Regulating the "Dark Side" of financial blockchain

Daniel Broby

1.1 Introduction

The use of financial blockchain and decentralised ledgers system has many benefits. These include immutability, efficiency and security. Digital financial information can be securely stored on a network of computational devices, with changes to those records being reflected simultaneously across that network, but there is also a dark side. Public blockchains, although visible, are typically anonymous and this presents its own challenges. The source and destination of digital asset transfer can be misleading and masked, sometimes resulting in money laundering. Tax can be evaded and the proceeds of trade transactions difficult to audit.

There are other concerns that need to be addressed as the increasing scale and sophistication of blockchain transactions grows. The digital wallet trail becomes more opaque with size. These dark traits will need to be properly regulated if the technology is to be used for societal good.

Blockchain is becoming more pervasive because of the popularity of cryptocurrencies. That said, the many devices that support blockchain usage enhances the ability for the cryptocurrency balances that sit on such platforms to be hidden. This secrecy, combined with the prospect that cryptocurrencies will replace fiat money, has sadly led to a number of reported frauds and pyramid schemes. Money has been raised through Initial Coin Offerings for online tokens designed to be exchanged for future products or services. In many instances these that have yet to materialize. The Initial Coin Offerings are typically promoted by entrepreneurs and program developers on the prospect that secondary trading will develop. These promotors often have little knowledge of financial markets and scant regulatory oversight, and often, such promises do not come to fruition.

There are many societal issues, some of them dark in nature. The energy used in creating the secure cryptographic protection for a public blockchain, for example, is computationally expensive The democrartization that blockchain facilitates has societal impliacations that need to be thought though. That said, the less well know dark side is the issue of unchecked international capital flows. The ease of blockchain based digital asset transfer has resulted in capital flowing

between new and emerging markets without resort to currency controls. The implications for economic stability and the role of central banks are profound. A number of jurisdictions have banned trading in bitcoin as a result of this. Regulators need to think about how to monitor and oversee such transfers.

As can be seen, there are many issues that have a dark side. The reason addressing them is important is that widespread blockchain adoption requires a critical and holistic understanding of the technology. The aim of this chapter, therefore, is to identify the key negatives, both technical and societal. This is done through the lens of international regulatory policy and digital audit trails. The chapter sections review the weakness of blockchain, from the perspective of ledger attacks, the problems of maintaining a robust distributed system and the approach used in transaction validation. Finally, conclusions are drawn in respect of regulation, governance, responsibility and liability.

1.2 Background

Blockchain was first described by (Nakamoto, 2008) in a white paper that forms the basis of bitcoin, and indeed other public cryptocurrencies. It describes the mechanics of a distributed computer architecture and shows how this can be used to facilitate the sending of digital instructions by using programing code over the internet. In this respect, it was the catalyst behind blockchain. The bitcoin was devised as a consensus but anonymous protocol with built in constraints on the issuance. This feature has issues that regulators need to consider.

At its most basic, blockchain is essentially about records. Our society relies on records and as such the blockchain immutable nature is a paradigm shift. In technical terms, a blockchain has what is called network nodes that execute and record digital transactions. The programming code sends instructions grouped into blocks, hence the name. These blocks contain digital instructions linked in a chain secured by a unique identifying key. Such a blockchain, for example, can contain an instruction to send money from Bob to Alice. Once created, these coded messages can be used to facilitate financial market transactions, payments, and settlements.

The benefits of blockchain are many but there are, as mentioned, issues. There is a great deal of discussion in the media, banking circles and academia about the impact that blockchain will have on financial settlement and operations. A lot of this is misinformed, but the shortcomings should not be trivialised. Essentially the blockchain moves the emphasis from trusting regulated entities to trusting a secure distributed record. As such, it is important to know if we can rely on the technology, if we can trust it.

