# Blockchain for Flood Insurance Management

Guidehouse

# Agenda

| TOPIC | KEY POINTS |
|---|---|
| Module 1: **Blockchain Concepts** | • What is distributed ledger technology (DLT), how does DLT compare to (other) peer-to-peer software protocols, how can we link transactions together in a distributed ledger and keep distributed ledgers in sync<br>• Understanding blockchain components, how hashing and consensus algorithms secure blockchains and prevent changes to previously-recorded transactions, transaction immutability, understanding how transaction immutability impacts the anonymity / pseudonymity of a blockchain |
| Module 2: **Distributed Flood Insurance Management** | • Comparison of centralized vs. decentralized models for insurance claims processing, policy monitoring, risk assessments, and compliance monitoring |

# Module 1:
# Blockchain Concepts

Guidehouse

# Blockchain Concepts: Distributed Ledgers

## Distributed ledger

Every participant in the network has simultaneous access to a view of the information

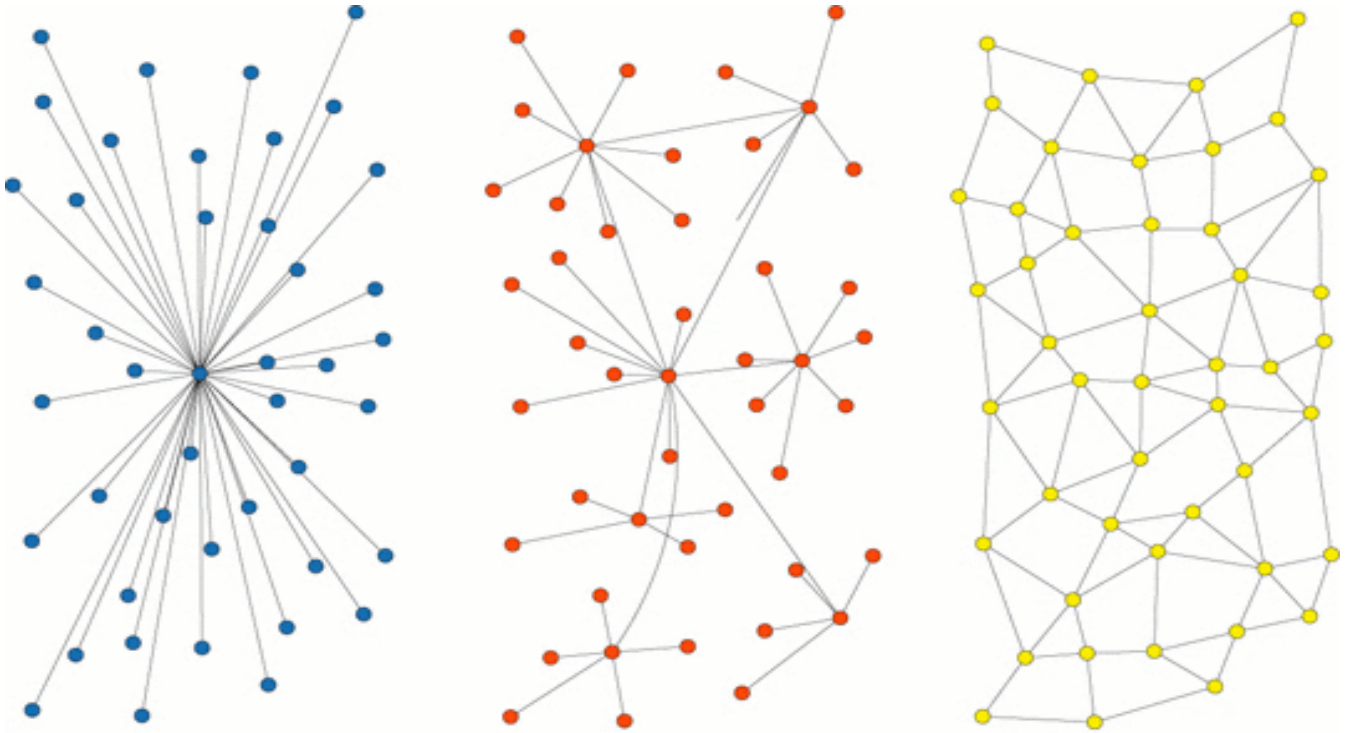
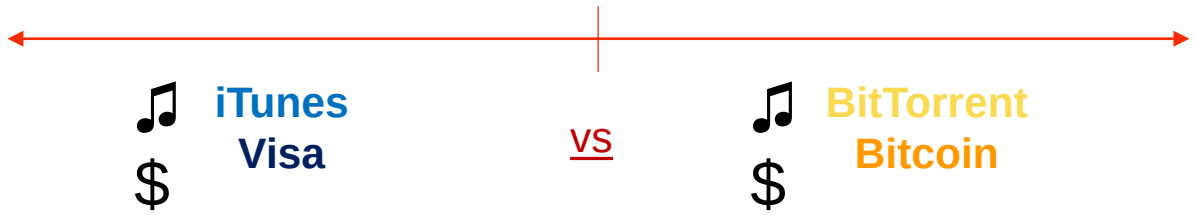
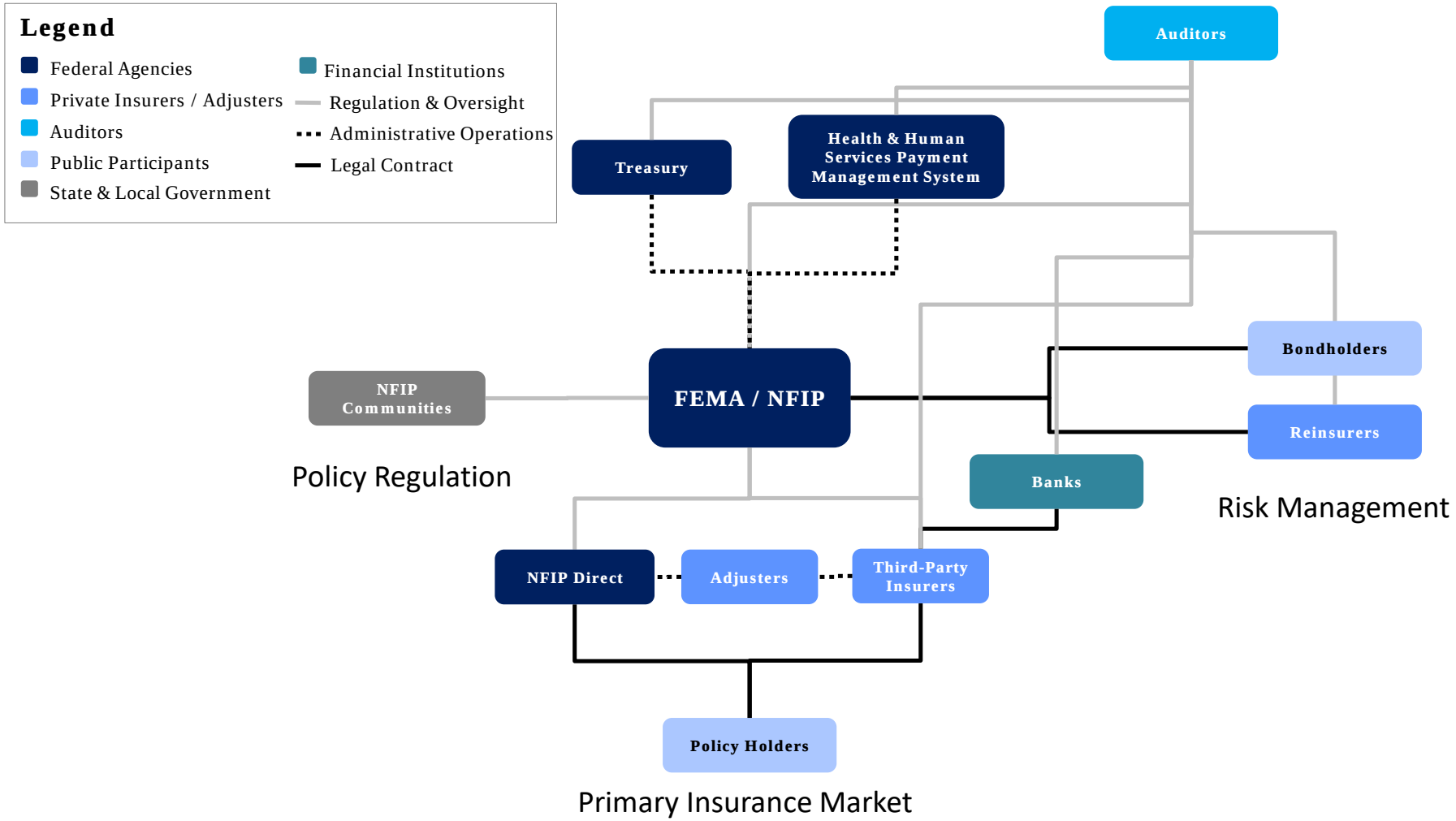



