CRYPTO TRANSACTION DISPUTE RESOLUTION

WULF A. KAAL* & CRAIG CALCATERRA **

Abstract

The rapid evolution of anonymous, autonomous, and distributed blockchain-based smart contracting creates friction and enforceability issues with existing legal and jurisdictional principles, calling the future governance of blockchain technology into question. The effective governance of blockchain technology and smart contracting is essential to ensuring its continuing evolution. Based on the mathematical principles underlying the disposition of blockchains, we propose and evaluate an alternative approach to the existing legal exercise of jurisdiction that is inherent in blockchain technology itself. We call this distributed jurisdiction.

This contribution is not merely theoretical. Several Ethereum smart contracting crypto startups demonstrate that anonymity can be perpetuated in blockchain technology, despite blockchains' eternal storage of information and its growing size working against anonymity. Startup applications highlight that the technology itself offers means of internal controls that help ensure effective governance in the continuing evolution of the technology.

Based on the concept of distributed jurisdiction, we suggest an open source platform ecosystem for smart contracting dispute resolution that allows users to opt into a conflict resolution mechanism that enables more nuanced crypto solutions and produces greater certainty in the process. Anonymized arbiter expertise via rankings in combination with a representation option for crypto disputes provide a resolution mechanism for legacy businesses that desire to participate

* Associate Professor, *University of St. Thomas School of Law (Minneapolis, USA).* The authors are grateful for outstanding support from research librarian Megan McNevin.

** Associate Professor, *Department of Mathematics, Metropolitan State University (St. Paul, USA).*

in the growth of crypto business opportunities, hope to avoid legacy system intermediation and the associated transaction costs, but require legal legacy system assurances and crypto dispute resolution equivalence.

Key Words: Blockchain, Distributed Ledger Technology, Artificial Intelligence, Machine Learning, Data Science, Data Scientists, Meta Models, Innovation, Entrepreneur, Start-up, Big Data, Smart Contract, Jurisdiction, Governance, Ties Network, Aragon, OpenBazaar, Ethereum, Platform, Ecosystem

JEL Categories: K20, K23, K32, L43, L5, O31, O32

TABLE OF CONTENTS

I. Introduction

Any existing business logic can be coded into a blockchain. Blockchain technology is a computer architecture for an open and secure distributed database. A blockchain, in essence, is an autonomous dynamically growing chain of blocks of encrypted data generated by a decentralized group of users. Most blockchains, such as Ethereum (but not Bitcoin) are Turing complete, or computationally universal, meaning any calculation possible can be simulated within a blockchain design. In other words, blockchain can do what any other computer program can do--from controlling a Mars lander to sending a cat video to China. Accordingly, any existing business logic can be coded into the blockchain, giving it extremely wide applicability in almost all industries and subject areas.[1]

What makes the blockchain architecture so successful is its ability to solve several seemingly-contradictory requirements: 1. The blockchain database gives users absolute privacy.[2] At the same time, the complete list of transactions on the public blockchain is open—anyone with an internet connection can view the entire history of transactions using the public key addresses. This gives users confidentiality and confidence in the accuracy and value of the transactions. 2. The system is open, meaning that anyone connected to the internet can participate in editing any part of the blockchain. At the same time, it is highly secure against malicious attacks on the integrity of the information within its transactional history. Thus, any participant has great power over the system, while still giving users short-term confidence in the system's validity which can be quickly

[1] We are not claiming that the broad applicability of blockchain systems necessarily leads to implementation or even implementation efforts. Legacy systems in the existing infrastructure undermine a substantial portion of blockchain-based system implementation in businesses across industries. It is, however, foreseeable that as the infrastructure in southeast Asian countries such as Singapore is being remodeled with blockchain solutions legacy systems in the infrastructure in the USA and Europe may over time make way for the efficiency gains possible through blockchain technology. *See*, *Singaporean Dollar Tokenized Through Ethereum's Blockchain by the Monetary Authority of Singapore*, TRUSTNODES (June 7, 2017, 3:15 PM), http://www.trustnodes.com/2017/06/07/singaporean-dollar-tokenized-ethereums-blockchain-monetary-authority-singapore. Existing shortcomings of the technology will also be addressed as the technology and its applications evolve.

[2] At least within the system this is true. Public key encryption is used, giving users private keys for information to the bitcoin contents of their personal accounts, while public keys are generated to give addresses for coins used in any expenditures.

verified by any modern computer. 3. The system is autonomous, meaning no central authority exists to actively maintain the integrity of the system. At the same time, an open system of coded consensus protocols regulates the building and maintenance of the ledger.[3] Concurrently, this open and dynamic system responds swiftly and automatically to any necessary changes to secure data, and adapts to fluctuating computational power. This gives users long-term confidence through the removal of larger historical forces that can determine the value of the currency, such as technological and political changes.

Because of its very expansive and near universal applicability, it is crucial for the broadening evolution of blockchain technology to find jurisdictional means for the governance of the crypto economy that is facilitated and sustained by blockchain technology. A lack of

[3] Efforts to move from proof of work to proof of stake are already underway, improving several of the shortcomings of the blockchain protocol: *See Proof of Stake FAQ,* GITHUB, *https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ (last visited June 16, 2017);* "What are the benefits of proof of stake as opposed to proof of work? *See* Vitalik Buterin, *A Proof of Stake Design Philosophy*, MEDIUM (Dec. 30, 2016), https://medium.com/@vitalikbuterin/a-proof-of-stake-design-philosophy-506585978d51 for a more long-form argument. In short:

- No need to consume large quantities of electricity in order to secure a blockchain (e.g. it's estimated that both Bitcoin and Ethereum burn over $1 million worth of electricity and hardware costs per day as part of their consensus mechanism).
- Because of the lack of high electricity consumption, there is not as much need to issue as many new coins in order to motivate participants to keep participating in the network. It may theoretically even be possible to have *negative* net issuance, where a portion of transaction fees is "burned" and so the supply goes down over time.
- Proof of stake opens the door to a wider array of techniques that use game-theoretic mechanism design in order to better discourage centralized cartels from forming and if they do form from acting in ways that are harmful to the network (e.g. like selfish mining in proof of work).
- Reduced centralization risks, as economies of scale are much less of an issue. $10 million of coins will get you exactly 10 times higher returns than $1 million of coins, without any additional disproportionate gains because at the higher level you can afford better mass-production equipment.
- Ability to use economic penalties to make various forms of 51% attacks vastly more expensive to carry out than proof of work - to paraphrase Vlad Zamfir, "it's as though your ASIC farm burned down if you participated in a 51% attack".

governance and conflict resolution mechanisms would undermine the democratized trust created by blockchain technology and hinder its broadening evolution and applicability. Jurisdictional means are the basis for effective conflict resolution mechanisms applicable to crypto transactions in the blockchain. Not having the required jurisdictional means necessary for conflict resolution mechanisms for Ethereum blockchain-based smart contracting, may invoke consumer mistrust in the new technology. This can then undermine the evolution of the blockchain-based crypto economy.

The increasing separation of physical and virtual identities driven by anonymity in the crypto economy challenges the existing jurisdictional means over virtual transactions involving blockchain technology and smart contracting. Encrypted distributed smart contracts are removed from otherwise applicable jurisdictional principles that govern virtual transactions.[4] Users and supporters of the crypto economy are anonymized through public-key encryption and virtual private networks (VPNs). While technically personal jurisdiction would still apply to parties transacting in encrypted distributed smart contracts, the practicability of enforcement is impossible given the separation of physical identifiers and encrypted distributed smart contracts. Because the system operates largely autonomously, even if every user and supporter of the blockchain and their location were known, it would still not be possible to exercise jurisdiction in the traditional meaning of the word. Such impracticability calls into question the existing jurisdictional means governing the evolution of distributed ledger technology.

Regulatory alternatives for blockchain-based conflict resolution are necessitated by the impossibility of consistently identifying the parties in any dispute in the context of crypto transactions on the blockchain and the associated problems of applying the existing legal infrastructure. We cannot conceptualize

[4] The creation and maintenance of a blockchain cannot be controlled directly in any practical way. As long as the internet exists in two competing jurisdictions, the creation of blockchains cannot or can only very limitedly be controlled. Because of the fully networked nature of the technology, the associated variability in possible legal enforcement of blockchains further complicates the application of jurisdictional means to govern blockchains. Even if traditional jurisdiction could be exercised, comprehensive and universal enforcement would be extremely difficult, if not impossible, as blockchain designs either give users complete privacy or no privacy at all, or anywhere in the spectrum between.

opportunities in the crypto transactional universe that could possibly enable and allow a court in the existing legal infrastructure to decide and enforce any disputes between crypto transactional parties. Because of the severity of these challenges for the existing legal and jurisdictional infrastructure, we conclude that the sensible approach for including good governance in crypto transactions necessitates instituting governance solutions inherent in the blockchain technology itself. Accordingly, we introduce the concept of a distributed jurisdiction, which we hereinafter evaluate.

This article highlights the need for creating blockchain-based jurisdictional means as a basis for emerging conflict resolution mechanisms. Solutions for the incompatibility problem between blockchain technology and the existing legal jurisdictional infrastructure will evolve with the evolution of the technology itself. While conceptually we believe in the incompatibility of the crypto evolution via blockchain technology with the existing regulatory infrastructure, it is important to appreciate the many gradations of blockchain technology and its broadening application bases. Given the gradations, it would be imprudent to claim perfect and universal solutions to the incompatibility problem we highlight in this article.[5]

II. Blockchain Technology

Blockchain technology has been defined in many different ways and no truly uniform definition seems to exist. Some refer to it as a giant worldwide distributed immutable "google spreadsheet" for transactions.[6] Others define blockchain by focusing on its central

[5] When discussing the abstract concept of blockchain architecture we have the luxury of assuming an idealized form. In particular, the abstract blockchain is perfectly autonomously run, whereas the particular bitcoin and Ethereum blockchain examples were created in the real world in 2009 and 2015 and have not yet bootstrapped their way to full autonomy, since there are still human actors who have outsized power in affecting the code. Further, it is important to recognize that it is possible to create blockchains that are intentionally not fully decentralized or autonomous, in which case the traditional legal structure automatically applies. *See*, *White Paper*, GITHUB, https://github.com/ethereum/wiki/wiki/White-Paper (last visited June 16, 2017). However, we believe we are justified in our assumption of an ideal blockchain because of the swift and substantial progress towards perfect autonomy in the most important blockchain applications of bitcoin and Ethereum. In these cases, and in any future implementations of the ideal blockchain, we are arguing that the traditional legal infrastructure will be challenged.

[6] Jonathan Shieber, *Colu Aims To Bring Blockchain Technology Everywhere*, TC (Jan. 27, 2015), https://techcrunch.com/2015/01/27/colu-aims-to-bring-blockchain-

elements of blockchain, e.g. transaction ledger, electronic, decentralized, immutable, cryptographic verification, among several others.[7] Vitalik Buterin, the founder of Ethereum perhaps most prominently defined blockchain as follows:

> "Public blockchains: a public blockchain is a blockchain that anyone in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process – the process for determining what blocks get added to the chain and what the current state is. As a substitute for centralized or quasi-centralized trust, public blockchains are secured by crypto economics – the combination of economic incentives and cryptographic verification using mechanisms such as proof of work or proof of stake, following a general principle that the degree to which someone can have an influence in the consensus process is proportional to the quantity of economic resources that they can bring to bear. These blockchains are generally considered to be 'fully decentralized'."[8]

---

technology-everywhere; Craig Leppan, *Who Is Blockchain Going to Affect the Most,* OVATIONS, July 29, 2015), http://www.ovationsgroup.com/blockchain/.

[7] *See, e.g.,* ALAN MORRISON, BLOCKCHAIN AND SMART CONTRACT AUTOMATION: BLOCKCHAINS DEFINED, PWC (2016), http://www.pwc.com/us/en/technologyforecast/2016/blockchain/pwc-smart-contract-automation-definition.pdf; Alistair Dabbs, *What Is Blockchain, and Why Is It Growing in Popularity?* , ARSTECHNICA (Nov. 6.2016, 8:00 AM), https://arstechnica.com/informationtechnology/2016/11/what-is-blockchain/; Lee Grant*, Blockchain – Definition, Origin, and History*, TECHBULLION (Sept. 6, 2016), http://www.techbullion.com/blockchain-definition-origin-history; DELOITTE, BLOCKCHAIN ENIGMA. PARADOX. OPPORTUNITY 4–7 (2016), https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf.

[8] Vitalik Buterin, *On Public and Private Blockchains*, ETHEREUM BLOG (Aug. 7, 2015), https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains, Contrasting public blockchains (the original idea) with:" Consortium blockchains: a consortium blockchain is a blockchain where the consensus process is controlled by a pre-selected set of nodes; for example, one might imagine a consortium of 15 financial institutions, each of which operates a node and of which 10 must sign every block in order for the block to be valid. The right to read the blockchain may be public, or restricted to the participants, and there are also hybrid routes such as the root hashes of the blocks being public together with an API that allows

Rather than attempting to agree on a mutually acceptable phraseology for a definition, a description of the core elements of ledger technology can help define the blockchain. As such, a blockchain is a shared digital ledger or database that maintains a continuously growing list of transactions among participating parties regarding digital assets – together described as "blocks."[9] The linear and chronological order of transactions in a chain will be extended with another transaction link that is added to the block once such additional transactions are validated, verified and completed.[10] The chain of transactions is distributed to a limitless number of participants, so called nodes,[11] around the world in a public or private peer-to-peer network.