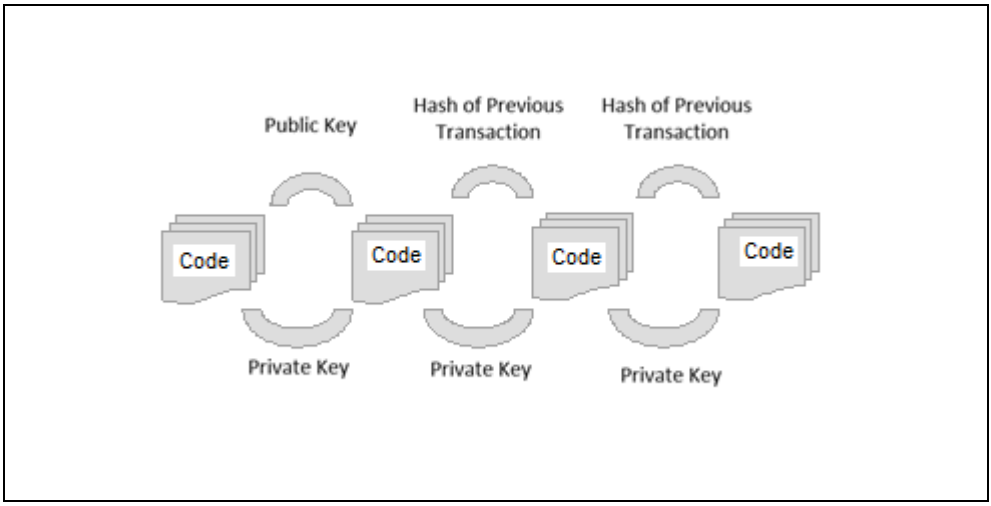
Blockchain is often confused with bitcoin because of its origins. Bitcoin is just one digital currency that “utilizes blockchain“. It is also the one that attracts the most negative comments. The news flow on it has a habit of alienating informed discussion by practitioners. This is because financial

and technical jargon do not mix well. Academics tend to focus on the engineering and cryptographic issues. They often overlook the negatives, instead concentrating on the transformational benefits blockchain brings to legacy payment systems.

Concerns about the dark side of the technology by the public or incumbent financial institutions is hindering informed debate. In the light of this research asymmetry there has, in turn, been a slower uptake than some observers had predicted. This is another reason why the regulations need to be addressed in a critical manner.

In order to explore the dark side, it is necessary to explain the basics behind the concept of blockchain. This is not as complex as it sounds. As already mentioned, it consists of programing code linked to historic data. In the case of financial transactions, that data is kept on a ledger. A cryptographic hash links the blocks of code chronologically. The latter is a unique secure identifying tag embedded in the code of a prior block. This element is what creates the chain. The blocks are verified by cryptographic hash which in turn cannot be easily changed or falsified.

The chronological blocks in a blockchain can hold multiple transaction records which in turn can be distributed through nodes as explained in Decker and Wattenhofer (2013). If a more detailed explanation is required, it is well documented by Peters et al (2015). The uniqueness of the blockchain is based on the fact that a change to any part of the data would make the hash appear to be totally different, and therein lies the key to its the security. Attempts to tamper with the record are immediately exposed. The sequence is illustrated in Figure 1 below.



The Figure 1 The Mechanism of Securing Transactions on Blockchain

Source: Broby and Paul (2017)

The good thing about blockchain is that the inclusion of the cryptographic hash makes fraud difficult. Indeed, this is the key innovation that makes a blockchain secure. The hash, as illustrated above, solves the "copied and pasted" problem, namely that digital transactions can be broadcast multiple times unless secured by such a protocol. These unique hash identifiers can be designed so as to automatically change if any or all of the transactions are compromised. Buyya, et al. (2008) illustrated how this facilitates financial transactions over decentralized networks, in other words over the internet. This is done through a process called validation, the converse of the dark side, and the reason that blockchain is proving popular.

Through the blockchain protocol financial payments can be sent and stored by lodging them on multiple online distributed ledgers. In ensuring that all participants are able to jointly agree and view previous transactions, the blockchain is highly visible to all parties. The dark side of this visibility is that it leaves financial value vulnerable to those intent on misusing such data.

