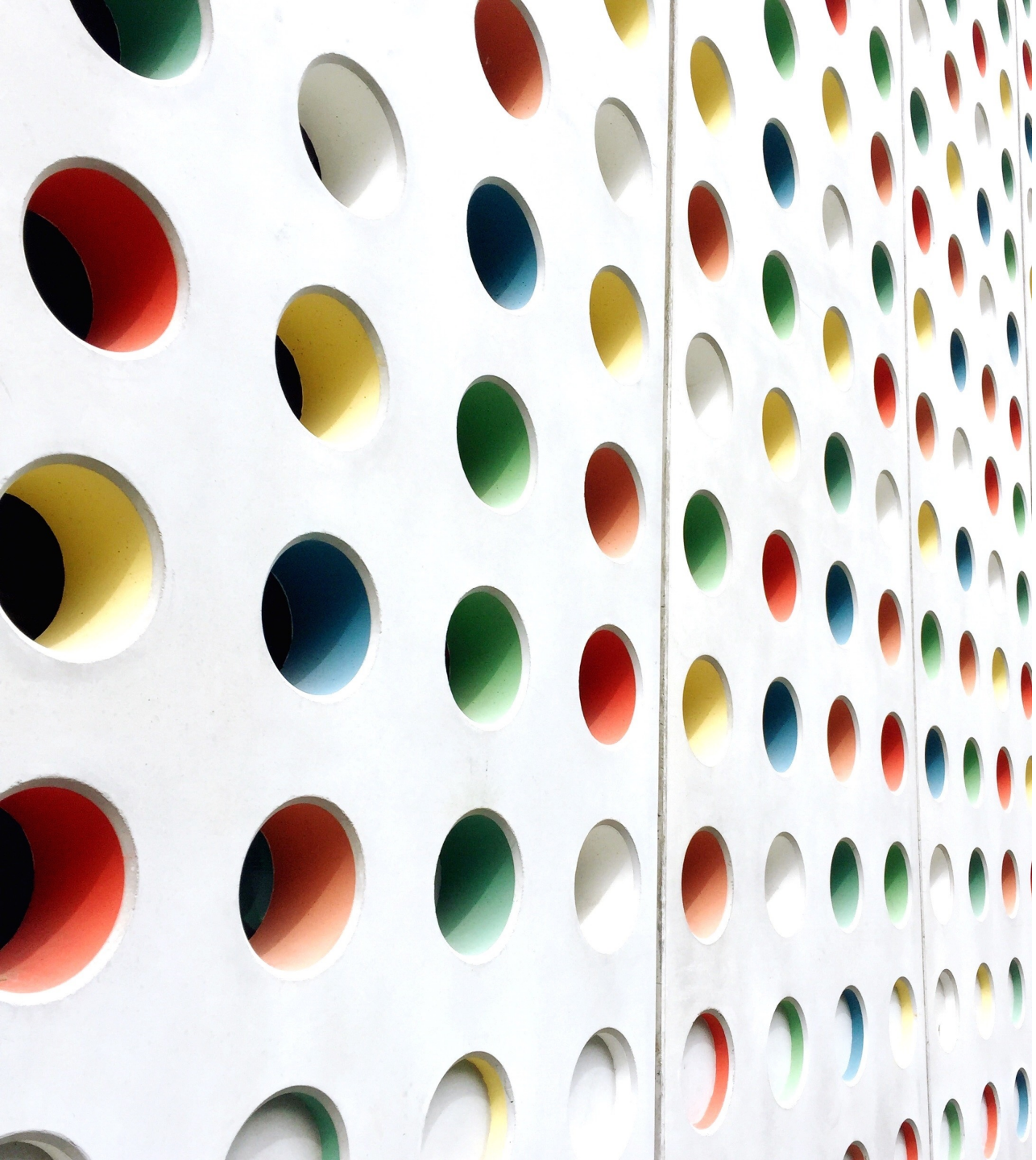
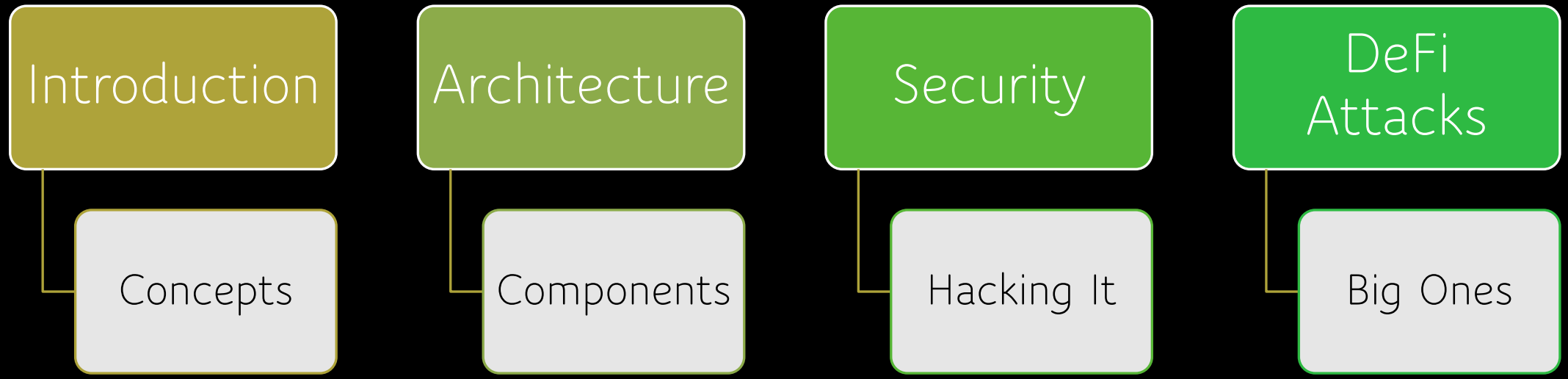