Blockchain technology removes fraudulent transactions. Compared with existing methods of verifying and validating transactions by third party intermediaries, blockchains security measures make blockchain validation technologies more transparent and less prone to error and corruption. While blockchains use of digital signatures helps establish the identity and authenticity of the parties involved in the transaction, it is the completely decentralized network connectivity via the internet that allows the most protection against

---

members of the public to make a limited number of queries and get back cryptographic proofs of some parts of the blockchain state. These blockchains may be considered "partially decentralized". "Fully private blockchains: a fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent. Likely applications include database management, auditing, etc internal to a single company, and so public readability may not be necessary in many cases at all, though in other cases public auditability is desired."

[9] *See, e.g.,* Michele D'Aliessi, *How Does the Blockchain Work?,* MEDIUM (June 1, 2016), https://medium.com/@micheledaliessi/how-does-the-blockchain-work-98c8cd01d2ae#.w76hifcu2; Monica Pearson, *Blockchain Is the New Buzzword*, EXPERIAN, (Jan. 31, 2016), https://www.experian.com/blogs/insights/2016/01/blockchain-is-the-newbuzzword.

[10] D'Aliessi, *supra* note 9.

[11] Participants can be individuals, organizations, and even things. Sloane Brakeville & Bhargav Perepa, *Blockchain basics: Introduction to distributed ledgers*, IBM (May 09, 2016), https://www.ibm.com/developerworks/cloud/library/cl-blockchain-basics-intro-bluemix-trs. The only condition for participants is the necessity of an internet connection. *Blockchain Technology*, SIA PARTNERS (Oct. 6, 2015), http://en.finance.sia-partners.com/blockchain-technology.

fraud.[12] Network connectivity allows multiple copies of the blockchain to be available to all participants across the distributed network.[13] The decentralized fully distributed nature of the blockchain makes it practically impossible to reverse, alter, or erase information in the blockchain.[14] Blockchains' distributed consensus model, e.g. the network "nodes" that verify and validate chain transactions before transaction execution, make it extremely rare for a fraudulent transaction to be recorded in the blockchain.[15] Blockchain's distributed consensus model allows node verification of transactions without comprising the privacy of the parties. Therefore, blockchain transactions are arguably safer than traditional transactions that require a third-party intermediary validation of the transactions.[16]

Cryptographic hashes further increase blockchain security. Cryptographic hashes are complex algorithms that use details of the existing entirety of transactions of the existing blockchain before the next block is added to generate a unique hash value.[17] That hash value ensures the authenticity of each transaction before it is added to the block. The smallest change to the blockchain, even a single digit/value, results in a different hash value. A different hash value makes any form of manipulation immediately detectable.[18]

Smart contracts and smart property are blockchain enabled computer protocols that verify, facilitate, monitor, and enforce the

---

[12] D'Aliessi, *supra* note 9.
[13] *Id.*
[14] *Id.*
[15] *See, e.g.,* Francois Janinotto, *The Blockchain Explained to Web Developers, Part 1: The Theory*, MARMELAB BLOG (Apr. 28, 2016), https://marmelab.com/blog/2016/04/28/blockchain-for-web-developers-thetheory.html; Razvan Peteanu*, Fraud Detection in the World of Bitcoin*, BITCOIN MAG. (Mar. 26, 2014, 5:50 AM EST), https://bitcoinmagazine.com/articles/frauddetection-world-bitcoin-1395827419/ (noting, "Fundamentally, detecting fraud is hard precisely because it is rare, dynamic and not necessarily obviously fraudulent.").
[16] *See* Michael Crosby et al., *BlockChain Technology: Beyond Bitcoin*, APPLIED INNOVATION REV. (June 2016), http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf.
[17] ERIC PISCINI, BLOCKCHAIN: DEMOCRATISED TRUST 8, DELOITTE U. PRESS (Feb. 24, 2016), https://dupress.deloitte.com/dup-us-en/focus/tech-trends/2016/blockchain-applications-and-trust-in-a-global-economy.html.
[18] Antony Lewis, A Gentle Introduction to Immutability of Blockchains (Feb. 29, 2016), https://bitsonblocks.net/2016/02/29/a-gentle-introduction-to-immutability-of-blockchains.

negotiation and performance of a contract.[19] The term "smart contract" was first introduced by Nick Szabo, a computer scientist and legal theorist, in 1994.[20] An often-cited example for smart contracts is the purchase of music through Apple's iTunes platform.[21] A computer code ensures that the "purchaser" can only listen to the music file on a limited number of Apple devices.[22]

More complex smart contract arrangements in which several parties are involved require a verifiable and un-hackable system provided by blockchain technology.[23] Through blockchain technology, smart contracting often makes contractual legal contracting unnecessary as smart contracts often emulate the logic of legal contract clauses.[24] Merkel trees of these valid smart contracts are

---

[19] *See e.g.,* Alan Morrison, BLOCKCHAIN AND SMART CONTRACT AUTOMATION: INTRODUCTION AND FORECAST, PWC (2016), http://www.pwc.com/us/en/technology-forecast/2016/blockchain/pwc-smartcontract-automation-introduction.pdf; Nicolette Kost De Sevres & Bradley Cohen, *The Blockchain Revolution, Smart Contracts and Financial Transactions*, DLA PIPER (Apr. 26, 2016), https://www.dlapiper.com/en/czech/insights/publications/2016/04/the-blockchainrevolution.

[20] *Smart Contracts: The Blockchain Technology That Will Replace Lawyers*, BLOCKGEEKS, http://blockgeeks.com/guides/smart-contracts (last visited June 16, 2017); *Not-So-Clever Contracts*, ECONOMIST, July 30, 2016, at 53, http://www.economist.com/news/business/21702758-time-being-least-humanjudgment-still-better-bet-cold-hearted.

[21] *See, e.g.,* HORSTEN KOEPPL & JEREMY KRONIK, BLOCKCHAIN TECHNOLOGY—WHAT'S IN STORE FOR CANADA'S ECONOMY AAND FINANCIAL MARKETS? 15 (2017), https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Commentary_468_0.pdf; R. Douglas Vaugh & Anna Outzer, *Understanding How the Block Chain Could Impact the Legal Industry*, LAW 360 (Jan. 11, 2107), https://www.law360.com/articles/879810/understanding-how-blockchain-couldimpact-legal-industry.

[22] Vaugh & Outzer, *supra* note 21.

[23] *See, e.g.*, ETHEREUM, https://www.ethereum.org; Gavin Wood, *Etherium: A Secure Decentralised Generalised Transaction Ledger*, http://gavwood.com/paper.pdf; Luke Parker, *Industry Research Papers Highlight Blockchain Technology's Disruptive Potential*, BRAVE NEWCOIN (July 3, 2016), https://bravenewcoin.com/news/industry-research-papers-highlight-blockchaintechnologys-disruptive-potential.

[24] Mark Anderson, SMART CONTRACTS AND BOCKCHAIN TECHNOLOGY, IP DRAUGHTS (June 18, 2106, 12:14 PM), https://ipdraughts.wordpress.com/2016/06/18/smartcontracts-and-blockchain-technology. *See generally* Josh Stark, *Making Sense of Blockchain Smart Contracts*, COINDESK (June 4, 2016, 18:39 GMT),

combined and included in blocks on the Ethereum blockchain. The Ethereum platform is the leading platform for smart contracting and has a virtual machine that directs the nodes of the blockchain to compute the smart contracts whenever a user makes a valid request.

Ethereum describes smart contracting in this context as follows:

> "Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property. This enables developers to create markets, store registries of debts or promises, move funds in accordance with instructions given long in the past (like a will or a futures contract) and many other things that have not been invented yet, all without a middle man or counterparty risk."[25]

It is Ethereum's goal to provide a platform for writing any sort of contract, business or otherwise, which is automatically enacted without recourse to dispute, i.e., self-executing and self-enforcing. A commonly used example is a smart contract for purchasing music online: A customer might buy the rights to play a song on 5 devices. The contract would automatically determine whether the user is allowed to download the song at any point in the future, based on whether the user has already downloaded the song to 5 devices or not. Ethereum provides a platform for writing and executing such contracts where no legal dispute is possible from any party.

Such a system has serious inherent flaws in its scalability for making more complicated contracts. Within one year of the creation

---

http://www.coindesk.com/making-sense-smart-contracts; Josh Stark, *How Close Are Smart Contracts to Impacting the Real World of Law*?, COINDESK (Apr. 11, 2016, 14:00 GMT), http://www.coindesk.com/blockchain-smarts-crntracts-realworld-law; Ted Mylnar & Ira Schafer, *Why Smart Contracts Will Need 'Smart Term Sheets' to Match*, COINDESK (Dec. 9, 2016, 14:36 GMT), http://www.coindesk.com/smart-contracts-will-need-smart-term-sheets-match. For an example of what startups hope to accomplish with smart contracting, *see* Legalese, https://legalese.com/.

[25] ETHEREUM, *supra* note 23.

of Ethereum, in May 2016 the DAO[26] was created as a smart contract on the Ethereum platform with $150 million US in crowdfunding[27]. The DAO was the first decentralized autonomous organization, intended to work as a venture funding cooperative. One month later a hack sequestered one third of its capital. The month after that Ethereum initiated a hard fork which undid the hack; i.e., the Ethereum blockchain computer code was directly altered to change the DAO smart contract. This was controversial, because it violated the autonomy and decentralization goals of any blockchain. Consequently, Ethereum split into two blockchains, the unedited fork of the chain being called Ethereum Classic. However, new DAOs are already created that fix the former coding shortcomings.

1. Mathematical Principles and Foundations

In this section, we explain the general technical details underlying the function of blockchain architecture. To illustrate the ideas, we will use the specific example of the first blockchain implemented, Bitcoin. Starting from $0 net worth in 2009, the total USD value of bitcoin supply in circulation as of March, 2017 was estimated at greater than $20 billion[28]. What makes the bitcoin blockchain successful is that it is a novel database design which solves several seemingly contradictory requirements:

1. The database gives users absolute privacy.[29] At the same time the complete list of bitcoin transactions is open—anyone with an internet connection can view the entire history of changes in bitcoin ownership following the public key addresses of every bitcoin. This gives users confidentiality and confidence in the value of any transaction with the digital currency.
2. The system is open, in the sense that anyone connected to the internet can participate in editing any part of the blockchain. At the same time, it is highly secure against malicious attacks against the integrity of the information in the whole history of

[26] "The DAO" refers to this first decentralized autonomous organization. "A DAO" refers to other organizations of the same model.

[27] Morgan Peck, *Ethereum's $150-Million Blockchain- Powered Fund Opens Just as Researchers Call for a Halt*, IEEE SPECTRUM (May 28, 2016), http://spectrum.ieee.org/tech-talk/computing/networks/ethereums-150-million-dollar-dao-opens-for-business-just-as-researchers-call-for-a-moratorium.

[28] https://blockchain.info/charts/market-cap

[29] At least within the system this is true via public key cryptography explained in the following section.

its transactions. This gives users short-term confidence in the integrity of the system, because any modern laptop computer can quickly verify the validity of the entire chain.

3. There is no central authority which actively maintains the integrity of the system. At all times, an open system of consensus regulates the building and maintenance of the ledger. At the same time this open and dynamic system responds swiftly and automatically to any changes needed to further secure the data, as computational power changes year to year. This gives users long-term confidence, as larger historical forces such as technological and political changes are removed as factors in the value of the currency.

The goal of this section is to explain how the blockchain architecture achieves these three twin demands. They all rest on two mathematical constructions: public-key cryptography maintains the anonymity of its users, while giving a mechanism for permanently tracking all transactions; and cryptographic hash functions ensure the security and permanence of the data in an open, distributed environment where theoretically anyone can edit the blockchain.

The bitcoin program is a distributed ledger. Being a ledger means it keeps a record of transactions. Each transaction represents the transfer of ownership of one user's bitcoins to other users. Being distributed means the creation and maintenance of the blockchain ledger is accomplished by a network of nodes. The nodes are computers which contain a copy of part or all of the blockchain data. Each block of the blockchain contains a cryptographically secured tree of data bundled together from the transactions within the system which occurred in the last 10 minutes of operation on average. The nodes communicate with each other and maintain consensus on the definition of the official blockchain data, by continuously verifying the integrity of the data in the other nodes. The chain of the blockchain is generated by bitcoin miners who sequentially add blocks which are time-stamped and cryptographically connected to previous blocks in the chain. In addition to maintaining the ledger, many nodes are bitcoin miners which further perform the encryption work necessary to create new blocks. Their work is motivated by transaction fees and newly created bitcoins that occur each time a new block is created.

a) Public-Key Cryptography

Public-key cryptography is a crucial element in building anonymity into blockchain transactions. Public-key cryptography protects every bitcoin user's identity, in the same way that a credit card number is protected when sent over an insecure line to purchase products over the internet.

Public-key cryptography empowers the entire online economy. When consumers make a purchase online, they send valuable personal information through unprotected hubs in the internet, where unknown, potentially malicious agents (hackers) can read the information. In any major vending website, the information is automatically encrypted so that these unknown agents cannot understand the information sent. The vending website can communicate with millions of purchasers in various countries on diverse technological platforms and agree on a secure encryption scheme, even while malicious agents are watching the entire interaction.

