The Alt-Chain Revolution: Regulatory Considerations for the Next Wave of Bitcoin Innovation

David B. Rivkin, Jr., and Andrew M. Grossman

March 2016

THE
FEDERALIST
SOCIETY

About the Federalist Society

The Federalist Society for Law and Public Policy Studies is an organization of 40,000 lawyers, law students, scholars, and other individuals located in every state and law school in the nation who are interested in the current state of the legal order. The Federalist Society takes no position on particular legal or public policy questions, but is founded on the principles that the state exists to preserve freedom, that the separation of governmental powers is central to our Constitution and that it is emphatically the province and duty of the judiciary to say what the law is, not what it should be.

The Federalist Society takes seriously its responsibility as a non-partisan institution engaged in fostering a serious dialogue about legal issues in the public square. We occasionally produce white papers on timely and contentious issues in the legal or public policy world, in an effort to widen understanding of the facts and principles involved and to contribute to dialogue.

Positions taken on specific issues in publications, however, are those of the author, and not reflective of an organizational stance. This paper presents a number of important issues, and is part of an ongoing conversation. We invite readers to share their responses, thoughts, and criticisms by writing to us at info@fedsoc.org, and, if requested, we will consider posting or airing those perspectives as well.

For more information about the Federalist Society, please visit fedsoc.org.

About the Authors

David B. Rivkin, Jr., and Andrew M. Grossman practice litigation in the Washington, D.C. office of Baker & Hostetler LLP. Mr. Rivkin served in the White House Counsel's Office and the Justice Department in the Reagan and George H.W. Bush administrations, and Mr. Grossman has served in numerous policy roles, frequently commenting on Internet technology and regulation.

The Alt-Chain Revolution:

Regulatory Considerations for the Next Wave of Bitcoin Innovation

David B. Rivkin, Jr., and Andrew M. Grossman

The Alt-Chain Revolution:
Regulatory Considerations for the Next Wave of Bitcoin Innovation

David B. Rivkin, Jr., and Andrew M. Grossman

Bitcoin is dead. Long live Bitcoin. A counterintuitive feature of the groundbreaking cryptocurrency—and there are many—is that both statements may simultaneously be true. The Bitcoin economy is robust and growing, with access to Bitcoin-denominated services expanding and more and more startups and established businesses seeking to capitalize on its popularity.[1] At the same time, the Bitcoin network—literally, the interconnected web of computers that records transactions in Bitcoin's distributed ledger known as the "blockchain"—is showing the strain of the currency's success, while disagreements threaten to stymie efforts to scale Bitcoin usage further.[2] Bitcoin-the-network may soon become too overloaded to fulfill the Bitcoin-the-currency's promise of fast, secure, and low-cost transactions.

And, in the end, that may not make a whit of difference. Even as political disputes threaten disruption of the core Bitcoin blockchain, developers are just beginning to introduce the next wave of innovation that has the potential to replace political stalemate with market competition. Alternative blockchains, or "alt-chains," are drop-in replacements for the Bitcoin network and blockchain that facilitate Bitcoin-based transactions off the core blockchain—in the same way that stocks can be traded on a myriad of competing electric trading networks, apart from primary exchanges like NYSE and NASDAQ. Not only do alt-chains present a solution to the current woes of Bitcoin governance—indeed, they may be able to dispense with much of the need for governance at all—but they also open a world of opportunity for innovative services that are ill-suited to the original Bitcoin network's design. From high-speed transactions to auditing to micropayments and more, alt-chains provide a means to move away from a one-size-fits-all network to a myriad of interacting networks tailored to specialized applications. And unlike experiments involving competing cryptocurrencies that have struggled to win uptake, alt-chains do not compete against Bitcoin, but instead work with it, leveraging its popularity, familiarity, and significant first-mover advantages. Indeed, alt-chains and related technologies may be central to preserving Bitcoin's key speed and cost advantages over traditional financial networks in the years ahead.

But, as in many innovative fields, some of the greatest barriers to alt-chain success are legal and regulatory uncertainty, far more than technological issues. Bitcoin was fortunate in being developed by a pseudonymous creator who later withdrew from participation in the project and never had to face the complexities of federal and state money transmission laws.[3] By contrast, alt-chains and related technologies are being developed and brought to market today by inventors and businesses that struggle to navigate the regulatory landscape for financial services that were inconceivable when, for example, money-transmission laws were drafted. While the Treasury Department has done much to clarify the application of the Bank Secrecy Act and other anti-money laundering laws, significant uncertainties still remain, particularly regarding the interaction of virtual currencies and their networks with one another. And state law remains a confused mess, in many places still uncertain in its application to Bitcoin, much less cutting-edge services that interact with it.

This White Paper discusses Bitcoin, blockchain technology, the concept of alt-chains, and their promise. It begins at the beginning, describing how distributed cryptocurrencies like Bitcoin function, their general

1   *See, e.g.*, Will Deener, *Bitcoin's Popularity Continues To Grow Despite Risks*, Dallas Morning News (Nov. 29, 2015), http://www.dallasnews.com/business/columnists/will-deener/20151129-will-deener-bitcoins-popularity-continues-to-grow-despite-risks.ece.

2   *See generally* Timothy B. Lee, *The Esoteric Debate That's Tearing the Bitcoin World Apart, Explained*, Vox (Jan. 26, 2016, 9:00 AM), http://www.vox.com/2016/1/26/10829488/bitcoin-block-size-debate.

3   *See Who Is Satoshi Nakamoto?*, The Economist Blog, (Nov. 2, 2015, 11:27 PM), http://www.economist.com/blogs/economist-explains/2015/11/economist-explains-1.

technological underpinnings, and how the systems underlying them can be swapped out and replaced. It proceeds to catalogue the diversity of potential applications for blockchain alternatives, as well as how these systems interact with the core Bitcoin blockchain and one another. Finally, it addresses the issues raised by alt-chains and other blockchain supplements and replacements under federal and state law, considering hypothetical examples of how the law might apply to several kinds of transactions undertaken off the core blockchain. It concludes that, while pure alt-chains that do nothing more than serve as decentralized replacements for the Bitcoin blockchain are unlikely to be subject to money transmission regulation, more advanced and hybrid services face greater uncertainty, and the application of such regulations can and should be clarified.