The ability to validate transfers and transactions cryptographically provides opportunities for enhancing the security of current trading and settlement platforms. That said, this feature does come with large storage requirements that will only increase as usage becomes greater, another dark side not often mentioned. This is illustrated in the table below, which compares the various blockchain approaches with central databases. It should be noted that much of what can be achieved with a blockchain can also be achieved with the use of a simple database.

	Centralised Database	**Distributed Database**	**Mutual Distributed Database (Unpermissioned)**	**Mutual Distributed Ledgers (Permissioned**
Storage	Single master	Multiple copies	Multiple copies	Multiple copies
Definition of Data	Multidimensional	Multidimensional	Single dimensional	Single dimensional
Participation	Closed	Closed	Open	New modes added by agreement
Rights	Data base management system	Data base management system	Built into protocol ledger	Configured file

Validation	Data base management system	Data base management system	Proof of Work	Confirmation by participants and/or its inner circle.
Reconciliation	Only if data moved	Iterative	Iterative	Iterative
Robustness	Historically vulnerable	Resilient	Resilient	Resilient

Table 1: Comparison of centralised versus decentralised database

As can be seen, validation is one of the core elements of blockchain. Others include reconciliation and robustness, all of which are viewed as positives. This robustness is built into the blockchain's inherent peer-to-peer network, explained in Koshy et al (2014). This process solves the so-called Byzantine General Problem. This is where no network user can game others unless they control more than half of the network. This is, in essence, the strength of the protocol. That said, Feldman and Micali (1997) demonstrated where control of the network could be gained.[1] They exposed the fact that such attacks are possible. Houy (2017) even suggests that if one wanted to, the cost of destroying a proof of stake crypto-currency was minimal.

As a final background observation, blockchain technology is heralded as disruptive. It allows for a new model of consensus and validation of records and events. Disruption, as is commonly known, has its dark side. This also needs to be subject to critical thought and evaluation.

1.3 Money transfer and capital flight

There are a few hundred cryptocurrencies, called altcoins. Whether any of these become a global success is debatable, but clearly, the world is predicted to move to a digital currency future now the technology is available. Bitcoin was the first to use the blockchain with this vision in mind. It relies on proof of work from its community of miners, is independent from any legal jurisdiction. Some regulators consider this independence as a negative. Many central banks are considering the implications of the rise of this and other unaccountable cryptocurrencies.

Clearly, there are many advantages in cheap, efficient and secure money transfer. The evangelists tend to overlook the challenge to the widespread adoption of the protocol, namely its lack of speed. Using blockchain requires that both computational time and the Cryptographic hashes are used

[1] This is called a "51 percent attack". Lamport and Fischer (1982) demonstrated how this problem can be overcome by the distributed nature of the network.

for connecting the blocks and for confirming transactions. Barber et al (2012) explain this. Cryptocurrencies, such as Bitcoin and Litecoin, use such confirmations; as do currency exchange and transfer services such as Transferwise. These have all adopted the structure of blockchain as the basis of their security. That said, the creation of blocks is slow and as such the claim that this is efficient is not currently substantiated.

Capital flight from emerging economies is a dark side of blockchain money transfers, the technology being used to enable cryptocurrencies to evade capital controls. Emerging countries often have exchange control regulations and this effectively bypasses them. A number of emerging countries, including China, have therefore banned the use of cryptocurrencies. As more and more transactions migrate to blockchain enabled platforms, capital flight will become increasingly difficult to control, and indeed faster. Regulators will have to adapt to keep pace.

The disruptive nature of untracked capital flows is not extensively researched. Simply banning the use of cryptocurrencies may well not prove effective, because individuals may still access the internet using Virtual Private Networks (VPN's). That said, VPN's need to have robust encryption and not leak data to be of use in a secure blockchain. As a result, regulators have to be more proactive.

1.4 Timestamping

The lack of a precision time stamping protocol in financial blockchains is another unreported dark side. There is no inherently accurate time-stamps of transactions, the majority being just timestamped with the internal clock of the server. This presents a problem for banks and financial institutions. In this respect, the blocks are ordinal, they are stamped as and when they are produced. Basu, Broby and Arulselvan (2017) document how to overcome this by timestamping blockchains using atomic clocks and reordering them into batches. That said, this solution is not yet common practice and was proposed for use in distributed marketplaces.

