Are Cryptocurrencies Truly Trustless?

Usman W. Chohan

Abstract A common narrative of cryptocurrencies presents them as "trustless," decentralized, and autonomous systems. The "trustlessness" is meant to suggest lack of need for third-party verification in blockchain technologies, but the term has been somewhat conflated with broader connotations of "trust." This chapter draws out that nuance, and critically assesses that claim, by emphasizing the human element of trust in cryptocurrencies across various contexts. It does so by highlighting four activities that require both direct human intervention and direct human participation, including: "hard forks" to directly change protocols, the management of cryptocurrency exchanges, the emission of ICOs, and investor recourse to traditional governance institutions including courts of law. The findings of the chapter therefore suggest that the cryptocurrency space is not "trustless" in every sense as it is still reliant on the trust-element in human agency and structure.

1 Introduction

As the appeal of cryptocurrencies has grown, there are certain adjectives that have been ascribed to them to emphasize their distinctions with the monetary systems of traditional finance. Four of those adjectives are decentralized, autonomous, immutable, and trustless. Decentralization is meant to refer to the distribution of information across a panoply of users on the blockchain system without centralized control (see Chohan 2017a). Autonomous refers to the ability of the system to work under pre-programmed algorithms without the need for constant human interventions or oversight (Chohan forthcoming-b). Both of these terms are encapsulated in the Decentralized Autonomous Organization (DAO), a short-lived experiment based on an offshoot of blockchain technology which, despite practical failings (hacks), constituted a conceptually rich topic of enquiry (see Chohan 2017b). Immutability refers to the fact that tampering and erasure cannot generally occur once information is put into the blocks of a chain.

U. W. Chohan (✉)
UNSW School of Business, The University of New South Wales, Sydney, NSW, Australia
e-mail: u.chohan@adfa.edu.au

S. Goutte et al. (eds.), *Cryptofinance and Mechanisms of Exchange*, Contributions to Management Science, https://doi.org/10.1007/978-3-030-30738-7_5

Yet the fourth adjective, and the one of greatest import to this chapter, is trustlessness, It does not refer to the absence of trust, but rather to the absence of a need for trust in the system. Specifically, it was intended to refer to the lack of third-party verification requirements that blockchain allows for when it solves the double-spending problem (Chohan 2017c). However, the term has been somewhat conflated with broader connotations of "trust." By extension, an insinuation in the popular discourse (see discussions in Chohan 2019a, b) has been that blockchain technologies have no significant trust-requirements of any sort.

In other words, a point of nuance has been lost. Although third-party verification is effectively not required in the blockchain architecture and it is therefore "trustless" in one sense, there is indeed a significant element of trust that permeates the socioeconomic realm of cryptocurrency transactions. Whenever trust is compromised in the commercial transactions of cryptocurrencies, the risk to their viability as monetary instruments grows. Infractions along those lines might include: malpractice in cryptocurrency exchanges (referred to henceforth in portmanteau as "cryptoexchanges"), hacking, thefts, deception, money laundering, Ponzi schemes, and fraud (see Chohan 2018a, b, c). As such, there is a need to correct the dissemination of inaccurate representations of cryptocurrencies among a public audience, which includes investors who have made decisions to buy and sell cryptocurrencies without being entirely aware of the nature of "trustlessness."

Why should so much attention be paid to what might appear to be a semantic issue in non-specialist popular discussions? To put it plainly, trust is the bedrock of all sustained commercial life. Cryptocurrencies have suffered a dent in their popular appeal and credibility because of issues of trust which, although not emanating directly from the structure of blockchains, have made themselves manifest in the social realm where anonymous users and groups have compromised trust to the ultimate detriment of investors and network participants (Chohan 2018a, b, c). By extension, this has led to reputational damage to cryptocurrencies to a degree that might threaten their long-term viability, since their wider adoption is necessary for them to become effective complements (and for idealists: substitutes) to traditional monetary instruments.

