Cryptosecurity

Brian Haney[1]

Abstract

This Essay makes three contributions to the blockchain and law literature. First, this Essay explores technical security aspects evolving with various governance mechanisms across blockchain networks. Next, this Essay analyzes digital assets under U.S. securities laws and executive enforcement policies, in light of several new developments at the U.S. Securities Exchange Commission. Third, this Essay crystalizes cryptocurrency compliance toward an autonomous governance system, introducing a new algorithm for compliance automation.

[1] Thank you to Archie Chaudhury, Mark Lemley, Fabrice Benhamouda, Ryan Fox, Elizabeth Baran, Fernando Morera, Veronica Root Martinez, Joel Gottlieb, Arry Yu, Lawrence Ward, Jeff Minzel, Stephanie Minato, Jesse Proudman, Anthony Pompliano, Polina Pompliano, Branden Keck, Dylan Nock, Sam John, Brad Haney, Broderick Haney, Angela Elias and Joel Carben for the helpful thoughts and comments.

Table of Contents

Introduction

Writing under the pseudonym Publius in the year 1787, Alexander Hamilton wrote in Federalist No. 30, "Money is, with propriety, considered as the vital principle of the body politic; as that which sustains its life and motion, and enables it to perform its most essential functions." [2] Consider then, not much has changed about money since the Founding Father responsible for American Economics wrote in the late 18th Century, cash is still king of the world. On the other hand, digital systems started reforming technology infrastructures in the middle of the 20th Century.[3] And in a nascent new millennium, these systems transformed the world economy completely.

On November 1, 2008, an unknown person with the pseudonym Satoshi Nakamoto sent an email to a cryptography mailing list to announce he had produced a "new electronic cash system that's fully peer-to-peer, with no trusted third party."[4] Later that year, Nakamoto published the Bitcoin White Paper, which serves as the foundation for most blockchain technology today. In the Bitcoin White Paper Nakamoto presents a problem, "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments."[5]

Nakamoto claims what is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a third party. They explain for transactions in such a system to be valid, there needs to be a way in which to verify electronic coins are not spent twice. In other words, there must be a method for the payee to know the previous owners did not already spend the electronic coin. Thus, Nakamoto proposes a solution to the double-spending problem using "a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions."[6] The solution has come to be known as a blockchain.[7]

In short, blockchain is better money. It's a technology representing technical convergence in currencies, security, and in some cases securities. Technically blockchain's are decentralized databases, maintained by distributed networks of computers. Scholars, industry leaders, and commentators rave about blockchain technology. For example, Harvard Scholar, Primavera De Filippi argues, "blockchain technology constitutes a new infrastructure for the storage of data

[2] Alexander Hamilton, Concerning the General Power of Taxation, Federalist No. 30, New York Packet (December 28, 1787).

[3] C.E. Shannon, *A Mathematical Theory of Communication*, Bell Systems Technical Journal (1948). U.S. Patent No. 2,801,281 to Oliver and Shannon, Communication system employing pulse code modulation (July 30, 1957).

[4] Saifedean Ammous, The Bitcoin Standard xv (2018).

[5] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1 (2008).

[6] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1 (2008).

[7] Riley T. Svikhart, *Blockchain's Big Hurdle*, 70 Stan. L. Rev. Online 100, 101 (2017). *See also* Emily Wells, et al., Blockchain Benefits and Risks, The Military Engineer, 62 (2018), https://www.researchgate.net/profile/Igor_Linkov/publication/325385235_Blockchain_Benefits_and_Risks/links/5df6b251a6fdcc2837245f1e/Blockchain-Benefits-and-Risks.pdf. ("Blockchain technologies are being considered as solutions to various cybersecurity and information technology threats and challenges.") *See also* Elona Marku, et al., General Purpose Technology: The Blockchain Domain (2019).

and the management of software applications, decreasing the need for centralized middlemen."[8] But, at its core, a blockchain is simply a distributed ledger than can record transactions between two parties.

Blockchain technology constitutes an infrastructure for the storage of data and the management of software applications. This Essay proceeds in three parts to detail certain security considerations for new money markets. Part I explores technical security aspects and mechanisms in blockchain technologies. Part II analyzes digital assets under U.S. securities laws and executive enforcement policies. Part III crystalizes cryptocurrency compliance toward an autonomous governance system. The theme throughout the Essay is fostering secure financial innovation.

[8] PRIMAVERA DE FILIPPI, AARON WRIGHT, BLOCKCHAIN AND THE LAW 33 (2018).

I. Technical Security

Security is the most important feature for blockchains. In fact, if transactions are not secure, then users will not engage because the risk for loss will be too high. In short, if information is not secure, then it can be accessed and thus taken. Indeed, the United States Department of Justice warns against cryptocurrency stealing as one of the main security concerns for blockchain technologies.[9]

Blockchain networks like Algorand and Ethereum comply with the federal standards published by the U.S. Department of Commerce for key pair management.[10] However, optimizing security protocol remains an ongoing task. Most blockchain security and encryption methods use the RSA algorithm[11] or the SHA-256 hash algorithm,[12] however post-quantum[13] measures are now developing. Conceptually, there are two ways to hack blockchains – malicious hacking and consensus change.

A. Malicious Attacks

The first is stealing a private key to siphon funds from a victim's wallet, which is probably criminal hacking.[14] For example, malicious hacking involves taking unauthorized control of private keys to secure protected funds.[15] To prevent this from happening, cryptocurrency exchanges develop robust software frameworks to ensure financial security.[16] However, some recognize threats from quantum machines.[17] So, Algorand and other blockchain networks have partnered to develop a quantum secure network.[18]

[9] U.S. Department of Justice, Cryptocurrency Enforcement Framework, Report of The Attorney General's Cyber Digital Task Force, 6 (October 2020).