In public-key cryptography, the vendor has two complicated numbers, a public key *e* and a private key *d*. The numbers *e* and *d* are very large, seemingly random numbers, but they are chosen carefully so that *any* message can be encrypted and decrypted with two simple operations.

First, the vendor sends out his public key *e* which is seen by everyone, while his private key *d* is kept secret. Secondly, the purchaser encrypts any chosen message *m* with the public key. In the original RSA public-key algorithm, the encrypted message was simply calculated as

$$c = m^e \bmod n$$

by taking the message to the power of the public key under modular arithmetic[30]. Now the encrypted message *c* is a garbled version of the original purchaser's message *m*.

In the third step, the purchaser sends the encrypted message *c* back to the vendor across unsecured lines. The final, crucial step is that the vendor, and only the vendor, can now decrypt the message using the private key *d*. No other choice of number will work. Therefore, if the private key is kept secret, hackers will not be able to decrypt the message without trying all the numbers up until the very

[30]Modular arithmetic sounds difficult, but it is elementary school arithmetic. In particular $a \bmod n$ means the remainder of a upon division by n. For example, $23 \bmod 7 = 2$ since $23 = 7\times3 + 2$ or $164 \bmod 10 = 4$ since $164 = 10\times16 + 4$.

large private key. In the original RSA algorithm, this decryption step works because *d* and *e* are chosen from the beginning with the property that

$$m^{ed} = m \bmod n$$

for any number *m*.

In this RSA scheme the vendor merely takes *c* to the power of *d* in order to decrypt the message, a simple calculation for a computer which takes a fraction of a second. But if a hacker tried to decrypt the message they would have to try a great many numbers to find the correct value *d*, so many that it would take the fastest computer longer than the age of the universe to succeed.

In the case of bitcoin, the owners' identities are protected because the location of every bitcoin is cryptographically secured with a public-key encrypted address, i.e. the location of each bitcoin is a long number, a private key. Since only the owner has the private key, no one else can use that bitcoin for a transaction.

Further, if the owner wants to prove they have a bitcoin without revealing the private key, they could send an encrypted message

$$c = m^d \bmod n$$

and anyone can use the public key *e* for the bitcoin to check the decoded message *m* comes out when taking *c* to the power of *e* since

$$m^{de} = m^{ed} = m \bmod n$$

thus, proving the owner truly has the correct private key. This is called message authentication code, or more specifically, a digital signature. In summary, the private key owner is not required to reveal any private information in order to prove ownership.

In point of fact, the Bitcoin protocol[31] does not use the simple RSA algorithm described above, but instead uses a slight variant called ECDSA (Elliptic Curve Digital Signature Algorithm) to encrypt the addresses of bitcoins. This scheme uses elliptic curve algebra in order to garble the message, but otherwise it is very similar to the RSA method of taking powers of large numbers with modular arithmetic. ECDSA also naturally incorporates a changing scale of encryption strength, which is one minor way bitcoin security responds automatically to improvements in computing power through the years, giving users long term confidence in the system.

The public-key algorithm makes the location and ownership of

[31] https://en.bitcoin.it/wiki/Protocol_documentation#Addresses

bitcoins as perfectly anonymous within the system as is practically possible. Experts are confident this protocol will resist any foreseeable development in computing, such as changes in hardware like the imaginable switch from electronic to quantum computing.[32] As anecdotal evidence of its security, the founder of Bitcoin, who goes by the pseudonym Satoshi Nakamoto, is still unknown, despite owning billions of dollars in bitcoins.

b) Cryptographic Hash Functions

The second mathematical tool that makes blockchains practically realizable is the cryptographic hash function. A hash function takes an input message and deterministically returns a number of fixed length, called the hash. Ideally, a hash function satisfies the following properties:

1. Hashes are easy to calculate.
2. It is difficult to invert a hash.
3. Small changes in the hash value correspond to large changes in the corresponding message.
4. It is unlikely to find two messages with the same hash.

Consider the following toy example of a hash function. Imagine we wish to encrypt and store a list of 100 names. Take each name and convert the letters to numbers:

$$A \rightarrow 1, \ldots, Z \rightarrow 26$$

so

$$\text{John Smith} \rightarrow 10\text{-}15\text{-}8\text{-}14\text{-}19\text{-}13\text{-}9\text{-}20\text{-}8.$$

Remove the dashes and break it into 5 digit chunks:

$$10158, 14191, 39208$$

Add the decimal part of $\sqrt{2} \approx 1.41421$ to each chunk:

$$51579, 55612, 80629$$

Cycle the *n*th chunk *n* digits to the right. The first is cycled 1 digit, the second 2 digits, the third 3 digits:

$$95157, 12556, 62980$$

Sum the chunks and take the remainder upon dividing by 100,000:

$$(95157+12556+62980) \bmod 100{,}000 = 70693$$

The result 70693 is then the toy hash for John Smith.

[32] ARVIND NARAYANAN, ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES (2016).

If we hash all the other names on the list we will have 100 numbers representing the encrypted names. It is easy to see the 4 properties are satisfied: the operations are extremely easy to perform (meaning a computer can compute the algorithm very quickly). It is extremely difficult to guess a name corresponding to any given number. Changing the final letter to the name John Smitt hashes to 84907, so small changes in the message give big changes in the hash. Finally, it is always possible for two messages to give the same hash, but it is extremely unlikely. The likelihood of any two names giving the same hash using our toy hash function is roughly 1 in 100,000 since we've used 5 digits to encrypt the data. So, in a list of 100 names of any size, there is a less than 1% chance any two correspond to the same hash. If we want to decrease this chance we can use more than 5 digits.

The hash function used in bitcoin is called SHA-256 which uses a more complicated scheme of adding, rotating, and threading chunks of numbers, but still restricts itself to such simple computations. SHA-256 gives hashes with 256 bits, meaning there are $2^{256} \approx 1.1579 \times 10^{77}$ different possible hashes under the scheme, a number almost as big as the number of atoms in the observable universe. So, SHA-256 is quite capable of encoding all the transactions that can ever be performed by bitcoin with unique addresses. This ensures the extensibility requirement of contemporary computer science, as the system can theoretically adapt automatically to exponentially multiplying scales of use for centuries. This is a crucial requirement for blockchain applications such as Bitcoin or Ethereum, which hope to become global platforms for business.

c) Transactions and Block Creation

The use of hash functions helps explain the encryption of transactions and the block creation stage of bitcoin. Each transaction in the bitcoin scheme represents the transfer of bitcoins from one user to others. A transaction can correspond to the purchase of a cup of coffee, a new automobile, or the transfer of large amount of stocks from one portfolio to another. Both purchaser and seller need to be guaranteed the proper number of bitcoins have moved from one bitcoin account to another. This is achieved by incorporating the transaction into the blockchain ledger, which happens when it becomes a part of a newly created block.

Each transaction is represented with a numerical address, in the same way John Smith was given the numerical address 70693 in the example above, except each transaction is represented with a 256-digit binary number using the SHA-256 algorithm instead of a 5-digit decimal number using the toy hash.

Every 10 minutes on average a bundle of transactions are encrypted in a block which is added to the blockchain. Bitcoin miners bundle the transactions in a block by hashing the transactions together in a Merkle tree then solving a so-called "proof-of-work" puzzle.

As an example of creating a Merkle tree, imagine we had 4 transactions to hash, A1, A2, A3, and A4. Then we would combine the first two 256 digit addresses A1 and A2 into one address B1 with a hash, and similarly A3 and A4 produce B2. Then B1 and B2 hash to C1. Then C1 is the root of the Merkle tree and represents the bundle of 4 transactions.

Now comes the difficult part for the miner, the proof-of-work puzzle, described as follows: Take three numbers—the previous block's address (P), the current block's Merkle root hash (M), and an arbitrarily chosen number called the nonce (N). Combine the three numbers with SHA-256 to create a resulting hash (R). If the resulting hash R begins with a specified number of 0s, the miner has solved the puzzle and a new block is created and added to the chain with a new address given by hashing its Merkle root and nonce. For any given nonce it is easy to hash P, M, and N to get R. However, it is very unlikely to result in a number with the required number of 0s, so the miner will need to try a large number of nonces before succeeding.

The difficulty of the proof-of-work puzzle is adjusted every two weeks to give an average block creation rate of six times per hour. The difficulty level in July 2016 was set to approximately 20 zeros[33] and it was estimated a miner would need on average 2×10^{17} hashes to find a successful nonce.[34]

Once a miner solves their proof of work puzzle, the results (the previous block's address, the collection of transactions in the block, and the nonce) are published to the network for verification. The other nodes automatically check whether the results are valid, which happens nearly instantaneously because hashing one set of numbers is easy. If the results are valid, the other nodes add the block to their

[33] https://blockchain.info/block/000000000000000002cce816c0ab2c5c269cb081896b7dcb34b8422d6b74ffa1

[34] https://blockchain.info/charts/difficulty

copies of the block chain. The successful miner receives the reward of the newly created bitcoins and any transactional tips. Then a new round of block creation begins. Each miner creates a new Merkle tree from the unused valid transactions (which happens nearly instantaneously because hashing one set of numbers is easy), and they begin their search anew for a successful nonce.

When a new block is created, all of the unsuccessful miners receive no reward for their efforts—they have wasted their energies. Thus, to have any success at bitcoin mining users recognized within the first year that miners needed to combine their efforts. Mining pools were created where rewards are shared amongst members. However, competition quickly grew to the point that today the most profitable bitcoin mining operations use large banks of computers with custom designed hardware, programmed in parallel, in locations where energy for operation and cooling is almost free, such as Tibet and Iceland.

d) Ethereum – Proof-of-Stake

An open distributed database can be adapted for other purposes beyond digital currencies. In July 2015, Ethereum created the most significant new public blockchain since Bitcoin. Ethereum's major innovation is Turing complete scripting functionality.[35] As opposed to Bitcoin transactions which are simple records of transfer of ownership of digital currency, Ethereum transactions are executable computer programs, called smart contracts.[36] Each node contains protocol for a virtual machine which can execute these programs. To guard against spam (anyone can ask the network to run any program added to the blockchain) users must pay for each step of each program they call with Ethereum's digital currency, Ether (ETH).

Another variation on the Bitcoin blockchain protocols that is

[35] A transaction in bitcoin is represented with a 256 digit binary number. Even under this protocol, much more information than a history of monetary transfers can be stored. The number 2^{256} means each atom in our galaxy can be given a unique address. Any information or instructions we can imagine can be encrypted as transactions in a blockchain. The physical actions of every person on earth for every second for the next billion years, if they can be recorded, can be stored eternally on the blockchain without running out of space.

[36] Smart contracts are self-executing, self-regulating agreements between users of the blockchain. For example, a smart contract might automatically release funds or ownership documents once both parties agree stipulations have been fulfilled. The goal is to reduce (almost entirely) associated intermediary costs of traditional contracts, such as negotiation, enforcement, and arbitration.

gaining traction is a change from proof-of-work mining to proof-of-stake mining. One problem with proof-of-work mining is that there are significant externalities. Before the publication of this article, the total energy costs for running the global network of computers devoted to solving the proof-of-work puzzles was estimated at around $700 million USD per year. Each transaction with bitcoin currently uses as much energy as a typical American household uses in 5 days.[37] This enormous energy consumption created an urgent motivation to find a better solution.

To this end, Ethereum announced its intention to institute CASPER, a proof-of-stake consensus protocol, to be adopted in late 2017. It has not been finalized as of this writing, but the general idea given by Ethereum founder Vitalik Buterin, is for Ethereum stakeholders to create blocks with their own security deposits attached. Whenever the system finds irregularities associated with a block creation, the stakeholder causing the irregularities is punished by losing their stake/deposit. If it can be designed in a way that prevents the many attacks that have been enumerated against past proposals, then proof-of stake block creation will eliminate much of the energetic externalities of the blockchain.

e) Technical Summary

With the use of public-key cryptography and cryptographic hash functions, blockchain architecture gives its users long term confidence in anonymity, security, and decentralized autonomy.

Users' accounts are encoded by private keys, so their information is securely encrypted. They have complete power over whether they share information and with whom. When sharing generic information, such as the fact that they own more than 10 bitcoins, they reveal no private information. Further, each time a transaction is made, a new private key can be made. So, while we can track the public key of the addresses of each transaction, and that information is stored eternally in the blockchain, each transaction allows for an entirely new private identity which is cryptographically secured. This gives more anonymity in business transactions than ever before imagined.

No outside, centralized agency can exert any type of independent power over the blockchain ledger, because it is decentralized, autonomous, and secured by the proof-of-work energy

[37] CITE http://digiconomist.net/bitcoin-energy-consumption retrieved 6/26/17.

expenditure of the entire planet.

Since a blockchain is decentralized, governmental powers cannot exert authority over its growth or maintenance. If the U.S. government attempted to exert power over the system by influencing any number of individuals within their jurisdiction, they would need complete control of 51% of the anonymous global users before they could change any part of the code.

The system is autonomous, so even assuming a government did find some of the anonymous individuals whose work maintains the ledger, it would be difficult to argue personal responsibility for any crime. The miners are simply running a universal algorithm which was created in 2009.

