CHAMBER OF DIGITAL COMMERCE

BBA
BOSTON BLOCKCHAIN ASSOCIATION

MASSACHUSETTS LEGISLATOR'S TOOLKIT FOR BLOCKCHAIN TECHNOLOGY

JULY 2021

DIGITALCHAMBER.ORG | BOSTONBLOCKCHAINASSOCIATION.COM

CHAMBER OF DIGITAL COMMERCE

BBA BOSTON BLOCKCHAIN ASSOCIATION

ABOUT THE CHAMBER OF DIGITAL COMMERCE

The Chamber of Digital Commerce is the world's leading trade association representing the digital asset and blockchain industry. Its mission is to promote the acceptance and use of digital assets and blockchain-based technologies. Through education, advocacy and working closely with policymakers, regulatory agencies and industry, our goal is to develop an environment that fosters innovation, jobs and investment.

ABOUT THE BOSTON BLOCKCHAIN ASSOCIATION

The Boston Blockchain Association is a community of innovators, collaborators, and entrepreneurs excited about the promise of blockchain technology. Its mission is to build an ecosystem that supports, educates, promotes, and advances blockchain technology, establishes greater Boston has an international hub for blockchain technology, and supports and connects entrepreneurs with useful resources.

Table of Contents

Foreword

A REFLECTION ON U.S. BLOCKCHAIN POLICY, AND CHARTING A PATH FORWARD FOR MASSACHUSETTS

Three years ago, the Washington, D.C.-based Chamber of Digital Commerce published the **State Legislator's Toolkit for Blockchain Technology**. Its purpose was to educate state lawmakers about this new and important technology, and various policy proposals they could use to encourage its growth.

Since then, interest in blockchain and distributed ledger technologies (DLT) has continued to grow, with some states (notably Wyoming, Texas, and Florida) developing innovative policies and procedures that have resulted in their state laws becoming model legislation for other states. These legislative efforts have also captured the attention of federal lawmakers who have introduced legislation at the national level.

Meanwhile, the technology industry has started to decentralize geographically, sprawling out across the United States from Silicon Valley into new technology hubs, such as Atlanta, Austin, Dallas-Fort Worth, and Boston. This movement has accelerated in light of the COVID-19 pandemic. Accordingly, state legislators should capitalize on this trend by learning about blockchain and DLT and its applications and introducing blockchain-friendly legislation to attract blockchain innovators to their states.

After partnering with the Texas Blockchain Council to publish the Texas Edition of the State Legislator's Toolkit, the Chamber partnered with Media Shower and the Boston Blockchain Association to create a Massachusetts edition of the Toolkit. Consequently, some of the legislative proposals from the original Toolkit have been tailored specifically to the developing blockchain industry in Massachusetts. We have otherwise preserved the Toolkit's content, so legislators may still refer to the policy proposals detailed within the document. (The first edition of the Toolkit is available here.)

The State Legislator's Toolkit is intended to serve as the first step towards adopting supportive policies and legislation, helping legislators identify the various tools available to address the issues blockchain innovators are facing. We encourage lawmakers who want to support growth of this technology and its applications to work with industry in achieving carefully considered public policy.

We look forward to seeing what lies ahead for blockchain innovation across the Commonwealth, and working with leaders in Massachusetts industry and government to help this emerging technology continue to develop and grow.

PURPOSE OF THIS TOOLKIT

Blockchain and Distributed Ledger Technologies (DLT) offer immense possibilities for business, government, and consumers. These include the opportunity for extraordinary economic growth and cost efficiencies. Massachusetts should encourage the growth of these industries to ensure its economy and consumers can benefit from this opportunity for growth.

Much legislative activity has occurred at the state and federal level supporting the benefits of blockchain technology. Some efforts, such as legislation coming from Wyoming, were quite progressive. Others were well-intentioned, but could have benefitted from additional guidance from industry experts. Overall, this level of interest shows that U.S. policymakers are starting to realize the importance of blockchain technology, the commercial potential it brings, and the need to support its responsible growth. Nevertheless, more needs to be done to support this industry. Countries around the world are taking this opportunity to pass legislation and develop regulatory frameworks to encourage blockchain-related companies to relocate to their jurisdictions. The United States and Massachusetts need to foster that interest and energy to ensure that they continue to lead in technological advancement. This Toolkit is a resource for state legislators as they explore ways in which to encourage these industries to grow and bring economic benefits to states.

THE TRANSFORMATIVE POWER OF BLOCKCHAIN

The transformative possibilities of blockchain and its tremendous positive impact for economic advancement have been recognized by policymakers on local, state, and federal levels. Its ability to improve business processes, increase efficiency, and promote transparency in numerous industries is reforming the ways in which companies conduct business. Its quick, secure, and immutable nature is helping retail giants such as Walmart, using IBM technology, trace produce back to its source within seconds, rather than days or weeks.[1] Government agencies within the United States are exploring blockchain technology to streamline procurement. Additionally, as a result of the efforts of Massachusetts-based Voatz, overseas service members have gained the ability to cast secure, tamper-proof votes through blockchain-based voting systems in West Virginia's and other states' elections.[2]

For the avoidance of doubt, this Toolkit does not constitute legal advice.

[1] Michael Corkery and Nathaniel Popper, ***From Farm to Blockchain: Walmart Tracks its Lettuce***, NY TIMES (Sept. 24, 2018), https://www.nytimes.com/2018/09/24/business/walmart-blockchain-lettuce.html.

[2] Hargrave, John, and Evan Karnoupakis. "Chapter 7: Blockchain-Based Voting." Essay. In *Blockchain Success Stories: Case Studies from the Leading Edge of Business*. Sebastopol, CA: O'Reilly Media, Inc., 2020.

ECONOMIC GROWTH & JOB CREATION

Investment in blockchain companies and projects has skyrocketed from millions of dollars in 2014 to hundreds of billions of dollars in 2020. Demand for blockchain technology has created thousands of jobs, with IBM reporting that it increased the number of employees focused on blockchain projects from 400 to 1,500 in the span of a year.[3] TechCrunch estimates that venture capital funds, and other private investors, invested $1.3 billion between January and May of 2018 into "blockchain and blockchain adjacent" early stage companies.[4] Closer to home, Fidelity Digital Assets recently announced plans to increase its headcount by 70% to meet growing institutional demand.[5]

According to the Bureau of Labor Statistics' Occupational Outlook Handbook, "[e]mployment of computer and information technology occupations is projected to grow 13 percent from 2016 to 2026, faster than the average for all occupations. These occupations are projected to add about 557,100 new jobs."[6] The median salary for these jobs in May 2017 was $84,580.[6] Blockchain is in its early stages and its development is often compared to the early days of the Internet. It is an essential piece in the next wave of technological development, often called the "Internet of Value."

Adopting blockchain-friendly policies can turn states into FinTech hubs, such as Arizona and Wyoming. Other states have created task forces and initiatives such as the Illinois Blockchain Initiative and the Illinois Blockchain Task Force; the Delaware Blockchain Initiative; the Wyoming Blockchain Task Force, and an office within Florida's Chief Financial Officer's department to oversee how state securities and insurance laws apply to virtual currencies and initial coin offerings (ICOs). Twenty-nine (29) states have also introduced legislation related to blockchain technology between the 2017 and 2018 legislative sessions.

KEY TAKEAWAYS

- Blockchain and DLT have enormous potential for innovation and economic growth, but this potential will not be realized in Massachusetts or in the United States without the support of policymakers.
- Some states have introduced legislation to encourage and foster the development of blockchain businesses and innovative products, while others have enacted statutes, such as those addressing smart contracts, that may negatively impact the blockchain industry. A cautious, thoughtful approach to legislation is needed to ensure a positive impact.
- Tools such as tax incentives, regulatory sandboxes, government blockchain initiatives, procurement, and direct investment can help foster the development of blockchain businesses and innovative products based on blockchain systems.
- Blockchain and DLT can be used in many ways, including, among others: facilitating trade finance; supply chain management; securities recordkeeping and governance; healthcare management; insurance recordkeeping; energy distribution; digital identity solutions; consumer banking; international payments; facilitating institutional custody; and voting.
- Policymakers can work with innovators to craft responsible statutes and regulations that provide the clarity and flexibility necessary to stimulate blockchain development.

[3] Michael del Castillo, ***Blockchain's Boom Year: Job Market Grows 200%***, COINDESK (Dec. 12, 2017), https://www.coindesk.com/blockchains-big-year-competitive-job-market-grows-200/.
[4] Jason Rowley, ***With at least $1.3 billion invested globally in 2018, VC funding for blockchain blows past 2017 totals***, TECHCRUNCH (May 20, 2018), https://techcrunch.com/2018/05/20/with-at-least-1-3-billion-invested-globally-in-2018-vc-funding-for-blockchain-blows-past-2017-totals/.
[5] https://www.coindesk.com/fidelity-digital-assets-to-increase-headcount-by-70-report
[6] BUREAU OF LABOR STATISTICS, OCCUPATIONAL OUTLOOK HANDBOOK, https://www.bls.gov/ooh/computer-and-information-technology/home.htm (last visited Sept. 27, 2017).
[7] ***Id.***

Impact on Massachusetts

A HISTORY OF INNOVATION IN THE COMMONWEALTH

From its days as a colony, Massachusetts was one of the first technology hubs in the United States by making commitments to education, productivity, global trade, and military-industrial-academic partnerships. In the 1960s through the 1980s, the Massachusetts 128 Belt, which circled the heart of Boston, became a hotbed of high-tech activity. Referred to by *Business Week* as "The Magic Semi-Circle," it nurtured a generation of tech giants like Digital Equipment Corporation, Wang, Honeywell, and Polaroid.[8]

During the Internet boom of the 1990s, as Silicon Valley and New York City became the new hotspots for tech entrepreneurship, the City of Cambridge reinvented itself as a center for life sciences. This was supported by a ten-year, $1 billion government investment.[9] Today, the area around Harvard and the Massachusetts Institute of Technology has the highest concentration of biotech and biopharma companies anywhere in the world. As a result, Massachusetts now leads the nation in biotech.

These two models – the 128 belt of the 1980s, and the Cambridge life sciences hub of today – can serve as frameworks for a new Massachusetts initiative around blockchain.

