2021 IISE Annual Conference

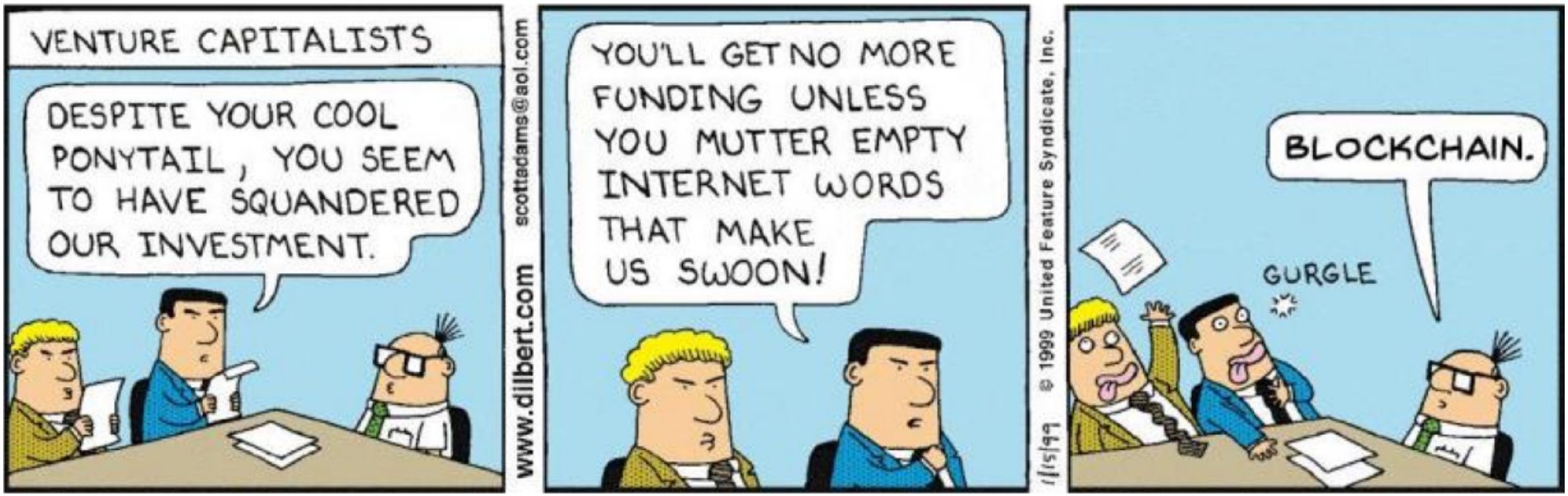
BLOCKCHAIN: A REVIEW FROM THE PERSPECTIVE OF OPERATIONS RESEARCHERS
or How I lost money in bitcoin but is still doing research on blockchain

Hong Wan, Yining Huang, and Kejun Li

Department of Industrial and Systems Engineering
NC State University

June 3, 2021

First Things First



https://bit.ly/37oCmHi

Disclaimer: 2017, Dr. Wan's Welcome Message

What to Cover and What Not

https://dilbert.com/

What Is Blockchain

Blockchain is a digital, append-only, timestamped ledger. It is literally a chain of data blocks

- Immutability
- Decentralization
- Transparency
- Security

Let us get some hand-on experience! (`https://blockchaindemo.io`)

Components of a Blockchain

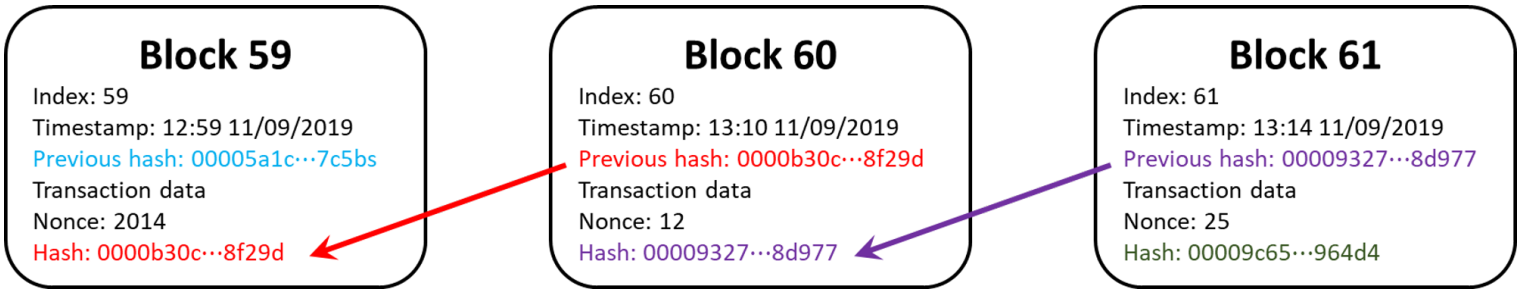


Figure: A demonstration of blockchain: the Bitcoin blockchain.

- Index: the position of the block in the chain. The genesis block has an index of 0. The next block will have an index of 1.
- Timestamp: a record of when the block was created.
- Data: depending on the applications of the blockchain, blocks store the data or data address. In cryptocurrencies such as Bitcoin, the data would be record of transaction.

