UNIVERSITY OF
ARKANSAS
SAM M. WALTON
COLLEGE OF BUSINESS
Department of Information
Systems

Blockchain
Center of Excellence

Blockchain Center of Excellence
White Paper Series

Blockchain Governance Models: Insights for Enterprises

(BCoE 2019-02)

Proof of existence using poex.io service; hash on BCoE website

UNIVERSITY OF ARKANSAS
SAM M. WALTON
COLLEGE OF BUSINESS
Department of Information Systems

Blockchain
Center of Excellence

Blockchain Governance Models: Insights for Enterprises

Blockchain Center of Excellence Research White Paper

(BCoE 2019-02)

By

Mary Lacity
Walton Professor and Director of the Blockchain Center of Excellence

Zach Steelman
Assistant Professor of Information Systems

Paul Cronan
Professor and M.D. Mathews Chair in Information Systems

Proof of existence using poex.io service; hash on BCoE website

Blockchain
Center of Excellence

About the Blockchain Center of Excellence (BCoE):

The BCoE is housed in the Information Systems Department of the Sam M. Walton College of Business at the University of Arkansas. The BCoE was the officially launched by US State Governor of Arkansas, the Honorable Asa Hutchinson, on August 1, 2018. The center's vision is to make the Sam M. Walton College of Business a premier academic leader of blockchain application research and education. The BCoE's white paper series is one activity towards achieving that vision. As the BCoE aims to be platform agnostic, open, and inclusive, our white papers are available to the public following a 60 day sequester period with our Executive Advisor Board member firms. In keeping with the spirit of blockchains as an immutable ledger, the copyright is recorded on the Bitcoin blockchain using a service by poex.io.

White paper audience:

The BCoE's white papers are written for multiple audiences, including senior executives looking for the *"So what?"*, IT and innovation directors in charge of blockchain initiatives needing deeper insights, and students at both the graduate and undergraduate levels. Given the readership diversity, we write an Executive Summary for senior executives interested in the overall findings, a Full Report for managers directly engaged with enterprise blockchains, and often include a number of Appendices to assist novice readers.

Research objective and methods:

The Executive Advisory Board members for the BCoE selected the topic for this white paper. Members from ArcBest Technologies; E&Y; FIS; Golden State Foods; IBM; J.B.Hunt; McKesson; Microsoft; Tyson Foods; and WalMart, posed the research question: *"What are emerging models and practices for shared governance over blockchains?"* The Director of the BCoE assembled an academic research team that reviewed the academic and practitioner literature (see *Appendix A: Research Methods*). Executive Advisory Board members hosted a workshop where experts shared their insights with the research team.

Acknowledgements:

We thank and acknowledge the input and suggestions from our executive advisor board and workshop guests, including Dale Chrystie, Blockchain Strategist at FedEx and Chair of BiTA Standards Council; Susanne Somerville, CEO of Chronicled and co-founder of MediLedger; and Aaron Lieber, Head of Offering Management, TradeLens. Special thanks also to Chen Zur, Partner/Principal-US Blockchain Practice Leader for EY; and Mike Walker, Sr. Director, Applied Innovation Team, Microsoft.

Blockchain Governance Models: Insights for Enterprises

Executive Summary

> *"Governance is an essential component to any successful Blockchain effort. The architecture, business process, and data definition are all key to ensuring the right business value is delivered to key stakeholders."*
>
> Lee Slezak, Vice President – IT Architecture, Tyson Foods

> *"The greatest challenge that new blockchains must solve isn't speed or scaling—it's governance."*
>
> Kai Sedgwick, BitcoinNews[1]

This white paper aims to answer the question: ***"What are emerging models and practices for shared governance over blockchains?"*** A blockchain application is a software application that maintains a distributed, immutable record of sequenced transactions (called a digital ledger) secured by a peer-to-peer network of independent computer nodes. While most innovation decisions happen within the boundaries of the firm, shared blockchain applications require coordination across firm boundaries. This requires a different approach to software governance because no single entity or individual can unilaterally make decisions regarding rule changes, code base upgrades, or record altering. This white paper is developed to help managers and developers think through, and assess, shared governance options even as they continue to evolve.

Based on a review of the literature, a shared governance workshop, and interviews, our research revealed that shared applications necessitate shared governance; moreover, enterprises have little to no experience with shared control. Research reveals that ***enterprise blockchains currently use a variety of governance models, with benefits for both centralized and decentralized decision-making***—such as benevolent dictatorships; oligarchies; stakeocracies; federations; representative meritocracies; meritocracies; and democracies. In addition, we found that blockchain systems often make use of advisory or steering committees, although influential, typically have no formal decision-making rights.

Moreover, ***blockchain governance is multifaceted;*** based on our interviews these include: mission; rights of participation; rights of validation; data policies; rights of overrides; rights of ownership and liability; software update control; governance residence (on-chain or off-chain), and the funding model. The influence of each of these should be considered before a governance structure is set up.

Of equal importance is that governance typically evolves. Launched by a few champions (serving as benevolent dictators), these typically move to distribute this power as the newly launched applications appear. Consequently, ***for blockchains to be successful in the long term, from the beginning founders need to plot a trajectory towards more decentralized models.***

Finally, in this paper, we offer advice to evolve from a centralized governance structure to a decentralized model. Adopters must provide assurances that governance will be truly shared; they may need to prove their intentions to share decision-making rights.

Blockchain Governance Models:
Insights for Enterprises

Table of Contents

Blockchain Governance Models

Full Report

"The greatest challenge that new blockchains must solve isn't speed or scaling—it's governance."

Kai Sedgwick, BitcoinNews[2]

"The only way we are going to get value for the whole industry is to think differently about working together. I've been calling blockchain a 'team sport' for a few years now. We have to work with our competitors on things that improve the entire industry, like safety, quality, and reducing barriers to trade across borders."

Dale Chrystie, Blockchain Strategist at FedEx, Chair of BiTA Standards Council

1. Introduction

At the simplest level, a blockchain application is a software application that maintains a distributed, immutable record of sequenced transactions (called a digital ledger). A peer-to-peer network of independent computer nodes validates transactions, updates the ledger, shares updates across the network and continually monitors the ledger's integrity. By design, blockchain applications should allow parties to transact directly and securely without relying on third-party intermediaries to mitigate counter-party risks. A honeypot of business benefits should follow, such as settling transactions quickly and cheaply among trading partners; eliminating the need for reconciliations, since transactions are confirmed before being committed to the ledger; instantly tracking an asset's location, condition, and custody across a supply chain; providing robust data provenance on an asset's complete history; and enabling a security model that is fault tolerant, resilient, and available.[3] Additionally, some blockchain applications promise a bounty of social value, such as bringing financial services to the 1.7 billion people who lack access (e.g. Stellar, Libra), protecting the property rights of people with low economic status, providing identities for displaced populations and protecting the integrity of political elections.

Early enterprise innovators like EY; Federal Express; IBM; J.B. Hunt; Maersk; McKesson; Microsoft; Tyson Foods; and Walmart (to name but a few) are indeed leading the way, but for the overall market, the pace of enterprise blockchain diffusion has been sluggish. Gartner estimates that the market will not even reach the 'trough of disillusionment' phase until 2021.[4] What's the holdup? The need for identity, data and event standards, regulatory clarity, and technology maturity are certainly reasons. While progress is being made on all these fronts, there is also the issue of managing blockchain applications. ***While most innovation decisions happen within the boundaries of the firm, blockchain applications require coordination across firm boundaries. This requires a different approach to software governance.***

Shared applications require shared governance, where no single entity can unilaterally make decisions about changing the rules, upgrading the code base, or altering the immutable records. Enterprises have little experience of sharing control and need a better understanding of shared governance models. This white paper aims to help enterprises think through, and assess, shared governance options. We aim to illuminate the following blockchain governance maxims uncovered by our research:

1. **Blockchains use a variety of governance models**, including benevolent dictatorships; oligarchies; stakeocracies; federations; representative meritocracies; meritocracies; and democracies. Many of these

models are supplemented with steering or advisory committees that provide guidance, but not decision rights. Each governance model has its advantages and disadvantages.

2. **Different stakeholders prefer different governance models**. In public blockchain applications like Bitcoin and Ethereum, stakeholders include a variety of participant types, such as miners; software developers; users; exchanges; hardware providers (e.g. mining equipment manufacturers); software providers (e.g. digital wallets); and regulators. In a private blockchain, like TradeLens, participants include ocean carriers; ports; terminals; government authorities; inland transportation; 3rd party logistics providers; cargo owners; freight forwarders; customs brokers; and financial institutions. We must consider how different governance choices influence and incentivize each stakeholder's behavior.

3. **Blockchain governance is multifaceted**; decision rights need to be defined for various aspects of a blockchain system, such as network access; data use; data ownership and control; the role of validator nodes; software updates; ledger overrides; funding models and more.

4. **Different governance models may be used to govern different aspects of a blockchain ecosystem.** Each blockchain ecosystem may end up with a portfolio of governance structures. For example, Bitcoin has a meritocracy as far as updating the Bitcoin Core, but each miner democratically decides whether or not to adopt the changes.

5. **Blockchain governance evolves**, often progressing from centralized to decentralized, and from simple to complex governance arrangements.

While our focus is on helping enterprises think through shared blockchain governance, we illustrate maximums and detail governance practices across a variety of blockchain applications including public blockchains like Bitcoin; Ethereum; EOS; Monero; and Stellar, as well as private blockchains like MedliLedger; TradeLens; the IBM Food Trust; WineChain; and the Libra Association. Appendix B provides an overview of these blockchains.

2. Governance models

> *"A neutral facilitator, who can establish trust among parties, can serve as a benevolent dictator—at least initially—because they are incentivized to solve the problem for everyone."*
>
> Susanne Somerville, CEO of Chronicled and co-founder of MediLedger

> *"We think that the TradeLens Advisory Board, as well as standards bodies, such as the Digital Container Shipping Association, will help accelerate the effort [to digitize the supply chain]."*
>
> The Chief Digital & Information Officer of MSC[5]

If one looks at the formation of blockchain applications and projects, the following governance structures operate in practice: benevolent dictatorships; oligarchies; stakeocracies; federations representative meritocracies; meritocracies; and democracies (see Table 1).

Governance structures have varying degrees of decentralization (see Figure 1) and have different advantages. ***The benefits of centralized decision-making include swift decisions, quick execution, high efficiency, and clear control and accountability***. Users have an identifiable person or group to address questions, concerns, or complaints. Issues that arise—such as the discovery of a software bug or an attack on the blockchain network—can be dealt with swiftly. Centralized governance, however, is antithetical to the principles and purposes of blockchains, which aim to dissipate power across a network of independent nodes. It makes little sense, for example, for a single organization to control the majority of nodes on a blockchain network—traditional database technologies would better serve this scenario. The main argument for centralized governance is to get a blockchain ecosystem launched with a core set of enthusiastic founders. Founders, however, need to commit to a plan for moving to more decentralized governance in order to attract a critical mass of additional adopters.

The benefits of decentralized decision-making are inclusion; individual empowerment (every voice counts); unity around decisions; individual freedom to join and leave; and low abuse of power. Bitcoin—the very first blockchain application designed, developed and launched by Satoshi Nakamoto in 2009—was founded on Cypherpunk and Libertarian values.[6] After the 2008 Global Financial Crisis—possibly the greatest economic disruption since the Great Depression of 1929—people became increasingly distrustful of financial institutions. Movements like Occupy Wall Street ranted against wealth inequality and the influence of large financial intuitions on government policy. People rallied against the government's power to control money.[7] Bitcoin aimed to create a peer-to-peer payment application that relied on cryptography and computer algorithms—rather than governments and financial institutions—to ensure individuals authorized payments, and that their accounts (called addresses) are funded before value is transferred.

At the beginning of many projects—including Bitcoin—control is often centralized to either the founder (if launched by an individual) or to a small group (if launched by a team). If launched by an individual, the founder serves as a ***benevolent dictator*** over the mission, and often over the initial source code. Examples of benevolent dictators at the launch of a project included Satoshi Nakamoto over the Bitcoin whitepaper and Bitcoin Core and Vitalik Buterin over the idea for Ethereum.[8] These projects succeeded because the earliest of adopters—typically other like-minded coders—trusted the founders' intentions, even in the interesting case of Bitcoin where we do not know the identity of Nakamoto. Nathanial Popper, reporter for the *New York Times*, wrote, *"Satoshi's anonymity, if anything, seemed to increase the level of faith in the system. The anonymity suggested that Bitcoin was not created by a person seeking personal fame or success."* [9]

If launched by a team, blockchain governance likely begins as an **oligarchy***,* where power rests with a few. Most permissioned blockchains are being developed by a core group of partners, sometimes referred to as the minimal viable ecosystem (MVE). These partners—often comprising competitors as well as trading partners—form some sort of a council charged with developing and enforcing the rules for the initiative. By their very nature, the rules represent a negotiated treaty among the founding partners, maximizing their benefits. Founders will likely need to alter rules as they seek to attract additional partners.

Table 1: Governance Models

Governance model	Who has voting/decision rights?	Examples
Benevolent Dictator	A single person holds decision making rights, even when seeking input from others	• Initially, Satoshi Nakamoto, over the Bitcoin whitepaper and Bitcoin Core • Initially, Vitalik Buterin over the idea for Ethereum • Initially, Maersk over the precursor of what would become TradeLens
Oligarchy	A few people or institutions hold decision making rights, even when seeking input from others	• Satoshi Nakamoto willingly gave Martti Malmi and Gavin Andresen access rights to update Bitcoin's website and source code[10] • Buterin cofounded Ethereum with Mihai Alisie, Amir Chetrit, Charles Hoskinson, and Anthony Di Iorio, and soon brought on Joseph Lubin, Gavin Wood, and Jeffrey Wilke[11]
Stakeocracy	'Pay to Play'; People/institutions' votes are weighted by the size of their investment	• The Libra Association refers to its decision-making process as 'proportional power', where voting powers of the council will be proportional to their stake
Federation	Decentralized groups specialize on parts of the project while coordinating with a central group	• The Hyperledger Project's overarching structure is a set of specialized projects
Representative Meritocracy	People/institutions who have proven their merit are eligible to be elected to a council based on votes from other meritorious members	• The Hyperledger Project's Technical Steering Committee is governed by 11 elected people from a pool of active contributors
Meritocracy	Power is held by people based on one's ability	• The Bitcoin community (miners, developers, and investors) vote on Bitcoin Improvement Proposals (BIP) based on the merit of the proposal
Democracy	Any participant can vote	• Bitcoin and Ethereum miners 'vote' by either installing or failing to install changes to the source code
Steering/Advisory Committee	Committees typically support other governance structures by providing advice and guidance	• IBM Food Trust has an Advisory Board of nine members from across the food industry as of mid-2019

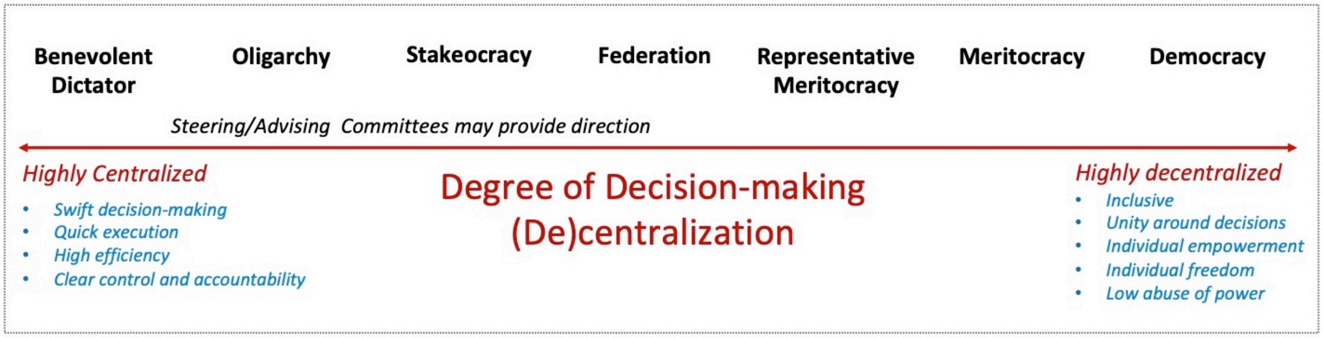


Figure 1: Blockchain Governance Models

'Staked' oligarchies, which we call ***'stakeocracies',*** is a governance model where people pay to become part of the oligarchy. Libra, the new token initiated by Facebook, is governed by the Libra Association. Council members (so far there are 28) need to buy *at least* $10 million in Libra Investment Tokens. The Libra Association refers to its decision-making process as 'proportional power', where voting powers of the council will be proportional to their stake, but with a cap to prevent an overtaking of the association.[12]

Federations allow decentralized groups to specialize on parts of the project while coordinating with a central group to integrate solutions. The Hyperledger Project's overarching structure is a set of specialized projects. However, the Hyperledger Project's Technical Steering Committee is governed by what can be called a ***representative meritocracy***, where people have to prove their merit to be eligible for election to the committee based on votes from other meritorious members. Working group leaders for Hyperledger's projects submit active contributors (there were 424 as of the last election) and all active participants vote to elect the 11 leaders. The 11-person Technical Steering Committee has decision rights over the admission of new projects, rules over projects, and status of projects (incubation/active).[13]

A ***meritocracy,*** where power is held by many people, based on one's ability (and goodwill), seems the ideal many strive for, particularly in open source projects. The aim is to elicit multiple views from informed stakeholders, debate views in open forums, and then stress-test ideas to find the best solution. Anyone, for example, can propose ideas to the Bitcoin Improvement Proposal (BIP). The whole Bitcoin community (miners, developers, and investors) can vote on the proposal based on its merit. As of this writing, 322 BIPs had been submitted, of which 35 had been finalized.[14]

A ***democracy*** is the most decentralized form of governance, where one participant gets one vote. That's why many people like the fact that Bitcoin and Ethereum miners 'vote' by either installing or failing to install changes to the source code.

In addition to the governance structures covered above, enterprise blockchains often use a ***steering committee*** or an ***advisory committee***. These committees typically do not have decision-making rights, but are nonetheless influential in guiding, recommending, and providing expertise on the development of the blockchain. Often used in conjunction with centralized governance structures, steering/advisory committees help ensure that decisions are transparent (at least to the members). The IBM Food Trust, MediLedger, and TradeLens rely on such committees for direction.

The IBM Food Trust—a platform for the global food supply chain—has an advisory council, comprising nine members as of July 2019: Walmart; Dole; Nestlé; Kroger; Carrefour; Danone; Driscoll's; Golden State Foods (GFS); and GS1. According to its website: "*An Advisory Council comprised of a range of industry representatives helps set the rules of engagement for the blockchain community, ensuring that the solution benefits all.*"[15] Council members *"share, learn, discuss, prioritize and address the opportunities and* *challenges relevant to the food industry globally. They actively learn from each other and the market to provide meaningful direction to IBM Food Trust."*[16] The chair of the Advisory Committee is elected for a two-year term by the other council members.

