importance

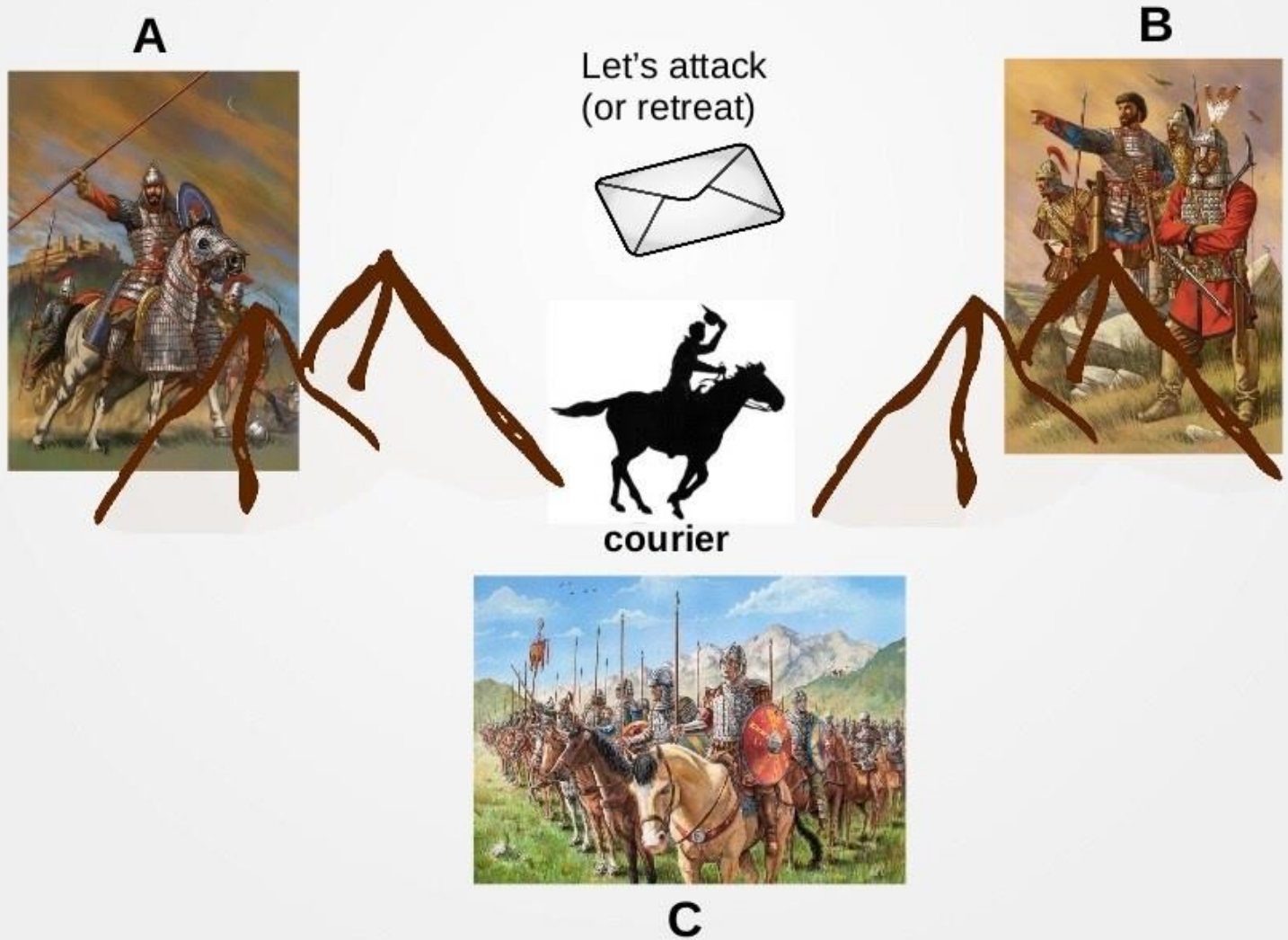
http://nem.io

PBFT (Practical Byzantine Fault Tolerance)

- PBFT as blockchain consensus algorithm
  - Nodes collecting transactions, select a leader for the next block
    - Can be random (deterministic) or random based on a stake
  - The leader orders the transactions + broadcasts the ordered list
  - Each node validates / executes the transactions + broadcasts the calculated hash of the new block
  - When 2/3 of the nodes have the same hash
    - The new block is published (mined)
  - Transactions are very fast



The Two Generals Problem



PBFT Variations and Cryptocurrencies

- Hyperledger Fabric
  - https://hyperledger.org/projects/fabric
- NEO – neo.org
  - Delegated Byzantine Fault Tolerance (dBFT)
- Ripple (XRP) – ripple.com/xrp
  - Ripple Consensus Algorithm
- Stellar – stellar.org
  - Federated Byzantine Agreement (FBA)

Proof of Authority (PoA)

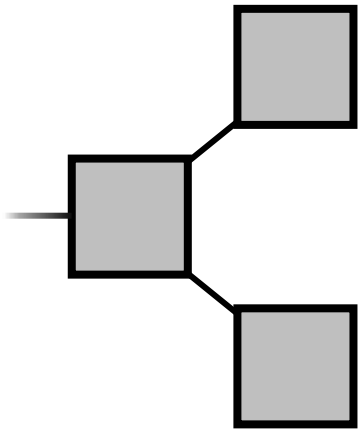
- Proof-of-Authority (PoA) assigns a set of trusted nodes (authorities) to process transactions and build new blocks
  - News blocks need to be signed by the majority of authorities
  - Works very well in private blockchains (cross validation)
  - Great performance, fast transactions, high throughput
- Examples:
  - POA Network – https://poa.network
  - Ethereum Rinkeby Testnet – https://www.rinkeby.io

Proof of Elapsed Time (PoET)

- PoET relies on a trusted execution environment (TEE)
  - Supported by modern CPUs from Intel, AMD and ARM
  - No cryptographic puzzle (like in PoW algorithms)

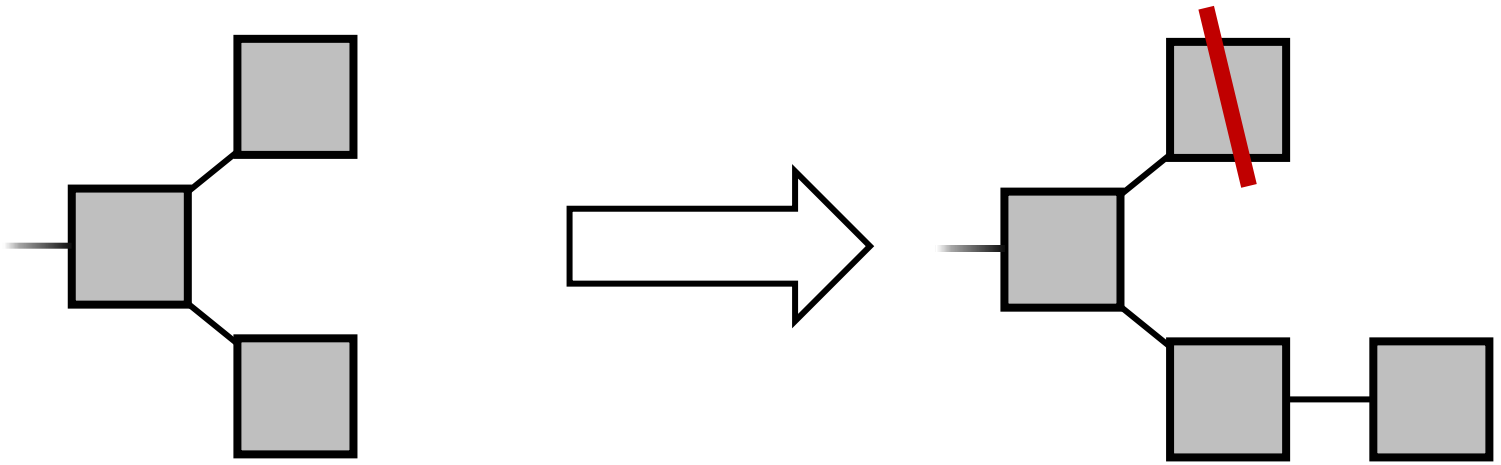
- PoET ensures blocks get produced in a random lottery fashion
  - Generates securely the next block + a proof of the waiting time inside the TEE
  - The proof of waiting time can be verified by all other nodes
- Problem: a small subset of compromised nodes can compromise the entire system

Forks



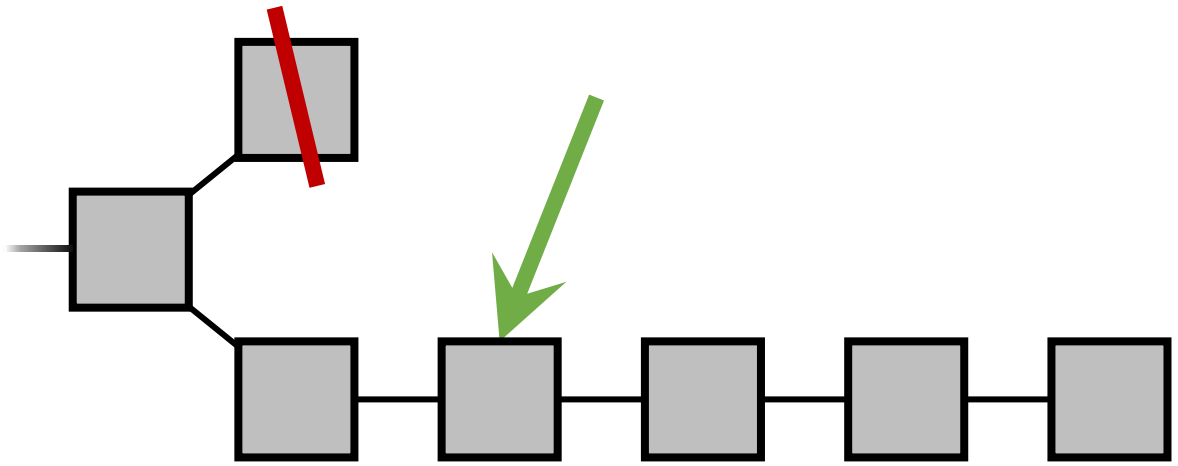
- Natural in a distributed system

Fork Resolution



- **Longest** chain wins
- Transactions are reverted
- Double-spending a threat

Fork Resolution



A transaction is **confirmed** when
it is **buried** deep enough

Key Challenges

1. No stealing: Only Alice can move her money

   Cryptographic signatures
2. No double-spending: Alice cannot duplicate her money

   Global ledger
3. Minting: Fair money creation

   Mint for proof of work

Decentralized

Java-Based Blockchains

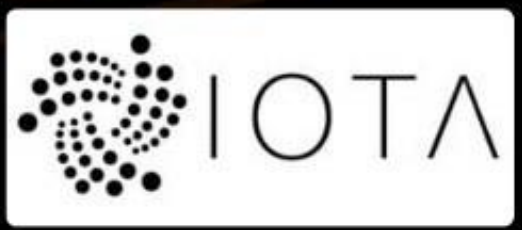
IOTA, NEM, TRON

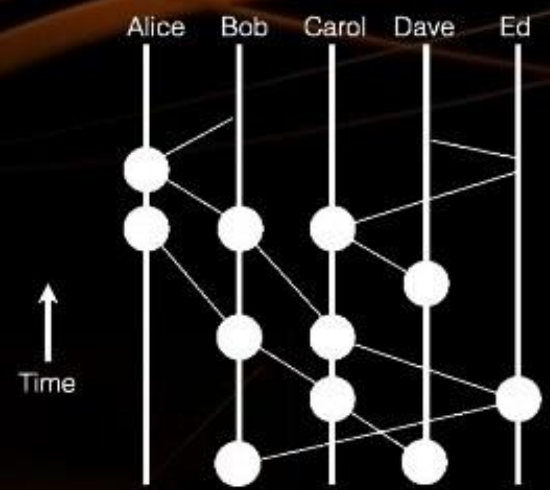
Blockchain Projects and Technologies

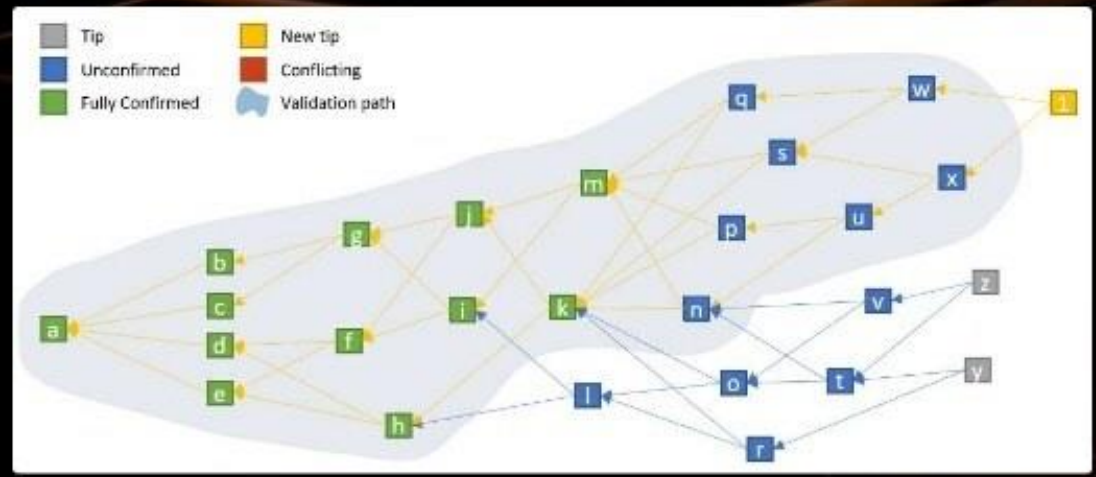
Project	Languages	URL
Bitcoin Core	C++, C	https://github.com/bitcoin/bitcoin
Ethereum	Go (primary), Rust, C++	https://github.com/ethereum
IOTA	Java	https://github.com/iotaledger/iri
Cardano	Haskell	https://github.com/input-output-hk/cardano-sl/
Bitcoin Cash	C++, C	https://github.com/Bitcoin-ABC/bitcoin-abc
Lisk	JavaScript	https://github.com/LiskHQ/lisk
NEO	C#	https://github.com/neo-project/neo
Stellar	C++	https://github.com/stellar/stellar-core
Ripple	C++, C	https://github.com/ripple/rippled

Java-Based Blockchains

- **IOTA** – https://github.com/iotaledger/iri
  - Scalable, almost decentralized DLT for the IoT
  - https://iota.org
- **NEM** – github.com/NemProject/nem.core
  - Blockchain platform – public & private
  - https://nem.io
- **TRON** – github.com/tronprotocol/java-tron
  - Chinese decentralized storage platform
  - https://tron.network







Non-Blockchain DLT

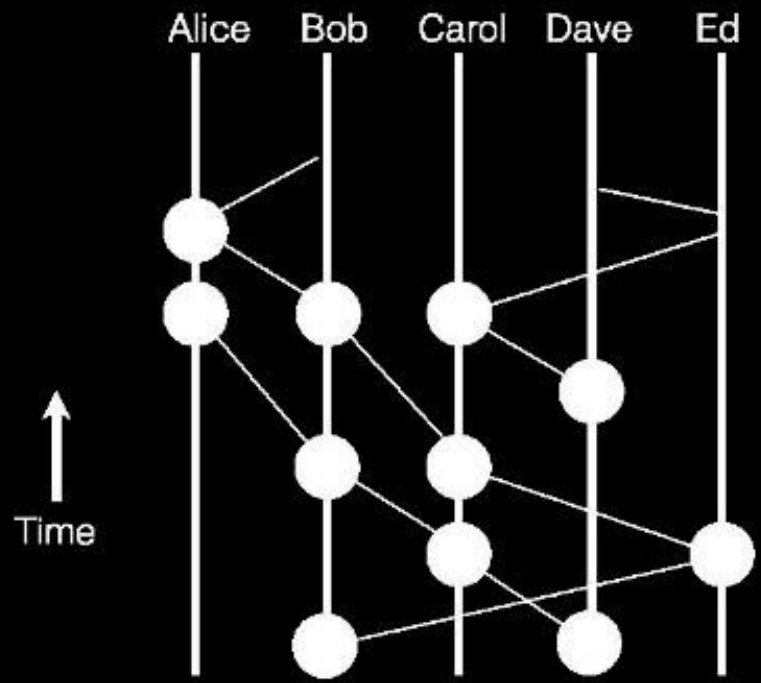
Distributed Ledger Technologies (DLT) without a Blockchain

