Blockchains for Government: Use Cases and Challenges

JAMES CLAVIN, SISI DUAN, HAIBIN ZHANG, VANDANA JANEJA, KARUNA P. JOSHI, YELENA YESHA, University of Maryland, Baltimore County
LUCY C. ERICKSON, American Association for the Advancement of Science
JUSTIN LI, Department of Homeland Security, Science and Technology Directorate

Blockchain is the technology used by developers of cryptocurrencies, like Bitcoin, to enable exchange of financial "coins" between participants in the absence of a trusted third party to insure the transaction, such as is typically done by governments. We introduce blockchains, describe their concepts, layout the challenges in using them, and discuss use cases from a governmental viewpoint. We find that a certain type of blockchain, permissionless, has not been adopted in governmental settings, and conclude that permissioned blockchains may best be suited to them due to better scalability, lack of anonymity, and better data integrity guarantees.

CCS Concepts: • **Computer systems organization → Redundancy**; • **Computing methodologies → Distributed computing methodologies**; • **Security and privacy → Distributed systems security**.

Additional Key Words and Phrases: blockchains, applications, security

ACM Reference Format:
James Clavin, Sisi Duan, Haibin Zhang, Vandana Janeja, Karuna P. Joshi, Yelena Yesha, Lucy C. Erickson, and Justin Li. 2020. Blockchains for Government: Use Cases and Challenges. 1, 1 (May 2020), 16 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Blockchain is technology that builds a trustworthy service in an untrustworthy environment. It uses replication of distributed systems to build a decentralized service that achieves the same goals with a trusted centralized one. Since 2008, blockchain implementation has exploded, primarily driven by its native ability to support any type of digital transaction. Blockchains have been adopted by Wall Street investment firms to enable transaction cost reduction, Silicon Valley startups as an alternative means of raising funds through initial coin offerings, and by one government, Venezuela, to encourage global investment into the country. The algorithms that power these distributed transactions have given rise to an altogether new method for securely storing data in a digital world that is oftentimes adversarial. Because blockchain guarantees high service availability as well as data integrity, any industry in which transactions or processes rely on the use of a trusted third party, or where a strong guarantee of security is required, should be considering implementing blockchain solutions, as should governments worldwide.

Authors' addresses: James Clavin, Sisi Duan, Haibin Zhang, Vandana Janeja, Karuna P. Joshi, Yelena Yesha, {jclavin,sduan,hbzhang,vjaneja, kjoshi1,yeyesha}@umbc.edu, University of Maryland, Baltimore County, 1000 Hilltop Cir, Baltimore, Maryland, 21250; Lucy C. Erickson, American Association for the Advancement of Science, Washington D.C., lcerickson@gmail.com; Justin Li, Department of Homeland Security, Science and Technology Directorate, Washington D.C..

XXXX-XXXX/2020/5-ART $15.00
https://doi.org/10.1145/1122445.1122456

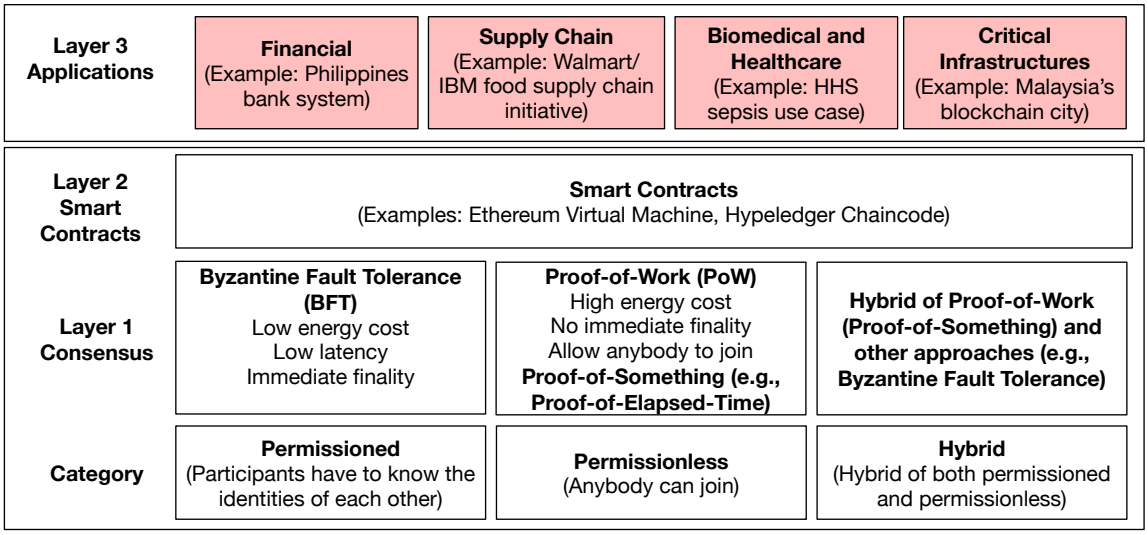

Fig. 1. Overview of blockchains: categories, underlying techniques, and use cases.

What Attributes of a Blockchain May Be of Use in Government? Blockchain provides a means to ensure that any copy of the data will always be available, verifiable, and trustworthy. It functions like an old Xerox machine in terms of data dispersion, in the sense that it can make copies of any item available to anyone who uses it. With respect to trust, it acts more like a notary public, guaranteeing that any copy of data is authentic and that the copies cannot be forgotten or counterfeited. Finally, in terms of transaction processing, it functions like a general ledger in which transactions must be recorded in the same order.

To handle data sharing, transaction processing, and validation, there is a set of replicated servers, called nodes. Each node runs a consensus algorithm, which provides a way to reach agreement with every other node about a given transaction, without any human intervention. The algorithm must enable the system to proceed even when some percentage of the nodes arbitrarily fail. There are various algorithms, discussed in detail later, but it is noteworthy that democratic concepts such as quorum and majority voting are incorporated into them. The overarching goal of such a system is to use replication to provide security (specifically availability and integrity), and to enable the distributed servers to behave like a centralized decision-maker.

How many failures blockchains can withstand—or the percentage of nodes that can fail without compromising security—depends upon the particular use case and the types of failures. For example, a distributed file system may need to withstand "crash" failures, or those failures that occur when faulty nodes simply stop processing requests. Such systems (e.g., Google File System [33]) are commonly able to mask the failures of up to one-half of the nodes. Failures like software bugs, hardware errors, and adversarial (cyber) attacks cause Byzantine faults. Byzantine Fault Tolerant (BFT) systems withstand up to one-third of their nodes failing by providing stronger guarantees between nodes through cryptographic techniques.