Founded by Chronicled, MediLedger is building in partnership with life science companies— manufacturers, wholesalers, dispensers, group purchasing organizations, and solution providers—an open and decentralized network for the pharmaceutical supply chain. MediLedger has a steering committee that serves as the final word on any issue that could not be resolved with working teams, project managers, or the network owner. So in this example, the steering committee *does* have decision-making rights.[17]

TradeLens—Maersk's major initiative to track cargo container shipments with IBM—was in the process of forming an Advisory Board comprised of ecosystem partners in July 2019. Members will likely include competitors like CMA CGM, MSC Mediterranean Shipping Company, Hapag-Lloyd, and Ocean Network Express (ONE).[18] According to the TradeLens website, *"This advisory board will work with TradeLens leadership to address key issues such as the use of open and fair standards. The board will also provide ongoing feedback to ensure all members have a voice in and benefit from platform development and growth."*[19]

In summary, there are a number of blockchain governance models. For a given blockchain ecosystem, several structures might be used because governance over a blockchain ecosystem is complex and ever evolving.

3. Facets of blockchain governance

> *"TradeLens has different types of participants, such as network members, cargo owners, clients, financial institutions. Our approach was to try and make sure that we had a unique value proposition and rules crafted for each different category of network member."*
>
> Aaron Lieber, Head of Offering Management, TradeLens, IBM

Blockchain governance is multifaceted. While some pundits primarily focus on two types of governance, namely the *rules of the protocol* as embedded in the code base and the *economic incentives* to attract adopters (and keep them honest)[20], governance is more complex, particularly for permissioned applications. Thus far, we've identified—with input from the Executive Advisory Board for the Blockchain Center of Excellence at the University of Arkansas—the following facets of blockchain governance: mission; rights of participation; rights of validation; data policies; rights of overrides; rights of ownership and liability; software update control; governance residence (on-chain or off-chain); and the funding model. Each facet may be overseen by a different governance model, forming a governance portfolio. A comprehensive governance portfolio needs to provide answers to the following questions:

1. **Mission:** What is the mission of the blockchain? Who is/are the founder(s)? Are the founders trustworthy?
2. **Rights of participation:** Who can join? Who can submit transactions? Who decides, or what is the process, to banish a participant?
3. **Rights of validation:** Who is allowed to operate the validation nodes in the network? Who operates the nodes today? Are the individuals or institutions that operate nodes truly independent and unlikely to collude? Who decides, or what is the process, to banish a node?
4. **Data policies:** What data is collected? Who can view data? Who decides how data can be used?
5. **Rights of overrides:** Who is allowed to submit counter transactions, which essentially reverse transactions? Who is authorized to roll back the ledger in the instance of egregious errors? (i.e. Who has the power to create a hard fork?)
6. **Rights of ownership and liability:** Who owns the data on a shared ledger? Who owns the software? Who is liable if a law is violated or a regulation is not followed?
7. **Software update control:** Who decides what patches and functionality will be added and when? How are software changes distributed to nodes?
8. **Governance residence:** What governance, if any, is on chain so that majority-rule decisions are automatically adopted (e.g. EOS, Cosmos), verses off-chain governance that requires human intervention (e.g. Bitcoin, Ethereum)?
9. **Funding model:** Who funds the project? Who decides who pays what? Who decides the pricing model (including transaction fees)?

We now consider each of these facets more thoroughly.

3.1. Mission

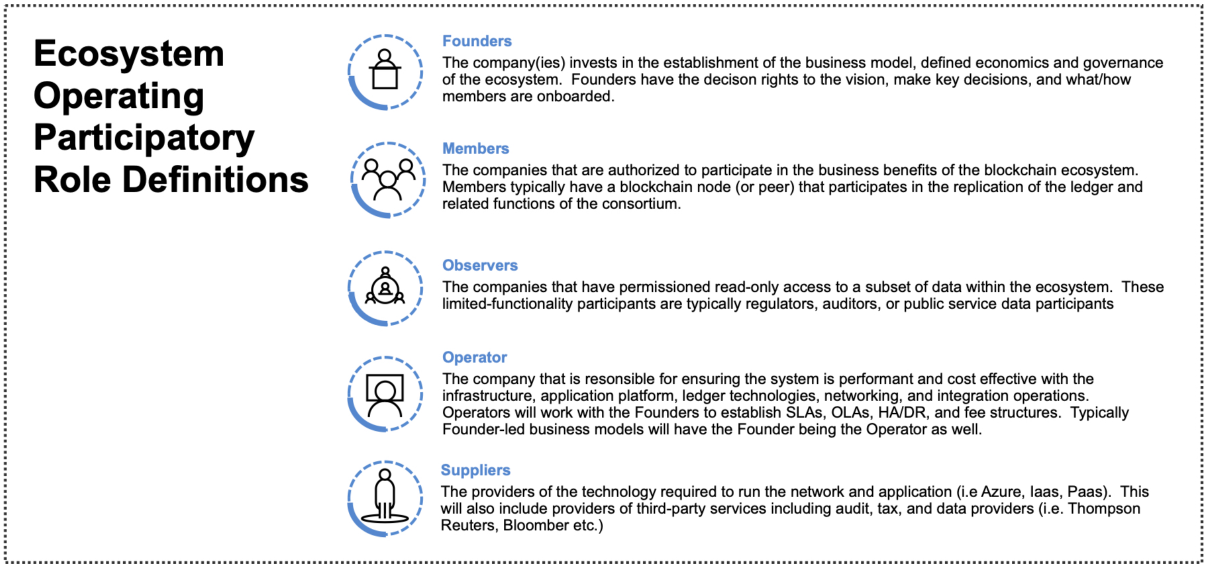
A formal mission statement should express the aspirations and values of the blockchain. A blockchain's mission should be used to guide governance choices. Furthermore, a compelling mission can keep members engaged—particularly when facing significant obstacles—and can inspire others to join the network. In general, ***a mission should appeal to a greater good beyond the founders.*** Table 2 includes examples of blockchain missions.

Table 2: Sample Blockchain Mission Statements

Blockchain	Description	Mission
Chronicled, founder of the MediLedger Project	A blockchain-enabled network solution for pharmaceutical industry	*"We're on a mission to bring more trust into supply chains by facilitating the creation of trusted and fully decentralized industry ecosystems - and by designing and building the tools to support them."* [21]
IBM Food Trust	A blockchain-enabled solution for food industry	*"IBM Food Trust, a blockchain-enabled global network of food chain participants, securely connects supply chain data across the ecosystem with trust and transparency. Food Trust connects the diverse food ecosystem, enabling increased efficiency, automated supply chain visibility, and strengthened consumer relationships from farm to store."* [22]
Libra Association	The association overseeing the Libra token, Libra reserve, and software	Libra's mission is *"… a simple global currency and financial infrastructure that empowers billions of people. Reinvent money. Transform the global economy. So people everywhere can live better lives."* [23]
Monero.Org	Created by a 'group of enthusiasts' of the cryptocurrency	*"We strongly believe in the future, where money, as an entity, is completely decentralized without being under control of any organization. This idea brings us to the ability of a new, fully transparent economic paradigm, built on laws of demand and supply rather than political intentions, financial manipulations and personal interest of small privileged groups."* [24]
Ripple	Company overseeing the Ripple network for global currency exchange	*"Enabling the world to move value like it moves information today."* [25]
Stellar Development Foundation	Non-profit foundation overseeing the Stellar protocol	*"The mission of the Stellar Development Foundation (SDF) is to promote global financial access, literacy, and inclusion. SDF accomplishes this by expanding worldwide access to low-cost financial services through the development and maintenance of technology and partnerships."* [26]
TradeLens	A blockchain-enabled solution for shipping industry	*"TradeLens is an open and neutral platform to help set trade free. TradeLens is a platform for digitizing and transforming trade for the benefit of industry and authorities all along the global supply chain. It offers a more open, trusted, transparent and secure way to conduct the business of trade."*[27]

3.2. Rights of participation and validation

Rights of participation define who is allowed submit transactions to the blockchain network. **Rights of validation** define who is allowed to run validator nodes in the blockchain network. The rights of participation and validation may vary by stakeholder type. In public blockchain applications, stakeholders include a variety of participant types, such as miners; software developers; users; exchanges; hardware providers (e.g. mining equipment manufacturers); software providers (e.g. digital wallets); and regulators. In private blockchains, Microsoft distinguishes among a variety of participants, including founders, members, observers, operators, and suppliers (see Figure 2).



Ecosystem Operating Participatory Role Definitions

Founders
The company(ies) invests in the establishment of the business model, defined economics and governance of the ecosystem. Founders have the decison rights to the vision, make key decisions, and what/how members are onboarded.

Members
The companies that are authorized to participate in the business benefits of the blockchain ecosystem. Members typically have a blockchain node (or peer) that participates in the replication of the ledger and related functions of the consortium.

Observers
The companies that have permissioned read-only access to a subset of data within the ecosystem. These limited-functionality participants are typically regulators, auditors, or public service data participants

Operator
The company that is resonsible for ensuring the system is performant and cost effective with the infrastructure, application platform, ledger technologies, networking, and integration operations. Operators will work with the Founders to establish SLAs, OLAs, HA/DR, and fee structures. Typically Founder-led business models will have the Founder being the Operator as well.

Suppliers
The providers of the technology required to run the network and application (i.e Azure, Iaas, Paas). This will also include providers of third-party services including audit, tax, and data providers (i.e. Thompson Reuters, Bloomber etc.)

Figure 2: Blockchain Participants

(Source: Microsoft, with permission)

At a very high level, rights of participation are either open to the public or private; rights of validation are either permissionless (anyone may operate a validator node) or permissioned (an individual or institution needs permission or must be selected/voted upon to run a validator node). However, there are nuances; EOS, for example, distinguishes between node validators—which anyone may run—and block producers, which must be voted upon using delegated proof-of-stake (dPoS) (see glossary). Permissionless blockchains need strong incentives to attract independent, 'well-behaving' validator nodes. Bitcoin and Ethereum rely on proof-of-work (see glossary) to incentivize good behavior. The more validators, the more secure the network. As of July 2019, Bitcoin had 9,705 reachable nodes;[28] Ethereum had 7,748 nodes.[29] Many permissioned blockchains rely on some form of Practical Byzantine Fault Tolerance (PBFT) consensus mechanism (see glossary). Permissioned nodes take turns validating the next set of transactions to the digital ledger. Consensus is reached when '*n* out of *m*' nodes reach agreement for that turn, typically '2 out of 3' for many Hyperledger Fabric applications; '4 out of 5' for Ripple.[30]

A Practical Byzantine Fault Tolerance (PBFT) consensus mechanism functions properly if:

- ***enough nodes operate to ensure fault tolerance (but not so many nodes that performance suffers);***
- ***nodes span nations to minimize the risks of censorship and government shutdowns;***
- ***nodes span geographies to minimize threats from a natural disaster;***
- ***nodes span multiple entities from across different sectors with low likelihood of colluding;***
- ***node operators are respected and trusted.***[31]

Plotting these two dimensions yields four types of blockchain networks (see Table 3):

1. **Public-permissionless** networks, like Bitcoin, Ethereum, and Monero.
2. **Public-permissioned** networks, like Ripple, Libra (still under development), and EOS (for block producers)
3. **(Virtual) Private-permissionless** networks, like EY Ops Chain Public Edition (still under development); and
4. **Private-permissioned** networks, like MediLedger, the IBM Food Trust, and TradeLens.

Table 3: Types of blockchain networks

		Who can operate a validator node?	
		Permissionless *(Anyone)*	**Permissioned** *(Requires permission, selection, or election)*
Who can submit transactions?	**Public** *(Anyone)*	**Public-permissionless** • Bitcoin • Ethereum • Monero • EOS (node validators)	**Public-permissioned** • Ripple • Libra • EOS (block producers)
	Private (*requires keys to access*)	**(Virtual) Private-Permissionless** • EY Ops Chain Public Edition (under development)	**Private-permissioned** • MediLedger • IBM Food Trust • TradeLens

Next, we examine the four types of blockchains in more detail.

3.2.1. Public-permissionless blockchains

With public-permissionless blockchains, anyone can participate, and anyone can run validator nodes. Bitcoin and Ethereum are the most popular permissionless blockchains. To transact on public-permissionless blockchains, users need some sort of application interface (such as a digital wallet). Anyone may run a validator node by downloading the source code and turning on the mining function. (Although Bitcoin miners need specialized Application-Specific Integrated Circuit (ASIC) hardware to competitively mine). Many enterprises will not adopt public-permissionless blockchains because of increased non-compliance risks. However, many cryptocurrency exchanges now comply with Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations, so enterprise adoption may accelerate.

3.2.2. (Virtual) Private-permissionless blockchains

For a long time, virtual private-permissionless blockchains were deemed to be either theoretical or nonsensical.[32] Theoretically, people described that a private-permissionless blockchain could exist, say, by deploying a smart contract on a permissionless network that restricts access and use to specific public keys.[33] In 2019, Ernst & Young (EY) took a major step to making it a reality; it launched Nightfall on Github.[34]

Nightfall is a set of protocols that provides private transactions on public Ethereum. Nightfall integrates a set of smart contracts, microservices, and zero knowledge proofs (see glossary) *"to enable standard ERC-20 and ERC-721 tokens to be transacted on the Ethereum blockchain with privacy. It is an experimental solution and still being actively developed."* [35] [36] In essence, EY's idea is a 'virtual private blockchain', similar to a virtual private network (VPN) that is connected to the public Internet, but data remains private from anyone not authorized to see the transaction. Authorized users, for example an organization's auditor or tax authority, will be able to decipher the data only with the right encrypted key.

EY's Ops Chain Public Edition, aims to use Nightfall by late 2019, early 2020.[37] Paul Brody, head of EY's Blockchain Technology, said, *"Blockchain technology holds tremendous promise to bring in a new era of transparency, accountability and efficiency in business. I am working to make sure that happens and, in particular, to ensure that open, decentralized and truly public blockchains are successful."* [38]

3.2.3. Public-permissioned blockchains

With public-permissioned blockchains, anyone can transact, but node validators are selected. Ripple, EOS and Libra are notable examples.

Ripple is a decentralized, real-time settlement system. Anyone can transact on the Ripple network by using a digital wallet or engaging a gateway partner, which are mostly financial institutions. Institutional customers use an API to connect to the Ripple network via a Ripple Gateway. When institutions join the ripple network, they can select which nodes they want to perform validation checks, which is called a Unique Node List (UNL), or they can accept the default list maintained by Ripple. Ripple maintains its own validator nodes around the world and also has CGI and MIT as transaction validators.[39] Without the incentives of mining, Ripple asks intuitions to run a validator node when they join the system to help secure the network.

EOS was developed to keep all of the advantages of a public blockchain platform—open, secure, decentralized; but without the latency, scalability, and resource intensity. Anyone can transact on EOS. Anyone can operate a validator node if they meet minimal criteria.[40] However, only 21 'block producers' can add blocks. The block producers are selected by a delegated proof-of-stake mechanism in which owners of EOS cast votes in proportion to their stake.[41] Block producers are rewarded with the issuance of new EOS tokens. Blocks are produced about every 500 milliseconds, with each of the 21 producers getting a turn. On the day of this writing, nine block producers were located in China, three in Singapore, and one or two in the Cayman Islands, BVI, Hong Kong, Japan, Ukraine, and the United States. Despite being globally distributed, publicly available, and providing a level of democracy in the selection of producers, concerns have been raised due to a large proportion of the producers being located in China. Even while attempting to develop a global, collaborative platform, localized biases and political concerns will arise and must be managed.

The Libra Association's project aims to launch in 2020. Any person will be able transact in the Libra network by accessing a digital wallet. Only Association members can operate validator nodes, which so far includes 24 companies, including Coinbase; eBay; Facebook/Calibra; Mastercard; PayPal; Spotify; Uber; and Visa. The Libra Association aims to recruit a total of 100 members to operate nodes in 2020. Finally—but with no concrete time horizon suggested—anyone will be able to operate a node when the Libra network matures into a fully permissionless blockchain.[42]

3.2.4. Private-permissioned blockchains

Private-permissioned blockchains are the most common enterprise blockchain solutions because they provide assurances of privacy, fast settlement times, resource efficiency, and regulatory compliance.

Permission is needed to participate and to operate validator nodes. MediLedger, the IBM Food Trust and TradeLens serve as examples of private-permissioned blockchains.

MediLedger, as noted above, is a block-enabled platform for the pharmaceutical sector. Qualified participants (such as licensed manufacturers and pharmacies) may join the network. Any qualified participant may operate a node, but it is likely that smaller players will engage a cloud provider or service provider to operate a node on their behalf. Consensus is reached through a proof-of-authority (PoA) (see glossary) mechanism, where the validator's identity is known, thereby staking the organization's reputation on preserving the network.[43] As the MediLedger network grows and as more participants operate nodes, it expects its consensus method will evolve from a PoA to a delegated PoA to avoid any latency issues.

IBM Food Trust platform relies on 'trust anchors' for validation using a Practical Byzantine Fault Tolerance (PBFT) consensus mechanism (see glossary). Trust anchors receive a full copy of the encrypted ledger but can only view the hashes of the transaction unless data owners grant access. Trust anchors are responsible for the following: [44]

- **Resource ownership**: Run accounts in tamper-resistant Z Secure Service Containers that ensure encryption of data, both in flight and at rest.
- **Verification**: Providing verification that events were submitted by an individual, with the corresponding hash.
- **Endorsement**: Trust Anchors can be added as endorsers to incoming transactions, providing an additional level of trust for the submitting company, such as private-label brands.
- **Data extractions**: In the event of an investigation, a member of the IBM Food Trust can use their decryption key and ask the Trust Anchors to extract the relevant data from the shared ledger and endorse its authenticity.