[10] U.S. Department of Commerce, Digital Signature Standard, Information Technology Laboratory, National Institute of Standards and Technology Federal Information Processing Standards Publication, FIPS PUB 186-4 (July 2013).

[11] R.L. Rivest, et. al., A Method for Obtaining Digital Signatures and Public-Key Cryptosystems (1977) https://people.csail.mit.edu/rivest/Rsapaper.pdf. The RSA algorithm creates a mathematically linked set of public and private keys generated by multiplying two prime numbers together. While, multiplying two prime numbers is computationally inexpensive, figuring out which prime numbers were multiplied to get a number is computationally complex.

[12] National Institute of Standards and Technology, FIPS Pub 180-4: Secure Hash Standard. Federal Information Processing Standards Publication 180-4, U.S. Department of Commerce, at 3 (August 2015). The SHA-256 algorithm is the foundation of blockchain mining. The SHA-256 is a one-way hash function, which processes any message of an arbitrary size into a condensed representation called a message digest.

[13] Stewart I., et al., *Committing to Quantum Resistance: A Slow Defence for Bitcoin Against a Fast Quantum Computing Attack*., R. Soc. open sci.5: 180410, at 3. (2018) http://dx.doi.org/10.1098/rsos.180410.

[14] United States Patent No. 10,891,600 to Rebernik, User private key control (January 12, 2021).

[15] U.S. Patent No. 10,354,236 to Wang, Methods for preventing front running in digital asset transactions (July 16, 2019).

[16] United States Patent No. 9,882,715 to Alness et al., API key generation of a security system forming part of a host computer for cryptographic transactions (January 30, 2018).

[17] Brian Seamus Haney, Blockchain: Post-Quantum Security & Legal Economics, 24 N.C. Banking Inst. 117 (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3444695.

[18] World Patent Publication No. 2019/126311 AI, Fast and partition-resilient blockchains (December 19, 2018). *See also* Xianhui Lu, et. al., LAC: Practical Ring-LWE Based Public-Key Encryption with Byte-Level Modulus (August 4, 2020).

Another worry for blockchain adoption is whether the technology will be used to advance criminal activity and money laundering. For example, Ross Ulbricht and Hugh Haney[19] were both convicted on charges relating to using Bitcoin to traffic narcotics across the Silk Road. Consider instead, the technology will have the opposite effect because it will become more difficult to exchange value without a digital trace. Moreover, new technologies are evolving to identify suspicious behavior across distributed ledgers.[20]

B. Consensus Change

The second blockchain hack is a majority override. A majority override is a hack which results from competitive advantage in mining. Majority overrides should not be considered criminal hacking because they result from the legitimately logical blockchain software code. In other words, one must first follow the rules to the change the rules on a blockchain. And changing rules fosters innovation.

Consider an example, where Developer A submits a smart contract to a blockchain network. Developer A intends the contract to allow other developers to stake a cryptocurrency in exchange for an annual return paid in a second cryptocurrency. However, after the contract is deployed Developer B comes across the contract and realizes there is a logical script which will move the entire reserve of the second cryptocurrency to their address and does so. This is not malicious, nor intentional hacking – rather, moving the reserve allows the natural evolution of the blockchain and promotes innovation. Ultimately, it is the fault of the Developer A for deploying an inadequate contract to the network because Developer B had no way to know its intended purpose.

Algorand is a proof-of-stake blockchain, which evolved to improve security and power efficiency across the network by limiting miners to validating transactions proportional to an ownership share.[21] To combat the majority override problem, Algorand developed a proof-of-stake chain, differing from classical blockchains, which use a proof-of-work to validate transactions.[22] Quantum computers could also be used to gain an unfair mining advantage.[23] However, it is much less likely quantum computers will be able to overside the consensus mechanism which validates transactions across the network because validation is distributed among a network of computers, rather than centralized, and based on computational power.

[19] No relation to the author.

[20] United States Patent No. 10,380,594 to Bayer et al., Systems and methods for monitoring and analyzing financial transactions on public distributed ledgers for suspicious and/or criminal activity (August 13, 2019).

[21] Yossi Gilad, et al., Algorand: Scaling Byzantine Agreements for Cryptocurrencies, 53 (2017).

[22] Fabrice Benhamouda, et al., Better Zero-Knowledge Proofs for Lattice Encryption and Their Application to Group Signatures, ASIACRYPT 2014, PART I, LNCS 8873, 551 (2014).

[23] Brian Seamus Haney, Blockchain: Post-Quantum Security & Legal Economics, 24 N.C. Banking Inst. 117 (2020).

C. Protecting Privacy

The United States Supreme Court first recognized a Constitutional right to privacy in the year 1965.[24] In the decades since, Governments around the world are adopting new privacy laws to control corporate actors collecting data.[25] In the year 2019, the United States Federal Trade Commission imposed a $5.00 billion penalty on Facebook for privacy violations and failures.[26]

Privacy problems plague cryptocurrency exchanges as well.[27] For example, one recent majority privacy problem is a phishing scheme run on CoinBase by a company called Plaid. Plaid, a financial services provider, steals user's information by deceptively luring personal bank information from CoinBase customers. Then, Plaid remotely accesses users bank accounts and downloads their personal financial information.[28] Plaid deceptively obtains bank account credentials from users.[29]

The late cryptographer, Hal Finney,[30] warned there is much potential for fraud in digital currency.[31] Privacy is impossible without security. Across distributed ledgers, no transactions are private. Instead, all transactions are public. In fact, companies and Alt Coins are working on

[24] Griswold v. Connecticut, 381 U.S. 479 (1965). *See also* Lawrence v. Texas, 539 U.S. 558 (2003). (Affirming a Constitutional right to privacy.)

