Synthesis Paper: Bitcoin: The Most Law-Abiding System Ever Created.

Dr. Craig Wright

Liberty University

14 Oct 2021

Abstract

It has been frequently argued that bitcoin is a “censorship resistant” immutable ledger that precludes law enforcement or government from acting against illicit actors in the system and precludes the freezing or seizing of assets. However, in this paper, it will be demonstrated that contrary to popular mythology, bitcoin can be easily frozen and seized under proceeds of crime legislation or even under the civil forfeiture rules. Furthermore, through the ability to enact punitive restraints against organizations that facilitate the operation of illicit transactions, law enforcement can ensure that the necessary controls that are designed to implement methodologies to ensure that financial crime using digital cash fails and that where criminal activity has been associated with digital currency or digital cash that the proceeds of crime can be removed from the benefit of the criminal actors. Importantly, as the bitcoin whitepaper notes, nodes enforce rules. Therefore, “any needed rules and incentives can be enforced with this consensus mechanism” (Wright, 2008b, p. 8).

Keywords: bitcoin, Cryptocurrency, tracing, proceeds of crime, enforcement against intermediaries.

Bitcoin: The Most Law-Abiding System Ever Created.

Kramer (2005) discussed a seminal case concerning peer-to-peer networks and the development of software for peer-to-peer networks in the Supreme Court decision of the Metro-Goldwyn-Mayer Studios Inc. v. Grokster, 125 S. Ct. 2764 (2005) case. To understand and move past much of the mythology around bitcoin and Blockchain systems, it becomes necessary to understand cases such as this and the nature of the Internet. Importantly, bitcoin nodes (also referred to as miners) and bitcoin exchanges are Internet businesses. As demonstrated in 2018 (Javarone & Wright, 2018, June), bitcoin nodes form a small-world network. All nodes broadcast to all other nodes (Wright, 2008b, p. 3). Consequently, as it is a commercial system, the necessity in broadcasting leads to losses for nodes (miners) that fail to adequately ensure connectivity across the network.

As a result of this network structure, there are very few nodes in the bitcoin network. The distinction between the reported numbers of nodes that some authors such as De Filippi and Loveluck (2016) falsely claimed to be in the thousands is that bitcoin is a transparent system where the only nodes are represented by those machines that create blocks on the network. The difficulty is that groups of individuals associated with crypto anarchy and criminal activities have used social media to spread a false narrative concerning the operation of bitcoin. The reality of the system is very different from this narrative. The narrative involves claims that bitcoin is "censorship-resistant" (Recabarren & Carbunar, 2018) and hence outside of the control of law enforcement.

The Electronic Frontier Foundation (EFF) developed the purported goal of bitcoin to be censorship resistant in 2011 in response to possible government action against WikiLeaks

(Grinberg, 2011). Unfortunately, as will be demonstrated in this paper, the touted resilience of bitcoin only works in respect of all legal transactions. Bitcoin can be seen to be one of the least resilient systems when applied to criminal activity. Bitcoin is traceable (Lane, 2013) and contrary to popular belief, bitcoin can be frozen and seized. The false mantra has already been questioned concerning how decentralization is not applied equally across all aspects of bitcoin, Blockchain or even Cryptocurrencies (Walch, 2019).

As Walch (2017) demonstrates, the entire field of Blockchain has been built upon misinformation and twisted vocabularies that are designed to confuse regulators. While Park et al. (2019) and other academics in the industry try to state how bitcoin has tens of thousands of nodes around the world that cannot be controlled, the reality is far different from the false narrative being promoted. In reality, they have never been more than 100 bitcoin nodes in the entire history of bitcoin. At any time, only three or four nodes hold the majority of computational power, hence enforcing rules on the network. The reason for this is that bitcoin is resistant to sybiling. This resistance to nefarious actors is achieved not by the nature of decentralization that is proposed but rather through the competitive proof of work system (Wright, 2017).

Through this, bitcoin nodes are restricted by introducing a proof of work system that works on a commercially focused verification mechanism that uses the introduction of a signaling process through proof of work. As a result, the consensus is agreed only from a small number of nodes on the network that can produce blocks. While some authors such as Thum (2018) opine on the cost of running a node on the bitcoin network and note that it can be in excess of several billion dollars a year to run a node (p. 44), the reality is that this is a key component of the design of bitcoin and is necessary to ensure that the system can be regulated

without the introduction of new law. Furthermore, the cost leads to the consolidation of nodes into commercial data centers.