Image source: http://www.wallstreettechnologist.com/2015/06/26/decentralized-what-does-that-really-mean/



# Blockchain: Insurance Management Ecosystem



# Learning Objectives

Understanding:

1. How blockchains can incentivize participation and investment in information infrastructure
2. How to support that participation through consensus algorithms
3. How immutable transactions support network security
4. How smart contracts enable embedded business logic and selective information-sharing
5. How flexible, secure information sharing can decrease insurance management costs and increase operational efficiency

# Blockchain Concepts: Consensus



# Blockchain Concepts: Consensus





# Blockchain Concepts: Consensus



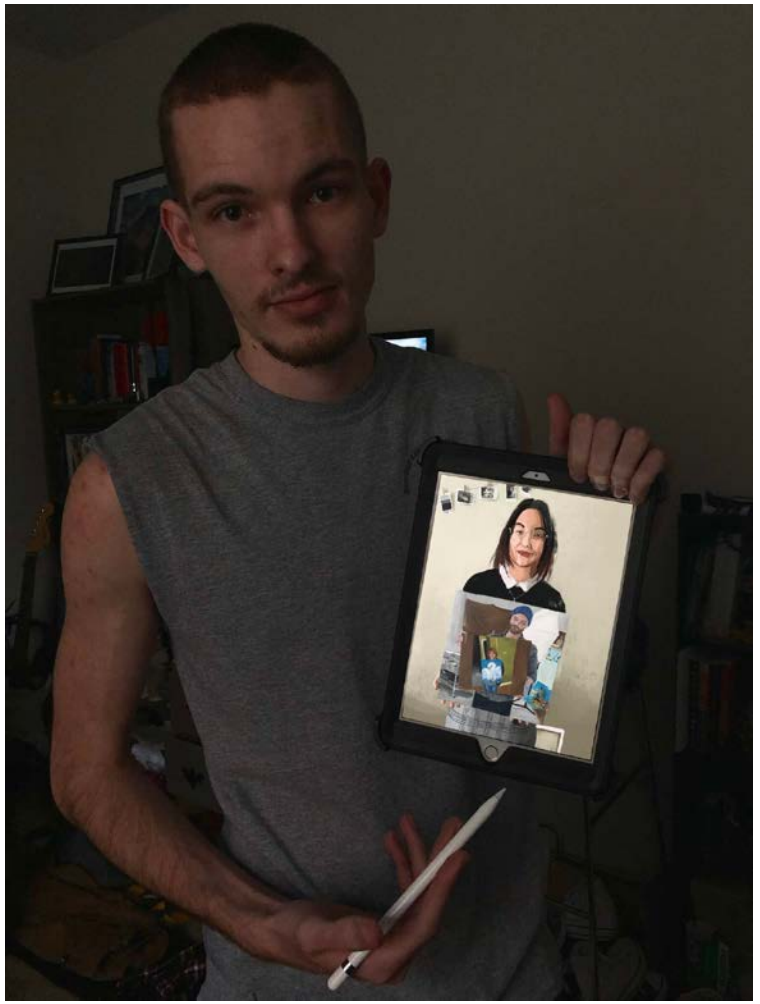




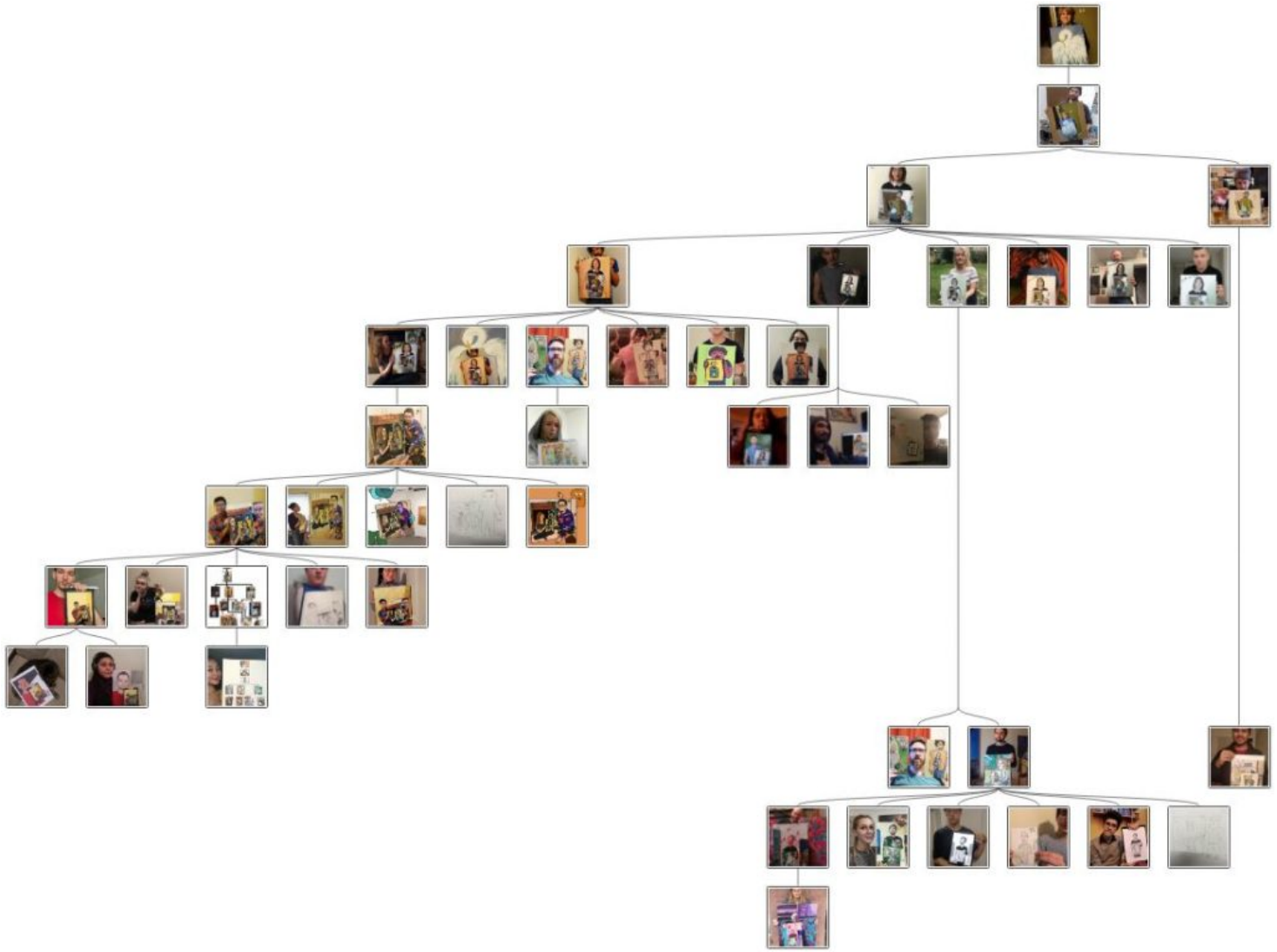
# Blockchain Concepts: Consensus







# Blockchain Concepts: Consensus



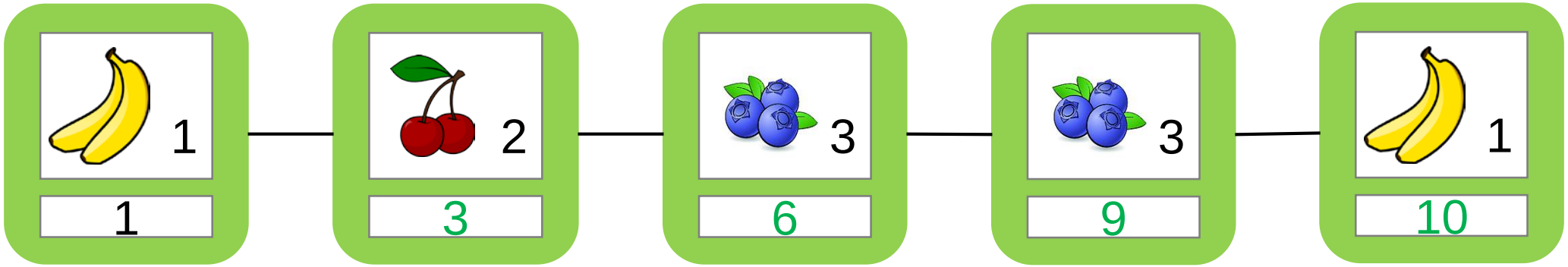
# Interactive Demo

Online demo

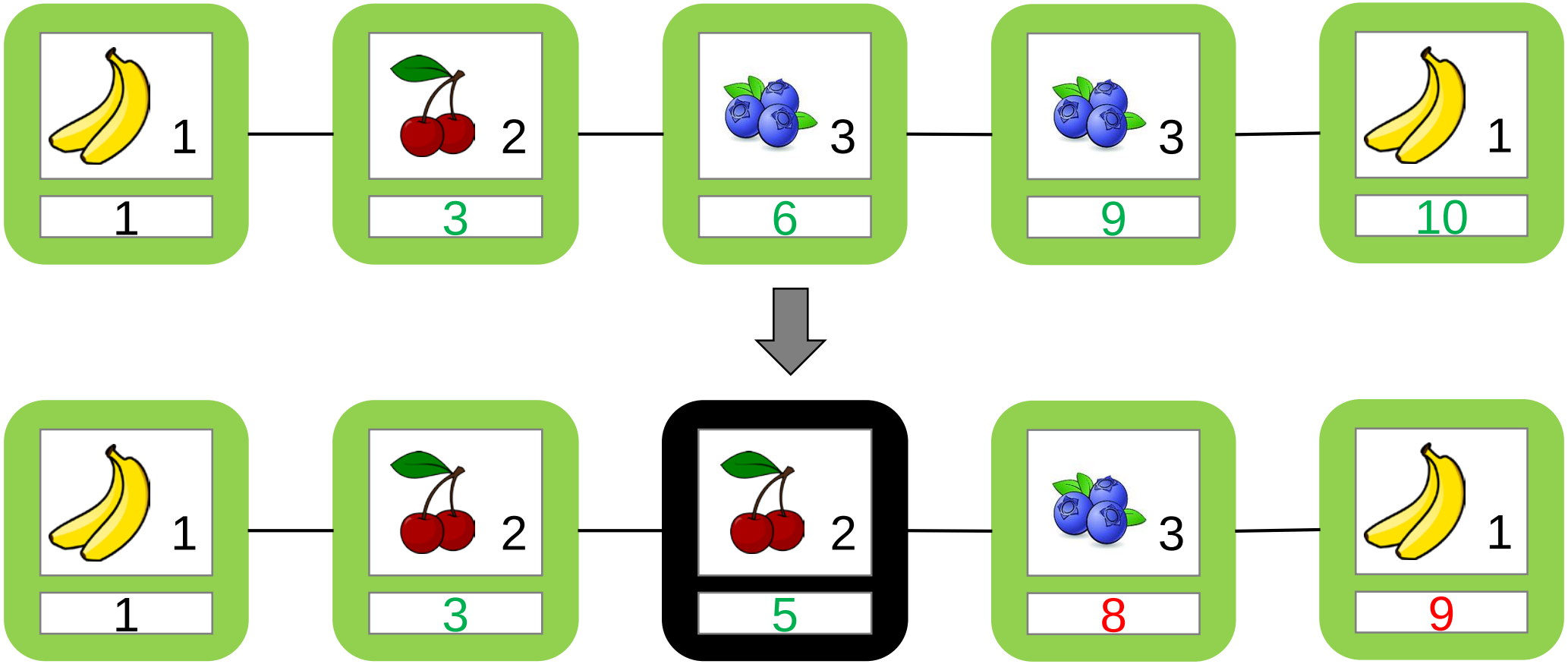
Goals (demo will cover):