Initially, trust anchors were operated by IBM in IBM's cloud, but as the network grows, more participants will run trust nodes and possibly on other cloud environments.[45]

TradeLens. TradeLens is an open platform jointly developed by Maersk and IBM. The Beta release went live in January of 2018, and had over 100 participants by mid 2019 (see Figure 3). TradeLens, which is owned by Maersk, also relies on 'trust anchors'. Trust Anchors participate in consensus to validate transactions, host data, and assume a critical role of securing the network. So far, Maersk (via IBM's cloud environment) operates nodes; Hapag-Lloyd and Ocean Network Express (ONE) announced they will each operate a blockchain node.[46]

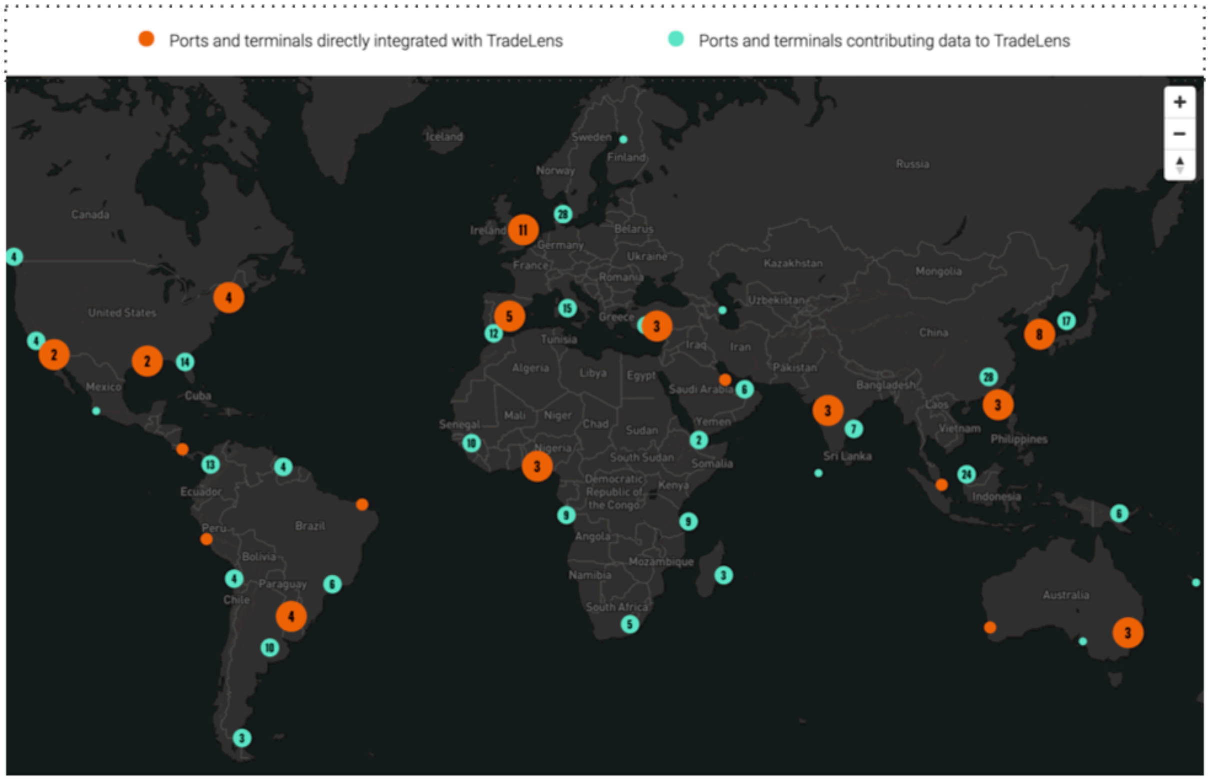
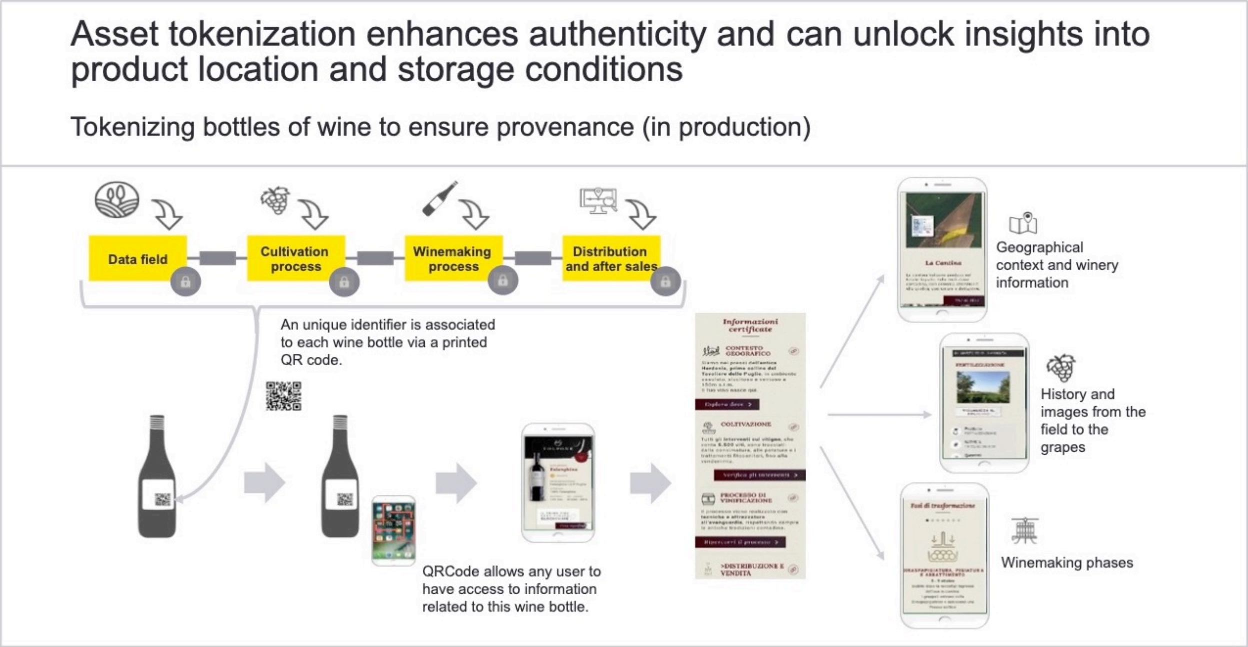


Figure 3: Screen shot of TradeLens Interactive Map of ports and terminals

(To view live interactive map of TradeLens, see [https://www.tradelens.com/ecosystem/)](https://www.tradelens.com/ecosystem/)

3.2.5. Hybrids

While Table 2 creates a helpful framework for categorizing blockchain networks, there are also hybrid blockchains. EY's WineChain serves as an example. EY developed WineChain to restore trust in the wine supply chain. Each wine bottle is tokenized with an Ethereum ERC721[(a)] non-fungible token (called WID), serving as a unique identifier.[47] The token is displayed as a QR code on the label (see Figure 4).



Asset tokenization enhances authenticity and can unlock insights into product location and storage conditions

Tokenizing bottles of wine to ensure provenance (in production)

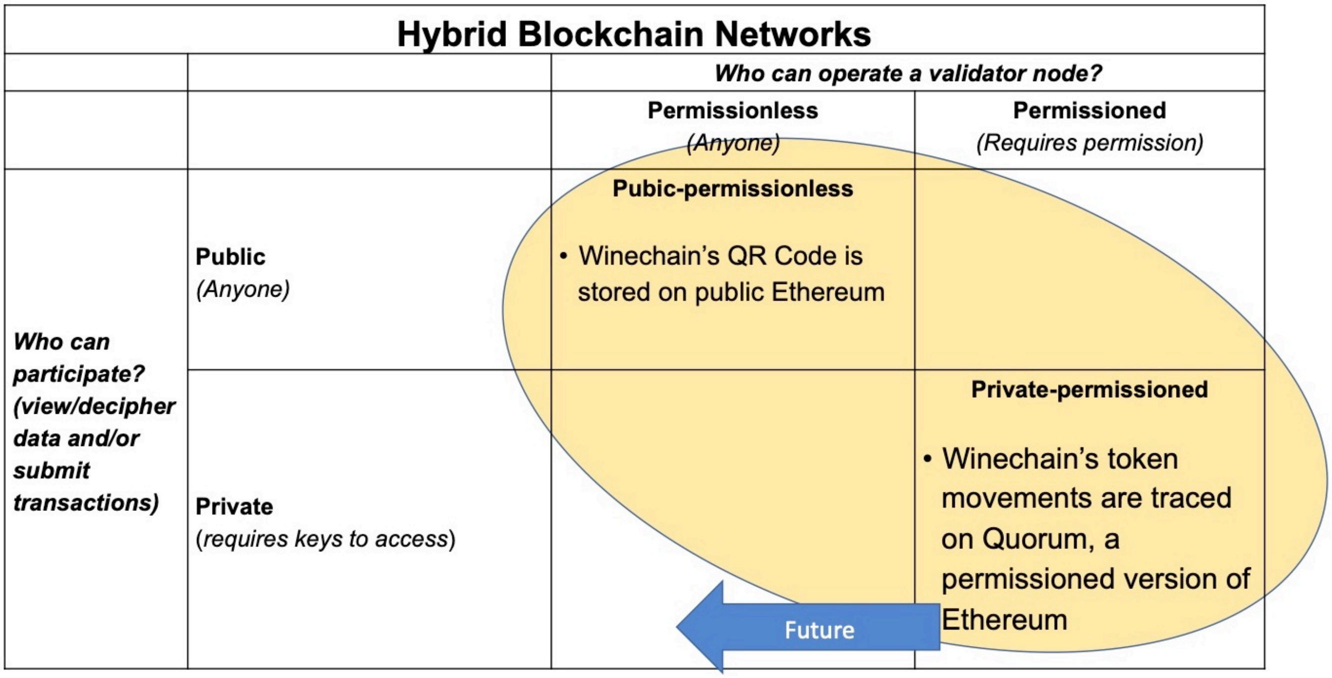
Data field
Cultivation process
Winemaking process
Distribution and after sales
An unique identifier is associated to each wine bottle via a printed QR code.
QRCode allows any user to have access to information related to this wine bottle.
Informazioni certificate
Geographical context and winery information
History and images from the field to the grapes
Winemaking phases

Figure 4: EY's WineChain Solution

(Source: EY, with permission)

There are two parts to the application, with one part running on public Ethereum, and one part running on a permissioned version of Ethereum called Quorum (see Figure 5). Hashes of the QR codes are registered on public Ethereum so that anyone who has access to the label on the bottle can make sure it is authentic. Furthermore, consumers can scan the QR code and go to a webpage that tells the story of the bottle, based on certifications stored on the blockchain. Consumers can learn about when and where grapes were harvested, bottling date, lot number, quality of sulphites, and other data. On Quorum, the blockchain is updated as the bottle moves through the supply chain of producers, brokers, importers, wholesaler, distributors, and retailers.[48] Specifically, the blockchain stores the transfer of tokens on the blockchain. Supply chain partners use digital wallets to store the private keys associated with the public addresses. Towards the end of 2019 or early 2020, EY hopes to have integration between this capability and Nightfall, enabling the same track and trace capability to run on a public blockchain (i.e. OpsChain Public Edition). The added benefits of transitioning these projects towards public blockchains, such as Ethereum, are (a) an ability to participate without investing in significant technology and hosting a node; (b) all relevant information remains on the public blockchain and available to all participants, even if the project fails or various individuals leave the project; and (c) an increased ability to leverage upcoming blockchain approaches and upgrades through community development so that the participants in the use-case specific network can focus on business rules, transactions, and governance and not the underlying development of a blockchain platform.

[(a)] An ERC721 token standard is *"a free, open standard that describes how to build non-fungible or unique tokens on the Ethereum blockchain. While most tokens are fungible (every token is the same as every other token), ERC-721 tokens are all unique."* (Source: http://erc721.org/)



Hybrid Blockchain Networks			
		Who can operate a validator node?	
		Permissionless *(Anyone)*	**Permissioned** *(Requires permission)*
Who can participate? (view/decipher data and/or submit transactions)	**Public** *(Anyone)*	**Pubic-permissionless** • Winechain's QR Code is stored on public Ethereum	
	Private (*requires keys to access*)		**Private-permissioned** • Winechain's token movements are traced on Quorum, a permissioned version of Ethereum

Figure 5: Winechain today is a hybrid blockchain

A number of clients are working with Winechain, including EXLab's AgriOpenData[49] and Blockchain Wine. Blockchain Wine, for example, is working with EY to develop and support the 'TATTOO' wine e-commerce, blockchain-enabled platform. TATTOO is an acronym for **T**raceability, **A**uthenticity, **T**ransparency, **T**rade, **O**rigin, and **O**pinion.[50]

3.2.6. Rights to terminate participants

> *"Consortiums with many members will present potential problems when attempting to define termination rights and triggers that are applicable globally to all members. Different members of a consortium sometimes have varying obligations, importance, and interests to the operations of a consortium. However, tailoring termination rights and triggers on a member by member basis, although a more desirable and equitable approach that takes into consideration the diversity of the consortium constituency, may become unwieldy and administratively burdensome if there are many members that have differing interests and roles."*
>
> Microsoft Blockchain Strategy Playbook

Who decides (or what is the process) to banish a participant or node? Most public blockchains automatically ignore a node whose hash of transactions does not match. Suppose, for example, a user operating one node changed a transaction so she could double spend from an address. The 'good' nodes would then be alerted to the change because the 'bad' node's hashed value will not match (see Figure 6)

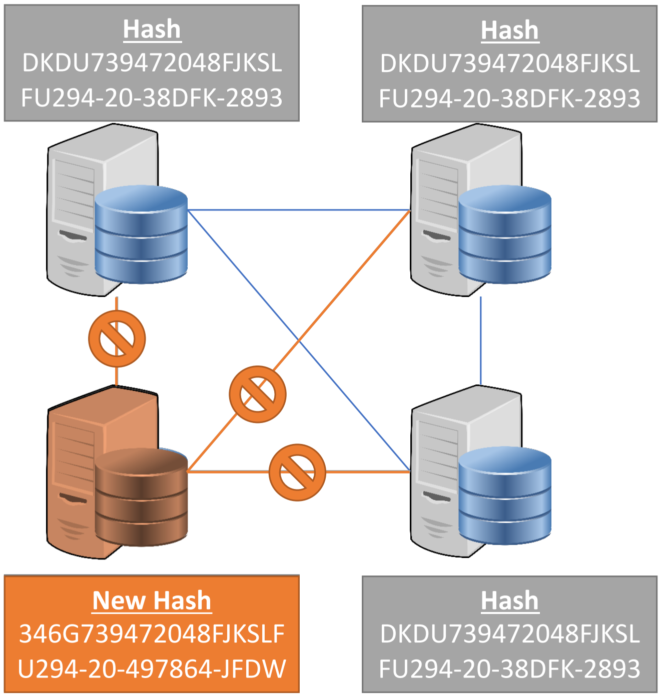


Figure 6: Automatic Exclusion of a Node

(Source: Dr. Zach Steelman)

In this figure, the node on the bottom left changed a transaction, so when all new transactions are combined with prior transactions, hashed, and compared with other peers, it will not match.

For permissioned blockchains, the governance structure should also define the process for removing a node. The Libra Association, for example, has this policy: any member whose node has *"not participated in consensus for ten consecutive days will be automatically removed."* The council has the authority to remove a council member with a super majority (2/3) vote. It's unclear what happens to the investment of a banished node operator.

3.3. Data policies

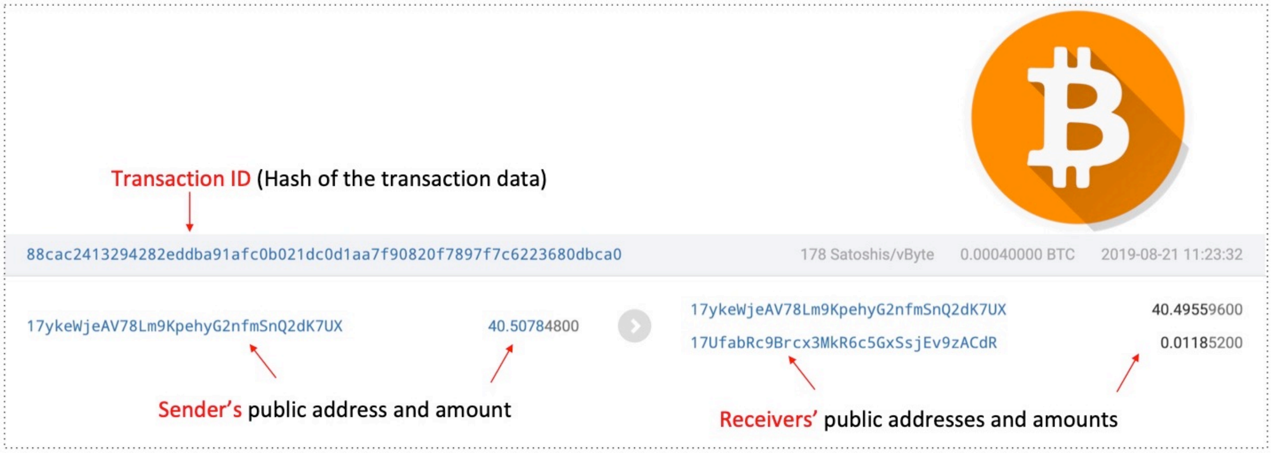
> *"Data is generally owned by the entity that published it. If that entity ends their participation, our contracts stipulate that we will remove the data published by that entity within a specific time period."*
>
> Aaron Lieber, Head of Offering Management, TradeLens, IBM

> *"The choice of data/information governance employed by a consortium will depend on the business objective and technical structure. For consortia that intend to leverage open-source development and/or open standards for data architecture, it may be preferable to look towards a United Nations Model. For consortia operating in a regulated environment, a benevolent dictator model may be beneficial. Read-Only Models are useful when information needs to be accessible to a large group and verifiable, but a smaller group has the ability to write or otherwise augment the data set."*
>
> Mike Walker, Sr. Director, Applied Innovation Team, Microsoft

Governance should also specify the data policies. What data is collected? Who can view data? Who decides how data can be used?

3.3.1. Public blockchains

For many public blockchains, the data stored on the public blockchain is visible to anyone with an Internet connection. People can view the full history of transactions on Bitcoin (https://btc.com/) (see Figure 7); Ethereum (https://eth.btc.com/); Ripple (https://xrpcharts.ripple.com/#/transactions); and EOS (https://bloks.io/). For these blockchains, anyone can view the public addresses used in a transaction, the transaction amount, and the validator's fees and rewards.



Transaction ID (Hash of the transaction data)

```
88cac2413294282eddba91afc0b021dc0d1aa7f90820f7897f7c6223680dbca0   178 Satoshis/vByte   0.00040000 BTC   2019-08-21 11:23:32

17ykeWjeAV78Lm9KpehyG2nfmSnQ2dK7UX   40.50784800   >   17ykeWjeAV78Lm9KpehyG2nfmSnQ2dK7UX   40.49559600
                                                       17UfabRc9Brcx3MkR6c5GxSsjEv9zACdR    0.01185200
```

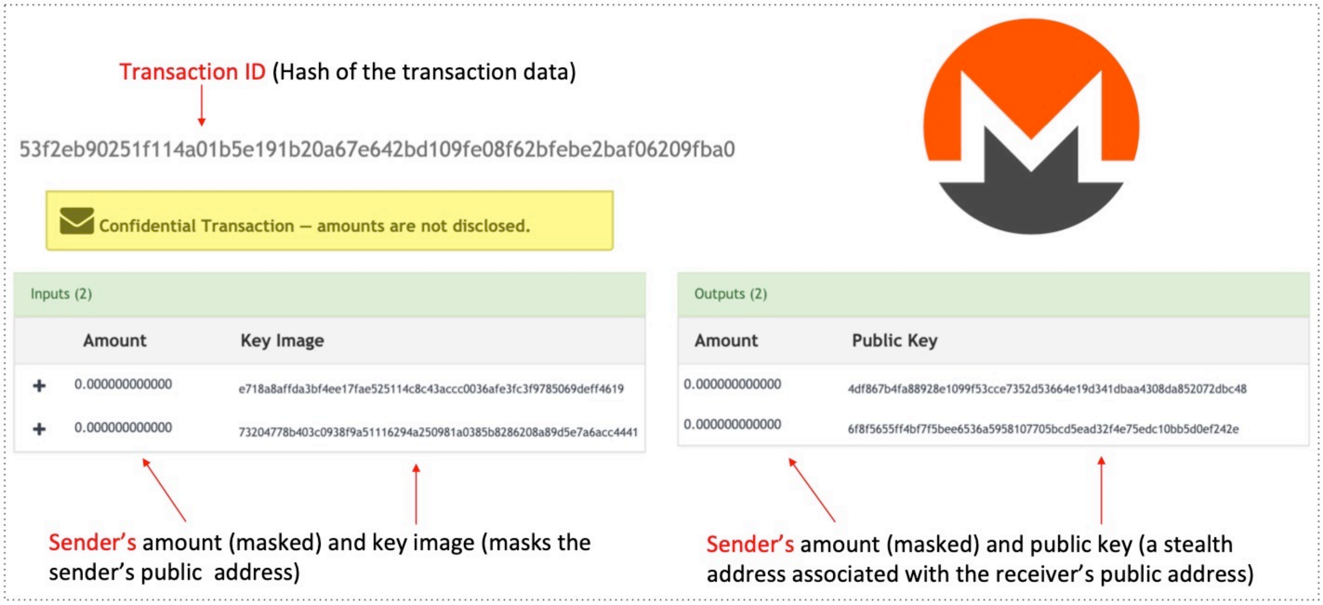
Sender's public address and amount

Receivers' public addresses and amounts

Figure 7: Data Observable on the Bitcoin Blockchain

In this figure, any person with access to the Internet may view transactions stored on Bitcoin's digital ledger. The identities of the public address holders are not known, except to the two parties of the transaction. However, one of the parties may follow all of the subsequent transactions associated with the addresses, which is why Bitcoin is considered to be 'pseudo-anonymous'. Furthermore, if the transaction was initiated through an exchange, the exchange likely will know the identity of the sending party because many exchanges now comply with KYC and AML regulations.