Blockchain and DeFi Attacks

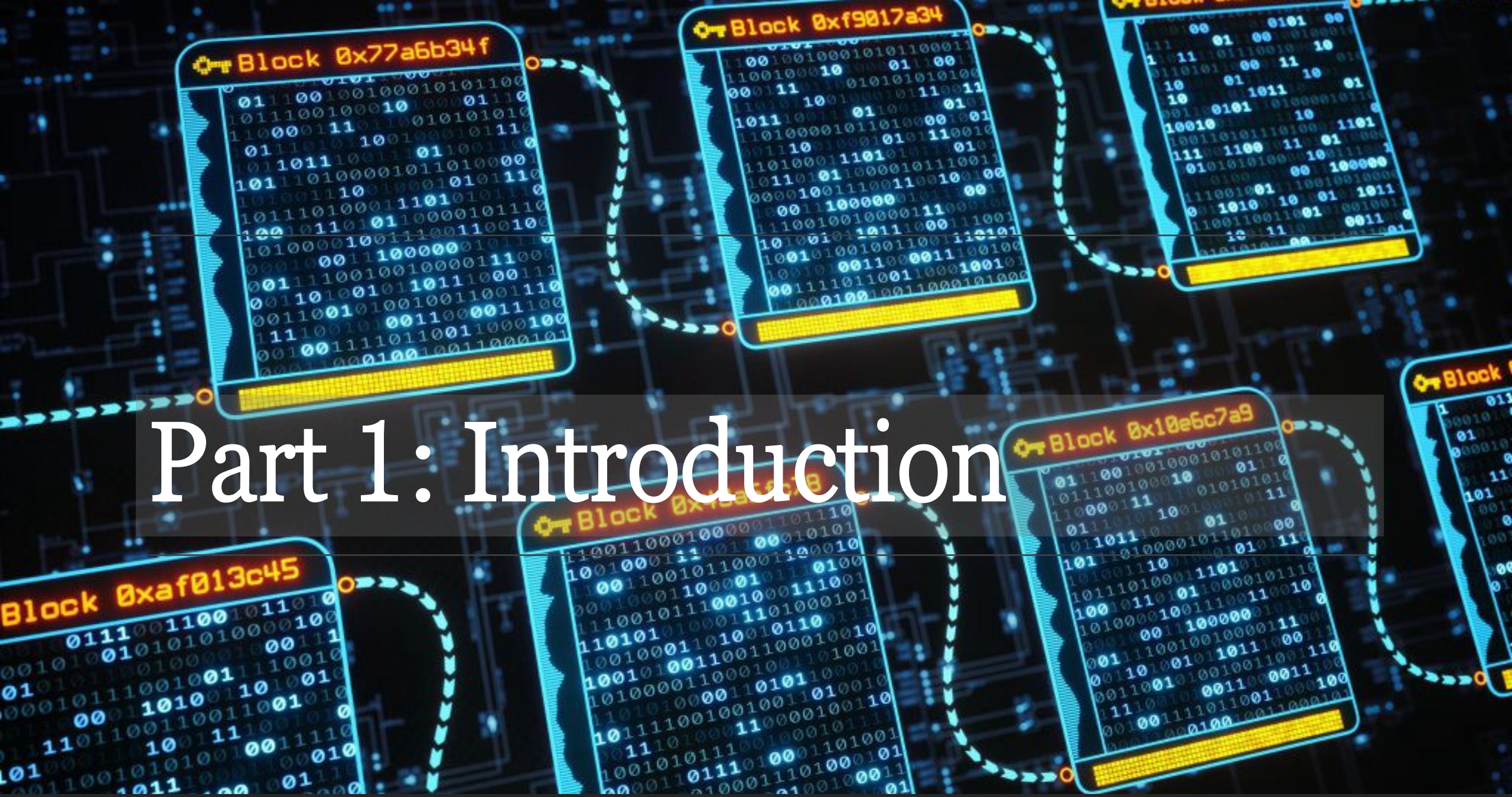
KARIM SULTAN
GAMZIA CORPORATION

Blockchain::Presentation Components



Goals

- To demystify blockchain concepts and related terminology
- To understand why it is secure;
- To understand why it isn't secure



Part 1: Introduction

About::Me

- Entrepreneur in the high tech space
- Part-Time Professor, University of Ottawa (Security, Web Services, and Blockchain)
- MBA, MEBT (e-Business Technology) from University of Ottawa
- PhD Candidate in Digital Transformation and Innovation (DTI) at University of Ottawa, Telfer School of Management
- CPIM (2011), PMP (2011)
- Contact: karimsultan@hotmail.com

Blockchain::Origins

Started with Bitcoin (2009)

Created by Japanese "cypherpunk" Satoshi Nakamoto (pseudonym) (2008)

- Billed himself as a financial anarchist and cryptologist
- Nothing is known about him/her personally
- After launching Bitcoin, he mined some $20 Billion USD worth of bitcoin, which has never been spent.
- In 2010, he handed over development on Bitcoin to a community working group, and then disappeared, never being heard from since
- This has spawned numerous conspiracy theories, from him being the NSA, to him having lost his private keys, to him having been assassinated by the Financial underworld
- Most likely: he was a private man who wanted anonymity, and withdrew from the public
- His wallets hold 1,000,000 XBT. At $22,200 CAD per XBT, that is a net worth of **$22 Billion CAD**

Blockchain::Origins

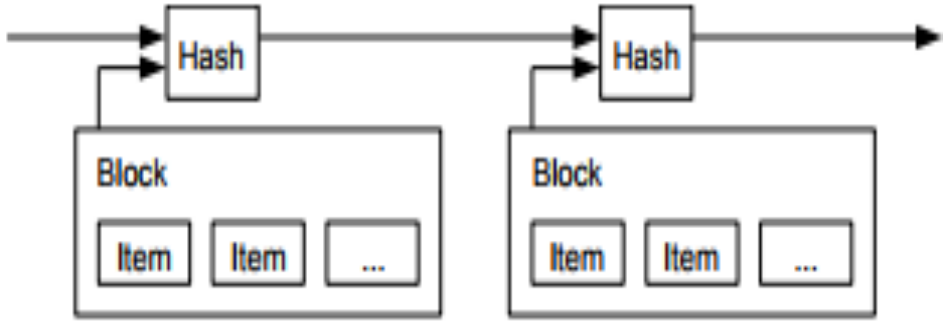
Continued with Ethereum (2015)

Created by Canadian Vitalik Buterin

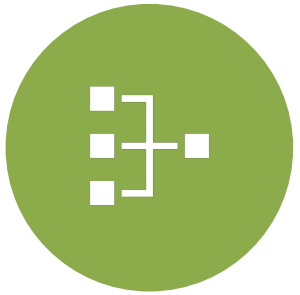
- Started as an “improved bitcoin blockchain”
- Uses the “Ether” cryptocurrency
- Supports user defined tokens
- Added a Virtual Machine (VM) with State Management
- Supports Smart Contracts -> coded logic that is stored on the blockchain and executed in the VM
- The code is permanent, can’t be tampered with, and reflects the terms of the parties that use it
- Ethereum is the next largest cryptocurrency after Bitcoin
- Buterin has remained active on the speaker circuit and as a contributor to new versions

Blockchain::High Level Overview

- Blocks of transactions (data) are linked together using a cryptographic hash
- Each successive block's hash is formed based on the hash from the previous one
- Therefore, if any block is altered / tampered, the successive block hashes will be invalid
- Essentially, a type of shared database



Immutable (permanent and tamper-proof)



Decentralized (networked copies)

Consensus Driven (majority trust)

Transparent (auditable)

Blockchain::Characteristics

Blockchain::Intro

Also known as Distributed Ledger Technology (although 'ledger' is a constraining term)

- Not all Distributed Ledgers are blockchains;
- A square is a rectangle, but a rectangle is not a square
- Blockchain is decentralized, so the "distributed" qualifier isn't accurate for new blockchains
  - From this perspective, **Distributed**=*Shared*; **Decentralized**=*Copied* but we will use interchangeably

Spurs innovation and disintermediation by establishing trust without a Trusted Third Party (TTP)

Can eliminate TTP (middlemen) from the equation (disintermediation)

- Makes workflows more efficient
- Reduces transaction costs
- Eliminates breach points (such as MITM attacks)

All participants can have an identical copy of the ledger (node)

Any change is propagated to all other participants, synchronizing the copies (decentralized)

Any participant can add data to the chain (transaction)

No participant, nor any entity, can stop, alter, or remove a previous transaction (tamper proof)

- Old blocks are not removed, and all transactions are permanent (immutable)

Shutting down one node does not stop the network (geographic resilience)

- As long as a single node is active, the blockchain is active (network autonomy)

All transactions are bundled into blocks, which are validated and chained together using a cryptographic hash function (mining)

- Mining is the process of validating and sealing new blocks of transactions

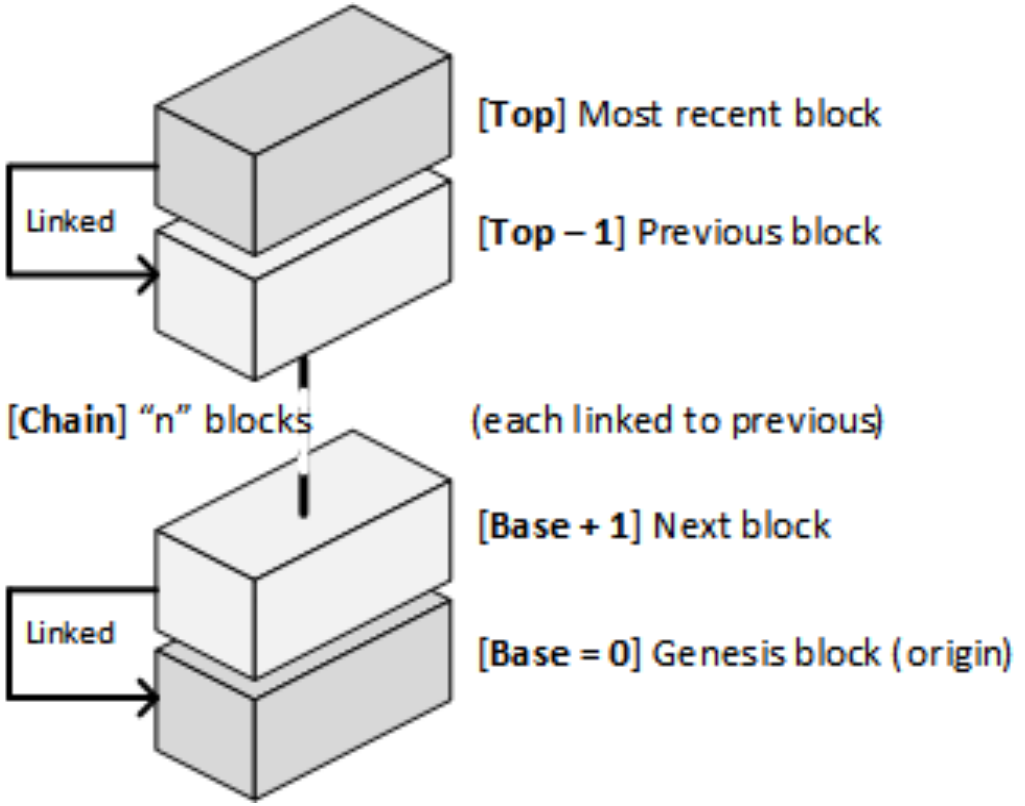
An incentive is used to reward honest participants (minting / coin grant)