- How current transactions keep track of the blockchain’s history
- How we choose a single “official” chain from multiple versions

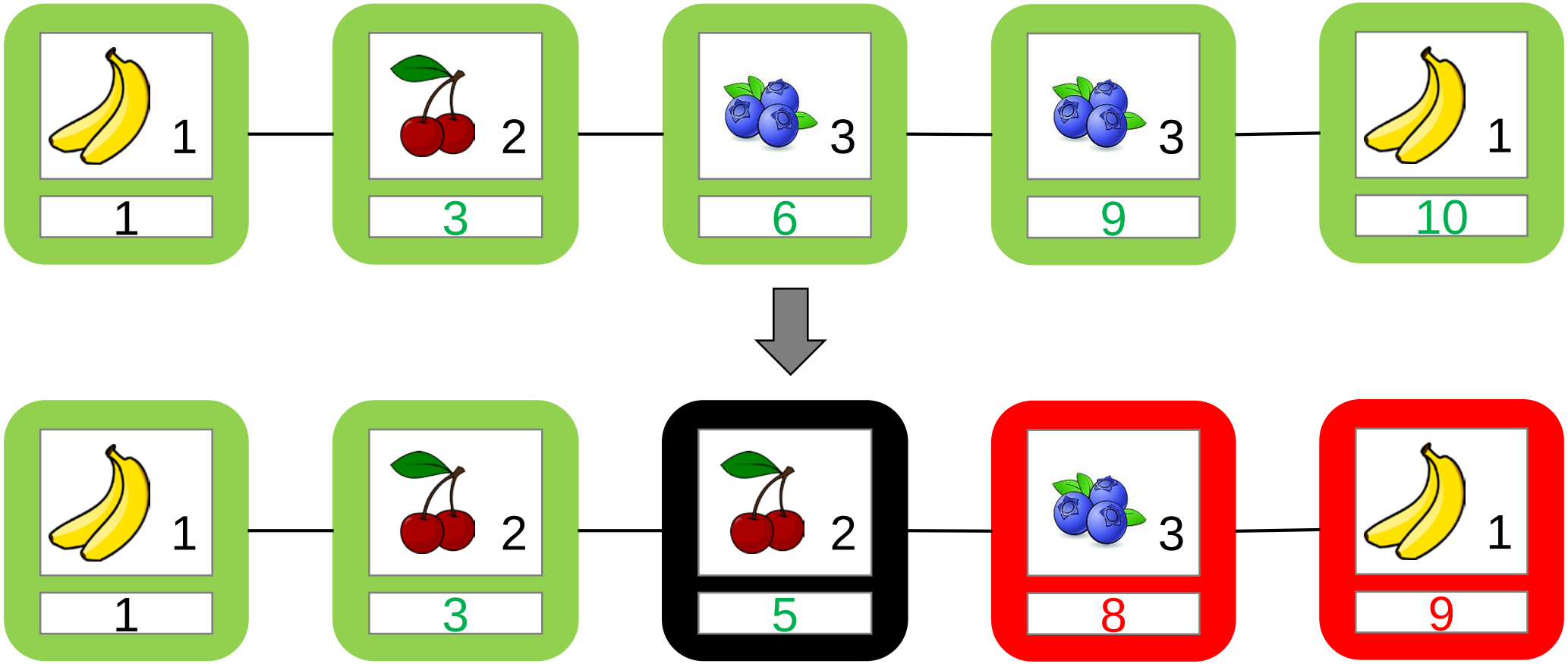
# Blockchain Concepts: Consensus (applied)



# Blockchain Concepts: Consensus (applied)



# Blockchain Concepts: Consensus (applied)



# Blockchain Concepts: Consensus (applied)

**Notes on real-world protocols**:

1. Block values (“Banana = 1”) are derived based on contents, not assigned

2. Block footers use more complicated algorithms than just summing values with previous footers

3. Block footer calculations are difficult *by design*



# Blockchain Concepts: The Fundamentals

A Blockchain is a ‘transaction database shared by all nodes participating in a distributed system’



## Distributed ledger

Every participant in the network has simultaneous access to a view of the information



## Consensus

Verification is achieved by participants confirming changes with one another, replacing the need for a third party to authorise transactions



## Cryptography

Integrity and security of the information on the Blockchain are ensured with cryptographic functions



## Smart contracts

Recording code to a blockchain (instead of raw data) allows users to **embed business logic**, and **selectively share information** with other network participants