With this in mind, the aim of this chapter is to critically assess and draw distinctions in the concept of "trustlessness" as it is understood in the realm of cryptocurrencies (see Chohan 2019a). To do so, the chapter first reviews the academic literature as it has referred to the trustless element in blockchain, including through normative expectations about the advantages that it is thought or expected to bring. The chapter then analyses and highlights four activities that require both direct human intervention and participation, including: "hard forks" to directly change protocols, the management of cryptocurrency exchanges, the emission of initial coin offerings (ICOs), and investor recourse to traditional governance institutions including courts of law. These activities emphasize the fact that, the lack of need for third-party verification notwithstanding, the cryptocurrency space is not truly "trustless" as it is still reliant on the trust-element in human agency and within human trust-bound structures. A final section concludes with a discussion of the cryptoanarchist philosophical implications of trust in trustless systems.

2 The Promise de Trustlessness

It is of great appeal to a segment of cryptocurrency participants that the blockchain system operates in a "trustless" manner without the need for third-party verification. Early academic work on blockchain technology has generally commended this trait, and highlighted it as a significant advantage of cryptocurrencies vis-à-vis the traditional financial system. For example, Forogolu and Tsilidou emphatically state the point that "the whole thing about blockchain-based architectures is that they allow trustless transactional activity," (Foroglou and Tsilidou 2015, p. 2), and Kiviat makes the bold assertion that "trustless means that—for the first time in history—exchanges for value over a computer network can be verified, monitored, and enforced without the presence of a trusted third party or central institution," (Kiviat 2015, p. 574). Bahga and Madisetti explain that "peers do not [*sic*] need a trusted intermediary for interacting with each other," since a "blockchain network is not controlled by a central authority and all the transactions are verified and validated by a consensus among the peers" due to which "the peers do not need to trust each other." (Bahga and Madisetti 2016, p. 543).

Because of this trustless element, blockchains have been advocated in numerous applied contexts. For example, Banafa claims that "the decentralized, autonomous, and trustless capabilities of the blockchain make it an ideal component to become a foundational element of IoT [Internet of Things] solutions." (Banafa 2017, p. 2). Similarly, Kurtulmus and Daniel propose that "it is possible to create contracts that offer a reward in exchange for a trained machine learning model for a particular data set [which] would allow users to train machine learning models for a reward in a trustless manner," (Kurtulmus and Daniel 2018, p. 1802).

Along similar lines, Schaub et al. propose a reputation system for e-commerce using blockchain which would be trustless because of its privacy-preservation mechanism (Schaub et al. 2016). Another intriguing example is when Klems et al. propose the concept of *trustless intermediation* in the context of decentralized service marketplaces, claiming that "by leveraging blockchain-enabled smart contracts, we eliminate the need for trust in marketplace intermediaries and reduce barriers of entry, lock-in, and transaction costs," going as far as to say that they would be "removing now *obsolete* trust-establishing mechanisms," (2017, p. 731, emphasis added). Strong wording such as "obsolete" goes to highlight the degree to which conventional notions of trust appear to have been superseded by the novel promise of blockchain trustlessness. Yet as mentioned in the previous section, this reflects a conflation of the specific trustless trait of blockchain (for third-party verification), with broader considerations of "trust." The following sections present examples of how the fostering and nurturing of trust still remain necessary due to a dimension of human engagement. The human element is highlighted in four instances: direct interventions of "hard forks," the [mis]management of cryptoexchanges, the emission of initial coin offerings, and recourse sought by investors in traditional accountability institutions.

3 Hard Forks

The first example of human engagement which requires an element of trust is in hard forks, which are implemented to remedy or repair issues in the establishment of blocks on a cryptocurrency chain. Put simply, a hard fork is a radical change to the protocol that makes previously invalid blocks/transactions valid, and in that sense, represents a direct human intervention in blockchain construction (see Chohan 2017b, 2019a). Hard forks constitute a permanent divergence from a previous version of the blockchain, and so require all users (or "participant nodes") to upgrade to the latest version of a protocol software (see Destefanis et al. 2018). This is a trust-based activity in that all participants must voluntarily adapt to a remedied version and agree to continue along a new path, thereby agreeing to no longer accept another version of the blockchain.

The term "fork" is used because diagrammatically there is a split in the chain which resembles the prongs of a utensil, where one path follows the new and upgraded blockchain, while the other path continues along the older chain (Chohan 2017b). Meanwhile, the distinction of "hard" and "soft" refers to the means of splitting the blockchain: a hard fork creates two blockchains, and a soft fork is meant to result in but one chain.