While the problem can be solved, as it stands the blockchain construct provides a fixed history and a verifiable sequence of events. This means individual events themselves can only be validated as existing at or after a given point. A dark side issue occurs when two competing blocks are generated at the same time. This results in a collision in which one block appears in front of the other. In this scenario, the transactions from the second block continue to be added to the network. They then appear later than would otherwise be the case. This is clearly undesirable and can facilitate the financial crime termed fount-running.

The reason timestamping is important is that in certain circumstances, such as for example, high value or priority transfers, one needs the ability to cryptographically prove that an attempt has been made to initiate a transmission at a particular time. It helps to ensure the correct relative

arrangement of blocks and provides evidence to a party of the existence of a signed transaction at any given time. In other words, timestamping helps fulfil contractual obligations.

The timestamping ambiguity is off concern because oversight and supervision usually begins at the end of the observed period. Within a blockchain, time is more discreet than continuous. The dark side from the regulators' point of view is that the capture of a transaction does not guarantee that a transaction occurred during generation and verification. This complicates regulation, especially when internal controls and procedures are loose.

Another dark side of the way timestamping is currently structured occurs when an authorised party acts maliciously and deliberately generates valid and signed transactions without broadcasting them to the blockchain. Regulators, in such cases, would find it difficult to detect these. The delayed transactions could then be presented to the network as valid after-the-fact which is clearly disadvantageous in a financial context.

1.5 Visibility and anonymity

The dark side of financial blockchain derives from the dichotomy between its visibility and its anonymity. Regulatory and compliance oversight requires visibility. Regulations and audit are implemented over finite period of time, for example a reporting period. This is not present in a blockchain despite their construct being continuous. As such, regulation need to become more dynamic.

An error in perception about blockchain comes from the belief, stemming from the visibility issue, that exposing transaction data over the Internet is unsafe. Contrary to widespread opinion, blockchains do not have to be made fully accessible to the public. Some of the concerns are due to an incomplete understanding of the technology. Not all blockchains need to be public and based on proof of work. A private blockchain is possible and many exist. Regulators will have to become more adept in understanding the distinction between the technologies.

Another fallacy, stemming this time from the anonymity, is that the blockchain is uncertain and unreliable because unknown and faceless programmers are developing it. This overlooks the power of open source software development, which has proven superior to single source software development. One of the solutions to address the fears for financial transaction security in this respect is the so-called hybrid blockchain. With this, it is possible for everyone to read the blockchain, but only for authorized users to transfer assets.

The way regulators can address visibility is through a register of ownership. This need not be in the public domain, thereby securing some level of annonymity.

1.6 Malleability

The evangelist claim that blockchain can not be altered but the dark side is that it is in fact malleable. Indeed, it has been publicly demonstrated that blockchains are not immutable. In March 2013, the bitcoin ledger forked in two parts. The bitcoin's community had to persuade members of the validating network to accept the ledger that was considered to be true. The redundant chain was deemed invalid. Likewise, the Ethereum record was revised following the "Dow theft". Ethereums core developers convinced the consensus to agree to deleted the previous record, invalidating the stolen proceeds of this digital heist.

Malleability of the code is a problem. One of the advantages of blockchain money transfer is that it enables what have become called smart contracts. In effect, such a contract instructs, verifies and enforces a set of contractual instructions. Smart contracts have the protocol to add functionality to many transfer instructions, but the dark side is that malicious code can be used to exploit those who are unfamiliar with them.

The malleability of blockchain means that a transaction can be changed after it has occurred. Regulators clearly have a problem with this concept. The issue was addressed by Andrychowicz, Dziembowski, Malinowski and Mazurek (2015). They showed that the instances of this can arise due to the implementation a transaction ID algorithm. In this respect, it is possible for a party relaying a transaction to modify the transaction in a minor way, leaving the contents of the transaction valid. In such cases, although only a small change, the transaction ID is altered and therefore differs from that originally produced.