CURRENT EMERGING TECHNOLOGY INITIATIVES

For the previous decade, the Massachusetts Technology Collaborative (MassTech) has invested public resources into emerging technologies to grow the economy, including projects for broadband expansion, renewable energy, life sciences, big data, robotics, and creating innovation hubs. After the Baker-Polito Administration introduced a new economic development bill at the start of 2020 with a focus on emerging technologies that included blockchain, MassTech initiated a blockchain education program for government leaders across the state. Partnering with Massachusetts-based Media Shower, they delivered a series of education and discovery sessions focusing on how the technology works, its potential impact, and real government use cases throughout the world in order to best meet the needs of the citizens of the Commonwealth.

Today, Massachusetts is the home to emerging blockchain industry leaders like Circle, Algorand, and Voatz. Financial industry leaders like Fidelity and State Street Global Advisors are building out their own blockchain businesses, and the Boston Federal Reserve is leading the research into Central Bank Digital Currency (CBDC), i.e., a blockchain-based digital dollar.

With its educated workforce, history of scientific innovation, and willingness to invest in building an innovation economy, Massachusetts is well-positioned to harness the massive opportunity of blockchain. This resource will show government leaders how to further build a favorable blockchain ecosystem in the Commonwealth.

[8] "Massachusetts Route 128." Wikipedia. Wikimedia Foundation, May 8, 2021. https://en.wikipedia.org/wiki/Massachusetts_Route_128. i

[9] Hargrave, John, and Evan Karnoupakis. "Massachusetts: The Hub of Technology." Essay. In *Blockchain Success Stories: Case Studies from the Leading Edge of Business*, 221–22. Sebastopol, CA: O'Reilly Media, Inc., 2020.

Overview of Legislative Developments

State lawmakers have already begun crafting legislation to spur blockchain-based economic activity or to regulate potentially harmful uses of blockchain.[10]

- **Government Task Forces and Working Groups:** The State of Illinois established the Illinois Blockchain Task Force to explore blockchain use cases applicable to state, county, and municipal governments. Additionally, the state launched a "Blockchain Initiative," a consortium of state and county governments to research and understand blockchain and its potential impact on the function of agencies.[11] In January 2018, the Task Force published its findings in a report.[12] Similar blockchain initiatives have been proposed by several states. Generally, these efforts are a combination of laws enacted to establish legal clarity for blockchain and virtual currency businesses. Additionally, a capstone effort that many states include is a law, similar to Illinois, that mandates an agency or agencies report on potential government applications of blockchain. States such as Delaware, California, and Wyoming have followed suit.[13]

- **Amending Electronic Records and Signatures Legislation to Include Blockchain and Smart Contracts:** In some cases, legislators have attempted to address the enforceability of blockchain and "smart contracts." While clearly an effort to promote the technology, smart contracts are already enforceable under existing federal and state law through application of the Electronic Signatures in Global and National Commerce (ESIGN) Act and state Uniform Electronic Transactions Act (UETA) provisions. Several states that initially introduced legislation attempting to correct existing statutes were later amended or withdrawn, or the legislation lapsed. This is the case for California, New York, Illinois, Florida, and others. Four states, Arizona, Nevada, Tennessee, and Ohio, enacted such legislation, thereby increasing confusion in an already settled area of jurisprudence.[14]

- **Exempting "Utility" Tokens from Securities Regulation:** In cases of securities regulation, both Arizona and Wyoming have defined and exempted "utility" type tokens from state securities laws. These laws provide exemptions for sellers of certain types of coins or tokens on a blockchain network. Essentially, each definition provides that a token or coin is a digital representation of value that can be digitally traded and functions as a medium of exchange, unit of account, or store of value. Each contains limitations to how these types of tokens are offered, as both states require that these tokens not be marketed as an investment.[15]

[10] Wyoming is of particular note here, as the laws it passed serve as a model for the types of lawmaking that can have a tangible impact on the development of state blockchain projects. In 2018, Wyoming passed a series of measures that impact the operation and use of blockchain technology and virtual currencies. These laws were enacted to clarify statutory and regulatory obligations, provide opportunities for innovators to create new products, utilize blockchain in corporate bookkeeping, and allow for novel business structures that could further the potential of blockchain. In so doing, Wyoming established itself as a forward-thinking state with respect to blockchain technology and its potential.

[11] IL H.J.R. 0025 (2017).

[12] ***See*** ILLINOIS BLOCKCHAIN AND DISTRIBUTED LEDGER TASK FORCE, FINAL REPORT TO THE GENERAL ASSEMBLY (Jan. 31, 2018), https://www2.illinois.gov/sites/doit/Strategy/Documents/BlockchainTaskForceFinalReport020518.pdf.

[13] ***Governor Markell Launches Delaware Blockchain Initiative***, DELAWARE OFFICE OF THE GOVERNOR (May 2, 2016), https://www.prnewswire.com/news-releases/governor-markell-launches-delaware-blockchain-initiative-300260672.html; CA A.B. 2658 (2018); WY H.B. 01 (2018).

[14] ***Smart Contracts: Is the Law Ready?,*** CHAMBER OF DIGITAL COMMERCE (Sept. 2018), https://digitalchamber.org/smart-contracts-whitepaper/.

[15] AZ H.B. 2601 (2018); WY H.B. 70 (2018).

- **Regulatory Sandboxes:** In 2018, Arizona became the first state to enact and operate a regulatory sandbox under the purview of Arizona's Office of the Attorney General.[16] In a regulatory sandbox, approved companies can receive exemptions from or modifications to regulatory requirements, such as licensing and capital requirements. Once accepted within the sandbox, these companies can test innovative financial products for a certain period of time and within specific parameters under government oversight. A sandbox proposal was introduced in Illinois, but failed to pass the legislature.[17]

- **Tax Policy:** Tax policy solutions vary from state to state. Wyoming exempted virtual currencies from tax obligations in order to further their use within the state by expressly declaring that they are not considered property subject to state income tax.[18] The interaction of tax law with virtual currencies is not limited to broad exemptions, however. In fact, the Nebraska Legislature put forth a bill that prohibits the taxing of virtual currencies by local governments.[19] The Arizona legislature proposed a bill that would allow citizens to pay their tax bill using virtual currencies.[20] Seminole County, Florida, accepts bitcoin and bitcoin cash for the payment of property taxes, driver's licenses, and other government services.[21] Finally, the State of Ohio now accepts bitcoin payments from businesses to pay certain taxes through a payment portal managed by the Office of the Ohio Treasurer.[22]

- **Money Transmitter Laws:** Many state money transmitter licensing statutes have either been interpreted or amended to cover certain transactions in virtual currency. On the other hand, Wyoming has explicitly exempted virtual currencies from money transmitter laws.[23]
    - In 2016, North Carolina enacted an updated money transmitter licensing law in an effort to clarify the obligations of virtual currency businesses. The legislation included the term "virtual currency" within the broader definition of money transmitting.[24]
    - The California State Legislature proposed a licensing scheme for virtual currency businesses, or businesses that maintain full custody or control of virtual currency in the State of California, on behalf of others. Ultimately, the bill failed to pass.[25]
    - Additionally, New York's Department of Financial Services established a stringent licensing rule (the so-called "BitLicense") for virtual currency-based businesses, in addition to the state money transmitter license also required in New York.[26] In the first three years after the rule's inception in 2015, only 10 companies received a BitLicense.[27] As of June 2021, 22 BitLicenses have now been issued.

[16] AZ H.B. 2434 (2018).
[17] IL S.B. 3133 (2018).
[18] WY S.F. 111 (2018); ***cf*** INTERNAL REVENUE SERV., NOTICE 2014-21 (2014) (stating that virtual currency is taxed as property).
[19] NE L.B. 694 (2018).
[20] AZ S.B. 1091 (2018).
[21] Joel M. Greenberg, ***Joel Greenberg Accepts Bitcoin and Bitcoin Cash for Payments through BitPay***, SEMINOLE COUNTY TAX COLLECTOR (May 14, 2018), http://www.seminolecounty.tax/forms/bitcoin-announcement.pdf.
[22] ***Ohio Becomes First State in Nation to Accept Taxes via Cryptocurrency***, OFFICE OF THE OHIO TREASURER (Nov. 26, 2018), http://www.tos.ohio.gov/News/15207.
[23] WY H.B. 19 (2018).
[24] NC H.B. 289 (2016).
[25] CA A.B. 1123 (2017).
[26] 23 NYCCR Part 200, Virtual Currencies (2015).
[27] Number of Virtual Currency Companies Regulated by the New York Department of Financial Services, DEP'T OF FIN. SERV., https://myportal.dfs.ny.gov/web/guest-applications/who-we-supervise (select "Virtual Currency" option in the "Type of Institution" field) (last visited Nov. 27, 2018).

- Corporate Recordkeeping and Business Organizations: States such as Delaware and Wyoming have expressly authorized the use of blockchain for corporate recordkeeping. While this use case may pave the way for novel business entities in the future, it will likely have a meaningful impact on corporate recordkeeping today. Permanence of information can strengthen a shareholder's ability to act on their rights and enable more efficient regulatory enforcement by state and federal securities regulators.

  In addition to allowing the use of blockchain technology for corporate recordkeeping, Wyoming has joined Delaware to provide for the establishment of Series LLCs. Series LLCs are business organizations that compartmentalize liability among different entities, referred to as "series," contained within the LLC; each "series" within the LLC is independently liable. Delaware and Wyoming have enabled the potential to combine the use of Series LLCs with a network such as Ethereum, opening the door for decentralized business organizations and other novel applications of blockchain. Vermont has also passed legislation allowing companies that use blockchain to facilitate their businesses to register as blockchain-based LLCs, which allow the use of blockchain technology for corporate governance and records maintenance.[28]

[28] VT S. 269 (2018).

UNIVERSAL PRINCIPLES FOR LEGISLATORS

Lawmakers can encourage blockchain and DLT innovation right now. These efforts are summarized below. For further discussion on these, and other points of action, please reach out to the Chamber of Digital Commerce at policy@digitalchamber.org,

- **Any Regulation Should be Based on the Function Performed, Not the Technology**
  - **Virtual currency and blockchain statutes and regulations should emphasize function.** New rules and statutes should not be based on the type of technology itself but, rather, the use or activity involving the technology.