DAG / Tangle / IOTA

- Tangle == blockless distributed ledger
  - Based on DAG (directed acyclic graph)
  - Used by **IOTA** – iota.org
- Transactions with zero fees
  - Validate 2 transactions to get your transaction validated for free
  - Conflicts detected later, not fully decentralized!
- Store data from sensors and dataloggers securely and verified
  - Scalable – more nodes add more processing power
  - Lightweight – validators don't need the entire blockchain

HashGraph

- Superior distributed ledger technology system
  - https://hashgraph.com
- Fast: with a very high throughput and low consensus latency
- Secure: asynchronous byzantine fault tolerant
- Fair: fairness of access, ordering, and timestamps



Resources for Java Developers

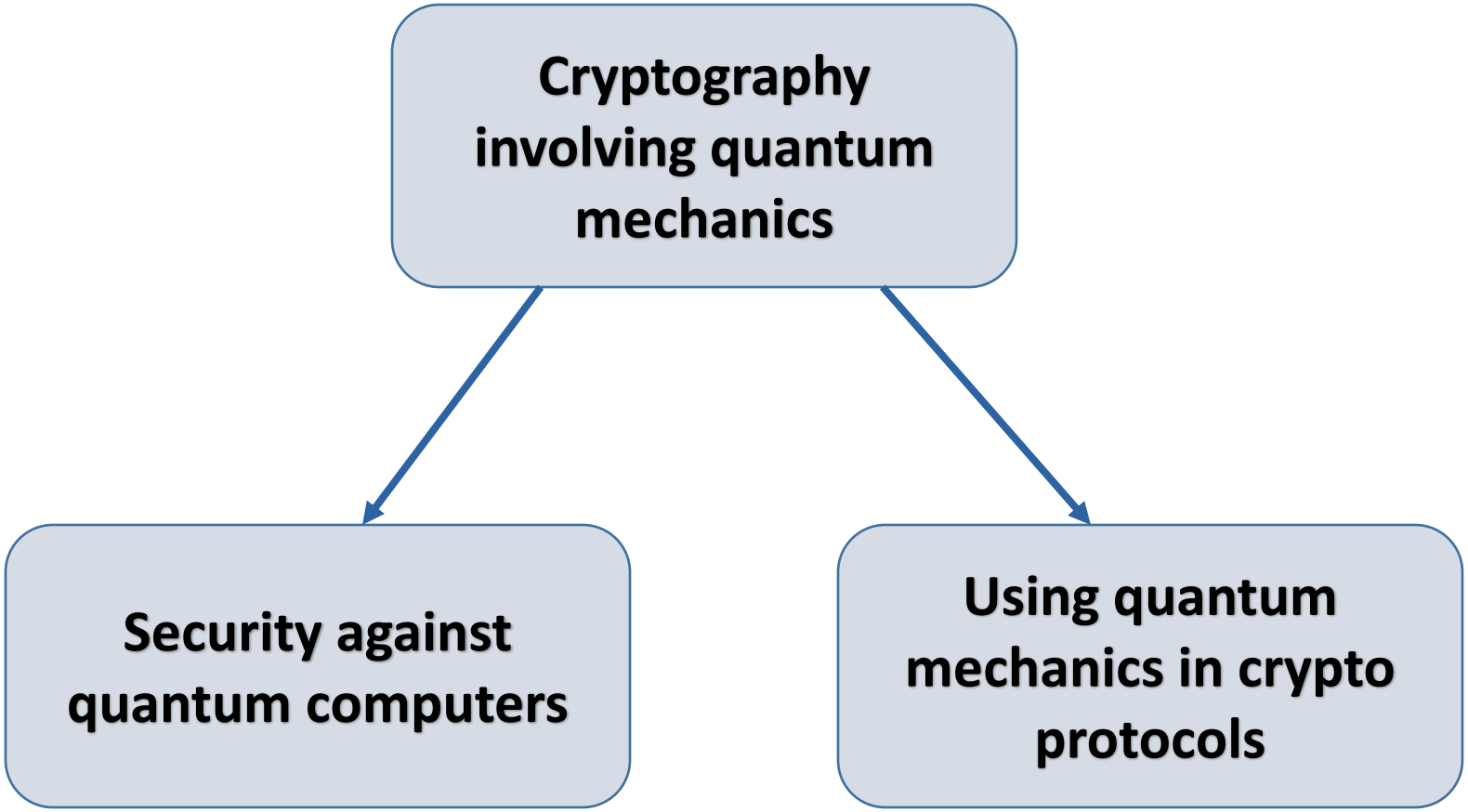
- Web3j – https://github.com/web3j/web3j
  - Ethereum client for Java
- BitcoinJ – https://github.com/bitcoinj/bitcoinj
  - Bitcoin client for Java

Quantum Era

- Quantum crypto:
  - What and why?
  - Challenges.

- Verification of quantum crypto
  - Motivation and challenges
  - Current work

What is quantum cryptography?



1. What is a Quantum and Quantum Bit?
2. Why can Quantum kill Blockchains?
3. How can we protect?
4. When will this all happen?

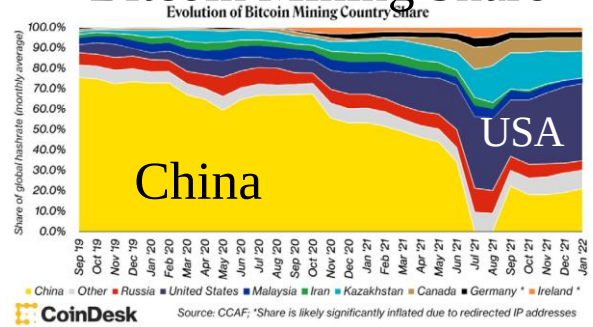
Key Strengths of Blockchains

1. **Distributed**: No single point of failure
2. **Decentralized Consensus**: Transactions are valid only if agreed by a majority
3. **Trustless**: Transacting or processing parties do not need to trust each other
4. **Cryptographic Security**: Elliptic Curve Cryptography
5. **Non-Repudiation Guarantee**: All transactions are signed

Key Weaknesses of Blockchains

1. **Distributed**: Everyone sees every transaction from a given address
   ⇒ reduced privacy.
2. **Decentralized Consensus**: If several mining pools allow a fraudulent block, the block becomes valid ⇒ 51% attack.
3. **Trustless**: No one is responsible ⇒ No one to complain to.
4. **Cryptographic Security**: Based on public-key cryptography.
   3. Stealing private key ⇒ ID theft.
      As of Dec 2017, around ฿980,000 have been stolen from crypto exchanges [Wikipedia]
   4. SHA-256 hash is used in the Merkle Tree inside the blocks
   5. SHA-256 hash is used as pointers between blocks
   6. Uses inverting SHA-256 hash in the Proof-of-Work puzzle to determine the winner of the new coins and transaction fees.
5. **Non-Repudiation Guarantee**: Signatures based on public-key cryptography.

Bitcoin Mining Share



How Quantum Threatens Blockchains?

1. Easy to factorize large numbers

- Easy to find the private key given the public key
- Anyone with your private key can sign your contracts ⇒ ID theft
- They can empty your wallet by giving away your cryptocurrencies

2. Easy to invert one-way hash functions

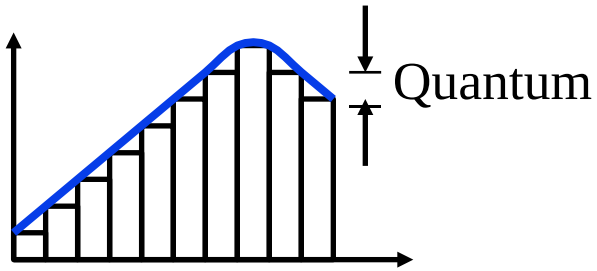
Proof-of-Work uses a puzzle to find the number that hashes below a threshold ⇒ Trivial to win Proof-of-Work puzzles

3. Easily find hash collisions: Two numbers with the same hash

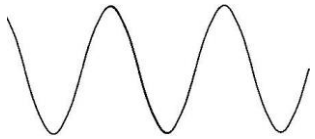
- Hash is used in Merkle tree ⇒ Can change a transaction with no change in hash
- Hash of a block is used as a pointer by the next block
  ⇒ Can change a block such that the hash does not change

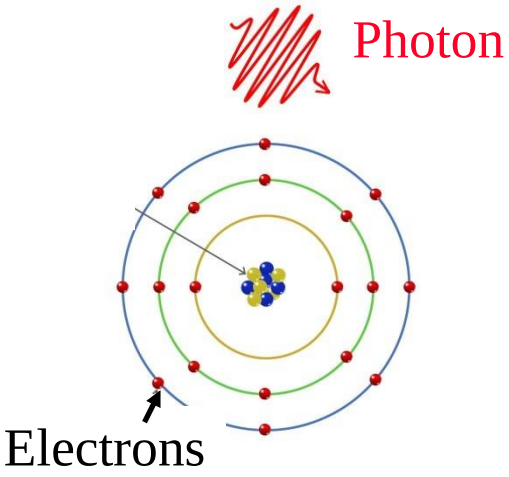
What is a Quantum?

- Quantization: Analog to digital conversion
  - **Quantum** = Smallest discrete unit



- **Wave Theory**: Light is a continuous wave. It has a frequency, phase, amplitude
- **Quantum Mechanics**: Light behaves like discrete packets of energy that can be absorbed and released
- **Photon** = One quantum of light energy
- Photons can move an electron from one energy level to the next higher level
- Photons are released when an electron moves from one level to a lower energy level





Quantum Bits

1. Computing bit is a binary scalar: 0 or 1
2. Quantum bit (Qubit) is a 2×1 vector of complex numbers,

$$\begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix} = \frac{3}{5}\begin{bmatrix} 1 \\ 0 \end{bmatrix} + \frac{4}{5}\begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

Dirac Notation $\quad |0> \quad |1>$

3. When a qubit is measured, the result is discrete (0 or 1) and probabilistic
   The probability of each vector element is proportional to its modulus square

$$\begin{bmatrix} 3/5 \\ 4/5 \end{bmatrix} \quad \begin{matrix} 9/25 \\ 16/25 \end{matrix} \quad \begin{matrix} 36\% \longleftarrow \text{Probability of being measured as 0} \\ 64\% \longleftarrow \text{Probability of being measured as 1} \end{matrix}$$

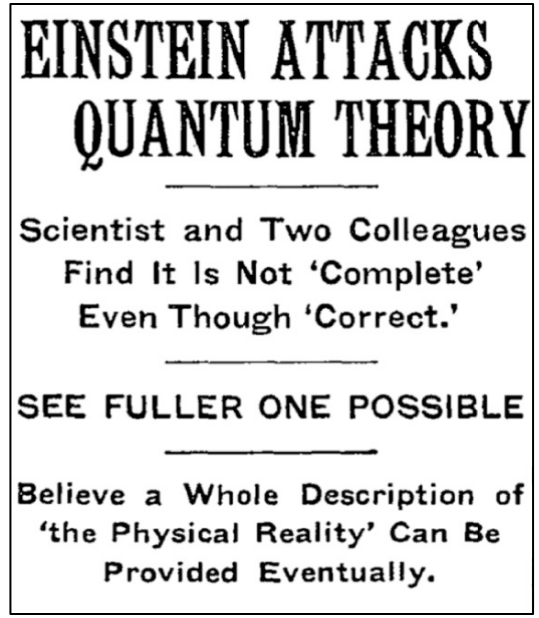
4. Qubit measurement can result in any of its two values. This is called superposition.
5. *n*-qubit are vectors of 2^n elements and can be written as expressions with 2^n coefficients

$$\begin{bmatrix} 4/5 \\ 1/5 \\ 2/5 \\ 2/5 \end{bmatrix} = \frac{4}{5}|00> + \frac{1}{5}|01> + \frac{2}{5}|10> + \frac{2}{5}|11>$$

Entanglement

- Two qubits can be entangled ⇒ Their states are correlated
  - Momentum, spin, polarization, or position are correlated
  - Even when they are far apart
  - Any change of one qubit affects the other
    ⇒ Teleportation of state ⇒ Quantum Key Distribution
- 1935: Einstein called it a paradox since change happens at speed faster than light
- 1967: Kocher developed an apparatus to produce entangled photons
- 1984: Quantum Key Distribution (QKD) protocols using entanglement
- 2022: Physics Nobel Prize for experiments with entangled photons

Both think the same



EINSTEIN ATTACKS QUANTUM THEORY

Scientist and Two Colleagues Find It Is Not 'Complete' Even Though 'Correct.'

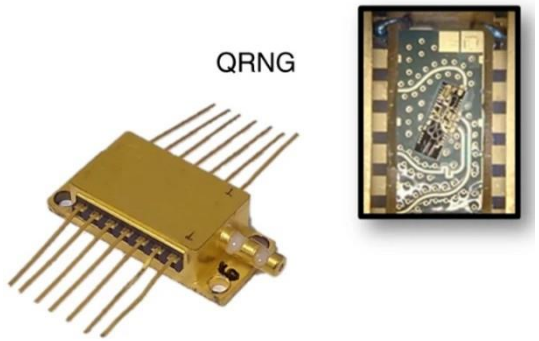
SEE FULLER ONE POSSIBLE

Believe a Whole Description of 'the Physical Reality' Can Be Provided Eventually.