Finally, and most importantly, the very security of the system guarantees no outside power will ever have the ability to control the blockchain. Anyone wishing to change the autonomous growth of the blockchain for their own purposes needs to outcompete the entire global network in the proof-of-work cryptographic hash function puzzles. Even if a major power attempted to take that extreme action, users would instantly know about the takeover due to the openness of the blockchain. In that event it would lead to a loss of confidence and ultimate failure of the entire structure. So, the agency would not control the blockchain, they would merely destroy it. Thus, no centralized agency, not the General Secretary of the People's Committee of China, not the Federal Assembly of the Russian Federation, nor the entire judicial branch of the United States, will ever have the ability, much less the authority, to dictate any changes to a public blockchain.

2. Regulatory Recognition

Regulatory recognition of blockchain technology in the United States is still largely unsettled. The United States Financial Industry Regulatory Authority (FINRA) has issued a report,[38] establishing a common basis for a dialogue with market participants, raising a multitude of questions, without providing specific answers. The U.S. Commodity Futures and Trade Commission (CFTC), compared the blockchain technology to the internet revolution and supported a "do no harm" approach in regulating blockchain technology. The CFTC

[38] FIN. INDUS. REGULATORY AUTH., DISTRIBUTED LEDGER TECHNOLOGY: IMPLICATIONS OF BLOCKCHAIN FOR THE SECURITIES INDUSTRY (2017), http://www.finra.org/sites/default/files/FINRA_Blockchain_Report.pdf

opined that this approach promoted at the time of the internet transformation by the American administration was successful and should be applied to blockchain.[39]

The states of Arizona, Vermont, and Delaware have launched specific regulatory initiatives. Delaware launched the Delaware Blockchain Initiative in 2016, to maintain its leading role in the context of corporate governance.[40] Arizona passed the so-called "Blockchain Bill"[41] into law, which provided specific regulation for electronic signature, blockchain, and smart contracts. The law now expressly defines blockchain[42] and smart contracts.[43] It also recognizes "a signature … secured through blockchain technology" as equivalent to an electronic signature in an electronic form and "a record or contract secured through blockchain" as equivalent to an electronic record in an electronic form, as well as the existence of smart contracts.[44]

The state of Vermont adopted a more prudent approach. The state report "Blockchain Technology: Opportunities and Risk"[45] considered that "at present, the costs and challenges associated with

---

[39] J. Christopher Giancarlo, CFTC Commissioner, Special Address Before the Depository Trust & Clearing Corporation 2016 Blockchain Symposium (Mar. 29, 2016), http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-13.

[40] *See* Andrea Tinianow, *Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance*, HARV. L. SCH. F. ON CORP. GOVERNANCE & FIN. REG., (Mar. 16 2017), https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance.

[41] Act of Mar. 29, 2017, ch. 97, 2017 Ariz. Sess. Laws, https://apps.azleg.gov/BillStatus/GetDocumentPdf/452616 (to be codified at Ariz. Rev. Stat. §44-7003) (making a signature on a blockchain a legal signature under Arizona law).

[42] *Id*. "*"blockchain technology" means distributed ledger technology that uses a distributed, decentralized, shared and replicated ledger, which may be public or private, permissioned or permissionless, or driven by tokenized crypto economics or tokenless. The data on the ledger is protected with cryptography, is immutable and auditable and provides an uncensored truth*".

[43] *Id*. "*"Smart Contract" Means An Event-Driven Program, With State, That Runs On A Distributed, Decentralized, Shared And Replicated Ledger And That Can Take Custody Over And Instruct Transfer Of Assets On That Ledger*".

[44] *Id*. "*a contract relating to a transaction may not be denied legal effect, validity or enforceability solely because that contract contains a smart contract term*"

[45] JAMES CONDOS, WILLIAM H. SORRELL, & SUSAN L. DONEGAN, BLOCKCHAIN TECHNOLOGY: OPPORTUNITIES AND RISK (2016), http://legislature.vermont.gov/assets/Legislative-Reports/blockchain-technology-report-final.pdf

the use of blockchain technology for Vermont's public recordkeeping outweigh the identifiable benefits."[46] The report also emphasized the relevance of recognizing blockchain technology, that would determine "a 'first mover'" advantage with the potential to bring economic activity surrounding the development of blockchain technology to Vermont", remarking the uncertainty around such potential as, "difficult to quantify and challenging to capture due to the nature of the technology."[47] For the moment, Vermont has recognized the possibility to use blockchain in the context of a trial under specific conditions.[48]

Several pending legislative proposals may increase the recognition of blockchain technology under existing law. In early 2017, legislators throughout the United States introduced legislation to explore virtual currency and blockchain technology. While some states evaluate opportunities for the technology to boost the local economy, other states are implementing specific use cases.[49]

---

[46] *Id.*
[47] *Id*.
[48] *See* VT. STAT. ANN. tit. 12, § 1913. The Statute defines "blockchain technology" as "a mathematically secured, chronological, and decentralized consensus ledger or database, whether maintained via internet interaction, peer-to-peer network, or otherwise".
[49] Illinois
Legislation: House Resolution 120
Sponsor: Representative Michael Zalewski (D)
Introduced on February 8 2017, H.Res. 120 creates a Legislative Blockchain and Distributed Ledger Task Force to "study how and if [s]tate, county, and municipal governments can benefit from a transition to a blockchain
New Hampshire
Legislation: House Bill 436
Sponsors: Representatives Barbara Biggie (R) and Keith Ammon (R)
Introduced on January 5, 2017, HB 436 amends New Hampshire's Licensing of Money Transmitters statute to specifically address virtual currency issues. The bill defines virtual currency as "a digital representation of value that can be digitally traded and functions as a medium of exchange, a unit of account, or a store of value but does not have legal tender status as recognized by the United States government."
Hawaii
Legislation: House Bill 1481
Sponsors: Representatives Chris Lee (D) and Mark Nakashima (D)
Introduced on January 25, HB 1481 "establish[es] a working group consisting of representation from the public and private sectors to examine, educate, and promote best practices for enabling blockchain technology to benefit local industries, residents, and the State of Hawaii."
24

III. Jurisdiction Over Blockchain

Vermont
Legislation: Senate Bill 59
Sponsor: Senator Ann Cummings (D), Representative William Frank (D)
Introduced on February 1, 2017, SB 59 focuses on the need "to amend and establish laws pertaining to consumer litigation funding companies; licensed lenders; money servicers; debt adjusters; and loan servicers." To accomplish that, the bill adds a definition of virtual currency to the state's money services statute (8 V.S.A. § 2500 et seq.): "stored value that (A) can be a medium of exchange, a unit of account, or a store of value; (B) has an equivalent value in money or acts as a substitute for money; (C) may be centralized or decentralized; and (D) can be exchanged for money or other convertible virtual currency."
Washington
Legislation: Senate Bill 5264
Sponsors: Senators Steve Conway (D) and Ann Rivers (R)
Introduced on January 18, 2017, SB 5264 seeks to amend Washington's Uniform Controlled Substances Act to restrict the use of virtual currency for the purposes of marijuana sale and distribution. The bill "prohibits a marijuana producer, processor, or retail outlet from paying with or accepting virtual currency for the purchase or sale of marijuana or marijuana products."
Arizona
Legislation: House Bill 2216
Sponsor: Representative Paul Boyer (R)
Introduced on January 17, 2017, HB 2216 would make it "unlawful to require a person to use or be subject to electronic firearm tracking technology or to disclose any identifiable information about the person or the person's firearm for the purpose of using electronic firearm tracking technology."
Arizona
Legislation: House Bill 2417
Sponsor: Representative Jeff Weninger (R)
Introduced on February 7, 2017, HB 2417 provides that smart contracts written on a blockchain are essentially equivalent to all other forms of contracts. The bill defines blockchain technology and smart contracts and then states that transactions based on these self-executing contracts could not be "denied legal effect, validity, or enforceability" because of the smart contract term. Further, any signature recorded on the blockchain would be equated to a legal signature under Arizona law and would be "considered to be in an electronic format and to be an electronic record." Lastly, the bill states individuals who own or have the right to use information they place on the blockchain retain those rights.
While most of the foregoing bills are at an early stage, and do not comprehensively regulate virtual currency or blockchain technology, it is encouraging that legislators on both sides of the aisle are increasing their focus on issues relating to this technology.

The lack of regulatory recognition of Blockchain technology creates uncertainty for the blockchain community. The lacking recognition hinders the implementation of the technology across industries and undermines infrastructure conversion via blockchain technology. The regulatory uncertainty derives from insufficient or non-existent regulatory guidance, sparse court decisions, uncertainty over jurisdiction, and a sense in the user community of interacting in an environment that is generally free of law. As the technology applications grow and the value of crypto currencies rises, the evolution of blockchain-based crypto economy will depend to some extent on users' trust in the efficacy of blockchain-based dispute resolution mechanisms and the immutability of the technology.

Courts have not yet recognized blockchain technology or addressed legal implications of blockchain-based applications. For the most part, the technology industry agrees that Blockchain technology is immutable and secure.[50] However, a review of published court opinions suggests that no court has had to review, assess, or scrutinize the uses and applications of blockchain technology at the time of publication of this article.[51] Thus creating uncertainty in how courts may perceive and treat blockchain technology.[52] While some judges are technology novices that could misunderstand and misinterpret the new technology, the technology is arguably no different from other virtual software that courts have evaluated.[53] Similarly, blockchain

[50] Ben Dickson, *Blockchain's Brilliant Approach to Cybersecurity*, VENTUREBEAT (Jan. 22, 2017), https://venturebeat.com/2017/01/22/blockchains-brilliant-approach-to-cybersecurity.

[51] A search of "blockchain" or "block chain" in federal and state cases on Westlaw reveals that only two cases have mentioned blockchain technology. The courts in both cases refused to discuss blockchain in depth, and did not take a position on the legitimacy of the technology. *See In re Dole Food Co., Inc. Stockholder Litigation*, C.A. No. 8703–VCL, 2017 WL 624843 at n. 1 (Del. Ch. Feb. 15, 2017); *United States v. Petix*, 15-CR-227A, 2016 WL 7017919 (W.D. N.Y. Dec. 1, 2016).

[52] "While countless undisputed transactions utilizing smart contracts are likely to move forward on the basis of such automatic, electronic enforcement, there will likely always be the need for human intervention to settle legal disputes." Reggie O'Shields, *Smart Contracts: Legal Agreements for the Blockchain*, 21 N.C. BANKING INST. 177 (2017).

[53] Ronald L. Chichester, *Wide Open Spaces*, 80 TEX. B. J. 228 (2017), https://www.texasbar.com/AM/Template.cfm?Section=articles&Template=/CM/HTMLDisplay.cfm&ContentID=36379 ("There is no reason to think that links within a blockchain could not be admissible in court. While an expert may be needed to opine on the authenticity of the particular blockchain and the specific transaction,

ledgers do not exist in a physical sense, and therefore have no specific location.[54] The nodes in the blockchain network can be located all over the world, and therefore arguably blockchain transactions can be subject to the legislation of any given node in the network.[55] Moreover, it may be difficult to identify parties to transactions recorded to the blockchain.[56]

1. Traditional Jurisdictional Means

In American law, the term jurisdiction has two distinguishable meanings with a correlating authority: personal jurisdiction and subject matter jurisdiction. Generally, jurisdiction may refer to the geographic distribution of disparate courts of particular levels[57] or it may refer to the official power of a court to exercise judicial authority over a particular matter.[58] To hear a case, courts are required to have both personal jurisdiction and subject matter jurisdiction.

Personal jurisdiction refers to whether a court has power over the person being sued. Personal jurisdiction has four major categories

---

there is nothing inherently different about blockchains than other software programs.").

[54] María Tena, *7 Regulatory Challenges Facing Blockchain*, BBVA (Jan. 16, 2017), https://www.bbva.com/en/news/economy/financial-and-commercial-services/fintech/7-regulatory-challenges-facing-blockchain.

[55] Gregory Brandman & Samuel Thampapillai, *Blockchain – Considering the Regulatory Horizon*, OXFORD BUS. L. BLOG (July 7, 2016), https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/blockchain-%E2%80%93-considering-regulatory-horizon.

[56] O'Shields, *supra* note 52; *also see* Catherine Martin Christopher, *The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain*, 17 NEV. L.J. 139, 180 (2016).

[57] *Jurisdiction*, BLACK'S LAW DICTIONARY (10th ed. 2014). Only one Supreme Court exists, the court of appeals is divided into 13 circuits, and there are 94 district courts. *Court Role and Structure*, UNITED STATES COURTS, http://www.uscourts.gov/about-federal-courts/court-role-and-structure (last visited June 16, 2016). In addition, each state court system comprises its own "jurisdiction.".

[58] Although the term most often is used in connection with the jurisdiction of a court over particular matters, one may also speak of matters being within or beyond the jurisdiction of any other governmental entity.

in case law: 1. Physical Presence,[59] 2. Domicile/Place of Business,[60] 3. Consent,[61] and 4. Minimum Contacts.[62] The doctrine of personal jurisdiction via minimum contact with a state has become more complex and circumstantial in the age of the internet. Citing *International Shoe*, courts apply a sliding scale to determine personal

[59] CHARLES ALAN WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE § 1064 - 1065 (4th ed. 2015). e.g. Physical presence in a state can grant courts jurisdiction over a person. A person being served with a copy of the summons and complaint while physically present in the forum state is sufficient to give a court in that state jurisdiction over the person who was served. That means that even if a person was just passing through the state for a few minutes, if the person was properly served, that person can be sued in that state.