The malleability of transactions can have a negative effect on the blockchain. It allows the transaction to be generated under one identifier, but broadcast and included in the block chain under another transaction identifier. This, of course, presents a problem for regulators, since usually the transaction identifier will be treated as unique. Where such payments are frequent, reconciling authorizations from the sender to block records can prove complicated.

As a consequence of the above, there is potential for double payment fraud. This is obviously something which regulators have to be vigilant about. For example, a participant in the blockchain, particularly one using simple payment verification, could be tricked into issuing a payment instruction twice. If, in such a scenario, a party claimed the payment did not go through, showing as evidence the lack of existence of a transaction under the ID generated by the sender, then the system can be gamed. This is clearly a dark side. If the sender does not verify their previous transactions properly, checking the blockchain for all recent transactions, they may not see the transaction, resulting in a double payment being made.

In order to stop such tampering, regulators need to ensure a more robust security model is adopted, cryptographically verified transactions against the bank of origin. In the event of the transaction being improperly signed, the cryptographic validation should fail, and regulators will detect this conflict, refusing to honour the transaction.

1.7 Auditing and oversight

An audit requires a true and fair view and clearly the dark side is where this is not present. There are many challenges in auditing financial data within a blochchain. These are addressed by Broby and Paul (2017) The most obvious of these is accounting year ends. As previously mentioned, these are reported at a static point in time but this is not the case in a blockchain. As such, the most recent transactions cannot be guaranteed as valid, which obviously is not acceptable from an audit perspective.

From a regulators point of view there are also problems with auditing distributed ledger records. If a third party, on behalf of the audited entity, holds funds in such ledgers, there could be concerns about the safety of these funds. Without the private keys being under the control of the organization concerned, the funds cannot be withdrawn in the event third party intervention. This can result in material loss of the asset and from a regulatory perspective should therefore be subject to audit. In a similar fashion, it is difficult to prove ownership of the cryptographic keys that control access to wallets. This is a regulatory concern when funds are held in either a third-party exchanges or an online wallet.

The audit trail in distributed environments also present problems. Online exchanges and wallets are often not the best place to keep records. If two users of the same platform are making transactions, the internal account balance is crossed thereby avoiding a blockchain transaction being sent, and thus publically documented. In such a scenario, it becomes difficult for an audit to verify the true value of funds within a wallet.

1.8 Money laundering and tax evasion

The darkest of the blockchain issues are money laundering and tax evasion. Such activities can occur when blockchain based transactions are made using cryptographic identities. Best practice to avoid this happening on a blockchain is to use the secure keys only twice. That is once to receive funds, and once to transfers funds out. This is because the security measures of many block-based currencies, including bitcoins, serve to hide and protect the user's public key after the transaction has been created. Only one side of the public key is visible in the block chain.

Using best practice means that even compromising the digital signature will not compromise the assets. Where parties follow this guidance, this poses a challenge to regulators, as recurring transactions to a recipient are not necessarily directed to the same recipient address. Indeed, ideally they shouldn’t, but it presents a problem none-the-less.

The regulatory solution to money laundering and tax evasion through blockchain is to ensure that the correct recipient has been specified and that the recipient's address can be verified from digital

invoices. The private keys used to access a wallet can be transferred between parties. This makes it difficult to ensure the identity of the party that operates an address and regulators should have oversight of such activities.

Another partial solution to money laundering is for regulators to match recipient addresses against invoices, as well as seek to locate duplicate receiving addresses. Repeat transactions should also be scrutinised, to ensure that malicious actors do not attempt to transfer funds to previously used addresses now under the control of a new beneficiary, a practice used by money launderers. Although there are ways financial blockchain can be used to facilitate such activities, it should always be remembered that by definition there is a digital footprint.

1.9 Digital Autonomous Organizations (DAO's)

Regulators like to have legal entities to regulate, so as to keep the data side in check. The blockchain, however, facilitates the existence of Digital Autonomous Organisations *(DAO's*). These are similar to conventional companies with their own memorandum and articles of association, although they do not exist as a legal entity in any given legal system. These structures were covered and explained by Ringelstein and Staab (2009). These forms are quite innovative and wider adoption raises societal questions about the legal nature of collaborative entities.