[25] California Consumer Privacy Act of 2018 § 1798.100 - 1798.199.100 (2018). *See also* Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4, 2016 O.J. (L 119) 33 (EU). *See also* United States Federal Trade Commission, Privacy & Data Security Update: 2019 (2020). See also David Hyman, William E. Kovacic, Implementing Privacy Policy: Who Should Do What?, 29 Fordham Intell. Prop. Media & Ent. L.J. 1117, 1119 (2019).

[26] Federal Trade Commission, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Press Release (July 24, 2019). *See also* Veronica Root, More Meaningful Ethics, U. Chi. L. Rev. Online (2019).

[27] Fabrice Benhamouda, et al., Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation, IBM Journal of Research and Development (April 2019), DOI: 10.1147/JRD.2019.2913621. ("Putting private data on the ledger comes with an inherent dilemma: If everyone sees the same ledger, how can we have private data that some can see but others cannot? A common solution in many systems is to put on the ledger only an encryption (or a hash) of the private data, while keeping the data itself under the control of the party that owns it.")

[28] Evans, Lenahen, et al., v. Plaid Inc., Class Action Complaint, Case No. 20-cv-4804, USDC No. D. Ca. (2020). (""First, Plaid induces consumers to hand over their private bank login credentials to Plaid by making it appear those credentials are being communicated directly to consumers' banks. Consumers are informed the connection is "private" and "secure," and their banking credentials will "never be made accessible" to the app. They are then directed to a login screen that looks like it is coming from their bank, complete with the bank's logo and branding. In reality, however, though Plaid does not disclose this, the login screen is created by, controlled by, and connected to Plaid.")

[29] Cottle, et al., Plaid Inc., Complaint for Damages Declaratory and Equitable Relief, Class Action, USDC No. D. Ca. (May 4, 2020). (""In a typical scenario, consumers log into their banks via an "OAuth" procedure, whereby users are redirected from the original webpage or app directly to their banks. There, consumers log into the bank's webpage or app, and then they are redirected back to the original app. Behind the scenes, the bank returns a "token" that allows the original app to access the consumer's bank information as necessary and authorized by the consumer, but without giving the app provider access to the login information.")

[30] Hal Finney was the recipient of the first Bitcoin transaction and thought by some to be Satoshi Nakamoto, the inventor of Bitcoin. *See* Hal Finney, Bitcoin and me, Bitcoin Forum (March 19, 2013).

[31] Hal Finney, Digital Cash & Privacy (August 19, 1993).

problems preserving privacy across the blockchain networks.[32] Various new technologies are developing specifically to address privacy concerns with the blockchain architecture.[33]

II. Financial Securities

Most broadly, securities are financial assets representing an interest in an object with value. Securities come in many forms, including stocks, bonds, and precious metals. As it pertains to cryptocurrency, one case is most prolific. In the year 2020, the United States Securities Exchange Commission (SEC), sued Ripple Labs for selling the Ripple cryptocurrency (XRP) without registering with the SEC.[34] The SEC's Lawsuit sought $1.3 billion in damages for an unregistered offering.[35] Moreover, some institutional investment firms are refraining from offering digital asset services due to the relative lack of regulation compared to traditional financial markets.[36]

A. Laws

Securities laws regulating public companies and the disclosure of information date back to post-depression reforms.[37] From their inception, the federal securities laws proposed a trade-off for U.S. companies, disclosure in exchange for access to public markets.[38] For purposes of raising funds, the securities laws create two things, disclosure obligations and penalties for violations of those disclosure obligations.[39] The Securities Act of 1933 ("Securities Act") and the Securities Exchange Act of 1934 ("Exchange Act") work in conjunction to regulate the disclosure of securities information to investors.[40]

The Securities Act was intended to prevent securities fraud.[41] The Securities Act ensures that issuers selling securities to the public disclose material information to investors and that any

[32] U.S. Patent No. 10,341,121 to Androulaki et al., System, method, and computer program product for privacy-preserving transaction validation mechanisms for smart contracts that are included in a ledger (July 2, 2019).
[33] Benjamin_btc, SwagStation0x, 13 (2021), https://www.swagstation.io/.
[34] Securities and Exchange Commission v. Ripple Labs, Inc., et al., United States District Court, 20 Civ. 10832, Complaint (December 22, 2020). ("From at least 2013 through the present, Defendants sold over 14.6 billion units of a digital asset security called "XRP," in return for cash or other consideration worth over $1.38 billion U.S. Dollars ("USD"), to fund Ripple's operations and enrich Larsen and Garlinghouse. Defendants undertook this distribution without registering their offers and sales of XRP with the SEC as required by the federal securities laws, and no exemption from this requirement applied.")
[35] However, Ripple was sold on the Coinbase cryptocurrency exchange throughout that period, but Coinbase was not party to the lawsuit. *See* U.S. Patent 10,878,389 to Shtylman et al., Cryptographic currency exchange (December 29, 2020).
[36] Jamie Dimon, Letter to Shareholders, J.P. Morgan Chase, 43 (2020).
[37] Daniella Casseres, *South Cherry Street, LLC v. Hennessee Group LLC: Investors' Desperate Plea for Second Circuit Standards*, 6 J. BUS. & TECH. L 231 (2011).
[38] Elisabeth de Fontenay, *The Deregulation of Private Capital and the Decline of the Public Company*, 68 HASTINGS L.J. 445, 448 (2017).
[39] James C. Spindler, *How Private is Private Equity*, 76 U. CHI. L. REV. 311, 320 (2009).
[40] *Id.*
[41] Deepa Sarkar, *Securities Act of 1933*, https://www.law.cornell.edu/wex/securities_act_of_1933. *See also* Daniella Casseres, *South Cherry Street, LLC v. Hennessee Group LLC: Investors' Desperate Plea for Second Circuit Standards*, 6 J. Bus. & Tech. L 231 (2011). The Securities Act prompts disclosure through a mandatory registration process in any sale of any securities. Section 5 of the Securities Act requires all issuers register non-exempt