[60] CHARLES ALAN WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE § 1069.2 (4th ed. 2015). e.g. The domicile or place of business of a person or business in a state can grant courts jurisdiction over the person or business. Domicile or residence in a state is enough to give courts in that state jurisdiction over a person. This also applies to wherever a person establishes a place of business. In practice, this means that even if the incident took place in another state or even in another country, a person can always be sued in the state in which the person has established residence or maintain a place of business.

[61] CHARLES ALAN WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE § 1067.3 (4th ed. 2015). e.g. "Persons can simply consent to a court having personal jurisdiction over the person. Consent comes in two basic forms, express and implied. Express consent can be given by voluntarily appearing before the court and submitting oneself to its jurisdiction. This means that even if a court otherwise had no power over a person, by showing up, a person can grant the court that power. Consent also can be implied, and one of the most common forms of implied consent is by driving on the roads of that state. Courts consider a person to have given implied consent to the laws regulating roads, and thus if a person has a car accident on the road in that state, a court has personal jurisdiction over that person."

[62] CHARLES ALAN WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE § 1067.2 (4th ed. 2015). *See*, *Burger King v. Rudzewicz*, 471 U.S. 462 (1985) (finding jurisdiction because of a "substantial and continuing relationship" between the franchisee in the forum and the franchise in the home office and not because of presence in the forum); *Zippo Mfg. Co. v. Zippo Dot Com, Inc.,* 952 F. Supp. 1119 (W.D. Pa. 1997) (maintaining that a passive Web site is not sufficient for personal jurisdiction).

"A court can also have personal jurisdiction over a person if the person maintains certain "minimum contacts" with the state where a court resides. Minimum contacts is somewhat of a catchall where a court decides that a person had enough interaction with a state to justify having personal jurisdiction over that person. The United States Supreme Court set forth a basic test to determine whether a particular person has established minimum contacts with that state/ Jurisdiction is permissible when the defendant's activity in the forum is continuous and systematic and the cause of action is related to that activity." *Int'l Shoe Co. v. Wash.,* 326 U.S. 310 (1945).

jurisdiction in the context of the internet.[63] Courts weigh whether the defendant does business over the internet[64] versus whether the information is merely accessible by residents of the jurisdiction.[65] If a court cannot exercise personal jurisdiction over a person, it may have in rem jurisdiction, which gives it jurisdiction over things, e.g. a piece of property owned by a person.[66]

Subject matter jurisdiction refers to whether a court can hear a case on a particular subject. Litigants can waive personal jurisdiction but cannot waive subject-matter jurisdiction. Subject-matter jurisdiction means that a given court can only exercise power over a claim that the laws of the jurisdiction authorize such court to hear.[67]

Under the Constitution of the United States, plaintiffs who wish to sue in federal court must find a constitutional or congressional grant of subject-matter jurisdiction to permit a federal court to hear the claim.[68] Diversity jurisdiction generally allows litigants to bring

---

[63] *Zippo*, 952 F. Supp. at 1124.

[64] *Id*. "If the defendant enters into contracts with residents of a foreign jurisdiction that involve the knowing and repeated transmission of computer files over the internet, personal jurisdiction is proper." Id. ref. *Compuserve, Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996).

[65] *Zippo*, 952 F. Supp. at 1124.

[66] CHARLES ALAN WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE § 1070 (4th ed. 2015). e.g. "This means that if a person owns property in another state, even though such person could not otherwise be sued there, the court does have jurisdiction over such property which in effect gives it power over to such person. However, in rem jurisdiction is considerably more limited than personal jurisdiction, because the lawsuit generally has to concern the property itself and damages are often limited to the fair market value of the property. This means that in practice, buying a house in another state would grant a court jurisdiction to hear a dispute regarding that house, but not necessarily regarding other disputes that involve the owner of that house."

[67] CHARLES ALAN WRIGHT, ET AL., FEDERAL PRACTICE AND PROCEDURE § 3522 (4th ed. 2015). "For instance, the United States Tax Court to cases related to taxation; thus, that court does not have subject-matter jurisdiction over any other matter. Most state courts are courts of general jurisdiction. That is, state courts are presumed to have power to hear virtually any claim arising under federal or state law, except those falling under the exclusive jurisdiction of the federal courts. However, for pragmatic reasons some states deny subject matter jurisdiction to specific claims, such as those arising in other states. In addition to courts of general jurisdiction, most states also maintain specialized courts of limited subject-matter jurisdiction. Examples of these types of courts include probate courts, traffic courts, juvenile courts, and small claims courts." E.g.

[68] U.S. CONST. art. III. § 2. Generally speaking, courts construe congressional grants of subject matter jurisdiction narrowing, resolving "ambiguities against the

claims in federal court if such claims exceed the total of $75,000 and the parties are citizens of different states.[69] Federal question jurisdiction, on the other hand, permits a litigant to bring a claim in federal court if such claim arose under federal law, including the U.S. Constitution.[70] Finally, claims over which a federal court would not have subject-matter jurisdiction independently can be adjudicated via supplemental jurisdiction, which permits a federal court to hear a claim, based on that claim's connection to an associated claim over which the federal court does have jurisdiction.[71]

2. Shortcomings of Traditional Jurisdictional Means

To appreciate the distinct nature of blockchain transactions and the specific legal issues they create for the application of traditional jurisdictional means, it helps to compare traditional internet transactions with blockchain-based smart contracting.

Traditional internet transactions are characterized by several attributes that make them fully accessible to traditional jurisdictional analyses. First, the parties of a traditional internet transaction are typically known, either by each other or by the provider or third-party service providers. If parties should not be known, the IP address of a given computer involved in an internet transaction will likely be known. Moreover, the location of property details will likely be available and/or known as well as the payment details used, e.g. PayPal, Apple Pay, and traditional credit cards. These payment structures are centralized and accessible. Traditional internet transactions use the legacy systems in the existing infrastructure with fiat currencies, not crypto currencies. Moreover, other traditional contracting mechanisms are also used including traditional legal tools but in electronic form. Finally, traditional internet transactions are characterized by the use of centralized server networks, not decentralized distributed networks.

By contrast, blockchain-based smart contracting is characterized by diametrically opposed parameters. First, the parties

---

assumption of jurisdiction". *Mars Inc. v. Kabushiki-Kaisha Nippon Conlux*, 24 F.3d 1368, 1373 (Fed. Cir. 1994).

[69] 28 U.S.C. § 1332. "For instance, if a citizen of New York sues a citizen of California for more than $75,000, a federal court would have subject-matter jurisdiction to hear that claim."

[70] 28 U.S.C. § 1331.

[71] 28 U.S.C. § 1367 provides for supplemental jurisdiction in federal courts.

are not necessarily known thus the IP address of a given computer involved in an internet transaction will likely not be known either. For example, the use of virtual private networks (VPN) and cryptography routinely make it impossible to identify the identities of smart contracting parties or computer networks / individual systems. Moreover, payment details like those of a credit card or the location of property may not be known in smart contracting because parties may decide to use cryptocurrencies, such as bitcoin. Bitcoin is also decentralized and autonomously run, so no governing body exists for which a court might access and demand restitution. Further, blockchain smart contracts are self-executing and self-regulating, i.e. all terms and parameters are coded and only executed and added to the given blockchain if and when all parameters of the smart contract have been fully executed. Traditional contracting mechanisms and their legal forms are typically not involved. The intermediation of traditional legal infrastructure is completely removed in smart contracting because the system that executes the contract (the blockchain) is autonomous and decentralized. Therefore, the blockchain cannot be coerced into any sort of remediation.

Traditional jurisdictional means have limited applicability in the context of Blockchain technology. Jurisdiction over the public blockchain does not exist within the present doctrinal infrastructure for jurisdiction. In practice, the blockchain itself cannot be regulated or governed because it is decentralized and autonomous. No traditional jurisdictional principles can apply because the blockchain is a mere collection of agreed upon calculations by decentralized computer systems. The blockchain is merely an idea reached by the consensus of computation; it is pure information, contained only in the mathematical rules of its inception and the sum of the computation. The blockchain is entirely maintained and owned by a distributed group of anonymous users located throughout the planet who would not likely recognize or comply with any legal authority.

The concept of location or presence in jurisdictional means does not apply to the blockchain. A location for the blockchain does not exist - not physically or even electronically. Nodes that contain the blockchain and all of its information are located all over the world. Transactions in the blockchain are fully networked and “present” only in cyberspace. The nodes hold imperfect partial copies of the blockchain; no particular node holds the entire blockchain.

a) Anonymity of Blockchain Transactions

The lack of identifiable parties in crypto transactions creates a distinct separation between real world and crypto transactions that has lasting implications for the application of existing jurisdictional principles. The aforementioned anonymity gained by the use of public-key encrypted identities and VPNs prevents the identification of the parties to a smart contract. Without identifiable parties, jurisdictional principles such as subject matter jurisdiction, personal jurisdiction, diversity jurisdiction, and federal question jurisdiction become irrelevant. To illustrate this point, proving personal jurisdiction by means of 1. Physical Presence, 2. Domicile/Place of Business, 3. Consent, and 4. Minimum Contacts becomes impossible as none of these elements are known of the parties in a smart contract. Physical presence is anonymous, as is domicile, consent, and minimum contacts. Subject-matter jurisdiction, e.g. a given court can exercise power over a claim that the laws of the jurisdiction authorize such court to hear, is inapplicable because no given law would be able to authorize such power. But even if a given State or even the Federal Government were to pass a law that would grant such authority to a court, it is hard to see how the court would in fact exercise such authority, short of limiting access to the internet itself.

Public-key encryption in blockchain transactions secures consumers. The lack of oversight in blockchain-based crypto transactions goes well beyond the government. In fact, those who may attempt to circumvent the existing regulatory framework are also restricted from interfering with blockchain-based smart contracting transactions. Hackers who watch people online sending their credit card information to online retailers, etc., may use their informational advantage to break the law and defraud consumers. However, hackers are unable to execute such fraudulent transactions in blockchain transactions among consumers. Like the government or any other authority, hackers are unable to interfere in blockchain because of public-key encryption.[72]

[72] Cryptographically secured (like public-key encryption or the hash functions at the basis of blockchain) is secure, i.e. secure enough for banks to trust operations with customers' encrypted bank account and social security numbers. When consumers send information over the internet, nearly anyone can get that information because it travels through many uncontrolled nodes. But, public-key encryption guarantees that anyone reading the information cannot understand it unless they were accepted by the respective consumer to have the key. If hackers could break public-key

Not all smart contracts are fully anonymous and untouchable by traditional jurisdictional means. Some smart contracts will not automatically anonymize the parties because there is a physical element to such a consumer contract. For example, service contracts involving a peer-to-peer transportation contract that is executed on the blockchain will not be anonymous because the passenger will be physically present for such a transaction. Other smart service contracts can be completely anonymous. For instance, a service contract involving services pertaining to cyberspace, such as programming services to create a given webpage, will be completely anonymous. It is important to note that as the technology becomes more widely accepted, such service contracts are going to become a highly important part of any given economy.

Even outside of cyberspace services, it is clearly possible that bounties for anonymous work executed via smart contracts will make traditional service contracts that require personal knowledge and physical appearance redundant. A bounty contract for anonymous work allows an anonymous person to put a bounty on a given job and offer such job on an anonymous smart contracting network to an anonymous counterparty. The contract acceptance and performance is dictated to some extent by reputational factors that link the counterparty and the performance under the contract.

b) Enforcement of Smart Contracts

The enforcement of smart contracts with traditional legal means is limited. First, disputing a smart contract with traditional means (in court, arbitration, mediation, etc.) is only marginally possible because of the aforementioned anonymity in blockchain transactions. Moreover, while smart contracts are coded as self-executing contracts, they do not necessarily provide effective mechanisms for enforcement if one party breaches his or her obligations in the smart contract. Arguably, breach of a smart contract is not even possible, the contract simply will not execute if a parameter is not fulfilled.

The literature is split on remedies for breaches of smart contracts. Some argue that because the smart contract replaces the existing legal contract in some circumstances, the smart contract will

encryption they would instantaneously be able to influence and control a significant proportion of the existing wealth of nations.

be governed by the same legal principles as the existing legal contract.[73] Others argue that the breaching party may not live in an area where the courts have jurisdiction, thus the breaching party cannot be liable.[74] In that case, assuming the operator[75] knows identities of contracting parties, the operator of the blockchain platform should have a legal obligation to identify who the breaching party was and serve as the counterparty in a dispute scenario.[76] These experts argue the operator of the blockchain should establish governing rules of the blockchain and specifications for dispute resolution.[77] However, these specifications would have to be disclosed upfront and agreed upon by the parties to the smart contract in order to be enforceable.