May 4, 1935 Issue of the New York Times, Source: Wikipedia

Quantum Random Number Generator

- Cryptographic keys generated using pseudo-random number generators (PRNG) can be broken using the known information about the PRNG.
- Need true random numbers to generate cryptographic keys that have no bias
- Thermal noise is sometimes used, but it has a bias
- It is easy to get true random numbers using quantum mechanics
- ID Quantique supplies quantum random number generator (QRNG) chips
  - Samsung uses it in Galaxy Quantum 2 smartphones



Factorization on Classical Computer

- Brute-Force using primes: 1, 2, 3, 5, 7, …, $\sqrt{N}$
- There is no general-purpose factorization algorithm
- In 2019, a group of scientists factored a 240-digit (795-bit) number (RSA-240) using 900 core years. RSA 1024 will take 500 times longer.
- Most difficult to factor are products of two primes of similar size ⇒ used for cryptography
- In 2020, RSA-250 was broken using 2700 core years (using an optimized algorithm).
- No published algorithm can factor a b-bit number in $O(b^k)$ time.
  ⇒ No polynomial time algorithm using classical computing
- In 1994, Shor published an algorithm to factorize in polynomial time on a quantum computer ⇒ Polynomial in log N

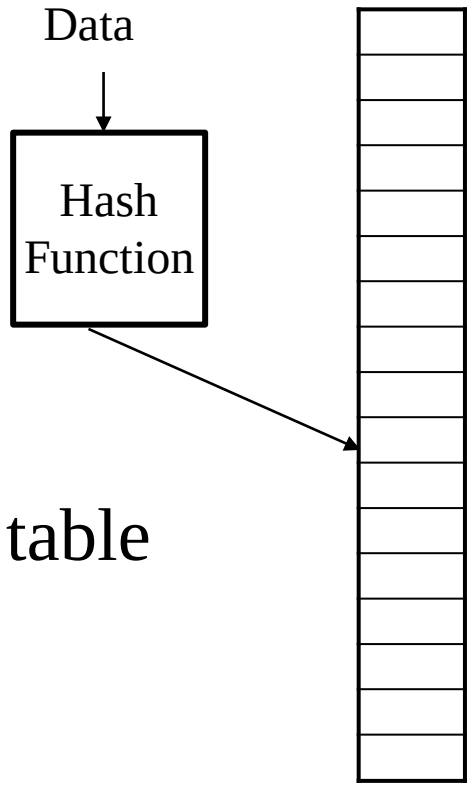
Shor's Factoring Algorithm

- Peter Shor, a graduate of and a professor at MIT developed an algorithm to find prime factors of numbers exponentially faster than conventional computers
- **Step 1:** Find the period of the a^i mod N sequence,
  i.e., find p such that Mod(a^p,N)=1
  Here a is co-prime to $N \Rightarrow a$ is a prime such that gcd(a, N) = 1
  gcd = greatest common divisor $\Rightarrow a$ and N have no common factors.
- **Step 2:** Prime factors of N might be gcd$(N, a^{p/2}+1)$ *and* gcd$(N, a^{p/2}-1)$
  If p is odd, you need to select another a and go back to step 1
- Example: N=15, a=2;
  2^i mod 15 for i=0, 1, 2, …
  = 1, 2, 4, 8, 1, … $\Rightarrow p$=4
- The factors are gcd(2^2+1, 15) and gcd(2^2-1, 15), i.e., 3 and 5.

Ref: P. W. Shor, "Algorithms for Quantum Computation: Discrete Log and Factoring," Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, IEEE, 1994, p. 124

Hash Function

Hash Function



- Database Search hash functions

1. Take variable size input
2. Produce fixed output size (Size of table N)
3. Be easy to compute
4. Be pseudorandom so that it distributes uniformly over the table
   - $\Rightarrow$ Minimizes collisions

- **Cryptographic Hash Functions**

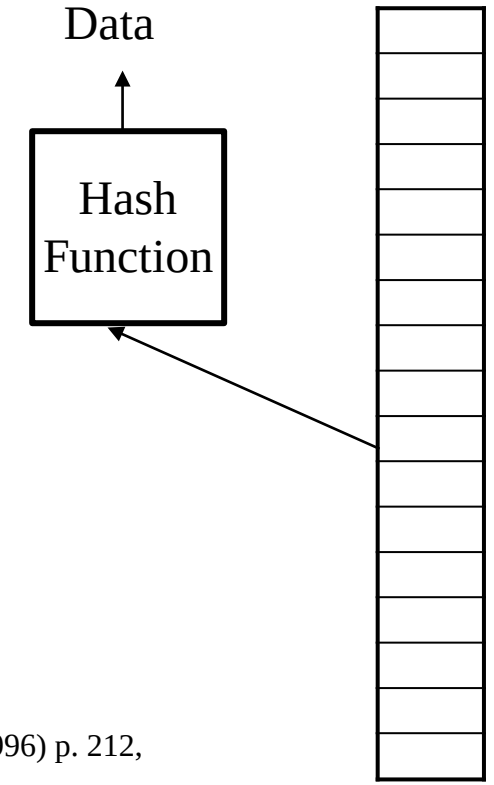
5. One-way. Very difficult to find x, given h(x).
6. Given x, It is not possible to find y, such that h(y)=h(x)
7. Strong Collision Resistant: It is not possible to find any two x and y, such that h(y)=h(x)

Inverting Hashes

- Hashes are one-way functions
- Given *x*, it is easy to find h(*x*),
  but given h(*x*), very difficult to find *x*
- Hash inversion is used as the puzzle in the Bitcoin blockchain
- Bitcoin miners try to find *x* that will hash to a number h(*x*)<N
- The difficulty increases as N is decreased
- As the computing power increases, Bitcoin difficulty is also increased, requiring more and more computing energy
- This applies to all other blockchains that use "Proof-of-Work" as the consensus algorithm

Grover's Algorithm

- Lov Kumar Grover, a graduate of IIT Delhi and Ph.D. from Stanford invented a "quantum mechanical database search algorithm."
- Unstructured search using $O(\sqrt{N})$ operations, where N is the size of the search table.



- Can invert any hash in $O(\sqrt{N})$ operations
  Classical computing takes O(N) operations
- Miners can solve an SHA-256 puzzle in 2^{128} iterations rather than 2^{256}
  $\Rightarrow$ 10 *quadrillion* times faster $\Rightarrow$ Big money saver for Bitcoin miners
- A hacker can find hash collisions a ten quadrillion times faster
  - Makes changing transactions/blocks a ten quadrillion times faster without affecting hash values

Ref: L. K. Grover, "*A fast quantum mechanical algorithm for database search*," 28th Annual ACM Symposium on the Theory of Computing, (May 1996) p. 212, https://arxiv.org/abs/quant-ph/9605043

How to Protect Blockchains?

A. **Quantum-Resistant Blockchains**

1. **Post-Quantum Cryptography**: Does not use factoring. NIST recommends:
   - ✓ CRYSTALS-KYBER for public-key encryption and key-establishment
   - ✓ CRYSTALS-DILITHIUM, FALCON, and SPHINCS+ for Digital signature
2. **Secret-Key Cryptography**: With sufficiently large keys
3. **Larger Hashes**: SHA-512

B. **Quantum Native Blockchains**: Hybrid of classical computing and quantum computing. Most quantum circuits require classical communication lines after measurement

Ref: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

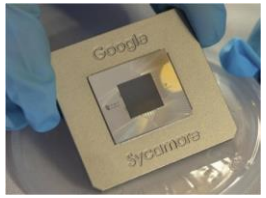
Challenges for Quantum

- **Decoherence**: Qubits lose their state over time.
  In nanoseconds to seconds, depending upon the temperature.
  - Need near zero-kelvin (10 milli Kelvin) temperature ⇒ Large cooling equipment.
  - Need extra qubits for quantum error correction to overcome decoherence
- Errors in quantum computers accumulate fast and require a thousand times more qubits to take care of errors
- Most of the research is theoretical.
  Practical experiments are limited to a tiny number of qubits

Ref: M. Dyaknov, "The case against Quantum Computing," IEEE Spectrum, Nov 15, 2018, https://spectrum.ieee.org/the-case-against-quantum-computing#toggle-gdpr
D. Monroe, "Quantum Computers and the Universe," Communications of the ACM, December 2022, p10-11, https://dl.acm.org/doi/pdf/10.1145/3565977

Challenges for Quantum (Cont.)

- Most promising method of quantum computing consists of interconnected Josephson junctions cooled to 10 milli-Kelvins.
  - Developed initially by D-Wave systems. Now used widely.
  - 49-qubit (Intel), 127-qubit (IBM), 256-qubit (QuEra), and 72-qubit (Google) chips announced but few details
  - November 9, 2022: IBM announced the world's largest quantum computer Osprey, with 433 qubits

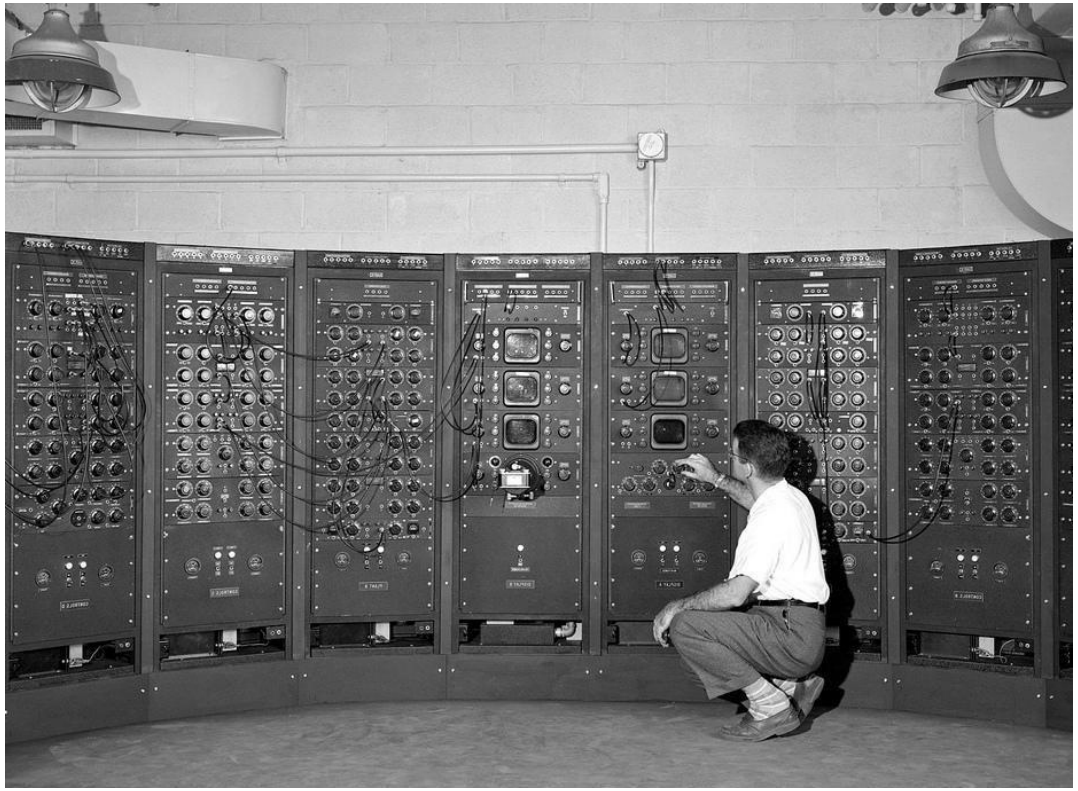


- Need 1000-100,000 qubit quantum computers to do interesting problems
  - 1000 qubits require $2^{1000} \sim 10^{300}$ parameters to describe its state
  - This number is larger than the *number of subatomic particles* in the observable universe.
  - One potential way is to reduce connectivity between qubits

Ref: https://www.newscientist.com/article/2346074-ibm-unveils-worlds-largest-quantum-computer-at-433-qubits/
http://www.cse.wustl.edu/~jain/talks/isba22.htm

Quantum Hardware

IBM's Quantum System One (2019) 20-qubit in a 9 ft cube



ENIAC (1943) 20 accumulators (10 decimal digits each)

Ref: https://www.datacenterdynamics.com/en/news/ces-ibm-announces-q-system-one-quantum-computer-9ft-cube/
http://www.cse.wustl.edu/~jain/talks/isba22.htm

Quantum Simulators

- QCEngine: https://oreilly-qc.github.io/
- Qiskit, https://qiskit.org/
  - Qiskit OpenQASM (Quantum Assembly Language), https://github.com/QISKit/openqasm/blob/master/examples/generic/adder.qasm
- Q# (Qsharp), https://docs.microsoft.com/en-gb/quantum/?view=qsharp-preview
- Cirq, https://arxiv.org/abs/1812.09167
- Forest, https://www.rigetti.com/forest
- List of QC Simulators, https://quantiki.org/wiki/list-qc-simulators
- See the complete list at: https://en.wikipedia.org/wiki/Quantum_programming

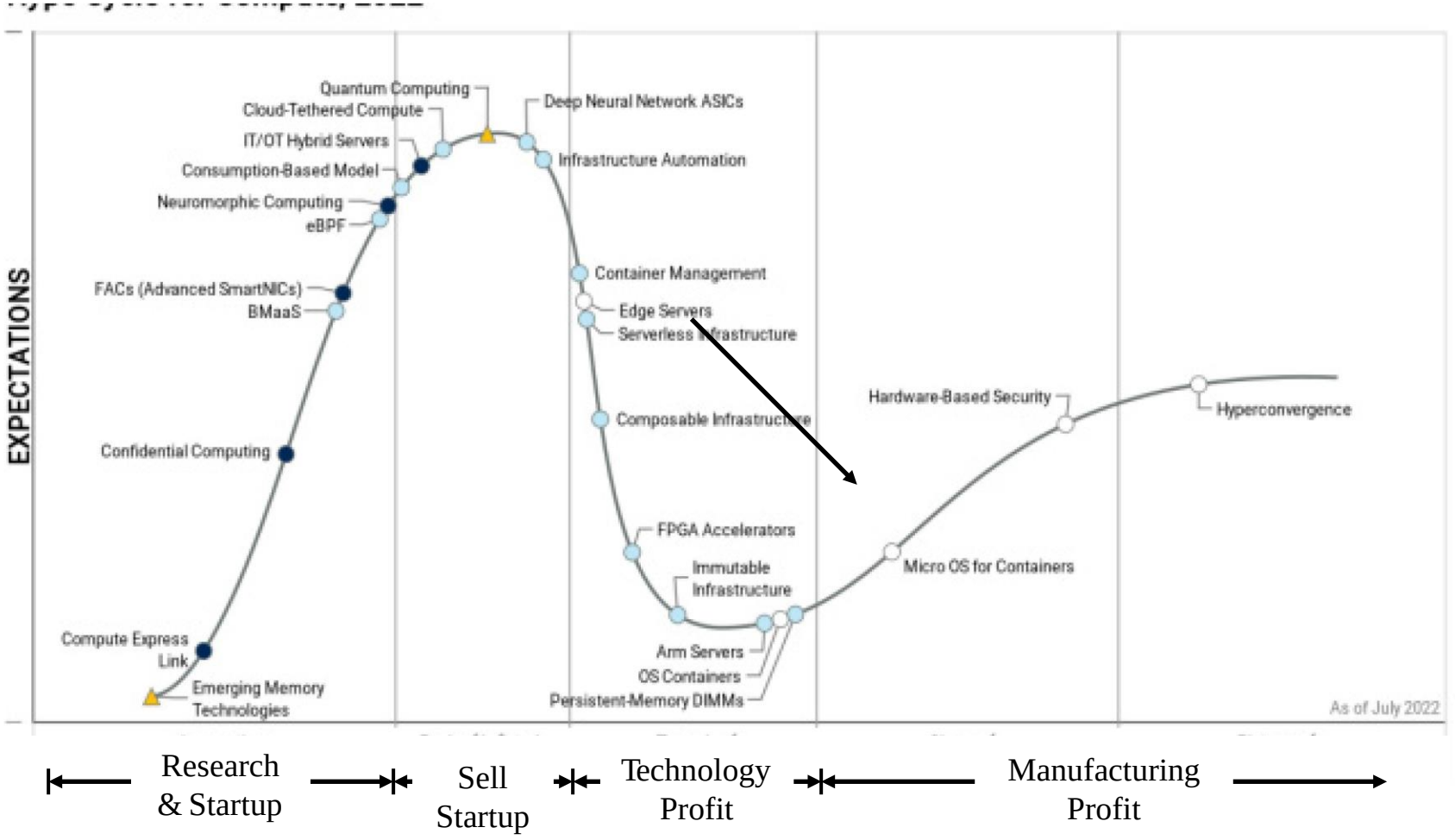
Ref: E. R. Johnston, N. Harrigan, and M. Gimeno-Segovia, "Programming Quantum Computers," O'reilly, 2019, ISBN:9781492039686, 320 pp.

