Blockchain and Suitability for Government Applications

Contents

Blockchain and its Suitability for Government Applications

Team Members

Mark G., Office of the Director of National Intelligence

Melinda N., Federal Bureau of Investigation

Lisa P., Office of the Director of National Intelligence

George Bell, Department of Defense

Jonathan Downing, SAS Federal

Kaivan Rahbari, FIS

Moh Kilani, Truman National Security Project

Katlyn Woods, DHS Immigration and Customs

Enforcement Scott S., Sojourn Consulting, LLC

Curtis T. Federal Bureau of Investigation

Everette J., Office of the Director of National Intelligence

Aaron Varrone, CISCO

Key Judgements

- Blockchain is a cryptographically-secured distributed ledger that records transactions chronologically, permanently, and unalterably. Blockchains vary in transactional throughput and cost depending on numerous factors, including the choice of consensus mechanism and permission status.

- Blockchain has multiple challenges to overcome in realizing its full potential. These challenges include scalability, data security, interoperability, governance, and the management of personally identifiable information.

- Foreign governments, including China, Russia, Estonia, and Canada, are investing heavily in blockchain technologies. Chinese use cases include paying intelligence informants and supply chain management, including weapon life cycle. Currently, the world's largest Bitcoin mining company, Bitmain, is in China.

- Blockchain is best suited for use cases requiring at least three of the following: data redundancy; information transparency; data immutability; and a consensus mechanism. If only one or two are required then blockchain may work, but there are likely simpler or cheaper ways to solve the problem.

- A permissioned blockchain may be a better option for government use since all parties afford some degree of trust to a central authority, permitting selection of a consensus mechanism that is more efficient and less expensive compared to a permissionless blockchain.

- Blockchain is not a silver bullet for the US Government; however, there are areas of government interest where distributed ledger technology appears to be well-suited to delivering specific and tangible benefits. These include public records, budget allocation, supply chain monitoring, and the government approval chain process.

- Distributed ledger technology is being deployed by government agencies within the United States in primarily a research capacity in areas such as supply chain, health care records, and identity management. More resources, training and development should be dedicated to pilot programs to determine the utility and impact of blockchain to the US government in the future.

I. Introduction

Traditional relational database management solutions (e.g. Oracle and SQL), deployed globally across millions of applications, have one major operational constraint – the management of data is performed by a few entities who must be trusted. Distributed Ledger Technologies (DLT, commonly referred to as blockchain), an alternative architectural approach to managing data, and removes the need for a trusted authority to store and share a perpetually growing set of data.

A foundational characteristic of a blockchain is trust. Blockchains have digital signatures and use keys to authorize and check transactions and positively identify the initiator. Once recorded to the chain, a blockchain record cannot be deleted or manipulated. New blocks may only be appended to the chain, ensuring data integrity and creating a verifiable audit trail where the shared ledger provides visibility to all participants, simultaneously. Additionally, data elements can be individually permissioned, so participants see only appropriate transactions. Applications managed by a single entity would typically not benefit from using blockchain technology.

The most famous application of blockchain, Bitcoin is an open and public ledger used to keep track of cryptocurrency. Bitcoin “miners” (the parties adding new data to the blockchain) neither know nor trust one another. Governance can be achieved by appointing a central group to determine how the application should evolve over time, rather than trying to gain consensus among thousands of stakeholders for every change. For heightened security and privacy (such as in government applications), a blockchain may be closed to unknown or untrusted entities; this is referred to as a "permissioned blockchain" and this model allows trusted entities privileges to update the chain in an accountable fashion.

Digital ledgers using blockchain can significantly shorten the time required to transact business by eliminating intermediaries to allow direct transactions between counterparties. One promising application of this technology is bank settlement – whereas transaction approval and acceptance takes a day using conventional data management solutions, blockchain can be deployed to significantly reduce timeframe, costs and error rates.

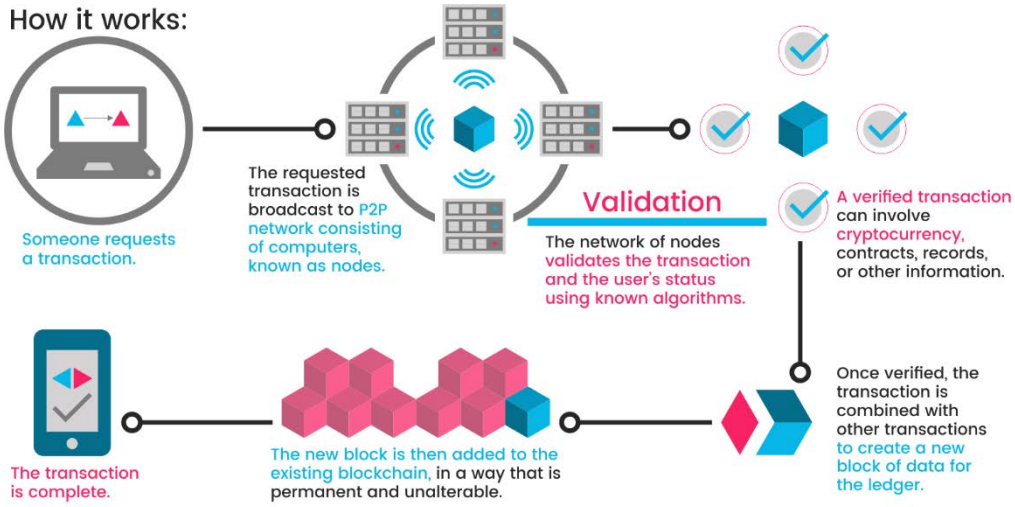
Change will not be easy, as distributed ledgers mature and disrupt how we think about data management. Incumbent technology leaders have spent billions of dollars enhancing their technologies and applications and are thus committed to preserving the status quo. However, the significant investment and recent growth in Bitcoin clearly signals that investors are interested in blockchain technology. Prominent technology providers such as IBM and Microsoft have announced foundational technology stacks for companies to use in building blockchain applications. The objective of this whitepaper is to educate key government decisionmakers on the benefits and challenges of using blockchain and the potential to deploy applications to speed up access to data, ensure integrity of data, and reduce overall cost.

II. What is Blockchain Technology?

A blockchain is a distributed ledger that does the following [1]:

- Records any transaction or information chronologically, permanently and unalterably
- Uses one-way hash cryptography[2] that is computationally impractical to break
- Is visible to all permissioned users
- Uses Peer-to-Peer transmission, with each node forwarding new transactional information to all others
- Can trigger transactions automatically, based on business logic and custom algorithms
- Verifies transactions through node consensus with no reliance on third-party intermediaries (e.g., clearinghouses)

This results in transparency of data and metadata of every transaction, in real or near real time, allowing auditability and analytics. Because transactions happen without intermediaries, they occur far faster than the current standard, in a real-time workflow, while lowering operational costs. All of this takes place on an immutable, permanently secured system, distributed across thousands or millions of devices. This is the promise of distributed ledger technology.



[1] M. Swan, *Blockchain: Blueprint for A New Economy*. Sebastopol, CA: OReilly Media, Inc., 2015.

[2] "A one-way hash function, also known as a message digest, fingerprint or compression function, is a mathematical function which takes a variable-length input string and converts it into a fixed-length binary sequence. Furthermore, a one-way hash function is designed in such a way that it is hard to reverse the process, that is, to find a string that hashes to a given value (hence the name one-way.) A good hash function also makes it hard to find two strings that would produce the same hash value. All modern hash algorithms produce hash values of 128 bits and higher. Even a slight change in an input string should cause the hash value to change drastically. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. This is called an avalanche effect. Since it is computationally infeasible to produce a document that would hash to a given value or find two documents that hash to the same value, a document's hash can serve as a cryptographic equivalent of the document. This makes a one-way hash function a central notion in public-key cryptography. When producing a digital signature for a document, we no longer need to encrypt the entire document with a sender's private key (which can be extremely slow). It is sufficient to encrypt the document's hash value instead. Although a one-way hash function is used mostly for generating digital signatures, it can have other practical applications as well, such as secure password storage, file identification and message authentication code (MAC.)" http://www.aspencrypt.com/crypto101_hash.html

Current Industry Challenges

While blockchain, and the larger distributed ledger technology arc, is a promising technology that may revolutionize the sharing of data across a variety of sectors, it is not without significant challenges.3 Blockchain's utility stems from its peer-to-peer nature, with each node validating and creating each transaction. Invalid transactions are discarded and not appended to the chain. Beyond cryptocurrencies and financial technology applications (fintech), blockchain may disrupt supply chain management, the Internet of Things (IOT), record keeping and identity management, with applications that have not yet appeared. These industry challenges will persist for some time to come. Here are some of the most common challenges:

- Scalability
    - Public
    - Private
    - Sharding
    - Side-Chains
    - Directed Acyclic Graphs
- Custody & Data Security
- Interoperability
    - Oracles
- Legality, Policy and Privacy Issues
    - Regulatory and Compliance Measures

Some of these challenges are regulatory, policy and governance related, while some are technical and are platform or use-case specific. Often, these are not discrete, with policy and technical issues blending.

Scalability

The ability to have a high amount of transactional throughput at an enterprise-level poses a problem for much of the blockchain ecosystem.[4] This issue has often been discussed in the context of cryptocurrency and financial technology applications, and so, here we the AEP team generally take a non-fintech perspective. Whether the chain is permissioned or permissonless, and public or private affects the type of consensus mechanism, algorithm, and block size. This ultimately alters the throughput capacity. There are several developing solutions to maximize scalability, in the forms of sharding, oracles, side-chaining and Directed Acyclic Graphs (DAG), among others.

Scalability constraints are in large part due to the permissioned or permissionless nature of a blockchain. Permissionless blockchains may create trust in a trustless world, but under current

[3] D. Tapscott, *Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies.* San Francisco, CA: World Economic Forum, 2017
[4] *Ibid*.

implementations, as they scale, they slow down.[5] On the other hand, private blockchain scalability is orders of magnitude higher, as they have fewer users, and a trusted environment without the burdensome computing power required to establish consensus before committing transactions.[6] The *raisons d'etre* of Bitcoin are trustlessness, decentralization and pseudonymity; these are paid for by intentionally expensive Proof-of-Work (PoW) consensus. A fully decentralized blockchain like Bitcoin has no central authority, making governance a challenge.[7]

This is further complicated by the possibility of "51% attack" on public chains – a formerly "theoretical" vulnerability that allows the chain to be corrupted by a brute force attack, which has recently been used in a number of cases to steal millions of dollars[8] – and the rise of "invisible powers," which are unknown actors who can buy, borrow, or steal sufficient computing capacity to subvert a public blockchain, and to do so at intermittent intervals – effectively placing a finger on the scale and tipping the balance only when it benefits them and is unlikely to be detected. Private, permissioned networks, in contrast, can be configured by a central authority to create parallelism, manage identity and trust.

Public Scalability

Public, permissionless blockchains like Bitcoin are vastly slower than standard credit card transactions. Anyone can join a public, permissionless blockchain like Bitcoin, and as the number of nodes grows larger it slows down. This is a result of its PoW consensus mechanism and complete decentralization.[9] Bitcoin, which by some estimates will have 200 million users by 2024[10], has every node verifying every transaction.

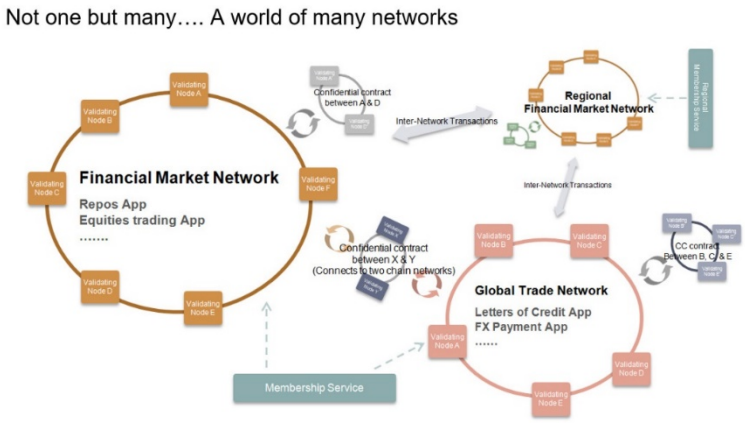
The PoW consensus mechanism that begets Bitcoin's completely decentralized and trustless nature requires significant time, and electrical energy to process. PoW, public and permissionless blockchains become slower with each additional participant, consequent to their Peer-to-Peer verification. Bitcoin ranges from 2 to 7 transactions per second[11],[12] (tps) while Ethereum (a similar and popular public Blockchain) ranges from 15 to 20 tps. Compare this with the Visa credit/debit card network at 65,000 tps. Some researchers view public blockchains, as they stand currently, as inefficient for global, mainstream adoption by nature.