I. Bitcoin and the Blockchain

Bitcoin is best known as a virtual or digital currency—that is, as a digital analogue to traditional legal tender as a means of storing and exchanging value. And it does serve that purpose: one can, for example, exchange dollars for Bitcoin and then use Bitcoin as payment for goods or services. But that is only scraping the surface of Bitcoin's full potential. As a decentralized network for facilitating and recording transactions, Bitcoin is capable of much more. This section discusses Bitcoin's technological underpinnings, the distributed ledger system that differentiates it from prior digital currencies, and the features of the Bitcoin network.

The term "Bitcoin" refers not only to the currency itself but also to the global network that is integral to the currency's design and use. The Bitcoin network and the "blockchain" ledger that the network maintains are a clever solution to an age-old problem. A currency relies on scarcity; a currency that anyone can counterfeit at will is not much use as a store of value or medium of exchange. In the field of digital currencies, this is referred to as the "double spending" problem, in that a party can simply copy the code representing a unit of digital currency and send that copy as payment to two (or more) recipients.[4] As financial intermediaries like

banks have done from time immemorial, pre-Bitcoin digital payment systems relied on centralized ledgers of balances and transactions to prevent double spending.[5] This had a major drawback: a centralized ledger needs someone to maintain it, and that introduces a central point of failure, whether through fraud, incompetence, insolvency, or any shortcoming that increases risks and other transaction costs.[6] For example, there is nothing to prevent the administrator of a digital currency, once the currency has gained a degree of popularity, from hiking fees or "printing" more currency for its own account, to the detriment of currency holders. To participate in a pre-Bitcoin digital currency system, a user had to place trust in the administrator and then hope for the best. As a practical matter, this meant that digital currencies were not really competitive against legal tenders administered by governments, and few obtained even modest usage—often to facilitate black- and gray-market transactions.[7]

That was the digital currency status quo until the advent of Bitcoin. Bitcoin's innovation was to replace the ledger maintained by a trusted central party with one maintained instead by a distributed network, where all the computers are peers and no single party exercises control. That network uses mathematical algorithms—public-key cryptography, in particular—to verify transactions against a distributed ledger called a "blockchain" and to reach consensus on which ones should be recognized as legitimate and entered on the blockchain to serve as a basis for future transactions. This is all done by groups of computers known as "miners," which are rewarded through fees paid for transactions and through newly "mined" Bitcoin for their work verifying transactions and adding them

4   Ivan Osipkov, et al., *Combating Double-Spending Using Cooperative P2P Systems*, http://sclab.cs.umn.edu/papers/

ecash_ICDCS2007_corrected.pdf.

5   European Central Bank, Virtual Currency Schemes 17–18 (Oct. 2012), https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf.

6   Rainer Böhme, et al., *Bitcoin: Economics, Technology, and Governance*, J. Econ. Persp., Spring 2015, at 213, 219–21, http://pubs.aeaweb.org/doi/pdfplus/10.1257/jep.29.2.213 219–21.

7   *See generally* Kim Zetter, *Bullion and Bandits: The Improbable Rise and Fall of E-Gold*, Wired (June 9, 2009, 12:00 AM), http://www.wired.com/2009/06/e-gold/.

in new blocks to the blockchain. The end result is a time-stamped public ledger of Bitcoin transactions associating each unit of the currency with an address that can be accessed by the holder of a private key (a secret code, like a password).[8] The blockchain fulfills the same purposes as a centralized ledger, but without any central point of failure or any of the trust problems that beset centralized digital currencies.[9]

Bitcoin won fame not for the cleverness of its design but for its use as a currency. The first wave of Bitcoin-based businesses exchanged legal tender for Bitcoin, provided managed wallet services and Bitcoin-based financial services, and provided avenues for businesses to accept Bitcoin as a means of payment.[10] The currency also won infamy for its quick uptake as the preferred currency of Internet-based black and gray markets like the Silk Road—although, as best anyone can tell, such transactions comprised only a small proportion of Bitcoin payments.[11] Use of Bitcoin as a currency has also been hampered by exchange-rate volatility, as well as the collapse of several early exchanges holding users' currency.[12] Although the volume of Bitcoin transactions continues to grow, the currency has yet to win broad mainstream acceptance as a means of payment.[13]

---

8   For a live feed of transactions among Bitcoin users, *see* Blockchain Bitcoin Block Explorer, https://blockchain. info/.

9   For an overview of how Bitcoin works, *see* François R. Velde, *Bitcoin: A Primer*, Chicago Fed Letter (Dec. 2013), https://www.chicagofed.org/~/media/publications/chicago-fed-letter/2013/cfldecember2013-317-pdf.pdf. The original design document for Bitcoin remains available online, despite its author's apparent withdrawal from the field. Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, https://bitcoin.org/bitcoin.pdf.

10   *See* Sean Ludwig, *Hotshot Investor Chris Dixon Says 'Second Wave' of Bitcoin Startups Is on the Way*, VentureBeat (Apr. 29, 2013, 6:57 AM), http://venturebeat.com/2013/04/29/chris-dixon-second-wave-bitcoin-startups/.

11   *See* Jerry Brito & Andrea Castillo, Mercatus Ctr., *Bitcoin: A Primer for Policymakers* 20–21 (2013), http://mercatus.org/sites/default/files/Brito_BitcoinPrimer.pdf.

12   Tim Swanson, *A Proxy for Users*, Great Wall of Numbers, (Jan. 3, 2016), http://www.ofnumbers.com/2016/01/03/a-proxy-for-users/.