Status of Shor's Algorithm

- 2001: IBM was able to factor 15 with a 7-qubit computer.
- 2012: the factorization of 15 was performed with solid-state qubits
- 2012: the factorization of 21 was achieved
- 2019: an attempt to factor 35 on an IBM Q System One failed because of accumulating errors.
- Quantum circuit for Shor's algorithm needs to be custom designed for each choice of N and each choice of a
- Needs two q-qubit registers, where $q \approx \log_2 N$

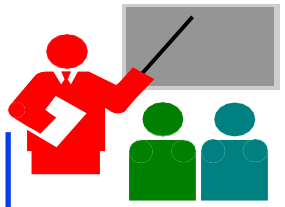
Ref: https://en.wikipedia.org/wiki/Shor%27s_algorithm

Gartner's Hype Cycle for Compute, 2022



▲ >10 years

Ref: T. Harvey, J. Donham, "Hype Cycle for Compute," Gartner G00770247, July 11, 2022.



Summary

1. Quantum computing is based on the discrete nature of photons (Quantum)
2. Qubits indicate the state of a photon.
   n qubits are represented by a vector of 2^n complex numbers
3. Quantum has several interesting phenomena, such as entanglement that can be used to teleport information or to link blocks
4. Shor's factorization algorithm allows the factorization of integers in less time than in classical computing
5. Grover's algorithm can help invert hashes in less time than in classical computing.
6. Blockchains can be broken by these algorithms
7. Quantum-Safe Crypto is in standardization
8. Fortunately, it isn't easy to make sufficient large quantum computers at this time.
   $\Rightarrow$ Not possible for Shor's algorithm or Grover's algorithm to have any impact on this generation of blockchains (2008-2128)

If quantum computers were here…

ElGamal, RSA,
elliptic curve crypto

All commonly used public key crypto:
BROKEN

Lattice-base
McEliec

ents:
died

If quantum computers were available today…

… we would be screwed.

Common symmetric
crypto (AES etc.)

Symmetric crypto:
Double the key length!

Post-quantum cryptography

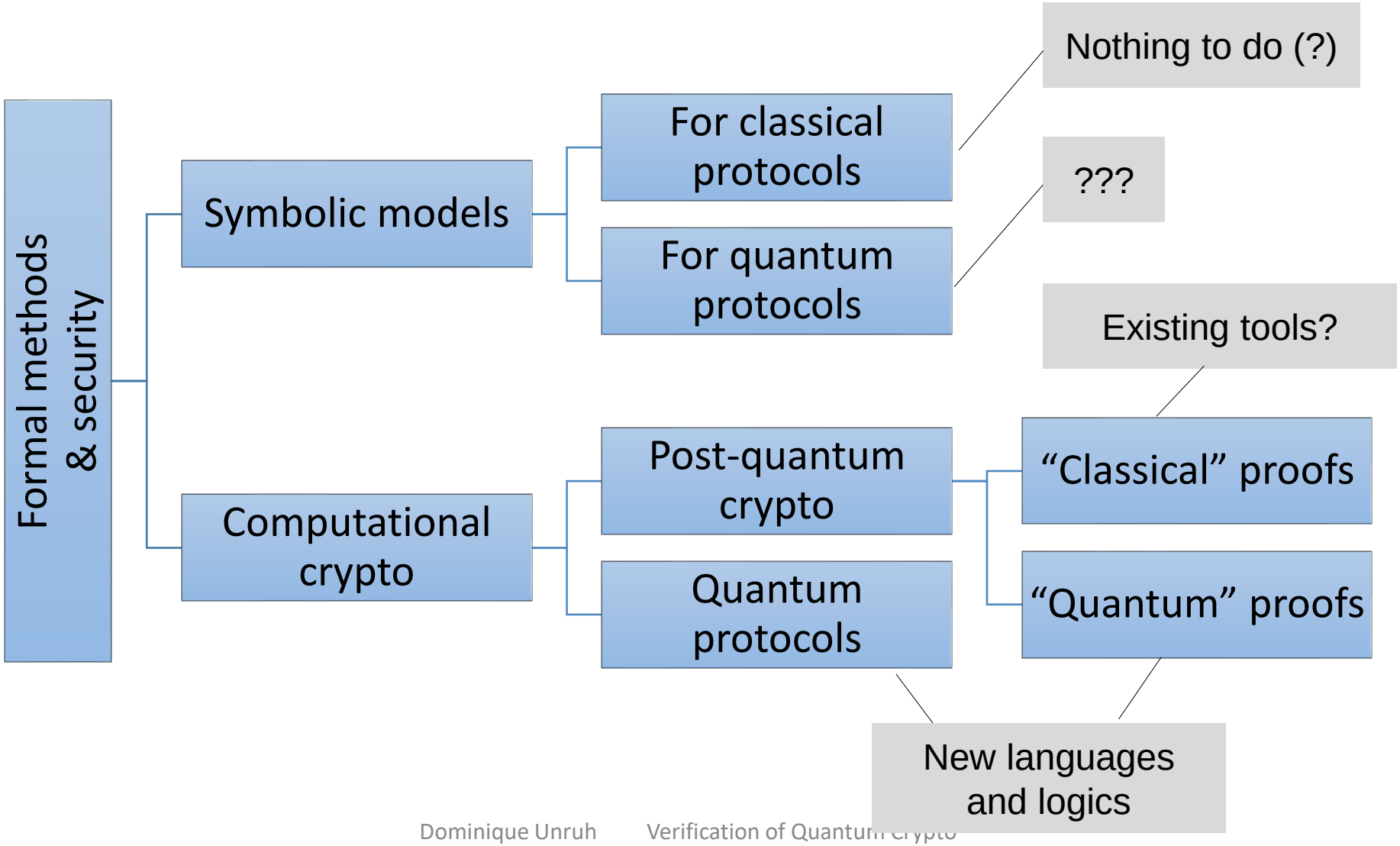
What must be done?

1. Identify assumptions that are not quantum-broken (e.g. lattice based crypto, not RSA)
2. Build cryptosystems based on those
3. Prove security

Needs quantum know-how/techniques

Possible without "quantum literacy"?

Quantum Crypto & Verification



Quantum Hoare Logic

Semantics of programs:

- $\boldsymbol{c}$ a program on classical and quantum variables
- ρ density operator (a "probabilistic quantum state")
- $[\![c]\!](\rho)$ the quantum state after execution

Assertions: Sets of density operators
(preferable closed vector spaces)

Hoare triples:

$$\{P\}\boldsymbol{c}\{Q\} \qquad \text{means} \qquad \forall \rho \in P.\ [\![\boldsymbol{c}]\!](\rho) \in Q$$

Classical Relational Hoare Logic

Assertions: Relations on states
(e.g., $x_1 = x_2 + y_2$)

RHL judgements:

$\{P\}\boldsymbol{c}_1 \sim \boldsymbol{c}_2\{Q\}$ means: if initial states in P,
then final states in Q

E.g.: $\{x_1 = x_2\}\ \text{skip}\ \sim\ x_2 \coloneqq x_2 + y_2\ \{x_1 = x_2 + y_2\}$

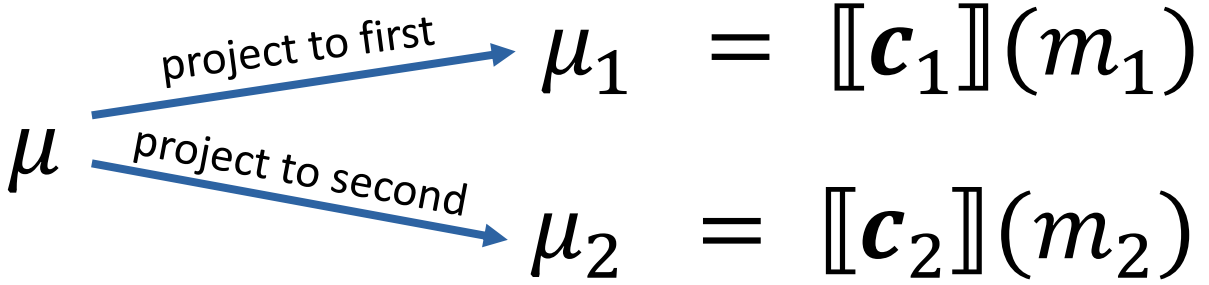
Classical Relational Hoare Logic

RHL judgements:

$\{P\}\boldsymbol{c}_1 \sim \boldsymbol{c}_2\{Q\}$ means: if initial states in P, then final states in Q

Formally: For any $(m_1, m_2) \in P$:
Exists distribution μ on pairs s.t.:

$\Pr[(m_1, m_2) \notin Q]_\mu = 0$ and



Quantum Relational Hoare Logic?

If analogous to classical, loose frame rule:

$$\frac{\{P\}\boldsymbol{c}\{Q\} \qquad R'\text{s variables distinct from } P, Q, \boldsymbol{c}}{\{P \wedge R\}\boldsymbol{c}\{Q \wedge R\}}$$

Without frame rule:

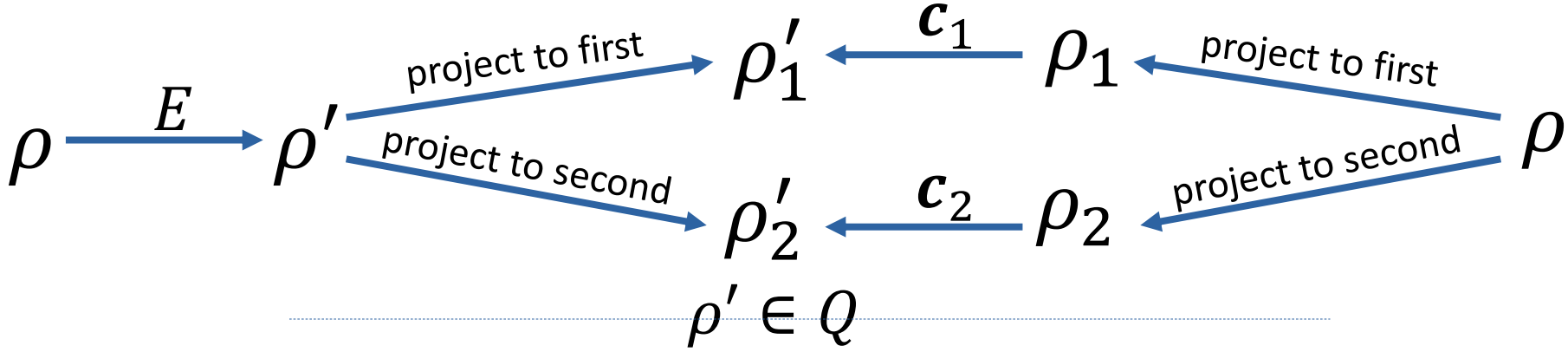
No compositional analysis → useless

Quantum Relational Hoare Logic?

Assertions: Sets of quantum states of systems with two states

qRHL: $\{P\}\boldsymbol{c}_1 \sim \boldsymbol{c}_2\{Q\}$ means:

Exists quantum process E:
For all $\rho \in P$:

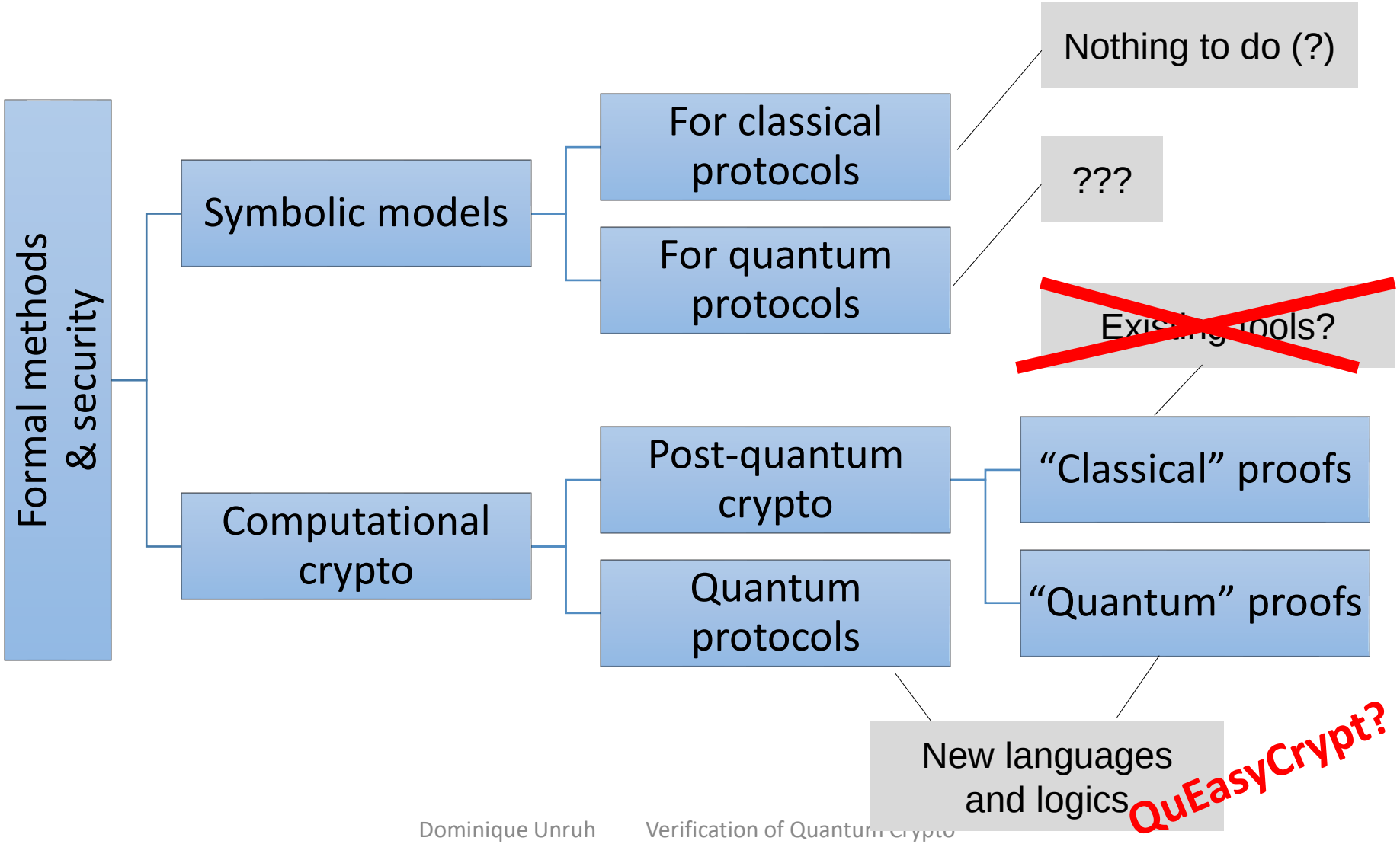


QuEasyCrypt – the future

- If you can use EasyCrypt, you can use QuEasyCrypt
  - Get post-quantum verification for free
    (when classical proof is quantum-sound)

- Verification of quantum protocols:
  - Should be possible
  - Time will show

Summary


Formal methods & security
Symbolic models
Computational crypto
For classical protocols
For quantum protocols
Post-quantum crypto
Quantum protocols
Nothing to do (?)
???
Existing tools?
“Classical” proofs
“Quantum” proofs
New languages and logics
QuEasyCrypt?

BASICS of QUANTUM INFORMATION PROCESSING

BASIC MOTIVATION

In quantum information processing we witness an interaction between the two most important areas of science and technology of 20-th century, between

quantum physics and informatics.

This is very likely to have important consequences for 21th century.

QUANTUM PHYSICS

Quantum physics deals with fundamental entities of physics – **particles** like

• protons, electrons and neutrons (from which matter is built);

• photons (which carry electromagnetic radiation)

• various "elementary particles" which mediate other interactions in physics.

•We call them particles in spite of the fact that some of their properties are totally unlike the properties of what we call particles in our ordinary classical world.

For example, a quantum particle can go through two places at the same time and can interact with itself.

Because of that quantum physics is full of counterintuitive, weird, mysterious and even paradoxical events.

FEYNMAN's VIEW

I am going to tell you what Nature behaves like.....