To increase data privacy, some permissionless blockchains like Monero (https://moneroblocks.info/) (see Figure 8), Zcash (https://explorer.zcha.in/), and the code released by EY's Nightfall, use advanced cryptography techniques like ring signatures, zero knowledge proofs, and key images. These methods allow only the parties to a particular transaction to decipher data and to access funds stored on the blockchain even when posted on a public blockchain.



Transaction ID (Hash of the transaction data)

53f2eb90251f114a01b5e191b20a67e642bd109fe08f62bfebe2baf06209fba0

Confidential Transaction — amounts are not disclosed.

Inputs (2)

	Amount	Key Image
+	0.000000000000	e718a8affda3bf4ee17fae525114c8c43accc0036afe3fc3f9785069deff4619
+	0.000000000000	73204778b403c0938f9a51116294a250981a0385b8286208a89d5e7a6acc4441

Outputs (2)

Amount	Public Key
0.000000000000	4df867b4fa88928e1099f53cce7352d53664e19d341dbaa4308da852072dbc48
0.000000000000	6f8f5655ff4bf7f5bee6536a5958107705bcd5ead32f4e75edc10bb5d0ef242e

Sender's amount (masked) and key image (masks the sender's public address)

Sender's amount (masked) and public key (a stealth address associated with the receiver's public address)

Figure 8: Transaction data stored on the Monero blockchain

In this figure, outside observers cannot decipher anything about the sender's or receiver's addresses or amounts transferred. Input addresses are masked with group signatures that display only a 'key image' that can only be used once in the future. Output addresses are masked with stealth addresses (called 'public keys' in the figure above). Amounts are masked with Ring Confidential Transactions (RingCT). Despite all the obfuscation, the protocol ensures that the sender's wallet has sufficient funds before transferring and recording the transaction on the blockchain.

3.3.2. Private blockchains

> *"There are rules around what information is shared and who have a link to it. That has been absolutely crucial to our ability to onboard clients and network members."*
>
> Aaron Lieber, Head of Offering Management, TradeLens, IBM

Within a private blockchain application, there are typically 'public' data that all approved network participants can view and 'private' data that only the parties to the transaction can submit and view. Quorum—the permissioned version of Ethereum—is an example (see Figure 9). In other protocols, like Hyperledger Fabric, there are no 'public' views, only channels for private views that must be configured and approved for each participant in the network.

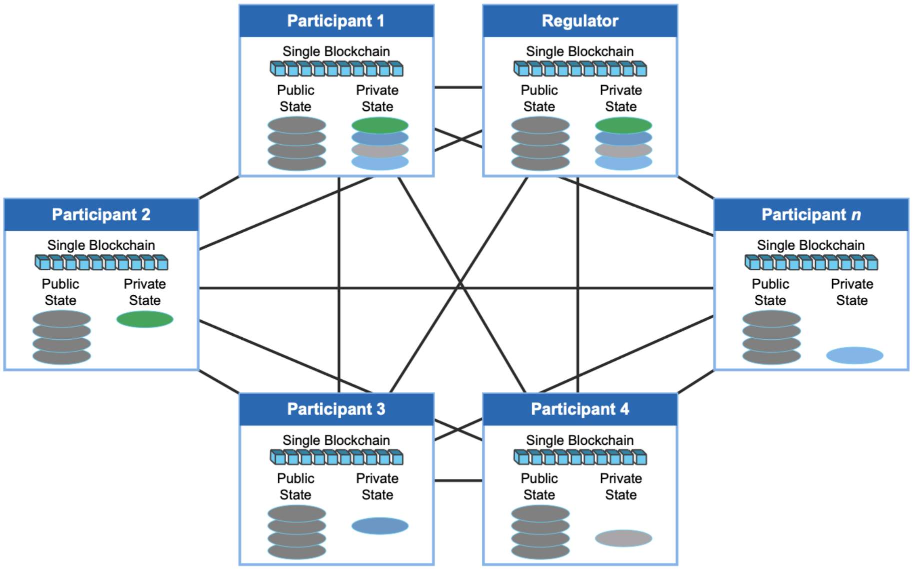
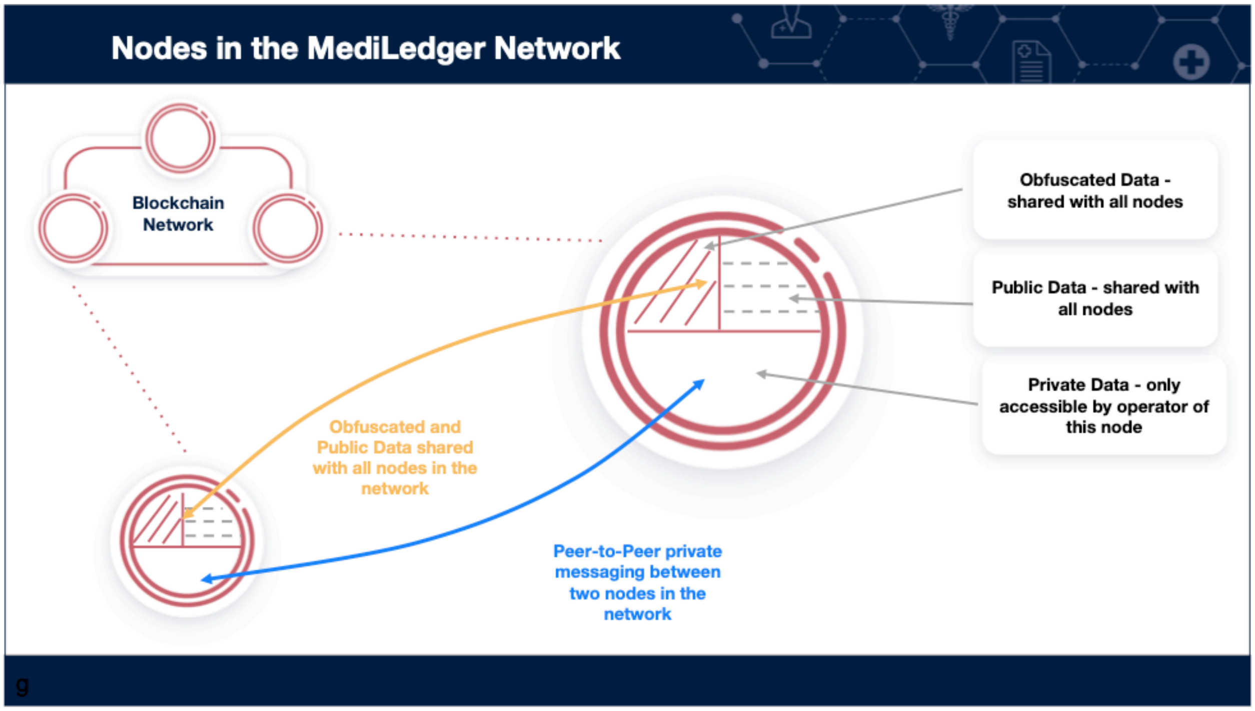


Figure 9: Quorum has public and private states stored on a single blockchain

(Source: Crosman 2017)[51]

MediLedger has approached data privacy from the philosophy of sharing as little data as possible while still realizing the expected business and social value. A MediLedger participant's node has three types of data: (1) public data shared with all nodes; (2) obfuscated data shared with all nodes; and (3) private data only accessible to the operator of the node (see Figure 10). Individual participants decide access rights to data. Susanne Somerville said, *"We don't want governance to decide the industry business rules or interpretation of business rules. We literally want companies to come with the rules they want, and we just implement them in software and code."* [52]



Nodes in the MediLedger Network

Blockchain Network

Obfuscated Data - shared with all nodes

Public Data - shared with all nodes

Private Data - only accessible by operator of this node

Obfuscated and Public Data shared with all nodes in the network

Peer-to-Peer private messaging between two nodes in the network

Figure 10: Nodes in the MediLedger Network

(Source: Chronicled, with permission)

The return verification application provides an example of this minimal data approach. A new regulation called the ‘Drug Supply Chain Security Act’ requires that all members of the pharmaceutical supply chain verify that returned pharmaceuticals are legitimate products of a licensed manufacturer.[53] The US government issued this law, in part, to help improve drug safety, as counterfeit or expired pharmaceuticals threatens people’s health. MediLedger’s return verification application only needs three readable data items to meet the regulation, namely: the company identifier, the medicine item numbers, and the URL end point where to request verification for that product. A smart contact ensures that only the manufacturer with the correct company identifier is allowed to add items to the look up directory. A wholesaler can submit a query to the manufacturer to ensure a returned item from a hospital, for example, is legitimate.

The right to be forgotten. Another issue is how to ‘delete’ select transactions, say when a participant leaves a network and requests that his or her data be removed, or to comply with ‘the right to be forgotten’ regulations, such as the General Data Protection Regulation (GDPR) passed by the European Union in 2016. Blockchains cannot physically remove individual transactions embedded within it, but there are solutions. Private data (such as a person’s identity) could be stored off-chain; or encryption keys to decipher the data stored on the ledger could be deleted, since such keys are always stored off-chain; or specific nodes could be designated to store all the transactions aimed to expire around the same time, upon which time the entire node could be deleted. Other solutions will also emerge. The main thing is to consider the ‘right to be forgotten’ *before* adopting a blockchain application.

3.4. Rights of overrides

Rights of overrides define who is allowed to submit counter transactions—which essentially reverse transactions—and who is authorized to roll back the ledger in the instance of egregious errors, i.e. who has the power to create a hard fork. A hard fork is a permanent, divergent path of a blockchain.

A hard fork is a highly contentious issue because it means that a blockchain ledger loses its property of immutability. In public blockchains, hard forks typically occur under two circumstances. First, someone may create their own blockchain or digital asset by copying and modifying source code. Second, hard forks can occur when the blockchain community disagrees on the rules of the next version of the protocol. For example, Bitcoin forked into Bitcoin and Bitcoin Cash when miners disagreed over a proposed upgrade in 2017. Bitcoin Cash was created to allow block sizes of up to 8 megabytes (MB), whereas Satoshi Nakamoto coded the Bitcoin Core to cap block sizes at 1 megabyte. In 2018, Bitcoin Cash split again over disagreements with extending the block size further. One branch became Bitcoin Cash (32 MB block size limit) and one branch became Bitcoin Cash SV (128 MB limit).[54]

In another example, Ethereum split into Ethereum and Ethereum Classic when the community disagreed about remediating the DAO hack. The DAO (Decentralized Autonomous Organization) is perhaps blockchain’s most ominous heist because its perpetrator(s) didn’t steal private keys from a digital wallet stored off a blockchain. Rather, the perpetrator(s) exploited a weakness in a smart contract launched on the Ethereum blockchain. The DAO was deployed in May of 2016. Despite the concerns some people voiced—like Professor Emin Gün Sirer of Cornell University—about the weaknesses in the code, money poured in.[55] The DAO raised $150 million worth of Ethereum’s native digital asset (ether), during its 28-day funding window, exceeding anyone’s expectations, as this represented 15 percent of the ether money supply. In June of 2016, a hacker (or hackers) exploited a weakness in the smart contract’s code. He, she or they began draining the DAO’s funds. The Ethereum community was powerless to stop it, as smart contracts run autonomously. The hacker syphoned $50 million in ether into another account. Vitalik Buterin, the co-founder of Ethereum, called for a complete stop in trading until the problem could be addressed. The price of ether fell immediately from $20 to $13.[56]

What should be done? Opposing views swarmed in: Vitalik Buterin wanted to *"freeze the account"*, which would require new code that had to be run by at least 50 percent of the nodes. Stephan Tual—Ethereum's Chief Compliance Officer—argued that the blocks should be unwound and that all the stolen ether should be returned to the investors' accounts.[57] Some members of the open source community insisted that ***nothing should be done***. The blockchain was not breeched; the coders of the smart contract did a poor job, so they should suffer the loss. Chat rooms were ablaze with analogies to the US federal government bailing out the banks during the Global Financial Crisis of 2008, and accused the Ethereum Foundation of acting like a government. The decision was made to let miners vote, weighing their votes by their hashing power. The miners voted for a hard fork, a permanent divergence in the Ethereum blockchain. The blocks were rolled back, and the stolen ether was returned. Those miners who refused to follow the fork proceeded mining with the original code, leaving us with Ethereum (fork followers) and Ethereum Classic (non-fork followers), where the thief can still cash out.

These stories from public-permissionless blockchains are highly relevant to permissioned blockchains. Clear procedures should exist for 'pulling the emergency brake' by forking the ledger. The Libra Association, for example, has the power to create a hard fork with a two third supermajority of votes. It might also have the power to issue counter transactions, a right that centralized parties like Mastercard and Visa exercise today.

3.5. Rights of ownership and liability

> *"As far as compliance, don't forget Bitcoin was designed to operate in an unregulated space. Now enterprises want to adapt the technology in highly regulated environments. We have to worry about things like subpoenas, record retention requirements, and compliance audits. If you receive a subpoena for somebody else's data stored on your copy of the ledger, do you have to respond?"*
>
> Scott Mooney, VP Distribution Operations, McKesson

Governance defines who owns the data on a shared ledger; who owns the software; and who is liable if the law is broken or if a regulation is not followed. Software liability laws are complicated, but in general, it's very difficult to hold authors of software liable. Courts have generally ruled that hackers, not software providers, are responsible for data breaches.[58]

3.5.1. Public blockchains

> *"Neither the data in the ledgers nor the software governing blockchain applications is claimed to be owned by anyone in particular."*
>
> Howell et al. (2018)[59]

For public blockchains, like Bitcoin and Ethereum, the public address data stored on the blockchain is a public good, and the private keys to control those public addresses are private goods, meant to only be in the possession of legitimate owners. The software is often owned by developers. For example, Bitcoin is copyrighted 2009-2019 by 'Bitcoin Developers'.[60] The Ethereum Foundation controls the Ethereum Core.[61] For public blockchains, the software is copyrighted with an open source software license such as GNU General Public License, MIT License, or Apache License. Bitcoin runs under an MIT License;[62] Ethereum is licensed under GNU.[63] Both have disclaimers of warranty and limitations of liability clauses.[64] [65]

3.5.2. Private blockchains

For private blockchains, most enterprise blockchain applications seem to operate under this rule: the organization that uploaded the data, owns the data and controls access to it. This holds true even when the software is proprietary**.** Table 4 provides examples of data ownership policies and software ownership for MediLedger, IBM Food Trust, and TradeLens. As far as liability, if the software is open sourced, it will have the same disclaimers of warranty and limitations of liability clauses. For example, The Libra Core is an open source code base that operates under the Apache 2.0 License.[66] For proprietary software, many software owners carry liability insurance.

Table 4: Blockchain Data and Software Ownership

	Data Ownership Policy	Software Ownership
MediLedger	'Company Controlled Data - By leveraging the blockchain and confidential data exchange, the Network is designed to ensure that each Participant's Private Data is owned by such Participant, and each Participant has full control of who and how it shares its Private Data.' [67]	Chronicled
IBM Food Trust	'Who owns the data? You upload, you own, you control. Your data belongs to you. Data is owned by the registered company or organization that owns the data prior to it being uploaded to Food Trust. Users can set permissions that govern what data can be seen and by whom – determined solely by the owner of the data. Data uploaded by a third party is owned by the original owner.'[68]	IBM owns the Food Trust Platform, but other service providers may build apps or services on top. Thus far, IBM has built three services: Trace, Certifications, and Fresh Insights
TradeLens	'A channel will be established for each node hosting organization. Sensitive information including documents are distributed only to those nodes participating in a channel; in addition, highly secure access control permissions guarantee that organizations only access information for which they are granted access. Documents are stored on a single node only and are accessed at runtime by other nodes on a channel as permissions allow.'[69]	'Maersk owns the intellectual property of the TradeLens platform'[70]

3.6. Software update control

Software update control is one of the greatest governance challenges for a shared application. ***Whether it's an emergency patch to remedy a newly-discovered software vulnerability, or a planned software release, the majority of validator nodes must choose to update the software for it to take effect.*** Decentralized software updates require a lot of planning and coordination.

Focusing on Bitcoin, any person may propose a change by submitting a Bitcoin Improvement Proposal (BIP) to Github.[71] Once proposals are reviewed and supported by Bitcoin developers, miners may be asked to vote using the following process: *'The proposal itself typically sets the requirements for agreement and adoption. For example, the proposal may say that a certain change requires the approval from a super-majority of miners (a typical number is 95%) during a given period (measured in blocks). Miners signal their support for a proposal by adding a line to the blocks they solve. Once the threshold is achieved, the proposal is said to be locked in, and it is activated at a predetermined later date.'*[72] However, a miner's vote is non-committal. It's more akin to a political pole as to how one intends to vole in an election. '*It is possible for proposals to secure support from a large number of miners and still be dropped. An example was the 2017 proposal called SegWit2x, which secured support from 100% of miners but was later dropped due to lack of consensus among different Bitcoin stakeholders.*'[73]

For this governance facet, centralization has the edge as far as expediency. The Libra Association, which will initially rely on a centralized governance model, invites anyone to submit ideas, code, and documents using a Contributor License Agreement (CLA). However, the Libra Association will be making the technology decisions, at least initially.[74] It will be able to decide software upgrades more quickly than the more decentralized governance models.

3.7. Governance residence

> *"I argue that 'tightly coupled' on-chain voting is overrated, the status quo of 'informal governance' as practiced by Bitcoin, Bitcoin Cash, Ethereum, Zcash and similar systems is much less bad than commonly thought, that people who think that the purpose of blockchains is to completely expunge soft mushy human intuitions and feelings in favor of completely algorithmic governance (emphasis on 'completely') are absolutely crazy…"*
>
> Vitalik Buterin, inventor of Ethereum[75]

> "*Most of our success is a lot of hard work; in the blockchain space, we talk about automatically executing smart contracts, but I spend a lot of time dealing with attorneys and good old-fashioned paper contracts to onboard participants."*
>
> Aaron Lieber, Head of Offering Management, TradeLens, IBM

Governance can be off-chain, on-chain, or a combination of both.

Human beings manage off-chain governance, and it is the structure with which we are all familiar. People govern cities, states, nations, institutions, clubs, consortiums, alliances, software, etc. While there may be encoded 'rules'—constitutions, bylaws, or contracts—people can change the rules, be it by vote, persuasion, or coups. As such, ***off-chain governance is alterable, allowing the governance model to evolve over time.*** Most blockchain governance is managed off-chain, whether its decisions over source code patches or updates, protocol changes, or membership changes. Given that governance structures tend to evolve, it seems ***off-chain governance is the lower-risk option***.