In essence, a DAO presents a form of cryptographically enforced organizational rules. In this respect, DAO controlled assets can not be issued without the agreement of the members of such an organization. That is, the interest groups in accordance with the rules defined and agreed by the entities founders. Various regulatory challenges are posed by DAO structures, not least that of jurisdiction of the entity, and how judgements could be enforced against it. Since the DAO in itself is not a legal entity, its position in law is unclear.

As Broby and Paul (2018) explain, the first DAO within Ethereum was built as an organizational form, with those who bought the DAO becoming stakeholders rather than shareholders. Those stakeholders who sold tokens at the original sale are effectively the group who get to vote on different any issues related to the DAO. The rules of the DAO would then be used to determine how the organization works.

As far as regulators are concerned, were a judgement to be issued against a DAO, the means of enforcement against it would also be unclear. The consensus requires agreement of a majority of shareholders, or whatever is defined in the DAO's smart contract rules, in order for funds to be taken from the organisation. As such, conventional jurisdictions do not have legitimacy over such a structure.

1.10 Chain and coin mixing

As explained, it is challenge for regulators to understand the identity and intentions of the parties using financial blockchains and/or cryptocurrencies. In this respect, another dark side is that it is possible to mix coins to conceal their history and/or source. In the first instance, transaction mixing may be used to provide a level of discretion to those who perform transactions. This is called chain and or coin. As yet, mixing is not a serious problem but has the potential to become so.

The technique of mixing is designed to hinder the tracing of transactions involving cryptocurrency coins. A party that wants to hide the past of their coins would transfer those coins to a blending service as part of a transaction. In return, if the blending service is honest, a set of coins would return to a new address that has different origins. Without compromising the mixing service, a regulator would not be able to track the funds through a well-implemented mixing service.

Using the technique, a single transaction can be hidden with multiple transactions from mutually suspicious parties. Mixers can create a new recipient address for their new coins and form a transaction between all parties. The inputs of each participant are then merged in the one transaction with an output for each party. The dark side of this is that it separates the connection between the inputs and the outputs. An ambiguity is introduced in the blockchain whereby inputs correspond to outputs. If this process is repeated several times, analysis by regulators to track funds is severely hampered. In order to determine what has happened within each operation, it would be necessary for the regulator to identify and communicate with all parties. A protocol has to be set up to do this.

To obfuscate the true destination or origin of transactions is clearly a dark side for regulators. It may hinder the process of verifying the destination of funds is as stated. For example, an insider attempting to steal company funds would almost certainly attempt to mix their coins using one of these techniques, to avoid their purchases being traceable.

1.11 Mining and energy demand

Another dark side of public blockchains is their mining process. This is unduly energy intensive and energy wasteful. This is because the concept behind public blockchains is the proof of work, sometimes called mining. Courtois, Grajek and Naik (2013) first highlighted the problem. In effect, mining becomes a race between many participants, which is energy wasteful.

To explain this, one should consider the process of adding a new block to a blockchain. To do this a key must be created that links the blocks. This requires a nounce value that is found by solving an equation, thereby creating a unique SHA 256 cryptographic hash. This is a computationally difficult process and requires raw computing power. The energy cost of this process is, for bitcoin alone, 46TWh, a global annualized cost of $2bn. The energy consumption is shown in Table 2.

Table 2: BITCOIN ENERGY CONSUMPTION (FEB 2018)

Bitcoin's current estimated annual electricity consumption* (TWh)	46.68
Annualized global mining revenues	$8,189,878,990
Annualized estimated global mining costs	$2,333,884,446
Electricity consumed per transaction (KWh)	524.00
Bitcoin's electricity consumption as a percentage of the world's electricity consumption	0.21%
Annual carbon footprint (kt of CO2)	22,872

Source: https://digiconomist.net/bitcoin-energy-consumption

Clearly, energy wastage is sub optimal for society. Not all blockchains have such a protocol, but even so policy makers should take note. As the table shows, in February bitcoin mining represented 0.21% of the world's energy usage, most of it largely being duplication of effort.