The splitting of the path of a blockchain is accomplished through the deliberate invalidation of transactions confirmed by nodes that have not been upgraded to the new version of the protocol software. Human engagement lies in those participant nodes on the old chain coming to the realization that their version of the blockchain is outmoded, thus requiring their voluntary upgrade onto the latest version. For larger blockchain instruments, this tends to occur within a brief interval, but it is nonetheless a function of human decisions and interventions.

The most important reasons for the implementation of hard forks include: correcting important security risks found in older versions of the code; adding new functionalities; and reversing transactions (see Destefanis et al. 2018). A famous example of the former objective (remedial action against security risks) occurred during the hack on the DAO ("Decentralized Autonomous Organization," see Chohan 2017b). As Chohan recounts, nearly as soon as the DAO was launched, it became the victim of predatory attacks (Chohan forthcoming-b), which then necessitated human intervention to remedy the nearly $50 million worth of funds that were compromised. Following the hack, the blockchain Ethereum community voted unanimously in favour of a hard fork to undo the transactions which were responsible for the siphoning of the funds (denominated in tokens of the DAO). Technically, the voting mechanisms did not unwind the transaction history of the DAO, but instead relocated funds tied to the DAO to a new smart contract (see "smart contracts" in Chohan 2017b), which was programmed to allow the original token holders to withdraw them. Evidently, voting in this instance cannot be construed as anything but a human trust-based activity, while the process of overseeing the restoration of the funds of the DAO also constitutes a trust-based action (the trust being instilled in the curators to execute).

But whereas many hard- and soft-forks represent a consensus-based effort to remedy a problem in a blockchain system, not all such interventions are benevolent. The case of the exchange Quadriga CX, which shall be discussed in subsequent sections, also involved the insertion of a hard fork which, according to previous legal counsel, "started the company down a path of lawlessness," (Duhaime 2019). Hard forks thus represent one of the various human trust-based elements in the realm of cryptocurrencies, since assigned persons act deliberately to alter the process of blockchain formation towards a new direction.

4 Cryptocurrency Exchanges

Cryptocurrency exchanges (also abbreviated as portmanteau to "cryptoexchanges") are clearinghouses, traders, stores and/or market-makers for the sale and purchase of cryptocurrencies (Chohan 2018a). They can be described as "nodes for the transactions of crypto instruments between buyers and sellers [and the] juncture at which the human element becomes crucial," (Chohan 2019b, p. 3). Given the proliferation of cryptoinstruments and the widening public interest in ownership of cryptocurrencies, the number of cryptoexchanges had ballooned in the past few years (although much market consolidation is now taking place). As of this writing, it is estimated that there are more than 200 cryptoexchanges worldwide, amounting to a daily volume of nearly $15 billion US dollars across more than 8000 daily transaction pairs (Coinmarket 2019). Some of larger and more famous exchanges currently in operation include Binance (Maltese), Huobi (Singaporean), and Upbit (South Korean).

Cryptoexchanges may exchange pairs of cryptocurrencies or deal in fiat currencies, and can either charge bid-ask spreads when acting as market-makers or charge fees as matching platforms (Chohan 2018a). These exchanges occupy a position of centrality within the commercial ambit of cryptocurrencies. However, their mushrooming has not come without drawbacks, emanating largely from the unregulated nature of these spaces (Chohan 2018a, 2019b). Situated largely outside the regulatory space of traditional finance (see Chohan forthcoming-a), cryptocurrency exchanges suffer from substantial risks of theft, malpractice, fraud, and losses of abrupt shutdowns, and two examples are illustrative of this: Mt. Gox and Quadriga CX (Chohan 2019b).

4.1 Mt. Gox

Mt. Gox was a behemoth exchange located in Japan (but with mostly Western managers) which was handling up to 70% of the global Bitcoin trades during the period 2013–2014 (Chohan 2018a). In February 2014, Mt. Gox suspended trading, closed its website and services, and filed for bankruptcy protection from creditors,

thereby spreading panic throughout the cryptocurrency markets. Two months later, the company began liquidation proceedings. It should not be lost on observers that human trust-based dealings were violated in the Mt. Gox episode, and it is important to see why.