However, do not keep saying to yourself, if you can possibly avoid it,

BUT HOW CAN IT BE LIKE THAT?

Because you will get ``down the drain'' into a blind alley from which nobody has yet escaped

NOBODY KNOWS HOW IT CAN BE LIKE THAT

Richard Feynman (1965): *The character of physical law*.

CLASSICAL versus QUANTUM INFORMATION

Main properties of classical information:

1. It is easy to store, transmit and process classical information in time and space.
2. It is easy to make (unlimited number of) copies of classical information
3. One can measure classical information without disturbing it.

Main properties of quantum information:

1. It is difficult to store, transmit and process quantum information
2. There is no way to copy unknown quantum information
3. Measurement of quantum information destroys it, in general.

Classical versus quantum computing

- **The essense of the difference between**
- **classical computers** and **quantum computers**
- is in the way information is stored and processed.

- In classical computers, information is represented on macroscopic level by bits, which can take one of the two values

  - 0 or 1

- In quantum computers, information is represented on microscopic level using qubits, (quantum bits) which can take on any from the following uncountable many values

$$\alpha \mid 0 \rangle + \beta \mid 1 \rangle$$

where α, β are arbitrary complex numbers such that

$$\mid \alpha \mid^2 + \mid \beta \mid^2 = 1.$$

CLASIICAL versus QUANTUM REGISTERS

An n bit classical register can store at any moment exactly one n-bit string.

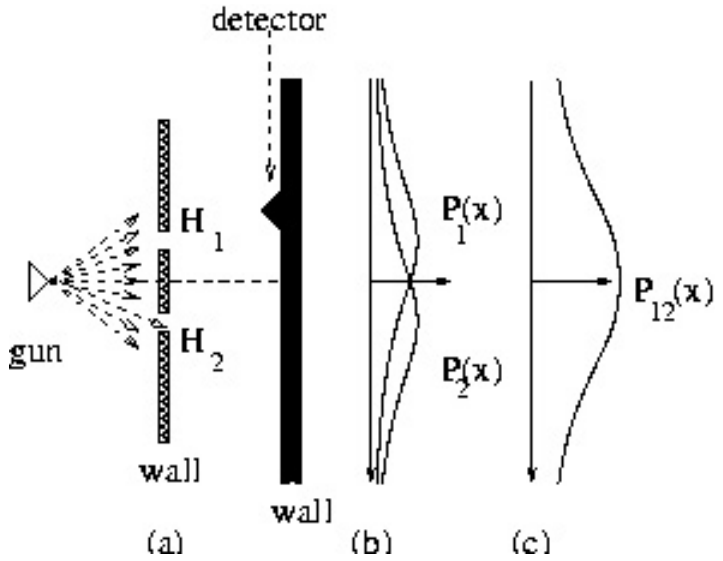
An n-qubit quantum register can store at any moment a superposition of all 2^n n-bit strings.

Consequently, on a quantum computer one can compute in a single step with 2^n values.

This enormous massive parallelism is one reason why quantum computing can be so powerful.

IV054

CLAS[illegible] EXPERIMENTS



•Figure 1: Experiment with bullets

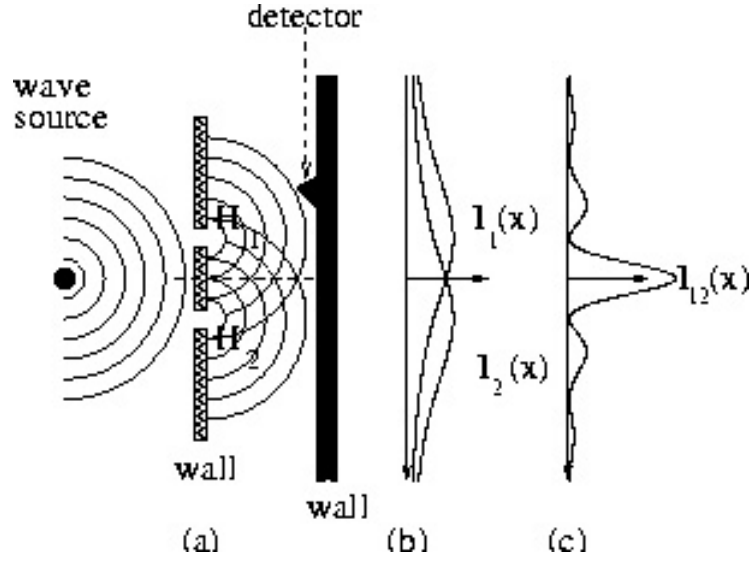
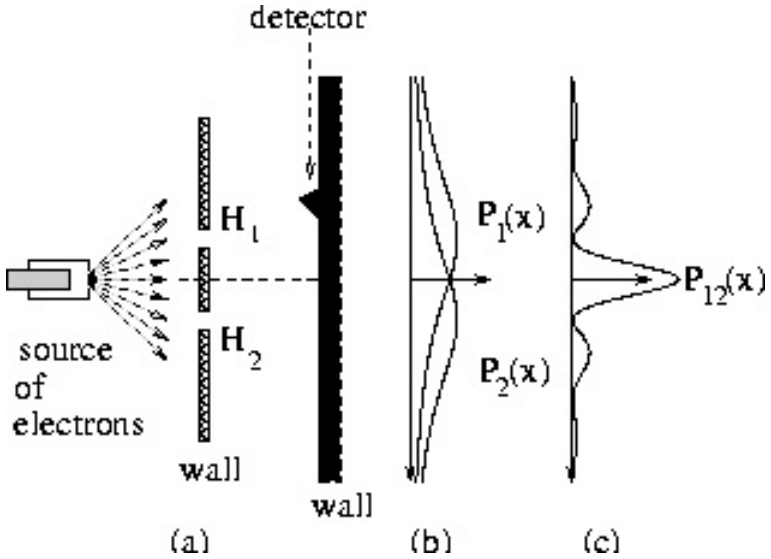


Figure 2: Experiments with waves

QUAN EXPERIMENTS



•Figure 3: Two-slit experiment

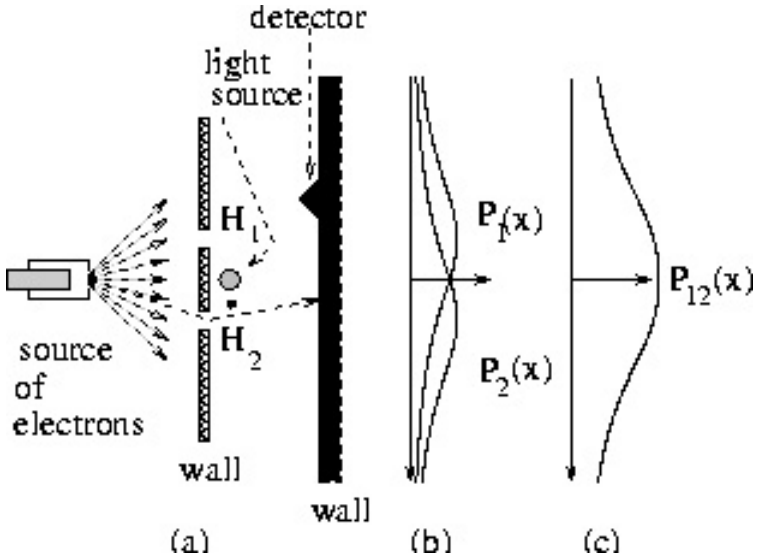


Figure 4: Two-slit experiment with an observation

THREE BASIC PRINCIPLES

•P1 To each transfer from a quantum state ϕ to a state ψ a complex number

$$\bullet \langle \psi \mid \phi \rangle$$

•is associated. This number is called the **probability amplitude** of the transfer and

$$\bullet |\langle \psi \mid \phi \rangle|^2$$

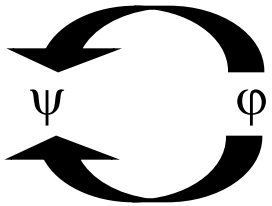
•is then the **probability** of the transfer.

P2 If a transfer from a quantum state ϕ to a quantum state ψ can be decomposed into two subsequent transfers

$$\psi \leftarrow \phi' \leftarrow \phi$$

then the resulting amplitude of the transfer is the product of amplitudes of subtransfers: $\langle \psi \mid \phi \rangle = \langle \psi \mid \phi' \rangle \langle \phi' \mid \phi \rangle$

P3 If a transfer from a state ϕ to a state ψ has two independent alternatives



then the resulting amplitude is the sum of amplitudes of two subtransfers.

QUAN SYSTEMS = HILBERT SPACE

•Hilbert space H_n is n-dimensional complex vector space with

•**scalar product**

$$\langle\psi|\phi\rangle = \sum_{i=1}^{n} \phi_i \psi_i^* \text{ of vectors } |\phi\rangle = \begin{vmatrix} \phi_1 \\ \phi_2 \\ .. \\ \phi_n \end{vmatrix}, |\psi\rangle = \begin{vmatrix} \psi_1 \\ \psi_2 \\ .. \\ \psi_n \end{vmatrix},$$

$$\| \phi \| = \sqrt{|\langle\phi|\phi\rangle|}.$$

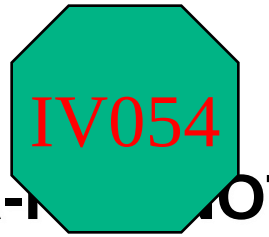
•**This allows to define the norm of vectors as**

•Two vectors $|\phi\rangle$ and $|\psi\rangle$ are called **orthogonal** if $\langle\phi|\psi\rangle = 0$.

•A **basis** B of H_n is any set of n vectors $|b_1\rangle$, $|b_2\rangle$,..., $|b_n\rangle$ of the norm 1 which are mutually orthogonal.

•Given a basis B, any vector $|\psi\rangle$ from H_n can be uniquelly expressed in the form

$$|\psi\rangle = \sum_{i=1}^{n} \alpha_i |b_i\rangle.$$



BRA-KET NOTATION

•Dirack introduced a very handy notation, so called bra-ket notation, to deal with amplitudes, quantum states and linear functionals f: $H \rightarrow C$.

•If $\psi, \phi \in H$, then

•$\langle\psi|\phi\rangle$ - scalar product of ψ and ϕ

• (an amplitude of going from ϕ to ψ).

•$|\phi\rangle$ - ket-vector (a column vector) - an equivalent to ϕ

•$\langle\psi|$ - bra-vector (a row vector) a linear functional on H

•such that $\langle\psi|(|\phi\rangle) = \langle\psi|\phi\rangle$

QUAN EVOLUTION / COMPUTATION

EVOLUTION	COMPUTATION
in	in
QUANTUM SYSTEM	HILBERT SPACE

•is described by

•Schrödinger linear equation

$$ih\frac{\partial \mid \Phi(t) >}{\partial t} = H(t) \mid \Phi(t) >$$

•where h is Planck constant, $H(t)$ is a Hamiltonian (total energy) of the system that can be represented by a Hermitian matrix and Φ(t) is the state of the system in time t.

•If the Hamiltonian is time independent then the above Shrödinger equation has solution

•where $$\mid \Phi(t) >= U(t) \mid \Phi(0) >$$

$$U(t) = e^{iHt/h}$$

•is the evolution operator that can be represented by a unitary matrix. A step of such an evolution is therefore a multiplication of a **unitary matrix** A with a vector $|\psi\rangle$, i.e. $A\ |\psi\rangle$

A matrix A is unitary if

$$A \cdot A^* = A^* \cdot A = I$$

PAULI MATRICES

•Very important one-qubit unary operators are the following *Pauli operators*, expressed in the standard basis as follows;

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

Observe that Pauli matrices transform a qubit state $|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$ as follows

$$\sigma_x(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle + \alpha|1\rangle$$
$$\sigma_z(\alpha|0\rangle + \beta|1\rangle) = \alpha|0\rangle - \beta|1\rangle$$
$$\sigma_y(\alpha|0\rangle + \beta|1\rangle) = \beta|0\rangle - \alpha|1\rangle$$

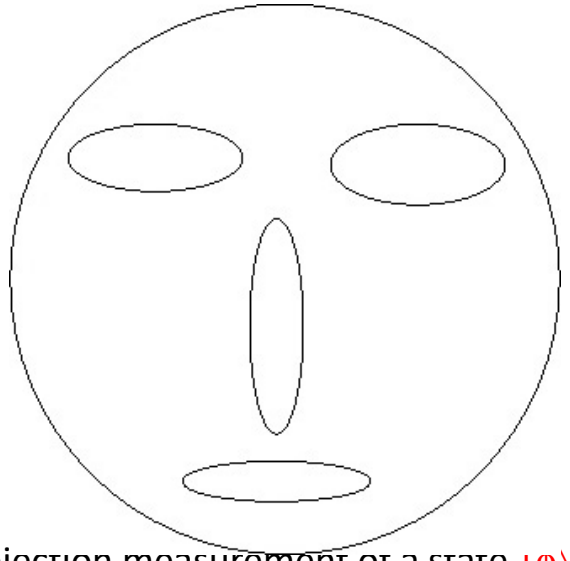
σ_x, σ_z σ_y *bit error* *sign error*

bit-sign error

IV054

QUAN (PROJECTION) MEASUREMENTS

•A quantum state is always observed (measured) with respect to an **observable** O - a decomposition of a given Hilbert space into orthogonal subspaces (where each vector can be uniquely represented as a sum of vectors of these subspaces).



•There are two outcomes of a projection measurement of a state $|\varphi\rangle$ with respect to O:

- 1. Classical information into which subspace projection of $|\phi\rangle$ was made.
- 2. Resulting quantum projection (as a new state) $|\phi'\rangle$ in one of the above subspaces.

•The subspace into which projection is made is chosen **randomly** and the corresponding probability is uniquely determined by the amplitudes at the representation of $|\phi\rangle$ as a sum of states of the subspaces.

QUANTUM STATES and PROJECTION MEASUREMENT

$\{\beta_i\}_{i=1}^n$ $|\phi\rangle \in H_n$

- In case an orthonormal basis is chosen in H_n, any state
- can be expressed in the form

$$|\phi\rangle = \sum_{i=1}^{n} a_i |\beta_i\rangle, \sum_{i=1}^{n} |a_i|^2 = 1$$

- where $a_i = \langle \beta_i | \phi \rangle$
  - are called probability amplitudes
- and
  - $|\phi\rangle$ their squares provide probabilities $\{\beta_i\}_{i=1}^n$
- that if the state is measured with respect to the basis , then the state collapses into the state with probability $|a_i|^2$.
- $|\phi\rangle$ $\{\beta_i\}_{i=1}^n$ $|\beta_i\rangle$

QUBI

•A qubit is a quantum state in H_2

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where $\alpha, \beta \in C$ are such that $|\alpha|^2 + |\beta|^2 = 1$ and

$\{ |0\rangle, |1\rangle \}$ is a **(standard) basis** of H_2

EXAMPLE: Representation of qubits by

(a) electron in a Hydrogen atom

(b) a spin-1/2 particle

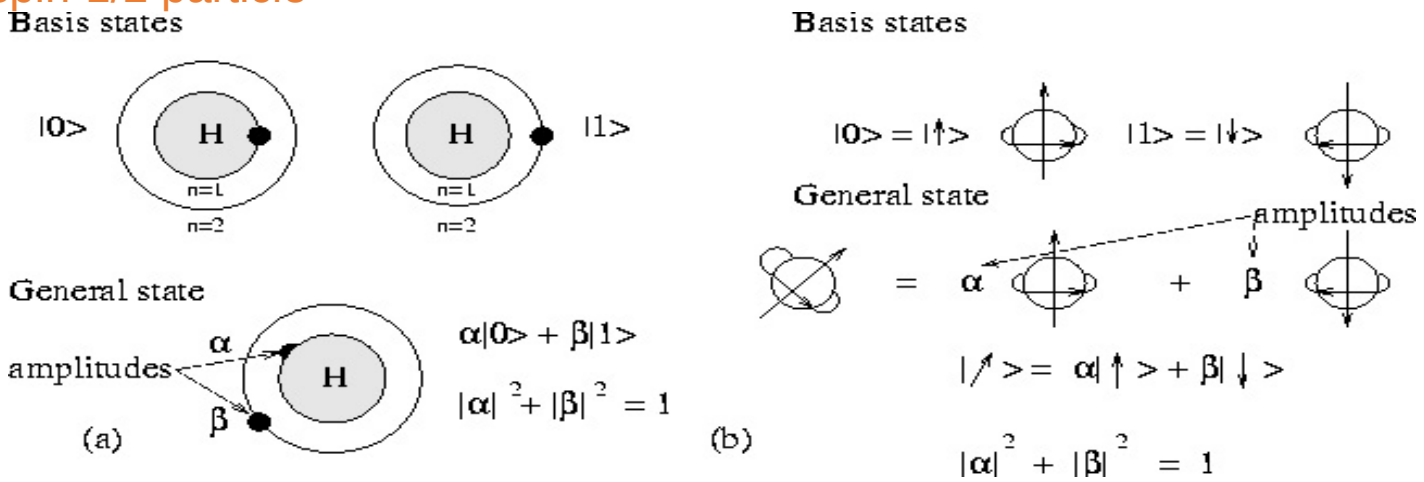
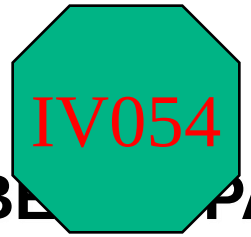


Figure 5: Qubit representations by energy levels of an electron in a hydrogen atom and by a spin-1/2 particle. The condition $|\alpha|^2 + |\beta|^2 = 1$ is a legal one if $|\alpha|^2$ and $|\beta|^2$ are to be the probabilities of being in one of two basis states (of electrons or photons).