# Module 2: Distributed Flood Insurance Management

Guidehouse

# Blockchain: Benefits & Use Cases

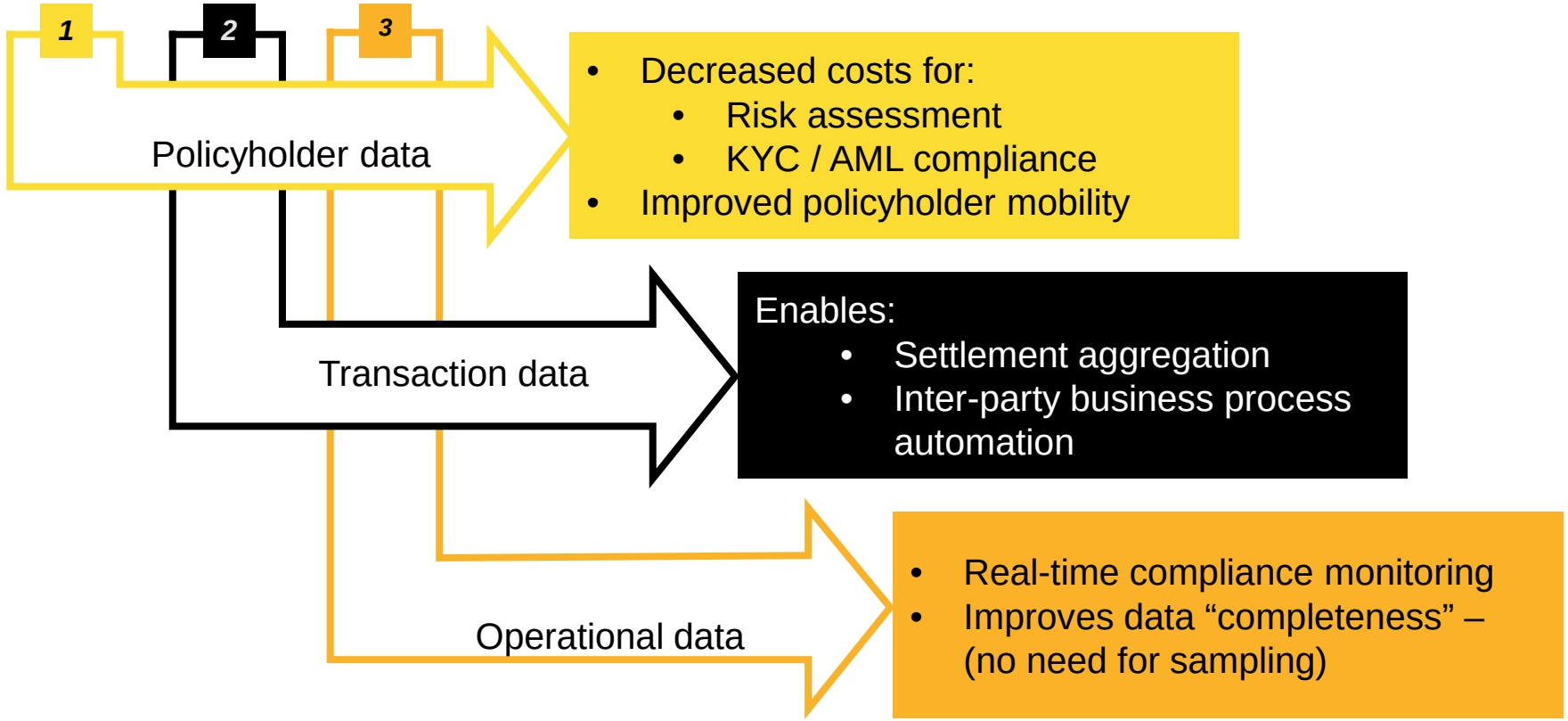
| Use Case | Transparency | Security | Auditability | Selectivity of Shared Information | Broader Participation | Reduced Costs |
|---|---|---|---|---|---|---|
| | **Blockchain Characteristics** | | | | | |
| Supply Chain | | | ✓ | | | ✓ |
| Transaction Processing | | ✓ | | | ✓ | ✓ |
| Identification | | ✓ | | ✓ | ✓ | |
| Voting | ✓ | ✓ | ✓ | ✓ | | |
| Records Management | | ✓ | ✓ | ✓ | | |
| Audits & Regulatory Compliance | ✓ | | ✓ | | | ✓ |

# Blockchain: Insurance Management Benefits

| Use Case | Blockchain Characteristics | | | | | |
|---|---|---|---|---|---|---|
| | Transparency | Security | Auditability | Selectivity of Shared Information | Broader Participation | Reduced Costs |
| Reduced Compliance & Monitoring Costs | ✓ | | ✓ | | | ✓ |
| Real-time Policy Updates | | ✓ | | ✓ | ✓ | |
| Increased Liquidity of Reinsurance Markets | ✓ | | | | ✓ | ✓ |
| Identity Management | | ✓ | | ✓ | | |
| Efficient Claims Processing | ✓ | ✓ | ✓ | ✓ | | ✓ |
| Increased Risk Transparency | ✓ | | ✓ | ✓ | | ✓ |