At the time of the company's immediate crisis, Mt. Gox announced that approximately 850,000 bitcoins belonging to customers and to the company had gone missing, suggesting that they had been stolen (Chohan 2018a). This amounted to more than $450 million at the time. In the period since, 200,000 bitcoins have been "found," and the reasons for the disappearance: theft, fraud, mismanagement, or a combination thereof; have also been clarified.

Evidence presented in April, 2015 by the Tokyo-based security company WizSec concluded that "most or all of the missing bitcoins were stolen straight out of the Mt. Gox hot wallet over time, beginning in late 2011," but also that mismanagement and fraudulent practices had permeated the workings of Mt. Gox (Chohan 2018a, 2019b). An alleged internal crisis management document that was leaked had claimed that the company was insolvent, after having lost 744,408 bitcoins in a theft which went undetected for years (Chohan 2018a). With this, Mt. Gox's French CEO Mark Karpelès was arrested in August, 2015 by the Japanese police and charged with fraud and embezzlement, and manipulating the Mt. Gox computer system to increase the balance of a private account. Pursuant to interrogation, Japanese prosecutors accused him of misappropriating ¥315 M ($2.6 M) in Bitcoin deposited into their trading accounts by investors at Mt. Gox, and moving it into an account he controlled, approximately 6 months before Mt. Gox failed in early 2014.

4.2 Quadriga CX

A second disaster in the cryptoexchange category was embodied by the Canadian exchange Quadriga CX, which up until the death of its founder in late 2018, was the largest exchange in Canada by volume traded (Chohan 2019b). Quadriga CX initially took great steps to comply with regulation (Duhaime 2019), and was responsible for establishing the second Bitcoin automated-teller machine (ATM) in Vancouver, British Colombia in January, 2014. Rapid expansion, as well as the overall bullish trend in cryptocurrency prices, propelled Quadriga to a substantial position within the international cryptocurrency space by 2017. However, Quadriga's progress was marred by difficulties similar to those of Mt. Gox (see discussion in Chohan 2019b), including persistent difficulties in allowing customers to withdraw dollars in exchange for cryptocurrency.

At the centre of both the rise and fall of Quadriga was its founder, Gerald Cotten, who had used extreme cybersecurity and anti-hacking measures to protect the access to held cryptocurrencies. In December, 2018, Mr. Cotten passed away from complications relating to Crohn's disease while he was in India building an orphanage. As the key man behind the Quadriga CX exchange, only he had total access to the entirety of the exchange's holdings. As of January, 2019, that holding amount was

equivalent to $190 million. Having rigorously protected the accessibility to the cryptoassets, Cotten's death forced the exchange to seek creditor protection, since it could not access its holdings to repay its counterparties. Accusations have been made, which are still under court proceedings as of this writing, that the underlying cryptocurrency assets may not have been present in the stipulated amounts—which is to say that the exchange did not have these holdings to repay counterparties in any case (Chohan 2019b), thereby suggesting fraud and theft.

Chohan (2019b) has highlighted that this creates the key man risk in the cryptocurrency space, which is usually associated with traditional financial firms that depend on the competency, power, or knowledge-base of a single individual. This is counterintuitive, given that cryptocurrencies purport to be decentralized, autonomous, and trustless systems. The risk of one individual's shortcomings, therefore, should not have a significant impact on the function of cryptocurrency systems, including exchanges. Yet the reality, as evidenced by Quadriga CX, is that these risks continue to loom large (Chohan 2019b).

Aside from the two major cryptoexchanges of Mt. Gox and Quadriga CX, there have been a slew of thefts, frauds, abrupt shutdowns, and regulatory actions against other exchanges (Chohan 2018a, b, c). Hong Kong-based Gatecoin was shut down due to failure to recover stolen funds in 2019, and the US Federal Bureau of Investigation (FBI) seized the assets of 1Broker, based in the Marshall Islands, for breaking a series of US security laws in 2018. The Australian financial intelligence agency AUSTRAC shut down two exchanges in the country after discovering links to illicit activities between the cryptoexchanges and organized crime rings in 2018. Regulatory authorities are also denying the applications of new exchanges for failing to meet standards relating to operations and compliance (Coin Asset Thailand is but one recent example).