When in 2008, using the pseudonym Satoshi the author of this paper stated that bitcoin was designed to end in data centers, many people argued that this was a design flaw (Kosik, 2018). In fact, this was a key aspect of the design of bitcoin and one of the fundamental reasons why bitcoin will continue and grow where systems such as eCash and eGold failed (Bećirović, 2014). These previous systems were designed to satisfy the desires of crypto-anarchist groups founded by individuals such as Tim May, who saw any interaction from the government as dangerous. Conversely, bitcoin was developed to ensure that the very problems that plagued systems based on a Cryptocurrency design would be mitigated.

While many in the "Cryptocurrency" industry argue that bitcoin is outside of the law because it's encrypted (Sapovadia, 2015; Dupuis & Gleason, 2020), the simple fact is that there is no encryption used in bitcoin at any point. The belief structure that has been developed using social media is different to the reality of the system. Bitcoin and any Blockchain, for that matter, are necessarily designed to be viewed by any party and audited at will. Therefore, the system is published in clear text with no encryption. Although digital signature algorithms (ECDSA) are used to secure transactions and maintain data integrity, the system in bitcoin does not encrypt the information at any point.

Consequently, the bitcoin Blockchain may be seen as an immutable database in the same manner that an Oracle system such as a financial accounting system associated with a Fortune 500 company is immutable. Under Sarbanes Oxley (S 302 & 404) legislation in the United States, it is illegal for any public company to run a financial systems database that is not

maintained immutably. To this end, authors such as Duncan and Whittington (2017) provide configuration guides on how information technology teams may implement WORM (Write Once Read Many) database settings that provide some of the same protections as Blockchain systems, including bitcoin. In addition, Antonopoulos et al. (2021) provide research papers into using cryptographic hash-based primitives on standard SQL ledgers. These techniques allow for many of the same controls as bitcoin but at a far greater cost.

Yet, with any accounting system updates and changes need to be made. As Mitra (2008) demonstrates in an analysis of the cost-effective maintenance of compliance records, immutable systems can be updated. Still, the requirement is that the errata entry does not change the original entry but adds and appends an extra record noting the mistake. Such changes are simple to be enacted within bitcoin or any Blockchain for that matter. Developers can change records within bitcoin, leaving a public record of the change. In part, this stems from the ability to restrict the number of nodes and operators within the system and the various requirements developed around Internet intermediaries following the decision of the Supreme Court concerning Grokster (Kramer, 2005).

Elkin-Koren (2005) discussed the liability of Internet service providers concerning the allowing of peer-to-peer network traffic. In many ways, much of the material in this article mirrors documentation preceding the creation and development of bitcoin (Wright, 2018a). This dissertation in law from the author of this paper details the various liabilities that apply to Internet intermediaries. Importantly, the basis of this research led to the development of bitcoin and Blockchain and the issue of the Bitcoin White Paper (Wright, 2008b). To this end, the work of Walch (rs) detailing how software developers may be considered fiduciaries becomes important. While interesting, the recommendations of Kasiyanto (2015) do not cover many of the

aspects of bitcoin and related systems as the author have failed to understand the technical aspects of bitcoin that make it easy to control by law enforcement and the judiciary.

Enforcement orders

A key facet of controlling major crimes such as people smuggling, and the organized drug trade derives from controlling the financial system. In an analysis of the tracing and confiscation of funds following proceeds of crime cases, Cribb (2003) documents many of the statutory powers that are associated with the ability of police officers to obtain search warrants, special procedure materials and production orders and to follow assets in financial investigations. In this paper, the author notes how the three stages of money-laundering include placement, layering, and integration. The ability to successfully launder money requires that the criminals involved obscure the trail of money as it moves.

Bitcoin removes many of these problems and stops criminal groups of money launderers from moving money without leaving permanent trails documenting the movement of all assets. Furthermore, multiple authors have noted how tracking and tracing bitcoin fund flows can be achieved (Cai & Wang, 2018) and how even hacked transactions may be followed across the bitcoin graph subnetwork (Goldsmith, Grauer & Shmalo, 2020). Consequently, computer scientists and researchers (Wu et al. 2021) are starting to realize that bitcoin can be followed even through mixers and anonymization. In any event, the same rules of tracing electronic funds (Smith, 1998) that traditionally applied to banking systems apply to bitcoin.