---

[5] V. Buterin, "On Public and Private Blockchains," *Ethereum Blog*, 07-Aug-2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. [Accessed: 16-Jun-2018].
[6] *Ibid*.
[7] *Ibid*.
[8] "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular", *Coindesk,* 9 June 2018 [Online]. Available: https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/ [Accessed:14 June 2018]
[9] V. Buterin, "On Public and Private Blockchains," *Ethereum Blog*, 07-Aug-2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. [Accessed: 16-Jun-2018].
[10] "A dollar spent on bitcoin 'lottery ticket' in 2010 now worth almost $4 million," *RT International*. [Online]. Available: https://www.rt.com/business/411713-bitcoin-value-now-and-then/. [Accessed: 16-Jun-2018].
[11] M. Scherer, *Performance and Scalability of Blockchain Networks and Smart Contracts*. Umeå, Sweden: Umeå University, 2017
[12] Z. Hintzman, *Comparing Blockchain Implementations: A Technical Paper prepared for SCTE/ISBE b. Broomfield, CO: CableLabs, 2017*

Private Scalability

Permissioned blockchains, which are usually private or federated, have a limited number of known participants, resulting in much faster processing time.[13] A private or consortium blockchain will naturally process transactions much faster, simply because it has fewer users. These blockchains don't generally require heavy computational loads to verify transactions or append to the chain, as the users are known and trusted.[14] As an example of a private blockchain, Hyperledger[15] benchmarks at 3,500[16] to 10,000[17] tps.



Sharding

Sharding divides the transaction load through different nodes on the network.[18] Consequently, each node processes a fraction of incoming transactions in parallel with the remaining nodes. Sharding verifies a higher load of transactions, simultaneously. In contrast with the Bitcoin PoW schema, as this network grows, and scales horizontally, so does its efficiency. Blockchain

---

[13] V. Buterin, "On Public and Private Blockchains," *Ethereum Blog*, 07-Aug-2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/. [Accessed: 16-Jun-2018].

[14] ENISA, "Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector," *Good Practice Guide for Incident Management - ENISA*, 25-Jan-2017. [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security. [Accessed: 17-Jun-2018].

[15] Hyperledger is an open source Linux Foundation project for permissioned, enterprise-grade blockchains, with several different consensus algorithms, including Proof of Elapsed Time (POET), Sieve, and KAFKA. Other permissioned blockchains with higher tps include Credits at 300ktps, BigChainDB at 1 million tps, and Domus Tower Blockchain, a DAG system, at 1.24 million tps. According to the Domus whitepaper, they can achieve 10 million tps.

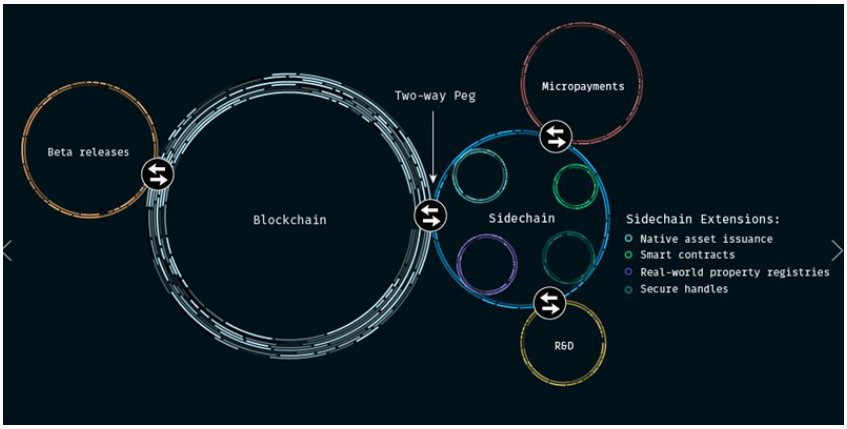
[16] M. Vukolić, "IBM Research: Behind the architecture of Hyperledger Fabric," *IBM Cognitive advantage reports*, 12-Feb-2018. [Online]. Available: https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/. [Accessed: 16-Jun-2018].

[17] Z. Hintzman, *Comparing Blockchain Implementations: A Technical Paper prepared for SCTE/ISBE b. Broomfield, CO: CableLabs, 2017*

[18] ENISA, "Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector," *Good Practice Guide for Incident Management - ENISA*, 25-Jan-2017. [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security. [Accessed: 17-Jun-2018]

sharding is largely driven by the Ethereum community and many believe that it is three to five years from wide implementation.[19]

Side-Chains



A side-chain is a separate blockchain that allows for separate computations off the parent chain.[20] Side-chains also allow permissioned users to exchange sensitive information off the main blockchain. Digital assets, currencies, transactions – essentially anything that could go on parent – can be added to a side-chain and placed on the parent as needed.[21] This results in higher scalability, as well as greater security and communication between users, particularly in permissioned networks. Side-chains also have a role in increasing blockchain interoperability.

Directed Acyclic Graphs (DAGs)

Directed Acyclic Graphs (DAGs) are not blockchains in the strictest sense, but they evolved in the same context, and are within the DLT family of technologies. It is interesting to note that in Nakamoto's groundbreaking work[22], the term "blockchain" is nowhere to be found. DAGs do away with the concept of blocks by linking transactions directly.[23] On "standard" blockchains, transactions are in blocks, while the sequence is linked by the pre-hashes between the blocks. By comparison, in DAGs, transactions themselves maintain the sequential order.

For simplicity, DAGs can be thought of as blockchain technology without blocks. While blockchains are linear, DAGs are a topology – a map – of directed transactions that connect to at

---

[19] S. Lee, "Five Issues Preventing Blockchain From Going Mainstream: The Insanely Popular Crypto Game Etheremon Is One Of Them," *Forbes*, 27-Dec-2017. [Online]. Available: https://www.forbes.com/sites/outofasia/2017/12/22/five-issues-preventing-blockchain-from-going-mainstream-the-insanely-popular-crypto-game-etheremon-is-one-of-them/. [Accessed: 17-Jun-2018].

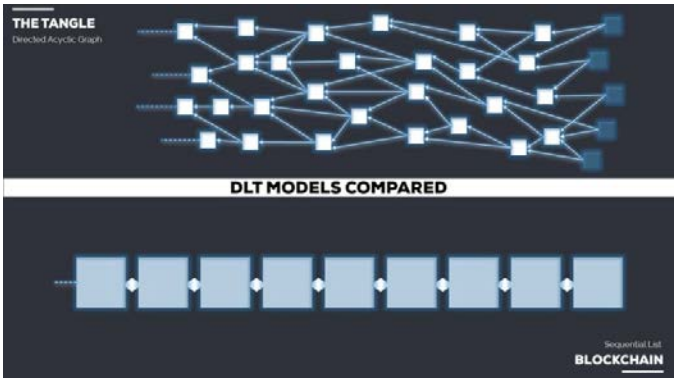
[20] V. Buterin, *Chain Interoperability*. New York, NY: R3CEV, 2016

[21] ENISA, "Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector," *Good Practice Guide for Incident Management - ENISA*, 25-Jan-2017. [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security. [Accessed: 17-Jun-2018].

[22] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org: 2009

[23] S. Lee, "Five Issues Preventing Blockchain From Going Mainstream: The Insanely Popular Crypto Game Etheremon Is One Of Them," *Forbes*, 27-Dec-2017. [Online]. Available: https://www.forbes.com/sites/outofasia/2017/12/22/five-issues-preventing-blockchain-from-going-mainstream-the-insanely-popular-crypto-game-etheremon-is-one-of-them/. [Accessed: 17-Jun-2018].

least two prior transactions, without looping back.[24] For the sake of simple interpretation, we will use terms from IOTA, a DAG system for Internet of Things.[25] Unverified IOTA transactions are called “tips of the tangle”, and the connections between them “edges.”



Each new transaction is attached via edges to two tips, and verifies their validity, selecting out fake or invalid transactions. If one is thrown out for invalidity, the algorithm chooses another tip which to attach the new transaction. Each new transaction performs a small PoW verification of the two tips. In this manner, as the tangle scales larger, transactional speed increases – the opposite of “standard” PoW or PoS, public blockchains like Bitcoin and Ethereum. Specifically, IOTA currently benchmarks 1,500 tps. A competitor to IOTA is the Chinese VC-backed IoT Chain (ITC). In the permissioned space, Domus Tower Blockchain[26] is an example of DAG technology.

Custody

While blockchain and DLT are regarded as cryptographically safe, they are not fail-proof nor immune to human error.[27]

Digital hygiene practices, such as applying security patches and performing regular system maintenance, are still necessary in these applications, perhaps more so than ever. For example, crypto-assets have been hacked via keyloggers that targeted private key and access information stored on Notepad. Ensuring safety of access information still rests on the users.

There are a few potential tools to amplify custody security like Shamir’s Secret Sharding (SSS)[28], multi-sig authentication, delegated services, or "cold storage" (hardware wallets). None

[24] S. Lee, “Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0,” *Forbes*, 24-Jan-2018. [Online]. Available: https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/. [Accessed: 17-Jun-2018].

[25] S. Popov, “The Tangle”, https://iota.org/IOTA Whitepaper.pdf (2016)

[26] The Domus Tower is a DAG private blockchain aimed at financial services and transaction clearing between existing business networks. It claims 1 million tps, with a potential for 10 million tps. This DLT is highly scalable, precisely for two reasons: a) it’s private, permissioned for business consortiums and b) it uses a DAG rather than a linear blockchain, which scales as it grows. Multiple Chinese firms are funding IOT Chain (ITC), which uses “a hybrid approach of blockchain, Practical Byzantine Fault Tolerance (PBFT), and blockless Directed Acyclic Graph (DAG) architecture” for a decentralized, secure and highly scalable IoT network. ITC benchmarks at 1,000 tps, with an aim to reach 100ktps in the coming year. It should be noted that IOTA is a public DAG blockchain, unlike Domus Tower, a private DAG blockchain, yet both scale far better than standard blockchains.

[27] ENISA, “Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector,” *Good Practice Guide for Incident Management - ENISA*, 25-Jan-2017. [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security. [Accessed: 17-Jun-2018].

[28] Shamir's Secret Sharing is an algorithm in cryptography created by Adi Shamir. It is a form of secret sharing, where a secret is divided into parts, giving each participant its own unique part, where some of the parts or all of

of these are perfect solutions – each sacrifice a measure of convenience for higher security. SSS is the breaking up of information into separate shards, requiring only a few of the shards to reconstitute the whole. For example, if a user shards a passphrase into 5 shards, the user only needs 3 shards to regenerate the whole passphrase. With Multi-sig, two keys are used for transactions: one by the user and the other by a custodial service, eliminating single point-of-failure. Cold storage is air-gapped hardware, unconnected until used. Hardware wallets can suffer from their own issues; the device itself can malfunction, they still require access information and software or firmware failures are a possibility.

All of these are imperfect, though nascent and promising. DLT and blockchain is a potentially powerful tool, but it is in a great state of hype, largely driven by avarice and "fear of missing out" (sometimes known as the "greater fool" theory). This family of technology is not a silver bullet through which we can ignore the ultimate point-of-failure: the human being. Digital hygiene and contextual understanding of social engineering are the paradigms that undergird cyber-security.

Interoperability

"Because they lack a central point of control, these networks, applications and organizations require new distributed governance systems to coordinate on matters such as interoperability, privacy and security, in a collaborative manner." Primavera De Filippi, Berkman Center at Harvard

There are thousands of blockchain projects in existence, many of which are cryptocurrencies or fintech generally. There is increasing diversification in non-fintech blockchain projects covering supply chain management, Internet of Things, identity management and many more. Many of these, if not most, are unable to communicate with each other directly.[29] It is a recurring problem that only becomes more complex as the larger ecosystem expands. It is likely that the various uses of blockchain will overlap (e.g., fintech with micro-payments in IOT or health care records and ID management). In essence, this is the verticalization of different blockchains into specialized uses. Interoperable blockchains create an ecosystem where different transactions and assets move between platforms and chains.