Hash function

The data stored in blockchain are encrypted using the **Hash(ing) Function**

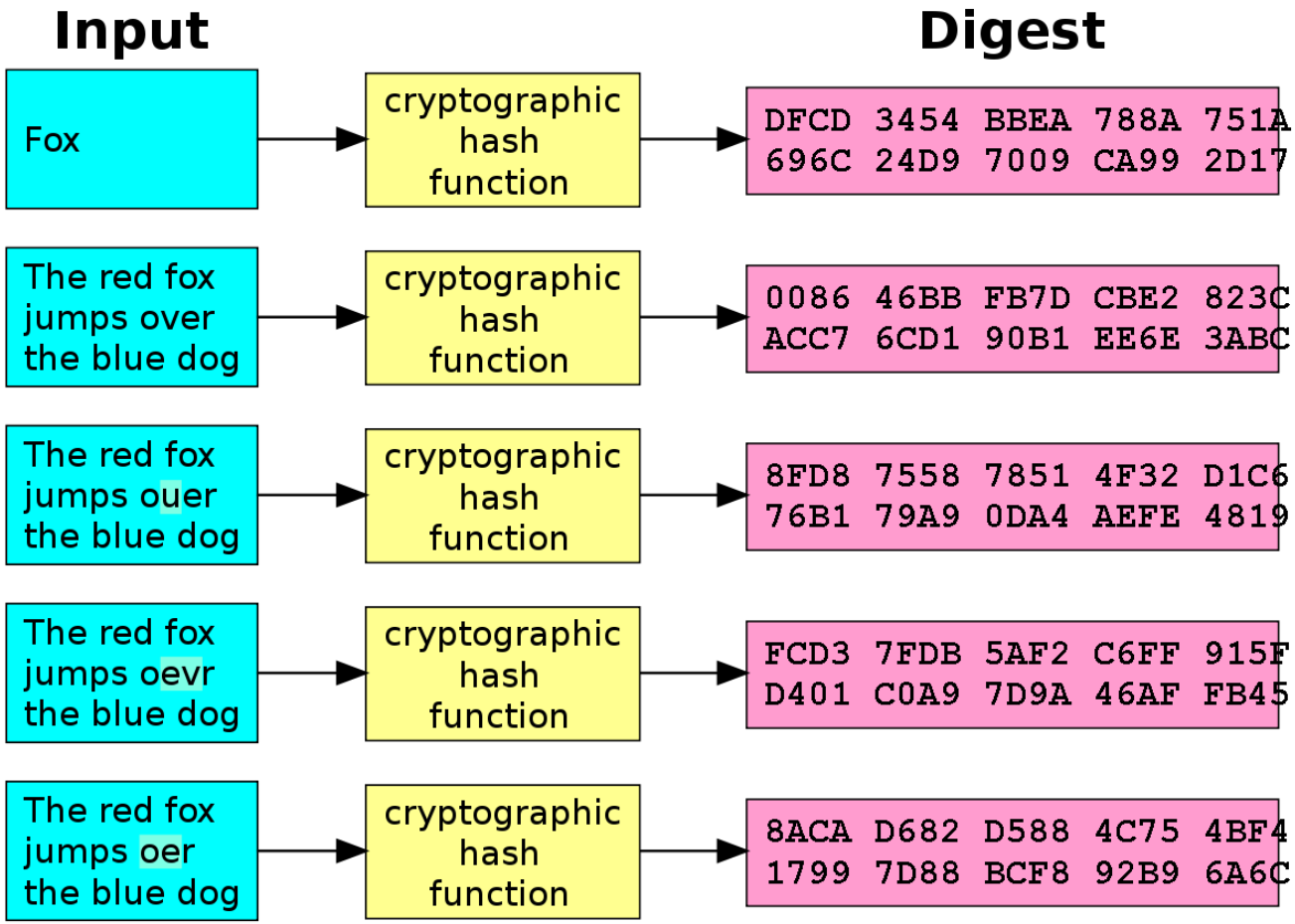


Figure: Hash function demonstration (`https://bit.ly/3ntMVOT`)

Hash function Requirement

- Input can be any length
- Output is fixed length
- Easy to calculate
- Hard to invert
- non-collision property, i.e., $H(x) \neq H(y), \forall x \neq y$

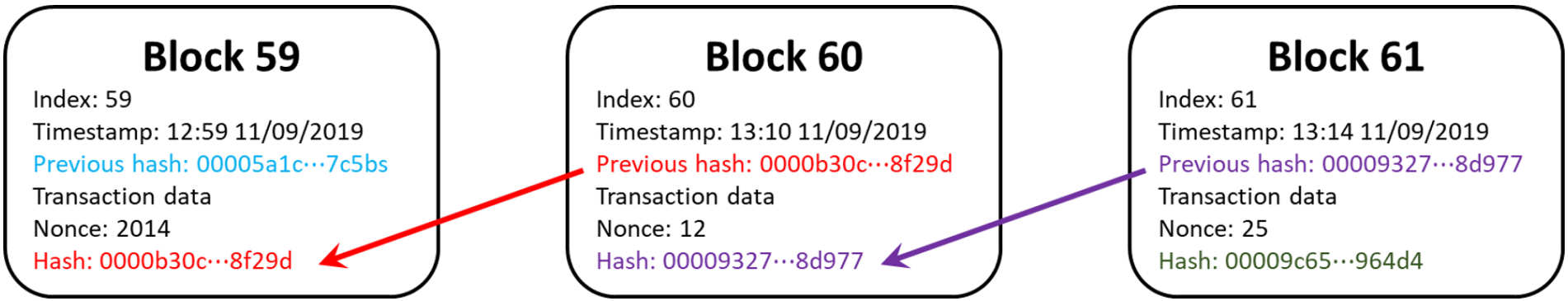


Figure: A demonstration of blockchain: the Bitcoin blockchain.

Blockchain Mechanism Design

- Who can view the data? (private v.s. public)
- Who can generate blocks (permissionless v.s. permissioned)
- How to reach agreement among users (consensus algorithm)