Further still, the economic pressures on cryptocurrencies owing to weak demand and cheap production (mining) of cryptocurrencies have also led to closures at smaller exchanges (Liquid in the Ukraine being but one example). This in turn is fostering a consolidation in the cryptoexchange space, with larger exchanges such as Binance and Coinbase acquiring smaller players (Chohan 2018a).

All of this market activity is quintessentially human, not just in the illegal or dubious activities, but also in the categories of regular market behaviour (consolidations etc.). The trust-element is particularly important in this context as the malpractices of certain exchanges and investor-participants has had reputational consequences for cryptocurrencies as a whole. Those malpractices are premised on human drivers (greed, competitiveness) and so they sully the repute of cryptocurrencies, itself a non-traditional financial and technological space, in a manner that may jeopardize the viability of the space as a whole in the longer run. What is to be emphasized is that such activities are premised on inherently human traits, and so the conflation of third-party "trustlessness" with the trust requirements of cryptocurrency market behaviour is misleading.

5 Initial Coin Offerings

An Initial Coin Offering (ICO) is the mechanism by which capital is raised from investors through the emission of cryptocurrency coins (or "tokens," see Adhami et al. 2018; Chohan 2017d), usually in exchange for another cryptocurrency or for fiat money such as the United States dollar or the Euro (Fisch 2019; Chohan 2019a, b), and often expressed as a percentage of total newly issued currency (Catalini and Gans 2018). Adhami et al. describe ICOs as "open calls for funding promoted by organizations, companies, and entrepreneurs to raise money through cryptocurrencies, in exchange for a "token" that can be sold on the Internet or used in the future to obtain products or services and, at times, profits," (Adhami et al. 2018, p. 64). Therefore, ICOs can be seen as a new motor for raising investment capital (Howell et al. 2018; Lee et al. 2018; Adhami et al. 2018; Catalini and Gans 2018), and they offer "significant promise for new startups in the cryptocurrency space as means of quicker and easier capital raise," (Chohan 2017d, p. 3).

Yet there is a quintessential element of trust that is necessary for the emission of coins and their subsequent trading, and as this section of the chapter discusses, that trust has been compromised to quite an extent. As with cryptoexchanges, hard forks, and cryptocurrencies themselves, ICOs have mostly occurred in the online realm that lies beyond regularized and traditional finance, devoid of the structures of financial regulation which allow for contemporary capitalism to function in a more lawful and stable manner (Fisch 2019; Howell et al. 2018; Chohan 2017b, 2019a, b).

ICOs are "bypassing any regulation that normally applies to businesses placing securities to retail investors, [and so] dozens of developer teams and entrepreneurs collect money in absence of official prospectuses, with no particular protection for contributors and disclosing only a very limited set of information," (Adhami et al. 2018, p. 65). Furthermore, "there are many scams, jokes, and tokens that have nothing to do with a new product or business," (Howell et al. 2018, p. 1).

To this point, ICOs have "low contributor protection, a limited set of available information, [almost] no supervision by public authorities, and [almost] no relevant track record for proponents," (Adhami et al. 2018, p. 73). Benedetti and Kostovetsky (2018) have surmised that ICOs are in fact a digital reiteration of the *Tulip Mania* which engulfed Europe in the early decades of the seventeenth century. Large numbers of ICOs have resulted in "substantial scam-artistry, phishing, Ponzi schemes, and other shenanigans" (Chohan 2017d, p. 5). According to one study which examined the lifecycle of ICOs from the initial proposal to the final phase of trading on a crypto-exchange, more than 80% of ICOs emitted in 2017 were scams (Satis Group 2017), amounting in value terms to more than $1 billion US dollars (value estimates of the total capital raised in that year was $11 billion). For 2018, another ICO advisory firm estimated that, for more $20 billion in capital raised from 789 ICOs, the 10 largest ICO scams swindled a combined amount of more than $700 million (Fortune Jack 2018). Benedetti and Kostoyevsky have determined that only 44.2% of startups survive after 120 days from the end of their ICOs (Benedetti and Kostovetsky 2018).