HILBERT SPACE H_2

- STANDARD BASIS — DUAL BASIS
- $|0\rangle, |1\rangle$ — $|0'\rangle, |1'\rangle$

$$|0\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \quad |1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$$

$$|0'\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}, \quad |1'\rangle = \begin{pmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{pmatrix}$$

- Hadamard matrix

$$H = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$$

- $H\,|0\rangle = |0'\rangle$ — $H\,|0'\rangle = |0\rangle$
- $H\,|1\rangle = |1'\rangle$ — $H\,|1'\rangle = |1\rangle$

- transforms one of the basis into another one.

$$U = e^{i\gamma}\begin{pmatrix}e^{i\alpha} & 0\\ 0 & e^{-i\alpha}\end{pmatrix}\begin{pmatrix}\cos\theta & i\sin\theta\\ i\sin\theta & \cos\theta\end{pmatrix}\begin{pmatrix}e^{i\beta} & 0\\ 0 & e^{-i\beta}\end{pmatrix}$$

- General form of a unitary matrix of degree 2

IV054

QUAN MEASUREMENT

•of a qubit state

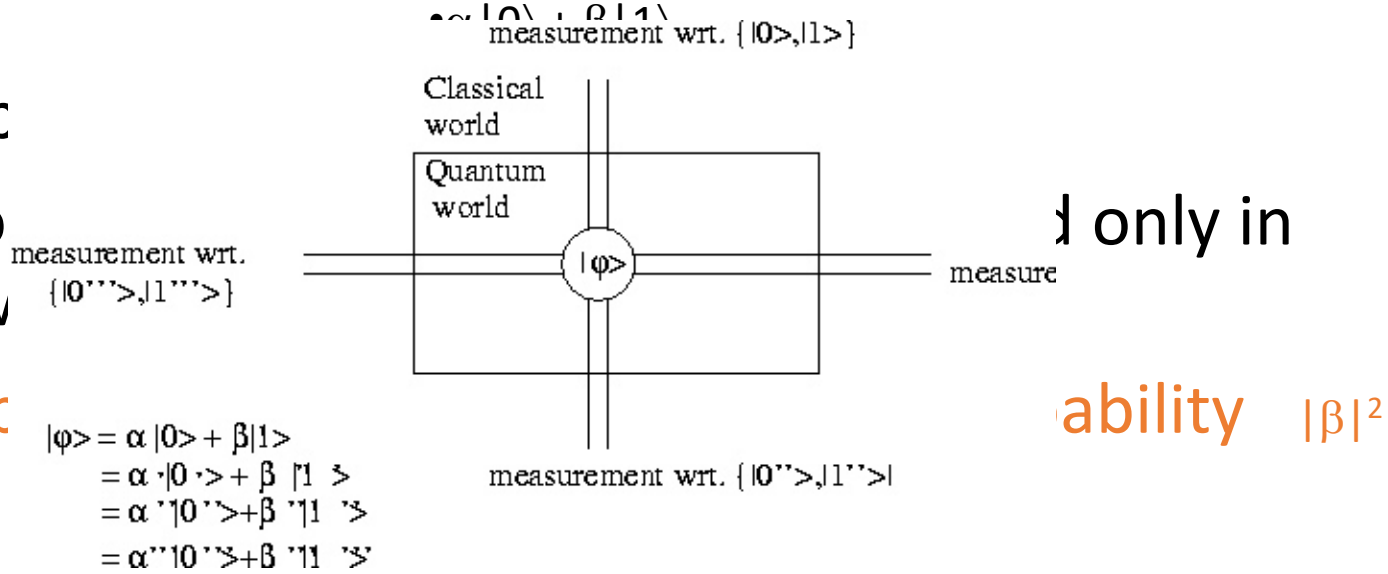
•A qubit state can "contain" unboundly large amount of classical information. However, **an unknown quantum state cannot be identified**.

•By a **measurement** of the qubit state

•with resp

•we can o only in the follow

•0 with p ability $|\beta|^2$



MIXED STATES – DENSITY MATRICES

•A probability distribution $\{(p_i, |\phi_i\rangle)\}_{i=1}^{k}$ on pure states is called a mixed state to which it is assigned a density operator

$$\rho = \sum_{i=1}^{n} p_i \, |\phi_i\rangle\langle\phi_i| .$$

•One interpretation of a mixed state $\{(p_i, |\phi_i\rangle)\}_{i=1}^{k}$ is that a source X produces the state $|\phi_i\rangle$ with probability p_i.

Any matrix representing a density operator is called density matrix.

To two different mixed states can correspond the same density matrix.

Two mixes states with the same density matrix are physically undistinguishable.

MAXIMALLY MIXED STATES

- To the maximally mixed state

$$(\frac{1}{2},|0\rangle),(\frac{1}{2},|1\rangle)$$

- Which represents a random bit corresponds the density matrix

$$\frac{1}{2}\begin{pmatrix}1\\0\end{pmatrix}(1,0)+\frac{1}{2}\begin{pmatrix}0\\1\end{pmatrix}(0,1)=\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}=\frac{1}{2}I_2$$

QUANTUM ONE-TIME PAD CRYPTOSYSTEM

- CLASSICAL ONE-TIME PAD cryptosystem
- plaintext: an *n*-bit string c
- shared key: an *n*-bit string c
- cryptotext: an *n*-bit string c
- encoding: $c = p \oplus k$
- decoding: $p = c \oplus k$

QUANTUM ONE-TIME PAD cryptosystem

plaintext: an *n*-qubit string $|p\rangle = |p_1\rangle \ldots |p_n\rangle$

shared key: two *n*-bit strings k,k'

cryptotext: an *n*-qubit string $|c\rangle = |c_1\rangle \ldots |c_n\rangle$

encoding: $|c_i\rangle = \sigma_x^{k_i} \sigma_z^{k_i'} |p_i\rangle$

decoding: $|p_i\rangle = \sigma_x^{k_i} \sigma_z^{k_i'} |c_i\rangle$

where $|p_i\rangle = \begin{pmatrix} a_i \\ b_i \end{pmatrix}$ and $|c_i\rangle = \begin{pmatrix} d_i \\ e_i \end{pmatrix}$ are qubits and $\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ with $\sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ are Pauli matrices

UNCONDITIONAL SECURITY of QUANTUM ONE-TIME PAD

•In the case of encryption of a qubit

$$|\phi\rangle = \alpha|0\rangle + \beta|1\rangle$$

•by QUANTUM ONE-TIME PAD cryptosystem, what is being transmitted is the mixed state

$$(\frac{1}{4}, |\phi\rangle), (\frac{1}{4}, \sigma_x|\phi\rangle), (\frac{1}{4}, \sigma_z|\phi\rangle), (\frac{1}{4}, \sigma_x\sigma_z|\phi\rangle)$$

•whose density matrix is

$$\frac{1}{2} I_2.$$

This density matrix is identical to the density matrix corresponding to that of a random bit, that is to the mixed state

$$(\frac{1}{2}, |0\rangle), (\frac{1}{2}, |1\rangle)$$

SHANNON's THEOREMS

- Shannon classical encryption theorem says that *n* bits are necessary and sufficient to encrypt securely *n* bits.

- Quantum version of Shannon encryption theorem says that *2n* classical bits are necessary and sufficient to encrypt securely *n* qubits.

COMPOSED QUANTUM SYSTEMS (1)

- Tensor product of vectors

$$(x_1,\ldots,x_n)\otimes(y_1,\ldots,y_m)=(x_1y_1,\ldots,x_1y_m,x_2y_1,\ldots,x_2y_m,\ldots,x_ny_1,\ldots,x_ny_m)$$

- Tensor product of matrices

$$A\otimes B=\begin{pmatrix} a_{11}B & \ldots & a_{1n}B \\ \vdots & & \vdots \\ a_{n1}B & \ldots & a_{nn}B \end{pmatrix}$$

- where $A=\begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$

Example

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\otimes\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}=\begin{pmatrix} a_{11} & a_{12} & 0 & 0 \\ a_{21} & a_{22} & 0 & 0 \\ 0 & 0 & a_{11} & a_{12} \\ 0 & 0 & a_{21} & a_{22} \end{pmatrix}$$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}\otimes\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} a_{11} & 0 & a_{12} & 0 \\ 0 & a_{11} & 0 & a_{12} \\ a_{21} & 0 & a_{22} & 0 \\ 0 & a_{21} & 0 & a_{22} \end{pmatrix}$$

COMPOSED QUANTUM SYSTEMS (2)

- Tensor product of Hilbert spaces $H_1 \otimes H_2$ is the complex vector space spanned by tensor products of vectors from H_1 and H_2. That corresponds to the quantum system composed of the quantum systems corresponding to Hilbert spaces H_1 and H_2.

- A state of a compound classical (quantum) system can be (cannot be) always composed from the states of the subsystem.

QUANTUM REGISTERS

- A general state of a 2-qubit register is:

$$|\phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- where

$$|\alpha_{00}\rangle^2 + |\alpha_{01}\rangle^2 + |\alpha_{10}\rangle^2 + |\alpha_{11}\rangle^2 = 1$$

- and $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ are vectors of the "standard" basis of H_4, i.e.

$$|00\rangle = \begin{pmatrix}1\\0\\0\\0\end{pmatrix} \quad |01\rangle = \begin{pmatrix}0\\1\\0\\0\end{pmatrix} \quad |10\rangle = \begin{pmatrix}0\\0\\1\\0\end{pmatrix} \quad |11\rangle = \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$$

- An important unitary matrix of degree 4, to transform states of 2-qubit registers:

$$CNOT = XOR = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$$

- It holds:

$$CNOT : |x, y\rangle \Rightarrow |x, x \oplus y\rangle$$

QUAN MEASUREMENT

•**of the states of 2-qubit registers**

•$|\phi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$

•**1.** Measurement with respect to the basis $\{ |00\rangle, |01\rangle, |10\rangle, |11\rangle \}$

• RESULTS:

- $|00\rangle$ and 00 with probability $|\alpha_{00}|^2$
- $|01\rangle$ and 01 with probability $|\alpha_{01}|^2$
- $|10\rangle$ and 10 with probability $|\alpha_{10}|^2$
- $|11\rangle$ and 11 with probability $|\alpha_{11}|^2$

2. Measurement of particular qubits:

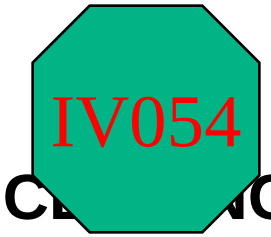
By measuring the first qubit we get

0 with probability $|\alpha_{00}|^2 + |\alpha_{01}|^2$

and $|\phi\rangle$ is reduced to the vector $\dfrac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

1 with probability $|\alpha_{10}|^2 + |\alpha_{11}|^2$

and $|\phi\rangle$ is reduced to the vector $\dfrac{\alpha_{10}|10\rangle + \alpha_{11}|11\rangle}{\sqrt{|\alpha_{10}|^2 + |\alpha_{11}|^2}}$



NO-CLONING THEOREM

- **INFORMAL VERSION:** Unknown quantum state cannot be cloned.

FORMAL VERSION: There is no unitary transformation *U* such that for any qubit state $|\psi\rangle$

$$U\,(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$$

PROOF: Assume *U* exists and for two different states $|\alpha\rangle$ and $|\beta\rangle$

$$U\,(|\alpha\rangle|0\rangle) = |\alpha\rangle|\alpha\rangle \qquad U\,(|\beta\rangle|0\rangle) = |\beta\rangle|\beta\rangle$$

Let

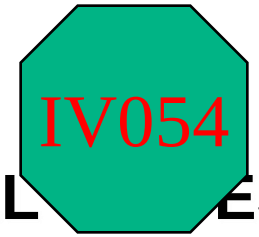
$$|\gamma\rangle = \frac{1}{\sqrt{2}}\left(|\alpha\rangle + |\beta\rangle\right)$$

Then

$$U\left(|\gamma\rangle|0\rangle\right) = \frac{1}{\sqrt{2}}\left(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle\right) \neq |\gamma\rangle|\gamma\rangle = \frac{1}{\sqrt{2}}\left(|\alpha\rangle|\alpha\rangle + |\beta\rangle|\beta\rangle + |\alpha\rangle|\beta\rangle + |\beta\rangle|\alpha\rangle\right)$$

However, CNOT can make copies of basis states $|0\rangle$, $|1\rangle$:

$$CNOT\,(|x\rangle|0\rangle) = |x\rangle|x\rangle$$



BELL STATES

•States

$$\left|\Phi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle + \left|11\right\rangle\right), \qquad \left|\Phi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|00\right\rangle - \left|11\right\rangle\right)$$

$$\left|\Psi^{+}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle + \left|10\right\rangle\right), \qquad \left|\Psi^{-}\right\rangle = \frac{1}{\sqrt{2}}\left(\left|01\right\rangle - \left|10\right\rangle\right)$$

•form an orthogonal (Bell) basis in H_4 and play an important role in quantum computing.

•Theoretically, there is an observable for this basis. However, no one has been able to construct a measuring device for Bell measurement using linear elements only.

QUAN n-qubit REGISTER

•A general state of an n-qubit register has the form:

$$|\phi\rangle = \sum_{i=0}^{2^n-1} \alpha_i |i\rangle = \sum_{i\in\{0,1\}^n} \alpha_i |i\rangle, \quad \text{where} \quad \sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$$

•and $|\phi\rangle$ is a vector in H_{2^n}.

•Operators on n-qubits registers are unitary matrices of degree 2^n.

•Is it difficult to create a state of an n-qubit register?