13   *Id.*

Over the past year, however, attention and investment have shifted from Bitcoin's role as a currency to potential uses of its underlying blockchain technology. Applications span a wide variety of fields:

One idea, for example, is to make cheap, tamper-proof public databases—land registries, say, (Honduras and Greece are interested); or registers of the ownership of luxury goods or works of art. Documents can be notarised by embedding information about them into a public blockchain—and you will no longer need a notary to vouch for them. Financial-services firms are contemplating using blockchains as a record of who owns what instead of having a series of internal ledgers. A trusted private ledger removes the need for reconciling each transaction with a counterparty, it is fast and it minimises errors. Santander reckons that it could save banks up to $20 billion a year by 2022. Twenty-five banks have just joined a blockchain startup, called R3 CEV, to develop common standards, and NASDAQ is about to start using the technology to record trading in securities of private companies.[14]

Some of these kinds of applications can be built with or on top of the Bitcoin blockchain, taking advantage of Bitcoin's infrastructure, tooling, and broad base of users. Others have needs that are incompatible with the Bitcoin platform as it exists today. Bitcoin, however, has been slow to evolve, with new developments requiring acceptance by at least a majority of the miners who comprise the blockchain network. Those who have invested in Bitcoin and Bitcoin infrastructure are understandably conservative when it comes to making big changes to the existing network.

As a result, despite its radical decentralization compared to traditional financial institutions and networks, Bitcoin is still subject to at least one potential central point of failure: the need for consensus to evolve the protocol and the network itself to adapt to new conditions or address new applications. In fact,

---

14   *The Trust Machine*, The Economist (Oct. 31, 2015), http://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine.

in recent months, the Bitcoin community has been fractured over the question of whether and how to expand the size of blocks added to the blockchain, which could speed transactions and reduce costs, at the expense of potentially increasing the dominance of the large mining pools that already form the backbone of the network.[15] The dispute, once viewed as a technical matter appropriately resolved by developers, has spilled out into the open, stoking conflict and controversy that may frustrate even modest efforts to address the Bitcoin network's technological growing pains.[16] To date, it is uncertain whether a fix will win the backing of enough of the network to take effect.[17]

Likewise, developers of applications that don't fit on the Bitcoin blockchain—whether due to lack of features or to differing design choices—face the similarly daunting prospect of attempting to add new features to Bitcoin or—even more daunting—going it alone by creating an entirely new blockchain separate from Bitcoin's. To date, many have tried. A large number of cryptocurrencies were released in the wake of Bitcoin, many sporting design improvements and innovative new features.[18] None have succeeded, however, in establishing a platform that shares Bitcoin's unique features: broad acceptance, global distribution, a large user base, and (as a result) resiliency against takeover by a small number of participants. Indeed, those things may be impossible to recreate in the face of Bitcoin's massive first-mover advantage. Quite understandably, users are reluctant to experiment with alternative blockchains using new and untested digital currencies that may expose them to even more risk and volatility than Bitcoin.

In short, Bitcoin's broad success may now be the most substantial barrier to innovation in public-facing blockchain technologies, stymying further development of the Bitcoin network as well as adoption of other public blockchain-based applications.

II. Same Bitcoin, New Chains

"Alt-chains" are a clever solution to the Bitcoin stagnation problem. The basic idea is to leverage Bitcoin's popularity by using Bitcoins-the-currency as tender on other blockchains and networks, ones that may differ substantially from the Bitcoin blockchain.[19] In this way, innovation can take place on alternative networks without requiring the buy-in of those operating the existing Bitcoin network, without the risk of disrupting the operation of the main Bitcoin blockchain, and without abandoning the built-in benefits of Bitcoin interoperability.

The key insight is that Bitcoin transactions need not take place on the Bitcoin blockchain, even if they may be eventually settled there. A simple example of this concept (albeit not a blockchain itself) is completing transactions by shifting balances among accounts in a bank. If a bank holds funds in its own Bitcoin wallet on behalf of customers Arthur and Bryan, Arthur can pay Bryan for goods or services by asking the bank to transfer Bitcoin from his to Bryan's account, with that transaction recorded on the bank's internal ledger—it simply debits the amount from one account and credits it to the other. There is no need for the bank to transfer any funds from its own Bitcoin wallet and so no need for the transaction to be entered on the Bitcoin blockchain. Only when Bryan asks the bank to transfer funds to an account outside of the bank, whether that is a wallet of his own or one belonging to a third party, will any intra-bank transactions be reconciled in the Bitcoin blockchain.

The insight of alt-chains is that a system for conducting off-blockchain transactions need not be one

15   Mike Hearn, *The Resolution of the Bitcoin Experiment*, Medium (Jan. 14, 2016), https://medium.com/@octskyward/the-resolution-of-the-bitcoin-experiment-dabb30201f7#.2kkt2co9p.

16   Pete Rizzo, *Bitcoin Branded a Failure as Media Erupts Over Mike Hearn Exit*, CoinDesk (Jan. 15, 2016, 7:18 PM), http://www.coindesk.com/bitcoin-branded-a-failure-as-media-erupts-over-mike-hearns-contentious-exit/.

17   Stan Higgins, *Bitcoin Miners Back Proposed Timeline for 2017 Hard Fork*, CoinDesk (Feb. 20, 2016, 10:58 PM), http://www.coindesk.com/bitcoin-miners-back-proposed-timeline-for-2017-network-hard-fork/.

18   *List of Cryptocurrencies*, Wikipedia, https://en.wikipedia.org/wiki/List_of_cryptocurrencies (last visited Feb. 22, 2016).

19   Adam Back, et al., *Enabling Blockchain Innovations with Pegged Sidechains*, Blockstream, Oct. 22, 2014, at 2–3, https://blockstream.com/sidechains.pdf [hereinafter "Sidechain White Paper"].

that is actively administered by a financial institution or any particular entity at all; instead, it can be another blockchain, separate from the "core" Bitcoin blockchain. In this way, Bitcoin can be transacted on and between different networks, just as other securities are often traded on multiple markets. For example, a financial institution might gradually purchase a block of shares on a primary stock exchange like NASDAQ and then sell it all at once on a secondary exchange that is geared for larger transactions like BATS or Instinet or one that specializes in high-speed trading.[20] Alt-chains and other alternatives to the core Bitcoin blockchain give Bitcoin users the same kind of choice, allowing them to choose among different exchanges, with differing features and benefits, and to do so while continuing to hold and transact in a single currency, Bitcoin, and avoiding the risks and uncertainties of a new currency.[21]

In that way, alt-chains open the door to many potential applications that would be difficult or impossible to carry out on the Bitcoin blockchain. These include:

- *Fast Iteration and Experimentation.* At the most general level, the use of non-core blockchain transactions permits experimentation and variation along any dimension relating to blockchain implementation. Alt-chains may serve, for example, as a proving ground for development and testing

of new features for the core Bitcoin blockchain, offering real-world advantages over the for-play "Testnet" currently used by Bitcoin developers.[22] As described further below, other alt-chains may serve to complement the core Bitcoin blockchain, implementing different tradeoffs than those made in Bitcoin so as to facilitate different kinds of transactions.