Much of this is premised on the breach of trust in the cryptocurrency domain due to lackadaisical levels of investor due diligence, the wildly inflated promises of transformation made by issuers, and the quintessential human traits of greed and "fear of missing out" (colloquially termed "FOMO"). Humans are the ones exerting agency, irrespective of the lack of third-party verification that characterizes blockchain technologies. Indeed, investors who have dealt with dubious ICOs have fallen prey to the seemingly endless rhetorical promises of the cryptocurrency realm, but there was far less complaint about ICOs when cryptocurrency prices were at their zenith (see Chohan 2018a, b, c). Rather, it was when the prices declined that the furore of losing investors spread across the online forums and into the public sphere.

As with cryptoexchanges, the scope of widespread financial abuse through ICOs came to jeopardize the reputation of the space as a whole (Chohan 2019a, b), with many small- and large-scale investors demanding recourse and recovery of funds. The dilemma that this has posed for recourse to traditional (human-led) institutions of regulation is discussed in the next section.

6 Recourse of Traditional Structures

Given that the inherent design of cryptocurrencies is to situate them outside the traditional financial architecture (Fisch 2019; Howell et al. 2018), any demand by investors for financial recourse from traditional institutions poses a dilemma for regulatory authorities around the world. Initially, the dilemma sprung from the sheer bewilderment at the meteoric rise of the sector (see Chohan 2017b, 2018c), but since then the dilemma has been spurred by the need to strike a balance between fostering innovation and imposing accountability (see Chohan forthcoming a, b). The Securities and Exchange Commission (SEC) and Commodities Futures Trading Commission (CFTC) have framed that balance as the need for regulations to "set and enforce rules that foster innovation, while promoting market integrity and confidence," (Clayton and Giancarlo 2018).

After all, it is humans who have wronged other humans, only to seek remedial action from yet other humans for those wrongs. A sense of trust has been breached, and now the onus is on regulatory authorities to restore trust. Two instances are illustrative of this problem, (1) the SEC and CFTC regulation on ICOs, and (2) the aforementioned case of Quadriga CX exchange.

6.1 SEC and CFTC as Regulators

First, the onus for the restoration of trust has fallen on regulators, particularly American authorities, who have had the richest experience with the regulation of cryptocurrencies thus far. Specifically, action has come from the SEC and CFTC in

the United States (Chohan forthcoming-a). As far back as 2017, the Chairman of the SEC had insisted upon investors that there was a need for investors to exercise greater caution, given the possible breaches of trust and the financial dangers of being misled by fraudulent cryptocurrency agents (Clayton 2017). He also demanded that laws "provide that investors deserve to know what they are investing in and the relevant risks involved," (Clayton 2017).

The SEC chairman then declared that the commission's Division of Enforcement would "police this area vigorously and recommend enforcement actions against those that conduct initial coin offerings in violation of the federal securities laws," (Clayton 2017). These are the sorts of breaches of trust that regulatory authorities have warned of and also taken action against. Chohan notes that a substantial series of enforcement actions have since been taken against ICO issuers and cryptoexchanges who have not complied with securities regulation (Chohan forthcoming-a), a few examples of which have been mentioned in previous sections of this chapter.

In June, 2018, a joint statement was issued by the chairmen of the SEC and CFTC (see Clayton and Giancarlo 2018) which emphasized closer cooperation between their agencies while insisting upon the need for regulations to strike a balance between fostering innovation on one hand and promoting market integrity and confidence on the other. Both of these regulatory bodies are setting the trend for international regulators in protecting investors and regularizing ICOs and cryptoexchanges, particularly since a growing public pressure in the wake of volatile (and declining) prices of cryptocurrencies and a massive scale of fraudulent activity has fomented investor anger and the desire for recourse in traditional institutions.

6.2 Quadriga CX in Court

The aforementioned Quadriga CX case, with the death of its CEO Gerald Cotton, also embodies an example of both (1) the key man risk, which is a human problem of entrusting an individual with excess knowledge or power (Chohan 2019b), and (2) the trend of investors seeking recourse in human institutions. As mentioned previously, upon the announcement of the Mr. Cotten's untimely demise in India while on a humanitarian trip, a frantic reaction pervaded the cryptocurrency markets, This is because the underlying amounts were by no means trifling: up to US$190 million owed to perhaps 115,000 customers has been missing or cannot be accessed as of this writing, because only Mr. Cotten held the password to off-line cold wallets (Chohan 2019b).