Blockchain History. The distributed systems technical concepts that underpin blockchain were proven in 1982 by Leslie Lamport. Lamport introduced and solved the distributed consensus problem for Byzantine Fault Tolerance (BFT), in a proof he named the Byzantine Generals Problem [46]. The solution states that: to tolerate one arbitrary failure, the system requires at least four replicated nodes so that they can reach a consensus on a specific decision. A more generalized statement is that to tolerate f Byzantine failures, the system has to have $n \geq 3f + 1$ nodes. In 1999 Miguel Castro and Barbara Liskov became the first to apply Lamport's

consensus in a functioning algorithm which they called “Practical Byzantine Fault Tolerance (PBFT).” [19] In 2008, a pseudonymous individual, or group, named "Nakomoto" used consensus protocols, similar to BFT, to create Bitcoin. Bitcoin’s innovation was to build a decentralized system as a trusted broker for exchanging money, and acts in a similar role as to the government and banking systems do with cash. Viewed historically, people used different types of exchange for trading things of value. In the case of Bitcoin, one of the most famous first purchases was pizza. Purchasing that same pizza over the ages would have been done differently, as is shown in Fig. 2, each with different trust providers.

Bitcoin uses an approach called “Proof-of-Work (PoW)” based consensus (described in greater detail later) to allow users to exchange digital “coins” with each other with confidence. Different from the classic BFT protocols which tolerates a fraction of node failures, PoW assumes a slightly different failure model called "computational threshold failure model". The system is considered valid so long as no adversary controls more than 51% of the total computational power. Through PoW, the system supports an open and transparent pseudonymous environment where any user can participate. But, PoW requires a lot of compute power, as the Bitcoin system retools itself constantly to keep the algorithm tuned to enforce time restrictions on transaction validation.

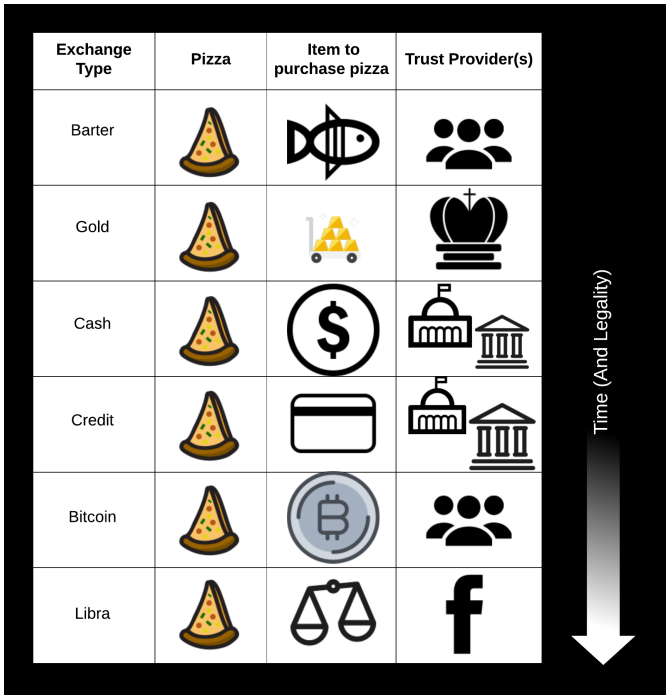

Fig. 2. The evolvement of how people exchange products (from exchanging products directly, to using currency, credit, cryptocurrency, up to the possible future, with Facebook proposing "Libra.").

In this article, we review what a blockchain is, how the underlying mechanism works, the technical and adoption challenges, and the governmental use cases. There are several survey papers in the literature, [23, 74], including ones about the consensus mechanisms for both permissionless [56, 73] and permissioned blockchains [16], as well as for BFT protocols [23, 62]; some papers have reviewed blockchain applications with a focus on e-government [7, 12]. Compared with existing survey papers, we aim to review the governmental applications of blockchains, with a focus on the technical perspective of the applications. Indeed, one of the major challenges for blockchain adoption

is the gap between the underlying technology and the understanding of the capabilities [16, 21]. Therefore, reviewing the use cases and applications of blockchains from the technical perspective can help both technical developers better understand how the technology could be improved and also decision makers better understand the pain points of the technology limitations and capabilities.

The rest of the articles is organizing as follows with an aim to answer the following questions.

- What is blockchain, its security goals, and its underlying mechanism?
  This is not considered as a *new* contribution. Indeed, a lot of online and research articles have introduced blockchain concepts. However, we found that a lot of existing articles provide inaccurate information or describe the concepts in greater details which make it challenging for general audience. Therefore, we answer the question by introducing different layers of blockchains, their capabilities, and how each layer is composed technically. Specifically, we layout in detail a 3-layer view of the technology used in both permissionless and permissioned blockchains and discuss their capabilities and limitations. With a slant toward government usage, the section will provide a foundation to discuss applications built on top of the technology. (Sec. 2)
- What are the adoption and technical challenges?
  Blockchains cannot solve *all* the problems. In fact, blockchain is not mature yet, as challenges exist for both adoption and technology development. It is desirable to discuss the challenges from both adoption and technology development perspective. Understanding the adoption challenges will lead the direction development of the technology. On the other hand, understanding the technical challenges will foster the adoption of the technology. In Sec. 3, we summarize and discuss both adoption and technical challenges, and discuss the potential solutions to address the problem.
- What are the governmental use cases for blockchains? What is the *best* blockchain model for each use case? What are the lessons learned?
  In Sec. 4, we present use cases from both researchers and white papers in the field, as well as those applied by decision makers around the world. We aim to group the applications by regions and countries to observe the *trend* in the adoption of blockchains. For each type of use cases, we also aim to discuss whether it is *appropriate* to use blockchain as a solution, the technical challenges, and how the challenges could potentially be solved.

2 BLOCKCHAIN CONCEPTS

All blockchains work to make decentralized nodes achieve an agreement on the total order of transactions through cryptography and an underlying consensus mechanism. Technically, blockchains generally fall into one of two categories: "permissionless" or "permissioned." Permissionless blockchains allow anyone to participate, are considered “open,” and have trust provided by algorithms. In contrast, permissioned blockchains are usually “private” or “consortium” and all participant identities are known but no participant needs to be trusted. In practice, variants exist where there is no clear line between different types of blockchains. For instance, Ethereum, a typically permissionless blockchains, can be setup as a private blockchains called Ethereum private network [1]. Efforts have also been made to achieve anonymity for permissioned blockchains [14, 40].

2.1 A Layered View of Blockchain

Blockchains can be abstracted into three different layers [4], as illustrated in Fig. 1. At the core of blockchain is layer 1: BFT consensus - also known as state machine replication - which is a generic approach to tolerate failures. BFT consensus has different forms, ranging from conventional BFT protocols to PoW based consensus. Despite fundamental differences in how consensus is achieved, any form must solve the same problem: how to enable nodes to reach consensus on the total order (i.e. consistency) of transactions submitted by clients in

the form of requests. After nodes reach a consensus about the order, the data/operations of the transactions are then processed according to the order of the transactions. As a result, distributed nodes functionally behave as if there were one centralized node. This ensures that there is only one sequence of client transactions, known as “the longest chain." Layer 2 of blockchain is the smart contract, which provides an interface for blockchain developers to implement new functions. Smart contracts can then facilitate, verify, or enforce the execution of business transactions. A smart contract can be viewed as a program that connects the underlying consensus protocols with layer 3, applications and use cases.