On-chain governance is a new option; ***on-chain governance is unalterable without a significant software fork or intervention approved by the majority of the participants***. It's meant to provide a guarantee—a programmed-in commitment, as it were—to how decisions will be made in the blockchain network now and in the future. EOS is its most visible poster child. It launched its blockchain network with guaranteed democratic voting rights. Whereas Bitcoin and Ethereum miners vote on changes, EOS shifted the decision rights from developers and miners to users. As of July 21, 2019, nearly 63,000 of 1.3 million EOS account holders participated in 1,030 votes taken since its launch, but the on-chain voting still remains at less than 5% of the total participants, indicating that not all participants in a blockchain may be an active participant in the governance process, but instead simply users of the developed platform.[76]

Other blockchain networks with on-chain governance include DFINITY (a blockchain-based cloud computing project aiming to reduce the costs of cloud computing); Tezos (a blockchain-based project aiming to improve smart contract safety); and Decred (a cryptocurrency like bitcoin but with on-chain governance). ***The arguments for on-chain governance are guaranteed inclusion and decentralization. The arguments against are unanticipated consequences; the inability to adapt; ill-informed voters; and low voter turn-out***. [77]

3.8. Funding model

“Follow the Money,”

Deep Throat, *All the President's Men*

“In order to have a decentralized database, you need to have security. In order to have security, you need to have incentives.”

Vitalik Buterin, Inventor of Ethereum[78]

“A common challenge in low co-specialization alliances is that a differentiated contribution that might be strategically vital to the alliance may not be financially feasible or attractive for the partner making that contribution.”

Yves L. Doz, Institut Européen d’Administration des Affaires [79]

Although we explore the funding model as the last facet of shared governance, it may be one the most important; ***funding often serves as the primary way to incentivize proper behavior in blockchain applications***. For example, Bitcoin and Ethereum incentivize miners with block rewards and transaction fees. In the original Bitcoin white paper, Nakamoto wrote that the mining reward: *“… may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favor him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.”* [80]

Initial Coin Offerings (ICOs) were a primary funding model where investors send money directly to a smart contract or an account controlled by the startup in exchange for digital tokens (i.e. cryptocurrency). With an ICO, investors are not buying shares in a company, which bypassed many onerous regulations—at least until mid-2018 when the US Securities and Exchange Commission began charging some ICO issuers. Mastercoin was the first ICO, which raised $5.5 million in 2014; Ethereum was the second ICO, which raised over $16 million that same year.[81] Block.one for EOS raised $4.1 *billion* in May 2018.

Startups typically explain how the funds will be used, such as the percentage that went directly to founders. For example, Ripple’s owners retained 20 billion ripples at launch and gifted the rest to Ripple, charged with distribution to gateways, market makers, and charitable organizations.[82] The worry was this: What prevents owners from cashing in and thus devaluing the currency? After years of concern, Ripple’s owners promised in May of 2017 to put 55 billion ripples into escrow and release about 1 billion into the market each month.[83]

Many startups funnel most of the funds into a non-profit foundation. Here, too, complexity is evident; at least ten generic nonprofit funding models are recognized: heartfelt connector; beneficiary builder; member motivator; big bettor; public provider; policy innovator; beneficiary broker; resource recycler; market maker; and local nationalizer.[84]

The Libra Association’s funding will come from an investment of at least $10 million in Libra Investment Tokens per council member, but only for the for-profit members. The validator nodes will collect transaction fees for securing the network. According to the technical report, the fees will be set by the sender (as it is in Bitcoin and Ethereum) using a gas price (the number of Libra Coins that the sender is willing to pay per unit of gas in order to execute the transaction) and a maximum gas amount the sender is willing to spend before halting the transaction. On the positive side, users appear to control fees inside the network; on the negative side, it is unclear how the validator nodes will prioritize transactions. In Bitcoin, for example, miners process the transactions with the highest fees first, which if adopted here, will disadvantage the low-income people Libra intends to uplift. At times of network congestion, will Libra's fees escalate like they do in public blockchains today? Additionally, services that interface with the network can also charge fees, such as digital wallets. Consumers will need a lot of market options to promote low service fees. People are concerned that Calibra (Facebook's digital wallet) will have an unfair competitive advantage.[85] It is early days, and the Libra Association's governance model will evolve.

4. Governance portfolio evolution

> *"Blockchain technology is coming to replace the old, rotten system of governance around the world. Embrace it!"*
>
> Olawale Daniel, principal consultant with Olda Consult[86]

> *"Enterprise corporations currently prefer private blockchains because they offer greater benefits in a secure environment for trading parties, including privacy, confidentiality, data governance, speed, and cost. As public blockchains prove their ability to effectively provide these attributes in a scalable, open-source setting, they will gain popularity in the industry and adoption will quickly proliferate."*
>
> Craig Harper, Executive VP and COO J.B. Hunt Transport Services, Inc.

> *"In terms of maintaining partner commitment in high co-specialization alliances, it is important to note the difficulty of equitably apportioning benefits to partners. Although they are mutually dependent for value creation, each partner will nonetheless measure the costs and benefits of its contribution against its own yardstick…To maintain loyalty across partners with such varying perspectives on the alliance, management needs to encourage partners' participation in collective decisions that influence the evolution of the alliance and drive collective prosperity."* [87]
>
> Yves L. Doz, Institut Européen d'Administration des Affaires [88]

How do governance portfolios typically evolve? Most blockchain applications/platforms/projects are launched by one, or a few, champions, serving as benevolent dictators. Initially, the champions have full control; they hold the access and decision rights, largely because there is no one else to delegate power to yet. Centralized decision-making can also expeditiously deal with the inevitable weaknesses in newly launched applications. But ***for blockchains to be successful in the long term, founders need to plot a trajectory towards more decentralized models from the beginning.***

The benevolent dictators of Bitcoin and Ethereum moved quickly distribute power fellow believers. Specifically, Satoshi Nakamoto willingly gave Martti Malmi and Gavin Andresen access rights to update Bitcoin's website and source code;[89] Buterin recruited Mihai Alisie; Amir Chetrit; Charles Hoskinson; and Anthony Di Iorio, and soon brought on Joseph Lubin; Gavin Wood; and Jeffrey Wilke, as co-founders.

The same rule applies to permissioned blockchains. Competitors and smaller-sized participants in the ecosystem are skittish of joining blockchain projects led by industry giants like Facebook, IBM, or Maersk. The industry giants need to purposely dissipate control to convince others they are working for the greater good, and not attempting to build their own competitive advantage within the network. IBM, for example, gave their rights away to control the source code for HyperLedger Fabric by giving it to the Linux Foundation to manage as open source. It is opening up its blockchain solutions to run on other cloud provider platforms.[90]

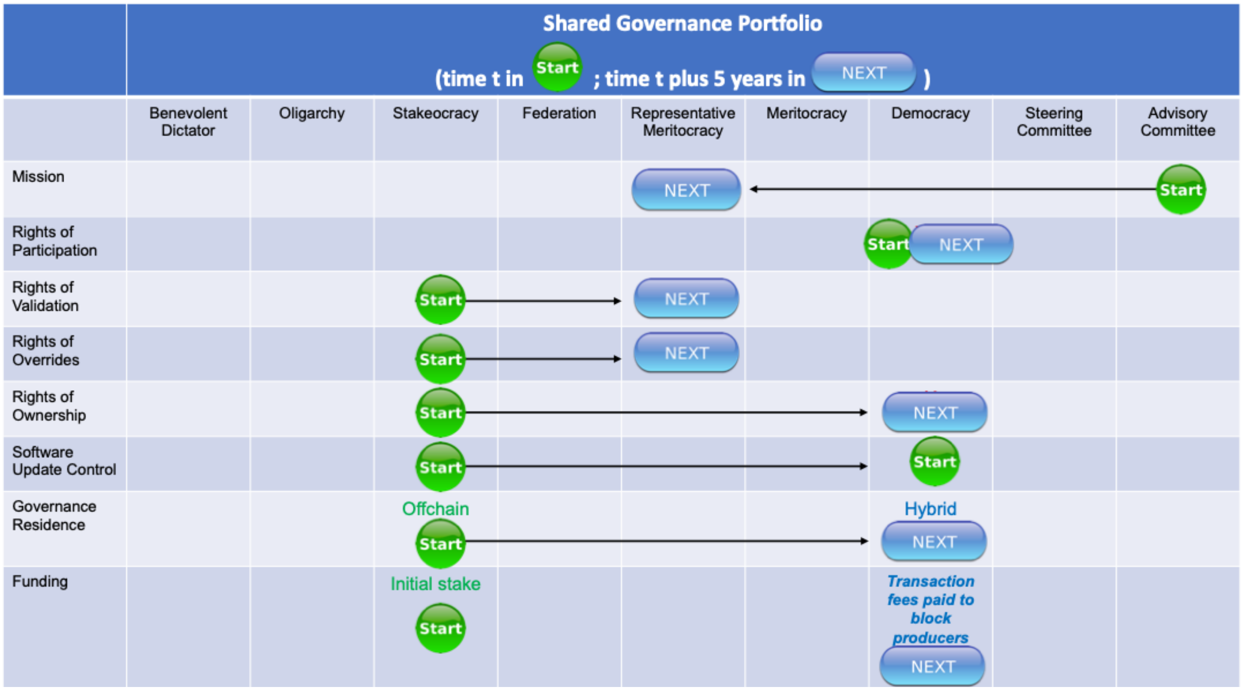
TradeLens provides another example of an evolving governance structure. Initially, Maersk was internally working on improving containerized shipping by itself in the wake of the Global Financial Crisis. In another part of Maersk, it was working with IBM on paperless trade (the digitization of shipping documents). In 2016, the projects were joined, and thanks to IBM's early foray into blockchain technologies, IBM showed Maersk the value of moving the project to a blockchain-enabled platform.[91] In January of 2018, TradeLens was announced as a 51/49 percent joint venture between Maersk and IBM.[92] Initially, each company intended to use their own sales channels, but IBM did not have the same global level of trade permissions as Maersk, so the TradeLens governance was changed again, this time to a subsidiary of Maersk in late 2018 with IBM as the solution provider. The next phase of governance involves more transparency and the creation of an Advisory Board to move to a more decentralized governance model.[93]

The Libra Association also intends to evolve its governance structure. Initially, Libra is governed off-chain by the Libra Association. It has plans to include on-chain governance for voting and changes over time as it evolves. Its white paper reads, *"Libra will start as a permissioned blockchain. To ensure that Libra is truly open and always operates in the best interest of its users, our ambition is for the Libra network to become permissionless. The challenge is that as of today we do not believe that there is a proven solution that can deliver the scale, stability, and security needed to support billions of people and transactions across the globe through a permissionless network. One of the association's directives will be to work with the community to research and implement this transition, which will begin within five years of the public launch of the Libra Blockchain and ecosystem."* [94]

Beyond these examples, how might enterprises think through governance evolution?

4.1. Example of portfolio evolution

Figure 11 provides a hypothetical example of governance portfolio evolution. Suppose the founders initially launch a blockchain application by agreeing to financially support the project with a stake, with power shared among the founders in proportion to their stakes.



Shared Governance Portfolio

(time t in Start ; time t plus 5 years in NEXT)

	Benevolent Dictator	Oligarchy	Stakeocracy	Federation	Representative Meritocracy	Meritocracy	Democracy	Steering Committee	Advisory Committee
Mission					NEXT				Start
Rights of Participation							Start NEXT		
Rights of Validation			Start		NEXT				
Rights of Overrides			Start		NEXT				
Rights of Ownership			Start				NEXT		
Software Update Control			Start				Start		
Governance Residence			Offchain Start				Hybrid NEXT		
Funding			Initial stake Start				*Transaction fees paid to block producers* NEXT		

Figure 11: Hypothetical Governance Portfolio Evolution

This figure shows an evolution from more centralized to less centralized governance

This 'stakeocracy' model enables efficient decision-making and control over the mission, rights of validation, overrides, ownership, and software update control (in Figure 11 the **green** 'Start' buttons indicate the initial governance model). An advisory committee may be used to ensure stakeholders are represented and stay informed. But for blockchains to be successful in the long term, founders need to plot a trajectory towards more decentralized models if they want to build the ecosystem to realize network effects. Returning to Figure 11, the founders may aim to move towards a representative meritocracy, where elected contributors guard the mission, hold rights of validation, overrides, and software update control. Some aspects of governance might move on-chain, resulting in a hybrid model. Funding models might also evolve to attract different types of participants (**blue** ‘Next’ buttons indicate the aspirational governance model.)

In summary, blockchain governance models should evolve by progressing from centralized to decentralized governance arrangements. ***Ultimately, if governance is not decentralized, why use a blockchain?***

5. Advice for enterprises

> *"Companies are interested in pursuing these problems together. And in principle, we're tackling problems that are not a strategic advantage for them but that they all share."*
>
> Susanne Somerville, CEO of Chronicle and co-founder of MediLedger

> *"Blockchains have competitors coming together in a platform, and that is different and counter-intuitive from how they have worked before. But the advantage of connecting one-to-many, of everyone seeing in real-time the information pertaining to the shipments they are involved in and visibility into the digital data documents, is a game-changer. Blockchain supports it and provides immutable trust."*
>
> Mike White, CEO of Maersk GTD[95]

> *"Maersk could not be seen as benefiting [from TradeLens] at the expense of other carriers. It took an effort to show this was a win-win."*
>
> Bridget van Kralingen, Senior VP for Blockchain at IBM[96]

As the quotes above attest, ***blockchain applications are ecosystem solutions that require enterprises to collaborate in new ways and to think differently about software governance*****.** No one enterprise should control the mission, participation, validation, overrides, software updates, or funding models. ***Decision-making rights have to be shared among ecosystem partners.*** Traditional enterprises struggle with this mindshift. How does an enterprise establish a business case, estimate a return on investment, or otherwise justify building an application that has to be shared with trading partners and, very likely, with competitors? The opportunities to add business (and social) value must be overwhelmingly compelling to warrant the risk.

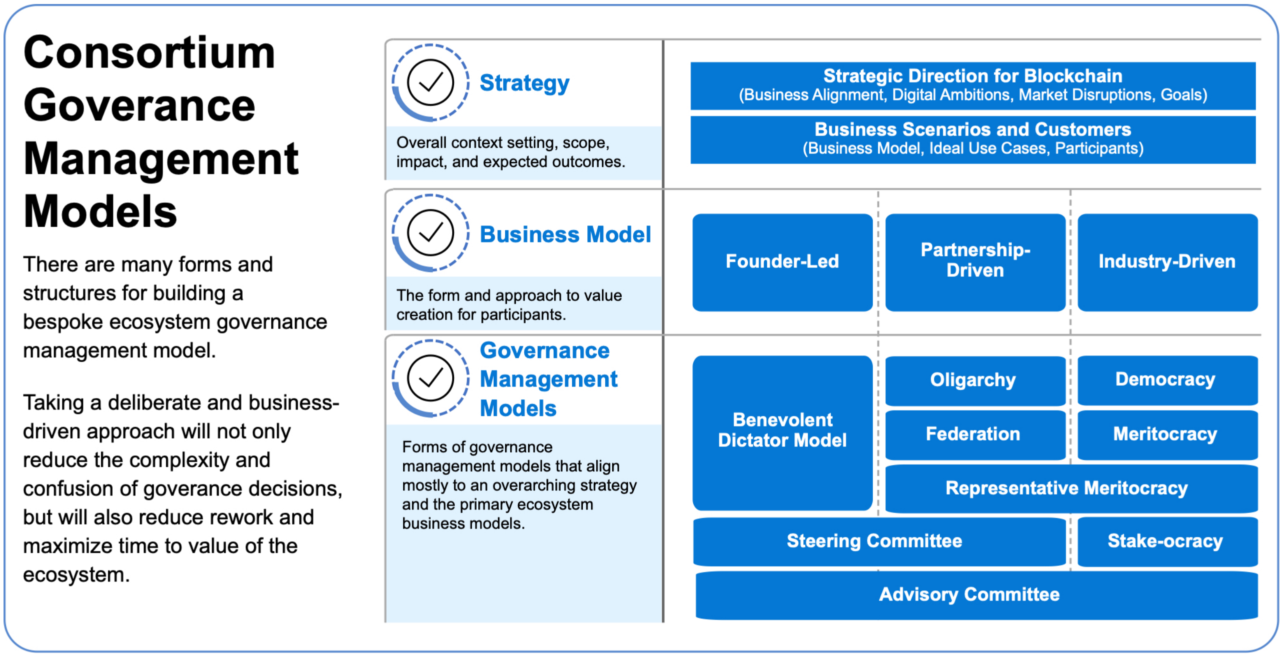
An enterprise must decide whether to lead blockchain development, participate in the development with ecosystem partners, or wait until others develop the application and join later. Each approach has different advantages and disadvantages. Leaders and active ecosystem participants architect the future, become renowned visionaries, and increase brand awareness, but they bear the most risk. Followers bear little risk, but may end up with suboptimal choices.

If *leading* the development as a sole enterprise, the initial governance model will be highly centralized. ***To have any chance of success, the leader must have a solid reputation that warrants trust as a benevolent dictator.*** The World Food Program (WFP) is one such example. As part of the United Nations, the WFP is recognized as the world's largest humanitarian effort to provide food assistance. When it launched a food distribution accounting system for over 100,000 Syrian refugees on Ethereum, the WFP was lauded.[97] Its intentions were not questioned. Few for-profit enterprises will enjoy such trust, and they will likely be more successful by building a minimal viable ecosystem (MVE). Facebook was wise to create the Libra Association, because regulators and the general population would doubt its munificence if it completely controlled Libra alone.

A minimal viable ecosystem (MVE) comprising a few trading partners—and perhaps competitors—that build the minimal viable product (MVP), will likely be governed as an oligarchy or stakeocracy.

To achieve network effects in the longer term, however, the initial MVE will need to attract many more participants to adopt its software.[b] In order to do so, the founders likely will need to evolve aspects of the governance model, particularly the funding model, to convince potential adopters.

Microsoft's Blockchain Playbook provides a useful way to map strategy, business models, and governance models (see Figure 12). Mike Walker, Sr. Director, Applied Innovation Team at Microsoft said, *"First the terminology. We refer to these as '**Governance Management Models**' rather than just 'Governance Models' because the latter is too generic and can be misleading. Second, everything ties back to the business strategy and business model of the ecosystem. We've found it's vital to be business outcome driven with governance."*



Consortium Goverance Management Models

There are many forms and structures for building a bespoke ecosystem governance management model.

Taking a deliberate and business-driven approach will not only reduce the complexity and confusion of goverance decisions, but will also reduce rework and maximize time to value of the ecosystem.

Strategy

Overall context setting, scope, impact, and expected outcomes.

Strategic Direction for Blockchain
(Business Alignment, Digital Ambitions, Market Disruptions, Goals)

Business Scenarios and Customers
(Business Model, Ideal Use Cases, Participants)

Business Model

The form and approach to value creation for participants.

Founder-Led | **Partnership-Driven** | **Industry-Driven**

Governance Management Models

Forms of governance management models that align mostly to an overarching strategy and the primary ecosystem business models.