Blockchain::Principle ‘Rules’

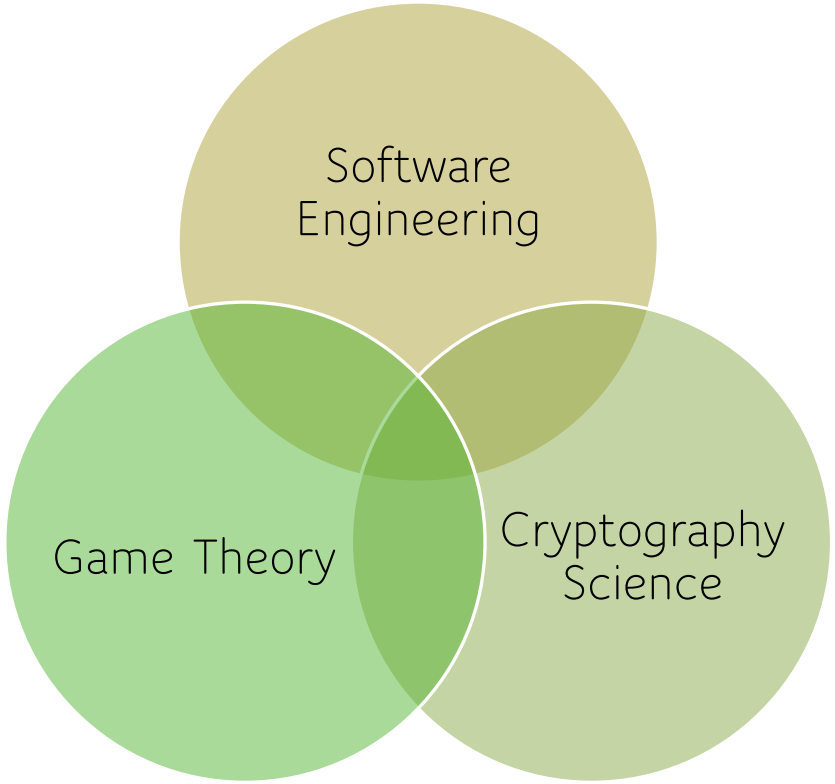
Blockchain::Visualization

THE CHAIN

- Starts at Block 0 (Genesis Block)
- Grows "upwards" (bottom-up)
- So each chain's "height" is their block count
- Like a Jenga tower: Altering a Block near the bottom causes integrity of chain to collapse
- Each block is a collection of transactions



Blockchain::Domains



MULTI-DISCIPLINARY

- Blockchain combines multiple fields in unique ways
- **Software Engineering** provides the P2P agency, APIs and transaction management
- **Cryptography** fundamentals secure it
- **Game Theory** monetizes it and provides incentive to the community to engage; for example, mining rewards and coin appreciation

Blockchain::Definition

"Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones behind it."

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin.Org*, 9.

NOTE that Nakamoto does not call it a blockchain; that would come later, by the community

"a digital ledger in which transactions made in bitcoin or another cryptocurrency are recorded chronologically and publicly."

Oxford Dictionaries. (2018). blockchain | Definition of blockchain in English by Oxford Dictionaries. https://en.oxforddictionaries.com/definition/blockchain

"a decentralized, sequential database containing cryptographically linked blocks of digitally signed asset transactions, governed by a consensus model."

Sultan, K., Ruhi, U., & Lakhani, R. (2018a). Conceptualizing Blockchains: Characteristics & Applications. In *11th IADIS International Conference on Information Systems* (pp. 49-57).

Blockchain::Purpose

Blockchain allows financial transactions *without a central authority*

- It creates trust in a trustless environment

It permits the free flow of capital globally between any parties, unrestricted, without the possibility of government intervention

It has disrupted the Financial / Banking world and spurred the FinTech era

Blockchain makes digital asset transactions possible, trustworthy, transparent, and traceable

Newer blockchains provide a way to execute logic in a trusted, stateful environment

- It is a disruptive technology that enforces *code as law*

It is a massively distributed network that can't be shutdown (can't pull the plug)

It is a secure medium that can't be hacked with current computing resources

It exists in the open

Blockchain Eduction::Threat to Australia

- In October 2018, the federal government's Digital Transformation Agency gave advice to those getting lost in the buzz of blockchain that they should turn their attention elsewhere.
  - The agency's chief digital officer Peter Alexander dunked on its use, saying that "*for every use of blockchain you would consider today, there is a better technology -- alternate databases, secure connections, standardised API engagement*".

- Blockchain Australia considered this determination to be an impediment to the consideration and development of the government and regulator narrative.
  - "Education is lacking, considered and consistent industry consultation has been largely absent notwithstanding recent efforts on the part of regulators to redress these shortcomings," it wrote.

https://www.zdnet.com/article/blockchain-australia-wants-safe-harbour-for-crypto-providers/

Blockchain::Security

- A Blockchain is secure entity
- It can play a role in a security architecture to strengthen network risks
- A Blockchain uses Public Key Infrastructure
  - Thereby sharing PKI's strengths and weaknesses
- There have been no instances of data in a major Blockchain being compromised (tampered)
- We will look closer at security concepts in Part 3 and at specific attacks in Part 4

Blockchain::Bitcoin

- Blockchain can be used as a platform for cryptocurrency
  - This is its “killer app”
- Blockchain serves as a secure digital ledger for Bitcoin.
  - *It is not Bitcoin*
- Blockchain can serve as a secure digital ledger for any cryptocurrency or token
  - Ethereum, Neo, Ripple, LiteCoin, NameCoin, DogeCoin, etc…

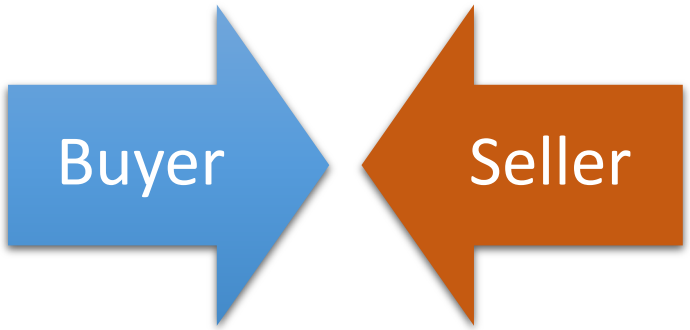
Blockchain::Other Networks

- Bitcoin
- Ethereum
- Ripple
- Neo
- Hyperledger
- EOS
- *Blockchain is a cryptocurrency platform; it can also execute code (smart contracts)*