1.12 Cryptocurrencies as commodities

In 2018, a United States federal judge ruled that cryptocurrencies can be treated as commodities by the U.S. Commodity Futures Trading Commission. Public cryptocurrencies differ from fiat currency/money in as much as they are not issued by Central Banks. The dark side of their status in this respect is that the volatility of cryptocurrencies has brought into question their use as a medium of exchange and/or store of value.

The blockchain facilitates cryptocurrencies that have taken on board commodity like characteristics. Hanley (2013) exposed a number of flaws in the assumptions behind them. A cryptocurrency is a digital or virtual currency that is stored on the. Programing code is used to create tokens and establish the process of transmitting their value. In this form, transactions can take place over the internet and they have currency like properties. Bitcoin, in particular, was devised for this purpose. As far as Bitcoin goes, however, Hanley argued it is false to assume it can be a reserve currency for banking and that it can expand by deflation to become a global transactional currency.

Bitcoin , specifically, is designed as a finite commodity along the same liens as rare metals such as gold. This is why the process of verification is called mining. Such constrained supply results

in a distortion in the price discovery mechanism. The dark side of this has been the bubble in cryptocurrency valuations that developed between 2017-2018.

1.13 Initial Coin Offerings (ICO's)

The aforementioned speculative interest in the value of cryptocurrencies has led to an explosion in the number in existence and their use cases. Tokens are now used as a means of substitute payment to a whole range of things. Entrepreneurs have sought to fund their concepts using Initial Coin Offerings (ICOs). These are unregulated means by which funds are raised for a new cryptocurrency venture, typically base on the back of a white paper. The dark side of this activity is that some of these are poorly designed and many are fraudulent.

Initial Coin Offerings are online token offerings designed to raise money through cryptocurrencies, the product of which is designed to exchange future products or services. They are typically promoted by entrepreneurs and program developers with the prospect of secondary trading in an online format. A German example of such an ICO is the „wysker Platform". This was created as an application providing a high-speed window shopping experience based on a „wys Token" for digital commerce. The question, from a regulatory perspective, is how to ensure that such tokens and fund raising schemes are not being misrepresented,

DAO was one of the first and most successful ICO's. It offered a decentralized venture capital vehicle with investment being generated through consensus voting, whereby the vote of each shareholder was weighted by the quantity subscribed during the ICO. Regulators will have to learn how to bring such offerings within the scope of existing securities law.

1.14 Societal implications and improving regulation and oversight

The widespread usage of blockckain will have societal implications. The biggest societal impact is the loss of jobs. As Broby and Karkkainen (2016) show, this can be substantial. Distributed distributed ledgers share information which is largely a positive for society, especially when safeguarding transactions and preserving data. One should not forget transactional data lies at the heart of global financial stability.

Society is also being changed by the way computing is done. There is now, for instance, a global virtual computer that facilitates blockchain. This is called Ethereum and was launched in 2015. Its platform allows intelligent blockchain based contracts to be handled through a decentralized network of peers. Indeed, the Ethereum Smart Contract is described as "an application programmed exactly as programmed without downtime, censorship, fraud, or third-party interference". The promise is that it will completely decentralize the Internet. With Ethereum, one can

launch blockchain based applications without launching a new blockchain protocol or a new crypto currency, thereby increasing the reach of such technology. Whether there is a dark side to such a global computer has yet to be seen.

Blockchain can also be used for other societal goals. As the content of a blockchain does not need to be financial, other assets or other property can use the protocol and enjoy verifiable and accountable ownership. For example, house sales could be carried out on a form of blockchain, allowing government to ensure that all transfers are properly registered (and thus that taxes paid). In addition, blockchain can be used for making business online easier.

In order to be effective, regulators should oversee the movement of all blockchain based funds between wallets (public keys). This addresses two issues, firstly ensuring funds are indeed under control of the organisation, and secondly preventing historical fraudulent transactions from being broadcast. By moving funds to a new wallet regulators can be sure funds are supervised.