Blockchain as a System of Record

- Immutability
- Decentralization
- Transparency
- Security

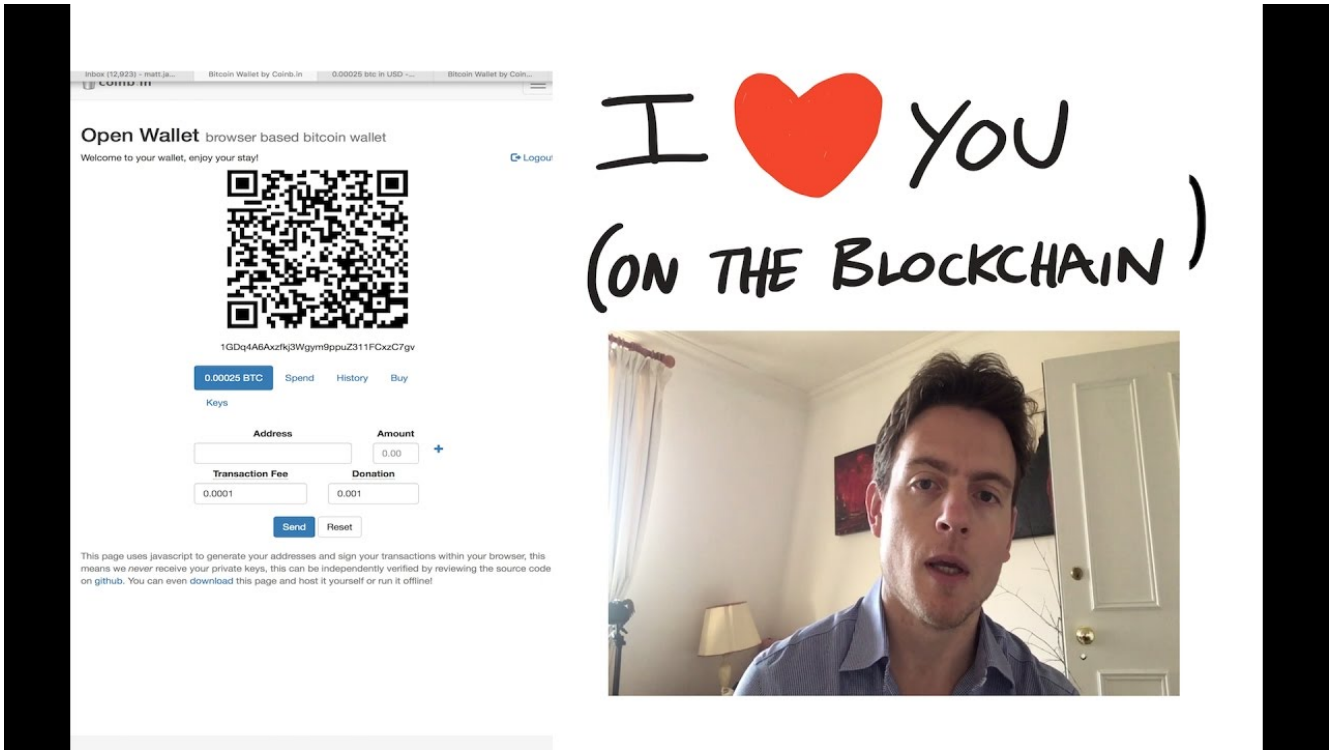


Figure: How much do I love you? (`https://bit.ly/3p4RBvh`)

Blockchain Types

- Public v.s. private
- Permissionless v.s. permissioned

Public-Permissioned	**Private-Permissioned (Consortium)**
+ Good scaling	+ Good scaling
∼ Private → Public ecosystem	∼ Completely isolated ecosystem
− Centralized	− Centralized
+ Independently verifiable	− Not independently verifiable
− Not yet implemented	+ Implemented by Hyperledger, etc.
Public-Permissionless	**Private-Permissionless**
− Poor scaling	− Poor scaling
∼ Completely public ecosystem	∼ Private → Public ecosystem
+ Distributed	+ Distributed
+ Independently verifiable	− Not independently verifiable
+ Implemented by bitcoin, Ethereum, etc.	− Not yet implemented

+ represents desired properties ∼ represents neutral − represents shortcomings

Table: Comparison of different blockchain categories [Parsons, 2018].