Benevolent Dictator Model

Oligarchy

Democracy

Federation

Meritocracy

Representative Meritocracy

Steering Committee

Stake-ocracy

Advisory Committee

Figure 12: Blockchain Strategy, Business Models, and Governance 'Management' Models

(Source: Microsoft, with permission)

Ultimately, the MVE must plan to evolve shared governance from centralized to decentralized models, or there is little point in using blockchain technology. However, even with a plan, people will not trust founding members to voluntarily relinquish power over time. (Certainly, there's not much in history to suggest people willingly give up power.) Beyond the founders**, *potential enterprise adopters need assurances that governance will be truly shared; that there are verifiable controls to prevent the rise of powerful alliances to prevent their self-interests from superseding the interests of all ecosystem participants*.** Founders will need to prove their intentions to share decision making rights, perhaps by taking the following actions:

[b] Network effects can be described by Metcalfe's law, which states that the cost of a network rises linearly as additional nodes are added, but that the number of connections (and presumably value) increases exponentially. In 2019, Timothy Peterson was the first person to find empirical support for Metcalfe's law in the blockchain space. Specifically, he found that the number of users is directly correlated to the value of bitcoin. Source: Peterson, T. (2019), *Bitcoin Spreads Like a Virus*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3356098

- ✓ define the process for moving to decentralization, even if it is immature to commit to a timeline for doing so;
- ✓ engage an advisory board staffed with respected and independent members, such as academic institutions and non-profits;
- ✓ create term limits or frequently rotate leaders (at both individual and organizational levels), including term limits on validator node operators, digital asset reserve managers, and software gatekeepers;
- ✓ publish frequent independent audits of network security and of the handling of user accounts and digital assets;
- ✓ open the source code for public scrutiny;
- ✓ be relentless about transparency, particularly concerning user privacy and data usage, (on private blockchains, new participants worry about what the incumbents might do with their data; on public blockchains, people worry about what wallet providers, exchanges, and validators will do with their data);
- ✓ work with regulators to define stringent data privacy and data use protections, (regulations, in conjunction with transparent self-governance, will provide the strongest safeguards for investors and consumers.)

To conclude, blockchain applications—like all software solutions—are governed by people; people decide access and decision rights. In order to realize the potential value of shared applications, enterprises need to embrace shared governance. This white paper aimed to help enterprises think through and assess shared governance options, which will continue to evolve.

Appendix A: Research methods

For this white paper, we reviewed the existing literature and incorporated, with permission, the presentations and discussions from the Executive Advisory Board workshop of the University of Arkansas Blockchain Center of Excellence (BCoE). Additional insights from interviews conducted by the Director of the BCoE are also included.

Literature review

We searched Google Scholar, ABI/Inform, and the publications of the Association of Information Systems (AIS) for current academic literature on the terms 'blockchain governance' and 'distributed ledger governance'. As of July 2019, there were relatively few academic publications, which is understandable given the lead times between author submission, peer review and publication. In contrast, there is an abundance of information about blockchain governance on the Internet:

Search Term **Search Site**	**'Blockchain Governance'**	**'Distributed ledger Governance'**
Google	270,000	1,180
Google Scholar	372	6
ABI/Inform	7	0
AIS	11	0

We read the abstracts for the Google Scholar, ABI/Inform, and AIS articles. We downloaded and read papers that were particularly relevant for this white paper and included their findings as credited in the endnotes.

BCoE Workshop

Members of the Executive Advisory Board of the BCoE met in June 2019 to address the issue of shared blockchain governance. Members invited experts to present and discuss governance concerns and solutions. Workshops use the Chatham House Rule:

"When a meeting, or part thereof, is held under the Chatham House Rule, participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed."

Chatham House Royal Institute of International Affairs

Members and additional interviewees gave permission to be cited in this white paper.

Appendix B: Blockchain applications/projects

Bitcoin. Satoshi Nakamoto created Bitcoin in a 2008 white paper.[98] Satoshi Nakamoto, a pseudonym used by an unknown person or persons, posted a paper entitled, *Bitcoin: A Peer-to-Peer Electronic Cash System* to a cryptographic mailing list in 2008. This remarkable nine-page paper is the foundation for all we have today in the blockchain world. Quite simply, Nakamoto proposed *"an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party."*[99] Nakamoto was solving this problem: How can a payment system be created that performs the vital functions of trusted third parties without using them? Rather than rely on institutions, Nakamoto proposed to rely on cryptography and computer algorithms, including a proof-of-work consensus algorithm (see glossary), to prevent double spending and to secure an immutable record of all transactions. If transactions were to exchange value electronically, the first thing needed was something of electronic value. Nakamoto thus created an 'electronic coin' called a 'bitcoin'. Miners were initially awarded 50 bitcoins for creating the next block of recently validated transactions, but the block reward halves every 210,000 blocks. As of August 5, 2019, the block reward was 12.5 bitcoins per block; bitcoin was trading at $11,753; the network had 9,544 active nodes and 588,746 blocks had been added to the bitcoin blockchain.[100]

Ethereum. Vitalik Buterin wrote the 2013 Ethereum white paper that would become the Ethereum platform when he was only 19 years old. Vitalik Buterin, Gavin Wood and Jeffrey Wilcke began work on Ethereum by launching The Ethereum Foundation, a non-profit organization based in Switzerland. According to the Ethereum Foundation: *"Ethereum is a community-driven project aiming to decentralize the Internet and return it to its democratic roots. It is a platform for building and deploying applications which do not need to rely on trust and cannot be controlled by any central authority."* [101] Ethereum's smart contracts are the primary innovation that extends Bitcoin's blockchain from a transaction verification and settlement protocol, to a full-fledged 'Turing Complete' platform.[102] The foundation was first funded in August 2014 using an Initial Coin Offering for its native digital asset called 'ether'. Ethereum went live in July of 2015, with a presale release of 60 million ether and 20 million ether retained by The Ethereum Foundation.[103] It raised over $16 million.[104] Ether is not intended so much as a cryptocurrency as much as it is a 'crypto-fuel', meaning it's a token whose main function is to pay for the Ethereum platform.[105] Like Bitcoin, ether is released through the process of mining blocks using a proof-of-work consensus algorithm. Miners also receive the ether that senders appended to their transactions as transaction fees. Ethereum's block reward was initially 5 ether, but new blocks are created more frequently than in Bitcoin. It was reduced to 3 ether in 2017 and to 2 ether in 2019.[106] As of August 26, 2019, ether was trading at $188.49; the network had 8,977 active nodes[107], and 8,426,754 blocks had been added to the ledger.

EOS was developed by Daniel Larimer and Brendan Blumer, CTO and CEO, respectively, of Block.one. They wanted the advantages—open, secure, decentralized—of a public blockchain platform, like Ethereum, to build and operate decentralized applications, but without the latency, scalability, and resource intensity. The EOS mainnet was launched live in June of 2018. Anyone can view the blockchain (https://bloks.io/) and use EOS. Anyone can operate a validator node if they meet minimal criteria: an individual or organization must have a public website URL; at least one social media account; an ID on Steemit; sufficient hardware; plans to scale hardware; plans to benefit the community; telegram and testnet nodes; a roadmap; and a dividend position.[108] However, only 21 'block producers' can add blocks. The block producers are selected by a delegated proof-of-stake mechanism (see glossary) in which owners of EOS cast votes in proportion to their stake.[109] Block producers are rewarded with the issuance of new EOS tokens. Blocks are produced about every 500 milliseconds, with each of the 21 producers getting a turn. On the day of this writing, EOS was trading at $3.59 and nine block producers were located in China, three in Singapore, and one or two in the Cayman Islands, BVI, Hong Kong, Japan, Ukraine, and the United States.

Hyperledger Project. The Linux Foundation launched this non-profit organization in December of 2015. Brian Behlendorf, the developer of the Apache Web server, serves as Executive Director. As of July 2019, 18 premier, 199 general, 42 associate and 19 academic members are listed on its website.[110] It aims to advance the application of enterprise-grade blockchains across industries.[111] Thus far, Hyperledger Project has six major blockchain frameworks: Fabric; Sawtooth; Iroha; Burrow; Indy; and Grid (see Figure B.1). Fabric—much of whose code was donated by IBM—is commonly used by enterprises, including IBM, WalMart, and Maersk.[112] The Hyperledger Project is also developing eight tools: Aries; Caliper; Cello; Composer; Explorer; Quilt; Transact; and Ursa.[113]

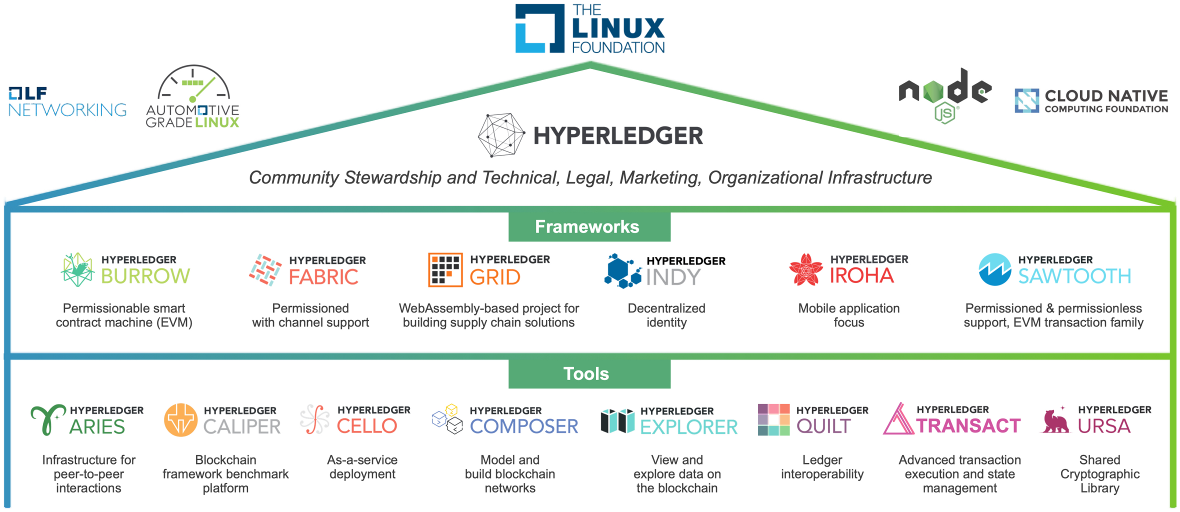

THE LINUX FOUNDATION
LF NETWORKING
AUTOMOTIVE GRADE LINUX
node JS
CLOUD NATIVE COMPUTING FOUNDATION
HYPERLEDGER
Community Stewardship and Technical, Legal, Marketing, Organizational Infrastructure
Frameworks
HYPERLEDGER BURROW
Permissionable smart contract machine (EVM)
HYPERLEDGER FABRIC
Permissioned with channel support
HYPERLEDGER GRID
WebAssembly-based project for building supply chain solutions
HYPERLEDGER INDY
Decentralized identity
HYPERLEDGER IROHA
Mobile application focus
HYPERLEDGER SAWTOOTH
Permissioned & permissionless support, EVM transaction family
Tools
HYPERLEDGER ARIES
Infrastructure for peer-to-peer interactions
HYPERLEDGER CALIPER
Blockchain framework benchmark platform
HYPERLEDGER CELLO
As-a-service deployment
HYPERLEDGER COMPOSER
Model and build blockchain networks
HYPERLEDGER EXPLORER
View and explore data on the blockchain
HYPERLEDGER QUILT
Ledger interoperability
HYPERLEDGER TRANSACT
Advanced transaction execution and state management
HYPERLEDGER URSA
Shared Cryptographic Library

Figure B.1: Hyperledger Project's Frameworks and Tools

(Source: https://www.hyperledger.org/wp-content/uploads/2019/06/HL_Greenhouse_6.20.19.png)

IBM Food Trust. The IBM Food Trust is a blockchain platform for global food supply. It was commercially available in October of 2018. It aims to improve food safety, food freshness, and supply chain efficiency while reducing food fraud and food waste. IBM offers three services on the platform so far: Trace, Certifications, and Fresh Insights. ***Trace*** helps participants follow products through the supply chain by tracking product identification, product labels, and purchase orders numbers. Trace can also be used to trace how ingredients are transformed from raw materials to finished products. ***Certifications*** monitor current, expiring, and expired certificates. ***Fresh Insights*** can monitor at risk inventory by tracking events such as time since harvest and dwell times at each location in the supply chain. IBM has a tiered pricing model based on size of business, starting at $100 per month. The platform is built on Hyperledger Fabric, which uses PBFT consensus (see glossary). Data items are based on GS1 standards.[114] As of 2018, the platform had over four million transactions on more than 350 SKUs, and more than 50 members adding data to the system.[115] Major enterprise adopters include Walmart; Carrefour; Smithfield; Topco; Golden State Foods; and Nestlé.

The Libra Association is a not-for-profit organization headquartered in Geneva, Switzerland. The association's purpose is *"to coordinate and provide a framework for governance for the network and reserve and lead social impact grant-making in support of financial inclusion."*[116] Any person will be able to view and transact in the Libra network by accessing a digital wallet. Only Association members will operate nodes, which so far includes 24 companies: Anchorage; Andresseen Horowitz; Bison Trails; Book Holdings; Breakthrough Initiatives; Coinbase; eBay; Facebook/Calibra; Farfetch; Iliad; Lyft; Mastercard; Mercado Pago; PayPal; PayU; Ribbit Capital; Spotify; Stripe; Thrive Capital; Uber; USV; Visa; Vodafone; and Xapo.

Four not-for-profit/multilateral organizations are also founders (Creative Destruction, Kiva, Mercy Corps, and Women's World Banking). The Libra Association aims to recruit a total of 100 members to operate nodes in 2020. Finally—but with no concrete time horizon suggested—anyone will be able to operate a node when the Libra network matures into a fully permissionless blockchain.[117]

MedliLedger. Founded by Chronicled in 2017, MediLedger is a block-enabled platform for the pharmaceutical sector designed to comply with drug regulations enacted in the United States, Europe, Asia and South America. Its first projects focus on compliance with the US Drug Supply Chain Security Act of 2013. The act requires that all participants in the US pharmaceutical sector track and trace sellable units for certain classes of pharmaceuticals from manufacturers to pharmacy on one interoperable electronic system. MediLedger's first service, called Product Verification, will go live October 2019. The service looks up the correct manufacturer based on product item numbers stored on the blockchain and then sends a private message to the manufacturer to verify the legitimacy of a return, i.e. that the drug is not counterfeit or expired. The solution uses zero-knowledge proofs (see glossary) to ensure data privacy while still demonstrating the authenticity of a transaction. So far, its working group members include McKesson; Pfizer; AmerisourceBergen; Cardinal Health; Genentech; Gilead; and Amgen. Overall, the MediLedger network promises to:[118]

- Keep an immutable record of transactions and data to demonstrate regulatory adherence and improve security
- Enforce cross-industry business rules without ever revealing companies' valuable, private data. This makes it easy to certify the authenticity of raw materials and drugs, stop counterfeit items from invading your supply chain, and easily manage payment contract terms.
- Protect your business intelligence, so your data stays behind your firewall and under your control.
- Use permission-based private messaging to share only the data you want to share with the partners you want to share it with.
- Connect with trading partners and trusted service providers at the vanguard of emerging solutions for the pharmaceutical industry today.

Monero. Monero was launched in 2015 as a cryptocurrency focused on data privacy. It is a public permissionless network, so that anyone may transact or operate a validator node. It uses CryptoNote, a white paper by Nicolas van Saberhagen, that defined a proof-of-work algorithm with increased data obfuscation compared to the proof-of-work used in Bitcoin.[119] The group signatures (called ring signatures) used in CryptoNote *"mix the spender's input with a group of others, making it exponentially more difficult to establish a link between each subsequent transaction. Monero requires senders to generate a one-time address using the receiver's public address. Although all transactions to a given public address end up in the same central wallet, an outside party can never know whether two transactions have been sent to the same public address."*[120] In May of 2014, Monero was at $2.47; its peak price was over $450 in January of 2018. On August 22, 2019, it was trading at $82.69.

Quorum: Quorum is an enterprise-ready distributed ledger and smart contract platform based on Ethereum.[121] The Enterprise Ethereum Alliance officially supports Quorum.[122] However, Quorum was led by J.P.Morgan as an open-source, enterprise grade version of Ethereum.[123] Quorum is a private/permissioned blockchain that requires permission to operate a node.[124] A key benefit is that it is designed to process and settle hundreds of transactions per second. J.P. Morgan licensed Quorum with a General Purpose License (GPL) so that the platform will be free to use. It plans to co-evolve in cooperation with Ethereum.[125] QuorumChain is the original consensus protocol, with other Raft and Istanbul Byzantine Fault Tolerant (BFT) protocols added later.[126] [127] QuorumChain has three types of nodes: voter nodes, maker nodes, and observer nodes. Voter nodes vote on which block should be added to the blockchain.

Maker nodes are authorized to add the blocks after enough votes have been cast. Observer nodes receive and validate blocks, but do not vote or make blocks.[128] The ledger is segmented into a private state database and a public state database. Participants can execute private and public smart contracts. While all nodes validate public transactions, nodes can only validate private transactions if they are party to the private smart contract.[129] Notable adopters include Accenture: EY: Reuters: Microsoft: and Chronicled.[130] Microsoft added Quorum to the Azure cloud marketplace and can be used with Microsoft's Coco framework for a trusted execution environment that is an additional layer of security.[131]

Ripple. Ripple was founded by Chris Larsen and Jeb McCaleb in 2012. It's a decentralized, real-time financial settlement system. Ripple aimed to overcome Bitcoin's relatively slow settlement times, inability to trade other currencies, and massive electricity consumption, while still being inexpensive, transparent, private, and secure. According to Ripple's website, its network handles 1,500 transactions per second (TPS), operates 24x7, and can scale to 50,000 TPS. It also claims a five-year track record of its distributed ledger closing without incidence.[132] Anyone can view the Ripple network (https://xrpcharts.ripple.com/#/transactions). Anyone can transact on the Ripple network by accessing a digital wallet. Institutional customers use an API to connect to the Ripple network via a Ripple Gateway. Gateways can establish trust lines up to certain amounts with other gateways. However, if the sending gateway does not have a direct trust line with the receiving gateway, the network protocol will find a path of trust, thus transactions will 'ripple' through the network. If no path of trust can be found, the value can be transferred using Ripple's native digital asset called 'Ripple' (symbol XRP). In this way, XRP can be used as a bridge currency if no paths of trust exist between trading partners.[133] When institutions or consumers join the ripple network, they can select which nodes they want to perform validation checks, which is called a Unique Node List (UNL), or they can accept the default list maintained by Ripple. Ripple maintains its own validator nodes around the world and also has CGI and MIT as transaction validators.[134] Without the incentives of mining, Ripple asks intuitions to run a validator node when they join the system to help secure the network.

Stellar. Jed McCaleb and Joyce Kim co-founded the Stellar Development Foundation (SDF), a US-based, non-profit organization in 2014. Stellar's mission is to expand financial access and literacy worldwide.[135] The white paper for the Stellar protocol was released in April of 2015 and the network went live in November of that year.[136] [137] Stellar's network for global payments settles transactions in two to five seconds at a very low transaction fee of one lumen (Stellar's native digital asset) for 100,000 transactions. Stellar can process over 1,000 operations per second. By the end of 2017, SDF employed 15 people and had secured $3 million in funding.[138] SDF does not have direct contact with users. Instead, SDF aims to have other intuitions develop business models and use the Stellar code base to develop applications for services such as remittances; micropayments; mobile branches; mobile money; and other services for the under-banked. Stellar does not charge institutions or individuals any fees to use the Stellar network beyond the modest per transaction fee. Its network is based on open source code that is supported by the foundation, but adopters are free to develop commercial applications, modify or distribute the source code.