2.2 Building the Hash Chain

The cryptographic concepts of "hashing" and "digital signatures" provide tamperproofing and validation. One way hash functions generate a unique output of alphanumeric text given an input of a list of transactions. Change a single thing about the list of transactions, and the resulting hash is significantly different. Digital signatures, like Rivest–Shamir–Adleman (RSA) or Elliptic Curve Digital Signature Algorithm (ECDSA) are used to "sign" transactions. The hashes are then linked together in a chain of blocks, with any block accept the first one, called the genesis block, pointing to prior hashes and signatures. Such a hash chain ensures that no one can manipulate the contents of any block or reverse the chain order.

2.3 Permissioned Blockchains

Permissioned blockchains provide consensus and security through the use of provably secure distributed consensus protocols. The consensus protocols do not involve and expensive procedures such as PoW. Therefore, permissioned systems have low latency (the time between the client sending a transaction until the client receives a reply); they are also scalable (both in the number of clients and transactions as well as the number of servers) [71]; and they consume less energy than permissionless blockchains (described in detail later).

Most permissioned blockchains, especially those widely employed or piloted by government, use provably secure BFT protocols. Among these BFT solutions, the leader-based protocols are widely used, e.g., PBFT [19] and its variants [67, 69]. In these types of protocols, there is a specific leader, which proposes the order of transactions. The nodes then communicate with each other in several steps to reach agreement on the order. In most leader-based protocols, each node sends messages to all other nodes in each step and collects matching messages from a fraction of nodes before moving to the next step. If the leader is potentially faulty or malicious, other nodes will run a leader change protocol until a new leader is elected.

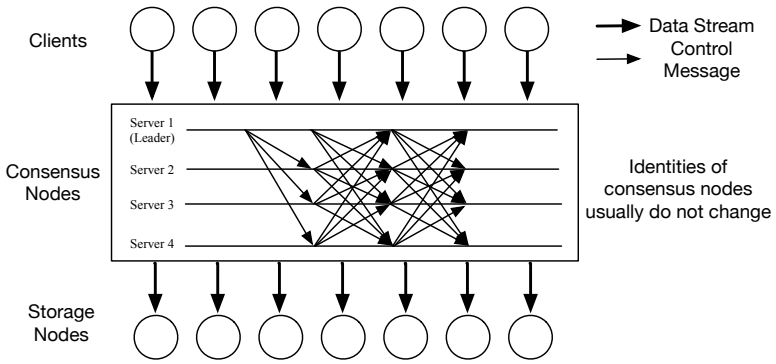

Fig. 3. The normal operation for a permissioned blockchain running a BFT protocol Practical Byzantine Fault Tolerance (PBFT) [19]. Control messages refer to the messages for nodes to reach a consensus.

On top of the consensus protocols, blockchains have different approaches to store the transactions. Fig. 3 illustrates a typical system architecture used by permissioned blockchains. Specifically, after receiving requests from the clients, a number of nodes run a BFT protocol to assign order to the transactions. The transactions and their order are then forwarded to all other nodes in the system. Finally, the transactions are stored and processed according to that order. In this architecture, the nodes that store the transactions act as *learners* that passively learn the order from the consensus nodes.

Numerous BFT protocols have been proposed in the literature [22, 24, 27, 29, 38, 67]. Chain-based approaches organize nodes in a logical chain where a node only needs to communicate with its previous node and its subsequent node, if any [28], avoiding the all-to-all communication described previously, resulting in performance improvements. Another approach is a hybrid that combines BFT protocols; e.g., Aliph [38]. The reason Aliph take a hybrid approach is to combine the best features from more than one BFT protcol because there no one-size-fits-all consensus protocol exists. In Aliph, the protocol can use one cheap protocol to achieve great performance with fewer failures. When failures occur or become more frequent, the system switches to another more expensive one to guarantee system security.

2.4 Permissionless Blockchains

Most permissionless blockchains adopt a "Proof-of-Something" strategy. In the case of Bitcoin, this is Proof-of-Work (PoW), a mathematical challenge offered to all nodes in the system to try to overcome (or work though) by an activity called mining. Once mined, a node can propose a block of transactions and get rewarded in Bitcoin if the proposal is accepted. The drawback to this approach is that throughput (the number of transactions processed per second) is limited, and the energy consumption is high. Furthermore, collusion occurs - nodes form cartel-like entities called mining pools - concentrating mining activity under the control of one organization. With mining pools, the blockchain becomes less decentralized and therefore less secure, and more susceptible to attack and manipulation.

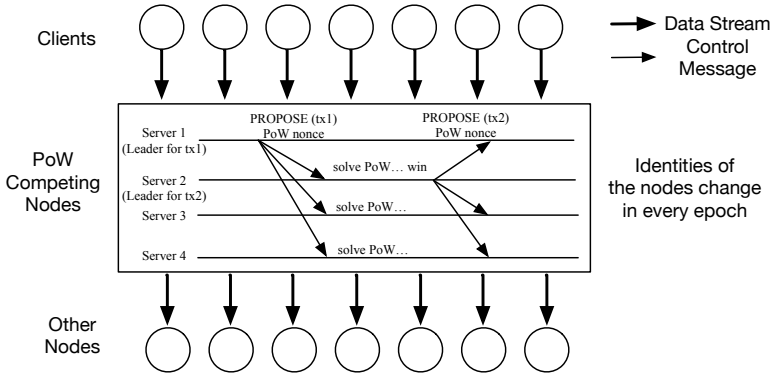

Fig. 4. The message flow for Proof-of-Work (PoW) based blockchains. Control messages are the messages for nodes to compete for PoW.

Compared with BFT based consensus, PoW based consensus does not have a fixed leader and can be viewed as a system where the leader changes after each block of transactions. In order to propose a new transaction, a node needs to first solve PoW from the previous transaction. When a node proposes a transaction n, it also generates a pseudorandom number that is called a cryptographic nonce. As illustrated in Fig. 4, the nonce is broadcast to all other nodes. Nodes compete to become the next leader by selecting random pending transactions and generating a hash of the selected transactions. The node that first generates a hash smaller than the nonce

Table 1. Permissionless systems/cryptocurrency and the proof they use to come to a consensus.

System/Cryptocurrency	Proof-of-Something	Strategy
Bitcoin [54], Ethereum [75]	Proof-of-Work	Computing a nonce
Ethereum, Hybrid Consensus [61], Elastico [49]	Proof-of-Stake	PoW with weighted value
Hyperledger Sawtooth [58]	Proof-of-Elapsed-Time	PoW done by computer processors
PoA Network [3]	Proof-of-Authority	PoS with weighted reputation

value is the winner, and becomes the next leader. Compared with BFT consensus, PoW based consensus involves fewer messages for nodes to reach a consensus on the transactions. The blockchains based on it can easily scale to thousands of nodes. The challenge is that more than one node might solve the puzzle at the same time, creating a fork of the hash chain. Nodes in the PoW consensus will detect the fork, eventually agree on the longest hash chain, and use it. It takes time for each transaction to be finalized after it has been proposed, usually after six blocks, each taking about 10 minutes, in the case of Bitcoin - about an hour. This finalization time can be reduced using different approaches.