The inaccessibility to the cryptocurrencies thus incited creditors of the company to take Quadriga CX to a source of traditional recourse—a court in Halifax, Nova Scotia, Canada. In that jurisdiction, Quadriga CX has been granted, as of this writing, a stay order under the temporary legal protection from its creditors under the Companies' Creditors Arrangement Act, a form of bankruptcy protection instated during the Great Depression to prevent firms from falling into total

insolvency. That stay order will remain in effect until the middle of 2019, but may be extended thereafter. It has yet not been determined if foul-play is involved, in the manner that the aforementioned Mt. Gox case in Japan came to reveal.

What is of more pressing concern is that the trust-based element in the Quadriga CX case has been breached, and the remedial action is being sought in the traditional domain (a Canadian court). Since Mr. Cotten had not instated any mechanism for access to his off-line cold wallets in a situation of extended actuarial absence (death or disability), the cryptocurrency may be missing, lost, or irretrievable. An element of trust between the parties has been violated, and the traditional judicial system has been brought to bear on the matter.

7 Conclusion

This chapter has sought to present a nuance around the concept of "trustlessness." While it is indeed true that blockchain technologies do not require third-party verification and are therefore trustless in one sense, the conflation of the term with other notions of trust has been an unproductive one. Trust is basis of all sustained commercial life, and to suggest that the older trust-establishing mechanisms are "obsolete" (Klems et al. 2017, p. 731) is misleading, as four different forms of examples in this chapter show. Indeed, the problem of human trust persists in the domain of cryptocurrencies, and has been summarized thus:

> Much of the discourse on cryptocurrencies has sought to detach it from problems that beset the domain of traditional finance. This is somewhat misleading, for while the substance of cryptocurrencies themselves may be congruent with the decentralized, trustless, autonomous, immutable principles championed by cryptoanarchism, the praxis of cryptocurrency transactions still contains a significant human element, including that of engaging in transactional activity (Chohan 2019b, p. 3).

The notion of exaggerating "trustlessness" stems in part from inaccurate marketing, but also in part from the philosophical underpinnings of cryptocurrencies, which lie within *cryptoanarchist thought*. Cryptoanarchism seeks to cultivate decentralized, autonomous, and voluntary exchange among individuals in a manner that protects their identities, and therefore their risk of persecution, from structures of established authority (Chohan 2017e). This creates an ambiguity as to the level of trust that would be forthcoming in the course of regular engagement among participants.

For cryptoanarchism, as with anarchism itself (see Wolff 1998; Marshall 2009), there are utopian expectations of human beings that remain wanting, including a selflessness and trust between groups of people who will demonstrate respect and consideration in an effort to come to mutual aid. In an anonymous world of trading bits of code as monetized instrument, even as it may be nominally "trustless," issues of trust have indeed surfaced, and often bitterly so.

Sometimes the fault has been exogenous, as with the hacks and external attacks on the security of networks, exchanges, and tokens. At other times, however, the

problem has been endogenous, as with the thefts, misrepresentations, Ponzi schemes, and frauds that have been perpetrated across the cryptocurrency space, whether on cryptoexchanges, coin offerings, or on networks themselves.

The principle assertion of this chapter then becomes that fuller clarity is required in the universe of cryptocurrency participants as to what trustlessness really means. Third-party verification aside, there is indeed a dire need for strengthening trust in a realm that is both digital and largely anonymous. Regulation and oversight are natural mechanisms for helping to ensure this, but there are many limitations to the implementation of cryptocurrency regulation, accountability and enforcement, not least at the international level. Indeed, it is inherent to the very design of cryptocurrencies that they should help to mask and protect the identities of participants. But the failures of such systems, as indicated throughout this chapter, thus raise questions about the viability of cryptocurrencies as complementary (or to the idealists: parallel) monetary systems in the longer-run. A balance too must be struck between fostering continued innovation and insisting upon accountability. These questions must be more fervently explored in future research, as well as in policy praxis, as cryptocurrencies shed the perception of being disruptive shadowy technologies, and begin to collectively come-of-age as mature technological and financial instruments.

