Transparency International Anti-Corruption Helpdesk Answer

Blockchain, bitcoin and corruption

A review of the linkages

Author(s): Niklas Kossow and Victoria Dykes, tihelpdesk@transparency.org
Reviewer(s): Matthew Jenkins, Transparency International Secretariat
Date: 22 January 2018

Bitcoin and the blockchain technology which drives it has emerged as one of the most disruptive digital innovations in recent years.

These technologies are posited as being potential catalysts of transnational crime on one hand and as potential tools in the fight against corruption on the other. Neither perspective is true in the absolute sense. Bitcoin and other digital currencies can be used to expedite cross-border crime, tax evasion and corruption. However, Bitcoin transactions are meticulously recorded, and digital currencies are increasingly accepted as a legitimate investment.

Blockchain technology provides huge potential for more transparent, more accountable and efficient ways of storing government data and administering transactions. Yet, there are many challenges to overcome before the technology can be scaled. Legal frameworks need reform to regulate digital currency markets and to harness the full potential of blockchain technology.

Query

Please provide an overview of the linkages between blockchain technology and corruption issues. Some trumpet blockchain technology as a potential anti-corruption tool, while others argue that cryptocurrencies may facilitate money laundering or other corrupt activities.

Contents

Main points

- Cryptocurrencies like Bitcoin can be used to expedite cross-border crime, tax evasion and corruption
- However, Bitcoin transactions are meticulously recorded, and increasingly regarded as a legitimate investment
- Blockchain technology offers vast potential for more transparent, accountable and efficient ways of storing data and overseeing transactions
- However, there are existing legal and infrastructural challenges to the widespread adoption of blockchain

What are bitcoin and blockchain?

The development of Bitcoin

Bitcoin is a decentralised digital currency based on a peer-to-peer payment system built on cryptographic principles. It is often also referred to as a cryptocurrency, as cryptography provides its technological backbone. Its concept was first published in a whitepaper by a person or a group of people under the pseudonym Satoshi Nakamoto (2008). It was published as a functional open source code in 2009 and has grown in popularity ever since.

The architecture of Bitcoin relies on a decentralised computing system of nodes that communicate with each other to record and verify each Bitcoin transaction. Rather than data being stored on one central server, it is simultaneously stored on all full nodes in the system. A node can technically be any device with an IP address that is able to become part of the Bitcoin system; this means that the device is able to run a programme that validates Bitcoin transactions.

To turn this into a functional data-storing system, information is recorded in publicly available ledgers, which are commonly referred to as blocks. Blocks are simply collections of data, and can store any type of data; indeed, data related to Bitcoin transactions is simply one of the many applications of the technology.

Blocks contain not only data that was recently stored in them, but all data from previous data points. This makes it possible to link one block to its previous block and creates a chain of information and data points; this is why the underlying technology of the Bitcoin system is referred to as a blockchain. As a block is a type of

public ledger and operates within a decentralised system, this type of technology is referred to as distributed ledger technology (DLT). Different types and applications of DLT are outlined further below.

In the process of linking new transactions to previous blocks, the information on the block is time-stamped and cryptographically sealed. As a result of this process, no data that was entered in the blockchain can later be changed or deleted; all data can be traced back to the exact moment it was added to the blockchain.

The Bitcoin blockchain uses the SHA256 hash algorithm to seal the transaction and create a so-called hash, which is effectively a fixed-length string of text that is uniquely representative of a file or piece of data in the exact instant the hashing algorithm was applied. This means that changing the source data even minutely, and then re-applying the hash algorithm would generate a completely different hash.

The hash contains information on the data within the block, and also provides a cryptographic puzzle that has to be solved to link a new block to the blockchain. The type of puzzle will stay the same regardless of the number of transactions or amount of data stored within a block.

A certain amount of computing power, effort and luck is required to solve the problem and add data to the blockchain. Solving this puzzle is thus referred to as providing a proof-of-work (Nakamoto 2008). This process of adding new blocks to the blockchain is called mining in reference to it being a laborious effort (Kroll et al. 2013).