- **Prevent Regulatory Patchwork**
  - **State and federal government entities should cooperate in their policymaking efforts to prevent a patchwork of regulations and statutes related to similar functions.** The most enduring example of a 50 state (and territories) patchwork of regulations occurs with state money transmitter laws. Companies involved in virtual currency activities are multi-jurisdictional by virtue of the fact that they operate on the internet. The costs associated with an inconsistent and varied multi-state licensure system — both in application process and in ongoing maintenance and examinations — substantially undermines the efficiencies blockchain provides. This complexity is furthered by the lack of cooperation between federal and state policymakers. In order for the United States to obtain an effective competitive edge in the blockchain industry, it is crucial that a standard framework across federal and state governments be implemented that clearly defines the obligations, and various legal regimes, that apply to virtual currency and blockchain-based companies.

LEGISLATIVE PROPOSALS

- **Create an Office Dedicated to Promoting Blockchain Technology**
  - **To better develop blockchain-based economic development and activity, policymakers should establish a state office or agency, or expand upon an already existing office, to promote the development of blockchain technology within the state.** As noted above, a cornerstone of any blockchain initiative requires the exploration and understanding of blockchain and DLT. **These technologies are often complex and must be properly understood and tested before implementation.** To further this effort, states should establish an office or agency dedicated to the promotion and development of blockchain technology within the state. Not only would this office work to determine applications of blockchain that could cut costs for taxpayers, this office may provide a gateway for entrepreneurs to best understand the laws of their state surrounding blockchain and virtual currencies.[29] Further, this office could be a champion for blockchain development and work to draw companies and innovators to the state. This office – which may be housed in the Office of the Governor, a state economic development corporation, or other government entity whose purpose consists of supporting innovation and growing the economy – may also oversee an interagency task force consisting of agency officials and industry members to research and develop proposals to implement DLT solutions within the state. The office would require funding to support blockchain initiatives.

- **Allow Businesses to Use Blockchain for Corporate Record Management and Amend Securities Laws to Exempt "Utility" Tokens**
  - **States should allow for privately-traded businesses to maintain corporate records, and memorialize ownership, through the use of blockchain technology.** Doing so opens a gateway for companies to develop new methods of organization, provides shareholders with better means to act on their rights within a corporation, and streamlines the efficiency of paying out distributions or dividends. The traditional corporate processes can be burdensome on the overall operations of a business. By eliminating the requirement for these processes, businesses and corporations can devote their time to economic activity.
  - **State "blue sky" laws should exempt "utility" tokens designed for consumptive use.** The issuance of securities by publicly traded companies are broadly regulated by the federal government, and these regulations are effective in outlining the obligations of issuers and other parties to securities transactions. However, states also have individual securities laws, commonly referred to as "blue sky laws." States should ensure that these laws exempt digital tokens that are intended to be used for consumptive purposes, rather than as investments. This effort will provide businesses with the necessary clarity to act without the concern of violating state securities laws.

[29] This includes working with other offices within the state to gather resources that may benefit blockchain companies (***e.g.***, working with the state's business development agency to educate businesses on tax credits for which they may qualify, or creating materials on business planning that include information about Opportunity Zone tax incentives). ***See Treasury, IRS Issue Proposed Regulations on New Opportunity Zone Tax Incentive,*** INTERNAL REVENUE SERV. (Oct. 19, 2018), https://www.irs.gov/newsroom/treasury-irs-issue-proposed-regulations-on-new-opportunity-zone-tax-incentive.

- **Clarify Application of Money Transmitter Laws**
  - **Policymakers should make clear whether virtual currencies are encompassed within money transmitter laws, and, if so, enforce these laws in a manner no more burdensome than traditional money transmitters.** Money transmission laws relate to the acceptance of money on behalf of another party for transmission to a third party or location. States differ on their views of virtual currencies as they apply to money transmission laws and whether or not this type of business encompasses transmissions involving virtual currencies. States are taking various approaches to this issue, and these approaches tend to fall somewhere along a spectrum of regulation. The goal of any legislation or regulation should be to (1) clarify the regulatory obligations for innovators to ensure market integrity and consumer protection, and (2) ensure that these obligations are not so burdensome as to stifle innovation. If a state does encompass virtual currencies under a type of money transmitter law, it should, at a minimum, track (and not duplicate) the rules and requirements of federal law.
  - **Virtual currencies should be included within the allowable permissible investments for money transmitters and related businesses.** In many states, the ability to operate in a state is limited due to the state's definition of permissible investments. Permissible investments are those investments that money transmitters and related businesses must hold for the benefit of the institution's outstanding obligations to customers. Essentially, this is intended to ensure that the institution has sufficient liquidity to meet outstanding obligations. Without allowing virtual currencies to act as a form of permissible investment, money transmitters and other businesses that take in substantial amounts of customer funds in the form of virtual currency, such as token trading platforms (also known as "virtual currency exchanges"), create substantial economic inefficiencies to meet such obligations by holding a duplicative amount of cash. This can make the business operations of a virtual currency exchanger too expensive to operate effectively within that state.

LEGISLATIVE CONCEPTS

- **Facilitate Regulatory Sandboxes**
  - **Policymakers should implement regulatory sandboxes to allow for the testing of innovative financial technologies, such as blockchain and DLT, in a controlled environment.** Innovators are using blockchain technologies to create promising new systems for finance and consumer use. In fact, these systems and products, known as Fintech, are now being used by 50% of consumers globally.[30] However, traditional firms can be resistant to the risk of new innovations, and early-stage companies may lack the funds to participate in a market given the numerous compliance obligations. Regulatory sandboxes allow for a temporary modification of regulations and licensing requirements to allow businesses to test approved products with consumers in the market. This regulatory tool is helpful in that it allows for the testing of financial products, within certain limitations, to protect consumers. It also provides regulators a way to better learn about and understand these technological innovations, thus enabling more effective and targeted regulation and oversight.
  - Multiple foreign nations have created regulatory sandboxes for Fintech companies and are encouraging U.S. businesses to relocate overseas.[31] This has encouraged many innovative technology companies to build and test their products in foreign jurisdictions, causing the United States to miss out on these potential opportunities for economic growth.[32]

- **Create a Tax Policy that Promotes Innovation**
  - **Lawmakers should limit and standardize virtual currency tax obligations.** Clarity is important for tax purposes; this is particularly true due to how virtual currencies work and for what they are meant to be used. To be effective as a method of exchange in e-commerce, virtual currencies cannot create new tax liabilities at each transaction point. This is currently the case under federal tax guidance, which treats virtual currency as property.[33] Not only is this inefficient in e-commerce applications, it hinders the use of virtual currencies as a payment method. A virtual currency cannot be effectively leveraged in situations where the tax liability must be calculated each time it is used to purchase a cup of coffee.
  - **States should allow taxes and fees to be paid to government agencies in virtual currency to facilitate their use as a payment method.** Such authorization would further promote use of the technology in commercial transactions. This ability has been implemented in Seminole County, Florida, which now accepts bitcoin and bitcoin cash for the payment of property taxes, driver's licenses, and other government services.[34] Further, Ohio has launched a payment portal for businesses to pay certain tax obligations through bitcoin.[35]
  - **Tax policy should be used to promote blockchain innovation.** Governments should encourage innovation through tax credits and write-offs. Costs associated with developing the technology, promoting its use, and improving it once it is distributed into the larger public should be considered business expense write-offs. Traditional write-off programs may be very beneficial to the creation of these projects or companies that wish to leverage blockchain technology. Additionally, tax credits can be effective at encouraging current businesses to expand their research and development and conduct business in that state.

- **Enforceability of Smart Contracts**
  - **States should not attempt to amend their electronic transactions laws, which already provide legal efficacy to smart contracts.** Existing U.S. law, without further revision, supports the formation and enforceability of smart contracts. The ESIGN Act and the UETA already provide sufficient legal basis for smart contracts executing the terms of a legal contract. Additional state legislation, inconsistently drafted, will confuse the marketplace, potentially lead to litigation, and hinder innovation.
  - **States should authorize remote notary services.** Although electronic signatures and records stored on a blockchain are enforceable under the ESIGN Act and UETA, obstacles currently exist for remote notary services. To date, only nine states have authorized notaries to perform remote notary services, where notaries observe signers through audio/visual technology rather than in-person.[36]

- **Promote Insurance Innovation**
  - **States should encourage use of blockchain in the insurance industry through claims management, record keeping, customer identification, and underwriting.** States should be proactive in clearing a path for innovation in the insurance industry by enacting policies that promote the development of blockchain projects to facilitate the technology's adoption. State regulators should confirm that they welcome the use of new technology to improve this industry and the services received by its customers. For example, regulators should seek out opportunities to learn from industry the potential uses for and benefits to this industry through blockchain. Support, and early engagement, from legislators and regulators for the adoption of blockchain in the insurance industry is essential to enabling adoption in this regulated marketplace.

- **Adopt Blockchain in Healthcare**
  - **State policymakers should ensure that laws and regulations do not inhibit the use of blockchain within the healthcare industry.** A variety of regulatory and legal requirements are imposed on entities within the healthcare system. For an early-stage business, or businesses exploring innovative technologies and their potential benefits in healthcare, these laws can be uniquely burdensome and prevent further development in the healthcare field. Policymakers should introduce legislation to pilot the use of blockchain technology for prescription supply chain monitoring, healthcare provider licensing through digital identity-based systems, and electronic health records and management. This form of cooperation may benefit the healthcare system, reducing inefficiencies and cost and increase understanding of the additional ways in which blockchain can be used in the healthcare industry.