•In general yes, in some important special cases not. For example if $H_n = \otimes_{i=1}^{n} H$. n-qubit Hadamard transformation

•is used then

$$H_n |0^{(n)}\rangle = \otimes_{i=1}^{n} H|0\rangle = \otimes_{i=1}^{n} |0'\rangle = |0'^{(n)}\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle = \frac{1}{\sqrt{2^n}} \sum_{x\in\{0,1\}^n} |x\rangle$$

•and, in general, for $x \in \{0,1\}^n$

$$H_n |x\rangle = \frac{1}{\sqrt{2^n}} \sum_{y\in\{0,1\}^n} (-1)^{x.y} |y\rangle.^1 \qquad (1)$$

•[1]The dot product is defined as follows: $x \cdot y = \otimes_{i=1}^{n} x_i y_i$.

QUANTUM PARALLELISM

- If
  - $f : \{0, 1,\ldots,2^n -1\} \Rightarrow \{0, 1,\ldots,2^n -1\}$
- then the mapping
  - $f' :(x, 0) \Rightarrow (x, f(x))$
- is one-to-one and therefore there is a unitary transformation U_f such that.

$$|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|0\rangle$$

  - $U_f(|x\rangle|0\rangle) \Rightarrow |x\rangle|f(x)\rangle$
- Let us have the state

$$U_f|\psi\rangle = \frac{1}{\sqrt{2^n}} \sum_{i=0}^{2^n-1} |i\rangle|f(i)\rangle$$

- With a single application of the mapping U_f we then get

- OBSERVE THAT IN A SINGLE COMPUTATIONAL STEP 2^n VALUES OF f ARE COMPUTED!

IV054

IN WH[illegible]ES POWER OF QUANTUM COMPUTING?

•In quantum superposition or in quantum parallelism?

•NOT,

•in QUANTUM ENTANGLEMENT!

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

•be a state of two very distant particles, for example on two planets

•Measurement of one of the particles, with respect to the standard basis, makes the above state to collapse to one of the states

• |00> or |11>.

•This means that subsequent measurement of other particle (on another planet) provides the same result as the measurement of the first particle. This indicate that in quantum world non-local influences, correlations, exist.

POWER of ENTANGLEMENT

- Quantum state $|\Psi\rangle$ of a composed bipartite quantum system $A \otimes B$ is called entangled if it cannot be decomposed into tensor product of the states from A and B.

- Quantum entanglement is an important quantum resource that allows

- To create phenomena that are impossible in the classical world (for example teleportation)
- To create quantum algorithms that are asymptotically more efficient than any classical algorithm known for the same problem.
- To create communication protocols that are asymptotically more efficient than classical communication protocols for the same task
- To create, for two parties, shared secret binary keys
- To increase capacity of quantum channels
-

CLAS[illegible]L versus QUANTUM CRYPTOGRAPHY

- Security of classical cryptography is based on unproven assumptions of computational complexity (and it can be jeopardize by progress in algorithms and/or technology).

- Security of quantum cryptography is based on laws of quantum physics that allow to build systems where undetectable eavesdropping is impossible.

- Since classical cryptography is volnurable to technological improvements it has to be designed in such a way that a secret is secure with respect to future technology, during the whole period in which the secrecy is required.

Quantum key generation, on the other hand, needs to be designed only to be secure against technology available at the moment of key generation.

QUAN KEY GENERATION

•Quantum protocols for using quantum systems to achieve unconditionally secure generation of secret (classical) keys by two parties are one of the main theoretical achievements of quantum information processing and communication research.

•Moreover, experimental systems for implementing such protocols are one of the main achievements of experimental quantum information processing research.

•It is believed and hoped that it will be

•quantum key generation (QKG)

•another term is

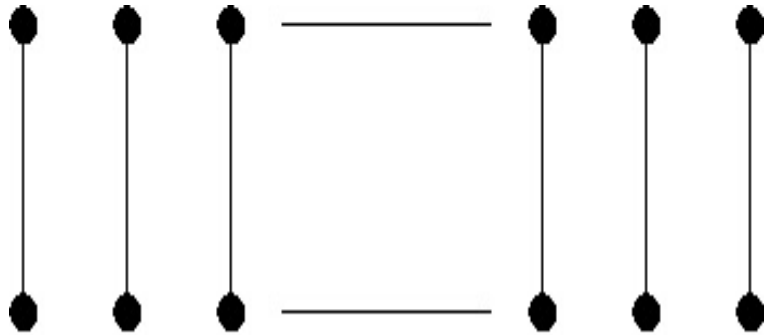
•quantum key distribution (QKD)

•where one can expect the first

•transfer from the experimental to the development stage.

QUANTUM KEY GENERATION - EPR METHOD

•Let Alice and Bob share *n* pairs of particles in the entangled EPR-state. $\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)$.



n pairs of particles in EPR state

• If both of them measure their particles in the standard basis, then they get, as the classical outcome of their measurements the same random, shared and secret binary key of length n.

IV054

POLA[illegible]ION of PHOTONS

•Polarized photons are currently mainly used for experimental quantum key generation.

•Photon, or light quantum, is a particle composing light and other forms of electromagnetic radiation.

•Photons are electromagnetic waves and their electric and magnetic fields are perpendicular to the direction of propagation and also to each other.

•An important property of photons is polarization - it refers to the bias of the electric fiel[illegible] photon.

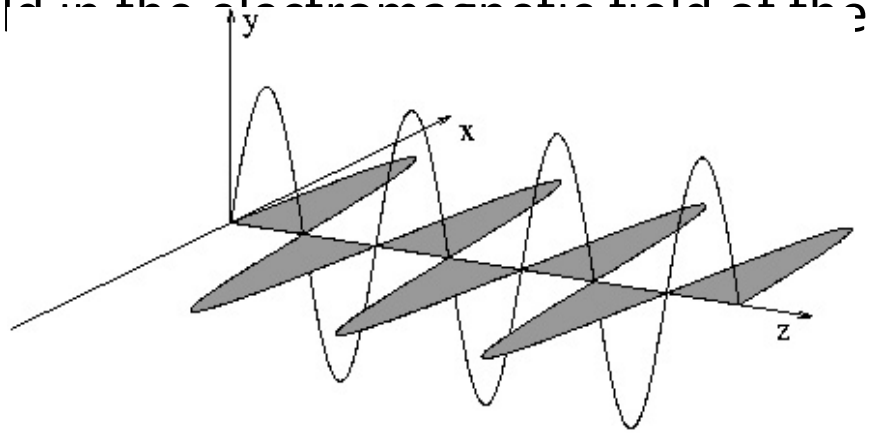
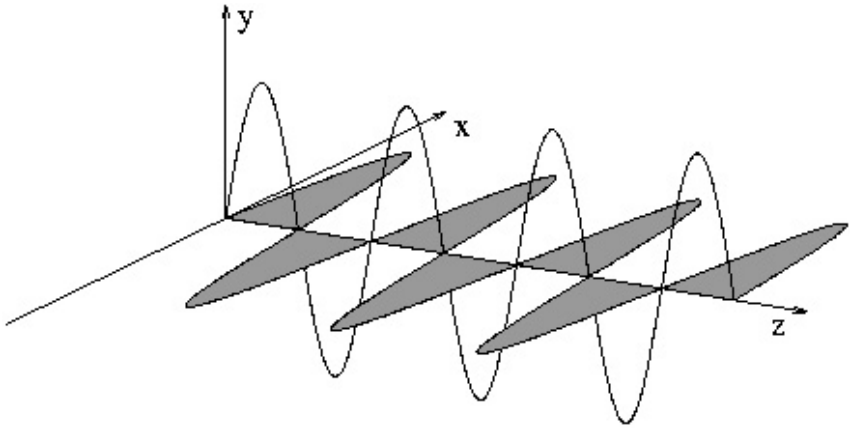


Figure 6: Electric and magnetic fields of a linearly polarized photon

IV054

POLA[illegible]ION of PHOTONS



- Figure 6: Electric and magnetic fields of a linearly polarized photon

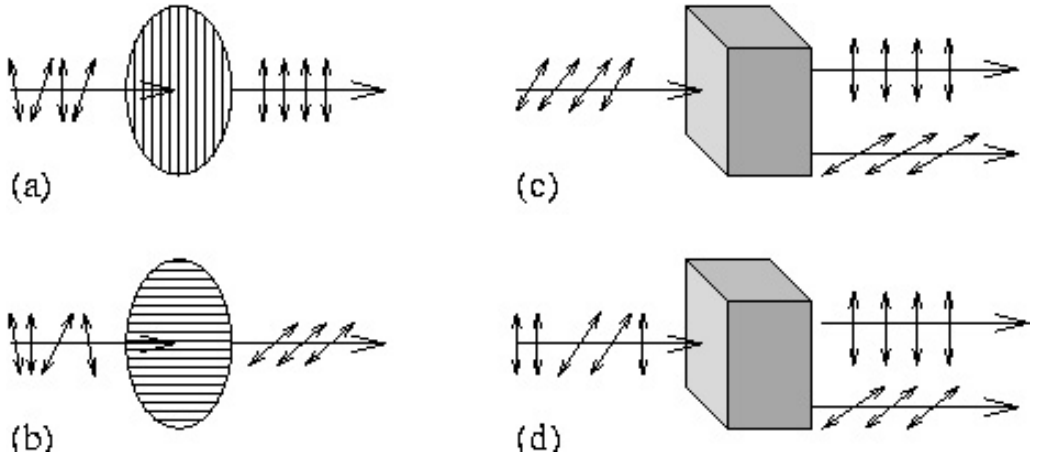
- If the electric field vector is always parallel to a fixed line we have **linear polarization** (see Figure).

IV054

POLA[illegible]ION of PHOTONS

•There is no way to determine exactly polarization of a single photon.

•However, for any angle θ there are θ-**polarizers** – "filters" - that produce θ-polarized photons from an incoming stream of photons and they let θ_1-polarized photons to get through with probability $\cos^2(\theta - \theta_1)$.



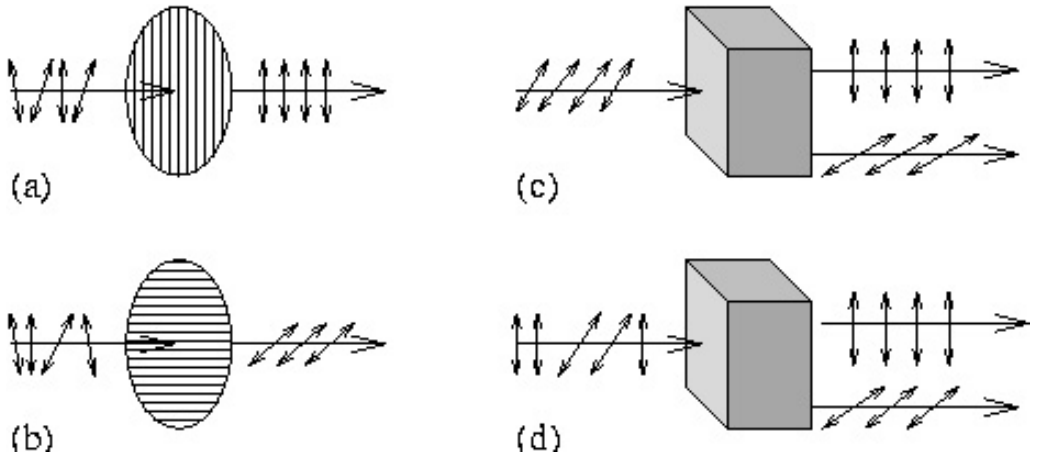
•Figure 6: Photon polarizers and measuring devices-80%

•Photons whose electronic fields oscillate in a plane at either 0^O or 90^O to some reference line are called usually **rectilinearly polarized** and those whose electric field oscillates in a plane at 45^O or 135^O as **diagonally polarized**. Polarizers that produce only vertically or horizontally polarized photons are depicted in Figure 6 a, b.

IV054

POLA[illegible]ION of PHOTONS

•Generation of orthogonally polarized photons.



•Figure 6: Photon polarizers and measuring devices-80%

•For any two orthogonal polarizations there are generators that produce photons of two given orthogonal polarizations. For example, a calcite crystal, properly oriented, can do the job.

•Fig. c - a calcite crystal that makes θ-polarized photons to be horizontally (vertically) polarized with probability $\cos^2\theta$ ($\sin^2\theta$).

•Fig. d - a calcite crystal can be used to separate horizontally and vertically polarized photons.

QUAN KEY GENERATION - PROLOGUE

•Very basic setting Alice tries to send a quantum system to Bob and an eavesdropper tries to learn, or to change, as much as possible, without being detected.

•**Eavesdroppers** have this time especially hard time, because quantum states cannot be copied and cannot be measured without causing, in general, a disturbance.

•Key problem: Alice prepares a quantum system in a specific way, unknown to the eavesdropper, Eve, and sends it to Bob.

•The question is how much **information** can Eve extract of that quantum system and how much it costs in terms of the **disturbance** of the system.

•Three special cases

1. Eve has no information about the state $|\psi\rangle$ Alice sends.
2. Eve knows that $|\psi\rangle$ is one of the states of an orthonormal basis $\{|\phi_i\rangle\}^n_{i=1}$.
3. Eve knows that $|\psi\rangle$ is one of the states $|\phi_1\rangle,\ldots, |\phi_n\rangle$ that **are not** mutually orthonormal and that p_i is the probability that $|\psi\rangle = |\phi_i\rangle$.

TRAN SION ERRORS

•If Alice sends randomly chosen bit

•0 encoded randomly as $|0\rangle$ or $|0'\rangle$

•or

•1 encoded as randomly as $|1\rangle$ or $\$|1'\rangle$

•and Bob measures the encoded bit by choosing randomly the standard or the dual basis, then the probability of error is ¼=2/8

•If Eve measures the encoded bit, sent by Alice, according to the randomly chosen basis, standard or dual, then she can learn the bit sent with the probability 75% .

•If she then sends the state obtained after the measurement to Bob and he measures it with respect to the standard or dual basis, randomly chosen, then the probability of error for his measurement is 3/8 - a 50% increase with respect to the case there was no eavesdropping.

•Indeed the error is $\frac{1}{2}\cdot\frac{1}{4}+\frac{1}{2}\left(\frac{1}{2}\cdot\frac{1}{4}+\frac{1}{2}\cdot\frac{3}{4}\right)=\frac{3}{8}$

IV054

BB84 QUANTUM KEY GENERATION PROTOCOL

•Quantum key generation protocol BB84 (due to Bennett and Brassard), for generation of a key of length *n*, has several phases:

•Preparation phase

Alice is assumed to have four transmitters of photons in one of the following four polarizations 0, 45, 90 and 135 degrees

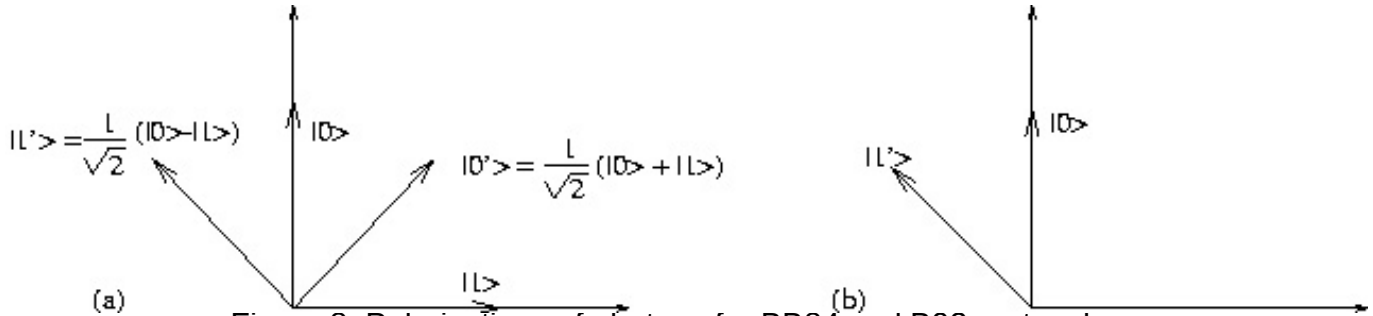


Figure 8: Polarizations of photons for BB84 and B92 protocols

Expressed in a more general form, Alice uses for encoding states from the set {|0⟩, |1⟩,|0'⟩, |1'⟩}.