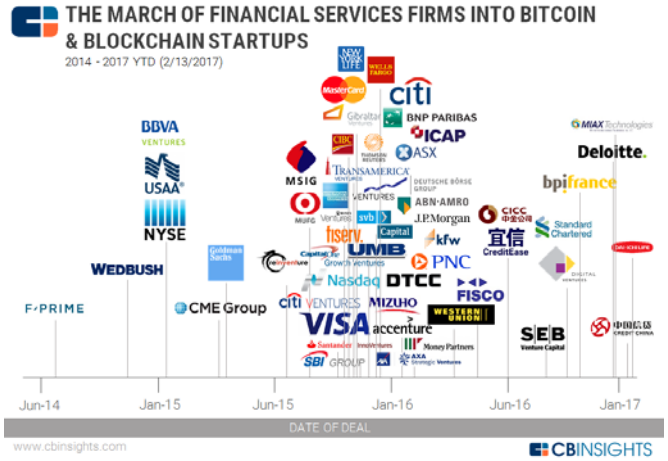
Ford, GM, and BMW are part of a coalition aiming to create standards to bring interoperability to the automotive industry in what they call the Mobility Open Blockchain Initiative (MOBI.) This would enable cars to share data for purposes such as alleviating traffic jams, promoting

---

them are needed in order to reconstruct the secret. Counting on all participants to combine the secret might be impractical, and therefore sometimes the threshold scheme is used where any k of the parts are sufficient to reconstruct the original secret. steempower (73), "Shamir's Secret Sharing Scheme - Storing Bitcoin seeds as Encrypted shards for geographically diverse backups - Steemit," - Steemit. [Online]. Available: https://steemit.com/bitcoin/@steempower/shamir-s-secret-sharing-scheme-storing-bitcoin-seeds-as-encrypted-shards-for-geographically-diverse-backups. [Accessed: 18-Jun-2018].

[29] A. Bridgwater, "Blockchains Are Verticalizing, So We Need Interoperability," *Forbes*, 07-Feb-2018. [Online]. Available: https://www.forbes.com/sites/adrianbridgwater/2018/02/07/blockchains-are-verticalizing-so-we-need-interoperability/#16f1c4e97ab9. [Accessed: 16-Jun-2018].

ride-sharing, and assisting self-driving cars.[30] Interoperable blockchains create an ecosystem where different transactions and assets move between platforms and chains.



The notion that there is ever going to be one single blockchain, for any use, is quickly receding into the distance, necessitating shared communication. In practice, real interoperability would require two fully stable and widely adopted blockchains, which has yet to occur.[31] Interoperability will become a serious question for legacy systems like SWIFT[32], which would be unlikely to connect to public blockchains.[33] Public, fully decentralized blockchains have no real central authority, complicating governance and interoperability. Private, permissioned blockchains, which are simpler to govern, have spent less time examining interoperability in comparison to the public blockchain space. Mainstream adoption of blockchain will require interoperability. Without industry standardization, who stewards connectivity and interoperability?

Oracles

Oracles are third-party data feeds that supply smart contracts with relevant information, like exchange rates, temperature or shipment delivery confirmation.[34] This allows smart contracts to execute when their conditions have been met.[35] In that sense, oracles are part of a multi-signature scheme: the signatories and the third-party oracle. Oracles bridge the deterministic blockchain with the non-deterministic real world. There a variety of oracle types including[36]: a) hardware feeding information from physical components like sensors; b) software collecting information

---

[30] I. Allison, "BMW, Ford, GM: World's Largest Automakers Form Blockchain Coalition," CoinDesk, May 4, 2018. [Online]. Available: https://www.coindesk.com/bmw-ford-gm-worlds-largest-automakers-form-blockchain-coalition/

[31] V. Buterin, *Chain Interoperability*. New York, NY: R3CEV, 2016

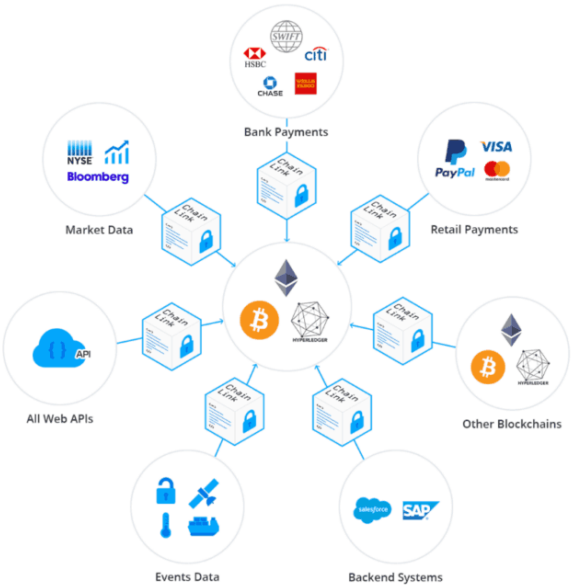
[32] SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, is the world's largest electronic payment messaging system, facilitating the exchange of more than $6 trillion a day "What is SWIFT?," Fin. [Online]. Available: https://fin.plaid.com/articles/what-is-swift. [Accessed: 18-Jun-2018].

[33] V. Buterin, *Chain Interoperability*. New York, NY: R3CEV, 2016

[34] "Blockchain Oracles," *BlockchainHub*. [Online]. Available: https://blockchainhub.net/blockchain-oracles/. [Accessed: 17-Jun-2018].

[35] J. Buck, "Blockchain Oracles, Explained," *Cointelegraph*, 17-Jun-2018. [Online]. Available: https://cointelegraph.com/explained/blockchain-oracles-explained. [Accessed: 17-Jun-2018].

[36] æternity, "Blockchain Oracles – æternity blog," *æternity blog*, 11-Apr-2018. [Online]. Available: https://blog.aeternity.com/blockchain-oracles-657f134ffbc0. [Accessed: 17-Jun-2018].



from online sources, like flight delays or weather forecasts; and c) consensus oracles that can be used in prediction markets, like Augur.[37] Oracles are usually thought of as sending information from the outside to the blockchain, but the opposite is also true. Smart contracts can use oracles to send information from the blockchain outwards.

Legality, Policy and Privacy Issues

Blockchains show great promise for securing transactions in an untrusted environment. Blockchains provide an inherently valid and permanent record of all records in the chain. This has naturally led to the development of blockchain based solutions for Personally Identifiable Information (PII) management. If PII is managed by a blockchain then users of the chain can be assured that the managed PII are as originally recorded and that all recorded PII are present in the chain. While blockchain's organic integrity assurance is a natural draw for PII management, there is a consequence to the immutability of the managed PII - there are laws governing the storage and retention of PII. For instance, the Privacy Act of 1974 governs the collection, maintenance, use, and dissemination of PII that is maintained in systems of records by federal agencies.[38]

Pertinently, it also provides individuals with a means to amend of their records. This is clearly at odds with blockchain PII management because the managed PII cannot be amended. They are immutable. The Electronic Freedom Foundation (EFF), a nonprofit organization respected for their views on and defense of digital privacy, believes this is an issue. The EFF also points out that in addition to Federal Law, there are state and local laws governing the retention of PII. They also believe that there will be a 4th Amendment Problem if the PII is deemed to have been wrongly acquired and the remedy is to purge the PII, especially if the Government knowingly retained PII with known problems of deletion. In recognition of these potential conflicts business have developed best practices regarding blockchain and PII.

The best practices include indirect referencing of the PII, Cryptologic Deletion of the PII, and the development of a mutable blockchain. However, depending upon the use case these best practices may be insufficient. This is what this section seeks to explore, the shortcomings of PII blockchain best practices.

---

[37] J. Peterson, "Augur: a Decentralized Oracle and Prediction Market Platform." Forecast Foundation. March 5, 2018

[38] gpo.gov, 'TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES', 2012. [Online]. Available: http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf [Accessed 10-June-2018].

Lastly, the European Union enacted the General Data Privacy Protection Regulation (GDPR) [39]on May, 25, 2018. GDPR seeks to protect the privacy of the EU's member state's residents by, among other things, enshrining a "right of erasure", which by definition conflicts with immutability. This section will end by highlight the issues with blockchain., PII and GDPR.

Indirect Referencing is storing a token and pointer to the PII's repository on a blockchain. This is done for cases where the PII must be updated or purged. To amend the PII, the off block record, which holds the PII, can be updated. To delete, the off-block record can be deleted and the on-block pointer points to nothing. However, for the deletion case, this leaves a token that equates to PII, but deletes the contextual information that explains the token's presence. The EFF believes that this is a Red Herring as the off-block record, rather than being deleted, could be updated to provide context.

Dr. Steven Bellovin, a respected security, privacy, and related legal and policy researcher for the University of Columbia's Department of Computer Science disagrees. Dr. Bellovin explained with mugshots as a use case. Mugshots are publicly available data. Consider the case where a PII's hash (token) and a pointer to the mugshot are stored on a blockchain, but the mugshot is stored elsewhere. While it is true that the mugshot can be deleted, the fact of the existence of a mugshot cannot. This would have a defamatory effect on one's reputation. Furthermore, the affected individual would have no recourse as the blockchain record cannot be purged.

This may be doubly egregious because mugshots are publicly available and there are businesses that extort the individuals by charging them a fee to stop advertising the fact of their mugshot. These individuals may not even stop the extortion by paying the ransom. Clearly, the mugshot use case cannot be extended to all cases. The mugshots are problematic precisely because the PII is public. Not all PII is public, and blockchains don't necessarily have to be public. There are private blockchains known as permissioned ledgers.

However, the mugshot use case is useful because it demonstrates that indirect referencing to solve blockchain's PII issue is not the panacea it is marketed as. If one is considering a blockchain based solution involving PII where the PII is secured by an indirect method, one must consider the consequences of having a fact of record pertinent to the PII that can be neither updated or destroyed.

Regulatory and Compliance Measures

Despite the legal ambiguity surrounding blockchain and other distributed ledger technologies, there remains a growing allure towards this platform and its core promises of enabling user anonymity, speed, direct and unmediated enterprise, and verified transactional transparency. However, as is the case with most maturing technologies that aim to unsettle legacy mechanisms, existing legislative and regulatory frameworks have proven to be ineffective and have failed to

[39] europa.eu, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)', 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 10-June-2018].

standardize, protect and address current liabilities faced by this technology. With a largely undefined and unregulated environment, most blockchain technologies operate in a tumultuous, uncontrolled, high-risk and uncertain ecosystem.

Compounding these risks, is a broad deficiency of subject knowledge, technical acumen, a stigma of malign activity attached to blockchain vis-à-vis cryptocurrency, and a lack of non-financially centric value transfer use cases – which have greatly limited inventorship and stifled governmental involvement. The current blockchain ecosystem is essentially unregulated and operates largely without oversight, consumer protections or comprehensive guidance from any U.S. or international regulatory body. Proactive efforts to resolve these matters requires greater collaboration and contributions between U.S. and international regulators, financial institutions, and technology leaders. Additionally, regulators have failed to adopt prudent legislation that embodies clear user and data protections, uniform language, and guidance for expanded law enforcement interventions. Regulatory bodies additionally need to establish uniform and industry specific, comprehensive frameworks that detail proper adaptability and interoperability with this technology. Drawing from the financial sector, examples of regulatory and protectionary measures currently absent would include basic identity management and personal information protections, Anti-Money Laundering/ Countering the Financing of Terrorism (AML/CFT) regulations and Know-Your-Customer (KYC) laws.

Nationally, due to a lack of administrative oversight and standards, companies, states and government departments are rushing to administer their own individualized guidance and operational involvement with this technology. This can be troublesome for businesses and individuals trying to incorporate or use this technology as there currently exist multiple and dissimilar rulings on using and classifying distributed ledger technology (I.e., Commodity, Security, Property, Etc...)

Internationally, some countries have purposefully implemented lax blockchain laws and have aggressively lobbied to draw companies and operations inside their borders to create tech jobs and start a blockchain-based economic surge.

Despite all this, blockchain has proliferated an environment for both startup businesses and major corporations who are witting to undertake and embrace the nontraditional risks associated to this fluid technology. Particularly with smaller blockchain start-ups, there is a concern for companies cultivating non-traditional methods of start-up capital. Where most traditional businesses gain financial investments through traditional venture capital means, most blockchain companies accrue capital investments by launching and farming publicly invested, Initial Coin Offerings (ICOs) which lack the stability, expertise and examination of traditional venture capital groups. In an ICO, “these offerings involve the opportunity for individual investors to

exchange currency such as U.S. dollars or cryptocurrencies in return for a digital asset labeled as a coin or token."[40]

Though fairly common for start-ups in the blockchain sector, the SEC reports that "A number of concerns have been raised regarding the... ICO markets, including that there is substantially less investor protection than in our traditional securities markets, with correspondingly greater opportunities for fraud and manipulation"[41]. Most ICO "investors" can be attracted by assurances of larger than average ROIs, which have only been exacerbated by the recent price fluctuations of Bitcoin and other cryptocurrencies. The SEC states that "It is especially troubling when the promoters of these offerings emphasize the secondary market trading potential of these tokens. Prospective purchasers are being sold on the potential for tokens to increase in value – with the ability to lock in those increases by reselling the tokens on a secondary market – or to otherwise profit from the tokens based on the efforts of others"[42].