- *High-Speed Transactions.* Alt-chains can be tuned for particular use cases, such as high-speed transactions among financial institutions. Liquid is one of the first production "sidechains"—a particular kind of alt-chain that is automatically pegged to the Bitcoin blockchain, without the need to rely on third parties to conduct transactions between the two networks—and is designed to facilitate rapid transfers among a relatively small number of Bitcoin exchanges and brokers, avoiding the latencies of conducting transactions on the core Bitcoin blockchain.[23] Particularly where users are conducting trading or other financial operations on a particular company's platform, latency requires that they maintain a balance on that platform, increasing complexity, the need for capital, counterparty risk, and ultimately transaction costs. Whereas verification of core Bitcoin blockchain transactions may take minutes or even hours[24]— still a dramatic improvement over wire-transfer services and other legacy financial networks— Liquid promises that transaction settlements among accounts at partnering institutions will take just seconds, allowing transactions at one institution to be funded from Bitcoin held by another. Liquid

---

20   For background on "alternative trading systems" in securities markets, see Laura Tuttle, Sec. and Exch. Comm'n, *Alternative Trading Systems: Description of ATS Trading in National Market System Stocks*, Oct. 2013, http://www.sec.gov/marketstructure/research/ats_data_paper_october_2013.pdf.

21   The relationship between the core Bitcoin blockchain and an alt-chain can be implemented with cryptographic techniques so that users can move funds seamlessly between chains without having to place much or any trust in an intermediary to complete the transfer between chains. A proposal on how exactly to implement such a relationship describes the arrangement as a "pegged sidechain." *See* Sidechain White Paper, *supra* note 19, at 8–11. Alternatively, alt-chains and other off-chain transaction systems can be implemented through one or more trusted intermediaries that, governed by contractual terms, administer transfers between networks without necessarily controlling transactions within a single network. *Id.* at 17–19.

22   *See generally Testnet*, BitcoinWiki, https://en.bitcoin.it/wiki/Testnet (last visited Feb. 16, 2016).

23   *See generally* Austin Hill, *Introducing Liquid: Bitcoin's First Production Sidechain*, Blockstream (Oct. 12, 2015), https://blockstream.com/2015/10/12/introducing-liquid/; Pete Rizzo, *Blockstream To Launch First Sidechain for Bitcoin Exchanges*, CoinDesk (Oct. 13, 2015, 8:01 AM), http://www.coindesk.com/blockstream-commercial-sidechain-bitcoin-exchanges/.

24   *See, e.g.*, Ken Griffith & Ian Grigg, *Bitcoin Verification Latency: The Achilles Heel for Time Sensitive Transactions*, http://iang.org/papers/BitcoinLatency.pdf.

is a good example of how alternative blockchain design choices can diverge from the tradeoffs made in the core Bitcoin blockchain and thereby provide differentiated services.

- *High-Volume Transactions and Micropayments.* The promise of micropayments is providing a simple mechanism for users to directly fund content creators for articles, music, and other media that are currently advertising-supported or generally uncompensated, as well as services metered in small increments. Micropayments have long been stymied by transaction costs—for example, payments service provider PayPal charges a fee of 30 cents, plus 2.9 percent of the transaction for processing credit card transactions.[25] The combination of high fees and the costs of reversed transactions renders small micropayments infeasible. While Bitcoin does provide a viable platform for micropayments, with much lower fees and the ability to send small sums, the core Bitcoin blockchain is not optimized for them. Among its shortcomings: large numbers of micropayment transactions threaten to trip the network's anti-flooding protections, fees don't scale well to extremely small payments of just a few cents, large numbers of transactions risk bloating the blockchain and burdening miners, and spending sums comprised of many small contributions can itself incur excessive fees.[26] A micropayments-optimized alt-chain, however, could address these issues by cutting back on some of the verification and security procedures employed by the core Bitcoin blockchain, while commensurately limiting the value of transactions—in other words, trading off some security and resiliency for lower fees for smaller transactions.

- *Control and Auditing.* While some alt-chain

developers may seek to optimize for speed and volume, others may attempt to exercise greater control over Bitcoin transactions. A blockchain could, for example, require cryptographic proof that a wallet is owned by a verified person or institution before allowing it to receive funds, thereby reducing the likelihood of fraudulent transactions, increasing auditability, and enforcing other policies that may be desirable by those using that blockchain.

- *Privacy and Resiliency Against Censorship.* Conversely, other developers may use alt-chains to provide privacy guarantees above and beyond those inherent in Bitcoin. For example, transactions may be hidden from public view, to prevent discovery of trading strategies and other proprietary information. Similarly, decoupling transactions from identification of users may serve to thwart censorship.[27]

- *Smart Contracts.* While Bitcoin does contain facilities to allow certain types of "smart contracts"—i.e., transactions that have built-in algorithmic properties, such as escrowing funds until the occurrence of some verifiable event—they are difficult to create and execute and limited in their abilities. Alt-chains, however, could incorporate richer scripting that allows such things as atomic transactions (i.e., a guarantee that certain transactions occur all at once, as a group), automatic escrows, automatic payment for performance, and many other financial products. Similar scripting capabilities could be used to represent non-Bitcoin assets, allowing them to be traded on a particular alt-chain.