securities transactions are not based on fraudulent information or practices.[42] The Act's goal is to provide investors with accurate information so that they can make informed investment decisions.[43] The Securities Act prompts disclosure through a mandatory registration process in any sale of any securities and is mainly applied to initial public offerings ("IPOs") by issuers.[44] Arguably, the registration process protects investors in two ways.[45] First, issuers cannot offer to sell securities without disclosing information about the company, and developing and delivering a prospectus that the SEC has reviewed.[46] Second, issuers are liable for any material misstatements or omissions in the prospectus or registration statement, providing a way to enforce truth in disclosure.[47]

The purpose of the Exchange Act is to regulate securities exchanges and over the counter markets, where securities are sold.[48] The Exchange Act primarily regulates transactions of securities in the secondary market, sales that take place after an issuer initially offers a security.[49] The Exchange Act purports to protect investors by making sure information is available, prohibiting fraud, and establishing severe penalties for those who defraud investors and those who engage in insider trading.[50] Further, the Exchange Act includes a mandatory disclosure process that is designed to force issuers to make public information that investors would find pertinent to making investment decisions.[51] In addition, the Exchange Act provides for direct regulation of the markets on which securities are sold and the participants in those markets.[52] This requires that issuers submit their periodic filings with the SEC, and the

securities with the Securities and Exchange Commission (SEC). Additionally, Section 5 regulates the timeline and distribution process for issuers who offer securities for sale. Section 6 provides the actual registration process in two parts. First, issuers must submit information that will form the basis of the prospectus, to be provided to prospective investors. Second, issuers must submit additional information that does not go into the prospectus but is accessible to the public. Section 7 gives the SEC the authority to determine what information issuers must submit. However, generally the SEC requires issuers submit information about the issuer and the terms of the offered securities that would help investors form a reasoned opinion about the investment. The requirements are extensive, and include descriptions of the issuer's business, past business performance, information about the issuer's officers and managers, audited financial statements of past business performance, executive compensation, risks of the business, tax and legal status, and the terms and information about the securities issued. All of this information becomes public soon after filing with the SEC, through the SEC's online EDGAR system.

[42] Daniella Casseres, *South Cherry Street, LLC v. Hennessee Group LLC: Investors' Desperate Plea for Second Circuit Standards*, 6 J. BUS. & TECH. L. 231 (2011).

[43] *Id.*

[44] Deepa Sarkar, *Securities Act of 1933*, https://www.law.cornell.edu/wex/securities_act_of_1933.

[45] *Id.*

[46] Laura Palk, *Gone but Not Forgotten: Does (or Should) the Use of Self-Destructung Messagins Applications Trigger Corporate Governance Duties?*, 7 Harv. BUS. L. REV. 115, 133 (2017).

[47] Deepa Sarkar, *Securities Act of 1933*, https://www.law.cornell.edu/wex/securities_act_of_1933.

[48] Daniella Casseres, *South Cherry Street, LLC v. Hennessee Group LLC: Investors' Desperate Plea for Second Circuit Standards*, 6 J. BUS. & TECH. L 231 (2011).

[49] Deepa Sarkar, *Securities Exchange Act of 1934*, https://www.law.cornell.edu/wex/securities_exchange_act_of_1934.

[50] *Id.*

[51] Jeaninie Nelson, *New Corporate Responsibility Law Increases Liabilities For Directors, Officers, and Attorneys, but Does it Increase Protections for Investors?*, 34 TEX. TECH L. REV. 1165, 1167 (2003).

[52] Deepa Sarkar, *Securities Exchange Act of 1934*, https://www.law.cornell.edu/wex/securities_exchange_act_of_1934.

regulatory agency makes this information available to all investors through EDGAR, its online filing system.[53]

B. Government Issuance

The U.S. Government owns and maintains significant interests in blockchain technologies. For example, in the year 2017, the United States Government seized more than 150,000.00 Bitcoins in connection with Silk Road founder, Ross Ulbricht's arrest.[54] In fact one reason for government ownership in blockchain technologies is recent reports explain most Bitcoin mining happens in China.[55] In fact, Carnegie Mellon Scholar, Emily Wells, emphasizes the importance of government blockchain use within the security context.[56] New movements in government backed blockchain networks are evolving to support a dialogue on Central Bank Digital Currency (CBDC).[57]

Stanford Law Fellow, Fernando Morera, explains CBDC is a "…form of digital money, intended to have both currency and legal tender status, which is issued, backed, and governed by central banks…"[58] On February 24, 2021, the Board of Governors of the Federal Reserve System ("FED") issued a press release highlighting it is critical for the FED to remain on the frontier for CBDC research and policy development.[59] According to the United States Supreme Court, what qualifies as money, "may depend on the facts of the day."[60]

The field of CBDC is still nascent. And there are several CBDC projects all around the world with different degrees of development.[61] Other research suggests, government blockchain technologies may be used for remote voting.[62] Some promote blockchain protocols may grow to support a solid foundation for distributed data management, auditing, and reporting. [63] Still, the

[53] *Id.*

[54] United States v. Ulbricht, 858 F. 3d. 71, 88 (2017).