Multiple Proof-of-Something approaches have been proposed to enhance the performance of PoW based consensus, some of which are shown in Table 1. The workflow usually remains the same but the protocols use other strategies. For instance, Proof-of-Elapsed-Time (PoET) replaces PoW with trusted hardware, using Intel Software Guard Extension (SGX), a Trusted Execution Environment (TEE). Specifically, computers running an Intel SGX processor have a set of security-related instruction codes built into them that makes the piece of hardware *protected*. Instead of generating hash to solve PoW, every node utilizes SGX to wait for a random amount of time. The node that finishes waiting earlier than all other nodes 'wins' and can propose new transactions. PoET is in use as a consensus option in the Hyperledger Sawtooth platform [58]. The major benefit is a greatly improved system performance. The drawback is that each TEE has its own vulnerability and one has to trust a single vendor to use the blockchain. Other examples include Proof-of-Stake (PoS) and Proof-of-Authority (PoA). PoS and PoA are each designed to improve the performance of Ethereum, and in both a small group of nodes is selected as *representatives*. PoA selects the representatives based on their reputation, whereas PoS selects representatives using one of several approaches. In Delegated PoS (DPoS), nodes can *vote* for certain replicas to select them as representatives. After the group of representatives are selected, the nodes have the authority to propose new transactions and notify others of the results. The major challenge with representative based systems is that the selected representatives must behave correctly in order to ensure system correctness. For instance, in PoA, the reputation system must be trusted and one has to assume that malicious nodes do not have motivation to build up their reputation and then corrupt the entire system.

2.5 Smart Contracts

Smart contracts are programs that automatically *fire* when nodes come to consensus, without any human intervention. The nodes are configured to check a series of conditions to see whether or not the triggering criteria has been met. If the requirements are met, then the nodes execute an agreed upon *contract*, a program that executes business-defined functions. Smart contracts allow users to deploy new capabilities and functions while the blockchains are running; services do not have to be stopped. Specifically, developers could write a new smart contract that includes a set of functions. After the contract is deployed on the blockchain, authorized users could call the contract to use those functions. Other running services on the blockchain do not have to be interrupted at all to support these new functions. The most popular smart contract platforms include the Ethereum Virtual Machine (EVM, written in a language called Solidity) and Hyperledger Fabric's Chaincode (written using a combination of the languages Go, node.js, and Java). Since all blockchain transactions are included in the hash

chain, and therefore unchangeable, having a bug in the contract, or a flaw that can be exploited, introduces risk into the system. It is also worth noting that the use of smart contracts will likely degrade the performance of the system, as observed by several research papers [9, 39].

2.6 Blockchain vs. Databases

Modern databases are frequently designed to be replicated and distributed to achieve high reliability. The most typical method is primary-backup replication, in which the data are replicated as copies across multiple servers or virtual machines. When one copy is lost, additional copies are available to continue the service. This shares certain similarities with blockchain systems, with three major differences. First, distributed databases focus on the management of data. In contrast, blockchains aim to ensure data security. Second, blockchain systems aim to tolerate Byzantine/arbitrary failures, whereas distributed databases usually handle only crash failures. Third, blockchain systems aim to achieve the strongest guarantee of data consistency across multiple machines, whereas distributed databases usually only achieve weaker guarantees of data consistency, e.g., causal consistency [15]. In causal consistency, data can be written concurrently by different nodes, introducing potential conflicts to be resolved later. In comparison, blockchain systems guarantee linearizability, the strongest consistency guarantee in distributed systems [41]. Informally, linearizability ensures that the data are always consistent across all the nodes so the distributed nodes behave like a centralized one.

3 CHALLENGES AND CONSIDERATIONS

In a 2018 report on cryptocurrencies and blockchain in Europe and Central Asia, the World Bank states, "...policy makers should strike a balance between curbing the hype surrounding these new technologies and unleashing potentially transformational new opportunities. While encouraging and facilitating these innovations, they should prepare to craft new regulations to create a level playing field for new and old industries, by adjusting financial oversight, consumer protection, and tax administration" [37]. Indeed, there is still a gap between the hype and the reality. Several challenges and concerns exist before the technology becomes mature. In this section, we review a few adoption challenges and technical challenges, and also discuss the potential solutions to the challenges.

3.1 Adoption Challenges

Industry Adoption. Grasping the different implementations of blockchain and their capabilities pose challenges for decision makers when it comes to data governance, privacy and security regulations, and standards [26, 72]. For instance, it was stated that establishing standards to address the security and resilience in data governance concerns for bloccкhains will greatly help create trust in the technology [26]. As a result, adoption of blockchain requires organizations that are willing to take the risk and have dedicated budgets for research and development. Currently, both academic and industrial efforts have been made to discuss and create standards for blockchains [2, 26], the effect of which are yet to be discovered.

Data Quality. Blockchain does not protect against data from untrustworthy sources, i.e., authorized but potentially tainted parties. It cannot prevent well-formatted but incorrect or inaccurate data from being sent and stored in the system [77]. As a result, blockchain may be used as an illegal content distribution channel. The system may also consist of data with low quality or high inaccuracy. Although blockchain can be used as an auditing system for validating these data, the data are already distributed and cannot be retrieved from all parties with certainty. A decentralized system that allows any two parties to anonymously exchange assets may provide a safe haven for those wishing to perform illicit activities without fear of reprisal. As a result, existing solutions usually involve additional layers to detect or ensure data quality [18, 77]. It is not clear whether such a layer will provide the desirable analysis and become generic enough to ensure data quality.

Correctness and Security of the System. Several blockchain systems intentionally make their consensus protocols proprietary, making it difficult to trust in the correctness and security of the platforms [16]. Consensus protocols are complicated and the implementation in a complex real system requires extensive development, which may introduce unintended consequences, as has been observed [20]. Before adopting a blockchain solution, the underlying mechanism and the system implementation should be carefully reviewed.

3.2 Technical Challenges

The Performance Trade-offs. There is no one-size-fits-all blockchain system [11, 24, 38, 71]. Different approaches have been proposed to meet different needs such as improved latency, throughput, scalability, and bandwidth [22, 24, 28, 38]. Before widespread development and adoption, some innovative first movers must implement solutions that consider the trade-offs among security, efficiency, and robustness.

Although significant effort has been put into developing new blockchain platforms, it is not easy to develop both correct and efficient systems. In fact, developing consensus protocols is similar to engineering cryptographic systems, which require expertise in cryptography, security, and the theory of distributed systems [16]. Therefore, expert review, validation of both the theory and implementation of new blockchain platforms, and standards recommendation [2] (such as cryptocurrency exchanges, running blockchains in applications such as clinical trials, etc.) are desirable if the full potential of blockchain is to be realized.