Bob has a detector that can be set up to distinguish between rectilinear polarizations (0 and 90 degrees) or can be quickly reset to distinguish between diagonal polarizations (45 and 135 degrees).

BB84 QUANTUM KEY GENERATION PROTOCOL

•(In accordance with the laws of quantum physics, there is no detector that could distinguish between unorthogonal polarizations.)

•(In a more formal setting, Bob can measure the incomming photons either in the standard basis $B = \{|0\rangle, |1\rangle\}$ or in the dual basis $D = \{|0'\rangle, |1'\rangle\}$.

•To send a bit 0 (1) of her first random sequence through a quantum channel Alice chooses, on the basis of her second random sequence, one of the encodings $|0\rangle$ or $|0'\rangle$ ($|1\rangle$ or $|1'\rangle$), i.e., in the standard or dual basis,

•Bob chooses, each time on the base of his private random sequence, one of the bases *B* or *D* to measure the photon he is to receive and he records the results of his measurements and keeps them secret.

Alice's encodings	Bob's observables	Alice's state relative to Bob	The result and its probability	Correctness
$0 \rightarrow \|0\rangle$	$0 \rightarrow B$	$\|0\rangle$	0 (prob. 1)	correct
	$1 \rightarrow D$	1/sqrt2 ($\|0'\rangle + \|1'\rangle$)	0/1 (prob. ½)	random
$0 \rightarrow \|0'\rangle$	$0 \rightarrow B$	1/sqrt2 ($\|0\rangle + \|1\rangle$)	0/1 (prob. ½)	random
	$1 \rightarrow D$	$\|0'\rangle$	0 (prob. 1)	correct
$1 \rightarrow \|1\rangle$	$0 \rightarrow B$	$\|1\rangle$	1 (prob. 1)	correct
	$1 \rightarrow D$	1/sqrt2 ($\|0'\rangle - \|1'\rangle$)	0/1 (prob. ½)	random
$1 \rightarrow \|1'\rangle$	$0 \rightarrow B$	1/sqrt2 ($\|0\rangle - \|1\rangle$)	0/1 (prob. ½)	random
	$1 \rightarrow D$	$\|1'\rangle$	1 (prob. 1)	correct

•Figure 9: Quantum cryptography: the BB84 protocol

•Figure 9 shows the possible results of the measurements and their probabilities.

BB84 QUANTUM KEY GENERATION PROTOCOL

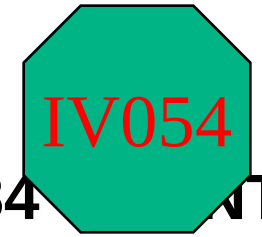
•An example of an encoding - decoding process is in the Figure 10.

•Raw key extraction

•Bob makes public the sequence of bases he used to measure the photons he received - but not the results of the measurements - and Alice tells Bob, through a classical channel, in which cases he has chosen the same basis for measurement as she did for encoding. The corresponding bits then form the basic raw key.

1	0	0	0	1	1	0	0	0	1	1	Alice's random sequence
|1⟩	|0'⟩	|0⟩	|0'⟩	|1⟩	|1'⟩	|0'⟩	|0⟩	|0⟩	|1⟩	|1'⟩	Alice's polarizations
0	1	1	1	0	0	1	0	0	1	0	Bob's random sequence
B	*D*	*D*	*D*	*B*	*B*	*D*	*B*	*B*	*D*	*B*	Bob's observable
1	0	*R*	0	1	*R*	0	0	0	*R*	*R*	outcomes

•Figure 10: Quantum transmissions in the BB84 protocol - *R* stands for the case that the result of the measurement is random.



BB84 QUANTUM KEY GENERATION PROTOCOL

•Test for eavesdropping

•Alice and Bob agree on a sequence of indices of the raw key and make the corresponding bits of their raw keys public.

•**Case 1.** Noiseless channel. If the subsequences chosen by Alice and Bob are not completely identical eavesdropping is detected. Otherwise, the remaining bits are taken as creating the final key.

•**Case 2.** Noisy channel. If the subsequences chosen by Alice and Bob contains more errors than the admitable error of the channel (that has to be determined from channel characteristics), then eavesdropping is assumed. Otherwise, the remaining bits are taken as the next result of the raw key generation process.

Error correction phase

In the case of a noisy channel for transmission it may happen that Alice and Bob have different raw keys after the key generation phase.

A way out is to use qa special error correction techniques and at the end of this stage both Alice and Bob share identical keys.

BB84 QUANTUM KEY GENERATION PROTOCOL

•Privacy amplification phase

•One problem remains. Eve can still have quite a bit of information about the key both Alice and Bob share. Privacy amplification is a tool to deal with such a case.

•Privacy amplification is a method how to select a short and very secret binary string s from a longer but less secret string s'. The main idea is simple. If $|s| = n$, then one picks up n random subsets $S_1,\ldots, S_n$ of bits of s' and let s_i, the i-th bit of S, be the parity of S_i. One way to do it is to take a random binary matrix of size $|s| \times |s'|$ and to perform multiplication Ms'^T, where s'^T is the binary column vector corresponding to s'.

•The point is that even in the case where an eavesdropper knows quite a few bits of s', she will have almost no information about s.

•More exactly, if Eve knows parity bits of k subsets of s', then if a random subset of bits of s' is chosen, then the probability that Eve has any information about its parity bit is less than $2^{-(n-k-1)} / \ln 2$.

EXPE NTAL CRYPTOGRAPHY

- Successes

1. Transmissions using optical fibers to the distance of 120 km.
2. Open air transmissions to the distance 144 km at day time (from one pick of Canary Islands to another).
3. Next goal: earth to satellite transmissions.

All current systems use optical means for quantum state transmissions

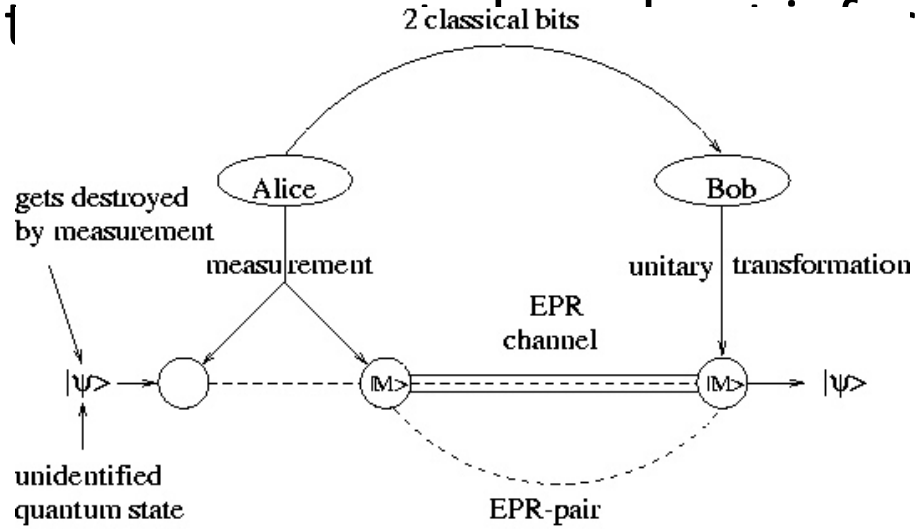
Problems and tasks

1. No single photon sources are available. Weak laser pulses currently used contains in average 0.1 - 0.2 photons.
2. Loss of signals in the fiber. (Current error rates: 0,5 - 4%)
3. To move from the experimental to the developmental stage.

IV054

QUAN TELEPORTATION

- Quantum teleportation allows to transmit unknown quantum information to a very distant place in spite of impossibility t mation to be transmitted.



$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad |EPR-pair\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$$

$$|\psi\rangle|EPR-pair\rangle = \frac{1}{\sqrt{2}}\left(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right)$$

- Total state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \qquad |\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right)$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \qquad |\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle - |10\rangle\right)$$

- Measurement of the first two qubits is done with respect to the "Bell basis":

IV054

QUANTUM TELEPORTATION I

•Total state of three particles:

$$|\psi\rangle|EPR-pair\rangle=\frac{1}{\sqrt{2}}\left(\alpha|000\rangle+\alpha|011\rangle+\beta|100\rangle+\beta|111\rangle\right)$$

•can be expressed as follows:

$$|\psi\rangle|EPR-pair\rangle=|\Phi^{+}\rangle\frac{1}{\sqrt{2}}\left(\alpha|0\rangle+\beta|1\rangle\right)+|\Psi^{+}\rangle\frac{1}{\sqrt{2}}\left(\beta|0\rangle+\alpha|1\rangle\right)$$

•and therefore Bell measurement of the first two particles projects the state of Bob's particle into a "small modification" of the state $|\Psi\rangle=\frac{1}{\sqrt{2}}(\alpha|0\rangle+\beta|1\rangle)$, $|\Psi^{-}\rangle=\frac{1}{\sqrt{2}}(\alpha|0\rangle-\beta|1\rangle)$

•

$|\Psi_1\rangle$ = either $|\Psi\rangle$ or $\sigma_x|\Psi\rangle$ or $\sigma_z|\Psi\rangle$ or $\sigma_x\sigma_z|\psi\rangle$

•The unknown state $|\psi\rangle$ can therefore be obtained from $|\psi_1\rangle$ by applying one of the four operations

•σ_x, σ_y, σ_z, *I*

•and the result of the Bell measurement provides two bits specifying which

•of the above four operations should be applied.

•These four bits Alice needs to send to Bob using a classical channel (by email, for example).

IV054

QUAN TELEPORTATION II

- If the first two particles of the state

$$|\psi\rangle|EPR-pair\rangle=|\Phi^+\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle+\beta|1\rangle)+|\Psi^+\rangle\frac{1}{\sqrt{2}}(\beta|0\rangle+\alpha|1\rangle)$$

$$+|\Phi^-\rangle\frac{1}{\sqrt{2}}(\alpha|0\rangle-\beta|1\rangle)+|\Psi^-\rangle\frac{1}{\sqrt{2}}(-\beta|0\rangle+\alpha|1\rangle)$$

- are measured with respect to the Bell basis then Bob's particle gets into the mixed state

$$\left(\frac{1}{4},\alpha|0\rangle+\beta|1\rangle\right)\oplus\left(\frac{1}{4},\alpha|0\rangle-\beta|1\rangle\right)\oplus\left(\frac{1}{4},\beta|0\rangle+\alpha|1\rangle\right)\oplus\left(\frac{1}{4},\beta|0\rangle-\alpha|1\rangle\right)$$

- to which corresponds the density matrix

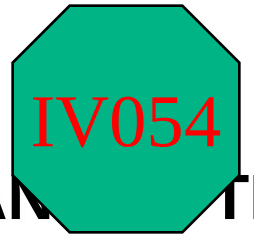
$$\frac{1}{4}\begin{pmatrix}\alpha^*\\ \beta^*\end{pmatrix}(\alpha,\beta)+\frac{1}{4}\begin{pmatrix}\alpha^*\\ -\beta^*\end{pmatrix}(\alpha,-\beta)+\frac{1}{4}\begin{pmatrix}\beta^*\\ \alpha^*\end{pmatrix}(\beta,\alpha)+\frac{1}{4}\begin{pmatrix}\beta^*\\ -\alpha^*\end{pmatrix}(\beta,-\alpha)=\frac{1}{2}I.$$

- The resulting density matrix is identical to the density matrix for the mixed state

$$\left(\frac{1}{2},|0\rangle\right)\oplus\left(\frac{1}{2},|1\rangle\right)$$

- Indeed, the density matrix for the last mixed state has the form

$$\frac{1}{2}\begin{pmatrix}1\\ 0\end{pmatrix}(1,0)+\frac{1}{2}\begin{pmatrix}0\\ 1\end{pmatrix}(0,1)=\frac{1}{2}I.$$



QUAN TELEPORTATION - COMMENTS

- Alice can be seen as dividing information contained in $|\psi\rangle$ into

- quantum information - transmitted through EPR channel
- classical information - transmitted through a classical cahnnel

- In a quantum teleportation an unknown quantum state $|\phi\rangle$ can be disambled into, and later reconstructed from, two classical bit-states and an maximally entangled pure quantum state.

- Using quantum teleportation an unknown quantum state can be *teleported* from one place to another by a sender who does not need to know - for teleportation itself - neither the state to be teleported nor the location of the intended receiver.

- The teleportation procedure can not be used to transmit information faster than light

but

it can be argued that quantum information presented in unknown state is transmitted instanteneously (except two random bits to be transmitted at the speed of light at most).

- EPR channel is irreversibly destroyed during the teleportation process.

DARPA Network

- In Cambridge connecting Harward, Boston Uni, and BBN Technology (10,19 and 29 km).
- Currently 6 nodes, in near future 10 nodes.
- Continuously operating since March 2004
- Three technologies: lasers through optic fibers, entanglement through fiber and free-space QKD (in future two versions of it).
- Implementation of BB84 with authentication, sifting error correction and privacy amplification.
- One 2x2 switch to make sender-receiver connections
- Capability to overcome several limitations of stand-alone QKD systems.

WHY IS QUANTUM INFORMATION PROCESSING SO IMPORTANT

Several areas of science and technology are approaching such points in their development where they badly need expertise with storing, transmision and processing of particles

- Quantum cryptography seems to offer new level of security and be soon feasible.

UNIVERSAL SETS of QUANTUM GATES

•The main task at quantum computation is to express solution of a given problem *P* as a unitary matrix *U* and then to construct a circuit C_U with elementary quantum gates from a universal sets of quantum gates to realize *U*.

$$CNOT = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \sigma_z^{1/4} = \begin{pmatrix} 1 & 0 \\ 0 & e^{\frac{\pi}{4} i} \end{pmatrix}$$

FUNDAMENTAL RESULTS

•The first really satisfactory results, concerning universality of gates, have been due ti Barenco et al. (1995)

•Theorem 0.1 *CNOT gate and all one-qubit gates from a universal set of gates.*

•The proof is in principle a simple modification of the RQ-decomposition from linear algebra. Theorem 0.1 can be easily improved:

•Theorem 0.2 *CNOT gate and elementary rotation gates*

• $$R_\alpha(\theta) = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2}\sigma_\alpha \qquad \alpha \in \{x, y, z\}$$ *for*

•*form a universal set of gates.*

QUANTUM ALGORITHMS

•Quantum algorithms are methods of using quantum circuits and processors to solve algorithmic problems.

•On a more technical level, a design of a quantum algorithm can be seen as a process of an efficient decomposition of a complex unitary transformation into products of elementary unitary operations (or gates), performing simple local changes.

The four main features of quantum mechanics that are exploited in quantum computation:

- Superposition;
- Interference;
- Entanglement;
- Measurement.

EXAMPLES of QUANTUM ALGORITHMS

$\rightarrow$

- Deutsch problem: Given is a black-box function f: {0,1} {0,1}, how many queries are needed to find out whether f is constant or balanced:
- Classically: 2
- Quantumly: 1

- Deutsch-Jozsa Problem: Given is a black-box function $f : \{0,1\}^n \rightarrow \{0,1\}$ and a promise that f is either constant or balanced, how many querries are needed to find out whether f is constant or balanced.
-
- Classically: n
- Quantumly 1

- Factorization of integers: all classical algorithms are exponential.
- Peter Shor developed polynomial time quantum algorithm

- Search of an element in an unordered database of n elements:
- Clasically n queries are needed in the worst case
- Lov Grover showen that quantumly queries are enough

$\sqrt{n}$