Moreover, the Law of Tracing (Hoyano, 1998) documents the principal problem of following when assets are mixed with similar substances. In traditional analysis, the mixing of grain has been handled by courts for centuries. The fungible tokens held within bitcoin

transactions may be analogized to individual grains in a mixed sale of wheat. In these scenarios, few criminal actions occur as the parties receiving stolen goods without adequately following up on the sources of the property lose rights under existing legal rules. As Chason (2018) notes, bitcoin has already been determined to be property through the actions of courts in multiple countries. As a consequence, the rules of property apply.

Whilst researchers such as Christiansen and Jarrett (2019) correctly note how the nature of bitcoin is analogous to a Post deposit facility or safe-deposit box and that the private key can be analogized as the physical key to such a system (p. 158), the authors fail to note that bitcoin is not a public-private key encryption system. Hence, like a safe deposit box, it is possible to gain access to the locked material. Whilst accessing safe-deposit boxes is not considered lightly, and the drilling of the deposit box comes with a cost (Šimonová, Čentéš & Beleš, 2019), but, equally, this cost can be seen in the requirements that would be associated with court actions to recover money associated with bitcoin and related systems.

Solutions to the Issue

Law enforcement has acted against Internet-based criminals for decades. In this process, law enforcement has seized Internet domains (Moringiello, 2003) and has closed ISP connections. Acting against Internet providers is an important component in controlling malfeasance in bitcoin and Blockchain-based systems. Despite the rhetoric around the resilience of bitcoin and related systems, the reality is that “Cryptocurrency” exchanges require both access to the global banking system and, more importantly, access to the Internet. For example, bitcoin nodes require access to the Internet to mine and process and verify bitcoin. Without this, access cannot achieve the primary function defined within the bitcoin White Paper (Wright, 2008, p. 3).

Consequently, these nodes operated commercially for billions of dollars per year (Thum, 2018, p. 44) cannot sustain operation without Internet connectivity.

Mellyn (2010, p. 1241) has argued that what the author defines as “virtual raids” form a growing trend in U.S. law enforcement to facilitate extraterritorial legal actions. The reality is that these are legal and powerful tools in the law enforcement arsenal. Further, these tools are a method in which law enforcement can legally control and seize criminal proceeds held on accessible bitcoin wallets even today. The developers of bitcoin are not anonymous. Walch (rs) has demonstrated that developers act as fiduciaries on the Peer network in the same manner that the developers of Grokster (Kramer, 2005) acted as fiduciaries in the provision of software purposely designed to breach copyright laws.

Digital currency exchanges such as Coinbase have achieved valuations in excess of US$100 billion (Crabb, 2021). Moreover, the operators are bitcoin nodes that have migrated to the United States (Sigalos, 2021) and are thus subject to U.S. law and court actions directly. Whilst each entity is subject to the long arm of U.S. law through domain seizures or Internet filtering, which would effectively devalue these organizations, the migration of entities into the United States and the political protections that are associated with the U.S. legal system come with a second edge that cuts into the ability to act anonymously.

An action against a digital currency exchange such as Coinbase would force Coinbase to take action and ensure that only legitimate versions of digital currency or Cryptocurrency were available. This reaction goes beyond merely the price of the shares. Companies such as coinbase are listed public companies in the United States. As with the banking scenario presented by Akgün, Altunbaş and Uymaz (2021), financial fiduciaries such as Coinbase are covered by

existing legislation that criminalizes financial irregularities and associations with money-laundering. These actions present a dilemma to the CEO of the company, who can face up to 20 years in prison for each offence. In this, failure to act against digital cash systems that enable or facilitate crime is itself a crime.

The end analysis is that while bitcoin is incredibly resilient when used within existing legal frameworks, once the mythology is dispensed with it can be seen to be a proverbial nightmare for criminal activity. The ease of tracing, following, and seizing bitcoin is far simpler than either digital cash or anything in the global banking system. The ability of the United States government to put pressure against Internet service providers, the main registers and corporations provides an unlimited level of power against criminal activity while also providing strong protections against the individual.