TradeLens. Developed by Maersk and IBM, TradeLens is an industry platform—released in 2018, after years of development—and used to track shipping containers in the global supply chain.[139] [140] Built on HyperLedger Fabric, it is a permissioned blockchain. As of April 2019, it had 60 members and over 100 ecosystem partners, including carriers, ports, terminals operators, 3PLS, and freight forwarders. Mike White, CEO of Maersk GTD leads TradeLens. According Bridget van Kralingen, Senior VP for Blockchain at IBM, TradeLens had tracked 500 million events on 20 million containers by April 2019. TradeLens was adding between 25,000 to 30,000 documents a day.[141]

WineChain. EY developed WineChain to restore trust in the wine supply chain. Each wine bottle is tokenized with an Ethereum non-fungible token (called WID), serving as a unique identifier.[142] The token is displayed as a QR code on the label and stored on public Ethereum. On a permissioned version of

Ethereum (Quorum), the blockchain is updated as the bottle moves through the supply chain of producers, brokers, importers, wholesaler, distributors, and retailers.[143] Specifically, the blockchain stores the transfer of tokens on the blockchain. Supply chain partners use digital wallets to store the private keys associated with the public addresses. Towards the end of 2019 or early 2020, EY hopes to have integration between this capability and Nightfall, EY's open source protocols for enabling private transaction on public Ethereum.

Appendix C: Glossary

Delegated Proof-of-Stake (DPoS) is a consensus protocol created by Daniel Larimer, founder of BitShares, Steemit and EOS.[144] With this method, anyone who possesses the cryptocurrency can vote to elect validator nodes. The validator nodes with the most votes become a ‘delegate’ (see Figure C.1). The algorithm takes turns selecting a leader from among the panel of delegates for a current time period. After the time period elapses, another round of voting occurs to select the next panel of delegates. Delegates are rewarded with transaction fees. DPoS settles transactions faster and with fewer resources than proof-of-work, and is more democratic than permissioned protocols.[145] EOS uses DPoS.

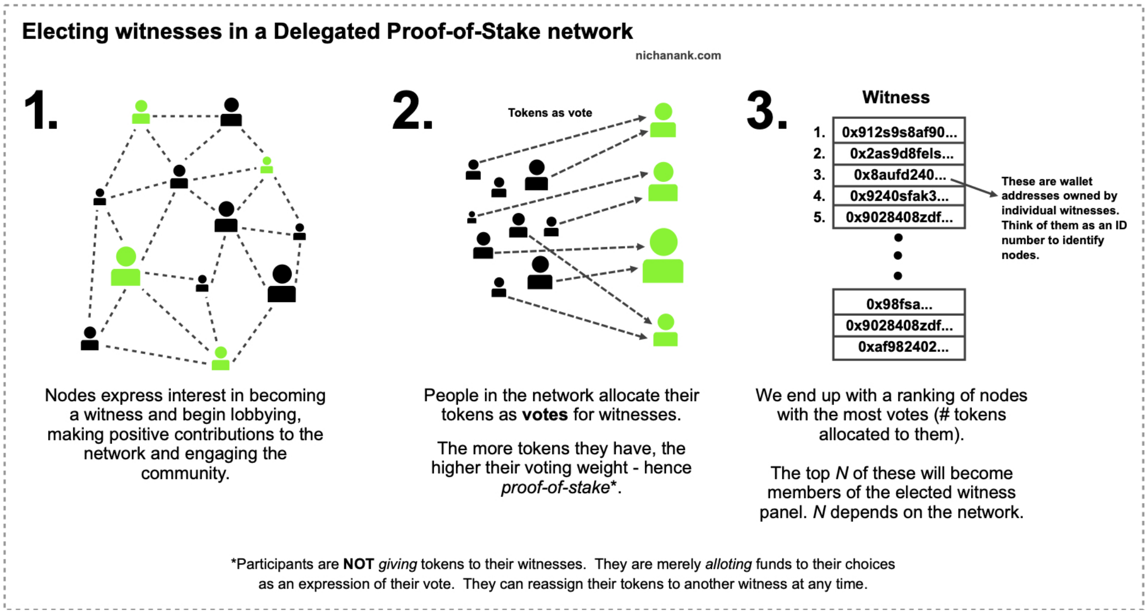

Electing witnesses in a Delegated Proof-of-Stake network
nichanank.com
1.
Nodes express interest in becoming a witness and begin lobbying, making positive contributions to the network and engaging the community.
2.
Tokens as vote
People in the network allocate their tokens as **votes** for witnesses.
The more tokens they have, the higher their voting weight - hence *proof-of-stake**.
3.
Witness
1. 0x912s9s8af90...
2. 0x2as9d8fels...
3. 0x8aufd240...
4. 0x9240sfak3...
5. 0x9028408zdf...
0x98fsa...
0x9028408zdf...
0xaf982402...
These are wallet addresses owned by individual witnesses. Think of them as an ID number to identify nodes.
We end up with a ranking of nodes with the most votes (# tokens allocated to them).
The top *N* of these will become members of the elected witness panel. *N* depends on the network.
*Participants are **NOT** *giving* tokens to their witnesses. They are merely *alloting* funds to their choices as an expression of their vote. They can reassign their tokens to another witness at any time.

Figure C1: Delegated Proof-of-Stake (DPoS) Voting Process

(Source: https://en.bitcoinwiki.org/upload/en/images/8/8b/Consensus-algorithms-pos-dpos.png)

Practical Byzantine Fault Tolerance (PBFT) is a consensus protocol created by Miguel Castro and Barbara Liskov in 1999.[146] With PBFT, nodes need permission to serve as validator nodes, forming a member list. Each round, a node from the member list is selected as leader (see Figure C.2). A client node sends a request to the leader node to validate a transaction. The leader node multicasts the request to all the other authorized nodes. The authorized nodes execute the request independently and then send to each other and reply to the client. The client waits for a certain percentage of replies to confirm validation, typically waiting for 2/3 of the nodes to agree. Leader node changes for next round.

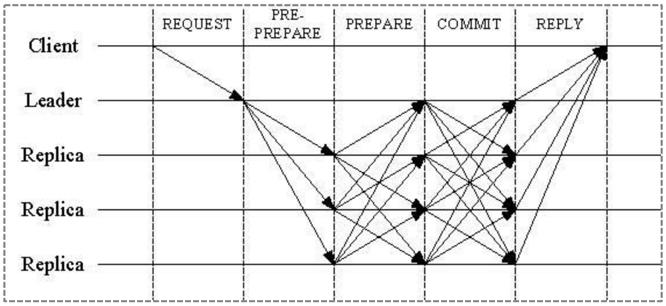


Figure C.2: Practical Byzantine Fault Tolerance (PBFT) Consensus Process

(Source: Castro & Liskov (1999) https://theintelligenceofinformation.files.wordpress.com/2017/02/hotdep_img_1.jpg)

Proof-of-Authority (PoA) is a consensus mechanism that preauthorizes nodes with the authority to validate and add transactions to a distributed ledger. The algorithm takes turns selecting a leader from among the list of authorized nodes (see Figure C.3). The leader node checks each transaction in the transaction queue; organizes valid transactions into a block; signs the block with the node's private key; and distributes the block to other nodes. The other nodes validate that the block was signed by the current leader and recheck each transaction within the block, resulting in an acceptance or a rejection of the entire block. As a permissioned consensus algorithm, it settles transactions faster and with fewer resources than permissionless algorithms, but it is more centralized.[147]

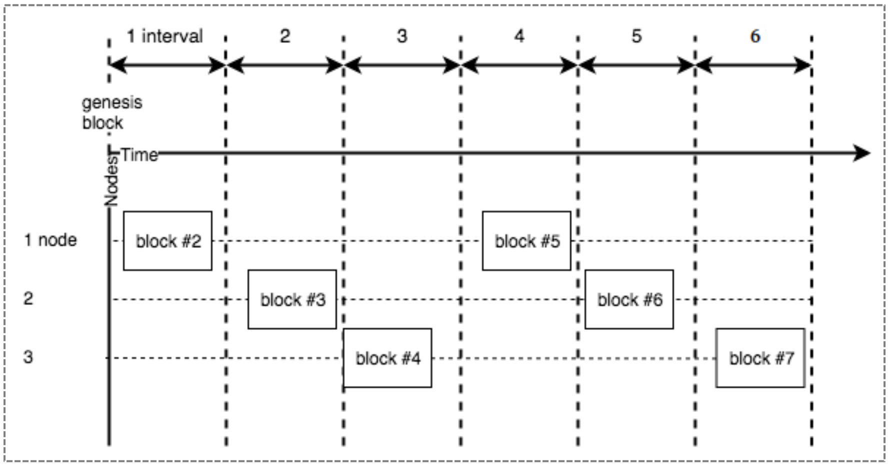
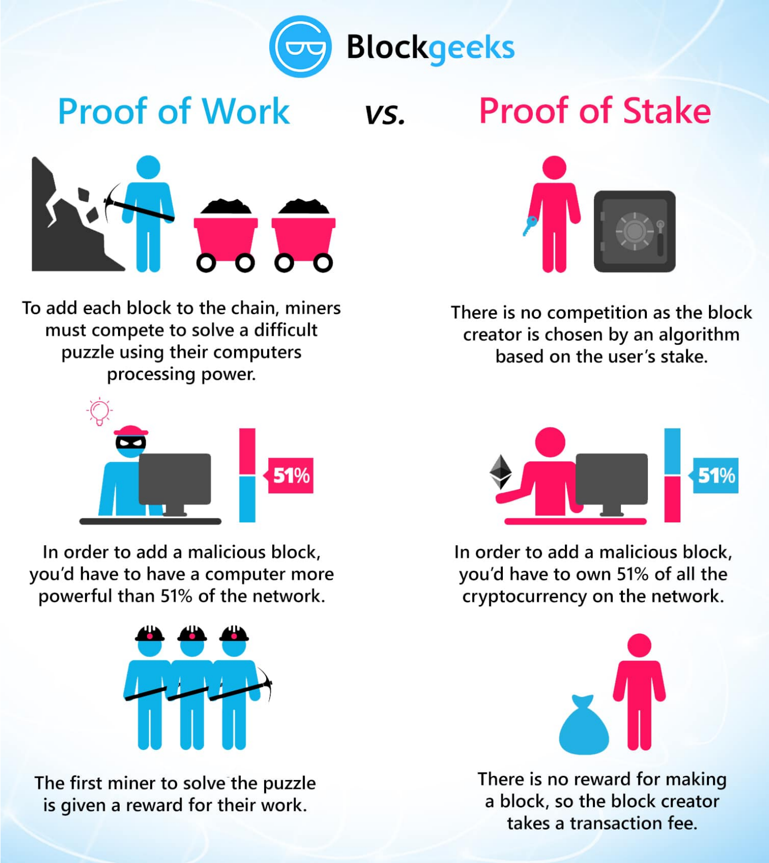


Figure C.3: Proof of Authority: Authorized nodes take turns creating blocks

(Source: https://apla.readthedocs.io/en/latest/_images/block-generation.png)

Proof-of-Stake (PoS) is a consensus protocol created by Sunny King and Scott Nadal, in a 2012 white paper.[148] Instead of 'mining' for coins, the protocol selects a member to 'forge' new currency as a reward for validating the transactions and creating the next block. Essentially, the selected member node is awarded a transaction fee. The member node is selected in a semi-random way. It's called a 'proof-of-stake' because the members with the highest 'stake' (e.g. have the largest account balances; holding the coins the longest period of time) are giving priority in the selection algorithm. Participants in the blockchain can estimate with some certainty which member will likely be the next 'forger'. A proof-of-stake process uses much less energy than a proof-of-work process (see Figure C.4). It creates a highly secure ledger, as an attacker would need to gain control of more than 50 percent of the cryptocurrency to rewrite the ledger. However, critics claim it is less secure than proof-of-work because people with small stakes have little to lose by voting for multiple blockchain histories, which leads to consensus never resolving.[149] Another downside is that the 'richest' participants are given the easiest mining puzzle. Peercoin and Nxt use proof-of-stake.



Proof of Work vs. Proof of Stake

To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.

There is no competition as the block creator is chosen by an algorithm based on the user's stake.

In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.

In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.

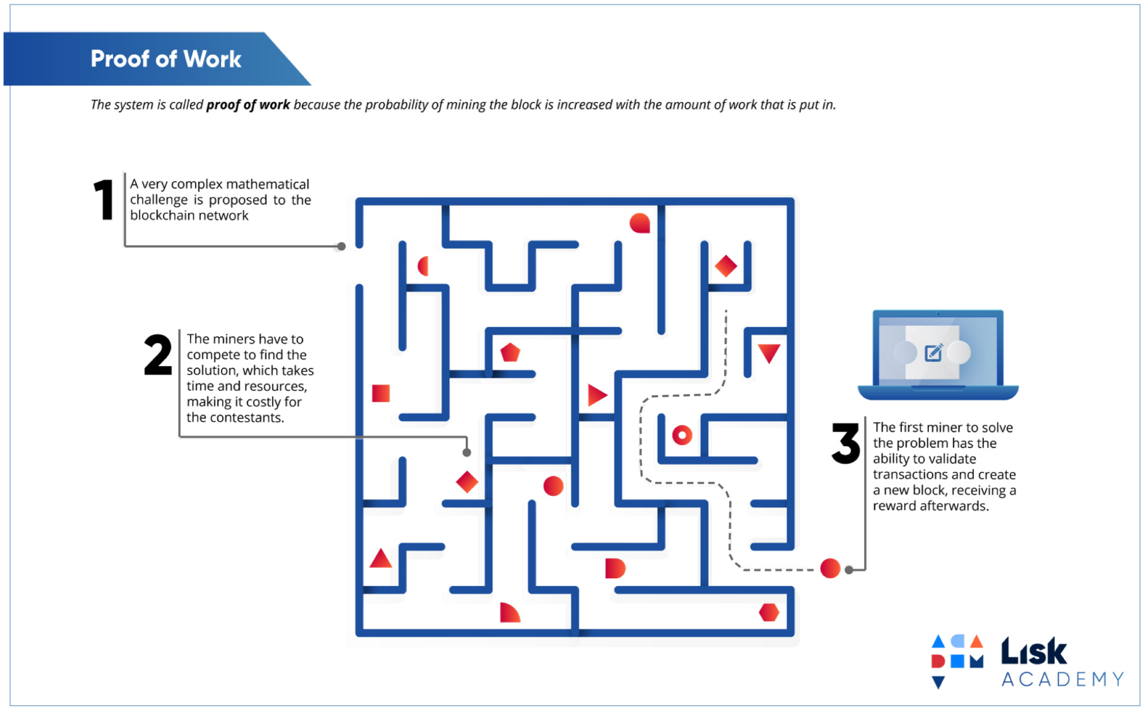
The first miner to solve the puzzle is given a reward for their work.

There is no reward for making a block, so the block creator takes a transaction fee.

Figure C.4: Proof-of-Work *vs.* Proof-of-Stake

(Source: https://blockgeeks.com/wp-content/uploads/2019/05/proofofworkvsproofofstake-1.jpg)

Proof-of-Work (PoW) is a consensus protocol created by Cynthia Dwork and Moni Naor in 1993 to prevent junk email.[150] Satoshi Nakamoto adopted the 'proof-of-work' consensus protocol for Bitcoin in the 2008 white paper.[151] Ethereum also uses proof-of-work (for now). Nakamoto needed a way to find independent verifiers to validate transactions and add blocks to the blockchain without relying on trusted third parties. Nakamoto proposed to reward other nodes in the network with newly issued bitcoins when they validate all recently submitted transactions and create the next block. So that validator nodes take the task seriously, Nakamoto proposed a competition among computer nodes in the blockchain network to be the first to collect recently verified transactions into a block and then to find an acceptable block identification number (known as the blockhash) for the next block in the blockchain (see Figure C.5). It's not easy to find an acceptable number—it takes a lot of computing power to perform the brute force guesses to find a hash number that is less than the current mining 'difficulty'. The difficulty is part of the proof that the miner's computer did a significant amount of work to earn the block reward. The proof-of-work protocol creates a highly secure ledger, as an attacker would need to gain control of more than 50 percent of the nodes, rewrite history and find all new hashes that adhere to the protocol before other nodes notice. The cons of the protocol include slower transaction settlement times and higher electricity consumption compared to other protocols.



Proof of Work

The system is called ***proof of work*** *because the probability of mining the block is increased with the amount of work that is put in.*

1 A very complex mathematical challenge is proposed to the blockchain network

2 The miners have to compete to find the solution, which takes time and resources, making it costly for the contestants.

3 The first miner to solve the problem has the ability to validate transactions and create a new block, receiving a reward afterwards.

Figure C.5: Proof-of-Work: Miners compete to make the next block

(Source: https://lisk.io/content/5-academy/2-blockchain-basics/4-how-does-blockchain-work/9-proof-of-work/10-pow-infographic.jpg)

Zero knowledge proofs were developed in 1985 by Shafi Goldwasser, Charles Rackoff, and Silvio Micali in 1985.[152] Zero knowledge proofs are a method for one party (or node) to verify possession of a piece of information to other parties (or nodes) without revealing the information. As a simple example, suppose Alice wants to prove to Bob that she knows the exact number of jellybeans that fills a large barrel without telling Bob the exact number. What might Alice do to convince Bob she knows the amount? Alice could instruct Bob to take any number of jellybeans out of the barrel after she leaves the room. Bob makes his choice. Alice reenters the room and Bob exits the room. Alice recounts the beans and compares the current count with the previous count to calculate exactly how many jellybeans (if any) Bob removed. When Bob returns, Alice tells Bob exactly how many jellybeans he took. If Bob thinks Alice made a lucky guess, rounds of the same choice could be made over and over again. Eventually, Bob will be convinced that Alice possesses the knowledge of the exact number of jellybeans without ever revealing the number. In blockchain applications, zero-knowledge proofs are used to guarantee that transactions are valid without revealing information about the sender, receiver, and/or transaction. Zcash, EY's Nightfall, MediLedger, and many other blockchains use zero knowledge proofs.

Endnotes

[1] Sedgwick, K. (July 15, 2018), *Why Governance is the Greatest Problem for Blockchains To Solve,* https://news.bitcoin.com/why-governance-is-the-greatest-problem-that-blockchains-must-solve/

[2] Sedgwick, K. (July 15, 2018), *Why Governance is the Greatest Problem for Blockchains To Solve*, https://news.bitcoin.com/why-governance-is-the-greatest-problem-that-blockchains-must-solve/

[3] Lacity, M. (2018), *A Manager's Guide to Blockchains for Business*, SB Publishing, Stratford-Upon-Avon, UK

[4] Panetta, K. (January 22, 2019), *The 4 Phases of the Garner Blockchain Spectrum*, https://www.gartner.com/smarterwithgartner/the-4-phases-of-the-gartner-blockchain-spectrum/

[5] Press Release (May 28, 2019), *Major ocean carriers CMA CGM and MSC to join TradeLens blockchain-enabled digital shipping platform*, https://www.maersk.com/news/articles/2019/05/28/cma-cgm-and-msc-to-join-tradelens-digital-shipping-platform

[6] Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

[7] Associated Press (June 28, 2015), 'The Latest: Strict limits on bank withdrawals will not apply to foreign credit cards', *US News*, https://www.usnews.com/news/business/articles/2015/06/28/the-latest-greece-wants-ecb-to-keep-giving-emergency-help

[8] Popper, N. (2015), *Digital Gold*, HarperCollins, New York, p. 82.

[9] Popper, N. (2015), *Digital Gold*, HarperCollins, New York, p. 82.

[10] Popper, N. (2015), *Digital Gold*, HarperCollins, New York, p. 82.