[55] Ben Kaiser, et al., The Looming Threat of China: An Analysis of Chinese Influence on Bitcoin (October 5, 2018).

[56] Emily Wells, et al., Blockchain Benefits and Risks, The Military Engineer, 62 (2018), https://www.researchgate.net/profile/Igor_Linkov/publication/325385235_Blockchain_Benefits_and_Risks/links/5df6b251a6fdcc2837245f1e/Blockchain-Benefits-and-Risks.pdf. ("Blockchain technologies are being considered as solutions to various cybersecurity and information technology threats and challenges. The Department of Defense (DOD) is evaluating blockchains for current and potential uses.")

[57] Fernando Morera, Central Bank Digital Currencies – Recent Transatlantic Developments, Stanford-Vienna Transatlantic Technology Law Forum News Letter (2021).

[58] Fernando Morera, Central Bank Digital Currencies – Recent Transatlantic Developments, Stanford-Vienna Transatlantic Technology Law Forum News Letter (2021).

[59] Cheng, Jess, Angela N Lawson, and Paul Wong (2021). Preconditions for a general-purpose central bank digital currency, FEDS Notes. Washington: Board of Governors of the Federal Reserve System, (February 24, 2021), https://doi.org/10.17016/2380-7172.2839.

[60] *Wisconsin Central Ltd. v. United States*, 138 S. Ct. 2067 (2018), p. 10 of the majority vote.

[61] Fernando Morera, Central Bank Digital Currencies – Recent Transatlantic Developments, Stanford-Vienna Transatlantic Technology Law Forum News Letter (2021). *See also* Elona Marku, et al., General Purpose Technology: The Blockchain Domain (2019).

[62] Nuno Chainho Amiar, Remote e-voting overview, International Conference on Theory and Practice of Electronic Governance (2021).

[63] Moshen Toorani, Christian Gehrmann, A Decentralized Dynamic PKI based on Blockchain (December 30, 2020).

Government should respect ethical obligations to safeguard user's privacy to the best of its abilities.[64]

C. Coin Offerings

Traditionally, companies that went through an initial public offering (IPO) took on the obligations of public disclosure in exchange for access to capital investment from the general public.[65] Conversely, private companies were restricted to raising capital from insiders or financial institutions, which came with severe limitations.[66] As a result, corporate finance was divided into a public side, with larger companies, passive investors, and exchange-traded stock, and a private side, with smaller firms, owner-management, and illiquid equity.[67]

The truly public feature of the ledger is the documentation of ownership and transfers. [68] The owners themselves are not identified by name on the ledger, but rather by a set of letters and numbers representing their public cryptocurrency address.[69] Therefore, if Distributed Ledger Technologies (DLT) can prove secure, ICOs may represent a new wave corporate financing.[70] In fact, Ethereum's ability to run complex applications produced a torrent of Initial Coin Offerings ("ICOs").[71]

ICOs are a fundraising technique involving the exchange of Bitcoin or Ether for specialized cryptocurrencies, called tokens.[72] However, ICOs have had issues as well. Indeed, the first implementation of smart contracts, included over a $150 million in investment, where $50 million was lost in logic.[73] What differentiates ICOs from other token offerings is that tokens sold through an ICO represent an equity interest in a company.[74] In such cases, compliance is key because offering securities for sale may require registrations or exemptions from federal securities laws.

[64] Veronica Root, More Meaningful Ethics, U. CHI. L. REV. Online, 18 (2019).

[65] Elisabeth de Fontenay, *The Deregulation of Private Capital and the Decline of the Public Company*, 68 HASTINGS L.J. 445, 448 (2017).

[66] *Id.*

[67] *Id.*

[68] Craig Easland, *DAO Prompts SEC to Examine ICOs*, 21 No. 10 Wallstreetlawyer.com: Sec. Elec. Age NL 3 (2017).

[69] *Id.*

[70] Christian Catalina and Joshua S. Gans, Initial Coin Offerings and the Value of Crypto Tokens (March 5, 2019). MIT Sloan Research Paper No. 5347-18, Rotman School of Management Working Paper No. 3137213, https://ssrn.com/abstract=3137213.

[71] *Id.*

[72] *Id.*

[73] Saifedean Ammous, *The Bitcoin Standard* 254 (Wiley 2018). ("An attacker was able to execute the transaction in a way that diverted roughly $50 million to his account. It would be inaccurate to classify the attacker's action as theft because all the depositors in the smart contract had agreed their money would be controlled by the code. Ethereum developers then created a new version of Ethereum that protected against this type of attack and returned the money to the depositors.")

[74] In such a case, the company is offering coins as a security. See Edward O. Thorpe, A Man for All Markets 301 (2017). ("Derivative securities, which include warrants, options, convertible bonds, and many later complex inventions, derive their value – as we have seen – from that of an "underlying" security such as a common the common stock of a company.")

III. Cryptocurrency Compliance

Corporate financial compliance with regulatory oversight will be critical for firms using blockchain technology.[75] The future for innovation is bright with respect to cryptocurrency regulation because Gary Gensler, an expert on the intersections of blockchain and artificial intelligence,[76] was recently appointed the head of the Securities Exchange Commission. The current approach towards regulation has been gradual, seeking to build consensus among the development community, which is generally a good thing. One of the great innovations for blockchain technology is that compliance and governance systems may be embedded within the software architecture for blockchains.