- *Refining or Replacing Mining.* Developers could use alt-chains to explore alternative network configurations that may one day supplant the core Bitcoin blockchain. The Bitcoin network, and many other blockchain implementations, is comprised of computers performing computationally expensive calculations which compete with one another to add the next block of transactions to the chain, with the winner receiving any transaction fees and a "mined" reward. One drawback of this scheme is that it wastes

---

25   PayPal, *Merchant Fees*, https://www.paypal.com/webapps/mpp/merchant-fees (last visited Feb. 16, 2016).

26   *See, e.g.*, bitcoinJ, *Working with Micropayment Channels*, https://bitcoinj.github.io/working-with-micropayments (last visited Feb. 16, 2016); Pete Rizzo, *Lightning, Duplex and the Search for Scalable Bitcoin Micropayments*, CoinDesk (Oct. 7, 2015, 11:59 PM), http://www.coindesk.com/lightning-duplex-scalable-bitcoin-micropayments/.

27   *See generally* Sidechain White Paper, *supra* note 19, at 14.

enormous amounts of electricity on busywork the main point of which is to prove that it was done so as to thwart attackers from easily adding blocks containing false transactions to the blockchain.[28] Another is that Bitcoin mining is winner-take-all, with only the miner that adds a new block receiving the payout. Alt-chains could employ alternative approaches that dispense with mining altogether, in favor of other means of achieving consensus on valid transactions, or otherwise alter the economics of participating in the blockchain network, such as by providing more consistent returns. For example, the 21 Bitcoin Computer conducts mining through a separate network that allows for consistent, buffered payment of mining proceeds—both to operate that network and to profit from pooled Bitcoin mining.[29]

In short, just about any potential improvement or variation on Bitcoin can be more easily implemented as an alt-chain using Bitcoins as currency. In this way, alt-chains provide a mechanism for rapid innovation in digital currency and distributed transaction networks, with applications in many fields, while building on the success, mind-share, and familiarity of Bitcoin.

III. Money Transmission Regulation and Off-Blockchain Innovation

Although regulatory uncertainty has been a point of concern in the development and adoption of virtual currencies and Bitcoin in particular, Bitcoin's novelty and rapid spread have led regulators to clarify the application of money-transmission regulation or announce policies of forbearance with respect to certain kinds of activities. The result is that, while the law is not perfectly clear, enough guidance is available to provide innovators of certain kinds of alt-chain services with reasonable assurance that they will not face potential civil and criminal liability.

However, most guidance to date has focused on services transacting directly in Bitcoin—for example,

those exchanging Bitcoin for traditional currency, or vice-versa—while little attention has been directed at services and products that interact with Bitcoin, provide alternative platforms or networks for Bitcoin, or replace portions of the Bitcoin infrastructure. And in that field, there remain some significant areas of regulatory uncertainty. This section discusses federal and state money-transmission law relevant to developers of services that interface with Bitcoin, describes guidance in those areas where it is available, and identifies points of uncertainty that could benefit from additional guidance. It concludes that regulatory forbearance is warranted with respect to technologies that are not themselves likely to facilitate money laundering or other abuses targeted by money transmission regulation.

A. The Bank Secrecy Act and "Money Transmission Services"

When dealing with currency transactions, money laundering is a foremost legal concern, as is compliance with laws governing currency transactions to prevent or expose laundering. No less than traditional currencies, virtual currencies can be used to launder the proceeds of criminal activities, evade reporting requirements, and otherwise facilitate unlawful conduct. At the federal level, currency-transaction reporting is governed by the Bank Secrecy Act ("BSA"), which is administered by the Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN").

The BSA "requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering" by keeping records of certain cash transactions and filing reports on transactions and "suspicious activity that might signify money laundering, tax evasion, or other criminal activities."[30] As relevant here, the BSA and FinCEN implementing regulations apply to firms engaged in money transmission, which are referred to as "money services businesses" ("MSBs") and must register with FinCEN and adopt anti-money laundering programs. MSBs include foreign currency exchangers, check-cashing services, money order issuers, and operators of

---

28   *See, e.g.*, Daniel Cawrey, *How Consensus Algorithms Solve Issues with Bitcoin's Proof of Work*, CoinDesk (Sept. 11, 2014, 11:12 AM), http://www.coindesk.com/stellar-ripple-hyperledger-rivals-bitcoin-proof-work/.

29   The 21 Bitcoin Computer, https://21.co/ (last visited Feb. 16, 2016).

30   FinCEN, *Bank Secrecy Act Homepage*, https://www.fincen.gov/statutes_regs/bsa/ (last visited Feb. 16, 2016).

"money transmission services."[31] "Money transmission services" involve "the acceptance of currency, funds, or other value that substitutes for currency from one person *and* the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means."[32] That definition encompasses, for example, services like Western Union that facilitate the transmission of currency between different locations and persons.

The BSA looms large for blockchain innovators. Compliance can be complicated and expensive, potentially at odds with the "move fast and break things" attitude of many technology startups and the rapid iteration in the design and operation of live systems. An MSB subject to BSA must institute an anti-money laundering program designed to prevent its service "from being used to facilitate money laundering and the financing of terrorist activities."[33] The program must incorporate policies, procedures, and internal controls reasonably designed to assure ongoing compliance; designate an individual responsible for assuring day-to-day compliance with the program and BSA requirements; provide training for personnel, including training in the detection of suspicious transactions; and provide for independent review to monitor and maintain an adequate program.[34] In addition, an MSB must report transactions that it "knows, suspects, or has reason to suspect" are suspicious, based on a laundry list of factors.[35] They must implement "Know Your Customer" procedures and also obtain, verify, and maintain records regarding certain transactions.[36] At the very least, complying with BSA requirements exacts an opportunity cost, by requiring businesses to channel money, resources, and time into regulatory compliance

instead of developing new customer-facing features.