[11] https://en.wikipedia.org/wiki/Ethereum

[12] The Libra Association, https://libra.org/en-US/association-council-principles/#overview

[13] Hyperledger (September 6, 2017), *ABCs of Open Governance*, https://www.hyperledger.org/blog/2017/09/06/abcs-of-open-governance

[14] https://github.com/bitcoin/bips/blob/master/README.mediawiki

[15] https://www.ibm.com/blockchain/solutions/food-trust/food-industry-technology

[16] What is the Advisory Council? https://www.ibm.com/blockchain/solutions/food-trust/food-industry technology#1797811

[17] Somerville, S. (June 6, 2019), presentation to the University of Arkansas BCoE Workshop.

[18] Maersk Press Release (July 2, 2019), *TradeLens Blockchain-Enabled Digital Shipping Platform Continues Expansion With Addition of Major Ocean Carriers Hapag-Lloyd and Ocean Network Express*, https://www.globenewswire.com/news-release/2019/07/02/1877150/0/en/TradeLens-Blockchain-Enabled-Digital-Shipping-Platform-Continues-Expansion-With-Addition-of-Major-Ocean-Carriers-Hapag-Lloyd-and-Ocean-Network-Express.html

[19] TradeLens Advisory Board, https://www.tradelens.com/about/

[20] Alex T (April 25 2018), *On Chain vs. Off Chain Governance: The Ins And Outs*, CoinJournal

[21] https://www.chronicled.com/about

[22] Provided by Ramesh Gopinath, Vice President if Blockchain Solutions, IBM

[23] https://libra.org/en-US/

[24] https://monero.org/about-site/

[25] Ripple: Our Company, https://www.ripple.com/company/

[26] Stellar Development Foundation Mandate, https://www.stellar.org/about/mandate/

[27] https://tour.tradelens.com/mission

[28] To track current Bitcoin validator node counts and locations, see https://bitnodes.earn.com/

[29] https://www.ethernodes.org/network/1

[30] Seibold, S. and Samman, G. (2016) KPMG White Paper, https://assets.kpmg/content/dam/kpmg/pdf/2016/06/kpmg-blockchain-consensus-mechanism.pdf?aid=fndrabg_p?aid=fndrabg_p

[31] This list was adapted from Lerner, S. D. (April 2016), *Drivechains, sidechains, and hybrid 2-way peg designs*,

[32] Some authors only consider three types of blockchains, for example, Pedersen, A., Risius, M., and Beck, R. (2019), 'A Ten-Step Decision Path to Determine When to Use Blockchain Technologies', *MIS Quarterly Executive*, Vol. 18, 2, Article 3.

[33] Daniels, A. (October 18, 2018), *The Rise of Private Permissionless Blockchains*, Medium, https://medium.com/ltonetwork/the-rise-of-private-permissionless-blockchains-part-1-4c39bea2e2be

[34] Nightfall, https://github.com/EYBlockchain/nightfall

[35] Danielle Austin, *EY Blockchain Analyzer - Analyzing and monitoring zero-knowledge proof private transactions on the public blockchain*, EY Global Blockchain Summit, April 16, 2019

[36] https://www.coindesk.com/ey-open-sources-nightfall-code-for-private-transactions-on-ethereum

[37] Danielle Austin, *EY Blockchain Analyzer* - *Analyzing and monitoring zero-knowledge proof private transactions on the public blockchain*, EY Global Blockchain Summit, April 16, 2019

[38] https://www.ey.com/en_us/people/paul-brody

[39] Bauerle, N. (2017), *What is the Difference Between Public and Permissioned Blockchains?* https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains/

[40] To operate an EOS validator node, an individual or organization must have a public website URL, at least one social media account, and ID on Steemit, sufficient hardware, plans to scale hardware, plans to benefit the community, telegram and testnet nodes, a roadmap, and a dividend position. Source: Ben Sigman (May 8, 2018), EOS Block Producer FAQ, https://medium.com/@bensig/eos-block-producer-faq-8ba0299c2896

[41] To view the 21 EOS validator nodes and block producers, see https://bloks.io/vote

[42] Libra White Paper, https://libra.org/en-US/white-paper/

[43] POA Network, *Proof of Authority: Consensus Model with Identity at Stake*, https://medium.com/poa-network/proof-of-authority-consensus-model-with-identity-at-stake-d5bd15463256

[44] What are Key Responsibilities for a Trust Anchor? https://www.ibm.com/blockchain/solutions/food-trust/food-industry-technology#1797811

[45] IBM Press Release (October 23 2018), *IBM and Microsoft Announce Partnership Between Cloud Offerings*, https://www.pbsnow.com/ibm-news/ibm-and-microsoft-announce-partnership-between-cloud-offerings/

[46] Maersk Press Release (July 2, 2019), *TradeLens Blockchain-Enabled Digital Shipping Platform Continues Expansion With Addition of Major Ocean Carriers Hapag-Lloyd and Ocean Network Express*, https://www.globenewswire.com/news-release/2019/07/02/1877150/0/en/TradeLens-Blockchain-Enabled-Digital-Shipping-Platform-Continues-Expansion-With-Addition-of-Major-Ocean-Carriers-Hapag-Lloyd-and-Ocean-Network-Express.html

[47] WineChain token on Ethereum, https://etherscan.io/token/0x49d4c3629f93f49ba934debf28605d26caaf3acc

[48] *Restoring trust in the wine industry, from grape to glass*, https://www.ey.com/en_gl/global-review/2018/restoring-

trust-in-the-wine-industry

[49] Taylor, P. (April 18 2017), EY partners with EZLab on blockchain wine security project, https://www.securingindustry.com/food-and-beverage/ey-partners-with-ezlab-on-blockchain-wine-security-project/s104/a4014/#.XUhRWZNKgnc

[50] Williams, R. (May 28, 2019), *TATTOO – A Wine Platform Created for Blockchain Wine Pte. Ltd.,* https://www.cryptonewsz.com/ey-to-build-a-global-wine-platform-for-blockchain-wine-pte-ltd/22061/

[51] Crosman, P. (April 28 2017), *JPMorgan defection underscores tough blockchain choices*, American Banker, https://www.americanbanker.com/news/jpmorgan-defection-underscores-tough-blockchain-choices

[52] Quoted in Enterprise Blockchain News Ledger Insights (January 2019), *Chronicled, startup behind MediLedger pharma blockchain raises $16 million*, https://www.ledgerinsights.com/chronicled-startup-behind-medildger-pharma-blockchain-raises-16-million/

[53] Drug Supply Chain Security Act (DSCSA), https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa

[54] The Bitcoinist, *Bitcoin Cash ABC vs. Bitcoin Cash SV-Examining the Bitcoin Cash War*, https://bitcoinist.com/bitcoin-cash-abc-vs-bitcoin-cash-sv-examining-the-bitcoin-cash-hash-war/
Clifford, T. (November 14, 2018), "*Crypto civil war' slams bitcoin, but it won't last," says BKCM's Brian Kelly*, CNBC.
Retrieved 18 November 2018.

[55] Segal, D. (June 25, 2016), *Understanding the DAO attack*, http://www.coindesk.com/understanding-dao-hack-journalists/

[56] Segal, D. (June 25, 2016), *Understanding the DAO attack*, http://www.coindesk.com/understanding-dao-hack-journalists/

[57] Segal, D. (June 25, 2016), *Understanding the DAO attack*, http://www.coindesk.com/understanding-dao-hack-journalists/

[58] Insureon (January 28, 2016), *The State of Software Liability*, https://it.insureon.com/news/the-state-of-software-liability

[59] Howell, Bronwyn E. and Potgieter, Petrus H. and Sadowski, Bert M., (February 2019), *Governance of Blockchain and Distributed Ledger Technology Projects* Available at SSRN: https://ssrn.com/abstract=3365519 or http://dx.doi.org/10.2139/ssrn.3365519

[60] Bitcoin Licensing https://github.com/bitcoin/bitcoin/blob/master/COPYING

[61] Ethereum Licensing https://github.com/ethereum/wiki/wiki/Licensing

[62] https://github.com/bitcoin/bitcoin/blob/master/COPYING

For example, MIT's license reads, in part, "THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE."

[63] GNU General Public License: https://www.gnu.org/licenses/gpl-3.0.en.html

[64] GNU General Public License: https://www.gnu.org/licenses/gpl-3.0.en.html

[65] https://github.com/bitcoin/bitcoin/blob/master/COPYING

[66] https://developers.libra.org/docs/libra-open-source-paper

[67] Somerville, S. (June 6, 2019), presentation to the University of Arkansas BCoE Workshop.

[68] https://www.ibm.com/blockchain/solutions/food-trust

[69] TradeLens Overview, https://docs.tradelens.com/learn/tradelens_overview/

[70] Tinanow, A. (October 30, 2018), *How Maersk's Bad Business Model Is Breaking Its Blockchain*, Forbes, https://www.forbes.com/sites/andreatinianow/2018/10/30/how-maersks-bad-business-model-is-breaking-its-blockchain/#274ccf284f4d

[71] https://github.com/bitcoin/bips

[72] Ferreira, D., Li, J., and Nikolowa (2019), *Corporate Capture of Blockchain Governance*, London School of Economics Discussion paper DP13493, Financial Economics and Industrial Organization.

[73] Ferreira, D., Li, J., and Nikolowa (2019), *Corporate Capture of Blockchain Governance*, London School of Economics Discussion paper DP13493, Financial Economics and Industrial Organization.

[74] Libra Open Source. https://developers.libra.org/docs/libra-open-source-paper

[75] Buterin, V. (2017), Notes on Blockchain Governance, https://vitalik.ca/general/2017/12/17/voting.html

[76] EOS Block Producer Elections, https://eosauthority.com/producers_schedules

[77] Buterin, V. (2017), Notes on Blockchain Governance, https://vitalik.ca/general/2017/12/17/voting.html

[78] https://www.brainyquote.com/quotes/vitalik_buterin_847219

[79] Doz, Y. (2019), 'Governing Multilateral Alliances', *California Management Review* 61(3), pp. 93-114.

[80] Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, p 4, https://bitcoin.org/bitcoin.pdf

[81] Lacity, M. (2018), *A Manager's Guide to Blockchains for Business*, SB Publishing, Stratford-Upon-Avon, UK

[82] Branson, R. (2015), *Ripple: The Ultimate Guide to Understanding Ripple Currency,* Elliot Branson Publications.

[83] Levy, A. (May 26 2017), *Bitcoin rival Ripple is suddenly sitting on billions of dollars worth of cryptocurrency*, posted at CNBC News at http://www.cnbc.com/2017/05/26/bitcoin-rival-ripple-is-sitting-on-many-billions-of-dollars-of-xrp.html

[84] Foster, W., Kim, P., and Christiansen, B. (2009), 'Ten Nonprofit Funding Models', *Stanford Social Review*.

[85] Fisher, C. (July 15, 2019), *US Treasury has serious concerns Libra could be used for terrorism*, https://www.engadget.com/2019/07/15/facebook-libra-cryptocurrency-us-treasury-department-concerns/
Alexandre, A. (August 5, 2019), *UK Data Protection Watchdog Raises Concerns Over Facebook's Libra*, CoinTelegragh, https://cointelegraph.com/news/uk-data-protection-watchdog-raises-concerns-over-facebooks-libra

[86] https://www.goodreads.com/quotes/tag/blockchain

[87] Doz, Y. (2019), 'Governing Multilateral Alliances', *California Management Review,* 61(3), pp. 93-114.

[88] Doz, Y. (2019), 'Governing Multilateral Alliances', *California Management Review,* 61(3), pp. 93-114.

[89] Popper, N. (2015), *Digital Gold*, HarperCollins, New York, p. 82.

[90] IBM Press Release (October 23, 2018), *IBM and Microsoft Announce Partnership Between Cloud Offerings*, https://www.pbsnow.com/ibm-news/ibm-and-microsoft-announce-partnership-between-cloud-offerings/

[91] Jensen, T. (December 12, 2018), *Blockchain Strategize Digital Infrastructuring: Blockchain technology bridging the Document Platforms towards real business value in Maritime Supply Chains*, Pre-ICIS Workshop, San Francisco.

[92] IBM Press Release (January 16, 2018), *Maersk and IBM to Form Joint Venture Applying Blockchain to Improve Global Trade and Digitize Supply Chains*, https://www-03.ibm.com/press/us/en/pressrelease/53602.wss

[93] TradeLens Advisory Board, https://www.tradelens.com/about/

[94] Libra White Paper, https://libra.org/en-US/white-paper/#introducing-libra

[95] Bridget van Kralingen & Mike White at Blockchain Revolution Global 2019. https://youtu.be/7crOWQnz9tw

[96] Bridget van Kralingen & Mike White at Blockchain Revolution Global 2019. https://youtu.be/7crOWQnz9tw

[97] *Blockchain for Zero Hunger*, https://innovation.wfp.org/project/building-blocks

[98] Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

[99] Diedrich, H. (2016), *Ethereum: blockchains, digital assets, smart contracts, decentralized autonomous organizations*, Wildfire publishing

[100] https://bitnodes.earn.com/

[101] http://wiki.p2pfoundation.net/Ethereum
A Next-Generation Smart Contract and Decentralized Application Platform, posted on https://github.com/ethereum/wiki/wiki/White-Paper

[102] In layman's terms, 'Turing Complete' means a programming language has a comprehensive instruction set such that it can be programmed to perform all the other functions of Turing Complete programming languages/Bitcoin's scripting tool is not "Turing Complete" because it has no way to program logic loops, among other missing features. (See https://en.bitcoin.it/wiki/Script for Bitcoins command set.) Buterin proposed that Ethereum would include a Turing Complete programming language to enable coding of smart contracts.

[103] *Is the ether supply infinite?* https://www.ethereum.org/ether

[104] Levi, A. (May 21, 2017), *Corporate Trends in Blockchain*, CB Insights webinar presentation.

[105] Beigel, O. (2017), *What is Ethereum?* posted on March 3 at https://99bitcoins.com/guide-buy-ether-ethereum/

[106] ConsenSys (January 10, 2019), *The Thirdening: What You Need To Know*, https://media.consensys.net/the-thirdening-what-you-need-to-know-df96599ad857

[107] https://www.ethernodes.org/network/1

[108] Ben Sigman (May 8, 2018), *EOS Block Producer FAQ*, https://medium.com/@bensig/eos-block-producer-faq-8ba0299c2896

[109] To view the 21 EOS validator nodes and block producers, see https://bloks.io/vote

[110] https://www.hyperledger.org/members

[111] The Linux Foundation (January 22 2916), *The Hyperledger Project Charter,* available at https://www.hyperledger.org/about/charter

[112] Connell, J. (2017), *On Byzantine Fault Tolerance in Blockchain Systems*, posted June 2017 on https://cryptoinsider.com/byzantine-fault-tolerance-blockchain-systems/

[113] https://www.hyperledger.org/projects

[114] https://www.ibm.com/blockchain/solutions/food-trust

[115] IBM Food Trust Fact Sheet December 2018, https://newsroom.ibm.com/download/IBM+Food+Trust+-+Ecosystem+Fact+Sheet+Dec+2018.pdf

[116] https://libra.org/en-US/white-paper/

[117] https://libra.org/en-US/white-paper/

[118] https://www.mediledger.com/

[119] https://cryptonote.org/whitepaper.pdf

[120] https://en.wikipedia.org/wiki/Monero_(cryptocurrency)

[121] J.P. Morgan Quorum, https://www.jpmorgan.com/country/US/EN/Quorum

[122] Enterprise Ethereum Alliance (July 7, 2017), *Enterprise Etherum Alliance Announces Support for Blockchain Consensus Algorithm Integration*, https://entethalliance.org/enterprise-ethereum-alliance-announces-support-blockchain-consensus-algorithm-integration/

[123] The Quorum White Paper is available at https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum Whitepaper v0.1.pdf

[124] Hackett, R. (October 04, 2016), 'Why J.P. Morgan Chase Is Building a Blockchain on Ethereum', *Fortune Magazine*, posted on http://fortune.com/2016/10/04/jp-morgan-chase-blockchain-ethereum-quorum/

[125] J.P. Morgan Quorum https://www.jpmorgan.com/country/US/EN/Quorum

[126] https://www.ethnews.com/amis-technologies-new-algorithm-handles-more-transactions-per-second
https://github.com/ethereum/EIPs/issues/650
https://ethereumfoundation.org/devcon3/sessions/bft-for-geth/

[127] Quorum White Paper, https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum Whitepaper v0.1.pdf

[128] *QuorumChain Consensus,* https://github.com/jpmorganchase/quorum/wiki/QuorumChain-Consensus

[129] Quorum White Paper, https://github.com/jpmorganchase/quorum-docs/blob/master/Quorum Whitepaper v0.1.pdf

[130] Castillo, M (February 28, 2017), *Microsoft Adds JPMorgan's 'Quorum' Blockchain to Azure Platform,* https://www.coindesk.com/microsoft-azure-jpmorgans-quorum-blockchain/

[131] Castillo, M (February 28, 2017), *Microsoft Adds JPMorgan's 'Quorum' Blockchain to Azure Platform,* https://www.coindesk.com/microsoft-azure-jpmorgans-quorum-blockchain/

[132] https://ripple.com/xrp/

[133] Branson, R. (2015), *Ripple: The Ultimate Guide to Understanding Ripple Currency,* Elliot Branson Publications.

[134] Bauerle, N. (2017), *What is the Difference Between Public and Permissioned Blockchains?* https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains/

[135] https://www.stellar.org/about/mandate/

[136] Maziières, D. (2016), *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*, White Paper, available at https://www.stellar.org/papers/stellar-consensus-protocol.pdf.

[137] https://en.wikipedia.org/wiki/Stellar_(payment_network)

[138] Stellar Funding, https://www.crunchbase.com/organization/stellar

[139] TradeLens Overview (October 2, 2018), https://shipbrokers.fi/wp-content/uploads/2018/10/jeppe-kobbero-tradelens-presentation.pdf

[140] Jensen, T. (December 12, 2018), *Blockchain Strategize Digital Infrastructuring: Blockchain technology bridging the Document Platforms towards real business value in Maritime Supply Chains*, Pre-ICIS Workshop, San Francisco.

[141] Bridget van Kralingen & Mike White at Blockchain Revolution Global 2019, https://youtu.be/7crOWQnz9tw

[142] WineChain token on Ethereum, https://etherscan.io/token/0x49d4c3629f93f49ba934debf28605d26caaf3acc

[143] *Restoring trust in the wine industry, from grape to glass,* https://www.ey.com/en_gl/global-review/2018/restoring-trust-in-the-wine-industry

[144] https://en.bitcoinwiki.org/wiki/DPoS

[145] Delegated Proof of Stake, https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/delegated-proof-of-stake

[146] *Practical Byzantine Fault Tolerance*, Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999, http://pmg.csail.mit.edu/papers/osdi99.pdf

[147] Proof-of-Authority Consensus https://apla.readthedocs.io/en/latest/concepts/consensus.html#advantages-of-poa-consensus

[148] King, S., and Nadal, S. (2012), PPCoin: *Peer-to-Peer Crypto-Currency with Proof-of-Stake*, https://peercoin.net/assets/paper/peercoin-paper.pdf

[149] *Distributed Consensus from Proof of Stake is Impossible,* posted by Andrew Poelstra on https://www.smithandcrown.com/open-research/distributed-consensus-from-proof-of-stake-is-impossible/

[150] Dwork, C., and Naor, M. (1993), *Pricing via processing: Combatting Junk Mail*, http://www.hashcash.org/papers/pvp.pdf

[151] Nakamoto, S. (2008), *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf

[152] https://blockonomi.com/zero-knowledge-proofs/