[30] ***World FinTech Report 2017***, CAPGEMINI, https://www.capgemini.com/wp-content/uploads/2017/07/half_of_banking_customers_globally_now_using_fintech_firms.pdf (last visited Oct. 23, 2018).
[31] ***See, e.g., Global Regulatory Sandbox Review***, CHAMBER OF DIGITAL COMMERCE (Nov. 21, 2017), https://digitalchamber.org/wp-content/uploads/2017/11/Regulatory-Sandbox-Review_Nov-21-2017_2.pdf.
[32] The U.S. Department of the Treasury recommends the implementation of regulatory sandboxes in the United States. U.S. DEP'T OF TREASURY, ***A Financial System That Creates Economic Opportunities – Nonbank Financials, Fintech, and Innovation*** (2018).
[33] INTERNAL REVENUE SERV., NOTICE 2014-21 (2014).
[34] Joel M. Greenberg, ***Joel Greenberg Accepts Bitcoin and Bitcoin Cash for Payments through BitPay,*** SEMINOLE COUNTY TAX COLLECTOR (May 14, 2018), http://www.seminolecounty.tax/forms/bitcoin-announcement.pdf.
[35] ***Ohio Becomes First State in Nation to Accept Taxes via Cryptocurrency***, OFFICE OF THE OHIO TREASURER (Nov. 26, 2018), http://www.tos.ohio.gov/News/15207.
[36] Virginia, Montana, Michigan, Minnesota, Indiana, Tennessee, Vermont, Nevada, and Texas. Margo H.K. Tank, David Whitaker, and Andrew Grant, ***Remote Notarization: Authentication Requirements, by US State***, DLA PIPER (Sep. 14, 2018), https://www.dlapiper.com/en/us/insights/publications/2018/09/esignature-and-epayment-news-and-trends-sept-2018/remote-notarization-authentication-requirements-by-us-state/.

- **Enable Blockchain-based Digital Identity**
  - **Lawmakers should explore blockchain technology as a solution to the provision of identity services.** One of the principal roles of government is the establishment of identity through driver's licenses, birth certificates, social security numbers, passports, etc., in the form of paper certificates, plastic ID cards, and digital records. One of blockchain's most innovative, and potentially impactful, use cases is directly tied to the establishment of digital identity. Lawmakers and state agencies should begin exploring, and potentially implementing, blockchain-based identification systems to issue verifiable credentials that can be used universally. Lawmakers and state agencies should focus on interoperable solutions that leverage independently verifiable attestations, rather than using private chains and isolated systems, and comply with identity standards like Verifiable Credentials and Decentralized IDs (DIDs) (both standard candidates as part of the World Wide Web Consortium, also known as W3C) . These programs can occur through state Departments of Motor Vehicles, for example. These systems can streamline government services and reduce the costs to taxpayers.
  - **Use blockchain technology to facilitate voting in elections and track votes cast in a secure and transparent manner.** Due to the secure and immutable nature of blockchain technology, votes may be cast in place of mail-in-ballots which may be lost and must be processed manually by county clerks. Votes may be tracked through a blockchain to provide for a quicker, tamper-proof way of counting ballots and recording votes. One example is the state of West Virginia, which piloted the use of blockchain technology for overseas service members. Voting involves not only tracking votes cast on a blockchain, but the use of digital identity solutions to interface with the platform. When implementing blockchain-based voting solutions, lawmakers and state agencies should consider a secure identity verification in which the initial phase for proving identity occurs. The identity verification and ballot tracking solutions should not reveal a voter's identity to third parties, but be able to establish whether the voter was eligible to vote during the time of voting, based on the local criteria, and what the vote counts toward — candidate, proposition, etc.

- **Blockchain for Bond Issuance**
  - **States should consider issuing municipal bonds using blockchain.** Among the benefits of blockchain technology is the ability to reduce the number of intermediaries involved in a transaction. Bonds that are issued on a blockchain, for example, require less intermediaries to participate in the transaction leading to lower transaction costs. On a global level, the World Bank has launched a bond using blockchain technology;[37] while on a municipal level, the city of Berkeley, California has created a blockchain-based bond to publicly finance community projects. The project includes "micro-bond" offerings, allowing bonds to be issued in the range of $10 to $25.[38]

[37] ***World Bank Prices First Global Blockchain Bond, Raising A$110 Million***, THE WORLD BANK (Aug. 23, 2018), https://www.worldbank.org/en/news/press-release/2018/08/23/world-bank-prices-first-global-blockchain-bond-raising-a110-million.
[38] Helen Partz, ***Berkeley City Council Moves Ahead With Pilot Program For Issuing City Bonds On Blockchain***, COINTELEGRAPH (May 3, 2018), https://cointelegraph.com/news/berkeley-city-council-moves-ahead-with-pilot-program-for-issuing-city-bonds-on-blockchain.

THE CURRENT MASSACHUSETTS LEGAL ENVIRONMENT

Money Transmitter Laws

Massachusetts' money transmitter statue does not apply to domestic money transmission services. According to selected opinion 18-003 released in June 2018, a crypto exchange did not need to be licensed as a foreign transmittal agency.[39]

Other Relevant Recent Opinions from the Division of Banks

Massachusetts General Laws Chapter 169 requires that all people who engage in or are financially responsible interested in the business of receiving deposits for the purpose of transmitting the same or the equivalents thereof to foreign countries obtain a foreign transmittal agency license from the division.[40] The division has interpreted this to apply to cryptocurrencies in the following ways:

- **Opinion 20-004 Licensing requirements for interactive games using distributed ledger technology:** Mythical (the creator of the interactive gaming software) is not required to be a licensed foreign transmittal agency by the Division. The purpose of this Secondary Marketplace is not to transfer funds to another country, but rather to create a forum for players of the Game to trade assets for in-game play. It is the position of the Division that the virtual currency and virtual assets developed by Mythical for in-game use have no monetary value. Therefore, Mythical is not a foreign transmittal agency under Massachusetts General Laws chapter 169.[41]
- **Opinion 020-002 Licensing requirement for virtual currency services through a kiosk or website: ax policy should be used to promote blockchain innovation.** In a BOA website transaction, BOA receives U.S. dollars or funds from the user. The purpose is not for transmission to a foreign country but rather the purchase of bitcoin from BOA by the user. BOA will be selling its own bitcoin to the user-buyer on the BOA website and does not take possession of the user-buyer's funds for later transmission. See Division of Banks Selected Opinion 19-008. All bitcoin transactions with users will take place entirely in Massachusetts. Based on the facts presented, BOA is not required to be licensed as a foreign transmittal agency by the Division.[42]
- **Opinion 18-002 Do business activities involving the sale of cryptocurrency, as described require licensing from the division of banks?** In the transaction described, CreditCoin receives the buyer's funds not for the purpose of transmission to a foreign country, but rather solely for the purpose of selling such cryptocurrency to the buyer. CreditCoin will be selling cryptocurrency to the buyer from its own stock, separately obtained from its cryptocurrency supplier pursuant to a distinct credit agreement. CreditCoin does not take possession of the buyer's funds or purchased cryptocurrency for later transmission. As described by CreditCoin, there is no relationship between the buyer and CreditCoin's cryptocurrency supplier. Accordingly, based on the facts presented, CreditCoin is not required to be licensed as a foreign transmittal agency by the Division.[43]

[39] MA D.O.B. Op. 003 (2018) https://www.mass.gov/decision/opinion-18-003
[40] MA D.O.B. Op. 002 (2020) https://www.mass.gov/opinion/opinion-020-002
[41] MA D.O.B. Op. 004 (2020) https://www.mass.gov/opinion/opinion-20-004
[42] MA D.O.B. Op. 002 (2020) https://www.mass.gov/opinion/opinion-020-002
[43] MA D.O.B. Op. 002 (2018) https://www.mass.gov/opinion/opinion-18-002

BLOCKCHAIN LEGISLATION IN MASSACHUSETTS

The Massachusetts Legislature has the following legislation in process (as of the time of this writing):

- **Senate Bill 200** was introduced in January of 2019 by Massachusetts State Senators Cynthia Stone Creem and Eric P. Lesser and State Representative Tommy Vitolo for legislation relative to blockchain and cryptocurrencies, specifically, the establishment of a 15-member commission to investigate/study these emerging technologies. After being referred to the Committee on Economic Development and Emerging Technologies, in August of 2020, it was last referred to the Joint Committee on the Rules of the Two Branches, acting concurrently.

- In May of 2019, Massachusetts State Representative Andres X. Vargas and State Senator Harriette L. Chandler jointly presented **House Bill 3763** to establish a 7-member committee to implement a pilot program for the investigation to provide convenient voting for military personnel, their families, and civilians stationed or working abroad.[44] Specifically, smart phone technology combined with a secure and immutable storage of returned ballots will improve voter engagement, convenience, and security. It was referred to the Committee on Election Laws. In February of 2020, it was accompanied by a study order H4403.

- In March 2021, Massachusetts State Representative Kate Lipper-Garabedian introduced **House Bill 126** to establish a 20-member special commission on blockchain and cryptocurrency in Massachusetts with the goal of positioning the Commonwealth to be a leader in this new technology. Specifically, the group will develop a master plan for fostering the appropriate expansion of blockchain technology and the cryptocurrency industry in the Commonwealth.[45] At the time of publication, this bill has been assigned to the Joint Commission on Advanced Information, Technology, Internet, and Cybersecurity.