Scalability. Both permissionless and permissioned blockchains have scalability limits [71]. The open nature of the consensus mechanisms of permissionless blockchains allow anyone to join and therefore usually involves thousands of nodes. The problem for such blockchains is that they usually suffer from long transaction latency and have not scaled to a large number of client transactions in real world applications. On the other hand, permissioned blockchains can scale to a large number of clients with less latency, but they rely upon a small number of blockchain servers. Hybrid blockchains address the scalability problem [5, 32, 43, 44, 49, 61, 76], but each has its own challenges and most have a sufficiently large number of representatives to guarantee safety and liveness; e.g., greater than 600 [49]. A BFT protocol of such a size, however, can be impractical. Other BFT algorithms, such as the cryptocurrency Algorand [34], remove the need to run PoW by applying proven crytographic techniques along with verifiable random functions, and committees, but - again - has a limitation. Algorand relies upon the number of coins, which might limit its practicality in real-world deployment. The optimal blockchain that balances scalability for both clients and servers has yet to be found.

Privacy and Compliance. Although conventional blockchains provide availability and integrity, the data are essentially transparent–all participants may freely review transactions. This means an architect should be careful in selecting the type of blockchain, and perform a use case analysis that includes privacy and security guarantees relative to performance needs. With the current regulatory climate of governments focused on protecting user data, blockchains become especially problematic given their open and immutable nature. At the same time, laws designed to safeguard the privacy and security of individual's information do provide a roadmap for designers. Generalized examples include the California Consumer Privacy Act of 2018 (CCPA) and the European Union's General Data Protection Regulation of 2016 (GDPR). In the healthcare space, the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act are the basis for interoperability rule changes proposed by the Office of the National Coordinator as well as the Center for Medicare and Medicaid Services (CMS). With HIPAA and HITECH in mind, researchers at MIT built a PoW consensus protocol called Medrec for mining patient information. This type of clinical data is becoming standardized through the implementation of Electronic Health Records (EHR) systems that leverage messaging protocols, such as Health Level 7 (HL7) [10].

Timing Assumptions. Most permissionless blockchains assume a synchronous network, which is not a practical assumption. In order for the system to be correct (safety and liveness), there must be a large number of nodes that actively participate. Therefore, the correctness of such a system in a small-scale or private setting can be questionable. On the other hand, most permissioned blockchain protocols assume something called partial synchrony [30], in which the network delay and processing delay by the nodes are bounded by an upper limit unknown to all nodes. It is assumed that each node in the network will eventually respond, and if a given node does not respond, other nodes will handle it according to the protocol, providing an answer and ensuring the network will not get stuck waiting indefinitely. The shortcoming of this approach is that it introduces performance and security issues—what if an adversary can somehow manipulate this network delay in such a way that causes nodes to misbehave or to give up information? In this type of network, the system may simply stop processing any requests just like a crashed service, even if all the nodes in the system are correct. A potential solution to this may be the use of what is known as a purely asynchronous BFT consensus protocol, in which nodes have no upper bound in response time so the protocols are resilient to all kinds of attacks. Research into this area is ongoing and includes several possible solutions [6, 29, 50, 53].

4 GOVERNMENT ADOPTION OF BLOCKCHAIN

We have done an review of the known projects and use cases supported by governments across the world. Our goal is to provide a comprehensive, but not exhaustive, list. Our purpose is to discuss several applications that are both *representative* and *meaningful*. Indeed, with the increasing interests in blockchains, applications can be discovered in potentially all industries. A lot of them, however, are far away from being practical or useful. Therefore, we select the representative use cases and group them by countries and regions. In this way, we will be able to better see the *trend* in government use cases.

In this section, we review the governmental efforts made by countries world-wide in piloting blockchain solutions, the setup, and lessons learned. Since blockchains are widely used by cryptocurrencies, the majority of the applications reviewed were financial, and are summarized in Table 2, ordered according to the number of use cases we found. In Table 3, we include other domains such as medical, infrastructure, city governance, asset and data management and education.

4.1 US Government

The U.S. Health and Human Services (HHS) Department has developed an application called Accelerate for management of contract billing that utilizes blockchain, AI, ML and process automation. Accelerate is designed to better manage the HSS portfolio of 100,000 contracts worth around $25B across about 50 systems. The blockchain within Accelerate captures a pointer to unstructured data (such as documents), rather than storing the data itself. Accelerate was able to get contract information dispersed across the entire organization through replication of data, and became the first blockchain based application to be certified by the Designated Approving Authority as having the Authorization to Operate [51]. Accelerate was expanded to acquisition management – getting contract information to researchers more readily, so they could find and cost suitable materials for their research. HHS has projected savings at the point of purchase of up to $720M over time and may expand Accelerate into clinical data – HHS leadership discussed using blockchain for tracking sepsis data [65].

Research is being done by the United States Centers for Disease Control and Prevention (CDC) to use blockchain to help track public health outbreaks such as Hepatitis A [59]. In 2017, the chief software architect for the CDC's Center for Surveillance Epidemiology, and Laboratory Services began building proofs of concept for improving surveillance across state lines. Since then, the CDC and IBM have come together to work on a blockchain-backed solution for tracking the ongoing opioid disease crisis [52]. We assume using blockchain to track COVID-19 is a consideration. Fig. 5 shows that interest in blockchain for use in biomedical applications is growing rapidly after

Table 2. Global adoption of blockchain solutions and government adoption.

Country	Financial Systems	Governmental Adoption	National Cryptocurrency	Regulation
China	Strongly discouraged. Private industry only	Supportive	Yes, in progress	Yes, banned most cryptocurrencies.
United States	Private Industry	Yes	No	Forthcoming, disorganized
Switzerland	Private-public, positioning itself as a hub; home of Libra	Supportive	No	Forthcoming, organized
Russia	Private industry	Supportive	No	Forthcoming, financial, tax regulation
Philippines	Private-public	Supportive	No	No with certain guidelines
New Zealand	Private-public	Supportive	No	Yes, tax regulation
Malaysia	Private-public	Supportive	No	Yes, finance regulation
Japan	Private-public, focus upon cryptocurrency exchanges	Supportive	Yes, treats cryptocurrency as assets	
Brazil	Private-public, government active in monitoring cryptocurrencies and startups	Unknown	No	Yes, tax regulation
Venezuela	Private-public	No	Yes	No
Estonia	Private-public	Supportive	No	Yes, tax regulation, anti-terrorism
Australia	Private-public, securities exchange runs on blockchain	Supportive	No	Yes, tax regulation
Argentina	Private-public	Supportive	No	Yes, tax regulation
Uruguay	Unknown	Use Bitex	Unknown	Unknown
Portugal	Unknown	Supportive	No	None

Table 3. Blockchain use cases adopted by governments and the focus of blockchain applications.