Trade-off Among Performance Measures

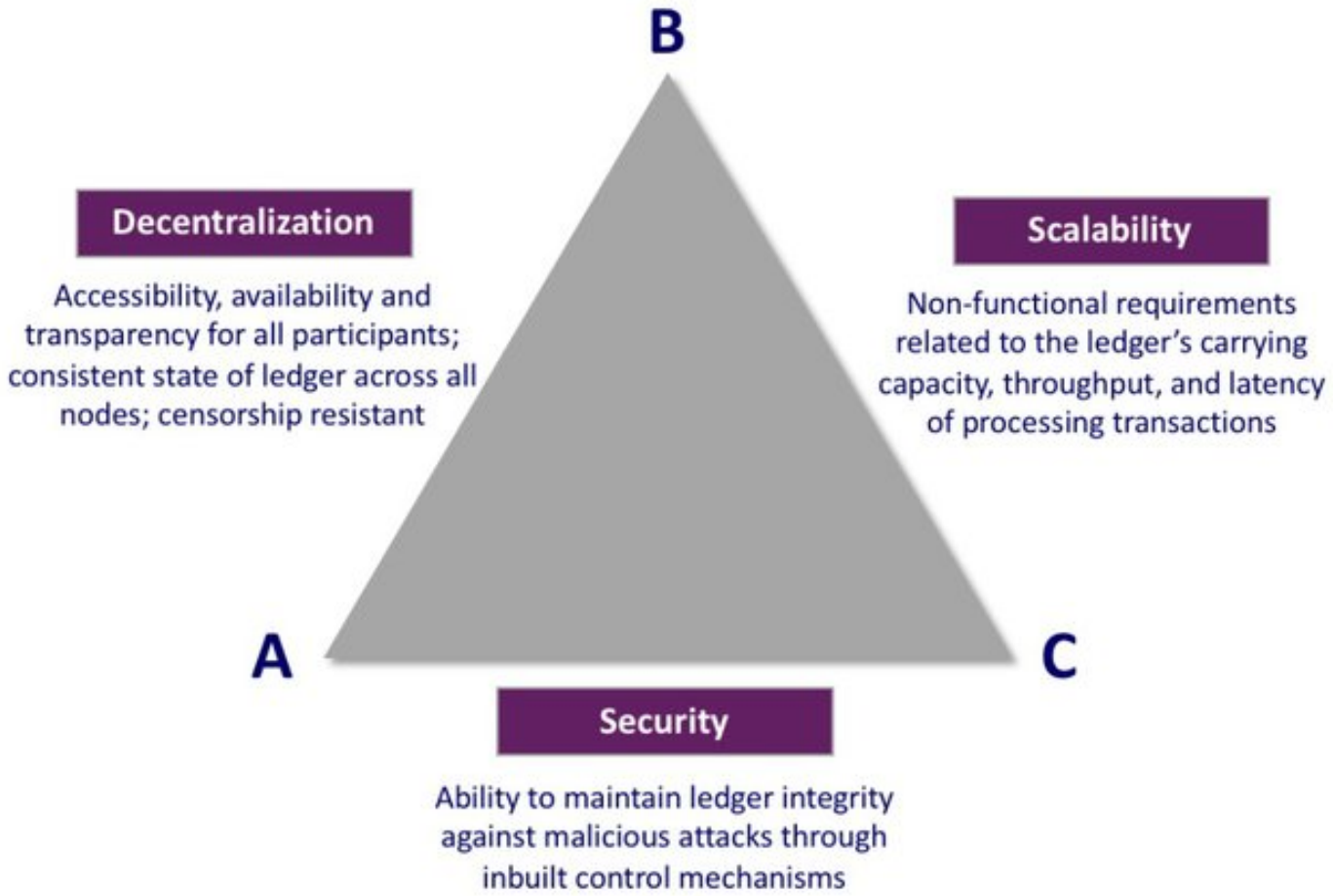


Figure: Blockchain scalability trilemma [ReverseAcid, 2018].

Consensus Mechanism

The consensus is an algorithm to reach agreements among different participants of the distributed system to determine the ordering and confirmation of transactions.

Proof of Work (PoW)

- Computational puzzle
- Probabilistic and winner-take-all game
- Slow and energy-consuming

Proof of Stake (PoS)

- Validators replace miners
- More efficient than PoW
- Nothing-at-stake problem

Bitcoin and Ethereum: Mining and Smart Contract

Bitcoin and Ethereum

Two of the most well-known public-permissionless blockchain applications:

- Bitcoin is considered the "new gold" in the digital currency era;
- Ethereum users have applied the smart contracts to create entire decentralized autonomous organizations (DAOs).

Bitcoin: The First Cryptocurrency

- Oct. 30th, 2008: Satoshi Nakamoto (we still do not know who he/she/they is (are)) posted "Bitcoin: A Peer-to-Peer Electronic Cash System" to a cryptography mailing list.
- Jan. 3rd 2009, Satoshi Nakamoto mine the genesis block of bitcoin (block number 0).

Bitcoin: The First Cryptocurrency

Bitcoin value history (comparison to US$)

Date	USD : 1 BTC	Notes
Jan 2009 – Mar 2010	basically nothing	No exchanges or market, users were mainly cryptography fans who were sending bitcoins for hobby purposes representing low or no value. In March 2010, user "SmokeTooMuch" auctioned 10,000 BTC for $50 (cumulatively), but no buyer was found.[144]
May 2010	less than $0.01	On 22 May 2010,[145] Laszlo Hanyecz made the first real-world transaction by buying two pizzas in Jacksonville, Florida, for 10,000 BTC, an amount that would be nearly $750,000 if held in March 2013.[146]
Feb 2011 – April 2011	$1.00▲	Bitcoin takes parity with US dollar.[147]
Nov 2013	$350–$1,242▲	Price rose from $150 in October to $200 in November, reaching $1,242 on 29 November 2013.[148]
Apr 2014	$340–$530▼	The lowest price since the 2012–2013 Cypriot financial crisis had been reached at 3:25 AM on 11 April[149]
2-3 March 2017	$1,290+ ▲	Price broke above the November 2013 high of $1,242[150] and then traded above $1,290.[151]
20 May 2017	$2,000 ▲	Price reached a new high, reaching $1,402.03 on 1 May 2017, and over $1,800 on 11 May 2017.[152] On 20 May 2017, the price passed $2,000 fo the first time.
1 September 2017	$5,013.91▲	Price broke $5,000 for the first time.[153]
17-20 November 2017	$7,600-8,100 ▲	Briefly topped at $8004.59. This surge in bitcoin may be related to the 2017 Zimbabwean coup d'état. In one bitcoin exchange, 1 BTC topped at nearly $13,500, just shy of 2 times the value of the International market.[154][155]
15 December 2017	$17,900 ▲	Price reached $17,900.[156]
17 December 2017	$19,783.06 ▲	Price rose 5% in 24 hours, with its value being up 1,824% since 1 January 2017, to reach a new all-time high of $19,783.06.[157]
22 December 2017	$13,800 ▼	Price lost one third of its value in 24 hours, dropping below $14,000.[158]
5 February 2018	$6,200 ▼	Price dropped by 50% in 16 days, falling below $7,000.[159]
31 October 2018	$6,300 –	On the 10th anniversary of bitcoin, the price held steady above $6,000 during a period of historically low volatility.[160][161]
7 December 2018	$3,300 ▼	Price briefly dipped below $3,300, a 76% drop from the previous year and a 15-month low.[162]
27 July 2020	$10,944 ▲	Price surged to the highest in almost a year.[163]
26 October 2020	$13,000 ▲	Price stayed above the $10,000 mark for an unprecedented three-month stretch.[164]
16 November 2020	$16,800 ▲	Bitcoin has been more expensive in only five other instances in the past decade.[165]
18 November 2020	$18,000 ▲	Bitcoin rallies above $18,000 to trade near all-time highs[166]
24 November 2020	$19,000 ▲	Bitcoin price reaches three-year high of more than $19,000.[167]
30 November 2020	$19,850.11 ▲	Bitcoin price reached new all-time high of $19,850.11.[168]
16 December 2020	$20,600 ▲	Bitcoin reaches all-time high of $20,600. [169]
17 December 2020	$22,166 ▲	Bitcoin reaches all-time high of $22,166.