Outside of the financial and token-based applications of blockchain technology, enabling digitized commerce is quickly becoming hard to overlook as more individuals and businesses are shifting into a predominately globally digitized existence. Blockchain technology attracts these individuals and companies in large part because it empowers the user to gain global interoperability and connectivity, speed and accuracy, provides immutability of records, provenance, and promotes an unrestricted reach. That said, no distributed ledger technology, including blockchain at this point, provides the "end-all/be-all" solution. However, blockchains adoption by the financial technology (fintech) sector and other commercial enterprises have demonstrated the usefulness of this technology, despite the lack of regulatory and compliance measures. Nonetheless, blockchain and other quickly evolving distributed ledger technologies need to incorporate expansive and specific oversight assurances to its users if they are to further demonstrate its true value, utility, and legal compliance benefits on a global scale.

Cryptologic Deletion is the practice whereby if one encrypts the PII stored on blockchain, then to delete the PII, one destroys the record's encryption key, which would have the effect of rendering the PII gibberish. This is considered to be the functional equivalent of deletion. So long as it is computationally difficult to crack encrypted data, this is true. However, Moore's Law predicts that every 2 years computational power doubles. If one considers the efficacy of historical encryption algorithms (DES and others) one can deduce an approximate fifty-year life span for data protection. Hence, after about fifty years, due to the march or Moore's Law, previously secure data is at risk because its encryption is "crackable". This means that within the lifetime of the affected individual their cryptologically deleted PII will be recoverable because the record will exist due blockchain's immutability and its encryption will be crackable.

---

[40] J. Clayton, "Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC," 2017. [Online]. Available: https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission.

[41] *Ibid.*

[42] *Ibid.*

Furthermore, the art of cryptography continues to advance. For example, Quantum computing promises to be able to instantly crack the encryption schemes (AES, BLOWFISH, etc…) used for the blockchain records. Additionally, while the cryptologic algorithms may be correct, their implementations may not be. For example, HeartBleed and WPACrack were not failures of the encryption algorithm but failures of their implementation. Again, due to the immutability of blockchain records, there would be no means to patch the record's encryption if it is found to have an error that renders it crackable. In short, there is risk that cryptologic deletion will fail over time due to the continued existence of the encrypted records and the ability to crack them.

Lastly, key management would be an issue. Dr. Bellovin observed: "How would the encryption keys' destruction be assured in a distributed environment?" Dr Bellovin's point is that so long as one key remains un-destroyed, then the cryptologically deleted PII is at risk for recovery.

All of this is not to suggest that cryptologic deletion is not a valid practice. Because there are no external dependencies, as is the case of indirect references requirement of an external repository, Cryptologic Deletion will be easier, and less costly to implement and deploy. Furthermore, unlike indirect referencing, Cryptologic Deletion deletes the blockchain record, albeit functionally, and likely for some fungible time frame. This may make it a better fit for those cases where the retention of fact of records is an issue, especially where it is not anticipated that the blockchain will be long lived.

Lastly, Dr. Green, a noted cryptologic expert and a Professor for the Department of Computer Science at Johns Hopkins University, believes that it is feasible to make a mutable blockchain. A mutable blockchain is a blockchain whose records could be updated. While this would solve the privacy concerns with storing PII in an immutable way, it undoes the principal advantage of using a blockchain - the intrinsic integrity of its records. That being said – because the records can be updated, there may be cases where a mutable blockchain is broken.

As mentioned before, the European Union, to protect the privacy of residents of the EU member states promulgated the "General Data Protection Regulation" (GDPR) on May 25, 2018. Among the protections that GDPR establishes is the "Right to erasure ('right to be forgotten')". GDPR Article 17 section 1 stipulates that "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay ..." This protection is at odds with blockchain's organic feature - the immutability of data. From the GDPR perspective erasure means what its plain language states - "removing records from existence", which, for a blockchain, cannot be done without invalidating the blockchain.

It is thought that indirect referencing could allow a controller to meet their GDPR erasure obligations. However, Article 4 of the GDPR defines personal data as "...any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social

identity of that natural person" Therefore because indirect referencing by definition indirectly refers to personal data, it may run afoul of GDPR.

Cryptologic deletion may also run afoul of GDPR. Cryptologic deletion is a functional deletion, whereas the plain language of GDPR Article 17 demands erasure, i.e.; actual deletion.

Lastly GDPR's preamble section 115 reads as follows: "Some third countries adopt laws, regulations and other legal acts which purport to directly regulate the processing activities of natural and legal persons under the jurisdiction of the Member States. This may include judgments of courts or tribunals or decisions of administrative authorities in third countries requiring a controller or processor to transfer or disclose personal data, and which are not based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State. The extraterritorial application of those laws, regulations and other legal acts may be in breach of international law and may impede the attainment of the protection of natural persons ensured in the Union by this Regulation. This is in short, claim to extraterritoriality for GDPR.

According to Black's Law Dictionary, extraterritoriality concerns the operation of laws outside the boundary of a state or country. This means that if, for example, a US company collects data on EU citizens, it is under the same legal obligation it would be if headquartered in the EU, even if it has no presence there.

As of this writing, no blockchain solutions have been scrutinized by the EU Regulators or Courts. Therefore, as of this writing, any blockchain controller that stores personal data is at risk of an EU Judgment against them and subsequent fines of up to the greater of €20 million or 4 percent of a company's annual worldwide revenue, which happened to Alphabet Inc's Google and Facebook on GDPR's First Day.

III. Stewardship and Blockchain: Where is This All Going?

The World Economic Forum has addressed the question of stewardship, identifying three layers[43]:

1. The Platforms: Ripple, Hyperledger, Ethereum, etc.
2. The Applications: smart contracts, cryptocurrencies, initial coin offerings, ID
3. The Overall Ecosystem: the ledger of ledgers; the connection between platforms

Collaborative governance, at each layer, is the defining meta-challenge that will determine the direction of the blockchain and DLT arc of development. Who will determine standards for interoperability? It is generally assumed in this sphere, that public blockchains will become interoperable at a fundamental protocol layer.

Jed McCaleb, found of Stellar, believes there will be a universal blockchain payments system, with dollars and euros.[44] He also contends that stock will find its way onto blockchains. If this is the case, public blockchain adoption by the mainstream will likely include identity management, finances, health and property records – essentially anything society records now. Adam Ludwin, founder of Chain, echoes McCaleb's comments about the financial public blockchain.[45] Likewise, internal databases will mirror blockchain data models that enable interaction with public blockchains. Much like intranets connect to the internet, private blockchains will interact with public ones. Ludwin downplays the hype, stating that blockchain is another type of database architecture, and stating that blockchain is useful in increasing trust and robustness, for specific uses. He stresses, on the other hand, that the blockchain niche is an "Internet counter-culture" challenges the status quo in Wall St. and Silicon Valley.[46]

By many accounts, blockchain and DLT are – or will be – features of Web 3.0. But this brings up philosophical and historical issues.[47] The Internet, from its inception, was multi-sector and collaborative. Even a cursory study shows the role of DARPA, UCLA, DOE, NASA and a host of others. Collaborative networks for standards, knowledge, delivery, policy, advocacy, scrutiny and convening shaped and continue to develop the Web.[48]

---

[43] D. Tapscott, *Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies.* San Francisco, CA: World Economic Forum, 2017

[44] E. Cheng, "An early bitcoin pioneer predicts how the blockchain will change banking," *CNBC*, 21-Mar-2018. [Online]. Available: https://www.cnbc.com/2018/03/21/an-early-bitcoin-pioneer-predicts-how-the-blockchain-will-change-banking.html. [Accessed: 16-Jun-2018].

[45] S. Silverstein, "CEO of blockchain company Chain on what everyone gets wrong about the technology," *Business Insider*, 31-Jan-2018. [Online]. Available: http://www.businessinsider.com/ceo-blockchain-chain-adam-ludwin-tech-merging-cryptos-database-2018-1. [Accessed: 16-Jun-2018].

[46] R. Staff, "Full transcript: Chain CEO Adam Ludwin answers cryptocurrency questions on Too Embarrassed to Ask," *Recode*, 14-Mar-2018. [Online]. Available: https://www.recode.net/2018/3/14/17121406/transcript-chain-adam-ludwin-answers-crypto-currency-bitcoin-blockchain-questions-too-embarrassed. [Accessed: 16-Jun-2018].

[47] M. Swan, *Blockchain: Blueprint for A New Economy*. Sebastopol, CA: OReilly Media, Inc., 2015.

[48] D. Tapscott, *Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies.* San Francisco, CA: World Economic Forum, 2017

Though blockchain and DLT is a nascent field, few argue that they represent a highly useful, yet potentially dangerous, new vista. This family of technologies will require the same kind of restraint and foresight by stakeholders, especially the USG. Given that blockchain and DLT are evolving as an outgrowth of the Internet, it follows logically that they need the same type of stewardship.[49]

In fact, stewardship may be more critical in this case, given the rapid pace of business development, the social implications of decentralization, the immutability of transactional data on blockchains and the free flow of open source code. This may be particularly true in a national security context.

IV. Blockchain in the Lens of Global and National Security: China, Russia, and Others

Adversarial nations, violent non-state actors and others are engaged in active measures and cyber- and hybrid war, running the spectrum of economic espionage, terrorist financing, electrical grid penetration, political influence and more. Blockchain could have a role in facilitating all of these activities. China is considering blockchain's role in paying "intelligence professionals and informants"[50] (情报工作绩效激励)[51], supply chain management and weapon life cycles[52]. North Korea is combining malware attacks with cryptocurrency as means of revenue generation. Russia and Venezuela are looking at cryptocurrencies as a method to circumvent sanctions.[53]

The Chinese National Defense and Science Journal (NDSJ) published a short work on the possible military applications for blockchain. Written by Lian Lin, Zhao Zhao, and Zhu Qichao, the article covered four general use-cases.[54] The NDSJ article was reprinted in the Liberation Army Daily by Zhang Min, in a shortened version. The four uses were:

---

[49] *Ibid*.

[50] W. VornDick, *China Brief: Beyond Bitcoin: Could China Embrace Blockchain for Defense and Security Applications?, Washington, DC: The Jamestown Foundation* Volume 18, Issue 2 2018

[51]廉 薤,朱启超,赵 炤.区块链技术及其潜在的军事价值[J].国防科技,2016,37(2): Lian Lin, et al, "Blockchain Technology and Its Potential Military Value [区块链 技术及其潜在的军事价值]," National Defense Science & Technology [国防科 技], vol. 37 no. 2. (Apr 2016); p. 30-34

[52]廉 薤, "区块链技术及其潜在的军事价值," *BTC123*, 20-May-2017. [Online]. Available: http://news.btc123.com/news/detail?id=6467. [Accessed: 16-Jun-2018].

[53] A. Panda, "Cryptocurrencies and National Security," *Council on Foreign Relations*, 28-Feb-2018. [Online]. Available: https://www.cfr.org/backgrounder/cryptocurrencies-and-national-security. [Accessed: 16-Jun-2018].

[54]廉 薤,朱启超,赵 炤.区块链技术及其潜在的军事价值[J].国防科技,2016,37(2): Lian Lin, et al, "Blockchain Technology and Its Potential Military Value [区块链 技术及其潜在的军事价值]," National Defense Science & Technology [国防科 技], vol. 37 no. 2. (Apr 2016); p. 30-34

1. Securing Battlefield Information: They refer to DARPA's blockchain research.

2. Weapons and Equipment Management: Life-cycle management, ease of secure & collaborative information management, and military human resources management

3. Smart Military Logistics: Intelligent warehousing, smart packaging, intelligent transportation, and intelligent distribution. They posit that blockchain may solve network communication, data preservation and system maintenance, as the disruptive technology of future network infrastructure protocols.

4. Covert Intelligence Incentives: Zhang Min claims that "*in recent years, the U.S. military has fully exploited the anonymity of the blockchain when recording transactions, and applied it to the field of intelligence gathering to achieve covert targeted payment of incentives for information provision.*"[55] Zhang believes that Bitcoin can protect intelligence personnel, by breaking the payment traceability.[56]

Likewise, Russia is adopting blockchain. The Financial Communications Transfer System (SPFS), the Russian equivalent of SWIFT created in 2014 as a response to sanctions, is adopting blockchain by 2019.[57] Sergei Glazev, a Kremlin economic advisor stated "This instrument suits us very well for sensitive activity on behalf of the state. We can settle accounts with our counterparties all over the world with no regard for sanctions."[58]

According to multiple sources, at a blockchain meeting of the International Standards Organization (ISO) in 2017, a Russian delegation, including FSB officer Grigory Marshalko, boasted that "the blockchain will belong to the Russians."[59] Another delegate at the ISO meeting, Maxim Shevchenko, spoke in Russia about their goals.[60] The slides included "possibility to influence the technology" and "implementation [of] Russian standards and solutions worldwide."