A. Securities

There are a myriad of regulatory issues relating to cryptocurrency, including securities regulation, taxation considerations, and criminal activity.[77] Indeed, the Federal Reserve states compliance with the Bank Secrecy Act and anti-money-laundering requirements as two of its chief concerns relating to blockchain regulation.[78]Additionally, the scope of cryptocurrency as an investment poses regulatory questions from a securities perspective. For example, the Securities Act of 1933 and the Securities Exchange Act of 1934 collectively regulate the disclosure of securities information to investors.[79] As such, corporate financial compliance with regulatory oversight will be critical for firms using blockchain technology.[80]

According to the United States Supreme Court, "An 'investment contract', as used in the Securities Act, means a contract, transaction, or scheme whereby a person invests his money in a common enterprise and is led to except profits solely from the efforts of [a] promoter or a third party…."[81] According to the Court, "The test of an investment contract within Securities Act is whether [the] scheme involves an investment of money in a common enterprise with profits to come solely from efforts of others, and, if test is satisfied, it is immaterial whether enterprise is speculative or nonspeculative or whether there is a sale of property with or without intrinsic value."[82]

In fact, *Securities and Exchange Commission v. W.J. Howey Co et al.*, establishes more than seven decades of precedent that to be a security pursuant to the Securities Act, the asset must

[75] Veronica Root, Coordinating Compliance Incentives, 102 Cornell L. Rev. 1003, 1010 (2017).

[76] Gensler, Gary and Bailey, Lily, Deep Learning and Financial Stability (November 1, 2020), https://ssrn.com/abstract=3723132.

[77] Jeremy Papp, *A Medium of Exchange for an Internet Age: How to Regulate Bitcoin for The Growth of E-Commerce*, 15 U. Pitt, J, L. & Pol'y 33 (2014). *See also* Benjamin Van Adrichem, Howey Should be Distributing New Cryptocurrencies: Applying the Howey Test to Mining, Airdropping, Forking, and Initial Coin Offerings, 20 Colum. Sci. & Tech L. Rev. 388 (2019).

[78] David Mills et al., Distributed Ledger Technology in Payments, Clearing, and Settlement 30 (Fed. Reserve Bd. Fin. & Econ. Discussion Series, Working Paper No. 95, 2016), https://perma.cc/UUU6-R2SY.

[79] 15 U.S.C.A § 77-78.

[80] Veronica Root, *Coordinating Compliance Incentives*, 102 Cornell L. Rev. 1003, 1010 (2017).

[81] Securities and Exchange Commission v. W.J. Howey Co et al., 328 U.S. 203 (1946). (Citing Securities Act of 1933 § 77b (1)).

[82] Securities and Exchange Commission v. W.J. Howey Co et al., 328 U.S. 203 (1946).

produce profits “solely from efforts of others.” First, cryptocurrencies are not investment contracts under the Securities Act because investments in cryptocurrencies, and the profits thereof, do not come “solely from the efforts of [a] promoter or a third party.” Instead, cryptocurrency profits come from both internal and external sources, with value manifesting in many myriads.

Moreover, cryptocurrencies, including Ripple (XRP),[83] are not investment contracts because they are not “schemes” – rather global computer networks facilitating innovation, transparency, and opportunity. Still, in December 2020, the SEC, sued Ripple Labs for selling XRP without the appropriate registration. The SEC sought $1.3 billion in damages for an unregistered offering.[84] The Ripple case is largely considered an anomaly and the SEC should ultimately lose in the event the case makes it to a fact finder before settlement.

It is generally accepted within the blockchain space that tokens like Bitcoin, Ethereum, and Algorand are not legal securities under United States Law. Adding further security to this novice truth, SEC Commissioner Hester Pierce released a new proposal in April of 2021, Safe Harbor 2.0.[85] She even released the proposal on GitHub – this was a brilliant move because it connected law and technology in a unique forum. The proposal seeks to add statutory support for a general policy of non-enforcement for startup companies operating with blockchain technologies.

Even if a token does qualify as a security, which almost none do, then the Jobs Act provides a listing exemption under the crowdfunding rules.[86] Title III of the JOBS Act amended the Securities Act of 1933 to include Section 4(6), the crowdfunding exception. Crowdfunding is a relatively new and evolving method of using the Internet to raise capital to support a wide range of ideas and ventures. So, the securities question is relatively solved, and tax law questions are similarly simple.

[83] Securities and Exchange Commission v. Ripple Labs, Inc., et al., United States District Court, 20 Civ. 10832, Complaint (December 22, 2020). (“From at least 2013 through the present, Defendants sold over 14.6 billion units of a digital asset security called “XRP,” in return for cash or other consideration worth over $1.38 billion U.S. Dollars (“USD”), to fund Ripple’s operations and enrich Larsen and Garlinghouse. Defendants undertook this distribution without registering their offers and sales of XRP with the SEC as required by the federal securities laws, and no exemption from this requirement applied.”)

[84] However, Ripple was sold on the Coinbase cryptocurrency exchange throughout that period, but Coinbase was not party to the lawsuit. *See* U.S. Patent 10,878,389 to Shtylman et al., Cryptographic currency exchange (December 29, 2020).

[85] https://github.com/CommissionerPeirce/SafeHarbor2.0

[86] James J. Williamson, *The JOBS Act and Middle-Income Investors: Why it Doesn’t Go Far Enough*, 122 YALE L.J. 2069, 2071 (2013). The crowdfunding provisions of the JOBS Act were intended to help provide startups and small businesses with capital by making relatively few low dollar offerings of securities, featuring relatively low dollar investments by the crowd, less costly. Title III of the JOBS Act added Securities Act Section 4(a)(6) that provides an exemption from registration for certain crowdfunding transactions and is referred to as Regulation Crowdfunding. Regulation Crowdfunding permits individuals to invest in securities based crowdfunding transactions. Regulation Crowdfunding also provides a framework for the regulation of registered funding portals and broker-dealers that issuers are required to use as intermediaries in the offer and sale of securities.