https://bit.ly/3gWIg5N

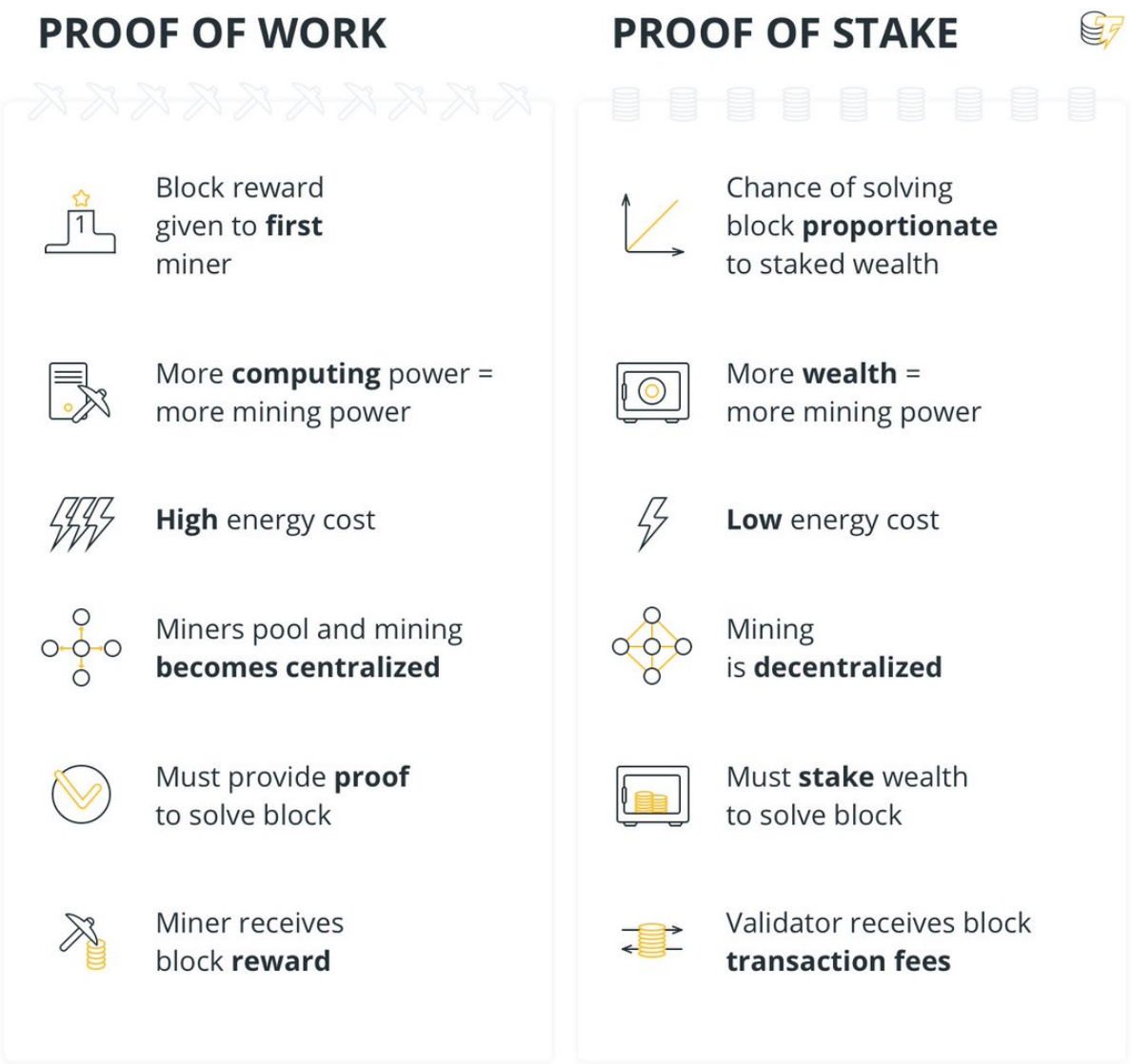
Proof of Work (PoW)

- f(index, previous hash, timestamp, transactions, nonce) = hash
  - Cryptographic hash function f: a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size, which is designed noninvertible.
  - SHA-256: from the Secure Hash Algorithm (SHA) family, output 256-bit hash. (`https://demoblockchain.org/hash`)
- Valid hash value: below certain threshold (i.e. begin with certain number of zeros).

$$
\begin{aligned}
f(\overbrace{762}^{\text{id}}, & \overbrace{12/03/18}^{\text{timestamp}}, \overbrace{0005a9\ldots}^{\text{previous hash}}, \overbrace{\{\text{txn123}, \text{txn987}, \ldots\}}^{\text{transaction data}}, \overbrace{3001}^{\text{nonce}}) = \overbrace{4378\ldots}^{\text{hash}} > \overbrace{000\ldots}^{\text{threshold}} \\
f(762, & 12/03/18, 0005a9\ldots, \{\text{txn123}, \text{txn987}, \ldots\}, 3002) = 0901\cdots > 000\ldots \\
f(762, & 12/03/18, 0005a9\ldots, \{\text{txn123}, \text{txn987}, \ldots\}, 3003) = 0005\cdots < 000\ldots
\end{aligned}
$$

- Winning probability: proportional to hashing capacity devoted to mining.

PoW and PoS



https://bit.ly/2KCsalS

Ethereum and Smart Contract

Ethereum

- A decentralized open-source blockchain platform that features smart contracts.
- Ethereum is currently using PoW as its consensus protocol but transitioning into PoS.

Smart Contract

- A piece of automatically executed code that implements certain activities when the condition fulfills.
- "Blockchain and smart contracts are governance technologies that have the potential to provide higher levels of transparency while reducing bureaucracy with self-enforcing code." [Voshmgir, 2019]
- Potential applications in various industries, especially in the filed of supply chain provenance.

Consortium Blockchain

Consortium Blockchain

- Multiple entities and stakeholders
- Customized authorizations
- Hyperledger: the most well-known umbrella projects of open-source consortium blockchains and tools developed by Linux.