Courts may be substantially challenged in interpreting smart contracts. Unlike the interpretation of a contractual dispute in the existing legal infrastructure where courts will assess what the contentious language in a given contract may mean to a reasonable human observer, smart contracts are not coded for a human observer. Rather they are intended for computer programming in a network of nodes (and in the future for artificial intelligence). To the extent that

---

[73] Cheng Lim, et al., *Smart Contracts: Bridging the Gap between Expectation and Reality*, OXFORD BUS. L. BLOG (July 11, 2016), https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smart-contracts-bridging-gap-between-expectation-and-reality; Martin von Haller Gronbaek, *Blockchain 2.0, Smart Contracts, and Challenges*, BIRD & BIRD (June 16, 2016), https://www.twobirds.com/en/news/articles/2016/uk/blockchain-2-0--smart-contracts-and-challenges; Josh Stark, *Making Sense of Smart Contracts*, COINDESK (June 4, 2016), http://www.coindesk.com/making-sense-smart-contracts

[74] Alexander Savelyev, *Contract Law 2.0: 'Smart' Contracts as the Beginning of the End of Classic Contract Law*, 26 INFO. & COMM. TECH. L. 116 (2017).

[75] However, in general blockchains, and in the most important cases of bitcoin and Ethereum, there is no "operator of the blockchain" except the entire democratic community, and there is no way for them to determine the identities of the parties, nor would they (ideally) be able to intervene in the blockchain.

[76] O'Shields, *supra* note 52 at 191; SAMUEL BOURQUE & SARA FUNG LING TSUI, A LAWYER'S INTRODUCTION TO SMART CONTRACTS 13 (2014), https://github.com/joequant/scms/blob/master/doc/pdfs/A%20Lawyer's%20Introduction%20to%20Smart%20Contracts.pdf.

[77] O'Shields, *supra* note 52 at 191. Riika Koula, *Blockchains and Online Dispute Resolution: Smart Contracts as an Alternative to Enforcement*, 13 SCRIPTED 40 (2016), https://script-ed.org/wp-content/uploads/2016/05/koulu.pdf; SEAN MURPHY, UNNBLOCKING THE BLOCKCHAIN: A GLOBAL AND LEGAL REGULATORY GUIDE 34, (2016), http://www.nortonrosefulbright.com/files/unlocking-the-blockchain-chapter-1-141574.pdf.

consumers are using smart contracts, the human element may be increased via the coding of graphical user interfaces. The basic premise of smart contracting remains emphasized on computer programming (and in the future artificial intelligence) not human interaction. Because of the emphasis on code for computer programming (and artificial intelligence), courts may not be able to hypothesize a reasonable human's interpretation of a given smart contract. Courts may also be limited in their ability to consult programmers to interpret the coded language at issue in a given case because the meaning and logical reasoning of coded language is substantially different from human language.[78]

From an evidentiary perspective, it is unclear who would own smart contracting blockchain contributions and whether there would be any applicable protections, such as work product or confidentiality. Without ownership rights for a blockchain transaction, it is also unclear who would be able to claim privileged information or how discovery would operate via existing laws. However, when the parties to a smart contract choose to reveal their identities, arguably privileged information or discovery laws should apply as if it was a written contract despite the fact that the contract was written in code.

Contract law remedies may not apply to smart contracts which raises possible enforceability issues. If a transaction in a smart contract fails to be completed or is partially completed but not added to the blockchain,[79] it is unclear how liability will be allocated if those

[78] Code is substantially different from human language. Code typically entails no ambiguity, no variant interpretation is possible. The computer just executes the code as written. A programmer can make an interpretation of the intention behind another programmer's code—whether they were trying to fraudulently take money from the other party in the smart contract. But in a very real sense, the contract is perfect, if the victim entered the contract, they did so with all the information at hand. Fraud is arguably im*possible*, in the sense that computer programs cannot lie—they do exactly what their instructions tell them to. Therefore, arguably deception is impossible. Of course that is merely academic, because coders can deliberately create very complicated code that confuses people in order to gain undue advantages.

[79] Two interpretations are possible for incomplete transactions: First, an Ethereum transaction is a complete smart contract. Therefore, the whole contract is either added to the blockchain or not. An Ethereum transaction can't be partially added to the blockchain. The second interpretation is the contract transactions between the parties. It is possible that parties can partially fulfil a smartcontract. But in that case the smart contract already has all eventualities accounted for—it is completely self-executing and self-regulating. Therefore, if one provision of the contract is fulfilled and another is not, the consequences of that situation is already stipulated in the code

eventualities have not been accounted for in applicable code. Because of the blockchains decentralized nature, it is unclear who or what is accountable and could require regulation. Without solutions for those issues, liability for failed transactions or conflicts between parties have little guidance as to being resolved.

c) Limited Regulatory Oversight

The regulatory oversight over blockchain-based transactions is severely limited. Courts arguably cannot have jurisdiction over blockchain-based smart contracts because it is unlikely a court could find out who transacted via the anonymized blockchain. Furthermore, the court could not change or otherwise affect the transaction as it was coded because once the coded parameters were fulfilled the transaction auto executed on the blockchain. Because of automated execution, contractual breach and damages are less likely to occur in smart contracts, especially as compared to traditional contracts. If a given smart contract transaction disadvantages one of the contracting parties, courts would have to change the blockchain in order to institute remedies in the traditional sense that could pertain to the smart contract in question. However, that scenario is computationally and practically impossible.

Assuming the parties to a given smart contract were known, courts could require the parties to create a new transaction to reverse undesirable outcomes of the coded and executed transaction that was disputed. This is a possible solution because courts are unable to affect the initial outcome of a disputed smart contract transaction. Courts cannot require a retroactive change in the blockchain because that is computationally near impossible. Given that the requirements for a court to exercise jurisdiction over a disputed smart contract are fundamentally different from courts' jurisdiction over contracts in the existing legal infrastructure, contracting parties would likely second guess courts' decisions pertaining to smart contract disputes. In other words, real world court decisions even if attainable may not have the same legitimacy and authority as other intra-blockchain dispute resolution mechanism may have. In summary, courts would only be able to force the parties to execute a secondary transaction or otherwise pay remedies for a smart contract that created damages for

with mathematical inevitability. Whatever the program stipulates will happen, happens; including if nothing happens.

one of the parties. Courts would not be able to actually change or interpret the terms of the given smart contract that was executed according to its parameters and added to the blockchain where it is immutable.

Because of these inherent limitations, courts will generally not be able to effectuate resolutions to disputes arising from blockchain-based smart contracts. Courts do not have the power over the coder and the code that was used by the parties that may have been injured. Courts do not have the authority to dictate to a programmer how, when, and where to change the existing code used by consumers. Even if courts were given such authority, no programmer so coerced by the court would be able to override the will of the majority of anonymous international blockchain users to make an effective change. Therefore, blockchain-based resolution mechanisms are the only possible recourse for smart contract disputes.

Our proposal for courts to leave dispute resolution to blockchain-based mechanisms is not a mere theoretical postulate. Rather, this need was already introduced in the second and third prongs in Aragon's whitepaper about blockchain-based solutions for consumers facing code execution problems in smart contracts.[80]

3. Hybrid Approaches Accelerate Crypto Evolution

Hybrid approaches intended to preserve the existing legal infrastructure facilitate the broadening evolution of the crypto economy. The limited applicability of traditional jurisdictional means in the context of blockchain applications may lead some critics and traditionalists to institute hybrid approaches that incorporate the existing legal infrastructure into blockchain-based smart contracting transactions. Ultimately, hybrid approaches intended to preserve traditional jurisdictional means may be necessary in the transition phase. Hybrid approaches can create and increase certainty and trust for consumers and legacy infrastructure leaders who are otherwise unfamiliar with the blockchain-based infrastructure and the opportunities it offers. While hybrid approaches may be necessary in the transition phase of the new crypto economy, they ultimately facilitate the broadening evolution of the crypto economy.

---

[80] Luis Cuende & Jorge Izquiredo, Aragon Network: A Decentralized Infrastructure for Value Exchange (Apr. 2017), https://github.com/aragon/whitepaper/blob/master/Aragon%20Whitepaper.pdf [hereinafter *Aragon White Paper*].

Hybrid approaches and meta-structures that attempt to connect the existing legal and regulatory infrastructure with the blockchain-based world of smart contracting may ultimately accelerate the bifurcation of the jurisdictional infrastructure into traditional and crypto prongs, rather than slow down the bifurcation. For instance, meta-structures and alliances between the fiat currency banking system and crypto currencies may only temporarily create a legacy infrastructure bridge between fiat currencies and crypto currencies that allows for the tracing of payments demanded by institutional investors and consumers. If the meta-structure that connects fiat- and crypto-currencies sacrifice anonymity of transacting parties, at least temporarily, the meta-structure may arguably pull smart contracting transactions back into the existing jurisdictional infrastructure. However, miners that continue to mine the growing and meta-structure supported crypto world will continue to create anonymous wealth.

The legacy infrastructure bridge (fiat to crypto currencies) accelerates the growth of the blockchain-based economy and infrastructure but cannot curtail its anonymous nature. Once the currency conversion from fiat to crypto is complete, such crypto currencies are ultimately untraceable and anonymous in cyberspace. The legacy infrastructure bridge that is currently evolving allows increasing and accelerating inflow of financing into crypto currencies. By investing increasing fiat currency in a blockchain, the blockchain currency becomes more valuable, which in turn encourages further mining/crypto currency creation that is automatically anonymously owned. While the crypto currency that was purchased with fiat currency may not be anonymous before it is spent, after the first purchase, it is given a new public-key encrypted address and the new owners are anonymous unless they actively choose to reveal their identities. Accordingly, the accelerating inflow of fiat currency financing into crypto currencies enhances and accelerates the evolution of the crypto economy.

a) Jurisdiction Over Creation and Use of Blockchain Technology

While the public blockchain itself may not be subject to traditional jurisdictional means itself, the creation and use of blockchain technology may be subject to traditional jurisdictional principles. In fact, governing the creation and use of a blockchain may be the only practical way of exercising any form of traditional jurisdiction over blockchain. People who are subject to jurisdictional

means may create blockchains. Blockchain creators also live in geographical locations subject to laws that govern their activities. Accordingly, blockchains could be governed by the jurisdiction of the creator of a blockchain.

The exercise of traditional jurisdictional means over the creator of blockchains may encounter problems over time. First, it is only a matter of time until blockchains are created by other blockchains. Moreover, governing the creation of blockchains may encounter practical problems associated with anonymity (see further below on anonymity). For instance, Satochi, the billionaire founder of bitcoin is unknown and most hackers make it their personal hobby to ascertain his/her identity.

Exercising traditional jurisdiction over the use of blockchain technology raises several practical issues. For instance, if the focus of exercising jurisdiction would be on the physical location of the use, it remains unclear what would count as "use" of blockchain technology. Use could mean the actual use of blockchain technology to engage in commerce with other individuals or use could be the creation of a blockchain platform/forum for commerce. If use means the actual use of blockchain technology to engage in commerce it remains unclear if jurisdiction would apply over each user of the Graphic User Interface (GUI) for a blockchain technology or if use would mean execution of a transaction on the blockchain. If use means the execution of a transaction, it would remain unclear if jurisdiction would only apply if the transaction was added to the blockchain or if use would also be the attempt of adding a transaction that ultimately failed to the blockchain. If it is the latter, legal issues may arise because each transaction parameter that was not fulfilled, and thus the transaction was not added to the blockchain and would have to be addressed/litigated in the legal system. It is unclear if the legal system would be adequately equipped to address these problems as they originate in cyberspace.

Exercising jurisdiction over the creation and use of blockchain technology is rooted in the traditional understanding of jurisdiction that may not apply as the technology evolves. In fact, the evolution of blockchain technology may demand a more proactive, anticipatory, distributed, or networked approach to jurisdictional issues.

b) Coding Existing Law Into Smart Contracts

A hybrid approach and a temporary solution for the lack of

traditional jurisdictional means and legal control over smart contracts could be the programming of existing legal rules, doctrines, precedent, and their existing legal interpretation into smart contract code. In essence, such existing rules that would pertain to a comparable and equivalent real-world transactions and would be simply added as smart contract parameters. Such additions would necessitate the adherence to existing laws for contract execution on the blockchain.

This hybrid approach has several benefits. First, it provides the contracting parties with a very high degree of regulatory certainty which increases commerce in smart contracts and supports the evolution of blockchain-based transactions. Second, because smart contracts cannot execute unless all regulatory conditions and parameters are fully complied with, regulators lower their cost of supervision and enforcement while substantially increasing their oversight by reviewing the initial setup of smart contracting parameters in a given market or market segment. Third, regulators seeking additional oversight and increased transparency may access the public audit trail of executed smart contracts on the blockchain. The public blockchain or private blockchains that are opened to regulators can give the regulators full access and certainty about the state of a given smart contract market.[81]

The benefits of this hybrid approach are only temporary. As smart contracting evolves over time, fewer smart contracting solutions will have a real-world equivalent. In fact, it may over time become increasingly difficult to find real world legal solutions that can become effective parameters for smart contracts. This may be particularly true if the distributed jurisdiction is not effectively encouraged to adhere to traditional legal standards.

Without strong external pressures from existing regulatory structures and a distributed jurisdiction for crypto transactions that is responsive to such pressure, the anonymity of smart contracting will ultimately undermine the coding of existing legal rules into smart contracts. Blockchain-based cryptology in Ethereum virtual private networks do not allow the identification of the transacting parties if

[81] While public blockchains that are fully distributed and autonomously run technically cannot be opened to regulators, outside regulators can regulate from outside. Outside regulators can decide whether a blockchain is running according to their rules which might trigger labelling the blockchain as compliant or not, depending on whether the distributed jurisdiction is compliant. A government can allow its citizens to use only compliant blockchains (except they can't really stop the dedicated users who hide their IPs with VPNs, etc.).

the parties wish to remain anonymous. With the anonymity of contracting parties in smart contracts, it becomes unclear what specific laws / rules could be coded into the smart contract and who the contracting parties are.