[44] MA H.B. 3763 (2019) https://malegislature.gov/Bills/191/H3763
[45] MA H.B. 126 (2021) https://malegislature.gov/Bills/192/HD2065

RECOMMENDATIONS FOR MASSACHUSETTS

We recommend that Massachusetts legislators focus on the following five initiatives:

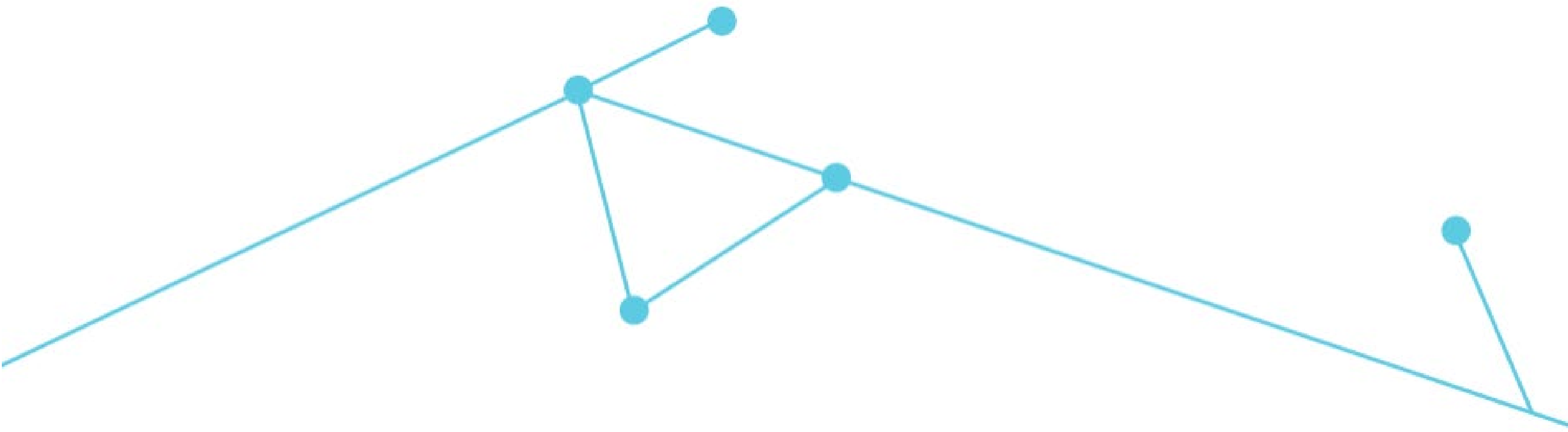
1. Establish a State Blockchain Working Group. Building upon the vision set forth in SB 200 and HB 126, establish a state blockchain working group of 10 to 20 members with a diversity of backgrounds including academia, government, law, cryptocurrency, business/entrepreneurship, and under-represented communities, to build out the blockchain-focused ecosystems across the Commonwealth so that Massachusetts can become a leader in this emerging technology.

2. Create a legal/regulatory "sandbox" for blockchain projects. Encourage investment, entrepreneurship, and innovation in the blockchain and cryptocurrency industries within a clearly-defined "safe harbor" framework. This framework will allow blockchain projects to be developed for a limited time (say, three years) without falling under securities regulation. At the end of this safe harbor period, projects will be evaluated and appropriate regulations applied,

3. Clearly define virtual currencies. Following Texas' lead, modify the state's Uniform Commercial Code defining virtual currency (see Texas HB 4474) as digital representations of value that function as a medium of exchange, unit of account, and/or store of value, often secured using blockchain technology.

4. Standardize tax obligations. Currently digital currencies are taxed as capital gains at every transaction, making them impractical to use for everyday purchases. We recommend removing these tax obligations, allowing digital currencies to function more like traditional currencies when they are used in that manner, yet still functioning like securities when intended for investment purposes.

5. Develop a blockchain "pilot project." Invest in a Massachusetts-based blockchain project that will benefit the Commonwealth. Potential blockchain projects include municipal bonds to raise funds while improving civic engagement, an identity management system to provide citizens access to government services, an innovation center hub to support blockchain development, a crypto-savings solution for the unbanked and underbanked, and improving the security and anonymity of blockchain-based voting.



In Depth: What is Blockchain Technology?

OVERVIEW

The following section provides background information for legislators who want to understand more about how blockchain technology works.

A blockchain is a specific type of distributed ledger technology that organizes data into blocks that are "chained" together chronologically by a cryptographic hash function and confirmed by a consensus mechanism. It serves as the foundational protocol upon which many applications can be built, much like how the internet underpins multiple applications such as e-mail, e-commerce, and business processes.

What Are Some of the Characteristics of Blockchain Technology?

- **Distributed**
  - Data is shared across nodes rather than being maintained by a central administrator. Each node maintains a copy of the blockchain, making it resilient to failures and attacks.
- **Consensus Algorithm**
  - A consensus algorithm consists of a set of rules by which a distributed network reaches agreement to verify a transaction's occurrence and ensures that that all nodes have an identical copy of the ledger of transactions.
- **Cryptography**
  - Blockchains use complex mathematical algorithms to secure and validate transactions on the network.
- **Immutability and Record Keeping**
  - Once a transaction occurs and is recorded on the blockchain, data may be added but not modified or removed.
- **Bitcoin is the first iteration of blockchain technology.** Bitcoin provided a solution to the operative problems of transferring value in a digital environment – specifically, how to ensure that digital value is not spent twice. Although the solution was beneficial to the promulgation of virtual currencies, its underlying value is in its potential to create transactional efficiencies in transferring value and recording transactions in a vast array of industries. This is due, in part, to the security of information stored on a blockchain.

- **Blockchain creates the opportunity for frictionless, permanent transfers of information or value without an intermediary.** Blockchain technology makes information immutable, as many computers on the network share the information such that a breach of one computer does not equate to a breach of the network. This is because information stored on a blockchain can only be changed with the approval of the network, otherwise known as a consensus mechanism. This gives data stored on a blockchain more permanence and has the added benefit of allowing users the ability to transact without an intermediary.

- **Blockchain is already receiving attention from investors and increasing job numbers.** TechCrunch estimates that venture capital funds, and other private investors, invested $1.3 billion between January and May of 2018 into "blockchain and blockchain adjacent" early-stage companies.[46] Companies in a variety of industries have announced plans to either create new products or services based on blockchain or to incorporate blockchain into their traditional product offerings. The growth in interest has also translated into job creation. A consortium of businesses focused on creating blockchain projects grew its staff from 30 in the early part of 2016, to 150 by the end of 2017. Additionally, IBM reported that it increased the number of employees focused on blockchain projects from 400 to 1,500 in the span of a year.[47]

TYPES OF CONSENSUS MECHANISMS

The method in which computers (referred to as "nodes" on a blockchain network) come to agreement on the validity of changes to the blockchain is known as the consensus mechanism. There are many types of consensus mechanisms, but this paper only details the processes of two: proof-of-work and proof-of-stake. The consensus mechanism outlines the rules in which nodes can work to "mine" (earn virtual currency in exchange for verifying transactions through complex mathematic algorithms) transactions and receive mining rewards. Thus, the mining rewards provide incentive for participants in a blockchain network to maintain the consistency and integrity of that network, thereby eliminating the need for any one participant to trust any of the others. It is important to note that some consensus mechanisms, such as those used in permissioned blockchains, are not incentive-based.

- **Proof-of-Work**
  - Nodes compete to "mine" virtual currency by solving complex mathematical puzzles in the Bitcoin software. After one node solves the puzzle to "unlock" and earn the virtual currency, other nodes on the network confirm whether the puzzle has been solved and the record of this transaction results in a new block being added to the blockchain. This solving and verifying process is known as proof-of-work.
  - Currently, the two largest blockchain networks, Bitcoin and Ethereum, use proof-of-work consensus mechanisms. However, the community of Ethereum's programmers are planning to switch from proof-of-work to proof-of-stake in order to increase scalability.

[46] Jason Rowley, ***With at least $1.3 billion invested globally in 2018, VC funding for blockchain blows past 2017 totals***, TECHCRUNCH (May 20, 2018), https://techcrunch.com/2018/05/20/with-at-least-1-3-billion-invested-globally-in-2018-vc-funding-for-blockchain-blows-past-2017-totals/.
[47] Michael del Castillo, ***Blockchain's Boom Year: Job Market Grows 200%***, COINDESK (Dec. 12, 2017), https://www.coindesk.com/blockchains-big-year-competitive-job-market-grows-200/.

- **Proof-of-Stake**
  - Proof-of-stake limits the number of computers working on each block, solving the energy consumption problems posed by proof-of-work. Instead of every computer simultaneously competing to win the mining reward, proof-of-stake provides the opportunity to solve a block based on the amount of digital tokens a user has. Randomly selecting "staked" users to provide the next valid block ensures they have incentives to maintain the network to preserve the value of their holdings
  - Additionally, in some proof-of-stake models, the user has to lock a portion of their coins or tokens to the network in order to be eligible to provide the block's solution. After this user has proposed a block, other users on the network are given the opportunity to validate the solution. If the validating users determine that the solution is invalid, the proposing user may lose some of the digital tokens they have staked, giving even greater incentives for participants to properly follow the rules for adding new blocks.

TYPES OF BLOCKCHAINS

PUBLIC BLOCKCHAINS[48]

Public blockchains are typically open to anyone in the world to view and participate. Transactions have to be viewable by the public at large in order to be verified; however, no identifying information is released outside of the public address associated to each person. This provides a level of "pseudo-anonymity" where transactions can be traced and linked to one another, but not directly connected to the personal identity of one individual person.[49]

- **Benefits**
  - The entry costs to new users are minimal. Because no participant or group of participants has exclusive control over a public blockchain, it is almost totally disintermediated, thus significantly increasing speed of transactions and reducing costs. Public blockchains can be easily spread across industries and geographies because they are open to all participants. Instantaneous access to the same shared ledger can make processes more efficient.

- **Limitations**
  - Public blockchains tend to be relatively slow due to the sheer magnitude of the data processing that has to take place in order to validate a transaction and incorporate it into a block. A blockchain network must store every transaction that has ever taken place within the network, creating data storage demands. Additionally, obligations of the participants and liabilities of participants and actors on the network are unclear. Finally, data privacy may be limited.

[48] ***Applying Blockchain In Securitization: Opportunities For Reinvention***, CHAMBER OF DIGITAL COMMERCE (Feb. 2017), 4-5, https://digitalchamber.org/assets/sfig-blockchain-report.pdf.
[49] Using the public transactions on the Bitcoin blockchain, in tandem with other information associated with certain public addresses, law enforcement has been able to track criminal activity and associated suspects. Amos Zeeborg, ***Will Cryptocurrencies Spy on Us or Set Us Free?,*** NOVANEXT (Feb. 15, 2018), http://www.pbs.org/wgbh/nova/next/tech/cryptocurrency-privacy/.

- **Current Uses**
  - Public systems can be distributed across a much wider variety of network participants than permissioned blockchains. Because of this, public systems are more beneficial for transactions involving parties across geographies and who may not know or trust each other. International remittances are a good example of the current benefits of public systems, as they allow cross-border payments without the large fees of multiple parties to the transaction, potentially situated in multiple locations. The Bitcoin blockchain is an example of a public system as transactions are recorded on the blockchain and can be viewed by anyone who wishes to examine the digital ledger.

How Does the Bitcoin Protocol Work?