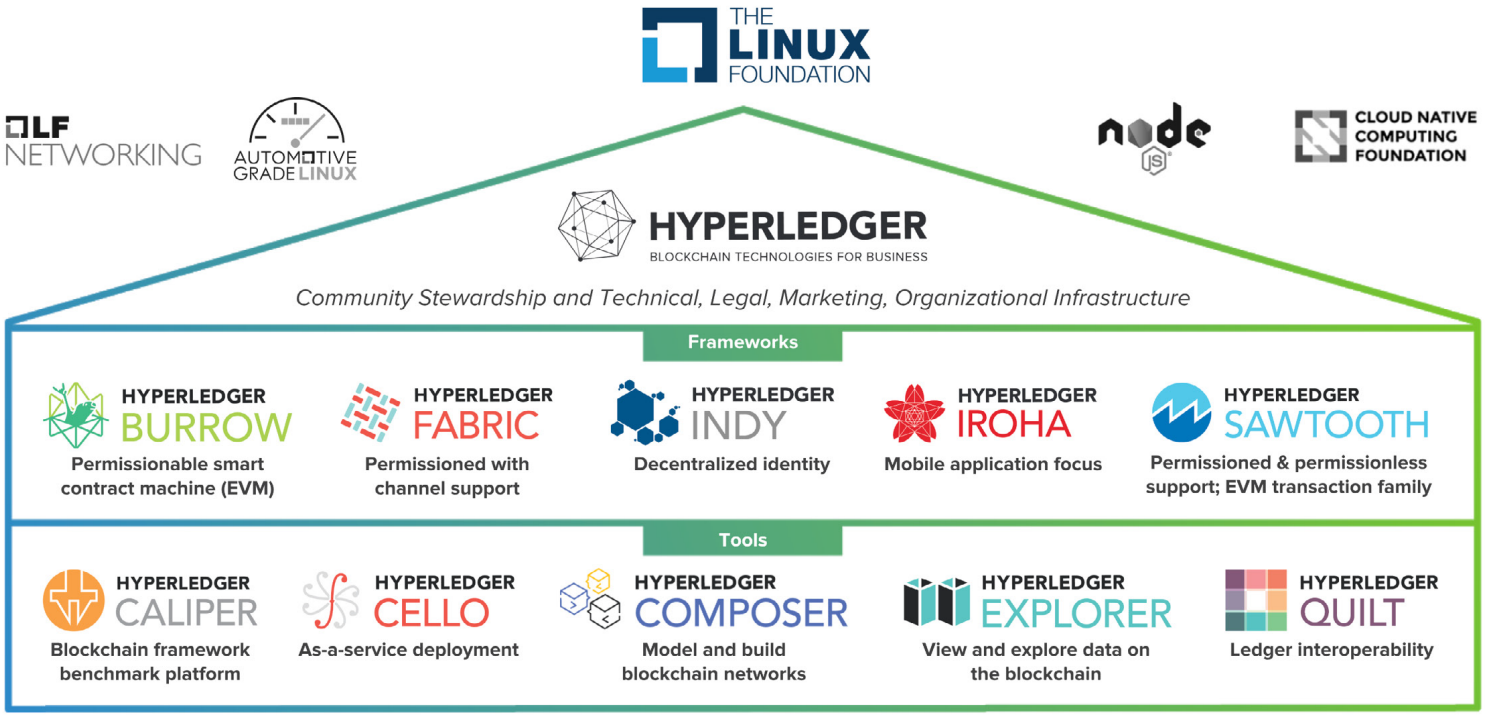


Figure: The Hyperledger greenhouse structure [Blummer et al., 2018].