The incentives for compliance, however, are overwhelming. In addition to the desire to avoid abuse of their services to launder money or finance crimes, businesses face substantial liability risks for failing to meet BSA requirements. Violations are potentially subject to civil and criminal penalties, including imprisonment.[37]

FinCEN clarified the application of the BSA to services involving "virtual currencies"—i.e., things that, while not legal tender, nonetheless operate as a medium of exchange in certain contexts and are convertible to other currencies—in a 2013 guidance document.[38] The guidance, like the underlying regulation, takes a functional approach to regulation, focusing on three potential roles: A user "is a person that obtains virtual currency to purchase goods or services"; an exchanger "is a person engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency"; and an administrator "is a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."[39]

Users are not subject to regulation as MSBs because their conduct does not fit the definition of "money transmission services." Accordingly, a person or business that merely spends virtual currency in exchange for goods or services need not take steps to comply with BSA registration, reporting, and recordkeeping requirements.

An administrator or exchanger, however, may be a MSB if it "(1) accepts and transmits a convertible virtual currency or (2) buys or sells convertible virtual currency."[40] As the guidance explains, that conclusion is a direct application of the regulatory definition of "money transmission service," which does not

---

31   31 C.F.R. § 1010.100(ff)(1–7).

32   *Id.* § 1010.100(ff)(5)(i)(A) (emphasis in original).

33   *Id.* § 1022.210(a).

34   *Id.* § 1022.210(d).

35   *Id.* § 1022.320(a)(2).

36   FinCEN Interpretive Release 2004-1, *Anti-Money Laundering Program Requirements for Money Service Businesses with Respect to Foreign Agents or Foreign Counterparties*, 69 Fed. Reg. 74,439 (Dec. 14, 2004); 31 C.F.R. § 1010.410(e–f).

37   *See, e.g.*, 18 U.S.C. § 1960(b)(1)(B).

38   FinCEN, *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, Mar. 18, 2013, at 1 (hereinafter "FinCEN Virtual Currency Guidance").

39   *Id.* at 2.

40   *Id.* at 3.

distinguish between real and virtual currencies.[41] It naturally follows that, for centralized virtual currencies, the administrator "will be a money transmitter to the extent that it allows transfers of value between persons or from one location to another."[42] That includes the acceptance of real currency to fund a user's virtual currency account, which the guidance regards as a "transmission to another location, namely from the user's account at one location (e.g., a user's real currency account at a bank) to the user's convertible virtual currency account with the administrator."[43] It similarly regards the transmission of virtual currency at the behest of a user—for example, carrying out a direction to send or otherwise credit currency to the account of a merchant selling goods.

That general approach informs FinCEN's treatment of decentralized virtual currencies like Bitcoin, which differ principally in that they do not rely on a central authority. Users are in basically the same position as with a centralized virtual currency, with the additional clarification that obtaining currency other than through transactions—for example, through mining activities—does not result in regulation as a money transmitter. However, as with centralized virtual currencies, a person who "creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location" and therefore must comply with BSA requirements.[44] Likewise, one who "accepts such de-centralized convertible virtual currency from one person and transmits it to another person as part of the acceptance and transfer of currency, funds, or other value that substitutes for currency" must comply.[45] While a bit vague, this latter provision refers to middlemen in virtual currency transactions—for example, marketplaces that intermediate payment transactions between buyers and sellers.

How FinCEN's guidance works in practice is reflected in the federal government's settlement of a civil

enforcement action against Ripple Labs Inc., a creator of a blockchain-based virtual currency known as XRP. Unlike Bitcoin, XRP is a "pre-mined" currency—that is, all units of it were generated at the time that Ripple founded its network. The company then sold XRP in exchange for legal tender, conduct that it later agreed (in a settlement document) subjected it to the BSA and required it to register and institute an anti-money laundering program.[46]

FinCEN's virtual currency guidance provides a great deal of regulatory clarity regarding alt-chains and other off-blockchain services. First, in general, merely creating a new blockchain that operates as a Bitcoin blockchain replacement—i.e., an alt-chain network—would not subject a party to BSA regulation, because such creation does not necessarily involve that party in exchanging or transmitting currency. Indeed, applying its guidance, FinCEN has already determined specifically that "[t]he production and distribution of software, in and of itself, does not constitute acceptance and transmission of value, even if the purpose of the software is to facilitate the sale of virtual currency."[47] Under that determination, the creation and organization of decentralized alternatives to the Bitcoin blockchain should not subject a party to BSA regulation.

Second, the result should not be any different if an alt-chain utilizes mining to incentivize participation in the network in the way the Bitcoin blockchain does. As FinCEN has determined, "[t]o the extent that a user mines Bitcoin and uses the Bitcoin solely for the user's own purposes and not for the benefit of another, the user is not an MSB under FinCEN's regulations, because these activities involve neither 'acceptance' nor 'transmission' of the convertible virtual currency and are not the transmission of funds within the meaning of the Rule."[48]

---

41   *Id.*

42   *Id.* at 4.

43   *Id.*

44   *Id.* at 5.

45   *Id.*

46   *See* FinCEN, *Ripple Attachment A: Statement of Facts and Violations*, https://www.fincen.gov/news_room/nr/pdf/Ripple_Facts.pdf.

47   FinCEN, *Letter Ruling: Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002, at 2 (Jan. 30, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf.

48   FinCEN, *Letter Ruling: Application of FinCEN's*

Third, that a new blockchain may utilize a new, additional virtual currency to be traded in tandem with or as a proxy for Bitcoins should not subject its creator to BSA regulation, so long as the alt-chain creator is not itself engaged in the exchange of currencies. For example, a blockchain might introduce a unit of exchange (say, "newcoin") that corresponds to Bitcoin but also encodes additional information or helps to facilitate additional services. So long as the creator itself does not exchange newcoin for legal tender or virtual currency, BSA regulation should not apply. Ripple, by contrast, went a step further by creating a new virtual currency *and* selling it for legal tender. If Ripple had instead designed its network to distribute XRP currency to third parties exclusively through mining, or if it had simply given away XRP to seed the network, or if it had undertaken some combination of the two, it would not have been involved in currency exchange and so would not have been subject to the BSA. In this respect, creators of new blockchain-based virtual currencies should view Ripple as a cautionary example.