Even if separate sets of existing legal rules could be identified for a given smart contract, it remains unclear how the contracting parties can turn such legal rules into code. The coding language used for a given smart contract and its parameters may be unable to spell out the intent of the legislator, court, or administrative agency in passing an applicable rule.

The supra-nationality of smart contracting may create additional burdens and exacerbate legal uncertainty of existing legal rules that already exists in the extraterritorial application of existing rules. For instance, the SEC jurisdiction over extraterritorial application of US Federal Securities Law is the subject of an ongoing debate and Supreme Court precedent. If ambiguous rules and precedent, even post Supreme Court decision in *Morrison,*[82] are applied to smart contracting parties, it is possible that the supranationality of smart contracting parties and/or lack of identification of such parties could exacerbate the legally ambiguous solutions of the existing world.

Finally, as Ethereum and other blockchain-based smart contracting networks become increasingly autonomous, legislators simply will not have the ability and authority to dictate to contracting parties and Ethereum itself whether or not to code existing legal rules into a given smart contract. Anonymity means the government cannot identify citizens with access to a free internet who use the blockchain. Nor can the government prevent citizens from adding contracts anonymously to the blockchain. Autonomy means the government cannot stop the blockchain miners from automatically adding contracts because the protocols do not recognize distinctions between good and bad contracts that any outside body dictates (as miners are also anonymous.) Also, the distributed nature of the blockchain means the government cannot control the nodes which maintain the blockchain without an effective world-wide governing body—which is obviously nowhere near feasible at this point in history—not even

[82] *Morrison v. Nat'l Australia Bank Ltd*., 561 U.S. 247 (2010); *See* Wulf A. Kaal & Richard W. Painter, *Forum Competition and Choice of Law Competition in Securities Law After Morrison v. National Australia Bank*, 97 MINN. L. REV. 132, 134 (2012).

if the nodes were known to the government, which they are not.

Because Ethereum, Aragon, and other blockchains, will be fully autonomous and decentralized in the near future, they cannot and will not be changed or superimposed by governments or any form of authority, unless it is in the interest of the majority of the blockchain community members. For instance, the vote to hard fork the first DAO would no longer be possible today as it evolved into a more autonomous structure. The goal of the distributed nature of all such structures is to become fully distributed and autonomous.

IV. Distributed Jurisdiction

The nature of smart contracting necessitates crypto dispute resolution mechanisms. Problems with smart contracts tend to be two-fold.[83] First, while smart contracts can be coded for and encapsulate a substantial portion of possible breaches of contract, subjectivity in human relationship, bounded rationality of coders and contracting parties, incomplete foresight, incomplete information, and opportunistic behavior[84] will make breaches or other problems in smart contracts inevitable. Second, the first DAO has demonstrated that software and coding bugs will be inevitable in the evolution of the crypto economy. As the existing jurisdictional infrastructure is bound to produce suboptimal results for such crypto disputes, intra-blockchain Distributed Jurisdictional means are needed.

Our proposal in this paper for a distributed jurisdiction over blockchains has to fulfill two core requirements: 1. The anonymity of blockchain-based smart contracting has to be maintained as the technology evolves. Without anonymity of blockchain-based smart contracting the existing jurisdictional means (in personam jurisdiction) can apply to smart contracting which would undermine

[83] *Aragon White Paper*, *supra* note 80. "Problems with existing smart contracts: - Subjective breaches: Smart contracts can encode most of the possible breaches of contract, but there is always subjectivity in human relationships. An unbiased arbitration system is needed for cases where conflicts are not explicitly resolved in the smart contract code. - Software bugs: The error is always between the chair and the keyboard. Code can contain bugs so the software needs to be easily upgradeable, and a sound bug bounty mechanism must exist to incentivize potential attackers to claim a bounty, rather than attack."

[84] *Evolution of Law: Dynamic Regulation in a New Institutional Economics Framework*, in FESTSCHRIFT IN HONOR OF CHRISTIAN KIRCHNER (Wulf Kaal, Andreas Schwartze & Matthias Schmidt eds.)(2014) (http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2267560).

the evolution of the crypto economy and make Distributed Jurisdictional means unnecessary. 2. Distributed Jurisdictional means necessitate governance from within the blockchain technology itself to effectively address the problems inherent in blockchain-based smart contracts. Without internal blockchain-based governance, a fully self-sufficient crypto economy may not be possible as legacy systems and governance intermediaries in the existing legal infrastructure will attempt to interfere with crypto transactions, resulting in suboptimal outcomes that cannot be fully resolved in the existing legal infrastructure.

Both requirements for the development of Distributed Jurisdictional means, full anonymity and intra-blockchain jurisdictional means, can already be accomplished. First, the Ties Network project demonstrates that anonymity can be perpetuated in blockchain technology,[85] despite blockchains' eternal storage of information and its growing size working against anonymity. Second, the Aragon Network demonstrates that the technology itself offers means of internal controls that help ensure effective governance in the continuing evolution of the technology.[86]

1. Securing Anonymity

The current blockchain characteristics undermine the continuing anonymity of blockchain-based transactions. Anonymity removal in blockchain transactions is a serious problem[87] that in fact

[85] DMITRY KOCHIN & ALEXANDER NEYMARK, ÜBERMENSCH WHITE PAPER 8 (2017) https://ties.network/files/%C3%9Cbermensch%20White%20paper.pdf [hereinafter *Ties White Paper*].

[86] The jurisdiction of the Aragon Network is distributed. Specifically, this means the network does not have a localized geographical existence; it is supranational. Therefore, no existing governmental entity has current legal jurisdiction over the regulation of general smart contracts. The Aragon Network's particular jurisdiction cannot be controlled by any nation-based court for the practical reason that all litigants and judges are anonymous, and so have no determinable national location. Consequently, no political entity will have any practical effect in the governance of general DAOs. *Aragon White Paper*, *supra* note 80. "The Aragon Network has three primary goals: 1. Provide models for starting well-designed DAOs. 2. Regulate the behavior of these DAOs according to rules decided upon by a dynamically evolving Aragon constitution, which rewards the discovery of potential hacks. 3. Provide a digital jurisdiction for settling contractual disputes in an anonymous and democratic manner.".

[87] *Ties White Paper*, *supra* note 85. "Problem of anonymity removal in blockchain transactions: The blockchain is immutable. All that is stored in blockchain remains

undermines the evolution of the technology. This is especially true because the application of traditional jurisdictional means due to a lack of anonymity provides suboptimal solutions that undermine trust in the technology-supported transactions. First, because the blockchain is immutable, blockchain-based transactions will be eternally stored and cannot be removed or deleted. Eternal storage itself works against anonymity.[88] Second, as blockchain-based transactions increase in popularity, the size of the blockchain grows rapidly[89] which will eventually require special equipment that can only be afforded by large corporations in the existing legal infrastructure. With such power for large corporations comes the possibility of dangerous centralization and a threat to undermining anonymity.[90]

2. Intra-Blockchain Solutions

Blockchain technology provides its own solutions for jurisdictional issues, governance, and conflict resolution. Blockchain technology resolves disputes of contracting parties by calculation. If a transaction is invalid it is checked automatically and quickly by any node and ignored. If two competing/contradictory transactions are valid, then the system automatically resolves the primacy of one over the other according to computing power. Whichever transaction is embedded in the longer computation chain will have primacy. No decisions can be made once a transaction is added to the network. No governing body currently exists to petition for recourse.

a) Aragon

Despite the dispute resolution mechanisms embedded in Blockchain technology, smart contracting in a commercial setting will

---

there forever and cannot be deleted. This is a serious drawback, given that most of the information in the interaction of users can be temporary and it could be deleted when the need for its storage disappears. Eternal storage of information also works against anonymity. Each node is a complete replica of other nodes. As a result, with the explosive growth of the application's popularity on the blockchain, the size of the blockchain grows rapidly at all nodes simultaneously. At some point, the size of blockchain can exceed the capacity of mass-produced hard disks and for the operation of the nodes, special equipment will be required, which only large companies can afford, which leads to dangerous centralization."

[88] *Id*.

[89] Most transactions, however, do not merit recording and in fact should be removed to avoid unnecessary increases in storage requirements.

[90] *Id*.

eventually require additional dispute resolution mechanisms. Problems with smart contracts are inevitable because of the subjectivity in human relationship, bounded rationality of coders and contracting parties, incomplete foresight, incomplete information, and opportunistic behavior.[91] Such human limitations will eventually make breaches or other problems in smart contracts inevitable, despite coders' attempts to optimize code in an effort to avoid such human traits in smart contracting. Add software and coding bugs to the human limitations and conflict resolution mechanisms become a necessity in the evolution of the crypto economy.

The Aragon Network already provides dispute resolution solutions that can help the consumer acceptance of smart contracting and crypto transactions. Aragon uses a form of digital jurisdiction governed by a representational democracy of anonymous judges and regulators, whose power is based on their stakeholder share of the network and supplemented by a reputation system.[92] Whenever a user wishes to dispute the execution of a contract in the Aragon Network, they post a bond (which will be returned if the dispute is decided in their favor) and a brief of their argument. 5 judges who have posted bonds will be randomly selected from all the users of the network. The judges read the litigants' briefs and issue their judgements. Majority decisions determine the outcome of the dispute. If a judge ruled with the majority, they are rewarded monetarily; if not, they are punished with the loss of their bond. 2 appeals are possible. If either party disagrees with the judgment they may appeal by posting a larger bond with their argument. This opens a prediction market, where any user in the organization may become a judge by posting a bond. The arguments are read and all judges return their verdicts. Again, majority determines the result of the dispute, with rewards or punishments for judges are given based on whether they sided with the successful party. The final appeal is made to a panel of 9 "supreme court" judges comprising the most successful judges in the network. A larger bond is posted by the appellant at each stage to prevent the wasting of system resources.

[91] Kaal, *supra* note 84.

[92] The Aragon Network offered a public token sale in May 2017 which raised $25 million US in the first 15 minutes.

b) Ricardian Contracts – OpenBazaar

OpenBazaar is a distributed program that provides an online trading platform for any type of merchandise using cryptocurrencies.[93] It does not use a blockchain for its core architecture, but it is a distributed network[94] and all parties and transactions are anonymous. Because of these core elements in the OpenBazaar network we consider it appropriate to compare its dispute resolution mechanism.

The essential ideas of OpenBazaar's system can be profitably employed on general distributed and anonymous business transaction platforms: 1. If both parties can agree on the type of transaction they are performing before signing a contract, a particular pool of arbiters can be chosen automatically. 2. A pseudonymous web of trust can be implemented to generate reputation for arbiters without compromising anonymity.

A core feature of the OpenBazaar dispute resolution mechanism involves so-called notaries. In the event of a dispute between parties, assuming alternative dispute resolution (ADR) had failed, the system includes a third party – the so-called notary. Users may choose not to involve the notary from the beginning of a transaction, in which case the smart contract has no transaction fees. However, the payment option without notaries involves risk because in that case, no arbitration is possible. The notary's primary job is to electronically verify the contract[95] has been signed by both parties and funds are available in escrow. Second, the notary verifies both parties are satisfied the terms have been fulfilled, then releases the bitcoin from escrow to the vendor. Finally, in case either party is not satisfied with the transaction, the notary acts as an arbiter in the dispute.

The allocation of notaries to contracts is an important mechanism for comparison of dispute resolution mechanisms.[96] Similar to Aragon, notaries in the OpenBazaar system are generally randomly chosen and allocated to a given contract. However, in

[93] http://docs.openbazaar.org/03.-OpenBazaar-Protocol/

[94] a Kademlia-style peer-to-peer distributed hash table

[95] Technically OpenBazaar uses "Ricardian" contracts, which have one extra layer of protocols on the smart contract, an encrypted identification between the human-readable version and the computer-readable version of the contract for the notary to interpret. The performance of the Ricardian contract is not always completely self-executing, and hence needs the third party notary. This is the primary distinction between OpenBazaar's system and Ethereum's smart contracts.

[96] At the time of writing, there have been no reported disputes in OpenBazaar, so the actual implementation of these protocols is entirely theoretical.

OpenBazaar the creators envision assorted pools of private notaries with varying expertise. Parties can theoretically agree which pool of notaries to choose before the contract is signed. This mechanism encourages the development of expertise within the system while satisfying the overarching goal of maintaining the anonymity of vendors and customers, since the details of a dispute are kept secret assuming the professionalism of the randomly chosen notaries.

The anonymity of the notaries is crucial to keep the system secure. Without anonymity, notaries could be coerced into revealing private information revealed in a given party's case. Therefore, the notary pool is reviewed using a pseudonymous web of trust to determine reputation. Pseudonymity is achieved using public keys.

OpenBazaar provides many benefits to disputants that are not included in the Aragon dispute resolution approach. Similar to Aragon's system of appeals, OpenBazaar imagines an appeal system that includes randomly selecting new notaries from the agreed upon pools according to reputation. However, OpenBazaar's more complex structure giving disputants the power of selecting between notary pools is a clear improvement over Aragon's method of completely random selection from the entire group of users posting judge bonds. OpenBazaar's approach naturally encourages notary pools to develop expertise in the various fields of law. Even though there is a chance that disputants' private information may be revealed in the course of a dispute, the reputation of a notary depends on their professionalism in maintaining the privacy of their clients. Aragon's whitepaper is not specific about how much private information is broadcast to the blockchain, but it seems to suggest their judgements have minimal information. In fact, Aragon appears to not even post a summary of their arbiters' reasoning which may cause the losing party to second guess the legitimacy of the entire dispute resolution mechanism in Aragon.