Use Cases	Representative Countries	Focus
Medical and Healthcare	China, US, Switzerland, Phillippines Japan, Brazil, etc.	Supply chain, IoT, etc.
Financial applications	(Almost) All	Cryptocurrencies, asset management, etc.
Critical Infrastructures	South Korea	Asset management, optimization, etc.
Blockchain City	Malaysia	Cryptocurrency, data management
Asset Management	Georgia, Sweden, Switzerland	Land registry, property transactions, etc.
Education	Japan, Malta	Certificate management
Data Management	Phillipine, Australia	Cloud data management

many years of no published research. Most of these publications are for theoretical research, with few discussing deployment of blockchain at the point of care. Several discuss blockchain's tamper resistant property, as well as its distributed nature - attributes relevant for health data interoperability. These blockchains tend to be private

permissioned ones; Ethereum is studied because of its smart contract capability, and Hyperledger Fabric because it is open source and has some support from large organizations such as IBM.

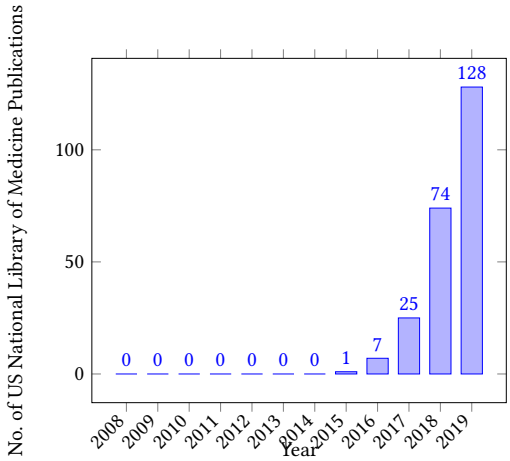

Fig. 5. National institutes of health Blockchain articles since Bitcoin was created.

4.2 Asian Governments

In 2019 the Filipino government approved the adoption of an Ethereum-based solution for about 80 rural banks to get access to financial services. Motivating the effort is the fact that only 42% of Filipinos aged 15 or older have a bank account due to a combination of factors [25, 78].

The concept of *blockchain city* has been used and made live at Malaysia's Melaka Straits city, a tourist city funded by the Chinese government. The project aims to use blockchain to track tourist visas, passengers, luggage, and booking services [64]. The city will also manage its own token, the DMI coin, for tourists to exchange their money into digital currencies for payment in the city via their mobile phones.

South Korea's government announced a 4 billion Korean won (KRW) (about $3.5 million) award to set up a blockchain-enabled virtual power plant in the city of Busan, the country's second-most populous city [60]. The power plans is to be cloud-based and should integrate multiple energy resources in order to optimize power generation.

4.3 European Governments

The European Horizon program supports blockchain projects across the European Union [70]. Luxembourg launched a digital Luxembourg initiative in 2017, with a focus of building a blockchian governance framework. The purpose is to build a blockchain competence community and develop blockchain governance standards; the project is still ongoing.

The e-Estonia program [31] supports multiple features such as e-identity, e-healthcare, and e-governance. Most are already operational, with 98% of Estonians filing tax declarations completed online, and 99% of their health data digitized and stored on blockchain. Although issues and concerns still exist [57, 68], blockchains have indeed revolutionized the way this government stores and processes data.

Countries such as Georgia, Sweden, and Switzerland use blockchains to manage assets [8]. Georgia (at the juncture of Asia and Europe) has implemented blockchain for land title registry and related property transactions;

the technology has helped make the process more efficient [66]. Sweden, too, has created a blockhcain-based application for land registration and real estate transactions [48].

Blockchain in education has been applied; [35, 36]; the Maltese government recently completed the first national pilot of a blockchain to manage academic credentials such as diplomas, school certificates, and transcripts. This has been shown to improve the safety of personal information, minimize bureaucracy, and allow students to access their credentials more easily.

4.4 Others

Several major Australian government departments use cloud-based blockchain solutions, or Blockchain-as-a-Service [55]. The Canadian government launched a pilot recently to use blockhcain for digital credentials management, allowing employees to maintain a permanent, self-owned and secure records of their digital credentials [47]. Anti-money launering (AML) is another major initiative for several governments [42, 45, 63]. For instance, the Financial Action Task Force (FATF), an intergovernmental organization, issued guidelines on virtual asset again anti-money laundering and counter-terrorist financing regulations [42]. It has been shown that existing approaches are effective in balancing between the threats and opportunities. Continuous monitoring and investigation are desirable as the technology rapidly changes [17].

4.5 Discussion

Permissioned vs. Permissionless. The majority of government blockchain implementations are permissioned. Although some use permissionless blockchain, in these cases the blockchain is still deployed in a closed, private setting. Fully permissionless blockchains in a government application remain to be seen. The majority of the countries we studied for blockchain adoption have either banned or regulated cryptocurrencies, which are fully permissionless, leading us to conclude it unlikely, without significant change in government or demand by citizens, that a permissionless blockchain will be adopted by any government.

The Quest for High Performance. We have not found any published results that have measured performance, or assessed the performance needs, in government blockchain implementations. Many applications are new, and the long-term feasibility will depend upon a cost-benefit analysis. Many use cases involve large volumes of data, though, so we expect scalability and throughput needs for these systems to drive changes to their blockchain implementation.

The Quest for Technology Improvement. We have found little information regarding the feedback or lessons learned based upon government blockchain implementations. We believe this to be in part because most projects are still in their early stages. We advocate for research and industry to continue to collaborate and improve systems, based upon our observations of past successes [16, 20].

Regulation. As shown in Table 2, many countries have developed regulations for cryptocurrencies, and yet, no country has fully determined how to implement the regulations. Part of the challenge is how to classify cryptocurrencies using existing financial constructs. Taxing or regulating a cryptocurrency as a currency, a security, or an asset is difficult, as a cryptocurrency can be any one or all three.

5 FUTURE OF BLOCKCHAIN AND CONCLUSION

Blockchains have evolved beyond cryptocurrencies to general-purpose, and can be used across an array of applications, particularly those that need high service availability and data integrity. If their adoption increases, then blockchain-based solutions may reintroduce a trusted broker: the data center, whether in the cloud or on premise. A cloud based blockchain system makes the cloud provider into a new type of trusted broker. If nodes are rather on premise of the organization, but are used by the public, then the organization becomes the trusted

broker, and the system becomes vulnerable to any failures that may render the entire system unreliable. So replacing a fallible human or bureaucracy with a blockchain may shift risk, rather than eliminate it [13].

The technical challenges for blockchains, such as being fully privacy preserving, ensuring compliance when necessary, and being scalable, have yet to be fully solved and more work is needed to address them. Yet despite these challenges, blockchains can make applications better and will begin to be the solution for use-case specific distributed systems problems. Most of blockchain applications have been financial at first, just as many good and proven technologies have been. Blockchains are now being used in other spaces, like government. They may be the best technology to deploy when a need to distribute data through a system that needs to guarantee data integrity and service availability exists, but the ability to make it happen is limited.