The most popular example of a public blockchain is the Bitcoin blockchain. Using Bitcoin as a guide, this is how a public blockchain can be used:[50]

- **Payment:** Using a hosted digital wallet, with an interface similar to PayPal or Venmo, a user can send and receive bitcoin. To submit a transaction, the sending user inputs the receiving user's address, similar to a public account number, and the number of bitcoin they wish to send. The sending user confirms this information and "signs" it with a private account number, essentially a private key or password. The transaction is then broadcast to a network of interconnected computers for processing and confirming.
- **Processing:** Transactions are processed through the network's chosen consensus mechanism, which is the method that the network uses to come to an agreement on transactions. Bitcoin's consensus mechanism is based on "proof-of-work" – a method by which the participants solve complex math problems to confirm transactions. Each computer running Bitcoin software, and thereby connected to the distributed Bitcoin network, receives transaction information each time users consummate a transaction. The network then works to verify this information and package this transaction data into a "block" together with other transactions. The block is then added and secured cryptographically to the Bitcoin network distributed ledger, or "blockchain."
- **Reward for Effort:** The individual computers on the network are given a "mining reward" for their efforts. To obtain this reward, each computer competes to verify and package the transactions within certain cryptographic parameters to "solve" a block. The winner of this process receives a predetermined amount of newly minted bitcoin each time a block is created.
- **Completion:** The transaction is complete when it becomes incorporated into a block. At this point, the sending user's balance of bitcoin is lowered; the receiving user's balance is increased; and the network represents that all of this is correct. In a blockchain consensus mechanism, each valid block is inextricably linked to one another using cryptography. This creates a chain of information that cannot be deleted or changed.

[50] The units of measurement that blockchain technology tracks through its operation can serve different purposes, the difference in use can be summed up in the terms that describe these units: coins and tokens. The term "coin" is used to describe a unit that acts as a medium of exchange or source of value and can be used as currency. Whereas the term "token" is used to denote the representation of something else, such as property or a right to use a service. This difference is important to understand when viewing the larger ecosystem of blockchain system use cases. For further reading, ***see*** Bonpay, ***What is the Difference Between Coins and Tokens***, MEDIUM (Mar. 13, 2018), https://medium.com/@bonpay/what-is-the-difference-between-coins-and-tokens-6cedff311c31.

PERMISSIONED BLOCKCHAINS[51]

Permissioned blockchains limit participation on the network, either to a single administrator or a consortium of participants (vetting parties, the level of participation, and the criteria for validating and recording information and transactions) or the types of transactions a participant in the network can execute. Permissioned blockchains generally limit authorization to perform certain functions, or access different types of information, to a select group of persons.

- **Benefits**
  - Permissioned blockchains allow participants to limit the access and authority of other users on the network. They typically require some method of authentication before access or modification to the system is granted. Transactions are much quicker on permissioned blockchains, as a lower level of trust is necessary for validation. Additionally, permissioned blockchains can establish a level of privacy that public blockchains cannot. This is particularly beneficial to parties that wish to record and transmit sensitive data, such as healthcare or financial information.
- **Limitations**
  - The original objective of a blockchain is to establish disintermediated trust across a large network of participants. In a permissioned blockchain, mathematical trust using a distributed group of participants must be replaced by actual trust and authentication protocols as the number of participants shrink.
- **Current Uses**
  - Permissioned blockchains are most valuable for institutional or regulated users. Parties that transact with one another on a regular basis may favor this method if they want to leverage some of the security and immutability characteristics of a blockchain for transactions while removing the potential for unknown actors to participate. This feature is important for regulatory and privacy purposes. A blockchain that transmits potentially sensitive data would need to ensure that only authorized users can participate, and that no authorized participants act in a way that is inconsistent with regulatory, compliance, or other expectations. Otherwise, a participant, through their noncompliance, may negatively impact the compliance status of the network as a whole. Because of this, entities such as banks and insurance companies have formed consortia that can work together to establish permissioned blockchains for their own institutional purposes.

[51] ***Applying Blockchain in Securitization: Opportunities for Reinvention***, CHAMBER OF DIGITAL COMMERCE (Feb. 2017), https://digitalchamber.org/assets/sfig-blockchain-report.pdf.

What are the Applications of Blockchain Technology?

USE CASES[52]

- **Trade Finance**
  - **Trade finance facilitates global trade.** But it also introduces friction into the process since a trade finance transaction involves the exchange and verification of various documents generated by many different entities across the jurisdictions. There are two primary categories of trade finance: open account, and documentary trade – the most prominent of which involves letters of credit (LCs). Process inefficiencies cover both categories. The first type of inefficiency is that trade instruments are costly and time consuming to issue and execute. The physical documents necessary for trade finance present further difficulties: physical documents must be received before other processes in a transaction may take place, causing unnecessarily delays, and physical documents are prone to fraud and forgery.
  - **Blockchain can create new efficiencies in the processing of trade-related transactions.** Moving documentation to a secure digital environment updated in real time provides new opportunities to create, modify, and validate trade, title, and transport-related agreements. Additionally, the immutability of blockchain transactions allows for the effective tracking of documents through the entirety of their existence. Payment methods can be automated, mitigating risk and improving financing processes for buyers, suppliers, and financiers. Ultimately, these changes will increase the speed and liquidity of global supply chains, providing substantial benefits to consumers, businesses, and financial institutions.

- **Supply Chain**
  - **Supply chain implementation can improve the identification of the source and path of produce and many other items.** Supply chains are complex networks. This is due in part to the number of variables that can impact the outcome of a delivered product. As nodes in the supply chain store, share, and transmit data in a variety of formats, this limits the ability of any individual entity to know the provenance and validity of the data they are receiving. When the origin of products is difficult to ascertain, neither intermediate buyers nor the ultimate consumers are able to reliably confirm the value of the goods they purchased. These internal challenges with supply chain management are increased by the character of today's global supply chain which is fragmented, complicated, and geographically diffuse, increasing the difficulty of effective cooperation. For example, tracking contaminated produce has been a significant challenge, causing much waste. These problems both reduce efficiency of the supply chain and prevent effective regulatory enforcement in areas such as counterfeit goods, forced labor, poor working conditions, or other criminal activities.

[52] The following are examples of important use cases for blockchain technology. Note that these use cases can involve complex operations involving multiple parties and processes which can be enhanced and more efficient if blockchain technology is used appropriately. These use cases are drawn from: ***Smart Contracts: 12 Use Cases for Business & Beyond*** , CHAMBER OF DIGITAL COMMERCE (Dec. 2016), https://digitalchamber.org/smart-contract-use-cases/.

- **Supply Chain cont'd**
  - **In the context of global supply chains, blockchain technology could provide businesses and individuals with an increased ability to track a product's entire path from manufacturer to consumer.** The opportunities that blockchain can provide for the supply chain are not limited to one entity or activity. Business processes can achieve cost reduction and higher levels of efficiency through a streamlined supply chain. Consumers will be able to better determine the quality, safety, and legality of their purchases. Lawmakers can harness this information to more effectively enforce and prevent child labor, forced labor, counterfeit goods, poor working conditions, or other criminal activities. Of particular note is the impact on food safety tracking. Less of the food supply would have to be destroyed if the source of food contamination can be more accurately pinpointed at the first signs of contamination arise. A blockchain-based supply chain would allow for this level of accurate tracking.

- **Securities**
  - **Today's securities markets are based on quick transactions, where settlement on a near-instantaneous (T+0) basis is increasingly desired by market participants.** Many times, securities are paper-based, and the registration process is manual. Various logistical challenges occur due to the physical nature of securities and the slow processes that surround them. Companies that fail to keep their corporate registrations up-to-date require clean-up certificates of good standing before they can issue securities. In an effort to work around paper-based securities, intermediaries were created that could hold onto the securities on behalf of their true owners; however, these intermediaries increase cost, counterparty risk, and latency.
  - **Blockchain, smart contracts, and virtual currencies can establish new levels of control, and substantial benefits, for the owners of securities.**[53] Capitalization table management will be more easily tracked on a blockchain. Blockchain may allow business structures, such as limited liability companies, to operate similar to corporations in terms of distributing profits. Additionally, equity holders can more easily act on their voting rights. End-to-end workflows can be digitized due to securities existing on a distributed ledger, enabling faster trade settlement cycles. Most importantly, the risks posed by intermediaries can be limited, as ownership and control becomes more decentralized and the need for custodians lessens.

- **Healthcare**
  - **Healthcare efficiency suffers due to the lack of data visibility. Clinical trials, patient information, and research can all exist independent of one another.** The processes for sharing research is cumbersome across institutions. Moreover, information sharing is discouraged as healthcare information is particularly sensitive. The lack of information sharing can have disastrous consequences: the response to epidemics may be delayed or the knowledge of the harms and benefits of different treatments may be limited. Additionally, the risk of data theft increases as copies of healthcare data are spread and stored across a multitude of data controllers offering multiple points of breach.

[53] Both Delaware and Wyoming have authorized the tracking of corporate records on a blockchain. WY H.B. 101 (2018); DE S.B. 194 (2018).

- **Healthcare cont'd**
  - **Many of the problems surrounding the transfer, storage, and access of healthcare information can be solved using blockchain.** Blockchain may provide new methods of data storage and access. Currently, healthcare information is stored independently by each person that collects it. A healthcare information exchange built on a blockchain changes this, allowing healthcare information to be spread and shared across a network. Blockchain can create new levels of security for healthcare information, increasing the difficulty of unauthorized access. This control can give ownership of healthcare information to the patients themselves, and, with this ownership, patients can determine what access to grant to specialists throughout the healthcare experience. Finally, as data controllers can rely on the access limits and protections of personally identifiable information, they will be more likely to share the important data with the persons that can benefit most from it.

- **Insurance**
  - **Insurance products, by their very nature, require a central authority under the current model.** Insurance companies use complex calculations to determine the rates set, the conditions in which payments can occur, and whether or not those conditions are met by customers. They offer multiple lines of coverage, which can involve multiple repositories for customer information. Claims processing can take some time as information works its way through legacy systems.
  - **A blockchain can streamline overall functions, recordkeeping, and the claims process through a combination of smart contracts and internet-of-things ("IoT") enabled devices.** First, blockchains enable efficient and effective recordkeeping and information sharing among stakeholders within an insurance company. Moreover, with the use of smart contracts, they can streamline the claims process and user experience. Using automotive insurance as an example, a smart contract can be executed to record the policy, driving record, and report of all drivers that have purchased the policy. Using IoT enabled devices, establishing vehicle self-awareness, the vehicle can assess its own damage using sensors and can execute initial insurance claims and police reports. This removes the duplicative work that is required by various agents within the insurance entity itself, saving money and time.