3. Limitations of Existing Solutions

Despite its much-needed introduction of dispute resolution and smart contract optimization improvements of the Ethereum network, the Aragon network still encounters several limitations. First, without full and continuing anonymity throughout the crypto evolution, the application and evolution of Aragon's distributed dispute resolution mechanisms may not be viable in the long run as traditional jurisdictional means would attempt to take over without the assurance

of full anonymity in blockchain transactions. Second, the random selection of judges from users of the Aragon network may only limitedly ensure the effective dispute resolution. Over time, users will inevitably demand the highest possible expertise of their judges and arbitrators. Without judge's expertise in a given smart contract subject matter of a dispute user confidence in effective and fair conflict resolution is undermined which leads to overall less confidence in crypto transactions as a whole and can undermine the evolution of the crypto economy. Third, the democratic decision of a majority of judges in the Aragon dispute resolution in combination with its lacking expertise of judges may undermine user confidence in effective and fair dispute resolution. Fourth, users in the Aragon system would only informally be able to use lawyers or other consultants and perhaps would use lawyers from the existing jurisdictional infrastructure to help optimize their arguments in support of their claims. Support from lawyers trained in the existing jurisdictional infrastructure and without additional training in quantitative science and coding can lead to suboptimal results for transacting parties in smart contracts. Fifth, Aragon does not allow opting into different dispute resolution mechanisms. Only user of Aragon can use their dispute resolution mechanisms. As other smart contracting platforms are being created, a need for more diverse, nuanced, and effective dispute resolution options emerges.

Several additional factors suggest that the dispute resolution scheme in Aragon could be improved. The random selection of user judges in the Aragon network introduces a level of arbitrariness to dispute resolution mechanisms that many private users but especially larger entities, including corporations in the existing legal infrastructure may not appreciate. Especially the submission of judges to the more popular vote and the economic incentives for judges to follow a more popular vote (in the Aragon system judges keep their bond if they voted with the majority), despite the overall anonymity of the voting, may call required notions of effective, non-arbitrary, and fair dispute resolution mechanisms into question. Users who are dissatisfied with such suboptimal conflict resolution mechanisms may wish to opt into a more nuanced conflict resolution network that helps them ascertain their rights and guarantees balanced outcomes.

Similarly, the OpenBazaar supported Ricardian Contract is subject to multiple shortcomings. Technically OpenBazaar does not use smart contracts. Instead "Ricardian" contracts are used, which

have one extra layer of identification between the human-readable version and the code-readable version of the contract. The performance of the Ricardian contract is not completely self-executing, and hence needs the third-party notary. The primary disadvantage of OpenBazaar's system, compared with Ethereum's smart contracts, is this extra layer of verification and the associated transaction fees. Because of these fees, the OpeanBazaar dispute resolution mechanism creates substantial transaction costs that can be avoided by pure Ethereum-based self-executing smart contracts. Because every single Ricardian Contract has an arbiter/notary connected with them to automatically, check the contract, and hold funds in escrow until the contract is validated, such contracts follow the established legal order for contracting to a significant extent. With it come additional significant transaction costs in various forms associated with an intermediator, here the notary/arbitrator, in the traditional financial system. Smart contracts make such transaction costs unnecessary but need a sound system for dispute resolution which we herein propose.

V. Open-Source Platform Ecosystem for Smart Contract Dispute Resolution

In light of the shortcomings of the available dispute resolution mechanisms for the crypto economy, and based on the concept of a distributed jurisdiction, we suggest an open source platform ecosystem of smart contracting dispute resolution that allows users to opt into the conflict resolution mechanisms that enable more nuanced crypto solutions and produce greater (legal) certainty in the process. First, an open source platform based ecosystem for dispute resolution of crypto transactions could help ensure full anonymity in blockchain transactions by instituting a requirement of anonymity for transaction parties to opt into the platform. Second, the platform would allow users to identify the highest possible expertise of their judges and arbitrators by way of reviewing the record of decisions of their judges across different fora and different types of conflicts.

At this point in time there are many new startups building contracting platforms using open, anonymous distributed architecture including Ethereum, Aragon, OpenBazaar, and Tezos, to name a few. Our proposed platform ecosystem would significantly boost consumer confidence in the non-arbitrary and fair resolution of their disputes. This proposal constitutes an open source ecosystem hybrid that

provides effective solutions for the shortcomings identified in the Aragon and OpenBazaar models.

In contrast with the OpenBazaar solutions, our proposed open source ecosystem allows dispute resolution only if and when a smart contract has resulted in a dispute. This solution ensures that smart contracting transaction costs remain near zero and the cost of paying an arbiter/notary/judge only occurs in cases of smart contract dispute resolution issues which will be a fraction of the overall quantity of smart contracts executed in the evolving crypto economy. As such, our proposal helps stimulate the evolution of the crypto economy. We envision a further improvement in comparison with OpenBazaar's approach which includes an open review system for evaluating the reputations of arbiters. Arbiters would submit their judgements to the community for review, removing all personal information to ensure anonymity. The community could upvote or downvote such judgments. Arbiters could improve their reputations by submitting comments and counter-judgements in an open forum.

This proposal has several benefits that can be distinguished from the Aragon network in several important ways. It involves the same necessarily democratic solution as in the Aragon system, except for several core differences: 1. The cases are not bound to binary decisions (it's unclear how 5 anonymous judges would collaborate to give a nuanced answer in Aragon). 2. Crowdsourcing the judgments leads to more efficient appeals. 3. Decisions would be open to re-evaluation for all eternity, so the judges' reputations are subject to a greater ideal than mere contemporary popularity. Further, this approach still promotes the eternal anonymity of parties and arbiters, as judges who revealed private information would be severely downvoted. Thus, our proposal provides more nuanced and better outcomes with better representation for parties in smart contract dispute resolution.

By way of analogy, just as federal courts in the existing legal infrastructure often provide better outcomes for litigants than state courts, because of the better qualifications of judges and the higher stakes involved, among other factors, our open source ecosystem would allow litigants more choice among dispute resolution mechanisms, enable better representation, and facilitate increased quality of arbiters. For claimants who have an interest in the best possible outcomes and are willing to wait analog times (≈1 month) the platform provides ideal fora to settle disputes.

1. *Legal Equivalence*

Stakeholders in legacy systems will likely hesitate transferring their legacy infrastructure businesses, and revenue streams derived therefrom, to an uncertain blockchain infrastructure and crypto systems without significant and sufficiently incentivizing assurances that they are not sacrificing any attained existing legal rights in exchange for smart contract efficiency in a blockchain system. Accordingly, the adjudication, dispute resolution, and enforcement of smart contracting disputes in the evolving crypto economy have to provide equivalent measures that assure legacy businesses that they can operate in crypto systems without a surrender of existing rights.

Legal equivalence can be assured in the implementation and transition phase of the crypto economy via dual integration. Dual integration refers to the use of legacy legal infrastructure in smart contracting dispute resolution, such as via the Ricardian contracts, among other measures, in combination with intra-blockchain systems for the resolution of smart contract disputes.

For participants in the crypto economy who wish to minimize the transaction costs of dual integration and retain anonymity our proposed open platform ecosystem is more likely than all other solutions to provide legal equivalence of dispute resolution mechanisms. Our proposed system would maintain the importance of good education and reputation on the principles of law. Yet, it would still eradicate much of the corrupting collection of power that specialized knowledge and relationships give to analog lawyers.

2. *Anonymous Arbiter Expertise*

The platform ecosystem would allow users to identify the highest possible expertise of their anonymous judges and arbitrators by way of reviewing the record of decisions of their judges across different fora and different types of conflicts. We propose using the open and eternal ledger for purposes of listing the following information pertaining to a given decision maker in smart contracting disputes: 1. Contractual Subject Matter, 2. Cases, 3. Decisions, 4. Justifications for Decision, 5. Dicta. Based on such disclosures, we propose an open system that allows comments which could be up-voted or down-voted.

The system allows for the expertise of judges to be determined by anonymous rating systems or anonymous reputational reporting,

similar to the token holder proposals in DAOs where token holders whose proposals are voted in but the token holder proponent who cannot perform in the implementation of such proposal will rarely get a second chance at making and implementing a given optimization proposal.

To mitigate the inevitable centralization that comes with expert involvement[97] in a decentralized dispute resolution platform and ecosystem we provide several solutions. Because our proposed system is based on upvotes from users who have an interest in the subject, abuse of authority that happens naturally in the non-anonymous world would be rather limited if not non-existent. And, crucially important for the success of the system in a legal realm, any abuse of authority would quickly be dis-incentivized by the deluge of downvotes such infamy would bring. Our solution allows anonymous contributors to gain reputation in certain areas of disputes based on whether their opinions are well-received. Such systems already exist in non-dispute resolution contexts.[98] Reputation may also accrue and promote decision makers in dispute resolution by means other than erudition, such as network recognition, connectivity, among others.

---

[97] A possible downside in the system pertains to the danger of centralization that comes with expertise of decision makers in decentralized dispute resolution mechanisms. Arguably the reputational elements in the proposed ecosystem could lead to superstars and with it to dangerous centralization. Decision makers in decentralized dispute resolution mechanisms with genuine educational and/or philosophical expertise can quickly gain a reputation in such systems, enabling an inevitable and natural centralization of power.

This could create a potentially serious corruption problem, as arbiters with the highest reputation will likely become valued counselors for disputants. Conflicts of interest occur in the possible scenario when a randomly chosen judge works for one of the parties. If the platform is small, or a domain of interest is small, the likelihood of this occurring is high. Since judges are anonymous, this is difficult to police. Because no conceivable way exists to permanently hide an arbiter's reputation from the arbiter in an open system, this is an insoluble problem with the proposal.

However, the problem can be mitigated by two factors in our proposed platform ecosystem: 1. the system randomly allocates judges based on disputants' reputation preferences, and 2. judges who advertise, and prove, their high reputation may be down voted for that very hint of corruption. If any system is large enough to need a robust dispute resolution mechanism, arguably there should be enough judges that the potential for corruption is watered down. And the larger a platform gets, the less susceptible it is to this type of corruption.

[98] See https://stackexchange.com/ or reddit. The mathematics version of stack exchange is called mathoverflow and in that narrow area, the answers are often of very high quality without any monetary incentive.

3. Optimized Representation

The open source platform ecosystem of dispute resolution in a distributed jurisdiction also facilitates optimized representation of a given party who in the Aragon system would only informally be able to use lawyers and perhaps would use lawyers from the existing jurisdictional infrastructure. The ecosystem allows for a more diverse allocation mechanism for smart contracts disputes to the most appropriate decision-making body/forum. But also, a platform ecosystem of dispute resolution fora would allow the integration of user representation in a given dispute.

The Aragon network does not facilitate a representation system for dispute resolution. In the Aragon network, a user who wishes to dispute the execution of a contract in the Aragon Network posts a bond and prepares a brief on their argument. Such briefs are not necessarily written by a representative of the user. However, as the stakes get higher in the crypto economy and smart contracting, users may want to seek smart contract representation on their behalf to optimize their chances of success in front of decision makers in their respective disputes. Such representation in the platform ecosystem of decentralized jurisdictions would be enabled. The ecosystem would allow for a matching of representation and dispute resolution fora.

VI. Conclusion

Distributed jurisdictional means for blockchain technology enabled smart contracting provides much needed governance from within the blockchain technology itself. Intra-blockchain distributed jurisdictional means such as via distributed jurisdiction are needed because the existing jurisdictional infrastructure produces suboptimal results for smart contract disputes. Distributed jurisdictional means effectively address the problems inherent in blockchain-based smart contracts. Our proposal in this paper for a distributed jurisdiction over blockchains ensures the maintenance of anonymity of blockchain-based smart contracting as the technology evolves.

Building on the concept of distributed jurisdiction, we propose an open source platform ecosystem for smart contract disputes. Our proposal ensures anonymity in blockchain transactions by promoting arbiters' reputations according to their discretion. The platform also ensures users can identify the highest possible expertise of their judges and arbiters. Our proposed system maintains the importance of good

education and reputation on the principles of an evolving crypto law. Yet, through its anonymization it also eliminates the corrupting collection of power that specialized knowledge and relationships give to analog lawyers.

Implementation of the proposed platform ecosystem for smart contract disputes would significantly boost consumer confidence in crypto transaction through the non-arbitrary, low to no-transaction cost inducing effective, and fair resolution of possible crypto disputes. For participants in the crypto economy who wish to minimize the transaction costs of dual integration and retain anonymity, our proposed open source platform ecosystem is more likely than all other available solutions to provide legal equivalence of dispute resolution mechanisms. For legacy businesses that desire to participate in the growth of crypto business opportunities, hope to avoid legacy system intermediation and the associated transaction costs, but require legal legacy system assurances and crypto dispute resolution equivalence, our proposed system offers a preferable solution. By attracting legacy businesses and instilling confidence in the legal equivalency of dispute resolution in crypto transactions, our proposed solution makes an indispensable contribution to the evolution and significant growth of the crypto economy.