The technology can also be used to police technology. In this respect, Treleaven and Batrinca (2017) showed that the regulation of blockchain can be done using Artificial Intelligence and regulatory algorithms.

1.15 Conclusion

The future use of blockchain should have a significant impact on the efficiency and competitiveness in the financial sector. This chapter has, however, outlined its dark side. There is broad agreement the technology can potentially reduce costs and help understand and manage risks. It can also facilitate financial transfers, particularly in the form of cryptocurrencies. That said blockchain has a number of shortcomings, inappropriate uses and potential negative outcomes for society.

The positive features of blockchain mean that the internet will evolve to include the digital transmission of assets. This is because blockchain can facilitate the exchange of assets or information between various parties without the need for a trusted intermediary. This, combined with the immutability of digital records, their traceability and their ownership, make the take up of the technology an exciting prospect. Whilst the security and privacy of blockchains have captured the attention of financial market participants, they have also attracted the attention of money launders and tax evaders.

With controlled access to distributed ledgers, financial transactions can be stored on the internet rather than simply on the server of individual banks. That makes them less dependent on legacy systems. That said, the dark side is that the transmission of data is subject to the speed of the

network. That makes the timing of transactions extremely relevant for the development of financial markets in the future. The way that timestamping is currently done is a key weakness in the blockchain as not all information is always visible.

The disintermediation that the blockchain facilitates will have an impact on the future required labor force. Jobs in the banking and insurance sectors will come under increasing pressure as blockchain automates the clearing and settlement process. This is a challenge society has to face. That said, there will also likely be changes to the types of services that can be delivered across the financial spectrum, especially over mobile devices and over the Internet, and this will create new job opportunities.

The final word on the dark side is the observation that all human activity has a dark side. The blockchain in itself is not inherently evil or bad. Likewise, its downsides in respect of time and processing power are issues that can be overcome with more research.

1.16 References

Quelle: Basu, Devraj; Broby, Daniel; Arulselvan, Ashwin. *The role of precision timing in stock market price discovery when trading through distributed ledgers.* Glasgow : University of Strathclyde, 2017. p. 1-23.

Quelle: Broby, D & Karkkainen, T 2016, 'FINTECH in Scotland: building a digital future for the financial sector' Paper presented at Future of Fintech, Glasgow, United Kingdom, 2/09/16 - 2/09/16, pp. 1-30

Quelle: Broby, D & Paul, G 2017, 'The financial auditing of distributed ledgers, blockchain and cryptocurrencies' Journal of Financial Transformation, vol 46, pp. 76-88

Quelle: Buyya, R., Yeo, C. & Venugopal, S., 2008. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In High Performance Computing and Communications. s.l., HPCC'08

Quelle: Courtois, N.T., Grajek, M. and Naik, R., 2013. The unreasonable fundamental incertitude's behind bitcoin mining. arXiv preprint arXiv:1310.7935.

Quelle: Decker, C. & Wattenhofer, R., 2013. Information propagation in the bitcoin network.. s.l., IIEEE P2P 2013 Proceedings (pp. 1-10)

Quelle: Hanley, B.P., 2013. The false premises and promises of Bitcoin. arXiv preprint arXiv:1312.2048.

Quelle: Houy, N., 2014. It will cost you nothing to" kill" a proof-of-stake crypto-currency. Economics Bulletin, 34(2), pp.1038-1044.

Quelle: Koshy, P., Koshy, D. & McDaniel, P., 2014. An analysis of anonymity in bitcoin using p2p network traffic. In International Conference on Financial Cryptography and Data Security. March ed. Berlin Heidelberg: Springe

Quelle: Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system., s.l.: Private distribution.

Quelle: Peters, G., 2015. Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective. Working Paper

Quelle: Scharfstein, D.S. and Stein, J.C., 2000. The dark side of internal capital markets: Divisional rent-seeking and inefficient investment. The Journal of Finance, 55(6), pp.2537-2564.

Quelle: Treleaven, P. and Batrinca, B., 2017. Algorithmic regulation: automating financial compliance monitoring and regulation using AI and blockchain. Journal of Financial Transformation, 45, pp.14-21.