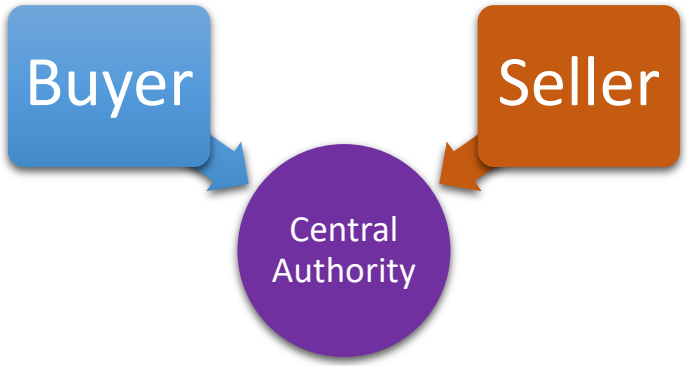
Blockchain::Uses

- Trusted transactions without a central authority (trust)
- Financial transactions of cryptocurrency (fintech)
- Immutable record storage (permanency)
- Creation and use of tokens (tokenomics)
- Non Fungible Transfers of digital assets (NFTs)
- Borderless transfer of wealth (remittances)
- Investment vehicle (portfolio)
- Open record of legacy transactions (auditable, traceable, provenance)

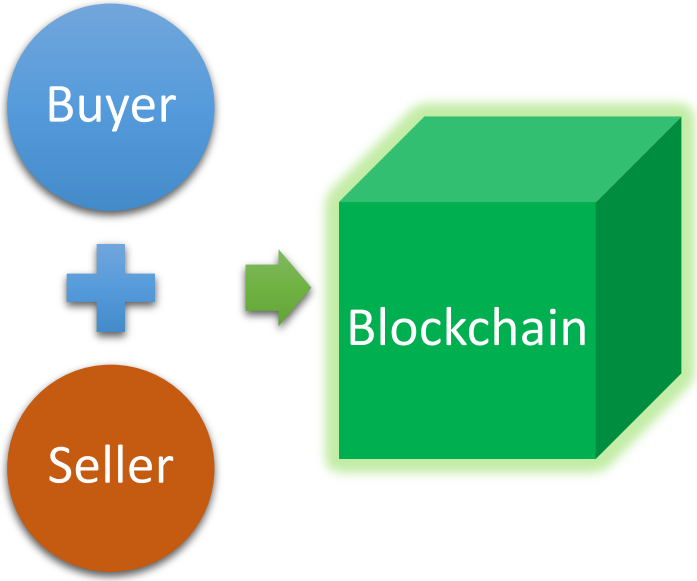
Examples of Trust in E-Commerce



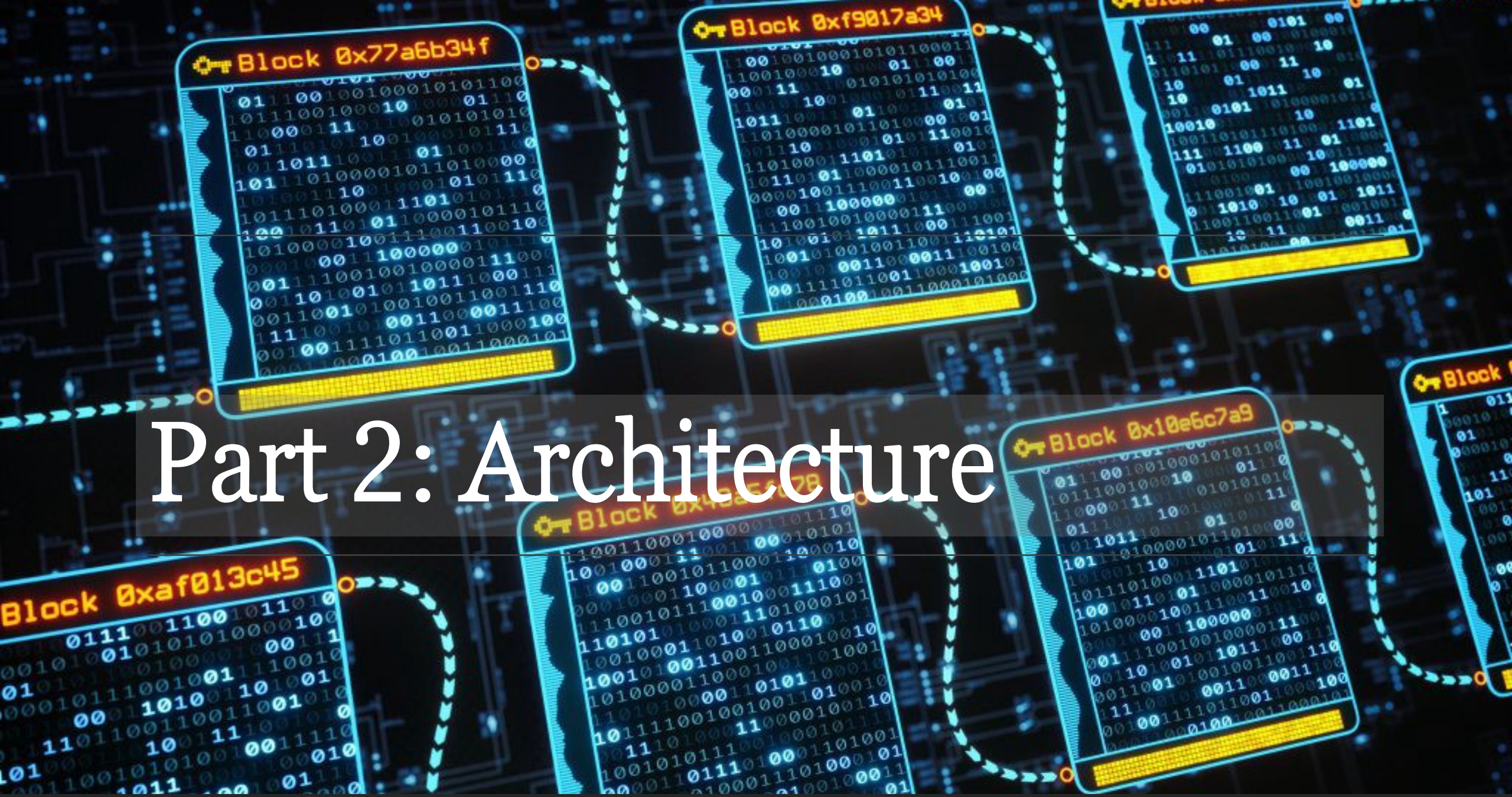
- Buyer knows Seller
- Requires relationship
- Direct transaction
- **Not scalable**