Fourth and finally, BSA regulation should not hinder transactions between different decentralized virtual currency networks. As an initial matter, to the extent that such a transaction can be accomplished through distributed, algorithmic means—as with "pegged sidechains"[49]—there would seem to be no party to the transaction that could be regulated as an exchanger or administrator. Logically, the result should be the same for facilitated transactions. A user holding newcoin in his own newcoin wallet, for example, should be able to exchange it for Bitcoin in his own Bitcoin wallet without the transaction triggering BSA requirements, because such a transaction would constitute neither a transmission to another person nor a transmission to another location. As to the latter, FinCEN's virtual currency guidance explains that the sale of centralized virtual currency for legal tender "constitutes transmission to another location, namely from the user's account at one location (e.g., a user's real currency account at a bank) to the user's

convertible virtual currency account with [the virtual currency] administrator."[50] By contrast, the exchange of units of one decentralized virtual currency for units of another arguably does not actually transmit value to another location—the value remains in the user's possession, not in any account. FinCEN's guidance implicitly recognizes as much in that it limits the exchanger designation to a party that "accepts such de-centralized convertible virtual currency from one person *and* transmits it to another person…."[51] In other words, where a transaction is entirely in decentralized virtual currency, only transmission to a third party (for example, an account administered by a third party) can trigger BSA regulation. Nonetheless, further clarification on this point by FinCEN would be useful.

How these principles fit together is best illustrated by an example. The core Bitcoin network, as described above, uses a winner-take-all approach to awarding the proceeds from mining; in other words, only the first party to mine a new blockchain block obtains the proceeds for doing so. That, in turn, encourages centralization: with more mining power, a party has a greater chance of mining new blocks and profiting. To encourage decentralization, and thereby greater resiliency, a developer might create a buffered mining pool (i.e., a network of computers) that rewards users on a constant basis for contributing computing power to the pool, with the constant reward set to correspond with the statistically probable rewards of winner-take-all Bitcoin mining. To reduce transaction costs, such a network might employ a new virtual currency (say, "newcoin") to pay mining proceeds that could be exchanged among users and ultimately exchanged for Bitcoin. This new currency could be decentralized itself—that is, built atop a new blockchain that, in turn, interacts with the Bitcoin blockchain—or it could be centralized under the control of the pool operator.

Applying the principles described above, the creation and operation of such a system, if decentralized, would not be subject to BSA regulation for the same reason that Bitcoin is not: no party is engaged in money transmission services. Mining, after all, is not regarded

Regulations to Virtual Currency Mining Operations, FIN-2014-R001, at 3 (Jan. 30, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf.

49   Sidechain White Paper, *supra* note 19, at 8–10.

50   FinCEN Virtual Currency Guidance, *supra* note 38, at 4.

51   *Id.* at 5 (emphasis added).

as transmission, the exchange of newcoin among users would be nothing more than user activity, and the exchange of newcoin for Bitcoin would not transmit value to any third party or different location.

The result could be the same with a centralized currency, although the analysis is more complicated. To begin with, paying users for contributing computing power to the pool by crediting newcoin to their centralized accounts should not trigger BSA regulation, as the transaction is simply payment for services. Nor would it necessarily trigger regulation to redeem that newcoin in exchange for Bitcoin—that would be part of the same payment process. Transactions among users, however, present a more difficult question, as does allowing the redemption of newcoin in exchange for Bitcoin following such transactions. Potentially, such transactions could be regarded as, respectively, "transfers of value between persons or from one location to another,"[52] which would trigger BSA regulation. An argument could be made, however, that, in these circumstances, newcoin is a not a convertible virtual currency at all because it can be obtained, in the first instance, only though mining activities and cannot be purchased from the administrator. That argument gains force when viewed in light of the purposes of BSA regulation, as well as the coverage of existing regulation—the service described is just not susceptible to the concerns that animate anti-money laundering law. Those concerns are better and more easily addressed when transactions involve legal tender or transfer to other persons or locations, as provided for in FinCEN's guidance.

The more general policy point is that there is no obvious reason why anti-money laundering law should concern itself specifically with how value is represented in virtual currency systems, or with what name is given to units of value, as opposed to the movement and exchange of value. And that point is important because it implicates the interconnection and interaction of alternative blockchains and related technologies, which may employ different terms and units of measure "under the hood" for internal accounting purposes or to facilitate new applications, such that shifting between them (without in fact moving value) does

not necessarily implicate the purposes of anti-money laundering law. Application of such law, however, would impose enormous costs and burdens, frustrating the kind of frictionless interaction that is essential for blockchain alternatives to thrive.

BSA implementing regulations provide that "[w] hether a person is a money transmitter [subject to regulation] is a matter of facts and circumstances," and the example described here is the kind of gray area where further clarification of relevant facts and circumstances could provide useful regulatory certainty to innovative virtual currency services. Fortunately, FinCEN has been responsive so far in issuing administrative rulings addressing particular business models.[53] Where blockchain alternatives are concerned, there is a strong case for regulatory forbearance.

B. State Regulation of Money Transmission Businesses

While federal law requires registration of money transmission businesses, most states impose far more onerous licensure requirements for such businesses operating within their borders or, in some instances, servicing customers within their borders.[54] Given the wide variety of state regulatory regimes, as well as the

---

52   *Id.* at 4.

53   *E.g.*, FinCEN, *Application of FinCEN's Regulations to Virtual Currency Mining Operations*, FIN-2014-R001 (Jan. 30, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R001.pdf; FinCEN, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity*, FIN-2014-R002 (Jan. 30, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R002.pdf; FinCEN, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Payment System*, FIN-2014-R012 (Oct. 27, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R012.pdf; FinCEN, *Request for Administrative Ruling on the Application of FinCEN's Regulations to a Virtual Currency Trading Platform*, FIN-2014-R011 (Oct. 27, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R011.pdf; FinCEN, *Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency*, FIN-2014-R007 (Apr. 29, 2014), https://www.fincen.gov/news_room/rp/rulings/pdf/FIN-2014-R007.pdf.