- **Energy**
  - **Today's energy grids use central networks to operate.** The energy industry is highly regulated in most countries, and electric production currently uses large powerplants that distribute electricity for broad geographic areas. Such large, centralized distribution networks require extensive physical infrastructure. While there are efforts to move towards more decentralized transmission and distribution, the need to adapt legacy infrastructure has considerably slowed this process. Another impetus to change the centralized system is for cybersecurity. As our distribution systems require computer networks to operate, they are susceptible to network attacks. These attacks highlight the need for increased security measures.

- **Energy cont'd**
  - **Blockchain may make the distribution of power more efficient, lowering the costs for consumers.** Energy distribution networks of all sizes can benefit from blockchain systems. Centralized distribution networks can implement blockchain systems in order to further secure the power grid. These networks can confine attacks and limit their potential impact on the larger grid. Additionally, centralized distributors can use smart contracts to distribute power more efficiently, lowering the costs to consumers. Finally, smart contracts enable micro-grids and energy independence. One of the common problems with energy independence is the individual generation of more power than needed. With blockchain, excess energy producers can trade energy with users that are not generating sufficient energy to meet their needs. This allows energy users and producers to project their energy generation and use and then structure their output and intake accordingly. This would provide a multitude of independent and institutional stakeholders with the ability to cooperate in the generation, transfer, and use of energy.

- **Digital Identity**
  - **The amount of data that consumers share online and the number of data thefts that occur are continuing to increase.** Identity cuts across all industries and can vastly improve consumer access as well as enable efficient government and business functions. Of particular importance is information that is used to prove identity. This information is both highly sensitive and widely used online. Social security numbers, names, and birthdates are all used to establish identity online, and the theft of this information can be used to file fraudulent tax returns, obtain personal loans, and open credit cards, for example. Regaining identity information and clearing fraudulent items on a record attached to that identity can be costly and time-consuming.
  - **Blockchain can provide new methods of securing and sharing identity information.** Proving identity should not require the divulging of information, as the risk for identity theft increases each time identity information is transmitted. By leveraging asymmetric key encryption, identity can be validated without distribution of that sensitive information. Additionally, smart contracts can enable greater control over identifying personal information, giving consumers the ability to limit access to personal information or gain compensation for that access. This benefits counterparties to transactions that require identity verification as well. Storing personal information can trigger regulatory obligations depending on the type of transaction and the nature of the information. If the counterparty can verify information without storing it, they can limit their regulatory duties. This allows businesses to verify identities as required by law (***i.e.,*** KYC) in an efficient way, without having to retain records of that information. Legislators may also enable programs to test blockchain and DLT system use in voting, through the use of blockchain-based digital identities, to create a more secure and accountable voting mechanism.

- **Consumer Banking**[54]
  - **Blockchain is a tool that can help to eliminate, or reduce, the total number of underbanked and unbanked internationally and within the United States.** There are approximately 2 billion individuals who lack financial access and an additional 1.5 billion individuals who are underserved by the financial services industry.[55] Further, "derisking," the closure or determination not to open accounts for certain high-risk customers due to regulatory compliance concerns, has impacted the industry and customers.
  - **Virtual currency use can eliminate the potential costs to the unbanked and underbanked, providing them new access to financial services.** First, virtual currencies do not require a physical location or an initial deposit (for example, they can be accessed via a mobile phone), making them more cost effective and easy to use than traditional bank accounts. Additionally, using bank accounts can create unseen costs that do not apply to virtual currencies. Banks may require minimum deposits to keep accounts active or charge users a certain rate to continue to keep their account. Virtual currencies run strictly off of code and typically have no account fees or minimum deposits.

- **International Payments**
  - **For institutional entities, the most immediate application of blockchain is within the international transfer system.** Transfers between banks internationally rely on an expensive messaging network, known as the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") Network. The SWIFT network does not settle funds itself; rather, it sends messages on financial transactions between the banks, who then settle the transactions between themselves using corresponding accounts. As the transfer of virtual currencies is the equivalent of transferring information, they effectively perform the same function as the SWIFT network and reduce the high transaction costs of international transfers. Consumers already see the value of virtual currencies in international payments and are currently using them for international remittances outside of the traditional banking system. Further, virtual currencies can operate globally while remaining compliant with Anti-Money Laundering ("AML") and Know Your Customer ("KYC") regulations, without requiring strong central parties. Moreover, a company's AML and KYC obligations can actually be enhanced due to the mechanics of a blockchain because transactions are recorded immutably on the blockchain.

- **Institutional Custody**
  - **The rise in value of virtual currencies has created a new business model, virtual currency institutional custodians.** Storing virtual currencies entails certain operational complexities. Virtual currencies, and other blockchain-based assets, are tied to their address and that address' corresponding private key. If the key is lost or stolen, so is the ability to send the asset tied to that address. Although the key may be more secure than a password, it presents risks when a user wants to store large amounts of virtual currency. In response to this, companies are creating new methods to provide secure institutional custody for large amounts of virtual currency. This raises questions around compliance with custodial rules under various regimes.

[54] *See Blockchain and Financial Inclusion: The Role Blockchain Technology Can Play In Accelerating Financial Inclusion,* CHAMBER OF DIGITAL COMMERCE (Mar. 2017), https://digitalchamber.org/assets/blockchain-and-financial-inclusion.pdf.
[55] *Id.*

- **Voting**
  - **Blockchain technology can facilitate voting in elections and track votes cast in a secure and transparent manner.** Due to the secure and immutable nature of blockchain, votes may be cast in place of mail-in-ballots which may be lost and must be processed manually by county clerks. The votes may also be tracked through a blockchain to provide for a quicker, tamper-proof way of counting ballots. The State of West Virginia has piloted the use of blockchain technology for overseas service members, demonstrating how blockchain may add a measure of transparency and accountability to the voting process.

- **Central Bank Digital Currencies (CBDC)**
  - **Central bank-issued digital currencies may become a widely used form of government-backed fiat currencies.** An example of virtual currency acceptance by large institutional parties is the efforts by central banks to explore virtual currencies for their own use. An example of this is the Bank of Thailand, which is exploring virtual currency use in the context of interbank settlements. Similar to the international payment system described above, the Bank of Thailand would leverage central bank digital currency in order to streamline payments between domestic banks. This application is a perfect demonstration of a permissioned blockchain, as it entails transactions between a core group of trusted parties. Interbank settlements are not the sole application of CBDCs. Central banks are also exploring derivatives and securities settlements between institutions as well as general use payment systems, as an alternative to cash, for the general public.
  - **Regulators urge caution in exploring the technical aspects of the issuance of CBDCs.** While officials from some central banks have expressed skepticism towards the implementation of CBDC in the near future, others plan to introduce it in the near future. Most central banks are still researching CBDCs.

What Are Smart Contracts?

SMART CONTRACTS EXPLAINED

A smart contract is computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions.[56] The code can be stored and processed on a distributed ledger and can write any resulting change into the distributed ledger. This concept is what motivates much of the excitement surrounding blockchain technology. Smart contract use cases span a variety of industries and could lead to significant economic efficiencies, as they eliminate the intermediaries required for many transaction types and can operate automatically.

- **What They Are**
  - **"Smart contracts" are self-executing functions that exist within the blockchain.** Understanding smart contracts requires conceptualizing a blockchain as a collection of participants agreeing on the state of a network. Participants work together to verify that changes made to the network are accurate, and each change is recorded and immutable. Smart contracts are implemented within the blockchain and execute upon the occurrence of a variable, either external or internal to the blockchain. At a basic level, a smart contract can be thought of as an if-then statement—upon the occurrence of one thing, another thing happens automatically. Once a smart contract is logged onto the blockchain, it must execute as written, and a record of that smart contract, if on a public blockchain, remains publicly available.
  - **The variable that triggers the smart contract's execution may be internal or external to the blockchain, and the person/source that sends this information is an oracle.** In the case of external variables, external oracles submit information to the blockchain that triggers the execution. External oracles can collect and submit information as varied as the weather, the stock market's performance, or the outcome of a sporting event. Internal oracles, on the other hand, automatically execute upon the occurrence of a variable native to the blockchain itself. This type of information can be the number of transactions that have occurred, the date/time, or the occurrence of a third-transaction.

- **Legal Efficacy**[57]
  - **Existing U.S. federal and state law supports the formation and enforceability of smart contracts.** The ESIGN Act and the UETA provide sufficient legal basis for smart contracts executing the terms of a legal contract.

[56] *Smart Contracts: 12 Use Cases for Business & Beyond,* CHAMBER OF DIGITAL COMMERCE (Dec. 2016), https://digitalchamber.org/smart-contract-use-cases/.
[57] *Smart Contracts: Is the Law Ready?,* CHAMBER OF DIGITAL COMMERCE (Sept. 2018), https://digitalchamber.org/smart-contracts-whitepaper/.

- **Legal Efficacy cont'd**
  - **A contract does not have to be a physical document in order to be legally enforceable. In fact, commentators tend to agree that "mutual assent can take many forms, so long as it clearly implies agreement."**[58] The first two elements of a legally enforceable agreement are likely be met by the smart contract's mechanics. First, if any participant on a blockchain is entitled to execute on the smart contract, it constitutes an offer; additionally, if the smart contract is sent to a counterparty directly, that smart contract can constitute an offer solely to that counterparty. Second, at the time that the counterparty signs their private signature to the smart contract, they have effectively given acceptance to the agreement. Finally, the element of consideration can be satisfied so long as each party in the smart contract exchange some form of value.[59] Consideration can come in two forms—an exchange of value or performance at the outset of the contract, or a promise to perform or pay something of value in the future. For example, a conditional statement, such as "if it rains on Tuesday, Alice will give Bob $10" is not a contract unless Bob reciprocates consideration to Alice. A smart contract has the ability to provide a form of value and exchange it between two parties; however, it is up to the parties within the agreement to incorporate the necessary consideration into the smart contract.