Conclusion and Christian Worldview

Aiding criminal activities and conducting fraud is little better than theft, lying and deception rolled into one. Scripture states, “Woe to those who call evil good and good evil, who put darkness for light and light for darkness, who put bitter for sweet and sweet for bitter.” (Isaish 5:20). Those who argue that bitcoin is about freedom and yet do nothing to stop the various crimes and illegal activity financed using the system (Foley et al., 2019) aid in the problem. Money laundering and other crimes remain a problem being promoted using “Cryptocurrencies” and other digital cash systems (Forgang, 2019).

God does not want dirty money to be circulated. The story of Judas and the silver coins paid in the betrayal of a friend and his God (Matthew 27:5) shows only one example of the prohibition against dirty money. Deuteronomy 23:18 provides another example of how money

can be detestable to God when not earned and through wrong action. In acquiring dirty money exchange currency in this manner, those involved are morally unclean lives (Ezekiel 7:19) and those that are facilitating actions for which they will be held accountable (Revelations 18:4,5,8,24). Consequently, it becomes important to remember that it is not merely following a right past but also not turning a blind eye to the criminal actions of others that matters.

References

Akgün, A.İ., Altunbaş, Y. & Uymaz, Y. (2021), "The relationship between financial reporting standards and accounting irregularities: evidence from U.S. banks", *Journal of Financial Crime*, Vol. 28 No. 4, pp. 1161-1178. https://doi.org/10.1108/JFC-10-2020-0218

Andrews, N. (2018). Enforcement of Court Judgments and Orders. In *The Three Paths of Justice* (pp. 165-177). Springer, Cham.

Antonopoulos, P., Kaushik, R., Kodavalla, H., Rosales Aceves, S., Wong, R., Anderson, J., & Szymaszek, J. (2021, June). SQL Ledger: Cryptographically Verifiable Data in Azure SQL Database. In *Proceedings of the 2021 International Conference on Management of Data* (pp. 2437-2449). https://doi.org/10.1145/3448016.3457558

Bećirović, S. (2014). Challenges facing e-money. *University Journal of Information Technology and Economics*, *1*, 28-36.

Cai, L., & Wang, B. (2018, December). Research on tracking and tracing bitcoin fund flows. In *2018 IEEE 4th Information Technology and Mechatronics Engineering Conference (ITOEC)* (pp. 1495-1499). IEEE. DOI: 10.1109/ITOEC.2018.8740574.

Chason, E. D. (2018). How bitcoin functions as property law. *Seton Hall L. Rev.*, *49*, 129.

Christiansen, N. B., & Jarrett, J. E. (2019). Forfeiting Cryptocurrency: Decrypting the Challenges of a Modern Asset. *US Att'ys Bull.*, *67*, 155.

Crabb, J. (2021). Opinion: Coinbase IPO will be a turning point. *International Financial Law Review*.

Cribb, N. (2003), "Tracing and confiscating the proceeds of crime", *Journal of Financial Crime*, Vol. 11 No. 2, pp. 168-185. https://doi.org/10.1108/13590790410809103

De Filippi, P., & Loveluck, B. (2016). The invisible politics of bitcoin: governance crisis of a decentralized infrastructure. *Internet Policy Review*, *5*(4).

Duncan, B., & Whittington, M. (2017). Creating and Configuring an Immutable Database for Secure Cloud Audit Trail and System Logging. *International Journal On Advances in Security*, *10*(3&4), 155-166.

Dupuis, D. & Gleason, K. (2020), "Money laundering with cryptocurrency: open doors and the regulatory dialectic", *Journal of Financial Crime*, Vol. 28 No. 1, pp. 60-74. https://doi.org/10.1108/JFC-06-2020-0113

Elkin-Koren, N. (2005). Making technology visible: Liability of internet service providers for peer-to-peer traffic. New York University Journal of Legislation and Public Policy, 9(1), 15-74.

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies?. *The Review of Financial Studies*, *32*(5), 1798-1853.

Forgang, George, "Money Laundering Through Cryptocurrencies" (2019). *Economic Crime Forensics Capstones*. 40. https://digitalcommons.lasalle.edu/ecf_capstones/40

Goldsmith, D., Grauer, K., & Shmalo, Y. (2020). Analyzing hack subnetworks in the bitcoin transaction graph. *Applied Network Science*, *5*(1), 1-20. https://doi.org/10.1007/s41109-020-00261-7

Grinberg, R. (2011). Bitcoin: An innovative alternative digital currency. *Hastings Science & Technology Law Journal*, *4*, 160.