REFERENCES

[1] [n.d.]. Ethereum private network. https://github.com/ethereum/go-ethereum/wiki/Private-network.
[2] [n.d.]. IEEE Blockchain Standards Initiatives. https://blockchain.ieee.org/standards.
[3] [n.d.]. POA Network. https://www.poa.network/.
[4] Ittai Abraham, Dahlia Malkhi, et al. 2017. The blockchain consensus layer and BFT. *Bulletin of EATCS* 3, 123 (2017).
[5] Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Alexander Spiegelman. 2017. Solida: A blockchain protocol based on reconfigurable Byzantine consensus. In *OPODIS*.
[6] Ittai Abraham, Dahlia Malkhi, and Alexander Spiegelman. 2019. Asymptotically Optimal Validated Asynchronous Byzantine Agreement. In *Proceedings of the Symposium on Principles of Distributed Computing*. ACM, 337–346.
[7] Ahmed Alketbi, Qassim Nasir, and Manar Abu Talib. 2018. Blockchain for government services—Use cases, security benefits and challenges. In *2018 15th Learning and Technology Conference (L&T)*. IEEE, 112–119.
[8] David Allessie, Maciej Sobolewski, Lorenzino Vaccari, et al. 2019. *Blockchain for digital government: An assessment of pioneering implementations in public services*. Technical Report. Joint Research Centre (Seville site).
[9] Elli Androulaki, Artem Barger, Vita Bortnikov, Christian Cachin, Konstantinos Christidis, Angelo De Caro, David Enyeart, Christopher Ferris, Gennady Laventman, Yacov Manevich, et al. 2018. Hyperledger fabric: a distributed operating system for permissioned blockchains. In *EuroSys*. ACM, 30.
[10] Asaph Azaria, Ariel Ekblaw, Thiago Vieira, and Andrew Lippman. 2016. Medrec: Using blockchain for medical data access and permission management. In *2016 2nd International Conference on Open and Big Data (OBD)*. IEEE, 25–30.
[11] Jean-Paul Bahsoun, Rachid Guerraoui, and Ali Shoker. 2015. Making BFT protocols really adaptive. In *IPDPS*. IEEE, 904–913.
[12] F Rizal Batubara, Jolien Ubacht, and Marijn Janssen. 2018. Challenges of blockchain technology adoption for e-government: a systematic literature review. In *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*. 1–9.
[13] Spencer Bogart. 2019. The past & future of blockchain: Where we're going and why. https://medium.com/blockchain-capital-blog/the-past-future-of-blockchain-where-were-going-and-why-2b26acb45091.
[14] Christian Cachin, Daniel Collins, Tyler Crain, and Vincent Gramoli. 2019. Byzantine Fault Tolerant Vector Consensus with Anonymous Proposals. *arXiv preprint arXiv:1902.10010* (2019).
[15] Christian Cachin, Rachid Guerraoui, and Luís Rodrigues. 2011. *Introduction to reliable and secure distributed programming*. Springer Science & Business Media.
[16] Christian Cachin and Marko Vukolić. 2017. Blockchain consensus protocols in the wild. In *DISC*. 1:1–1:16.
[17] Malcolm Campbell-Verduyn. 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change* 69, 2 (2018), 283–305.
[18] Roberto Casado-Vara, Fernando de la Prieta, Javier Prieto, and Juan M Corchado. 2018. Blockchain framework for IoT data quality via edge computing. In *Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems*. 19–24.
[19] Miguel Castro and Barbara Liskov. 2002. Practical Byzantine fault tolerance and proactive recovery. *ACM Transactions on Computer Systems (TOCS)* 20, 4 (2002), 398–461.
[20] Tushar D Chandra, Robert Griesemer, and Joshua Redstone. 2007. Paxos made live: an engineering perspective. In *Proceedings of the twenty-sixth annual ACM symposium on Principles of distributed computing*. 398–407.
[21] James Clavin and Sisi Duan. 2019. Global Transformation with Blockchain: From Lab to App: Workshop Summary.
[22] Allen Clement, Edmund L Wong, Lorenzo Alvisi, Michael Dahlin, and Mirco Marchetti. 2009. Making Byzantine Fault Tolerant Systems Tolerate Byzantine Faults.. In *NSDI*, Vol. 9. 153–168.
[23] Miguel Correia, Giuliana Santos Veronese, Nuno Ferreira Neves, and Paulo Verissimo. 2011. Byzantine consensus in asynchronous message-passing systems: a survey. *International Journal of Critical Computer-Based Systems* 2, 2 (2011), 141–161.