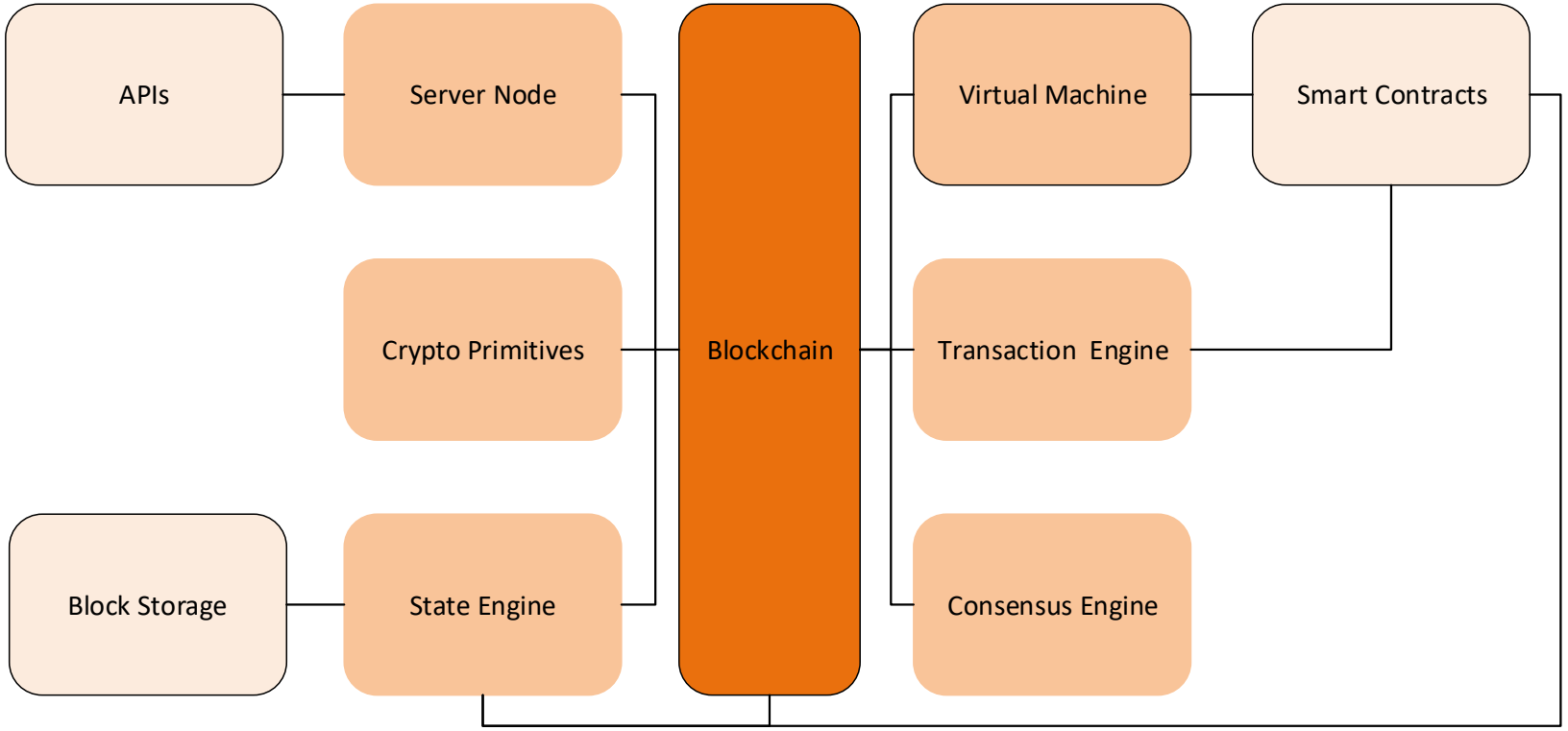
- 3rd party vouches for Seller
- Uses Certificate Authority
- Needs Digital Certificate
- **Open to abuse**



- Transaction done over blockchain
- No intermediary required
- Consensus creates “Trustless Env”
- **No remediation…**



Part 2: Architecture



Blockchain::Architecture

Framework::X.800 Security Categories

Confidentiality

- Encryption, AES, RSA

Integrity

- Hash algorithms, SHA256, SHA-2, MD5, RIPE160

Non-Repudiation

- Digital Signatures

Authentication

- Digital Certificates, TTP

Authorization

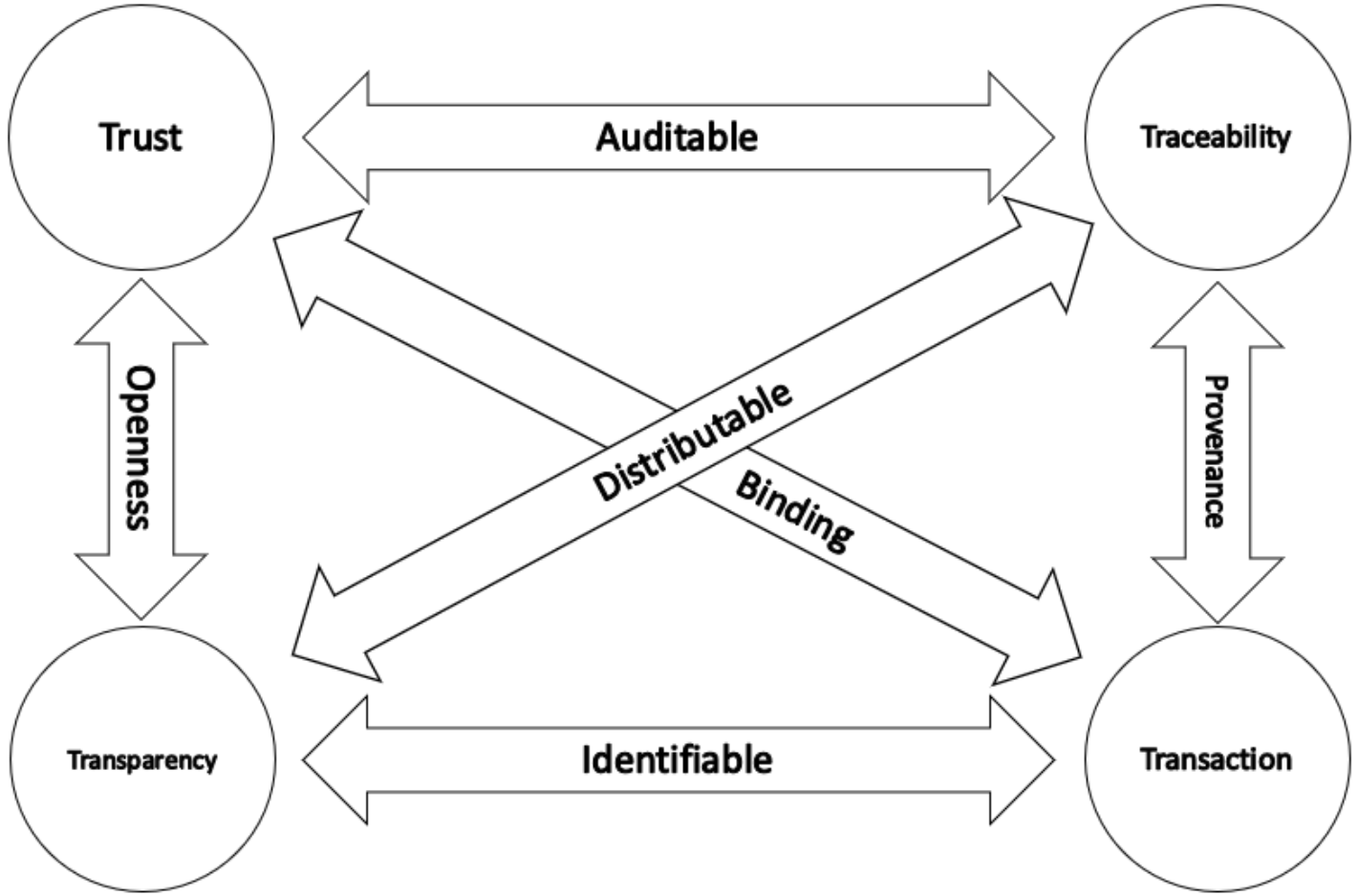
- ACS, RBAC, Passwords, SSH Keys

Availability

- P2P, API, Replication

Framework::4-T Model

*Source: Unpublished Paper: *Karim Sultan & Umar Ruhi. The 4-T Model for Blockchain. Unpublished. Ottawa, 2021.*