B. Taxes

Tax law is a key consideration for cryptocurrency compliance. According to the Internal Revenue Service (IRS), "Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value."[87] Still scholars rightfully contend this definition is too broad.[88] Although, recent IRS guidance suggests virtual currencies may be considered property for tax purposes, and thus outside the scope of federal taxes.[89] Indeed, a recent IRS Notice explicitly states, "For federal tax purposes, virtual currency is treated as property."[90] Moreover, the IRS has also excluded virtual currency from the currency category for U.S. federal tax laws.[91]

The two main types of federal tax which apply to cryptocurrency are income tax and capital gain tax. Income tax for cryptocurrency follows the standard tax brackets defined by the IRS.[92] Similar to income collected in fiat money,[93] income collected in cryptocurrency may be divided into categories of taxable and non-taxable income.[94] However, because cryptocurrencies are extremely volatile, it is not clear what value should be assigned to cryptocurrency received as income.[95] Additionally, it is not clear when the income should be reported as the cash value may not be derived for years to come.[96]

[87] IRS Notice 2014-21, IRS Virtual Currency Guidance (April 14, 2014). https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21.

[88] Nika Antonikova, *Real Taxes on Virtual Currencies: What Does the IRS Say?,* 34 Virginia Tax Review, No. 3, 4 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2559839. ("This paper argues that the Service should develop a narrower definition of what qualifies as a convertible virtual currency to remove pure game experiences from the regulation.")

[89] IRS, IRS Virtual Currency Guidance, Notice 2014–21 (2021), https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21. ("Q–1: How is virtual currency treated for federal tax purposes? A–1: For federal tax purposes, virtual currency is treated as property. General tax principles applicable to property transactions apply to transactions using virtual currency.")

[90] *Id.*

[91] *Id.* ("Q–2: Is virtual currency treated as currency for purposes of determining whether a transaction results in foreign currency gain or loss under U.S. federal tax laws? A–2: No. Under currently applicable law, virtual currency is not treated as currency that could generate foreign currency gain or loss for U.S. federal tax purposes.")

[92] For 2021 for single individuals filing the tax rates are 10.00% for incomes under $9,950.00; 12.00% for incomes under over $9,950.00; 22.00% for incomes over $40,525.00; 24.00% for incomes over $86,375.00; 32.00% for incomes over $164,925.00; 35.00% for incomes over $209,425.00; and 37.00% for incomes over $523,600.00. *See* Internal Revenue Service, 26 CFR 601.602, Tax forms and instructions., Rev. Proc. 2020-45 (2020).

[93] The U.S. Dollar is fiat money, it is not backed by anything and only has value because the U.S. Government assets its value. *See* John J. Chung, Money as Simulacrum: The Legal Nature and Reality of Money, 5 HASTINGS BUS. L. J. 109, 112 (2009).

[94] Department of the Treasury, Internal Revenue Service, Publication 525 Taxable and Nontaxable Income (April 6, 2021).

[95] Nika Antonikova, *Real Taxes on Virtual Currencies: What Does the IRS Say?,* 34 Virginia Tax Review, No. 3, 12 (2014), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2559839. ("…it is not clear that including the value of a virtual currency in gross income at the time it is obtained is the best approach to taxing it.")

[96] One way in which clarity may be conveyed is that cryptocurrency earned as income does not become taxable until it is liquidated to cash, at which time it will be taxed at the cash value taxpayer receives. *See* EDWARD O. THORPE, A MAN FOR ALL MARKETS 287 (2017).

Generally, capital gains tax may apply to cryptocurrency investors. The tax rates that apply to a capital gains are generally lower than the tax rates for other types of income.[97] The capital gains rate is generally 15.00% for most individuals.[98] Capital gains are reported through a Form 8949, which allows for reporting the sale of capital assets.[99] In general, capital gains are not realized until the asset is liquidated. As such, the door remains open, the future uncertain for how cryptocurrency will be taxed.

C. Algorithmic Automation

Economic regulation refers to taxes and subsidies, as well as to explicit legislative and administrative controls over rates, entry, and other facets of economic activity.[100] However, governments can also influence behavior indirectly through economic regulation.[101] For blockchain, a persuasive argument is the technology is a response to public demand for the correction of inefficient and inequitable economic markets.[102] Some suggest, it is impossible to develop wealth in government money without government acceptance.[103] However, given the semi-autonomous nature of blockchain systems, the object of regulation, is unclear at best.[104]

The lack of clarity as to the object of regulation makes writing legislation, procedures, and policies a difficult task. But, to succeed in this task – it is necessary to measure performance according to defined, measurable, and objective features. Compliance with all bodies of law and regulation can be automated according to a design for optimality. The below equation measures compliance, C using a geometric mean to measure defined factors.[105]

$$C = \sqrt[\Sigma_{j=1}^{n} w_j]{\prod_{i=1}^{n} F_i^{w_i}}$$

[97] Internal Revenue Service, United States Department of the Treasury, Investment Income and Expenses IRS Publication 550, 67 (2020).

[98] Internal Revenue Service, Topic No. 409 Capital Gains and Losses (2021), https://www.irs.gov/taxtopics/tc409. ("Some or all net capital gain may be taxed at 0% if your taxable income is less than $80,000.") *See also* Internal Revenue Service, United States Department of the Treasury, Investment Income and Expenses IRS Publication 550, 67 (2020). ("For 2020, the maximum capital gain rates are 0%, 15%, 20%, 25%, and 28%.")

[99] IRS, About Form 8949, Sales and other Dispositions of Capital Assets (2021), https://www.irs.gov/forms-pubs/about-form-8949.

[100] Richard A. Posner, Theories of Economic Regulation, National Bureau of Economic Research Working Paper No. 41 at 1 (1974).