An Application of Hyperledger Sawtooth

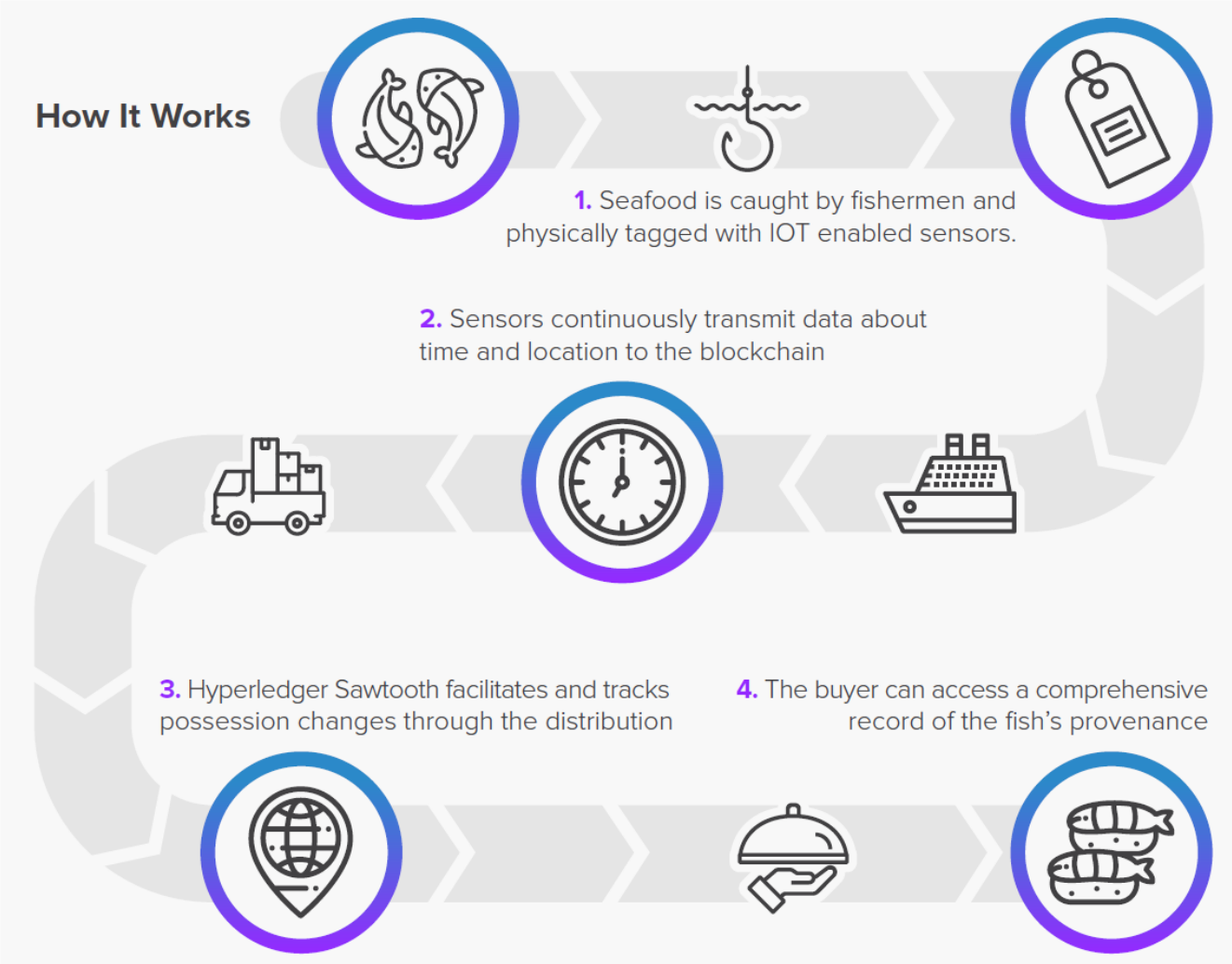


Figure: Flowchart of the seafood supply chain using Hyperledger Sawtooth [Blummer et al., 2018].

System and Data Analysis of Blockchain Systems

Simulation Study of Blockchain Systems

Models

- Discrete-event simulation
- Agent-based simulation

Current Study

- Mining behaviors of cryptocurrencies
- Scalability of blockchain simulation models
- Performance of blockchains under different conditions/attacks

Game Theory

Models

- Non-cooperative game
- Extensive-form game
- Stackelberg game
- Stochastic game

Current Study

- Security
- Mining Management
- Blockchain platform

Machine Learning in and for Blockchain

Models

- Machine learning
- Deep learning
- Reinforcement learning

Current Study

- Blockchain-based data sharing platform
- Categorization of bitcoin transactions and prediction its price
- Optimization of resource allocation

Blockchain characteristics comparison			
Characteristics	**Bitcoin**	**Ethereum**	**Hyperledger**
Permission restrictions	Permissionless	Permissionless	Permissioned
Restricted public access to data	Public	Public or private	Private
Consensus	Proof-of-Work	Proof-of-Work	PBFT
Scalability	High node-scalability, Low performance-scalability	High node-scalability, Low performance-scalability	Low node-scalability, High performance-scalability
Centralized regulation (governance*)	Low, decentralized decision making by community/miners	Medium, core developer group, but EIP process	Low, open-governance model based on Linux model
Anonymity	Pseudonymity, no encryption of transaction data	Pseudonymity, no encryption of transaction data	Pseudonymity, encryption of transaction data
Native currency	Yes, bitcoin, high value	Yes, ether	No
Scripting	Limited possibility, stack-based scripting	High possibility, Turing-complete virtual machine, high-level language support (Solidity)	High possibility, Turing-complete scripting of chaincode, high-level Go-language

Figure: Comparison of Bitcoin, Ethereum, and hyperledger [Blummer et al., 2018].

Limitations of Blockchain

- Trade-off among scalability, decentralization, and security
- Time and energy inefficiency
- 51 percent attack
- Self-organizing cheating behavior
- Garbage in garbage out (GIGO)
- Pseudo anonymity