Hoyano, L. C. (1998). The Law of Tracing by Lionel D. Smith. *Alberta Law Review*, 810-810. https://doi.org/10.29173/alr1494

Kosik, B. (2018). Data centers used for bitcoin mining: Data centers used for bitcoin mining have significant differences from their commercial data center counterparts. *Consulting Specifying Engineer*, *55*(5), 20-25.

Kramer, K. M. (2005). Metro-Goldwyn-Mayer Studios v. Grokster-The Supreme Court's Balancing Act Between the Risks of Third-Party Liability for Copyright Infringement and Rewards of Innovation. *Santa Clara Computer & High Tech. L.J.*, *22*, 169.

Javarone, M. A., & Wright, C. S. (2018, June). From Bitcoin to Bitcoin Cash: a network analysis. In *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems* (pp. 77-81).

Kasiyanto, S. (2015). Regulating peer-to-peer network currency: Lessons from Napster and payment systems. *Journal of Law, Technology and Public Policy®*, *1*(2), 26.

Lane, J. (2013). Bitcoin, silk road, and the need for a new approach to virtual currency regulation. *Charleston L. Rev.*, *8*, 511.

Mellyn, J. (2010). Reach out and touch someone: The growing use of domain name seizure as a vehicle for the extraterritorial enforcement of U.S. law. *Geo. J. Int'l L.*, *42*, 1241.

Mitra, S. (2008). *Trustworthy and cost effective management of compliance records*. University of Illinois at Urbana-Champaign.

Moringiello, J. M. (2003). Seizing Domain Names to Enforce Judgments: Looking Back to Look to the Future. *U. Cin. L. Rev.*, *72*, 95.

Park, S., Im, S., Seol, Y., & Paek, J. (2019). Nodes in the bitcoin network: Comparative measurement study and survey. *IEEE Access*, *7*, 57009-57022. https://doi.org/10.1109/ACCESS.2019.2914098

Recabarren, R., & Carbunar, B. (2018). Tithonus: A bitcoin based censorship resilient system. *arXiv preprint arXiv:1810.00279*.

Sapovadia, V. (2015). Legal issues in cryptocurrency. In *Handbook of Digital Currency* (pp. 253-266). Academic Press. https://doi.org/10.1016/B978-0-12-802117-0.00013-8

Sigalos, M. (2021). *U.S. officially the top destination for bitcoin miners, beating out China for the first time*. Crypto Decoded. Retrieved 13 October 2021, from https://www.cnbc.com/2021/10/13/us-beats-china-as-the-number-one-destination-for-bitcoin-miners.html.

Šimonová, J., Čentéš, J., & Beleš, A. (2019). Financial analysis of innovative forms of money. *Entrepreneurship and Sustainability Issues*, *7*(1), 69.

Smith, L. D. (2020). Tracing and Electronic Funds Transfers. In *Restitution and Banking Law* (pp. 120-134). Informa Law from Routledge.

Thum, M. (2018). The economic cost of bitcoin mining. In *CESifo Forum* (Vol. 19, No. 1, pp. 43-45). München: ifo Institut-Leibniz-Institut für Wirtschaftsforschung an der Universität München.

Watts, D. J., & Strogatz, S. H. (1998). Collective dynamics of 'small-world' networks. *nature*, *393*(6684), 440-442. https://doi.org/10.1038/30918

Walch, A. (2017). blockchain's treacherous vocabulary: One more challenge for regulators. *Journal of Internet Law*, *21*(2).

Walch, A. (2019). Deconstructing'Decentralization': Exploring the Core Claim of Crypto Systems. *Crypto Assets: Legal and Monetary Perspectives (OUP, Forthcoming)*.

Walch, A. In Code (rs) We Trust: Software Developers as Fiduciaries in Public Blockchains. In *Regulating Blockchain* (pp. 58-82). Oxford University Press.

Wright, C. S. (2008a). The Impact of Internet Intermediary Liability. *Available at SSRN 2953929*.

Wright, C. S. (2008b). Bitcoin: A peer-to-peer electronic cash system. *Available at SSRN 3440802*.

Wright, C. S. (2017). Proof of Work as it Relates to the Theory of the Firm. *Available at SSRN 2993312*.

Wu, J., Liu, J., Chen, W., Huang, H., Zheng, Z., & Zhang, Y. (2021). Detecting mixing services via mining bitcoin transaction network with hybrid motifs. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*. DOI: 10.1109/TSMC.2021.3049278.