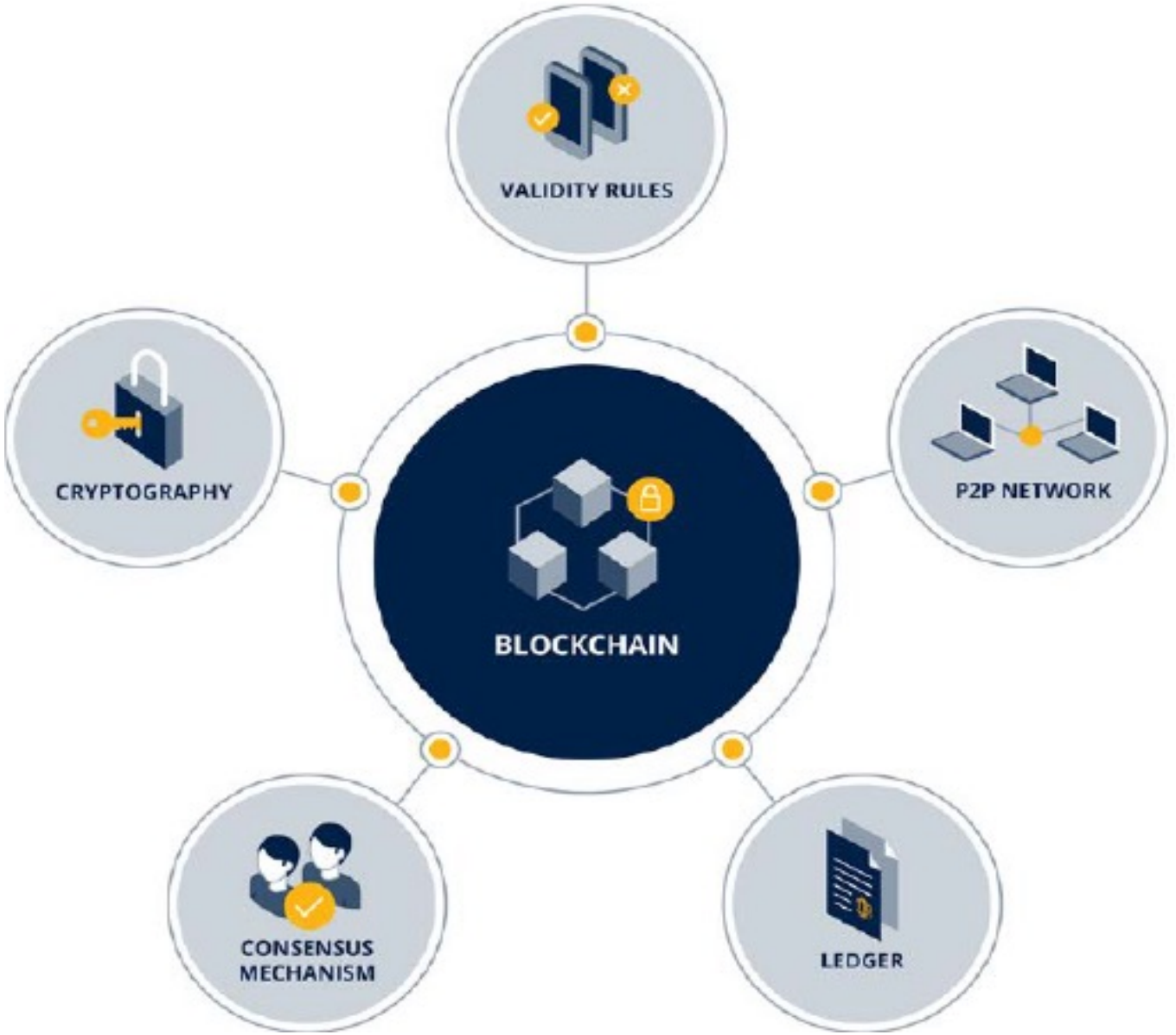
Blockchain::Types

Table 1: The main types of blockchains segmented by permission model. (Source: Hileman & Rauchs, 2017:20)

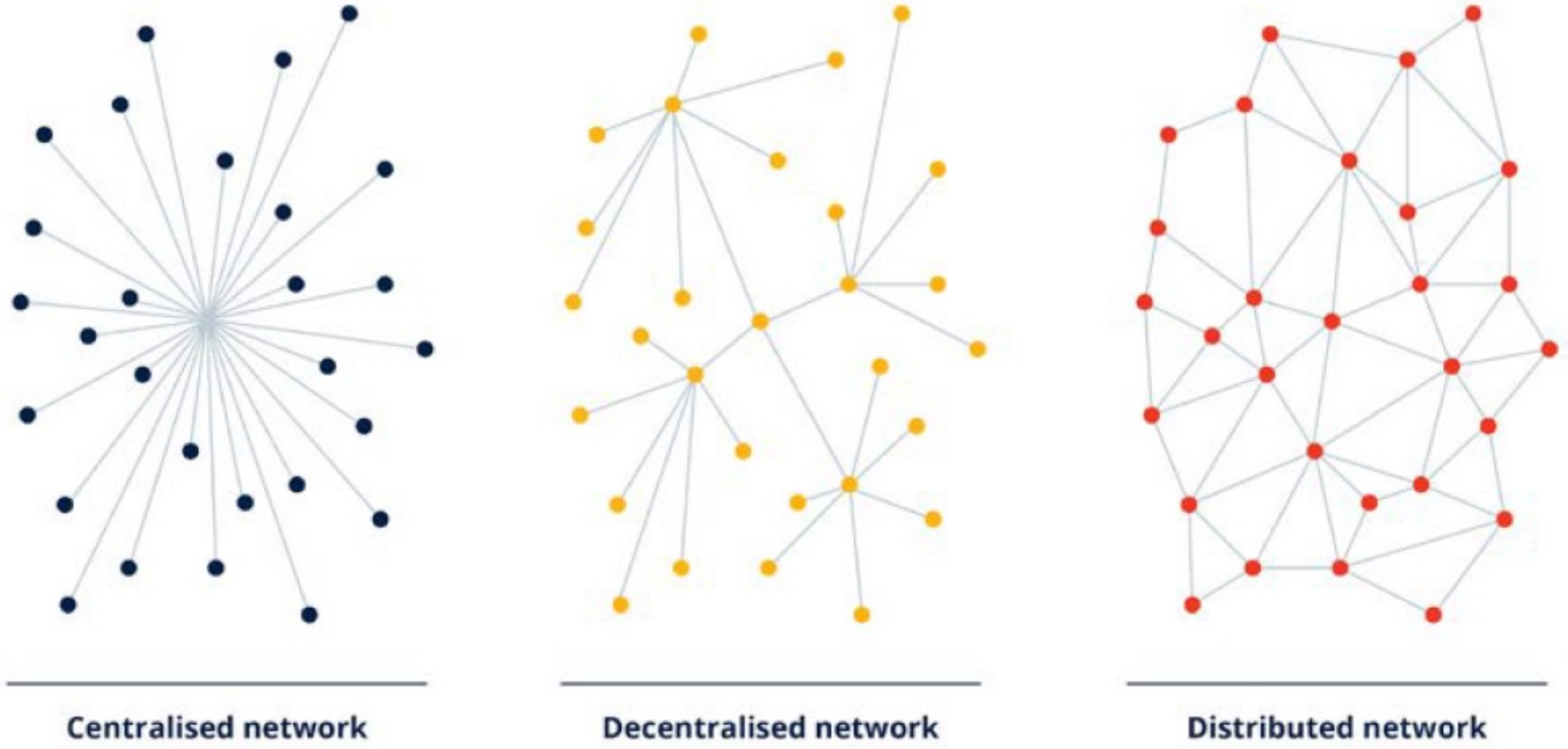
			Read	Write	Commit	Example
Blockchain types	Open	*Public permissionless*	Open to anyone	Anyone	Anyone	Bitcoin, Ethereum
		Public permissioned	Open to anyone	Authorised participants	All or subset of authorised participants	Sovrin
	Closed	*Consortium*	Restricted to an authorised set of participants	Authorised participants	All or subset of authorised participants	Multiple banks operating a shared ledger
		Private permissioned ("enterprise")	Fully private or restricted to a limited set of authorised nodes	Network operator only	Network operator only	Internal bank ledger shared between parent company and subsidiaries

Oxford University. (2018). The Oxford Blockchain Strategy Framework. *Blockchain Programme*

Blockchain::Elements



Hileman, G & Rauchs, M. 2017. *Global Blockchain Benchmarking Study*



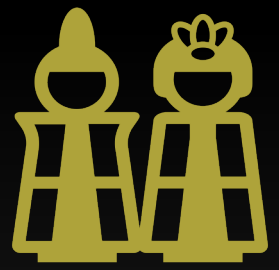
Baran, P. 1964. On distributed communications networks. *IEEE Transactions on communications systems.*

Blockchain::Decentralization

Blockchain::Consensus

- With so many participants providing blocks, which block does everyone agree on?
- Miners will take the block and verify it, then return it to the chain. How do nodes decide which block to accept?
- Two rules:
  - Consensus -> proof that the block was verified
  - Longest Chain -> accepting the chain that most nodes have already accepted (confirmations)

Consensus::Byzantine



Solution to Byzantine Generals' problem

Thought to be **unsolvable** until Satoshi Nakomoto's paper in 2008

Consensus achieved via proof-of-work to establish coherent global state

Algorithm: Proof-of-work

Actors compete to solve computationally hard problems (**investment**)

First actor to present solution is rewarded (**incentive**)

Results are "**chained**" and process continues (**game theory**)

Blockchain::Block Lifecycle

A **Genesis** event creates **Block 0**; the node begins listening for transactions on the P2P network.