[24] James Cowling, Daniel Myers, Barbara Liskov, Rodrigo Rodrigues, and Liuba Shrira. 2006. HQ replication: A hybrid quorum protocol for Byzantine fault tolerance. In *OSDI*. USENIX Association, 177–190.
[25] Asli Demirguc-Kunt, Leora Klapper, Dorothe Singer, Saniya Ansar, and Jake Hess. 2018. *The Global Findex Database 2017: Measuring financial inclusion and the fintech revolution.* The World Bank.
[26] Advait Deshpande, Katherine Stewart, Louise Lepetit, and Salil Gunashekar. 2017. Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards. *Overview report The British Standards Institution (BSI)* (2017), 1–34.
[27] Sisi Duan, Karl Levitt, Hein Meling, Sean Peisert, and Haibin Zhang. 2014. ByzID: Byzantine fault tolerance from intrusion detection. In *SRDS*. IEEE, 253–264.
[28] Sisi Duan, Hein Meling, Sean Peisert, and Haibin Zhang. 2014. BChain: Byzantine Replication with High Throughput and Embedded Reconfiguration. In *OPODIS*. 91–106.
[29] Sisi Duan, Michael K Reiter, and Haibin Zhang. 2018. Beat: Asynchronous bft made practical. In *CCS*. 2028–2041.
[30] Cynthia Dwork, Nancy Lynch, and Larry Stockmeyer. 1988. Consensus in the presence of partial synchrony. *Journal of the ACM (JACM)* 35, 2 (1988), 288–323.
[31] E-Estonia. [n.d.]. *https://e-estonia.com.*
[32] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. 2016. Bitcoin-NG: A Scalable Blockchain Protocol.. In *NSDI*. 45–59.
[33] Sanjay Ghemawat, Howard Gobioff, and Shun-Tak Leung. 2003. The Google file system. In *Proceedings of the nineteenth ACM symposium on Operating systems principles*. 29–43.
[34] Yossi Gilad, Rotem Hemo, Silvio Micali, Georgios Vlachos, and Nickolai Zeldovich. 2017. Algorand: Scaling Byzantine agreements for cryptocurrencies. In *SOSP*. ACM, 51–68.
[35] Wolfgang Gräther, Sabine Kolvenbach, Rudolf Ruland, Julian Schütte, Christof Torres, and Florian Wendland. 2018. Blockchain for education: lifelong learning passport. In *Proceedings of 1st ERCIM Blockchain Workshop 2018*. EUSSET.
[36] Alexander Grech and Anthony F Camilleri. 2017. Blockchain in education.
[37] World Bank Group. 2018. Cryptocurrencies and Blockchain. http://documents.worldbank.org/curated/en/293821525702130886/pdf/Cryptocurrencies-and-blockchain.pdf.
[38] Rachie Guerraoui, Nikola Knežević, Vivien Quéma, and Marko Vukolić. 2015. The next 700 bft protocols. *ACM Transactions on Computer Systems* 32, 4 (2015), 12:1–12:45.
[39] Guy Golan Gueta, Ittai Abraham, Shelly Grossman, Dahlia Malkhi, Benny Pinkas, Michael K Reiter, Dragos-Adrian Seredinschi, Orr Tamir, and Alin Tomescu. 2019. SBFT: a scalable decentralized trust infrastructure for blockchains. *DSN* (2019).
[40] Thomas Hardjono and Alex Pentland. 2019. Verifiable anonymous identities and access control in permissioned blockchains. *arXiv preprint arXiv:1903.04584* (2019).
[41] Maurice P Herlihy and Jeannette M Wing. 1990. Linearizability: A correctness condition for concurrent objects. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 12, 3 (1990), 463–492.
[42] Yurika Ishii. 2019. Blockchain Technology and Anti-Money Laundering Regulations under International Law. (2019).
[43] Eleftherios Kokoris Kogias, Philipp Jovanovic, Nicolas Gailly, Ismail Khoffi, Linus Gasser, and Bryan Ford. 2016. Enhancing bitcoin security and performance with strong consistency via collective signing. In *USENIX Security*. 279–296.
[44] Eleftherios Kokoris-Kogias, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, and Bryan Ford. 2017. OmniLedger: A Secure, Scale-Out, Decentralized Ledger. *IACR Cryptology ePrint Archive* 2017 (2017), 406.
[45] Karry Lai. 2018. Blockchain as AML tool: A work in progress. *International Financial Law Review* (2018).
[46] Leslie Lamport, Robert Shostak, and Marshall Pease. 1982. The Byzantine generals problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)* 4, 3 (1982), 382–401.
[47] Natalie Leal. 2019. Canada pilots blockchain staff records.
[48] Victoria L Lemieux. 2017. Evaluating the use of blockchain in land transactions: An archival science perspective. *European Property Law Journal* 6, 3 (2017), 392–440.
[49] Loi Luu, Viswesh Narayanan, Chaodong Zheng, Kunal Baweja, Seth Gilbert, and Prateek Saxena. 2016. A secure sharding protocol for open blockchains. In *CCS*. ACM, 17–30.
[50] Ethan MacBrough. 2018. Cobalt: BFT governance in open networks. *arXiv preprint arXiv:1802.07240* (2018).
[51] Government Matters. 2018. HHS obtains first blockchain ATO in federal government.
[52] S Melendez. 2018. How IBM and the CDC are testing blockchain to track health issues like the opioid crisis. *Fast Company* 4 (2018).
[53] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. 2016. The honey badger of BFT protocols. In *Proceedings of the SIGSAC Conference on Computer and Communications Security*. ACM, 31–42.
[54] Satoshi Nakamoto et al. 2008. Bitcoin: A peer-to-peer electronic cash system. (2008).
[55] Micky News. 2018. WORLD FIRST: Blockchain system developed to secure Australia's 'national capabilities'.
[56] Giang-Truong Nguyen and Kyungbaek Kim. 2018. A Survey about Consensus Algorithms Used in Blockchain. *Journal of Information processing systems* 14, 1 (2018).

[57] Adegboyega Ojo and Samuel Adebayo. 2017. Blockchain as a next generation government information infrastructure: a review of initiatives in D5 countries. In *Government 3.0–Next Generation Government Technology Infrastructure and Services*. Springer, 283–298.
[58] Kelly Olson, Mic Bowman, James Mitchell, Shawn Amundson, Dan Middleton, and Cian Montgomery. 2018. Sawtooth: An Introduction. *The Linux Foundation, Jan* (2018).
[59] Mike Orcutt. 2017. Why the CDC wants in on blockchain.
[60] Helen Partz. 2018. Major South Korean city to build blockchain-enabled virtual power plant.
[61] Rafael Pass and Elaine Shi. 2017. Hybrid consensus: Efficient consensus in the permissionless model. In *DISC*.
[62] Marco Platania, Daniel Obenshain, Thomas Tantillo, Yair Amir, and Neeraj Suri. 2016. On choosing server-or client-side solutions for BFT. *ACM Computing Surveys (CSUR)* 48, 4 (2016), 61.
[63] Michael J Rennock, Alan Cohn, and JR Butcher. 2018. Blockchain technology and regulatory investigations. *Journal of Practical Law* (2018), 33–44.
[64] Asia Blockchain Review. 2019. Malaysia's Melaka Straits city to become world's first blockchain city.
[65] Benjamin Ross. 2018. US health and human services looks to blockchain to manage unstructured data.
[66] Qiuyun Shang and Allison Price. 2019. A Blockchain-Based Land Titling Project in the Republic of Georgia: Rebuilding Public Trust and Lessons for Future Pilot Projects. *Innovations: Technology, Governance, Globalization* 12, 3-4 (2019), 72–78.
[67] João Sousa, Eduardo Alchieri, and Alysson Bessani. 2014. State machine replication for the masses with BFT-SMaRt. In *DSN*. 355–362.
[68] Clare Sullivan and Eric Burger. 2017. E-residency and blockchain. *Computer Law & Security Review* 33, 4 (2017), 470–481.
[69] Tendermint Core. [n.d.]. *https ://github.com/tendermint/tendermint*.
[70] Trustnodes. [n.d.]. The European Blockchain Partnership Signed, €300 Million Allocated to Blockchain Projects. https://www.trustnodes.com/2018/04/11/european-blockchain-partnership-signed-e300-million-allocated-blockchain-projects.
[71] Marko Vukolic. 2015. The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication. In *iNetSec*. 112–125.
[72] Angela Walch. 2016. The path of the blockchain lexicon (and the law). *Rev. Banking & Fin. L.* 36 (2016), 713.
[73] Wenbo Wang, Dinh Thai Hoang, Zehui Xiong, Dusit Niyato, Ping Wang, Peizhao Hu, and Yonggang Wen. 2018. A survey on consensus mechanisms and mining management in blockchain networks. *arXiv preprint arXiv:1805.02707* (2018), 1–33.
[74] Xu Wang, Xuan Zha, Wei Ni, Ren Ping Liu, Y Jay Guo, Xinxin Niu, and Kangfeng Zheng. 2019. Survey on blockchain for Internet of Things. *Computer Communications* (2019).
[75] Gavin Wood. 2014. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper* 151 (2014), 1–32.
[76] Mahdi Zamani, Mahnush Movahedi, and Mariana Raykova. 2018. RapidChain: A Fast Blockchain Protocol via Full Sharding. In *CCS*. 931–948.
[77] Xiaochen Zheng, Raghava Rao Mukkamala, Ravi Vatrapu, and Joaqun Ordieres-Mere. 2018. Blockchain-based personal health data sharing system using cloud storage. In *Healthcom*. IEEE, 1–6.
[78] Siegfried Zottel, Bilal Zia, and Fares Khoury. 2016. *Enhancing financial capability and inclusion in Sénégal: A demand-side survey*. World Bank.