References

Adhami S, Giudici G, Martinazzi S (2018) Why do businesses go crypto? An empirical analysis of initial coin offerings. J Econ Bus 100:64–75

Bahga A, Madisetti VK (2016) Blockchain platform for industrial internet of things. J Softw Eng Appl 9(10):533

Banafa A (2017) IoT and blockchain convergence: benefits and challenges. IEEE Internet of Things

Benedetti H, Kostovetsky L (2018) Digital tulips? Returns to investors in initial coin offerings. Returns to investors in initial coin offerings (May 20, 2018)

Catalini C, Gans JS (2018) Initial coin offerings and the value of crypto tokens (no. w24418). National Bureau of Economic Research

Chohan UW (2017a) Cryptocurrencies: a brief thematic review. Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3024330

Chohan UW (2017b) The decentralized autonomous organization and governance issues. Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers. https://www.ssrn.com/abstract=3082055

Chohan UW (2017c) The double spending problem and cryptocurrencies. Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3090174

Chohan UW (2017d) Initial coin offerings (ICOs): risks, regulation, and accountability. Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers

Chohan UW (2017e) Cryptoanarchism and cryptocurrencies. Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers. https://www.ssrn.com/abstract=3079241

Chohan UW (2018a) The problems of cryptocurrency thefts and exchange shutdowns. Available via SSRN 3131702

Chohan UW (2018b) Bitconnect and cryptocurrency accountability. Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3131512
Chohan UW (2018c) Oversight and regulation of cryptocurrencies: bitlicense. Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3133342
Chohan UW (2019a) Are cryptocurrencies truly 'trustless'? Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3331544
Chohan UW (2019b) The key man problem in cryptocurrencies? Case of QuadrigaCX. Notes on the 21st century. Critical Blockchain Research Initiative (CBRI) Working Papers. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3329573
Chohan UW (forthcoming-a) Public value and citizen-driven digital innovation. Information Polity
Chohan UW (forthcoming-b) Public value without public managers? Decentralized autonomous organizations and public administration. Information Polity
Clayton J (2017) Statement on cryptocurrencies and initial coin offerings. In: Securities and exchange commission (SEC) statements. SEC, Washington, DC
Clayton J, Giancarlo JC (2018) Joint statement on cryptocurrencies and initial coin offerings. Securities and Exchange Commission (SEC) & Commodity Futures Trading Commission (CFTC), Washington, DC
Coin Market (2019) Top cryptocurrency exchanges list. https://coin.market/exchanges. Accessed 20 April 2019
Destefanis G, Marchesi M, Ortu M, Tonelli R, Bracciali A, Hierons R (2018, March) Smart contracts vulnerabilities: a call for blockchain software engineering? In: 2018 international workshop on blockchain oriented software engineering (IWBOSE), IEEE, pp 19–25
Duhaime C (2019) From law to lawlessness: bits of the untold QuadrigaCX story. Coindesk. March 26
Fisch C (2019) Initial coin offerings (ICOs) to finance new ventures. J Bus Ventur 34(1):1–22
Foroglou G, Tsilidou AL (2015, May) Further applications of the blockchain. In: 12th student conference on managerial science and technology
Fortune Jack (2018) Study on ICO scams in 2018. https://fortunejack.com/
Howell ST, Niessner M, Yermack D (2018) Initial coin offerings: financing growth with cryptocurrency token sales (no. w24774). National Bureau of Economic Research
Kiviat TI (2015) Beyond bitcoin: issues in regulating blockchain transactions. Duke Law J 65:569
Klems M, Eberhardt J, Tai S, Härtlein S, Buchholz S, Tidjani A (2017, November) Trustless intermediation in blockchain-based decentralized service marketplaces. In: International conference on service-oriented computing. Springer, Cham, pp 731–739
Kurtulmus AB, Daniel K (2018) Trustless machine learning contracts; evaluating and exchanging machine learning models on the ethereum blockchain. arXiv preprint arXiv:1802.10185
Lee J, Li T, Shin D (2018) The wisdom of crowds and information cascades in FinTech: evidence from initial coin offerings
Marshall P (2009) Demanding the impossible: a history of anarchism. PM Press, Oakland, CA
Satis Group (2017) Study on ICO scams in 2017. http://satisgroup.io
Schaub A, Bazin R, Hasan O, Brunie L (2016, May) A trustless privacy-preserving reputation system. In: IFIP international conference on ICT systems security and privacy protection. Springer, Cham, pp 398–411
Wolff RP (1998) In defense of anarchism. University of California Press, Berkeley, CA