- **Economic Impact**
  - **Smart contracts have enormous economic potential due to their frictionless nature. Smart contracts can increase the speed of transactions, executing them almost instantaneously.** A seemingly limitless number of miniature transactions can take place, on a rapid basis, through smart contracts. For example, the International Swaps and Derivatives Association has released a whitepaper that details how its standardized swap transaction documentation may be represented by a smart contract that, among other things, automates the exchange of margin payments among counterparties and reports transaction data to regulators.[60] This utility can be used to create disintermediated business processes: where payments across entire supply chains are streamlined, and equity holders or employees are compensated automatically upon the occurrence of certain events. The potential economic gain can be furthered with the addition of other types of new technologies, such as IoT-enabled devices. For example, an IoT device, such as a smart meter on a home, could record and log the usage of electricity. If the home is generating excess energy from a solar panel, the IoT device can automatically execute smart contracts to sell the unused energy to the grid.

[58] Kevin Werbach & Nicolas Cornell, ***Contracts*** Ex Machina, 67 DUKE L.J. 313, 328-34 (2017).
[59] Notably, the exchanged value need not be the exchange of equivalent value. See 1 J. STORY, COMMENTARIES ON EQUITY JURISPRUDENCE AS ADMINISTERED IN ENGLAND AND AMERICA 337 (14th ed., 1918).
[60] ISDA AND LINKLATERS, ***Whitepaper: Smart Contracts and Distributed Ledger - A Legal Perspective***, ISDA (Aug. 2017), https://www.isda.org/a/6EKDE/smart-contracts-and-distributed-ledger-a-legal-perspective.pdf.

- **Potential Hurdles**
  - **It should be noted that there remain logistical hurdles that must be overcome before the full economic benefit of smart contracts can be realized.** Contracts themselves are complex, and combining this complexity with the unforgiving logic of computer code could result in unintended outcomes for the parties involved. A slight error in the coding of the smart contract could lead to a result that no transacting party intended. Additionally, due to their immutability, smart contracts are rigid, and the means must be created to account for failure to perform or other items that are traditionally spelled out in a contract. Finally, certain subjective functions often found in traditional legal contracts, such as "best efforts," may be difficult to define by computer code.[61]

- **Support of the Technology**
  - **Because of the potential impact that smart contracts may have on the economy, they should be encouraged by policymakers.** First, government agencies should research the impact that smart contracts may have on the public sector. This interaction can allow lawmakers to understand their mechanics for use in the government and provide for better lawmaking. Second, lawmakers should establish incentives to encourage the use of smart contracts. Examples of incentive measures could include tax credits or write-offs for particular industries. Finally, lawmakers should refrain from drafting laws that limit the potential value of smart contracts, such as enacting enforceability provisions, establishing enhanced regulatory measures, or extend to smart contracts traditional contract law provisions that are ill-fitting for this novel technology.

[61] ***Smart Contracts: Is the Law Ready?,*** CHAMBER OF DIGITAL COMMERCE (Sept. 2018), https://digitalchamber.org/smart-contracts-whitepaper/.

Appendix

- **Technical Description of Bitcoin Protocol Operation**
  - Bitcoin was the first iteration of a blockchain protocol. It was established in 2008 as a peer-to-peer payment system for use in online transactions. In the Bitcoin blockchain, users transact directly with one another. To initiate a transaction, the spending user sends a message to the other computers in the network, announcing the transfer of a certain value in bitcoins from the user's public key to the recipient's public key. To verify the validity of this transaction, the spending user has to "sign" the transaction with a private key that corresponds with that user's public key. With asymmetric key encryption, users can sign the transaction, proving that they are the valid owner of that public key, without providing the private key itself. The process of validating that transaction, and including it within a block, begins after nodes on the network receive the transaction.
  - Nodes on the network work together to confirm and package transactions to create blocks. Nodes act out of their own self-interest, as the blockchain's protocol rewards them for their efforts independently. Using either their own full copy of the blockchain or querying other nodes that hold the Bitcoin blockchain in its entirety, the nodes work to confirm the validity of each transaction. Once a node has validated the transactions it has received, it begins to hash and combine them into a Merkle tree, to determine a Merkle root. The Merkle root acts as a reference to all transactions contained within a particular block. Nodes then create a hash of the block by combining the Merkle root, a timestamp of the block, and the hash of the previous block. Incorporating the previous block's hash ensures that the block is valid and inextricably linked to all other blocks on the blockchain.
  - At this point, the block holds all of the substantive data that it requires, but in the Bitcoin blockchain, which runs on a proof-of-work consensus protocol, nodes have to create a hash under a certain threshold in order to "win" that block's mining reward. The Bitcoin blockchain establishes a parameter that the hash of a block must meet for it to be valid. The hash must contain a certain number of leading zeroes, a level of difficulty set by the network. This is meant to ensure that a block takes around ten minutes to be validated. To create a hash solution that fits this parameter, each node must guess the nonce of a block. By adding the nonce to the block's other data, a new hash output is created. Nodes have to continually guess which nonce value will work to provide the hash solution with the requisite number of leading zeroes. This process ensures that no one computer can manipulate the network unless it has computing power that overwhelms all other nodes participating.

- **Technical Description of Bitcoin Protocol Operation cont'd**
  - Once the hash solution has been found, the other nodes on the network no longer have an incentive to continue providing work on that block; however, if they think the transactions within the block are invalid, they may put forth a competing block. Nodes choose which block solution to work from, and if they have determined that a block is invalid they will work from a block that they are more confident is correct. This means that a block becomes more valid as more blocks are chained to it. At a certain point, the nodes have "voted" on the validity of the block by continuing to work from its solution. Additionally, the mathematical difficulty of changing a previous block grows exponentially with each block that is chained to it.
  - Although the totality of this process seems complicated, through the Bitcoin software, much of it is handled automatically. For example, the nodes of the network use software that makes the entirety of the validation process automatic, rather than working by hand through the complex math required to create a block solution.

Glossary

- **Asymmetric Key Encryption**
  - Encryption, generally, is a tool used to codify information in an effort to hide its contents. Only a person that has access to the decryption tool for the underlying information is able to unlock the information for viewing. Asymmetric key encryption, also referred to as public key cryptography, creates different levels of access to the information. Asymmetric key encryption provides a user with a public key and a private key. The two are linked to each other, and an outside person cannot determine the digits of a private key from the public key. Individual can "sign" their private keys to a transaction to validate it, without divulging the contents of their private keys. This allows users to confirm that they possess a public key, without the requirement of divulging their private key.
- **Blockchain**
  - A specific type of distributed ledger technology that organizes data into blocks that are "chained" together chronologically by a cryptographic hash function and confirmed by a consensus mechanism.
- **Blockchain Protocol**
  - The underlying rules and processes of a blockchain is the blockchain's protocol. The protocol establishes how nodes come to consensus, how transactions are validated, and other monetary policies such as the mining reward or amounts of a particular virtual currency to be sent to dead-end addresses to be taken out of circulation, or "burned."
- **Blockchain-based Asset**
  - An asset that consists solely of a digital token on a blockchain.
- **Consensus Mechanism**
  - The method in which nodes come to agreement on the validity of changes to the blockchain is known as the consensus mechanism. There are many types of consensus mechanisms, but this paper only details the processes of two: proof-of-work and proof-of-stake. The consensus mechanism outlines the rules in which nodes can work to "mine" transactions and receive mining rewards.
- **Digital Token**
  - Transferable unit generated within a distributed network that tracks ownership of the units through the application of blockchain technology.

- **Distributed Ledger**
  - Computer software that employs a shared database architecture to maintain multiple, identical copies of an auditable, up-to-date distributed digital record of transactions or data.

- **Hash**
  - A hash is a mathematical function that produces an output of digits and characters from an input. What is significant about hashes is that they only work one-way. This means that the input is linked to that hash, and can be verified using the hashing algorithm, but it is mathematically improbable to determine the underlying information from the hash output. Even the slightest change in the underlying data will result in a wildly different output. Hashing differs from encryption due to the one-way effect it has on information.

- **Merkle Trees & Roots**
  - In a Merkle tree, each transaction is referred to as a "leaf." The transactions are each individually hashed and combined with another hashed transaction. The combination of hashes is, itself, hashed and combined. This process continues until there is one hash that contains the hashed reference of all transactions within the Merkle tree. This penultimate hash is known as the Merkle root and is contained within the block.

- **Node**
  - A node is a participant within the blockchain protocol. Generally, nodes work to validate transactions. How nodes go about this may differ depending on the consensus mechanism of the blockchain protocol. In the Bitcoin blockchain, nodes compete against one another to determine the hash solution of each block; whereas, in a proof-of-stake consensus mechanism, one node might propose a solution while other nodes on the network vote and validate that solution. Further, in the Bitcoin blockchain, certain nodes hold complete copies of the blockchain and do not compete to validate the block itself. Other nodes, that do not possess a full copy of the blockchain, then pay to submit queries to these nodes in order to determine the validity of the broadcast transaction.

- **Nonce**
  - In a proof-of-work consensus mechanism, even after a node has established all the substantive information within a block, it must ensure that the hash of all that information is a string of digits that contain a certain number of leading zeroes. To get to this number, nodes combine the information with a randomly selected digit, the nonce. Nodes continues to adjust the nonce until the resulting hash has the requisite amount of leading zeroes.

- **Public/Private Key Signature**
  - A method of ensuring data integrity and origin authenticity that uses a party's private key to sign and its corresponding public key to verify the validity of its signature.

- **Smart Contract**
  - Computer code that, upon the occurrence of a specified condition or conditions, is capable of running automatically according to pre-specified functions. The code can be stored and processed on a distributed ledger and would write any resulting change into the distributed ledger.

- **Virtual Currency**
  - A medium of exchange that operates like a currency in some environments, but that does not have all the attributes of fiat currency. In particular, it does not have legal tender status in any jurisdiction.

For more information please contact the
Chamber of Digital Commerce
policy@digitalchamber.org

For more information on the
Boston Blockchain Association
https://bostonblockchainassociation.com/

CHAMBER OF DIGITAL COMMERCE

BBA
BOSTON BLOCKCHAIN ASSOCIATION

digitalchamber.org

bostonblockchainassociation.com