Transactions are processed and bundled into a (proposed) **block**. Every 'confirmation interval' the new block is made available to miners.

Miners take the block, validate it, and calculate **hashes** on it, competing to find a hash that meets the difficulty level requirement.

The successful miner receives a financial reward. The block is added to the chain and the process repeats from this new, validated block.

Blockchain::Transaction Lifecycle

The sender selects a recipient address, and using a digital wallet, enters the amount of cryptocurrency to send

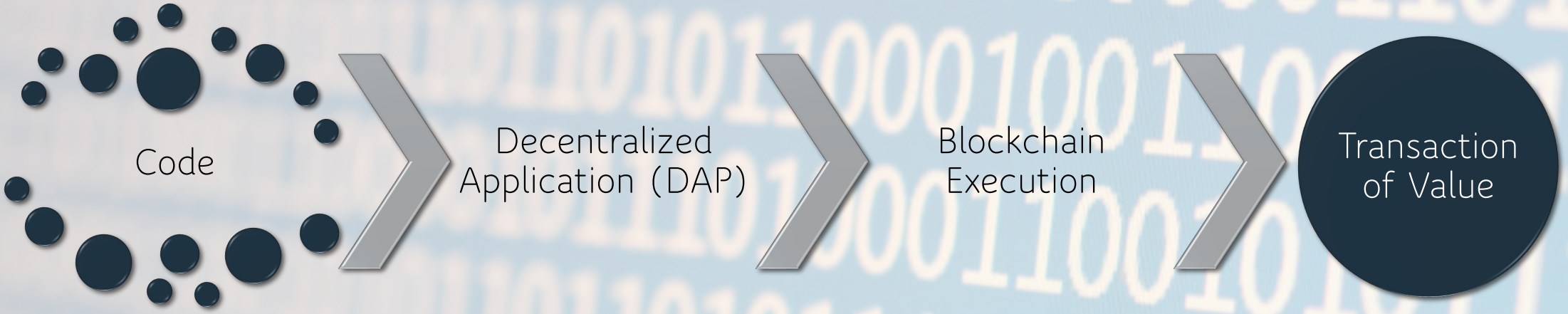
The wallet validates the user has the appropriate balance available, computes a transaction hash and digitally signs it with the sender's private key

Once submitted, the wallet communicates with the blockchain network via P2P and shares the details of the transaction.

The recipient blockchain broadcasts it to the network, perpetuating its distribution.

The recipient blockchain marks the transaction as pending, and places it in the next block.

A set of logical rules committed to a blockchain to govern transactions between actors.



The Future of Trust?

Concept::The "Smart" Contract

Blockchain::Issues

Performance

- Slow transaction rates (up to 20 TPS vs VISA's 2000 TPS)
- Can take time to confirm transaction; not good for retail and e-com

Scaling

- Bloat (can only increase in size, doesn't compact/prune)
- Doesn't distribute computing processes across network
- Node hardware demands exceeding enthusiast budget, capability

Mining

- Huge power requirements used to validate blocks and extend chains, not considered "Green"

Forks

- Issues with forcing updates to the network

Blockchain::Nodes

Who can run a node?

Anybody who can meet the current hardware and bandwidth requirements

Anybody can be a miner if they have the hardware capability

No incentive other than contributing to the network

Bitcoin Blockchain: Full node, 24/7

Ethereum Blockchain: Full node, 24/7

Part 3: Security

Blockchain::X.800 Security Compliance

Security Category	Blockchain Realization
Confidentiality (encryption)	Blockchains do not use encryption; one exception is digital signatures
Integrity	Transaction hashes, block hashes Bitcoin: SHA256; Ethereum: KECCAK-256
Non-repudiation (deniability)	Digital signatures on transactions
Authentication	Digital wallets with PKI / private key
Authorization	'Hybrid' chains are permissioned
Availability	A P2P network with each node holding a blockchain copy

Blockchain::Crypto-Primitives

- Blockchain uses several crypto-primitives (core cryptography building blocks) for security.

Crypto-Primitive	X.800 Category	Blockchain Usage
Hash	Integrity	Transactions, Blocks, Mining
Digital Signature	Non-Repudiation	Transactions, Smart Contracts
Public/Private Keys (PKI)	Authentication	Blockchain Address, Contract Address
Merkel Tree	Integrity	Transactions
Encryption	Confidentiality	NONE -> Not Used

Cryptography::PKI

PKI is Public Key Infrastructure

- A form of **Authentication**

Requires the use of **Key Pairs**:

- One **private key** which is kept **secret**
- One **public** key which is **shared**

Rules

- A private key **cannot be determined** from a public key, nor vice versa
- Encryption is **asymmetric**: The public key decrypts the private key's cipher text, and vice versa

The common **algorithm** is **RSA**, at the **2048**-bit level or higher, using **large primes**

Cryptographic Hashes

A repeating hash is called a **collision**

Collisions are useless in cryptography, as it means a data input can be easily forged

Cryptographic Hashes have several rules:

- **Deterministic** (always the same result)
- **Improbable to find a collision (repetition** is infeasible)
- A **small change** in the input causes a **significant change** in the output (cascade / avalanche)
- **Cannot be reversed** (one way / trap-door)
- Can be implemented for **fast processing** and computation (often in hardware)

Can be seen as a **digital fingerpint**

Function will map an infinite input space to a bounded, yet probabilistically infinite output space

- For example, SHA256 offers 2^{256} possible outputs which although fixed, are inexhaustible

Is binary and therefore is represented as a series of hex characters

Common Cryptographic Hashes

- MD5
  - Broken, retired; collisions can be found within 10 minutes on modern desktop hardware (128 bits)
- SHA-1
  - NIST: FIPS Pub-180; now considered broken (160 bits)
- RIPE (RIPEMD160)
  - Still used in some older applications (160 bits) – no known exploits
- SHA-2 Family
  - Three algorithms: SHA256, SHA384 and SHA512 (256, 384 and 512 bits respectively)
  - Solid workhorses, no known exploits, fast and secure; used in HTTPS
- SHA-3 Family
  - "Keccak" -> NIST algos; used in Ethereum Blockchain, similar variants as in SHA-2

Blockchain::Digital Signature Review

A **Digital Signature** combines a hash + PKI encryption to bind a document to a party

- The document can not be **repudiated**;
- **Non-Repudiation**: the sender cannot deny message originated from them

To **sign**, data is hashed, and the hash is encrypted using the signer's private key into a tag.

To **validate**, data is hashed, the tag is decrypted with the public key, values are compared.

Recall:

- Only a public key can decrypt a cipher made with a private key;
- Only the sender knows the private key; but everyone knows the public key;
- Therefore, anyone can validate the sender is **legitimate** / not a **forgery**

Attack::Double Spend

Summary

- The attacker attempts to spend the same cryptocoins twice

Execution

- The attacker uses two wallets to initiate valid transactions to two distinct merchants simultaneously, at the same time (same timestamp)

Defense

- As they are both at the same time, each node will randomly select one to be processed first, and reject the second transaction
- Consensus will be reached by using the longest chain
- Only one transaction will be confirmed (over time) and the other will disappear from chain

Attack::51%

Summary

- The attacker writes their own blocks to the chain, violating rules and allowing multi-spend

Execution

- The attacker controls 51% of the mining compute power, or greater, giving them a probable chance of finding the next block before competitor miners, thus allowing them to control the chain

Defense

- Public blockchains offer a cryptocurrency incentive for finding the next block
- This compels people to mine and compete, restricting collusion (game theory)
- RISK: Mining pools

Attack::Data Tampering

Summary

- The attacker changes information in a previous block

Execution

- The attacker, having a copy of the blockchain, changes the binary values in a block to desired values (ie, balance)

Defense

- Every node validates the blocks by calculating the hash for each one, based on the previous blocks hash
- This is a very fast process and immediately finds any discrepancies, invalidating the copy
- To change a block, the attacker must change all successive blocks by recomputing their hashes, a time and resource consuming operation, and then beat out all miners to form the longest chain (infeasible)

Attack::Infinite Loop

Summary

- A smart contract on the blockchain runs forever, infinitely exhausting resources

Execution

- The attacker deploys a smart contract that contains an infinite loop which when run will never stop

Defense

- Newer blockchains have timeouts on execution.
- In Ethereum, the user pays in Gas (a fraction of Ethereum) to execute a smart contract. When the contract 'runs out of gas' execution is halted.