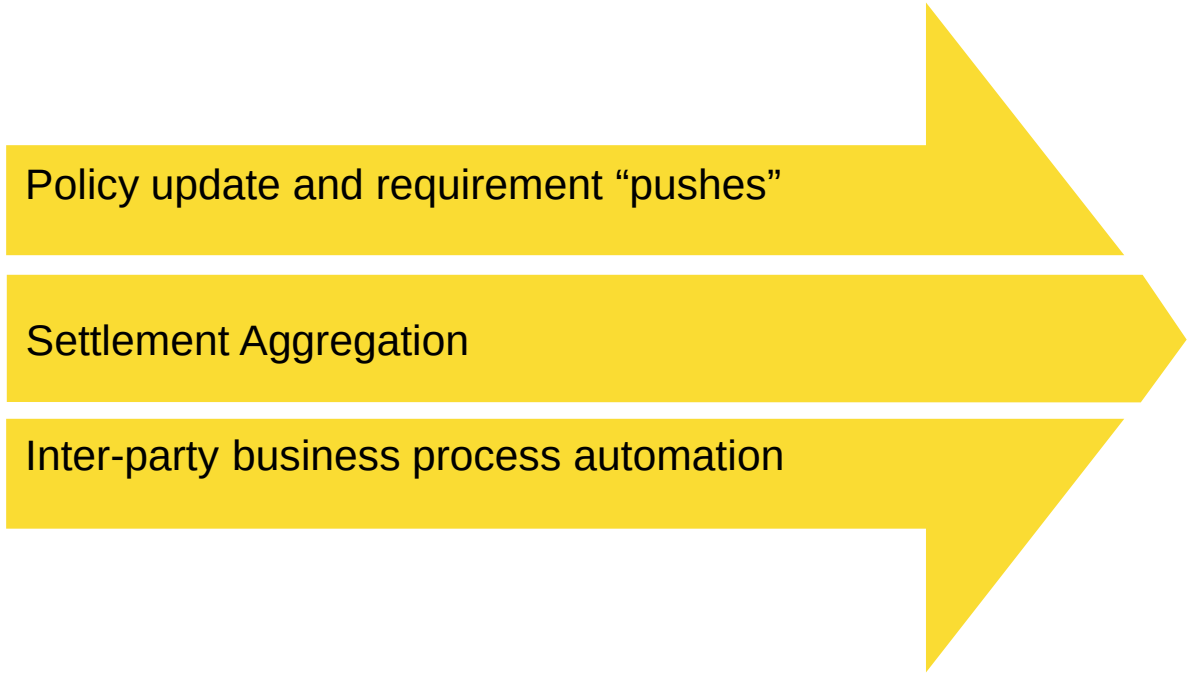
# Blockchain: Insurance Management Benefits

## Information selectivity



# Blockchain: Insurance Management Benefits

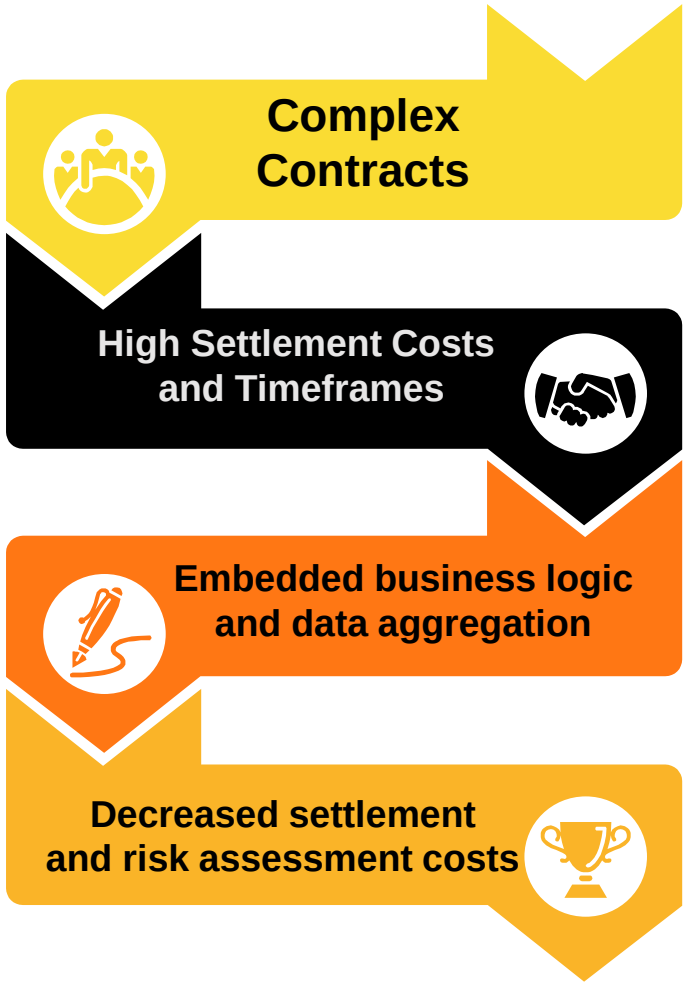
## Embedded Business Logic




Improves:

- Transaction timeliness
- Policy compliance
- Costs

# Blockchain: Insurance Management Benefits




## Increased Liquidity of Reinsurance Markets

- Reinsurance contracts generally require significant administrative costs and settlement periods once a payout is triggered
- Distributed ledgers can decrease settlement costs and timeframes by accessing stakeholder data in real-time and processing transactions through embedded business logic
- Improved data aggregation functions similarly for reinsurers as for underwriters
- Decreased settlement and risk assessment costs can pass through to decreased costs of individual insurance policies

# Q&A

Guidehouse

# Blockchain: Insurance Management Benefits

Incentivized participation

- Centralized networks concentrate both costs and benefits of information infrastructure
- By sharing both costs and benefits, a decentralized network:
  - Can incentivize individual stakeholders to buy-in
  - Doesn’t concentrate the burden for network improvements on any one stakeholder