---

[55] 廉 蔺, "区块链技术及其潜在的军事价值," *BTC123*, 20-May-2017. [Online]. Available: http://news.btc123.com/news/detail?id=6467. [Accessed: 16-Jun-2018].

[56] *Ibid*.

[57] S. Golstein, "Russian SWIFT to Transfer to Blockchain Technology by 2019 | Finance Magnates," *Finance Magnates | Financial and business news*, 07-May-2018. [Online]. Available: https://www.financemagnates.com/cryptocurrency/news/russian-swift-transfer-blockchain-technology-2019/. [Accessed: 16-Jun-2018].

[58] M. Seddon, "Putin considers 'cryptorouble' as Moscow seeks to evade sanctions," *Financial Times*, 02-Jan-2018. [Online]. Available: https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da. [Accessed: 16-Jun-2018].

[59] N. Popper, "Blockchain Will Be Theirs, Russian Spy Boasted at Conference," *The New York Times*, 29-Apr-2018. [Online]. Available: https://www.nytimes.com/2018/04/29/technology/blockchain-iso-russian-spies.html. [Accessed: 16-Jun-2018].

[60] BISTVru, "CTCrypt 2017 - Standartisation of blockchain (Maxim Shevchenko)," *YouTube*, 27-Jun-2017. [Online]. Available: https://www.youtube.com/watch?v=kvTmlNHE-3Y. [Accessed: 16-Jun-2018].

Vladimir Putin met with Vitalik Buterin, founder of Ethereum, while in St. Petersburg. They discussed the possibility of blockchain implementation in Russia.[61]

How does the U.S. stack up against other nations in terms of blockchain adoption? According to Deloitte, U.S. companies are more likely to feel that blockchain is "overhyped" and are less likely to invest in blockchain than their counterparts in other countries.[62] Countries leading the blockchain charge include China, Canada, Estonia, and UAE.

China leads the world in blockchain patent applications, submitting three times as many patents as the United States.[63] A blockchain white paper published by China's Ministry of Industry and Information Technology stated that "blockchain technology has risen to the level of a national science and technology strategy".[64] China hosts Bitmain, the world's largest Bitcoin mining company, which controls nearly 30% of all the processing power devoted to Bitcoin mining.[65] Alibaba, Tencent, Baidu, and Huawei have already deployed blockchains for various endeavors.

In a recent speech, China's president, Xi Jinping, called out blockchain as "accelerating breakthrough applications".[66] The Xiong'An Global Blockchain Innovation Fund announced it will have $1.6 billion available to invest in blockchain development. This fund will serve as an anchor for the new Blockchain Industrial Park in Hangzhou, China.[67] On a 3 June 2018 episode of China Central Television's show "Dialogue," the country's primary state broadcaster said that the economic value of blockchain is "10 times more than that of the internet".[68]

---

[61] "Meeting with founder of Ethereum project Vitalik Buterin," *President of Russia*, 02-Jun-2017. [Online]. Available: http://en.kremlin.ru/events/president/news/54677. [Accessed: 16-Jun-2018].

[62] D. Floyd, "Deloitte: 3 out of 4 Big Companies See 'Compelling' Case for Blockchain," CoinDesk, May 15, 2018. [Online]. Available: https://www.coindesk.com/deloitte-3-out-of-4-big-companies-see-compelling-case-for-blockchain

[63] R. Jennings, "China Leads The U.S. In Patent Applications For Blockchain And Artificial Intelligence," Forbes, May 17, 2018. [Online]. Available: https://www.forbes.com/sites/ralphjennings/2018/05/17/ how-china-pulled-ahead-of-the-u-s-in-patent-applications-for-new-technology/#229a9b5a6048

[64] "2018 China's Blockchain Industry White Paper," Ministry of Industry and Information Technology, Qifeng Financial Blockchain Institute, May 2018. [Online]. Available: http://xxzx.miit.gov.cn/download.jsp?path=/attach/20180521/20180521103244_603.pdf

[65] M. Huillet, "China's IT Ministry: 2017 Saw Peak Investment in Domestic Blockchain Industry," Coin Telegraph, May 21, 2018. [Online]. Available: https://cointelegraph.com/news/chinas-it-ministry-2017-saw-peak-investment-in-domestic-blockchain-industry

[66] E. Cheng, "Chinese President Xi Jinping calls blockchain a 'breakthrough' technology," CNBC, May 30, 2018. [Online]. Available: https://www.cnbc.com/2018/05/30/chinese-president-xi-jinping-calls-blockchain-a-breakthrough-technology.html

[67] W. Zhao, "$1 Billion Blockchain Fund Launches with Chinese Government Backing," CoinDesk, April 9, 2018. [Online]. Available: https://www.coindesk.com/1-billion-blockchain-fund-launches-with-chinese-government-backing/

[68] W. Zhao, "China State TV: Blockchain Is '10 Times More Valuable Than the Internet'," CoinDesk, June 4, 2018. [Online]. Available: https://www.coindesk.com/china-state-tv-blockchain-is-10-times-more-valuable-than-the-internet/

Of concern to U.S. national interests, China and Russia are collaborating on financial blockchain solutions. It is the opinion of Michael J. Casey, a blockchain advisor at MIT's Digital Currency Initiative, that:

This could end the [U.S.] dollar's role as the intermediating currency when exporters or importers wish to protect themselves from adverse moves in their local currencies. It would cut out Wall Street's middleman correspondent banks, slash transaction costs and undermine a triangulating system that has given the U.S. great influence on trade. For the U.S., the fallout could be intense. If Chinese and Russian businesses no longer needed to make trade payments in dollars, their governments might not have to hold greenbacks as a reserve currency, either. Meanwhile, if this disintermediated trade solution worked, most other countries would surely follow it. Americans cannot afford to be complacent about the dominance of the dollar and the advantages – lower interest rates, for starters – that has afforded them over the past 70 years."[69]

Both Estonia and UAE aim to run their governments entirely on blockchains. According to Forbes magazine, "By 2020, the emirate wants all visa applications, bill payments and license renewals, which account for over 100 million documents each year, to be transacted digitally using blockchain".[70] UAE believes the move to a paperless government will save 25 million man-hours for a savings of $1.5 billion per year.[71]

In Estonia, all government and healthcare records are integrated such that no information needs to be filled out more than once, and verification of records is instant. An article in the New Yorker stated, "The normal services that government is involved with – legislation, voting, education, justice, health care, banking, taxes, policing, and so on – have been digitally linked across one platform, wiring up the nation".[72] For example, Estonian citizens' tax forms are populated by data in the system, so they don't have to prepare a tax return. In an interview with Computerworld, Csilla Zsigri stated, "Today, most bureaucratic processes (except for marriage/divorce I think) can be done online, which reportedly saves Estonia ~2% of GDP a year. All databases – education, healthcare, tax, police, etc. – are digitally linked on the data exchange platform: X-Road."[73]

Similarly, the Government of Canada is looking to implement Ethereum blockchains across many applications. Toronto is home to the inventor of the Ethereum blockchain, Vitalik Buterin. Canada's National Research Council seeks to allow public institutions to publish data onto

---

[69] M. J. Casey, "It's Political: Why China Hates Bitcoin and Loves the Blockchain," CoinDesk, September 27, 2018. [Online]. Available: https://www.coindesk.com/political-china-hates-bitcoin-loves-blockchain/

[70] S. D'Cunha, "Dubai Sets Its Sights On Becoming The World's First Blockchain-Powered Government," Forbes, December 28, 2017. [Online]. Available: https://www.forbes.com/sites/suparnadutt/2017/12/ 18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/#2b9298e7454b

[71] "Smart Dubai," Government of UAE, Accessed June 12, 2018. [Online]. Available: https://smartdubai.ae/en/Pages/default.aspx

[72] N. Heller, "Estonia, the Digital Republic," *The New Yorker,* December 18, 2017. [Online]. Available: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic

[73] L. Mearian, "IBM sees blockchain as ready for government use," Computer World, February 14, 2018. [Online]. Available: https://www.computerworld.com/article/3254202/blockchain/ibm-sees-blockchain-as-ready-for-government-use.html

blockchains to increase transparency and auditability, while reducing overhead costs.[74] In a pilot program, the Government of Canada has launched a Known Traveler Digital Identity blockchain to store biometrics for air travelers.[75]

The scale of activities required for wholesale implementation of blockchain by the US Government would clearly be far greater - and the implications farther-reaching - than is the case in Estonia, the UAE, or Canada. However, the magnitude of investments by China and Russia dwarf those of the United States to this point.

[74] "Government of Canada exploring the potential of Blockchain technology," Bitaccess, January 19, 2018. [Online]. Available: https://blog.bitaccess.ca/government-of-canada-exploring-the-potential-of-blockchain-technology/

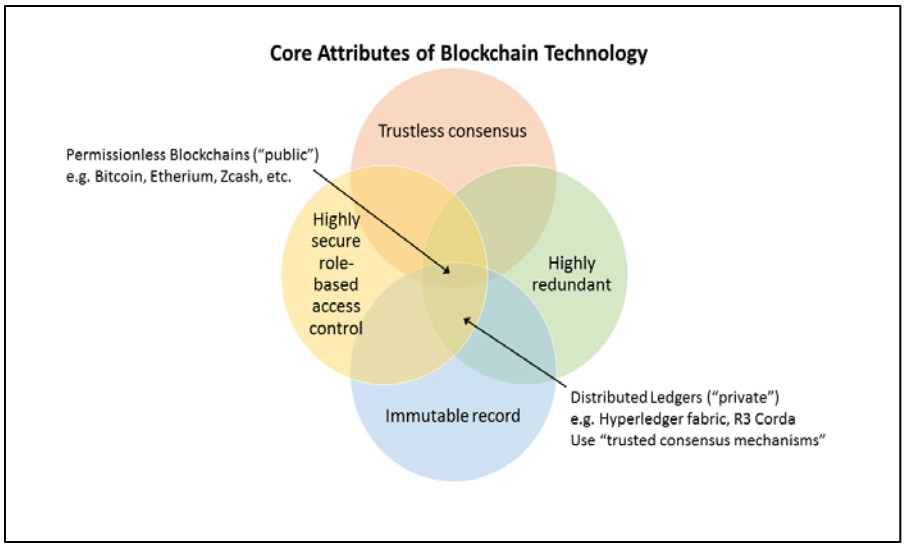
[75] "Canada to test biometrics and blockchain for international travelers," World Economic Forum, January 31, 2018. [Online]. Available: https://www.finextra.com/pressarticle/72424/canada-to-test-biometrics-and-blockchain-for-international-travellers

V. The Government's Role in Investing

As noted earlier, Blockchain technology is built upon four core principles. These are:

- The platform is itself widely distributed, so that the information contained in the ledger exists in multiple locations, leading to exceptional fault tolerance and resiliency;
- A record in the ledger can be plaintext, completely encrypted, or broken into separate elements, each encrypted with different keys, enabling a highly flexible model of information transparency;
- Each of the records in the ledger is immutable; once a record is committed, any change to that record would disrupt the computed digital hash code that links each block with the preceding block, breaking the "chain" and revealing the inconsistency;
- The mechanism used to commit a record to the ledger involves some form of consensus, and can in some sense be thought of as "democratic" in the sense that a majority rules in determining what transactions are true and correct.

In general, for any potential use case, blockchain is potentially appropriate when three or four of the criteria described above are critical aspects of the use case. If only one or two are required, then blockchain may work, but there are likely other ways to solve the problem that are simpler or less expensive. If only tamper-evidence is required, or only selective transparency, or only redundancy, then a more traditional type of database management can probably satisfy the requirement. Blockchain's unique contribution is to allow for high assurance of transaction completion in a trustless environment; at present, no other computing solutions provide as elegant a solution to this problem.



Blockchain Technologies for Government Activities

As we look at these core principles in the context of government use of blockchain-based systems, it is important to recognize that the requirement for consensus (principle #4) is unlikely to be acceptable to the United States government – or, indeed, to nearly any sovereign government – as this implies that none of the entities using the blockchain regard their peers with any degree of trust. A government typically insists that it be trusted in its conduct of any transaction; this is a basic element of the social contract. Indeed, if trust in government fails, commercial activities are forced to either operate at risk or to invest in mechanisms to mitigate

that risk, and this phenomenon can be observed to differing degrees throughout the developing nations of the world. In the case of blockchain-based cryptocurrency technologies like Bitcoin or Ethereum, a trustless environment is assumed, and the consensus mechanisms used to compensate for this lack of trust are all computationally challenging, and are thus quite inefficient and expensive. One estimate puts the energy consumed by a single Bitcoin transaction at 850 kilowatt-hours – enough to power the average US household for nearly a month.[76]

If we accept that at least one party to the blockchain is trusted to some degree by all the participants, then it is no longer necessary to employ a permissionless (Public) blockchain; a better (faster, more efficient and less expensive) model for this case is a permissioned (Private) blockchain, in which all parties afford some degree of trust to a central authority. The remainder of this section will consider some potential uses of permissioned blockchains in the context of governmental applications.

Government Applications Today

Blockchain is not a silver bullet for the U.S. government as society transitions to a state in which digital record-keeping becomes nearly universally accepted. However, as blockchain-related technology is more widely implemented, it could represent the future of legally-binding "smart" contracts, and shape how entire industries conduct their business in a transparent and streamlined manner, in partnership with the U.S. government. There are several working groups and pilot projects (in all stages of work ranging from proposed, to under development, to deployed) focused on applying blockchains within the U.S. government. The most common trends evaluated by federal agencies include: financial management, procurement, supply chain management, smart contracts, government-issued credentials, Federal personnel workforce data, Federal assistance programs, foreign aid delivery, health records and biometric data.

The following are just a few of the proposed or ongoing initiatives within the United States Government:

As of March 2018, the U.S. State Department along with Coca-Cola announced a project to use digital ledger technology to create a secure registry for workers that will help fight the use of forced labor, child labor and other exploitative practices worldwide. The State Department will be taking an advisory role and will provide expertise on labor rights and the protection of workers.

In March 2018, the U.S. State Department hosted the Boldline Accelerator[77] in which they discussed blockchain at the intersection of identity management, human trafficking, third-country workers and shipping fraud. One blockchain initiative that the U.S. State Department has

[76] "Bitcoin Energy Consumption Index", Digiconomist. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption [Accessed 8 May 2018].

[77] An accelerator for public-private partnerships, Boldline supports partnerships that address pressing global challenges and focuses on giving them tools to scale their missions. The main goal of Boldline is to build and deploy strategic connections and collaborations aimed at: a) strengthening the global partnership building ecosystem; b) promoting and facilitating connectivity between the private sector and governments; and c) fostering innovative partnership business models.

taken the lead on is the implementation of blockchain technology designed to combat labor fraud within the construction sector in Qatar.

Another proposed initiative includes the use of blockchain technologies for the Temporary Worker Visa Program in the United States. Each year, thousands of workers come to the United States under the H2 temporary visa program, working in industries such as agriculture, landscaping, seafood, shepherding and meat and dairy production. The normal process begins when an employer interested in hiring a temporary worker submits a temporary labor certification application to the Department of Labor (DOL). Once certified by DOL, the employer submits to U.S. Citizenship & Immigration Services (USCIS) a Form I-129 Petition for a Nonimmigrant Worker. Once approved by USCIS, the prospective worker may then apply for a visa at a U.S. consulate. A pilot program is exploring ways blockchain could streamline the process, making it more efficient for employers, less costly for the U.S. government, and safer for workers. For workers, this system would provide a job verification system, ensuring the job they are accepting actually exists and securing the terms of the employment contract. The system would also provide identity and immigration status verification, eliminating the threat to workers of document confiscation. For employers, the system provides skills verification to ensure that workers are qualified to meet the job requirements; it also would reduce paperwork and provide transparency in the recruitment process, increasing efficiency and trimming costs. For the responsible Federal agencies, such a system would provide streamlined workflows, reduce redundancy and enable instant status verification and tracking, with accountability at each step. Additionally, the system would increase interoperability between agencies, allowing separate agencies (e.g. USCIS and DOL) to communicate more transparently, while permitting granular control of the permissions on shared information by making certain fields visible to some users and restricting access to others.

The Department of Treasury, Bureau of the Fiscal Service's Office of Financial Innovation and Transformation (FIT) launched a pilot prototype using distributed ledger technology to track and manage physical assets (for example, government-issued computers and cell phones). The pilot project tested whether the inventory of an agency's physical assets can be continuously monitored and reconciled in real time as the physical assets are transferred from person to person throughout the pilot.

As of October 2017, the Centers for Disease Control (CDC) Center for Surveillance, Epidemiology and Laboratory Services is pursuing several blockchain proof-of-concept (POC) activities, with the aim to build real applications in 2018. The primary focus of these POCs will be the establishment of better public health surveillance. This in turn equates to an improved approach to the continuous and systematic collection, analysis and interpretation of health-related data needed for planning, implementation and evaluation of public health measures. As a result, blockchain technology could be used to more efficiently manage data during a public health crisis or related incident.

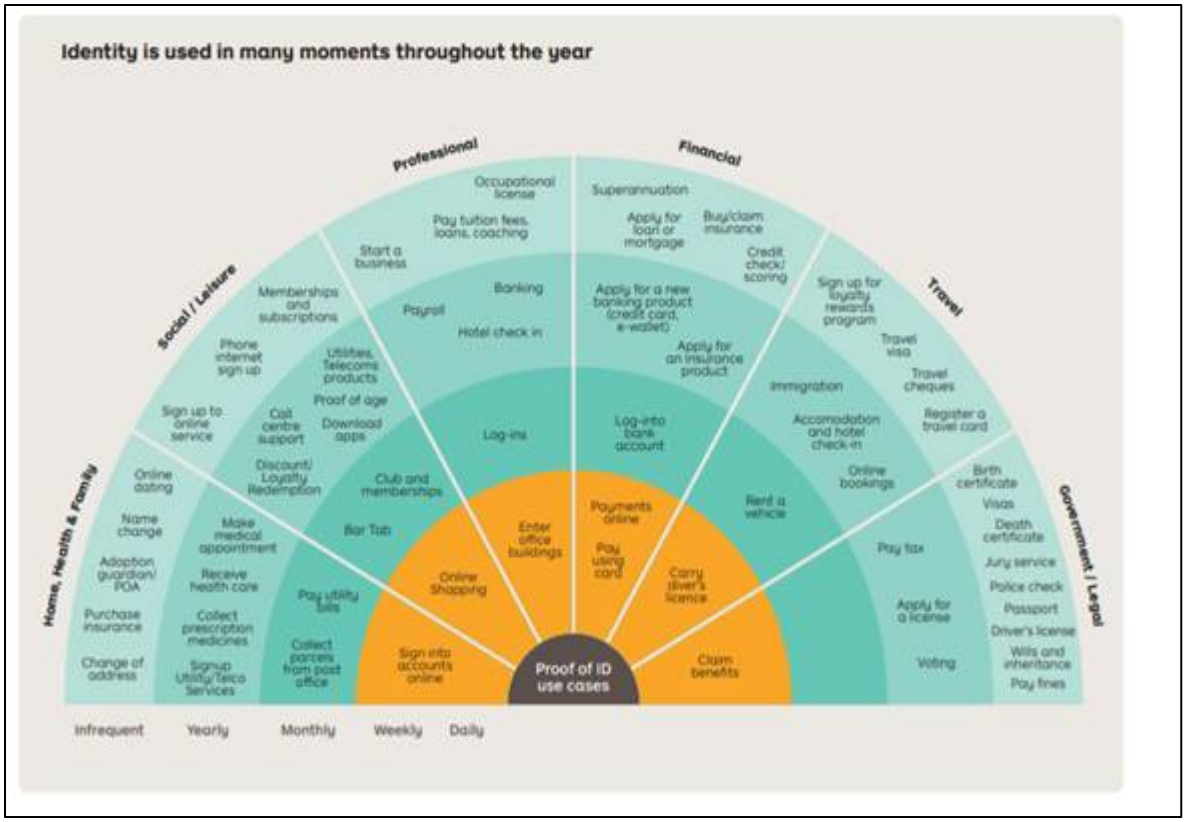
General Services Administration (GSA) is currently piloting Distributed Ledger Technology along with machine learning and artificial intelligence (ML/AI). GSA is looking to use blockchain to intelligently automate the FASt Lane contract review process, with a goal of

reducing “the amount of human interaction required to review new proposal documents, improve [the] offeror experience,” and reduce review time for proposal awards. Utilizing blockchain will aid in streamlining the procedures required to place an order, while providing agencies the tools and expertise needed to shorten procurement cycles, ensure compliance with all relevant federal regulations and achieve the best value to the government in obtaining innovative technology products, services and solutions.

The U.S. Postal Service Office of Inspector General (OIG) contracted with Swiss Economics, a consulting firm with interest and expertise in blockchain technology, to better understand the technology and its features, as well as identify areas of potential interest for the Postal Service. This partnership resulted in four potential use cases: financial services, device management, identity services and supply chain management. Of those, USPS has focused primarily on identity services. As of September 2017, the USPS filed a patent to implement a “digital trust architecture” made up of a “user account enrollment and verification component” based on user identity information; a “key provisioning component configured to generate a public and private key for the user account;” a user email component for signing the email with a private key; a data access component for accessing sensitive data; and a blockchain component for adding the records to the blockchain.

Outside of the Federal government, individual states have established working groups to develop pilot programs using blockchains. In particular the state of Illinois is establishing a pilot program exploring the use of blockchains to record the transfer of property titles. As of August 2017, Illinois announced its pilot to leverage the distributed ledger technology to create a secure, “self-sovereign” identity for Illinois citizens during the birth registration process. In the proposed framework, government agencies will verify birth registration information and then cryptographically sign identity attributes such as legal name, date of birth, sex or blood type, creating what are called “verifiable claims” or attributes. Permission to view or share each of these government-verified claims is stored on the tamper-proof distributed ledger protocol in the form of a decentralized identifier. The identifier guarantees each attribute is cryptographically sealed and only accessible with explicit consent of the identity holder (or in the case of a newborn child, the legal guardian). Businesses and governments will be able to verify and authenticate citizens by requesting encrypted access to these verifiable claims. This minimizes the need for entities to establish, maintain and rely upon their own proprietary databases of identity information.

The below graphic depicts additional types of ID use cases identified throughout studies of the blockchain technology:



The Future of Blockchain Within Government

These are only a few of the many instances of blockchain-related development activities underway within government organizations in the United States. There are many other areas of government interest where some type of DLT appears to be well-suited to delivering specific and tangible benefits. These might be good candidates for thoughtful and holistic consideration, including, in some cases, the need to amend legislation or rethink public policies to encompass the different ways of doing business that a blockchain-enabled solution might make possible (or require). Some of these are described briefly below.

The Public Records Challenge

Public records, which can be nearly any type of information that the government produces or administers, are an obvious use for a tamperproof, redundant and transparent ledger. This use of blockchain is underway in some other nations, and under consideration by the State of Illinois (as noted above), but is certainly a practical application of the technology for government entities within the United States. There may be some difficulties in recognizing the digital record, tied to the blockchain, as the true and legally binding document; legislative changes may be required to enable this use case. There may also be cause for concern in that the security of digital ledger technology is reliant upon the strength of cryptographic algorithms used to hash and encrypt data. Historically, as computers have become increasingly powerful, cryptosystems have been correspondingly weakened. In thinking about public records, this may present a problem because

we expect certain records to be secure against tampering in perpetuity (literally – consider property ownership records as an example of that). If the DLT selected by a municipality is determined to be cryptographically vulnerable, there could be leaks of sensitive information or the risk of modifications to the underlying data, which could cause great harm to specifically targeted users (by changing a property ownership record, for example) or generalized chaos (by corrupting large numbers of records over time, making it difficult to find a known "safe" state to revert to).

The Conveyance of Funds Challenge

Within the Federal government, each organization receives a budget, and is charged with the mission of using those funds to conduct its activities. A permissioned blockchain would enable the budget to be allocated, and funds to be tracked at every step of the process. Such a system would include the ability to conduct a complete audit of the transfer of funds from allocation through final spending, and to do so nearly instantly, at any time, simply by reading each sequential record in the ledger. An organization would record all transfers of funds whether intra-agency, inter-agency or external, and in doing so, would enable immediate obligation and expenditure of funds. Expenditures that are considered sensitive could have certain aspects masked by encryption so that only authorized users could see complete details of those transactions, while still allowing a less detailed view for other users.

Supply Chain Monitoring and the Delivery of Intellectual Property Challenge

Multiple presentations at the Blockchain West conference described a use of blockchain as a component of a supply chain security program. Supply chain verification and tracking is an application of DLT that has been successfully implemented in the commercial world, and for which the application to most government use cases is nearly identical. One particular – and different – case involved the on-demand fabrication of aircraft components at maintenance facilities[78]. This is accomplished by using 3-D printing technology. The maintenance facilities may be located anywhere in the world, which presents logistical challenges to the timely delivery of replacement parts. In this case, the original equipment manufacturer provided comprehensive design information and files that allow the parts to be printed on demand; however, both the consumer of the parts (the military customer) and the producer of the parts (Moog) wish to have complete confidence in the transaction. The motivations of the two parties are somewhat different. The most important thing for the consumer is to have confidence that the design files being fabricated on-site are a complete and true representation of the original equipment manufacturer's specification and have not been tampered with in any way (for example, by an adversary seeking to weaken a flight-critical component). While the commercial enterprise is also concerned that the part is being fabricated in accordance with their original design, they

[78] Blockchain West Conference, 26-28 March 2018, San Francisco, CA; presentations by CDR Steven Dobesh, USN of the Joint Chiefs of Staff and Mr. James Regenor of Moog, Inc.

have a more mercantile interest in ensuring that they are appropriately compensated for the use of their design, each time that part is fabricated.

The employment of a blockchain in this instance has successfully solved the problem, demonstrating the utility of blockchain in solving real and practical challenges. Based upon the team's understanding of this problem as it was presented at the conference, this is an instance in which the employment of a blockchain may not have been necessary. In considering the blockchain attributes – trustlessness, redundancy, transparency, and immutability – only immutability is strictly required. The other features are either "nice to have" or not required, depending on specific aspects of the problem and desired solution. A similar result could be achieved using a more conventional database in tandem with digital rights management software, to both ensure data integrity and to track and record access to the data required to fabricate the components.

The Approval Chain Challenge and Smart Contracts

A perennial complaint among both government employees and businesses that interact with the government is the time required to obtain the necessary approvals for some routine activities. Capabilities (called "smart contracts") have been built on distributed ledger technology that can help to streamline some of these processes. Smart contracts are simply applications that exist as integral parts of the distributed ledger; because of this, they are tamperproof and are relied upon to act as unbiased mediators in the conduct of some transactions. A smart contract works by awaiting some stimulus, and once that stimulus has occurred, performing some set of automated functions based upon the stimulus and potentially any number of other factors the smart contract can accept as input. These additional suppliers of information that may be applicable to a transaction are the "oracles" discussed in section II, above).

In the potential "streamlining" use case, smart contracts may be used to enforce conditions or actions within a set of defined parameters that are designed to promote efficiency. These parameters can include timeliness, cost comparison or any number of other factors. As a simple illustration, consider this example: if a person is traveling, they may receive lower rates from hotels or airlines by booking their reservations early. So, a travel request is submitted, and may be quickly approved by the office manager, but from there it goes to a different approval queue, where it languishes for weeks. When it is finally approved, the travel costs may have increased significantly (necessitating additional approvals and costing more money) or the trip may become effectively impossible (flights sold out / hotels booked up). In either case, the organization's mission suffers due to a failure of administrative process. A smart contract could help to ameliorate these circumstances in many ways; the contract could monitor airfare and flight or hotel availability, and increase the priority of the request in the approval queue as these constraints tighten; alternatively, a smart contract could impose a target timeline for approvals and take punitive action against organizations that impose delays. That might be something as simple as billing the approving organization for travel charges that increase beyond the submitted estimate due to an extended delay, or simply automatically approving travel request

(routing around the delaying organization) after the organization has delayed too many approvals for too long a time (where the meaning of "too many" and "too long" can be set on a case-by-case basis).

This is only one example, and it's a very simple one. Smart contracts can enforce behaviors that lead to efficiency and "good government", while making counterproductive behaviors expensive for the people or organizations who behave badly. It is important to note, however, that badly-designed smart contracts could have the opposite effect, by creating perverse incentives to game the system. For this reason, it is important to carefully consider the policy and legal implications of some of the more interesting uses of distributed ledger technologies.

Thus far, it appears that blockchain/distributed ledger technology is being deployed by government agencies within the United States in what is primarily a research capacity, and generally evaluated based upon the short-term impact. This is appropriate, given the nascent state of the technology and the lack of expertise in its application and implementation. Since these programs are new it is difficult to determine the longer-term impacts, positive or negative. According to some USG groups, their pilot programs resulted in the development of blockchain very like current SQL or Oracle database programs. In some respects, using the blockchain was cheaper and created a program that was perfect for the environment or task at hand but in other cases there was no significance difference. These activities have served to build expertise around blockchain, creating valuable human resources upon which the government can rely in the future. Now, it is crucial for the USG to determine the pros and cons of implementing blockchain and understand what use cases fundamentally change the ways that it processes and stores data to compete with the private sector and foreign partners. More resources, training and development should be dedicated to pilot programs to determine the utility and impact of blockchain to the USG in the future.

VI. Recommendations

- Increase technical understanding of blockchain within government by developing familiarity with the decentralized and distributed paradigms of DLT, blockchain and DAG, while tracking international developments

- Develop an internal USG blockchain subject matter expert workforce, and build internal pilot projects with in-house lines of R&D; leverage existing blockchain expertise available to the USG via Federally-Funded Research and Development Centers like Pacific Northwest National Laboratory

- Participate in the stewardship of blockchain and DLT by entering collaborative relationships with institutions like the World Economic Forum's Center for the Fourth Industrial Revolution, the Hyperledger Project, the Enterprise Ethereum Alliance, the Chamber of Digital Commerce, the Blockchain Research Institute, and the MIT Media Lab

- Increase government awareness of malign crypto-financial activity from foreign-built crypto-currencies like Petrocoin and the theoretical crypto-Ruble as well as extant crypto-currencies like Monero and Bitcoin

- Amplify knowledge of potential blockchain-based national security threats, particularly in intelligence, critical infrastructure, and the Internet of Things

- Participate in permissionless DLT consortium research; partner with private industry

- Consider and study privacy & legality implications especially regarding the intentional "right to be forgotten" and accidental private key destruction

- View with skepticism claimed "successful uses" of blockchain, recognizing that for many applications, there's another - and potentially easier - way to accomplish the task

Appendix A: Federal Security Clearance Use Case

A blockchain platform could store, track and secure documents related to the federal clearance process, providing a granular, auditable, multi-agency system.[79] This allows for a unified, modernized clearance process, with real-time analytics, including auto-notification for clearance renewal and cycled polygraphs. Within the chain, everything about the record can be unalterably known, including the data and meta-data.

Clearance itself could be a multi-step smart-contract, with each stage of the process acting as a condition. Meaning, that pre-investigation, investigation, and adjudication would be separate transactions on the chain. Only when each step is satisfied would the record be complete, granting the applicant clearance. Likewise, reinvestigation could be a smart-contract, auto-triggered once every 5 years or on a continuous evaluation with a baseline trend. Other notifications to administrators could include status of clearance: active, current or expired.

There could be multiple private, permissioned blockchains, each one belonging to a specific agency. This ensures the ownership of data. An agency could choose to share clearance and personnel information with a specific partner, institutional or individual. Additionally, this could prevent with expired clearance from reacquiring access. A private clearance blockchain could assist in the switching between agencies, without having to re-start the process, as well. A permanent clearance record, which could be shared, if agency and department administrations so choose.

In short, when combined with absolute administrative transparency, the hash cryptography and distributed nature of the network amplify the safety of Federal employees' information, while vertically integrating the process.

[79] While OPM oversees the majority of security clearance background investigations, at least 21 federal agencies have delegated or statutory authority to conduct all or some of their own investigations. For example, the Federal Bureau of Investigation (FBI), the U.S. Marshals Service (USMS), and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) have authority to conduct security clearance background investigations of certain categories of contractor positions. The Central Intelligence Agency (CIA) has authority to conduct its own security clearance background investigations..

Appendix B: Body of Research Interviewees

Over the course of this study, members of this group benefited from discussions and presentations by many individuals. Some met with us at conferences such as the Blockchain West Conference, while others agreed to be interviewed by phone. The insights and perspectives they provided were critical to our understanding of the challenges and opportunities presented by blockchain technology. We would like to thank all the individuals who shared their knowledge with us, including:

- Chris Spanton, T-Mobile
- Jim Nasr, Synchrogenix
- Nelson Petracek, TIBCO
- Dr. Steven M. Bellovin, Columbia University
- Dr. Matthew Green, Johns Hopkins University
- Dr. Joseph Williams, State of Washington
- Dr. Marta Piekarska, IBM Hyperledger
- Steven Dobesh, True Tickets
- Lee Tien, Electronic Freedom Foundation
- Andrew Crocker, Electronic Freedom Foundation
- Ms. Sydney, Electronic Freedom Foundation
- Mark Arrieta, Electronic Freedom Foundation
- Kyle Samani, MultiCoin
- Bart Stephens, Blockchain Capital
- Hunter Prendergast, MIMIR Blockchain Solutions
- Akshi Federici, ConsenSys
- Adam Ludwin, Chain Inc.
- Dave Kudla, Deloitte
- Wendy Henry, Deloitte
- Brandon Halergy, Deloitte
- David Houlding, Intel
- Usman Sheikh, Gowling WLG
- Mike Ferrari, In-Q-Tel
- Andrea Garrity, In-Q-Tel
- Ming Luo, In-Q-Tel
- Jonathan Smith, Civic Technologies
- Chris Hart Civic, Technologies

We also consulted with individuals from multiple federal agencies including the Office of Personnel Management and the State Department.

Appendix C: Resources

Below is a list of resources on blockchain technology and blockchain-related associations

Blockchain Basics:

- Blockchains: How They Work and Why They'll Change the World, 28 Sep 2017, IEEE Spectrum https://spectrum.ieee.org/computing/networks/blockchains-how-they-work-and-why-theyll-change-the-world
  Primer on blockchain including their history, how they work, smart contracts, and applications of blockchain technology.
- Blockchain Primer: Enabling Blockchain Innovation in the U.S. Federal Government, 17 October 2017, Blockchain Working Group, ACT-IAC Emerging Technology Community of Interest, https://www.actiac.org/act-iac-white-paper-enabling-blockchain-innovation-us-federal-government
  This Primer introduces blockchain and its related technologies, and discusses how blockchain can be applied to the government use cases.
- Blockchain for Dummies, 2017 IBM, Manav Gupta, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=XIM12354USEN
  This free E-book discusses what blockchain is, how it works, and applications and use cases.
- Blockchain Playbook for the U.S. Federal Government, April 2, 2018, American Council for Technology-Industry Advisory Council (ACT-IAC), https://www.actiac.org/act-iac-white-paper-blockchain-playbook-us-federal-government
  The playbook focuses on helping the United States federal government understand when to use distributed ledger technologies for its mission.
- Statement on Cryptocurrencies and Initial Coin Offerings. 2017, December 11, Securities and Exchange Commission, https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11

State and Federal Use Cases:

Blockchain Programs, GSA U.S. Emerging Citizen Technology Atlas, online at:
https://emerging.digital.gov/blockchain-programs/
A living list of some current blockchain programs, initiatives, pilot programs, and events.

Blockchain Associations and Mailing Lists

- General Services Administration (GSA) Blockchain Association mailing list, https://www.gsa.gov/technology/government-it-initiatives/emerging-citizen-technology/blockchain
  GSA's Emerging Citizen Technology Office hosts a Federal Blockchain Community listserv for individuals with .gov or .mil accounts, who are interested in exploring distributed ledger technology and its implementation within government. There also host a listserv for members of the public.
- American Council for Technology (ACT) and Industry Advisory Council (IAC) Blockchain group, https://www.actiac.org/groups/blockchain-0:
  ACT-IAC community of interest for government agencies looking to understand and incorporate blockchain functionality into their organization. Participation in the community of Interest is limited to ACT-IAC Members. Membership is free for federal employees.
- Global Blockchain Association (GBA), https://www.gbaglobal.org/membership/
  GBA is an International Professional Association and a US-based non-profit consisting of individuals and organizations that are interested in promoting blockchain solutions to governments worldwide. Membership is free for civil servants. GBA produces a free, weekly blockchain newsletter.

Appendix D: Work Cited

1. M. Swan, *Blockchain: Blueprint for A New Economy*. Sebastopol, CA: OReilly Media, Inc., 2015.
2. http://www.aspencrypt.com/crypto101_hash.html
3. D. Tapscott, *Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies.* San Francisco, CA: World Economic Forum, 2017
4. V. Buterin, "On Public and Private Blockchains," *Ethereum Blog*, 07-Aug-2015. [Online]. Available: https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains. [Accessed: 16-Jun-2018].
5. "Blockchain's Once-Feared 51% Attack Is Now Becoming Regular", Published 9 June 2018, collected 14 June 2018 https://www.coindesk.com/blockchains-feared-51-attack-now-becoming-regular/
6. "A dollar spent on bitcoin 'lottery ticket' in 2010 now worth almost $4 million," *RT International*. [Online]. Available: https://www.rt.com/business/411713-bitcoin-value-now-and-then/. [Accessed: 16-Jun-2018].
7. M. Scherer, *Performance and Scalability of Blockchain Networks and Smart Contracts*. Umeå, Sweden: Umeå University, 2017
8. Z. Hintzman, *Comparing Blockchain Implementations: A Technical Paper prepared for SCTE/ISBE b. Broomfield, CO: CableLabs, 2017*
9. ENISA, "Distributed Ledger Technology & Cybersecurity - Improving information security in the financial sector," *Good Practice Guide for Incident Management - ENISA*, 25-Jan-2017. [Online]. Available: https://www.enisa.europa.eu/publications/blockchain-security. [Accessed: 17-Jun-2018].
10. M. Vukolić, "IBM Research: Behind the architecture of Hyperledger Fabric," *IBM Cognitive advantage reports*, 12-Feb-2018. [Online]. Available: https://www.ibm.com/blogs/research/2018/02/architecture-hyperledger-fabric/. [Accessed: 16-Jun-2018].
11. S. Lee, "Five Issues Preventing Blockchain From Going Mainstream: The Insanely Popular Crypto Game Etheremon Is One Of Them," *Forbes*, 27-Dec-2017. [Online]. Available: https://www.forbes.com/sites/outofasia/2017/12/22/five-issues-preventing-blockchain-from-going-mainstream-the-insanely-popular-crypto-game-etheremon-is-one-of-them/. [Accessed: 17-Jun-2018].
12. V. Buterin, *Chain Interoperability*. New York, NY: R3CEV, 2016
13. S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*. www.bitcoin.org: 2009
14. S. Lee, "Explaining Directed Acylic Graph (DAG), The Real Blockchain 3.0," *Forbes*, 24-Jan-2018. [Online]. Available: https://www.forbes.com/sites/shermanlee/2018/01/22/explaining-directed-acylic-graph-dag-the-real-blockchain-3-0/. [Accessed: 17-Jun-2018].
15. S. Popov, "The Tangle", https://iota.org/IOTA Whitepaper.pdf (2016)
16. "Shamir's Secret Sharing Scheme - Storing Bitcoin seeds as Encrypted shards for geographically diverse backups - Steemit," - Steemit. [Online]. Available: https://steemit.com/bitcoin/@steempower/shamir-s-secret-sharing-scheme-storing-bitcoin-seeds-as-encrypted-shards-for-geographically-diverse-backups. [Accessed: 18-Jun-2018].

A. Bridgwater, "Blockchains Are Verticalizing, So We Need Interoperability," *Forbes*, 07-Feb-2018. [Online]. Available: https://www.forbes.com/sites/adrianbridgwater/2018/02/07/blockchains-are-verticalizing-so-we-need-interoperability/#16f1c4e97ab9. [Accessed: 16-Jun-2018].

17. "Blockchain Oracles," *BlockchainHub*. [Online]. Available: https://blockchainhub.net/blockchain-oracles/. [Accessed: 17-Jun-2018].
18. J. Buck, "Blockchain Oracles, Explained," *Cointelegraph*, 17-Jun-2018. [Online]. Available: https://cointelegraph.com/explained/blockchain-oracles-explained. [Accessed: 17-Jun-2018].
19. æternity, "Blockchain Oracles – æternity blog," *æternity blog*, 11-Apr-2018. [Online]. Available: https://blog.aeternity.com/blockchain-oracles-657f134ffbc0. [Accessed: 17-Jun-2018].
20. J. Peterson, "Augur: a Decentralized Oracle and Prediction Market Platform." Forecast Foundation. March 5, 2018
21. "What is SWIFT?," Fin. [Online]. Available: https://fin.plaid.com/articles/what-is-swift. [Accessed: 18-Jun-2018].
22. gpo.gov, 'TITLE 5—GOVERNMENT ORGANIZATION AND EMPLOYEES', 2012. [Online]. Available: http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf [Accessed 10-June-2018].
23. europa.eu, 'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)', 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj [Accessed 10-June-2018].

24. J. Clayton, “Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC,” 2017. [Online]. Available: https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission.
25. D. Tapscott, *Realizing the Potential of Blockchain A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies.* San Francisco, CA: World Economic Forum, 2017
26. E. Cheng, “An early bitcoin pioneer predicts how the blockchain will change banking,” *CNBC*, 21-Mar-2018. [Online]. Available: https://www.cnbc.com/2018/03/21/an-early-bitcoin-pioneer-predicts-how-the-blockchain-will-change-banking.html. [Accessed: 16-Jun-2018].
27. S. Silverstein, “CEO of blockchain company Chain on what everyone gets wrong about the technology,” *Business Insider*, 31-Jan-2018. [Online]. Available: http://www.businessinsider.com/ceo-blockchain-chain-adam-ludwin-tech-merging-cryptos-database-2018-1. [Accessed: 16-Jun-2018].
28. R. Staff, “Full transcript: Chain CEO Adam Ludwin answers cryptocurrency questions on Too Embarrassed to Ask,” *Recode*, 14-Mar-2018. [Online]. Available: https://www.recode.net/2018/3/14/17121406/transcript-chain-adam-ludwin-answers-crypto-currency-bitcoin-blockchain-questions-too-embarrassed. [Accessed: 16-Jun-2018].
29. M. Swan, *Blockchain: Blueprint for A New Economy*. Sebastopol, CA: OReilly Media, Inc., 2015.
30. W. VornDick, *China Brief: Beyond Bitcoin: Could China Embrace Blockchain for Defense and Security Applications?, Washington, DC: The Jamestown Foundation* Volume 18, Issue 2 2018
31. [1]廉 蔺,朱启超,赵 炤.区块链技术及其潜在的军事价值[J].国防科技,2016,37(2): Lian Lin, et al, “Blockchain Technology and Its Potential Military Value [区块链 技术及其潜在的军事价值],” National Defense Science & Technology [国防科 技], vol. 37 no. 2. (Apr 2016); p. 30-34
32. [1]廉 蔺, “区块链技术及其潜在的军事价值,” *BTC123*, 20-May-2017. [Online]. Available: http://news.btc123.com/news/detail?id=6467. [Accessed: 16-Jun-2018].
33. A. Panda, “Cryptocurrencies and National Security,” *Council on Foreign Relations*, 28-Feb-2018. [Online]. Available: https://www.cfr.org/backgrounder/cryptocurrencies-and-national-security. [Accessed: 16-Jun-2018].
34. 廉 蔺,朱启超,赵 炤.区块链技术及其潜在的军事价值[J].国防科技,2016,37(2): Lian Lin, et al, “Blockchain Technology and Its Potential Military Value [区块链 技术及其潜在的军事价值],” National Defense Science & Technology [国防科 技], vol. 37 no. 2. (Apr 2016); p. 30-34
35. 廉 蔺, “区块链技术及其潜在的军事价值,” *BTC123*, 20-May-2017. [Online]. Available: http://news.btc123.com/news/detail?id=6467. [Accessed: 16-Jun-2018].
36. S. Golstein, “Russian SWIFT to Transfer to Blockchain Technology by 2019 | Finance Magnates,” *Finance Magnates | Financial and business news*, 07-May-2018. [Online]. Available: https://www.financemagnates.com/cryptocurrency/news/russian-swift-transfer-blockchain-technology-2019/. [Accessed: 16-Jun-2018].
37. M. Seddon, “Putin considers 'cryptorouble' as Moscow seeks to evade sanctions,” *Financial Times*, 02-Jan-2018. [Online]. Available: https://www.ft.com/content/54d026d8-e4cc-11e7-97e2-916d4fbac0da. [Accessed: 16-Jun-2018].
38. N. Popper, “Blockchain Will Be Theirs, Russian Spy Boasted at Conference,” *The New York Times*, 29-Apr-2018. [Online]. Available: https://www.nytimes.com/2018/04/29/technology/blockchain-iso-russian-spies.html. [Accessed: 16-Jun-2018].
39. BISTVru, “CTCrypt 2017 - Standartisation of blockchain (Maxim Shevchenko),” *YouTube*, 27-Jun-2017. [Online]. Available: https://www.youtube.com/watch?v=kvTmlNHE-3Y. [Accessed: 16-Jun-2018].
40. “Meeting with founder of Ethereum project Vitalik Buterin,” *President of Russia*, 02-Jun-2017. [Online]. Available: http://en.kremlin.ru/events/president/news/54677. [Accessed: 16-Jun-2018].
41. D. Floyd, “Deloitte: 3 out of 4 Big Companies See 'Compelling' Case for Blockchain,” CoinDesk, May 15, 2018. [Online]. Available: https://www.coindesk.com/deloitte-3-out-of-4-big-companies-see-compelling-case-for-blockchain
42. R. Jennings, “China Leads The U.S. In Patent Applications For Blockchain And Artificial Intelligence,” Forbes, May 17, 2018. [Online]. Available: https://www.forbes.com/sites/ralphjennings/2018/05/17/ how-china-pulled-ahead-of-the-u-s-in-patent-applications-for-new-technology/#229a9b5a6048
43. “2018 China's Blockchain Industry White Paper,” Ministry of Industry and Information Technology, Qifeng Financial Blockchain Institute, May 2018. [Online]. Available: http://xxzx.miit.gov.cn/download.jsp?path=/attach/20180521/20180521103244_603.pdf

44. M. Huillet, “China's IT Ministry: 2017 Saw Peak Investment in Domestic Blockchain Industry,” Coin Telegraph, May 21, 2018. [Online]. Available: https://cointelegraph.com/news/chinas-it-ministry-2017-saw-peak-investment-in-domestic-blockchain-industry
45. E. Cheng, “Chinese President Xi Jinping calls blockchain a 'breakthrough' technology,” CNBC, May 30, 2018. [Online]. Available: https://www.cnbc.com/2018/05/30/chinese-president-xi-jinping-calls-blockchain-a-breakthrough-technology.html
46. W. Zhao, “$1 Billion Blockchain Fund Launches with Chinese Government Backing,” CoinDesk, April 9, 2018. [Online]. Available: https://www.coindesk.com/1-billion-blockchain-fund-launches-with-chinese-government-backing/
47. W. Zhao, “China State TV: Blockchain Is '10 Times More Valuable Than the Internet',” CoinDesk, June 4, 2018. [Online]. Available: https://www.coindesk.com/china-state-tv-blockchain-is-10-times-more-valuable-than-the-internet/
48. M. J. Casey, “It's Political: Why China Hates Bitcoin and Loves the Blockchain,” CoinDesk, September 27, 2018. [Online]. Available: https://www.coindesk.com/political-china-hates-bitcoin-loves-blockchain/
49. S. D'Cunha, “Dubai Sets Its Sights On Becoming The World's First Blockchain-Powered Government,” Forbes, December 28, 2017. [Online]. Available: https://www.forbes.com/sites/suparnadutt/2017/12/ 18/dubai-sets-sights-on-becoming-the-worlds-first-blockchain-powered-government/#2b9298e7454b
50. “Smart Dubai,” Government of UAE, Accessed June 12, 2018. [Online]. Available: https://smartdubai.ae/en/Pages/default.aspx
51. N. Heller, “Estonia, the Digital Republic,” *The New Yorker*, December 18, 2017. [Online]. Available: https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic
52. L. Mearian, “IBM sees blockchain as ready for government use,” Computer World, February 14, 2018. [Online]. Available: https://www.computerworld.com/article/3254202/blockchain/ibm-sees-blockchain-as-ready-for-government-use.html
53. “Government of Canada exploring the potential of Blockchain technology,” Bitaccess, January 19, 2018. [Online]. Available: https://blog.bitaccess.ca/government-of-canada-exploring-the-potential-of-blockchain-technology/
54. “Canada to test biometrics and blockchain for international travelers,” World Economic Forum, January 31, 2018. [Online]. Available: https://www.finextra.com/pressarticle/72424/canada-to-test-biometrics-and-blockchain-for-international-travellers
55. “Bitcoin Energy Consumption Index”, Digiconomist. [Online]. Available: https://digiconomist.net/bitcoin-energy-consumption [Accessed 8 May 2018].