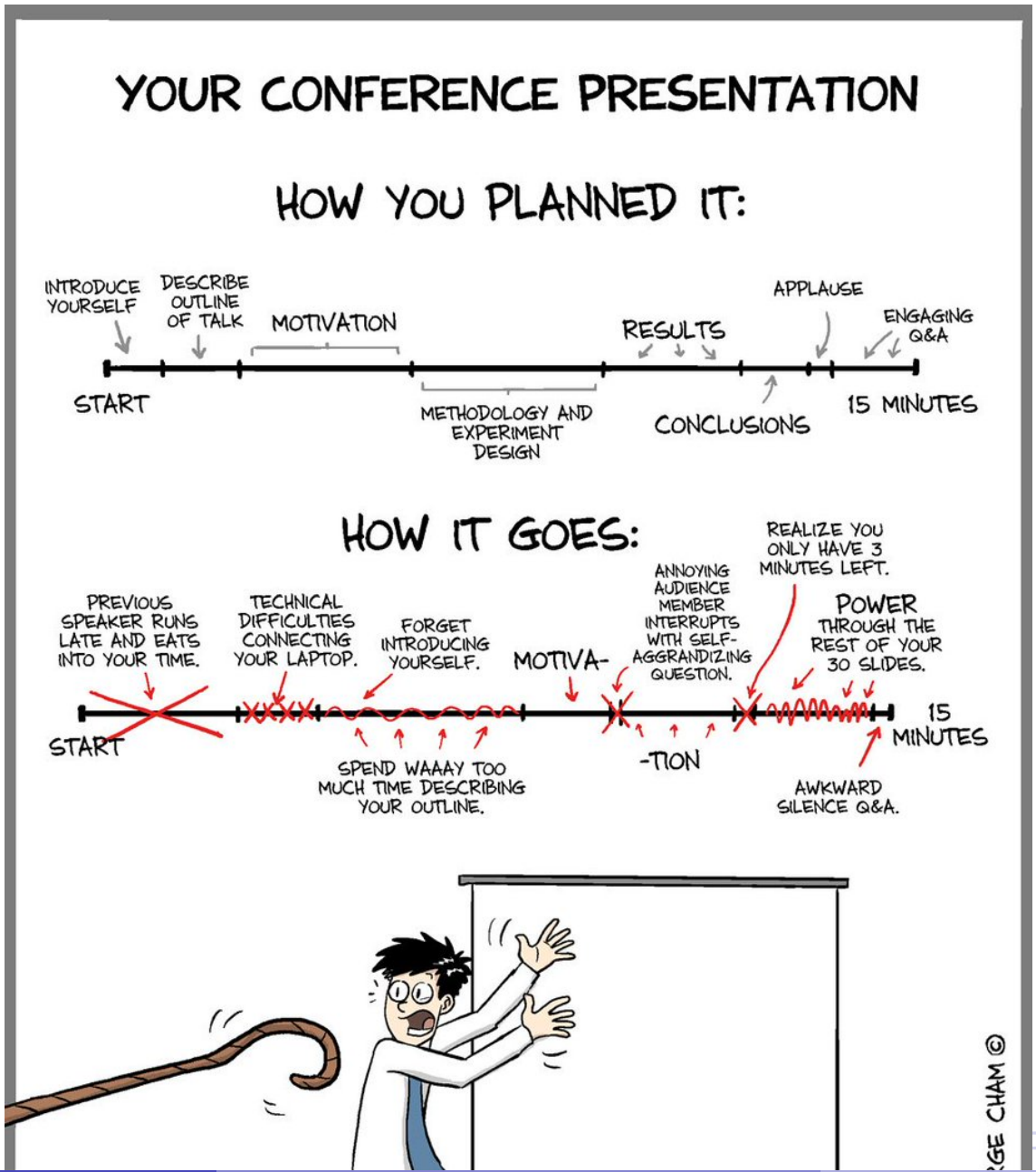
When Should Blockchain Be Applied

- The traditional (public permissionless) blockchain:
  almost no cases except for cryptocurrency.
- The consortium/private blockchain:
  when there is no or only partial trust toward a third party and/or each others.

https://bit.ly/3gUNLli

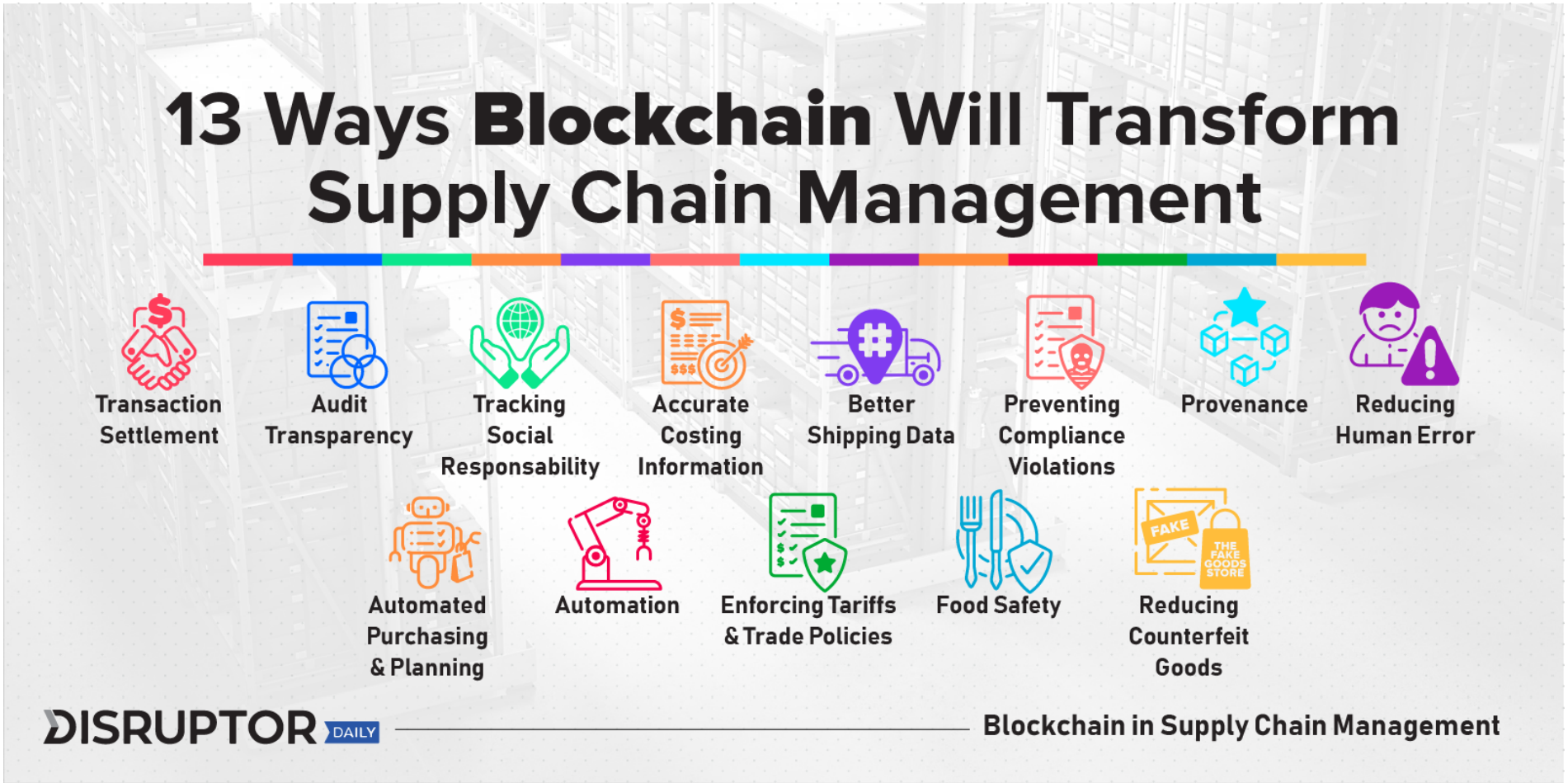
Discussions

https://pbs.twimg.com/media/CzGeSptUcAAJ-ve.jpg



Blockchain and Operations Research

- Sophisticated mathematical and simulation models:
  capture individual behaviors, interactions and system dynamics.
- Computational game theory approach:
  incorporate simulation and other numerical models with game theory.
- Data-related methodologies



https://www.disruptordaily.com/blockchain-use-cases-supply-chain-management/

Reference


Blummer, T., Sean, M., and Cachin, C. (2018).
An introduction to hyperledger.
Technical report, Tech. rep. 2018. url: https://www. hyperledger. org/wp-content/uploads/2018.


Parsons, J. (2018).
Blockchain types explained: It's more than public vs private – uledger.
http://159.65.79.6/blockchain-types-explained-its-more-than-public-vs-private/, accessed 29th June.


ReverseAcid (2018).
The scalability trilemma – steemit.
https://steemit.com/blockchain/@reverseacid/the-scalability-trilemma, accessed 29th June.


Voshmgir, S. (2019).
Token economy: How blockchains and smart contracts revolutionize the economy.
BlockchainHub.