[101] Primavera De Filippi, Aaron Wright, Blockchain and the Law 174 (2018).

[102] Saifedean Ammous, The Bitcoin Standard 136 (2018).

[103] Saifedean Ammous, The Bitcoin Standard 70 (2018).

[104] Primavera De Filippi, Aaron Wright, Blockchain and the Law 174 (2018).

[105] Brian S. Haney, Applied Natural Language Processing for Law Practice, 2020 B.C. Intell. Prop. & Tech. F. (2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3476351.
See also Brian S. Haney, Calculating Corporate Compliance & The Foreign Corrupt Practices Act, 19 U. Pitt. J. Tech. L. & Pol'y 1 (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3261443.

Certain factors F_i may be assigned based on various features for a specific asset or regulatory corpus. For example, one factor to consider may be utility because if a cryptocurrency is used for governance or voting, it is almost certainly not a security token. Similarly, if a token is backed by or tied to the value of another asset and pays dividends to investors, then the token is likely a security. Factors may also take account of existing legal frameworks for securities analysis – for example, a scorecard approach.[106]

The object oriented approach to compliance recognizes the existing legal infrastructe with particular focus on instilling optimal obedience in organizational protocol. In other words, following the algorithm makes securities compliance easy by adopting an informatics-based approach to legal and regulatory analysis.

$$C^* = \lim_{i \to n} f_i$$

The optimal compliance protocol C^* reduces to the minimized limit. Another way, the algorithm iterates toward reward-based incentive structures and continuous improvements.

In complex regulatory environments, the stakes are high. We can't forget what went wrong before, cases like *United States v. Swartz*[107] and *Gonzales v. Raich*[108] remind us of the harsh consequences associated with aggrandizing federal authority. Federal priorities need to be set straight, with power in the people and not the Republic. Given the priorities of the new administration, particularly the recent SEC comments on promoting blockchain innovation, we should expect a prosperous future for cryptocurrency in the United States.

[106] Cryptocurrency Rating Council, About Our Asset Rating Framework, Importance of the Howey Test for Classifying Digital Assets (2021), https://www.cryptoratingcouncil.com/framework.
[107] *United States v. Aaron Schwartz*, Criminal No. 11-10260-NMG (D. Mass. Aug. 1, 2011).
[108] *Gonzales v. Raich*, 545 U.S. 1 (2005).

Conclusion

In sum, this Paper provided needed analysis on the edge in law and financial technology in the digital public sphere. Great innovations are often born of focused solutions to small problems. For example, in the Bitcoin White Paper Satoshi Nakamoto presents a problem, "Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments."[109] Nakamoto's focused solution, a blockchain, has spawned a completely new economy on the internet today.[110] Now, cryptocurrency is legal and it's here to stay.

In fact, returns from blockchain technology are outpacing even the best investment firms, including Berkshire Hathaway. But as a system, for a while Warren Buffet's description that cryptocurrency is rat poison squared seemed significant.[111] However, now that Bitcoin is worth more than both Berkshire Hathaway and Tesla, blockchain is too big to fail.[112] Still economically, not much has changed since Hamilton wrote in the late 18th century.[113] Similar to the revolutionary period, in modern society, money remains the ultimate form of freedom. It enables the holder limitless power to cure disease, promote progress, and even explore space.

The software systems fostering global networks are changing transactions similar to the way the Internet revolutionized information.[114] This is particularly true in the developing world – for example, data retention in Malaysia for consumer markets is relatively limited.[115] However, with blockchains, data retention for all transactions is transparent and recorded on a public ledger.

Most importantly, cryptocurrency creates opportunities for the those in need. Programs like GitCoin Grants and Algorand Grants, allow developers to earn cryptocurrency by producing valuable code, intellectual property, and solutions to new cryptographic challenges. In fact, the respective programs have already allocated $22 million and $250 million in open source development funding respectively. Fundamentally, cryptocurrency creates a freer global society, providing more opportunity to those hungry to earn.

[109] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 1 (2008).

[110] Riley T. Svikhart, Blockchain's Big Hurdle, 70 STAN. L. REV. ONLINE 100, 101 (2017).

[111] Anna Fifield, Lyric Li, *Instead of lunch with Warren Buffet, Chinese Entrepreneur Justin Sun Eats Humble Pie*, Washington Post (July 25, 2019) https://www.washingtonpost.com/world/instead-of-lunch-with-warren-buffett-chinese-entrepreneur-eats-humble-pie/2019/07/25/b6370728-ae94-11e9-9411-a608f9d0c2d3_story.html.

[112] Even with companies like Tesla growing more than 200.00% in the year 2020, cryptocurrencies far outpaced the stock market. So, it isn't surprising Tesla bought $1.5 billion in bitcoin in January 2021. In its 2021 Form 10-K filing, an annual report to the SEC, Tesla explains the reason for the investment is because of the SEC's selective enforcement scheme and a deeply volatile market.

[113] Alexander Hamilton, Concerning the General Power of Taxation, Federalist No. 30, New York Packet (December 28, 1787).

[114] Dr. Thibault Schrepel, Collusion by Blockchain and Smart Contracts, 33 Harv. J. L. & Tech. 118, 118 (2019). ("Blockchain may transform transactions the same way the Internet altered the dissemination and nature of information.")

[115] Wei Mei Wong, Consumer Preferences Between Hypermarkets and Traditional Retail Shophouses: A Case Study of Kulim Consumers, 43 Asia Profile 6, 559, 559 (December 2015), http://d-scholarship.pitt.edu/39780/. ("Most data relating to retail choice in Malaysia is from surveys taken in urbanized areas of Malaysia.")