Attack::Denial of Service

Summary

- An excessive number of false transactions overwhelms the machine and it shuts down

Execution

- The attacker launches a large scale distributed network attack on the blockchain

Defense

- Individual machines can be overwhelmed
- The blockchain network will queue and process all transactions
- Infeasible to shutdown all machines in a P2P network.
- Blockchain has no special protection against D/DOS

Attack::Geo Denial / Internet Interruption

Summary

- A large-scale geographical catastrophe or a regional Internet disruption stops blockchain processing

Execution

- The attacker profits from a natural disaster, or government overreach and Internet censure

Defense

- As long as a single node is functioning, the blockchain remains online
- Massive amounts of participating nodes, globally, ensure no geo-centric fail points; only a complete Internet interruption (infeasible) could stop traffic
- Bottom Line: You can't pull the plug. Skynet?

All That Crypto::Hiding in Plain Sight

- I can see everyone's balance on a blockchain. Why can't I steal their cryptocurrency?
  - You would need to know that person's private key
  - Determining the private key from the public key is considered infeasible
  - Most nations do not have any regulatory framework for digital assets – would this even be considered theft?
- Quantum computers
  - Pose a risk to the public/private key system of Blockchains.
  - Still a long ways out
  - Do not pose a risk to the hash system used to secure blocks

Part 4: DeFi Attacks

DeFi::Weaknesses

- Uses blockchain's security to create decentralized financing services/products
- Introduces non-specific functionality to blockchain, via smart contracts
- Smart contracts are immutable – write once, wrong many
- Smart contracts of this nature are complex, and must consider edge cases
- Smart contracts require people
- People are fallible
- + Speculative investment

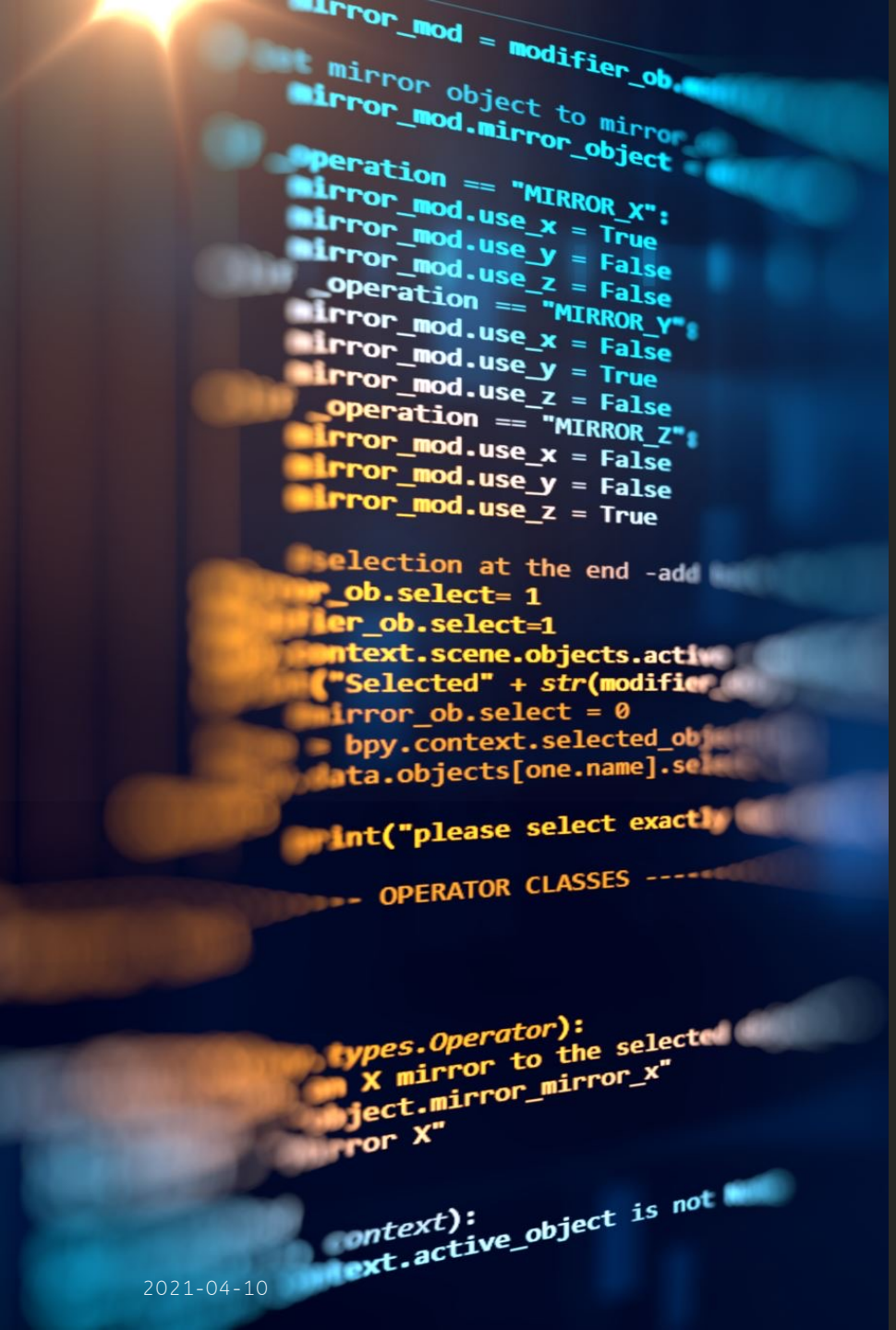
Wormhole::Human Incompetence

- What's wrong with this code? Consider:

```
bool sigVerified = verify_sig(user)
bool guardiansigVerified = verify_sig(guardian)

if (sigVerified == guardiansigVerified)
  performTransaction(transaction)
else
  abortTransaction()
```

- $326 Million USD error



Smart Contracts

- Smart Contracts are hard.
- Have an internal/external audit process.
- Never commit code to the chain until a sign-off process has occurred.
- Test edge cases!
- Hire smart people.
- Blockchain is an unforgiving environment for coding. Get it right once, or wrong forever.

Ronin::Human Sloth

- Ronin was a NFT based game, with progression
- The game was great. The implementation lacked.
- A Sky Maven developer had left in backdoor access to an RPC node, with private keys.
- Attacker could sign validator transactions onto Sky Maven's sidechain, by impersonating Sky Maven and publisher Axie Infinity.
- Loss of $525 million USD occurred.

Sloth

Never rely on backdoors for testing, or breaking into your code

Hackers **will** find it.

Test all paths.

See point #1. Easter Eggs, alright. Backdoors, nope.

FTX::Human Greed

- FTX, second largest crypto-exchange, failed / went bankrupt
- FTX was not following standard accounting practices
- Key figure: Sam Bankman-Fried (SBF) / mistakenly thought to be "Crypto's Saviour"
- Almeda, a seemingly separate company, was also owned by SBF.
- It provided tokens called FTT.
- Binance recognized risk and sold all their tokens, causing a price plunge
- An old fashioned bank-run resulted, with investors trying to get their money back (Nope)
- FTX wiped out $3.7 Billion from XBT, ETH, and other major cryptos; lost billions in their exchange, "misplaced" $370 million dollars, and left 1,000,000 creditors wiped out. Final loss total unknown.

Greed

- Speculative investing is dangerous.
- Blockchain accounts can be watched. Forever, in real time.
- Utility tokens are more desirable for one time use (value doesn't fluctuate).
- Remember, someone is always trying to get rich off a crypto or token. The temptation to cheat is always there.

Conclusion

QUESTIONS?

Contact: karimsultan@hotmail.ca