54   *See generally* Marco Santori, *Bitcoin Law: Money Transmission on the State Level in the US*, CoinDesk (Sept. 28, 2013, 12:47 PM), http://www.coindesk.com/bitcoin-law-money-transmission-state-level-us/.

number of states engaged in regulation, compliance with state law presents a greater burden than even the BSA. Moreover, because many of these laws do not specifically address virtual currencies, much less decentralized virtual currencies like Bitcoin, even determining whether compliance is required can be a daunting task.[55] Without any attempt at being exhaustive, this section addresses generally state regulation of money transmission and stored value.

With respect to the regulation of money transmission services, a threshold question is whether virtual currency constitutes "money" at all. The relevant state laws frequently, although by no means unanimously, define "money" as "a medium of exchange that is authorized or adopted by a domestic or foreign government."[56] Some states limit the definition of money transmission to the transmission of "money" only. In such states, alt-chains and related services are unlikely to be subject to money transmission laws.

Likewise, "pure," decentralized alt-chains—i.e., those like pegged sidechains that serve the same functions as the Bitcoin blockchain—are unlikely to be subject to state money transmission laws for the same reason that the Bitcoin network itself is not: there is no party engaging in transmission to regulate. That said, parties using such alt-chains may be subject to regulation in the same way that traditional money transmission services that conduct transfers over telephone networks or the Internet are.

More complex Bitcoin blockchain alternatives, however, may trigger state regulatory requirements. For example, New York's "BitLicense" law comprehensively regulates "virtual currency business activity," which is defined to include "receiving virtual currency for transmission or transmitting virtual currency, except where the transaction is undertaken for non-financial purposes"; "storing, holding, or maintaining custody

or control of virtual currency on behalf of others"; "buying and selling virtual currency as a customer business"; "performing exchange services as a customer business"; and "controlling, administering, or issuing a virtual currency."[57] Although exceedingly broad, that definition expressly excludes the "development and dissemination of software."[58] The application of this new law is still uncertain, but it would most likely reach the buffered mining service described above, in both its decentralized and centralized forms. Operated in decentralized fashion, the service may be subject to regulation for "performing exchange services," which the statute defines to include "the conversion or exchange of one form of virtual currency into another form of virtual currency,"[59] if it exchanges newcoin for Bitcoin. Absent such exchange, however, it would probably not be subject to regulation. And a centralized version of the service would likely be subject to regulation for, among other things, "controlling, administering, or issuing a virtual currency," as well as holding newcoin on behalf of users.

The centralized version of the service would also likely fall under the definition of "money transmission" contained in the Uniform Money Services Act, which includes "receiving money or its equivalent value to transmit, deliver, or instruct to be delivered the money or its equivalent value to another location."[60] States have interpreted the Uniform Act to require licensure of businesses exchanging legal tender for virtual currency (or vice versa) and exchanging one virtual currency for another.[61]

Finally, many states require licensure of entities that issue or sell stored value. "Stored value" is often defined as "monetary value that is evidenced by an electronic record."[62] "Monetary value" often means a "medium

---

55   *See id.*

56   *See, e.g.*, Ariz. Rev. Stat. § 6-1201; Iowa Code Ann. § 533C.102; Kan. Rev. Stat. § 286.11-003(16). *But see, e.g.*, La. Rev. Stat. Ann. § 6:1032(12) (defining both "money" and "monetary value" as "currency or a claim that can be converted into currency through a financial institution, electronic payments network or other formal or informal payment system").

57   23 CRR-NY § 200.2(q).

58   *Id.*

59   *Id.* § 200.2(d).

60   *E.g.*, Wash. Rev. Code § 19.230.010(18).

61   *E.g.*, State of Washington Dep't of Fin. Insts., *Uniform Money Services Act: Interim Regulatory Guidance* (Dec. 8, 2014), http://www.dfi.wa.gov/documents/money-transmitters/virtual-currency-interim-guidance.pdf.

62   *See, e.g.*, Alaska Stat. § 06.55.990(21); Ark. Code.

of exchange, whether or not redeemable in money,"[63] and a "record" is often defined as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form."[64] The Uniform Money Services Act regulates any "device that electronically stores or provides access to funds and is available for making payments to others,"[65] which some states have interpreted to regulate virtual currency wallets.[66] Again, "pure," decentralized alt-chains are unlikely to be subject to regulation as stored value providers, but hybrid services—particularly those administering centralized user accounts—may be.

Unfortunately, the enormous diversity of state law makes it difficult to draw general conclusions other than that the creation of "pure," decentralized alt-chains is unlikely to trigger state licensure or regulatory requirements. Normatively, however, regulatory forbearance is warranted with respect to blockchain alternatives for the same central reason it is warranted under federal law: to facilitate low-cost transactions that provide little or no risk of abuse in themselves.

IV. Conclusion

Bitcoin's future will have to be very different from Bitcoin's past if it is to continue to succeed and grow as an ecosystem and economy. The next generations of Bitcoin-based services will most likely require capabilities that are impossible to implement on the core Bitcoin blockchain, but would still benefit enormously from being able to leverage it. Alt-chains and other blockchain alternatives are the key to unlocking this wave of innovation, as well as maintaining Bitcoin's most successful features: its decentralization, its independence, its speed, and its low friction. Given the immense benefits of these technologies, and the thoughtful approach that regulators like FinCEN have already taken to combating money laundering and other criminal uses in virtual currency services, regulators should proceed in this area with a light touch, clarifying the application of existing law to new services while exercising reasonable forbearance to avoid choking off new approaches.

Ann. § 23-55-102(19); Haw. Rev. Stat. § 489D-6; Iowa Code Ann. § 533C.102.

63   *See, e.g.*, Cal. Fin. Code § 2003(m); Conn. Gen. Stat. § 36a-596; Fla. Stat. Ann. § 560.103; Iowa Code Ann. § 533C.102; Kan. Stat. Ann. § 9-508(f).

64   *See, e.g.*, Alaska Stat. § 060.55.990(21); Ark. Code Ann. § 23-55-102(16); Cal. Fin. Code § 2003(t). But note that other states limit stored value to cards or other tangible objects. *See, e.g.*, Ind. Code § 28-8-4-19.5.

65   *E.g.*, Wash. Rev. Code § 19.230.010(27).

66   *E.g.*, State of Washington Dep't of Fin. Insts., *supra* note 61.