# Cryptocurrency “attacks”

1. 51% attack
2. Exploiting code vulnerabilities
   - Example: DAO attack
     - 3.6m ETH (~$70M) stolen in June 2016
     - Ethereum community updated their code to block access to the stolen funds
3. Phishing targets
   - Users
   - Exchanges
4. Quantum algorithms
   - (Not a current threat):

| Year | Largest integer factored by a quantum computer |
|---|---|
| 2001 | 15 |
| 2012 | 143 |
| 2014 | 56153 |

   - 2015 – NSA announced plans for new quantum-resistant cipher suite

# Comparison of Money Transfer Methods

| | Cash | Check | Credit Card | Permissioned Blockchain Network | Pseudonymous Public Blockchain Network | Anonymous Public Blockchain Network |
|---|---|---|---|---|---|---|
| Electronic Transfer | | ✓ | ✓ | ✓ | ✓ | ✓ |
| KYC / AML | | ✓ | ✓ | ✓ | | |
| Traceability | (limited) | ✓ | ✓ | ✓ | ✓ | |
| Examples | N/A | N/A | N/A | JPM Coin, currencies built on Hyperledger Fabric / Corda / Enterprise Ethereum | Bitcoin, Ethereum | Monero, ZCash |

# Tax Regulations

IRS 2014-21:

- For federal tax purposes, virtual currency is treated as property.
- Taxpayers must recognize gains or losses upon an exchange of virtual currency for other property.

Tax Cuts and Jobs Act (2017):

- Clarifies that *like-kind exchanges* only apply to real estate.

# Securities Regulations

Offerors of *investment contracts* must register under the *Securities Act of 1933.*

## The Howey Test

Defines *investment contracts* as:

- An investment
- in a common enterprise
- with an expectation of profit
- generated through the efforts of others

Decided by *SEC v. W. J. Howey Co.* (1946)

# Securities Regulations

| |  W.J. Howey Co. | Bitcoin | Ethereum | VeChain |
|---|---|---|---|---|
| Investment | ✓ | ✓ | ✓ | ✓ |
| Common Enterprise | ✓ | * | * | ✓ |
| Expectation of Profit | ✓ | ✓ | ✓ | ✓ |
| Profits Generated through the Efforts of Others | ✓ | * | * | ✓ |

# Securities Regulations

SEC Chief Jay Clayton (April 2018):

"Every ICO I've seen is a security."

SEC Director of Corporate Finance William Hinman (June 2018):

"Putting aside the fundraising that accompanied the creation of Ether, based on my understanding of the present state of Ether, the Ethereum network and its decentralized structure, current offers and sales of Ether are not securities transactions"

"As a network becomes truly decentralized, the ability to identify an issuer or promoter to make the requisite disclosures becomes difficult, and less meaningful[…] As with Bitcoin, applying the disclosure regime of the federal securities laws to current transactions in Ether would seem to add little value."

# Definitions

| | |
|---|---|
| **Distributed Ledger** | A shared record of transactions or other data which is updated and verified by network participants without requiring a centralized authority |
| **Hash** | The output of a function which creates a string of characters which can identify matching inputs without revealing the original data. A digital “fingerprint”. |
| **Block** | A segment containing transactions or other data to be written to a blockchain, including security and consensus information |
| **Block Header** | The portion of a block which contains information from the previous block in the chain |
| **Nonce** | A random value included in a block, which can be altered to change the block’s hash without changing the transactions or data within the block body |
| **Blockchain** | A collection of blocks linked together and secured by a consensus algorithm |

# Definitions

| | |
|---|---|
| **Consensus Algorithm** | A set of rules used to determine which chain is valid and current in a network of multiple blockchains |
| **Proof-of-Work** | A consensus algorithm which limits the creation of new blocks by requiring computers to solve difficult calculations, and which selects the chain which has performed the most calculations (or “work”) as valid. |
| **Proof-of-Stake** | A consensus algorithm that requires validators to invest / “stake” funds, and revokes those funds if they try to cheat when updating the chain. |
| **Permissionless Blockchain** | A blockchain that can be accessed and altered by any participant. (Also called a public blockchain.) |
| **Permissioned Blockchain** | A blockchain that requires a central authority to identify and authorize access for new users. |
| **Zero-knowledge Proof** | In blockchains, a proof that a transaction has occurred without revealing the underlying transaction data. |

# Definitions

| | |
|---|---|
| **Public Key Exchange** | A method for exchanging keys in a non-secure environment so that two participants can encrypt and exchange messages across a public channel |
| **Quantum Cryptography** | A sub-discipline of cryptography focusing on how to exchange information in environments where quantum computers can overcome classic encryption tools |
| **Quantum-resistant Algorithm** | An algorithm that encrypts data using functions which are difficult for both classic and quantum computers to reverse-engineer |
| **Tumbler** | A software tool that can automatically “layer” cryptocurrency transactions |
| **Wallet** | An address in a cryptocurrency network that stores user funds |

# Helpful Resources

| Description | URL |
| --- | --- |
| Brief introduction to key blockchain topics (consensus protocols, permissioned ledgers, distribution mechanisms, and mining incentives) | https://bravenewcoin.com/assets/Reference-Papers/A-Gentle-Introduction/A-Gentle-Introduction-To-Blockchain-Technology-WEB.pdf |
| Blockchain features & potential use cases | https://blockgeeks.com/guides/what-is-blockchain-technology/ |
| NIST blockchain technology overview | https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf |