DEMOCRACY IN OUR NEW WORLD:

Utilizing Blockchain Technology to Digitize Government Functions

Abstract

If the question is what government can do, the answer is your imagination. Blockchain technology possesses many applications for wealth generation in the financial sector. First adopters pursued use cases that generated profits, which funded their work. They established the rails and digital infrastructure that governments can utilize to improve government functions. Instead of seeking to tamper innovation, governments should utilize the infrastructure developed by first adopters to improve the functions and services they offer to their citizens. This paper addresses the use cases of blockchain technology in government.

Arowolaju, Damilola G.
Brown, Devron

I. Introduction

Jospeh Schumpter coined the term creative destruction, which occurs when innovative technology improves (or destroys) old processes. Today, automation and globalization drive creative destruction. Technological advancements allow firms to automate domestic manufacturing; whatever cannot be automated, globalization enables companies to outsource—at low costs. While some decry this process and focus on the losses resulting from it, technological innovation and creative destruction are inevitable. So rather than focusing on preventing the inevitable, attention should focus on minimizing harms when losses occur—and maximizing the gains.

On the horizon of another technological revolution is 5G technology, enabling faster wireless connection with larger bandwidth. Proponents of 5G Technology confidently claim that it will render blockchain technology ubiquitous: from devices connected to the internet of thing, to smart cities, and more. This claim is buttressed by lawmakers, who recently encouraged utilizing blockchain solutions to respond to the coronavirus pandemic.[1] But lawmakers are also growing antagonistic towards blockchain, because they are yet to appreciate the use cases for every-day people.[2]

As governments advance, they seek solutions to meet new demands. COVID-19 forced governments across the world to rethink the functioning of government to best meet citizens' needs. Technological innovation improved the functioning of businesses across the world. So, too, can technological innovation improve the functioning of government. McKinsey estimates that "government digitization, using current technology, could generate over $1 trillion annually worldwide."[3] This digitization can occur utilizing blockchain technology. Governments are already establishing a framework to digitize functions with blockchain, such as Illinois in 2018, with the final report to the General Assembly from the Illinois Blockchain and Distributed Ledger Task Force. [4]

This paper first describes the best case study of what digitizing governmental functions with blockchain technology looks like in practice: Estonia. From there, it provides a background on blockchain technology and describes how it functions. Then, it addresses the use cases of the technology that governments should pursue. Finally, it addresses inherent concerns digitization brings—particularly privacy and loss jobs due to automation.

II. Estonia Case Study

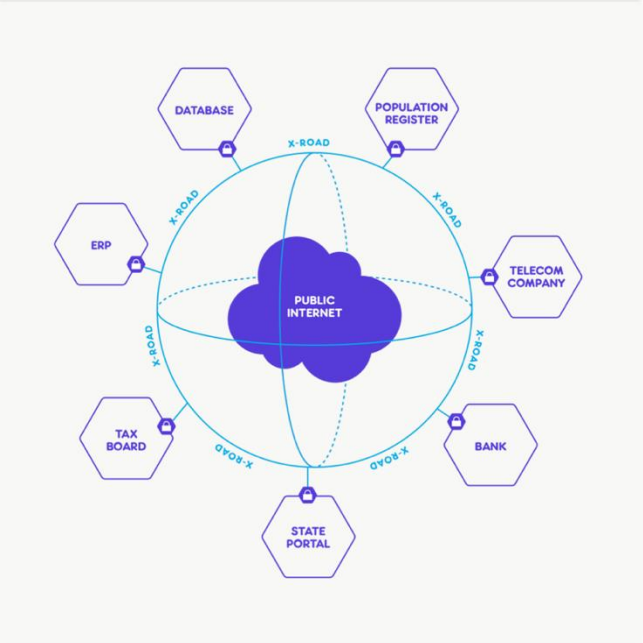
Estonia is a Baltic nation once known for its logging industry, but is now known as a digital democracy that even automates the counting of logs.[5] Estonia is a case study for what a digital democracy can look like.[6] Estonia's transition into a digital-democracy is housed under a project called *e-Estonia*, which is "a coördinated governmental effort to transform the country from a state into a digital society."[7] Under *e-Estonia*, the country digitized governmental functions such as legislation,

---

[1] Letter from Darren Sotto, Member of Congress & Tom Emmer, Member of Congress, to Steven T. Mnuchin, Secretary of the Treasury (Apr. 23, 2020).
[2] Letter from Elizabeth Warren, United States Senator, to Janet Yellen, Secretary of the Treasury (July 26, 2021).
[3] Bjarne Corydo, Vidhya Ganesan, and Martin Lundqvist, *Transforming government through digitization*, MCKINSEY.COM, https://www.mckinsey.com/industries/public-and-social-sector/our-insights/transforming-government-through-digitization#, Nov. 16, 2016.
[4] Cab Morris, John Mirkovic & Jennifer M. O'Rourke, *Illinois Blockchain and Distributed Ledger Task Force Report to the General Assembly* (January 31, 2018), https://www2.illinois.gov/sites/doit/Strategy/Documents/BlockchainTaskForceFinalReport020518.pdf; *see also*, Illinois House Joint Resolution 25.
[5] Nathan Heller, *Estonia, the Digital Republic*, THE NEW YORKER, December 11, 2017.
[6] *Id.*
[7] *Id.*

justice, policing[8] voting, education,[9] healthcare, banking, taxes[10], and more.[11] In fact, "apart from transfers of physical property, such as buying a house, all bureaucratic processes can be done online."[12] This process cuts down bureaucracy—saving the country 2% in G.D.P. a year.[13]

Here's how the program works. Basically, Estonia's data exchange platform, X-Tee (formerly known as X-Road) allows registered users to access data.[14] Once registered, every Estonian citizen owns a digital id card, allowing citizens to decrypt files, affix digital signatures on files, and engage within the digital society.[15] And in Estonia, you only need to enter data once. Once Estonian citizens



log their data, that information is stored locally at the specific institution. For example, your primary doctor maintains your medical records. But should you transfer to another institution and switch primary doctors, your new doctor can request access for your medical records on X-Tee. But not all data citizens enter is necessarily accessible. Citizens can choose to hide the data they enter. And that is because Estonia has decided that "[a] key tenet of [*e-Estonia*] is that an individual owns all information recorded about him or her."[16]

Looking at Estonia's digital success: The European Union developed its own digital strategy—working towards a digital government.[17][18] And the EU is already known for its progress in data

---

[8] *Security and Safety*, E-ESTONIA, https://e-estonia.com/solutions/security-and-safety/e-law/ (last visited Oct. 3, 2021).
[9] Sally Weale, *Lessons from Estonia: why it excels at digital learning during Covid*, GUARDIAN, Oct. 30, 2020, https://www.theguardian.com/world/2020/oct/30/lessons-from-estonia-why-excels-digital-learning-during-covid.
[10] *Business and Finance,* E-ESTONIA, https://e-estonia.com/solutions/business-and-finance/e-banking/ (last visited Oct. 3, 2021).
[11] Heller, *supra* note 5.
[12] *Id.*
[13] *Id.*
[14] *See generally*, Republic of Estonia Information System Authority, *Data Exchange Layer X-tee*, Republic of Estonia (last accessed May 13, 2020), https://www.ria.ee/en/state-information-system/x-tee.html.
[15] *Id.*
[16] Heller, *supra* note 5.
[17] *Id.*
[18] *See generally*, European Commission, *Shaping Europe's Digital Future: The European Digital Strategy*, European Union, (last accessed May 13, 2020) https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy.

regulation and protection, with their General Data Protection Regulation (GDPR).[19] Whereas, the U.S—according to Marten Kaevats, Estonia's national digital adviser—is a digital mess.[20] "Data architecture [in the U.S.] was too centralized. Citizens didn't control their own data; it was sold, instead, by brokers. Basic security was lax. . . . The U.S. had backward notions of protection . . . and the result was a bigger problem: a systemic loss of community and trust."[21]

In 2007, Estonia faced a massive cyber-attack from Russia that destabilized the digital society.[22] As a result: the NATO Cooperative Cyber Defense Center of Excellence was formed, which serves as a think tank and training facility.[23] Estonia also integrated K.S.I.—a blockchain platform—into its digital system to improve security.[24] The state also built a server closet in Luxembourg, with a backup of its systems.[25] So, if a digital invasion occurs, government officials can log on remotely—using digital signatures—to issue orders and run the government remotely through the cloud.[26] The following section will now describe how blockchain technology works. It is not a hyper-technical description, because a technical understanding is not necessary to utilize blockchain technology. For example, many people send emails and utilize the internet without a technical understanding of how it works.

III. Blockchain Technology Background

a. Origination of Blockchain

Before understanding how blockchain technology works, it is import to understand its genesis. Blockchain technology was originally created as a platform for Bitcoin, a cryptocurrency.[27] Bitcoin's goal: making electronic payments to other parties without third parties, like a bank—a peer-to-peer transfer of money.[28] When people engage in financial transactions through third parties, there are "inherent weaknesses."[29] The "inherent weaknesses" rest in relying on third parties and the transaction costs associated with these transactions.[30] For example, when sending money overseas, there are usually large transaction costs associated.[31] Further, the key issue is ensuring the purported seller is who they say they are and actually have the bargained for good or service.[32] For our electronic payments and transactions to occur, we must bare these transaction costs and trust the parties involved.[33] But at times, transaction costs are too high and we cannot trust parties. Bitcoin—a decentralized peer-to-peer payment network—reduced these transaction costs and the amount of trust one must have with the transacting party.[34] Through Bitcoin, parties can make payments without relying on banks and automatically verify the authenticity of the purported seller and their goods or

---

[19] Matt Burgess, *What is GDPR? The Summary guide to GDPR compliance in the UK*, WIRED, March 24, 2020.
[20] Heller, *supra* note 5.
[21] *Id.*
[22] *Id.*
[23] *Id.*
[24] Heller, *supra* note 5.
[25] *Id.*
[26] *Id.*
[27] SATOSHI NAKAMOTO, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008).
[28] *The great chain of being sure about things*, THE ECONOMIST, Oct. 31, 2015.
[29] NAKOMOTO, *supra* note 27.
[30] *Id.*
[31] ECONOMIC IMPLICATIONS OF REMITTANCES AND MIGRATION, (Dilip K. Ratha ed., 2006).
[32] NAKOMOTO, *supra* note 27..
[33] *Id.*
[34] *Id.*

services. This is what Satoshi Nakamato, the unknown creator(s) of Bitcoin had in mind when they released its white paper on blockchain and Bitcoin in 2008, in the wake of a massive financial crash.[35]

b. How Blockchain Technology Works

Blockchain technology, at its most basic level, is a computer file used for storing data.[36] The information stored varies. For example, the data could contain information about a transaction: purchaser i.d.; seller i.d.; the good or service; self-executing contract terms. The blockchain could contain information regarding a specific item, such as the owner of the deed to real property.[37] Each file or block contains one transaction or set of transactions, engrained with identifying codes.[38] Then, each subsequently validated transaction creates another block that links the earlier transaction and codes—creating a chain, a blockchain or electronic ledger.[39] This allows parties to trace transactions and items from their origin and verify authenticity because a block will not be added to the blockchain unless the transaction is validated as authentic.[40] When each block is added, every user or node's blockchain is updated to reflect it, thus, creating an open network of information.[41]

There are three key characteristics of blockchain technology: (1) decentralization, (2) cryptography, and (3) openness.[42] We will take them in turn.

i. Decentralization

Most computer files are stored only on a single computer. With blockchain, however, the files are distributed amongst any computer (or node) connected to a single network.[43] In this way, Blockchain technology is like a shared drive. But unlike a shared drive no single owner controls or edits the files (depending on if it is a public or private blockchain). Instead, changing or editing a file—altering—a block in the chain—requires achieving consensus amongst the users in the network that store their own separate and identical files on the blockchain.[44] If there is no consensus, no change can occur. In a blockchain platform that utilizes proof of work, this concept is called mining. It is energy intensive because it requires miners to guess the corresponding hash value first to validate the block, so they use fast computers guessing millions of numbers that require immense computing power. And the reward for mining is cryptocurrency.[45] But there is less energy intensive consensus protocol called proof of stake, which requires random groups or "committees" of users or "validators" to stake cryptocurrency before confirming individual transactions, risking losing the staked cryptocurrency for confirming invalid transactions, but gaining cryptocurrency by confirming valid transactions.[46]

---

[35] The great chain of being sure about things, *supra* note 3.
[36] Bernard Marr, *What Is Blockchain? A Super Simple Guide Anyone Can Understand*, BERNARD MARR & CO.
[37] The great chain of being sure about things, *supra* note 3.
[38] NAKOMOTO, *supra* note 27.
[39] The great chain of being sure about things, *supra* note 3.
[40] JAMIE BERRYHILL, THEO BOURGERY & ANGELA HANSON, *Blockchains Unchained: Blockchain Technology and its Use in the Public Sector*, OECD WORKING PAPERS ON PUBLIC GOVERNANCE, 13 (2018).
[41] *Id.* at 18.
[42] MARR., *supra* note 36
[43] *Id.*
[44] *Id.*
[45] *See generally* Andrew Tar, *Proof-of-Work Explained*, COINTELEGRAPH, https://cointelegraph.com/explained/proof-of-work-explained, Jan. 17, 2008.
[46] *See generally The Beacon Chain Ethereum 2.0 explainer you need to read first*, https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/, May 23, 2020.

ii. Cryptography

Blockchain technology uses asymmetric cryptography to encrypt and authenticate data within the chain, creating inherent security.[47] Asymmetric cryptography is an encryption mechanism where the sender uses one key to encrypt and recipient uses a different key to decrypt. This is different from symmetric cryptography where the same key is used to encrypt and decrypt. Imagine Alice wants to pay Bob for a sandwich using Bitcoin. Bob has a private key attached to his wallet and uses the private key to generate a public key for the specific transaction. Bob sends his public key to Alice. Alice uses her private key to encrypt the Bitcoin and transaction information, which creates a digital signature and a digest of the information. Digital signatures are like thumbprints or signatures unique to a party that bind a party to a specific transaction. (The transaction information also includes the earlier transactions or blocks associated to the cryptocurrency.) Then Alice uses Bob's public key to encrypt the digest and sends it to Bob. Bob uses his private key to decrypt the digest and authenticate whether the transaction is a valid transaction on the blockchain. If it is valid, nodes on the network confirm the transaction. The transaction would be invalid if Alice altered any of the information about the cryptocurrency, including any of the past transactions, because this would create a different digest. So, when Bob's private key authenticates the transaction, it will see that someone altered the transaction and reject the transaction.

Another way to conceptualize how asymmetric cryptography works is to think about Alice paying for the sandwich by depositing money to Bob in a locked box with an open slit. Bob gives Alice the locked box, but he does not give her the key to the box. Alice deposits the money in the box and a ledger detailing this transaction and past transactions. Then, she gives the box back to Bob. Bob then uses his key to open the box and takes the money and checks the ledger. Bob then cross references his ledger to make sure all the transactions match up. If the ledgers do not match, Bob will know something is wrong with the transaction.

This security protects against fraud and prevents someone from altering or fabricating the blockchain (or ledger). Blockchain, however, is not immutable or tamper proof—it is tamper evident. A "51 percent hack" can alter a blockchain.[48] This occurs when 51 percent of the users or nodes on the network are used to alter a particular chain.[49] First, however, in a public blockchain, it is nearly impossible for this to occur because it would require millions of unknown users to collaborate.[50] Second, in a private blockchain, only authorized users can make changes, so it is possible to identify who made the change. Lastly, if the changes did occur in a blockchain: Whether public or private, the blockchain would reflect a change in the blocks.

iii. Openness

The most important characteristic of blockchain is openness.[51] In a public blockchain every transaction made is visible to all users on the blockchain.[52] Since anyone with an internet connection can join a public blockchain—it is open to the world. In a private blockchain, anyone with permission to view the blockchain can view the transactions.[53] This openness increases transparency, thus increasing accountability.

---

[47] *Id.*
[48] BERRYHILL ET AL., *supra* note 40, at 18.
[49] *Id.*
[50] *See Id.*
[51] MARR., *supra* note 36
[52] BERRYHILL ET AL., *supra* note 40, at 19.
[53] MARR., *supra* note 36.

c. Public v. Private

Public and private blockchains effectively function the same way. The difference lies in who can engage in transactions, as well as who can view and edit the blockchain. In a public blockchain, on one hand, anyone with an internet connection can view, engage in transactions, and edit the blockchain. Moreover, all participants are pseudo-anonymous—each identifiable only by public keys. Public blockchains usually have an incentive system to encourage users to join and validate transactions. The largest public blockchain to date is Bitcoin.

Private blockchains, on the other hand, can be programmed to require permission to edit or view the blockchain and make transactions. Moreover, private blockchains require less energy output to operate, because they do not need mass consensus from a multitude of nodes (computers) to authenticate transactions. Private blockchains may offer the best use for the public sector because they "can greatly enhance accountability, as transactions can be transparent to everyone, while only authorized users are able to actually record new transactions."[54] In a private blockchain, all the users are known. Thus, a private blockchain can serve as an effective and reliable electronic ledger—tracing transactions and the parties conducting them from the inception to the present. Thus, allowing the owner to keep track of their transactions and identify irregularities.

d. Current Uses of Blockchain Technology

Blockchain technology can fundamentally alter how private parties, businesses, institutions, and governments transact. The following sections address some, but not all the current uses of blockchain technology.

i. Cryptocurrency

It is important to make the distinction between blockchain technology and cryptocurrencies like Bitcoin. In its inception, blockchain was a platform used to support the cryptocurrency Bitcoin, which launched in 2009.[55] Other cryptocurrencies soon followed suit, particularly after Bitcoin amassed immense value. Blockchain is to cryptocurrencies, as is the internet is to email—a platform. Cryptocurrencies are a means of conducting peer-to-peer payments without a third-party intermediary, like a bank. Cryptocurrencies, however, are not blockchain's only application.

ii. Smart Contracts

Blockchain technology can revolutionize government functions with smart contracts. Karim Lakhani and Marco Iansiti, professors at Harvard Business School, claim "'[s]mart contracts' may be the most transformative blockchain application at the moment."[56]

Smart contracts are contracts that self-execute once the conditions of the contract are met. Smart contracts retain all the benefits of blockchain technology while also fostering greater efficiency

---

[54] BERRYHILL ET AL., *supra* note 40, at 19.
[55] MARR., *supra* note 36.
[56] Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. (2017), https://hbr.org/2017/01/the-truth-about-blockchain (last visited Oct 28, 2018).

by diminishing the processing time associated with the execution of a contract or transaction. Ethereum is the most developed blockchain platform for smart contracts to date.[57]

iii. Tokens

Some blockchain platforms, like Ethereum, allow users to develop tokens that operate on the platform. Tokens vary based on their function. Some tokens function as securities or "digital assets" because they meet the definition of an investment contract under the Howey test.[58] Other tokens are utility tokens. Utility tokens—most commonly ERC-20 tokens—are analogous to arcade tokens.[59] Once someone places an arcade token in a machine, they can use the functions of the machine. Similarly, when someone acquires an ERC-20 token and pays a fee (gas), they can run the decentralized application programmed by the token on Ethereum. Lastly, there are non-fungible tokens (NFTs). NFTs represent a real-world item recorded or tokenized on a blockchain. They are an effective tool for record keeping.

iv. Stablecoins

Stablecoins are cryptocurrencies with a value fixed or pegged to a real-world currency, like the U.S. dollar. As its name suggests, Stablecoins do not fluctuate in value. Some Stablecoins are backed by bonds or other assets. Stablecoins present the solution to the problem Bitcoin cannot solve due its fluctuation in price—engaging in transactions without a bank or other intermediary.[60] Tether is a Stablecoin operated by Bitfinex that is pegged to dollar U.S. dollar, backed by large amounts of commercial paper, and maintains the largest market capitalization of all Stablecoins.[61] And Dai is a fascinating Stablecoin pegged to the U.S. dollar but is completely decentralized, collateralized by various cryptocurrencies, and is issued by one of the earliest decentralized applications (dapps) on the Ethereum blockchain—MakerDAO.[62] Dai presents a conundrum to regulators: how do you regulate a decentralized autonomous organization?

v. Decentralized Finance (DeFi)

Decentralized finance ("DeFi") displaces traditional finance and banking by maintaining a decentralized financial market accessible to anyone with an internet connection. According to the World Bank: "Globally, 1.7 billion adults remain unbanked, yet two-thirds of them own a mobile phone that could help them access financial services."[63] DeFi presents an opportunity to provide liquidity to those out of reach of the traditional financial systems due to systemic inequities or faulty

---

[57] BERRYHILL ET AL., *supra* note 40, at 19.
[58] *Framework for "Investment Contract" Analysis of Digital Assets*, U.S. Securities and Exchange Commission, Apr. 3, 2019, https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.
[59] *See generally ERC-20: The Definitive Ethereum Token Standard*, CRYPTOPEDIA, https://www.gemini.com/cryptopedia/erc20-token-standard-ethereum, May 17, 2021.
[60] *See generally* Christian Catalini and Jai Massari, *Stablecoins and the Future of Money*, HARV. BUS. REV., Aug. 10, 2021, https://hbr.org/2021/08/Stablecoins-and-the-future-of-money.
[61] *Why regulators should treat Stablecoins like banks*, THE ECONOMIST, Aug. 7, 2021, https://www.economist.com/leaders/2021/08/07/why-regulators-should-treat-Stablecoins-like-banks.
[62] *How MakerDAO Pioneered Decentralized Finance*, CRYPTOPEDIA, March 12, 2021, https://www.gemini.com/cryptopedia/makerdao-defi-mkr-dai-coins.
[63] *Financial Inclusion on the Rise, But Gaps Remain, Global Findex Database Shows*, WORLD BANK, Apr. 19, 2018, https://www.worldbank.org/en/news/press-release/2018/04/19/financial-inclusion-on-the-rise-but-gaps-remain-global-findex-database-shows.

credit underwriting processes. Under various DeFi protocols, users can transfer funds, provide loans, receive loans, invest, swap tokens, and more.[64]

IV. How Governments Should Utilize Blockchain

Blockchain initially gained prominence through the financial sector because of cryptocurrencies.[65] But blockchain is now spreading through the public sector. In fact, "at least 46 countries around the world have launched or are in the planning stages to launch over 200 [b]lockchain-related initiatives."[66] For example, Dubai partnered with IBM to develop the world's first government-backed blockchain platform.[67] Sheikh Hamdan Bin Mohammed Al Maktoum wants Dubai's entire government to operate on blockchain.[68] The first areas where Dubai will implement blockchain are in health records, securing the diamond trade, title transfers, business registration, digital wills, tourism engagement, and improved shipping.[69] In addition, American agencies are also seeking to implement blockchain to enhance various operations—particularly in procurement.[70] In a speech at the Blockchain Forum on October 10, 2017, Deputy Secretary of State, John J. Sullivan stated,

> "Blockchain has the potential to become a transformative technology of our lifetime. . . and is expected to play a major role in trade, business, healthcare management, and finance, and we hope at the State Department as well. . . . [S]peaking on behalf of the U.S. Government, we want to educate ourselves about how we can better leverage Blockchain technology. . . . [W]e're excited about the many ways Blockchain technology could also increase transparency and accountability here at the State Department and across the federal government."[71]

The following sections present opportunities for governments to digitize their functions utilizing blockchain.

a. Procurement

Public procurement or government contracting refers to the process of acquiring goods and services from private parties by a government agency [72]In other words, public procurement occurs when governments acts as a consumer.[73] Procurement is the life blood of developed nations. In fact, the 35 members of the Organization for Economic Co-operation and Development ("OECD") spend nearly 12 percent of their GDP on public procurement.[74]

---

[64] Alyssa Hertig, *What is DeFi?*, CoinDesk, Sep. 18, 2020, https://www.coindesk.com/tech/2020/09/18/what-is-defi/.
[65] BERRYHILL ET AL., *supra* note 40, at 20.
[66] *Id.*
[67] Alkesh Sharma, *From 45 days to seconds: Smart Dubai, IBM introduce Middle East's first government-backed blockchain platform*, THE NATIONAL, Oct. 31 2018.
[68] Saqr Ereiqat, *Blockchain in Dubai: Smart cities from concept to reality*, BLOCKCHAIN UNLEASHED: IBM BLOCKCHAIN BLOG, Apr. 10, 2017.
[69] Pete Rizzo, *Dubai's Global Blockchain Council Unveils First Pilot Projects*, COINDESK, May 30, 2016.
[70] *See generally*, Selva Ozelli, *US Government Implements Blockchain Programs to Improve Transparency and Efficiency*, COINTELEGRAPH, Jan. 23, 2018; HOUSE SCIENCE, SPACE, AND TECHNOLOGY SUBCOMMITTEE ON RESEARCH AND TECHNOLOGY AND OVERSIGHT HEARING, (2018).
[71] JOHN J. SULLIVAN, *Remarks at the Blockchain Forum*, http://www.state.gov/s/d/17/274725.htm (last visited Nov 20, 2018).
[72] *Public procurement*, OECD, http://www.oecd.org/gov/public-procurement/ (last visited Jan 21, 2019).
[73] Procurement, however, can sometimes embody the sale of government assets by a government.
[74] [74] Public procurement - OECD, *supra* note 73..

Procurement has such a large impact on the United States that during the government shutdown in 2018–19: The United States lost $200 million a day and its economic growth reduced by 0.13 percent every week the shutdown lasted.[75] And during the shutdown, more than 1 million government contractors were furloughed.[76] Since procurement is such a crucial component of a nation, the OECD states that governments are expected to carry out public procurement "efficiently and with high standards of conduct in order to ensure high quality of service delivery and safeguard the public interest."[77] This means that good procurement requires efficiency, transparency, and integrity, which blockchain can help promote. The best use for blockchain technology in procurement is through a private blockchain that allows the public to view but not edit the blockchain.

The following sections will address how blockchain technology can enhance procurement supply chain transparency and traceability. And how it can improve the contract awarding process.

i. Supply Chain Transparency/Traceability[78]

Utilizing blockchain technology in procurement will enhance the supply chain traceability and transparency of transactions between a government and private contractors, as governments can track goods and transactions from their origin.[79] One example of this in the private sector is Walmart: the store used blockchain technology to locate the source of romaine lettuce that caused an E. coli outbreak in the United States.[80] There are many steps in the supply chain that make it hard to track down one food item.[81] It usually takes at least seven days to find a contaminated food item—but with a blockchain system, it took as little as 2.2 seconds to find the source of the contamination.[82]

The enhanced traceability that blockchain technology brings surely can serve any government well—so can the added transparency. Since all transactions are permanently logged on the blockchain, the government and the public—depending on the setup of the blockchain—can trace exactly which parties were awarded contracts, what good or services the contracts were awarded for, and the amount of money awarded for the contracts. This increased transparency can lead to increased bid protests, which serves as another method of procurement accountability. As disappointed bidders have more clear and public information regarding the awarded contract, this clarifies and speeds up the bid protest process.

ii. Improve Contract Award Process

Information is powerful, particularly information that is easily and readily available. With more readily accessible information, governments can ensure they are engaging in transactions with responsible parties, particularly in countries like the United States, where the responsibility of the contractor is a factor considered in awarding a contract. The United States federal government has a database called the Federal Awardee Performance and Integrity Information System ("FAPIIS") that holds data like "contract terminations, past performance, responsibility determinations, administrative

---

[75] Ari Natter, *Government Contractors to Lose Out on Shutdown Pay, Dragging Down Economy*, BLOOMBERG, Jan. 17, 2019.
[76] *Id.*
[77] Public procurement - OECD, *supra* note 73.
[78] A natural byproduct of enhanced transparency and traceability in a procurement system is enhanced integrity.
[79] BERRYHILL, ET AL., *supra* note 40.
[80] Matt Smith, *In Wake of Romaine E. coli Scare, Walmart Deploys Blockchain to Track Leafy Greens*, WALMART https://news.walmart.com/2018/09/24/in-wake-of-romaine-e-coli-scare-walmart-deploys-blockchain-to-track-leafy-greens (last visited Jan 19, 2019).
[81] *Id.*
[82] *Id.*

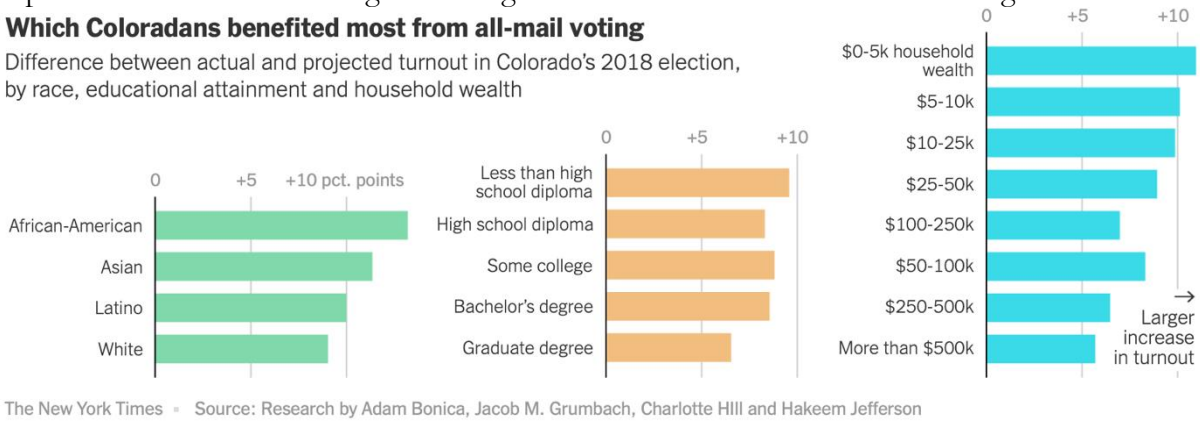
agreements, or criminal, civil, or administration actions involving the contractor."[83] Governments can incorporate the data on databases like the FAPIIS into a blockchain so the government and the public will have everything they need to know about a contractor. Faster responsibility determinations lead to faster contract awards. This also will increase efficiency, another important goal of good procurement.

The General Services Administration ("GSA")—a United States agency that oversees the management and operation of other government agencies—believes blockchain technology can shorten the time frame for its contract award process.[84] Smart contracts can drastically shorten the contracting process—allowing governments to engage in more contracts. Governments can configure the terms of a smart contract to automatically execute once the good or service is received in accordance with the specifications. The enhanced efficiency created will also save governments a tremendous amount of money, because it will cut down transaction costs. In sum, blockchain technology can lead to a more efficient and cost-effective procurement process.

The U.S. Department of Health and Human Services ("HHS") has launched Accelerate, a system to manage contracts and billing, utilizing blockchain, artificial intelligence, machine learning, and process automation.[85] This is one of the first federal blockchain applications and it has saved HHS over $720M.[86]

b. Voting

Voting for representatives are the foundations of any democracy. The coronavirus pandemic forced democracies around the world to contend with conducting voting from a distance. In America, state governments are grappling with whether to increase voting by mail, but some officials—mainly Republican officials—advise against doing so and have increased barriers to voting.[87]



A study done on voter information in Colorado (where ballots are mailed to all registered voters) shows mail ballots increased voter turnout for all groups—reducing inequities in voter

[83] Jessica Tillipman, *THE FOREIGN CORRUPT PRACTICES ACT & GOVERNMENT CONTRACTORS: COMPLIANCE TRENDS & COLLATERAL CONSEQUENCES*, BRIEFING PAPERS 25 (2011).
[84] Joe Kim, *Blockchain: A Path to Unblocking Government Procurement Processes*, THE AMERICAN CITY & COUNTY; PITTSFIELD (2018).
[85] Clavin, Erickson, Li, et al., *Blockchains for Gov. Use Cases and Challenges*, 1 DIG. GOV.: RES. AND PRACT. 3, Article 22, 8-9 (Nov. 2020), https://dl.acm.org/doi/pdf/10.1145/3427097.
[86] *Id.* at 10.
[87] *See* Charlotte Hill et al., *We Should Never Have to Vote in Person Again*, NEW YORK TIMES, May 4, 2020, https://www.nytimes.com/2020/05/04/opinion/coronavirus-vote-by-mail.html.

representation.[88] Increasing the number of potential voters is ideal for democracy.[89] So, if nations want to increase democratic representation, they should pursue methods for casting votes that achieve just that. The study from Colorado demonstrates mail ballots provides an opportunity to do just that.

Although "fraud is exceptionally rare, hard to commit without getting caught and nearly impossible to do on the scale necessary to affect [American] election results,"[90] mail ballots are admittedly susceptible to at least some degree of fraud. And because mail voting leaves behind a paper trail—which election officials can audit to verify that votes were counted as cast—it may actually be even more secure than in-person voting."[91] But for some, the risk of fraud (regardless of how minimal) is too large for comfort. This risk is heightened in emerging democracies were voter fraud already runs rampant.

Blockchain voting can create the same benefits of voting by mail but with decreased risks of fraud. In fact, West Virginia, Utah and the City of Denver have all utilized a blockchain voting application in elections.[92]Blockchain voting works like the transaction between Alice and Bob described above.[93] But instead of Alice giving Bob money, Alice gives Bob her vote. Let us imagine Alice is a voter and Bob is a state clerk. Prior to the election, Alice registers to vote with the clerk's office. Alice gives the clerk's office personal identifiable information (PII) that confirms she is eligible to vote. This then creates an ID for Alice that is not attached to her PII, which will allow her to vote on election day. On election day: Bob gives Alice a secured box, and Alice places her vote and ID into the secured box. Alice sends the box back to Bob. Bob unlocks the box and checks to see if the ID is a valid voter ID, which has not cast a ballot, and if it is valid—he records the vote. This process occurs through a mobile application or on a government website.

Like mail in ballots, blockchain voting would leave an electronic trail of votes that election officials can audit. The one concern, though, is the vulnerability of the devices individuals use to cast their votes and security of the server that holds the voting data. For example, in principle someone could hack a voter's phone and access it remotely. But a government could configure the system to require biometric recognition (face id or finger print) to proceed on the application. Also, the wide scale cyberwarfare required to hack enough phones to disrupt an election would indicate a larger issue requiring government intervention. If the servers were attacked, the hackers could not change the votes because they are encrypted and would not have permission to make changes on the blockchain. If, however, they were able to hack a user that had permission to edit the blockchain, any changes would be recoded on the blockchain and revealed by an audit.

c. Taxation

Since early civilization, governments struggle with decreasing the gap between taxes owed and taxes collected—the "tax gap." Each year, governments lose billions of dollars in potential revenue because many individuals and business fail to file and pay taxes. In fact, from 2011 to 2013, the Internal Revenue Service estimates the tax gap was $441 billion *per* year.[94] The taxation process requires

---

[88] *Id.*

[89] *But see* Aaron Blake, *Trump just comes out and says it: The GOP is hurt when it's easier to vote*, WASHINGTON POST, March 30, 2020.

[90] HILL ET AL., *supra* note 88

[91] *Id.*.

[92] Daniel Palmer, *Utah County to Offer Blockchain Voting App in Municipal Elections*, COINDESK, July 23, 2019, https://www.coindesk.com/markets/2019/07/23/utah-county-to-offer-blockchain-voting-app-in-municipal-elections/.

[93] *See supra* Section IIb.

[94] *The Tax Gap*, IRS.GOV, Oct. 21, 2020, https://www.irs.gov/newsroom/the-tax-gap.

authenticating records from businesses and personal records from individuals, which itself bears a significant administrative cost. Blockchain technology can automate the tax collecting process, allowing tax administrators to collect financial information from businesses and individuals in real time as transactions are made, authenticate financial data quicker, reduce paperwork, and increase the speed that refunds are distributed, using smart contracts.[95] This can also free up resources, allowing tax collectors to increase their enforcement and scrutiny of individuals that attempt dodge their tax bill. The newly recovered funds can then go government programs that need it the most—like social welfare.

d. Records & Data Management

Governments store and issue records: deeds, marriage licenses, driving records, health records, financial records, birth records, death records, corporate records, permits, etc. Many records are physical documents located at specific agencies. By using smart contracts and tokens on a blockchain platform, records management processes can be revolutionized. Governments can facilitate instant recordation of deeds and titles. For example, residents can purchase real property, logging the transaction on a blockchain platform in real-time by tokenizing it, creating a chain of title that allows a third party to easily authenticate and ascertain chain of title. There are several countries across the developing world seeking to update land registries through tokenization.[96]

The biggest problem when it comes to disputes regarding real property or secured transactions is figuring out which party had the best claim to the property or asset. Recording is the process that gives notice to prevent disputes. But this process can be more efficient and transparent if the transactions are automatically recorded, instead of requiring parties to record at the agency. When it comes to other records, digitizing the process on a blockchain platform can allow citizens easier access to their records without worrying about losing physical documents. Similar to its use Estonia, a centralized collection of records will further enable governments to share information and understand who is who, from parent companies and subsidiaries to parents and children.

Managing health care data with blockchain technology is an area with increased interest over the past decade.[97] The U.S. Center for Disease Control and Prevention ("CDC") is researching using blockchain technology to track public outbreaks of hepatitis A, and with IBM, began constructing a blockchain platform to track the opioid epidemic.[98] Imagine these very applications implemented to respond to the COVID-19 pandemic. For example, tracking cases and instead of requiring individuals to carry around physical vaccine cards, it was instead logged on a blockchain platform allowing for easier verification.

---

[95] *See generally*, Kuralay Baisalbayeva, Eelco van der Enden, Valentina Ion et al., *Blockchain for tax compliance*, PWC/MICROSOFT/VERTEX, https://clouddamcdnprodep.azureedge.net/gdc/gdcDQxrqP/original (2019).
[96] Georg Eder, *Digital Transformation: Blockchain and Land Titles*, 2019 OECD GLOBAL ANTI-CORRUPTION & INTEGRITY FORUM, Mar. 2019, https://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf.
[97] CLAVIN ET AL., at 11.
[98] *Id.* at 9.

e. Distributing Aid & Benefits

On September 16, 2020, the Director of D.C Department of Employment Services (the "Department") testified before Committee on Labor and Workforce Development that the current unemployment compensation systems requires technological improvements. The District, like other U.S. states, experienced a rapid increase in unemployment claims, which overwhelmed the Department and its operations. This is another government function that can be made more efficient utilizing a blockchain platform and smart contracts that can authenticate the benefit requestors and automatically issue benefits when the conditions for the benefits are met. This same concept is applicable to the disbursement of foreign aid. Governments could automatically condition foreign aid to governments or entities on various conditions and increase oversight on how funds are utilized.

f. Central Bank Digital Currencies (CBDCs)

Central bank digital currencies ("CBDCs") are effectively a Stablecoin issued by a state's central bank, like the U.S. Federal Reserve, which is a digital representation of the nation's fiat currency—backed by the full-faith of the government.[99] Over 81 countries, representing 90 percent of global GPD are considering CBDCs, with 5 countries already launching their own currencies—including China.[100] To fully optimize the use-cases listed above, a government could launch a blockchain platform with a CBDC as its native currency or token, which would be used to fully integrate payments and transactions on its blockchain. Launching a CBDC, however, presents a host of complications from privacy concerns to adequate control of monetary policy.[101] But there are also concerns for a country like the United States in not issuing a CBDC. The hard and soft power of the U.S. in large rests on the hegemony of the U.S. dollar. About 85 percent of all foreign exchange transactions, 61 percent of foreign exchange reserves, and 40 percent of international payments are in U.S. dollars. [102] The world is dependent on the U.S. dollar, but digital currencies, particularly CBDCs backed by a government present the opportunity for the world to wean itself from the U.S. dollar with a currency easier to transact and free from the heavy-hand of a U.S. sanctioning regime.

---

[99] *See generally Central Bank Digital Currencies*, BANK FOR INT'L. SETTLEMENTS, Mar. 2018, https://www.bis.org/cpmi/publ/d174.pdf.

[100] Central Bank Digital Currency Tracker, ATLANTIC COUNCIL, https://www.atlanticcouncil.org/cbdctracker/ (last visited Sept. 22, 2021).

[101] *Id.*

[102] *US dollar funding: an international perspective*, Bank of Int'l Settlements, CGFC Papers No. 65, at 3, June 2020, https://www.bis.org/publ/cgfs65.pdf.

V. Concerns

a. When the Private Sector Attempts Preempting the Public Sector: Libra, a Case Study

i. Background

History has dictated the path forward for fintechs. To understand the point of inflection for the United States' and the regulatory structure for Stablecoins and the like, it starts with Facebook. Facebook made all the mistakes and industry stakeholders learned how to introduce tech to congress in a productive way. For the first-time ever, the sections below provide background and overview as to how it all transpired and the gates of fintech opened up.

In 2019, the House Financial Services Committee ("HSFC") held two hearing's on Facebook's efforts to create a Stablecoin, Libra (now branded as Diem, Latin for "day" and without direct Facebook control)[103] and a digital wallet, Calibra (now branded as Novi, "a portmanteau of the Latin root words, "novus" meaning new and "via" meaning way")[104]. The Committee characterized Libra as an alternative to the U.S. dollar and viewed Calibra akin to a bank account. In June 2019, Facebook released a seven-page white paper on the Libra project without consulting Congress, key federal and state regulators, foreign regulatory bodies, or other relevant stakeholders. Facebook planned for the Libra Association ("Association") and its 27 other members to serve as an independent, not-for-profit organization headquartered in Geneva, Switzerland. And unlike most other Stablecoins built on blockchain technologies,[105] the Libra Association would be permissioned, whereby only members can validate transactions.

Shortly after Facebook's Libra plans were announced, Chairwoman Waters (D-CA), along with other members, wrote a letter to Facebook and called on it to agree to place a moratorium on any further development of Libra and Calibra until regulators and Congress had sufficient opportunity to review these products.[106]

ii. The Initial Hearing

The first hearing on July 17, 2019, entitled, "Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System" and convened two-panels: the first with David Marcus, CEO of Calibra and the second with leading monetary policy, systemic risk, and securities law experts. Committee members found the balance sheet size and management style of Facebook embarking on a monetary project of this magnitude alarming, considering the company's past failures. Facebook has more than 2.7 billion monthly active users—more customers than JP Morgan Chase, Wells Fargo, Citibank, and Bank of America combined.[107]

---

[103] See Nikhilesh De, *Libra Rebrands to "Diem" in Anticipation of 2021 Launch*, COINDESK, Dec. 1, 2020, https://www.coindesk.com/libra-diem-rebrand.

[104] *See* Sebastian Sinclair, *Facebook's Calibra Rebrands to Novi, Details Wallet Tie-Up With WhatsApp*, COINDESK, May 26, 2020, https://www.coindesk.com/libra-facebook-blockchain-digital-wallet-novi-calibra.

[105] Christine Kim, *New Libra Fork Will Create Permissionless Stablecoin Free of Corporate Control,* COINDESK Oct. 11, 2019, https://www.coindesk.com/new-libra-fork-will-create-permissionless-stablecoin-free-of-corporate-control.

[106] *See* House Committee on Financial Services, *Committee Democrats Call on Facebook to Halt Cryptocurrency Plans* July 2, 2019, https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=404009.

[107] Peter Rudegeair, *Venmo Has 40 Million Users, Outnumbering Most Big Banks*, WALLSTREET JOURNAL, Apr. 24, 2019, https://www.wsj.com/articles/venmo-has-40-million-users-outnumbering-most-big-banks-11556142906.

Cryptocurrency exchanges, including those that list Stablecoins,[108] are also frequently targeted by cyberattacks and data breaches.[109] To facilitate its cryptocurrency transactions, Facebook intended to manage and hold a detailed digital repository of social (Facebook and Instagram posts), financial (purchases and spending habits), and governmental data (name, address, and driver's license number), which may further increase their hacking risks. Facebook has had issues with safeguarding its users' information in the past. For example, Cambridge Analytica, a political consulting firm had access to more than 50 million Facebook users' private data which it used to influence voting behavior.[110]

iii. Domestic and Foreign Regulatory Concerns

U.S. regulators and financial leaders raised concerns with Libra. According to Federal Reserve Board Chairman Jerome Powell, "Libra raises many serious concerns regarding privacy, money laundering, consumer protection, and financial stability."[111] Chairman Powell stated that the project "cannot go forward" without addressing those concerns. Likewise, Federal Reserve Board Governor Lael Brainard stated that "there are likely to be financial stability risks for a Stablecoin network with global reach. If not managed effectively, liquidity, credit, market, or operational risks—alone or in combination—could trigger a loss of confidence and a classic run."[112] Governor Brainard also noted, "[t]he potential for risks and spillovers could be amplified by potential ambiguity surrounding the ability of official authorities to provide oversight and backstop liquidity and to collaborate across borders."[113]

Concerns mounted from overseas. After the Committee's July hearing, international regulators also expressed analogous concerns surrounding Facebook's plans with Libra and Calibra. In August, regulators from France and Germany both agreed to block Libra from their countries; in a joint statement, the two governments stated that "no private company can claim monetary power, which is inherent to the sovereignty of nations." The G-7 and the Financial Stability Board ("FSB") called for more scrutiny and higher regulatory standards for Stablecoins, such as Libra, particularly to protect consumers and ensure cryptocurrencies are not used to launder money or fund terrorism.[114] On October, 23, 2019, the Committee convened another hearing with Facebook's CEO, Mark Zuckerberg. Notably, seven of the original Libra Association signatories abandoned the project days before the hearing.[115] The Committee invited Zuckerberg to explain, how he intended to provide a sound financial product while Facebook failed protecting user trust on the company's platform. In an analysis of Facebook's efforts, Chairwoman Waters (D-CA) stated, "I've come to the conclusion that

---

[108] *See* Sebastian Sinclair, *Tether Froze $300K of Stablecoin Hacked After Victims Left Wallet Keys in Evernote*, COINDESK, Dec. 9, 2020, https://www.coindesk.com/tether-froze-300k-of-stablecoin-hacked-after-victims-left-wallet-keys-in-evernote.

[109] *See also* Brian Barrett, *Hack Brief: Hackers Stole $40 million from Finance Cryptocurrency Exchange*, WIRED, May 8, 2019, https://www.wired.com/story/hack-binance-cryptocurrency-exchange/.

[110] Kevin Granville, *Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens*, N.Y. TIMES, Mar. 19, 2018, https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html.

[111] Pete Schroeder and Trevor Hunnicutt, *4-Fed chief calls for Facebook to halt Libra project until concerns addressed*, CNBC (July 10, 2019).

[112] Lael Brainard, *Digital Currencies, Stablecoins, and the Evolving Payments Landscape*, FED. RESERVE BOARD, Oct. 16, 2019, https://www.federalreserve.gov/newsevents/speech/brainard20191016a.htm.

[113] *Id.*

[114] *See* Szu Ping Chan, *Facebook's digital currency dealt another blow*, BBC NEWS, Oct. 14, 2019, https://www.bbc.com/news/business-50037223.

[115] Lauren Feiner, *Facebook-led Libra project announces its 21-member council after exodus of top payments companies*, CNBC, Oct. 14, 2019, https://www.cnbc.com/2019/10/14/facebook-forms-its-cryptocurrency-council-after-key-backers-drop-out.html.

it would be beneficial for all if Facebook concentrates on addressing its many existing deficiencies and failures before proceeding any further on the Libra project."[116] Since the hearings, other stakeholders have raised a wide range of policy concerns about this project.[117] Ultimately, under the spotlight of the Committee, Facebook drastically scaled back the timeline for the Libra project, then, created more separation between the entities (staff moved to Switzerland and received "libra" domains for email address instead of "Facebook,") and started hiring anti-money laundering and veteran banking experts to help further build out the project.[118]

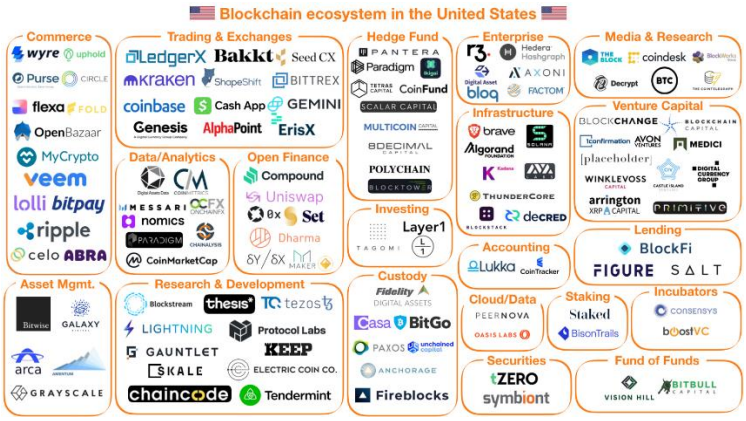
iv. An Unclear Regulatory Framework

Presently, it remains unclear which federal agency is leading the national discussion surrounding cryptocurrencies and digital representations of value. Former Acting Comptroller Brooks, through an interpretive letter, permitted federally charted banks and thrifts to provide custody services for cryptocurrency assets.[119] Considering the revenue generated from custody fees, institutional players are likely to benefit greatly from this interpretation. All the while, Treasury had (and still has) not provided clarity on banks taking custody of cryptocurrency assets and technically, prior to this action by Acting Comptroller Brooks, "banks were never prohibited to custody crypto assets, and there was never any transparency on the risks that might entail."[120] Prior to these actions, in late 2018, to better understand and assess the challenges posed by cryptocurrencies and digital representations of value, the Financial Stability Oversight Council ("FSOC") formed a Working Group on Digital Assets (which includes the OCC), concluding that cryptocurrencies pose risks to financial stability. Examples include how cryptocurrencies interact both directly and indirectly with banking services, financial markets, and financial intermediaries; risks to consumers, investors, and businesses associated with potential losses or instability in market prices; illicit financing risks; risks to national security; cybersecurity and privacy risks; and risks to international monetary and payment system integrity.[121]

---

[116] House Committee on Financial Services, *An Examination of Facebook and Its Impact on the Financial Services and Housing Sectors* (Oct. 23, 2019), https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=404487.
[117] *See Banking on Surveillance: The Libra Black Paper*, Americans for Financial Reform Education Fund and Demand Progress Education Fund, June 25, 2020, https://ourfinancialsecurity.org/2020/06/fact-sheet-banking-on-surveillance-the-libra-black-paper/.
[118] Alisha Roy, *Libra Association Appoints Former HSBC Exec to Move Their Project Forward*, AMBCRYPTO, Oct. 15, 2020, https://eng.ambcrypto.com/libra-association-appoints-former-hsbc-exec-to-move-their-project-forward/.
[119] Office of the Comptroller of the Currency, *Federally Chartered Banks and Thrifts May Provide Custody Services For Crypto Assets* (July 22, 2020), https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-98.html.
[120] Anirudh Tiwari, *US Banks Get Crypto Custody Nod, but Instant Demand Surge Is Unlikely*, COINTELEGRAPH, July 30, 2020.
[121] Dept. of Treasury, *Readout of Financial Stability Oversight Council Meeting* (Dec. 19, 2018), https://home.treasury.gov/system/files/261/December192018_readout.pdf.

US Blockchain Ecosystem Using Traditional Financial Services Terminology[122]



v. Current Oversight

Title X of the Dodd-Frank Act grants the CFPB certain rulemaking, supervisory, and enforcement authorities to implement and enforce certain laws that protect consumers from "unfair, deceptive, or abusive acts and practices."[123] These authorities apply to a broad range of financial industries and products and could apply to cryptocurrency exchanges. Although the CFPB has not exercised regulatory authority regarding the cryptocurrency industry, it is accepting cryptocurrency related complaints and has indicated it would enforce consumer financial laws in appropriate cases. In addition, the Federal Trade Commission ("FTC") has brought several enforcement actions against cryptocurrency promoters and mining operations due to potential violations of the Federal Trade Commission Act.[124] Further, all states have various laws against deceptive acts and practices, and state regulators can use their enforcement authorities against cryptocurrency-related businesses.[125]

While the federal government assesses the licensing of cryptocurrency and digital representations, the states are providing regulatory frameworks for companies to launch. In October 2020, the New York State Department of Financial Services ("NYDFS") granted Paypal (which maintains payment operations for 26 million merchants and is the parent company of Venmo, peer-to-peer electronic payment application) a conditional "Bitlicense,"[126] for a service that enables users to buy, hold, and sell cryptocurrency. In addition, Wyoming has recently approved a special purpose depository institution charter to crypto businesses, Kraken Financial and Avanti Bank & Trust, though these approvals have raised concerns from other stakeholders about the effectiveness of these

[122] Blockchain Association, *About Us*, https://theblockchainassociation.org/ (last visited Dec. 4, 2020).
[123] Consumer Financial Protection Bureau, *Unfair, Deceptive, or Abusive Acts or Practices* (Oct. 2012), https://files.consumerfinance.gov/f/documents/102012_cfpb_unfair-deceptive-abusive-acts-practices-udaaps_procedures.pdf.
[124] Federal Trade Commission, *FTC Sends Refunds to Victims of Deceptive Money-Making Schemes Involving Cryptocurrencies* (Nov. 4, 2020), https://www.ftc.gov/news-events/press-releases/2020/11/ftc-sends-refunds-victims-deceptive-money-making-schemes/
[125] Congressional Research Service, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, Apr. 9, 2020, https://www.crs.gov/Reports/R45427.
[126] New York Department of Financial Services, *Virtual Currency, BitLicense FAQs*, https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_faqs (last accessed at Nov. 6, 2020).

regulatory frameworks.[127] Quick Fixes: The SEC, in consultation with the Fed for monetary policy concerns, should issue clear guidelines on Stablecoins, cryptocurrencies, and other digital representations of value, particularly ones pegged to the US dollar. FSOC should use its authority to designate any new global payment system based on a cryptocurrency or stable coin, such as Libra, that poses a threat to U.S. financial stability as either a systemically important financial institution ("SIFI") or systemically important financial market utilities ("SIFMU") and subject it to enhanced oversight.[128] But even this presents a fundamental problem: How do you regulate a decentralized autonomous organization?

b. Data Privacy & Security

As noted above in Section II, one of the hallmarks of blockchain technology is the asymmetric cryptography that encrypts the information within the blockchain. The technology is inherently secure. The issue, however, is the humans who manage the technology. If governments decide pursuing blockchain digitization, they should establish laws similar to Estonia, making it illegal to unlawfully access information (there are already federal laws to this effect)[129] Governments also need cyber security officers, which conduct security audits and ensure integrity within the infrastructure. With the increase of cyber-attacks on state and local governments,[130] increased cyber-security is a necessary component of government operations.

But most importantly, as government increase its use of technology in government, it ***must*** address ways to improve the general data-privacy protection it offers its citizens from third parties as well as the government. Data, today, is the new oil.[131]

The vast amounts of consumer information and data collected and stored by financial institutions, data aggregators, and cloud providers, among others, is commonly referred to as "big data." The "big" in big data refers to the size, complexity, and newness of any given data set. Big data is integral to modern product development because it can be used to generate insights, support decision making, and enable automation for massive growing data sets. Innovation in this sector has grown, and today, because of the internet and ability to synthesize big data quickly into rapidly applied conclusions, it is easier and less expensive for companies to collect, store, process, and sell consumer data—regardless of the data's size, type, or location.[132] In fact, this development of new products and services is largely driven by data aggregators,[133] partly because of their ability to capitalize on huge

---

[127] *See, e.g.,* Bank Policy Institute, *Beware the Kraken*, https://bpi.com/beware-the-kraken/ (Oct. 21, 2020); *and also*, Bank Policy Institute, *Why a Wyoming Charter Is No Hail Mary for the Anti-Fractional Banking Team*, https://www.bpi.com/why-a-wyoming-charter-is-no-hail-mary-for-the-anti-fractional-banking-team/ (Nov. 9, 2020).

[128] *See, e.g.,* Americans for Financial Reform Education Fund and Demand Progress Education Fund, *Banking on Surveillance: The Libra Black Paper* (June 25, 2020), https://ourfinancialsecurity.org/2020/06/news-release-afr-education-fund-and-demand-progress-ef-reject-recent-changes-to-the-libra-associations-white-paper-as-insufficient/.

[129] 18 U.S. Code § 1030

[130] Todd G. Vare, *State and Local Governments Continue To Be Favorite Targets of Cyberattacks*, NAT'L LAW REV., https://www.natlawreview.com/article/state-and-local-governments-continue-to-be-favorite-targets-cyberattacks (Sept. 19, 2019).

[131] *The world's most valuable resource is no longer oil, but data*, ECONOMIST, May 6, 2017.

[132] Department of Treasury, *A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation*, 22-39 (July 2018), https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf.

[133] *See,* Consumer Financial Protection Bureau, *Request for Information Regarding Consumer Access to Financial Records*, 81 *Federal Register* 83808 (Nov. 22, 2016), https://www.federalregister.gov/documents/2016/11/22/2016-28086/request-for-information-regarding-consumer-access-to-financial-records; *See also*, Consumer Financial Protection Bureau, *Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform The Consumer Protection Principles*

caches of data from diverse sources on the internet, compiling it into a standardized and summarized form for sale to investors and other entities.[134] These practices and others, such as webscraping and permissioned credentialing, are subject to an unclear legal framework, especially when compared to more traditional financial institutions, and raises several questions related to the existing privacy protections.

As the use of consumer data has grown, many countries implemented robust legal frameworks that grant consumers more data-use rights and protections. For example, in 2018, the European Union implemented the General Data Protection Regulation ("GDPR"), which regulates the collection, use, storage, and disclosure of personal data, and any other information through which an individual can be directly or indirectly identified.[135] In the same year, California enacted the California Consumer Privacy Act ("CCPA"), which establishes three consumer rights: (1) a "right to know" the information that businesses have collected or sold about them; (2) a "right to opt out" of the sale of a consumer's information; and (3) a "right to delete" any information a company has collected about the consumer, with some exceptions. In November 2020, California also passed Proposition 24, also known as the Consumer Privacy Rights Act ("CCPA"), to further restrict the sale of data and to create a new enforcement agency.[136]

Before increasing citizens' digital footprints, regulators must increase and modernize data privacy and consumer protections. For example, Congress should pass the "Financial Information Data Modernization Act ("FIDMA"),"[137] a proposal that would set forth minimum data security standards by clarifying "financial data" and "non-financial institutions" under GLBA to protect consumers and provide guidance that contemplates advances in technology for entities interacting with financial data. The CFPB and the FTC should explore ways to clarify enforcement authority under GLBA to better use the law to provide substantive protections for citizens. In all, firms are making decisions that affect the livelihoods of citizens with little oversight. If a government pursue the benefits of blockchain digitization, it should also seek to protect citizens and their data as well. If not, they may establish a digital democracy rooted in surveillance from both the public and private sector.

c. Job Losses Due to Automation

A foreseeable consequence of automation is job loss. If a government adopts blockchain technology, some jobs may become redundant and therefore eradicated. A mitigation strategy, therefore is necessary to contain the economic fallout. For example, a government can pursue workforce development initiatives—especially jobs resistant to forces driving automation. These jobs will find increased demand in our new digital society.

(Oct 18, 2017), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[134] Steven Melendez and Alex Pasternack, *Here are the data brokers quietly buying and selling your personal information*, Fast Company (Mar. 2, 2019); *See also*, Lauren Saunders, *Fintech and Consumer Protection: A Snapshot*, NAT'L CONSUMER LAW CENTER, Mar. 2, 2019, https://www.nclc.org/images/pdf/cons-protection/rpt-fintech-and-consumer-protection-a-snapshot-march2019.pdf.

[135] Congressional Research Services, *Data Protection Law: An Overview* (Mar. 25, 2019), https://crsreports.congress.gov/product/pdf/R/R45631.

[136] Marketplace, *California's new privacy law could create haves and have-nots* (Nov. 6, 2020), https://www.marketplace.org/shows/marketplace-tech/california-proposition-24-consumer-privacy-rights-act-sharing-data-with-companies-inequality/.

[137] H.R.__, Safeguarding Non-bank Consumer Information Act (Discussion Draft), Cong. 116th (2019), https://financialservices.house.gov/uploadedfiles/bills-116pih-fidma.pdf.

Another growing trend in the U.S. is a gap between available jobs and qualified workers. In 2016, for example, nearly 46% of U.S. employers struggled filling jobs, citing alack of available talent.[138] The majority (roughly 53%) of the jobs in the U.S. labor market are middle-skill jobs that require more education than a high school diploma but less than a four-year degree.[139] To address this skill gap and create jobs: a pipeline program should be created, geared towards students who do not desire attending a four-year college but seek gainful employment. The pipeline should begin with students (and potentially an alternative program for high school dropouts and returning citizens pursuing a GED) gaining skills by taking career technical education ("CTE") courses and acquiring certifications.

Once students near the end of the pipeline, they will possess the skills, experience, and connections to work full-time at their site. Or at a partnering entity. In the end: the locality will develop a more skilled workforce and create a pathway to gainful employment for students immediately upon graduation.

VI. Conclusion

For governments, Bitcoin is a distraction. But the technology that underpins it presents opportunities that exceed simple financial transactions. This technology can make government operations more efficient, reducing operating costs, while improving transparency and the satisfaction of citizens in their interactions with government services. Blockchain technology can provide these benefits to governments. Thus, governments should move forward and determine how to digitize their functions with it. In moving forward, a government should establish a commission that analyzes areas—particularly the areas mentioned above—that would benefit the most from blockchain digitization. Then, engage in a cost-benefit analysis of the impact of digitizing the respective function. As far as creating their own blockchain platform, they could issue a request for production, or use a sole source contracting with Guardtime (the company that constructed Estonia's platform) or IBM (a leader in developing blockchain platforms for businesses).

In all, the world is yet to realize the opportunities provided by blockchain technology outside of the financial sector and illicit activities. There is a whole world left untapped—a new digital world. Instead of stifling innovation and taking an antagonistic approach to the technology, governments should embrace it and build on the rails already established to bring the benefits of blockchain technology to their citizens. The internet—the last greatest technological innovation—changed how people, institutions, and governments interact. Blockchain technology is doing the same for people and institutions. It is time for a paradigm shift. It is time for governments to digitize their functions with blockchain technology. But they ***must not*** do so without (1) modernizing and improving citizens' data privacy protections, and (2) investing in workforce development programs like a CTE pipeline program. If the question is what can government do, the answer is your imagination. And blockchain technology will allow governments to tap into their creativity, reforming how governments function.

---

[138] Katie Brown, *Powerful Partners: Business and Community Colleges, How investments in sector partnerships can help our economy thrive*, National Skills Coalition, at 1 (July 2018).
[139] *Id.*