Bitcoins are created as a reward for this effort and are distributed to miners, or rather to the computers which are doing the mining work. Transactions are only accepted if 51 per cent of the nodes in the blockchain network verify the transactions and agree that the correct data was stored and that the proof-of-work was accurately provided. The difficulty of the proof-of-work is automatically adjusted to reflect the difficulty of the blocks to be mined, the number of miners in the system (which increases the number of blocks that can be written) and to ensure that enough blocks are written.

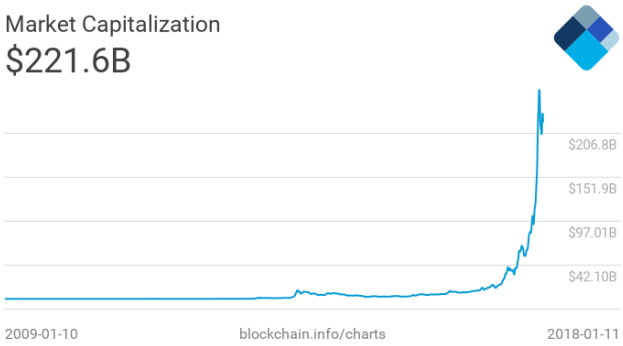
Generally, it is becoming increasingly hard to mine new bitcoins; the difficulty of the proof-of-work decreases very rarely. This is another factor which limits the number of bitcoins which can be in circulation. This principle which will be further outlined below.

The entire process behind Bitcoin transactions provides a solution to the potential problem of dual-spending of digital currencies. It ensures that the same money cannot be spent twice at the same time and it ensures that ownership of a currency is verified. It thus establishes trust without an intermediary agent, such as a bank or a state (Nakamoto 2008).

Market size

The difficulty of mining increases over time and thus requires more and more computing power. To limit the supply of bitcoins, artificial scarcity is created. This results in a cap of bitcoins to be created: once there are 21 million bitcoins in circulation, no more coins will be added to the market. This principle is enshrined in the Bitcoin code and cannot be altered; this functionality helps create the value of bitcoin and reflects the character of mining a finite resource. It can currently be divided up to eight decimal places and thus traded in smaller units (Bitcoin.org 2018b).

Over the past several years, the price of bitcoin has fluctuated greatly, reaching record highs in 2017 of almost US$20,000 and a market capitalisation of US$300 billion (Hackett & Wieczner 2017). The total market capitalisation of Bitcoin at the time of writing stood around US$222 billion.



While Bitcoin represents the most important digital currency, there are many other digital currencies with different degrees of market capitalisation. The leading alternative digital currencies are currently Ethereum, Ripple and Bitcoin Cash (Coinmarketcap 2018). Due to their attributes, Yermack (2013) argues that digital currencies behave more like a speculative investment than like a traditional currency.

Linkages to corruption

Misuse of Bitcoin

Most cryptocurrencies function in a similar way, with information on them stored using DLT like the Bitcoin blockchain. They all promise cost-effective, fast and secure transactions without reliance on an intermediary agent. As such, digital currencies offer users the possibility to conduct transactions without stating their real name as ownership information is only stored in the form of matching public and private cryptographic keys (Bitcoin.org 2018). Digital currencies can thus lend themselves to non-attributable transactions, which provides a potential for misuse.

Potential of blockchain

While Bitcoin and other digital currencies have soared in popularity and market capitalisation over the past several years, many people have also looked at other uses for the underlying DLT – a term often used interchangeably with blockchain, the most popular type of DLT. It essentially provides a decentralised and efficient way to store most types of data. It offers the possibility of making data entries more transparent, to verify the integrity and accuracy of stored data, and to make previously entered data immutable. As such, it offers opportunities for public administration and has the potential to address corruption problems. For the sake of this paper, DLT and blockchain are used largely interchangeably.

Misuse of cryptocurrencies

In September 2017, JP Morgan CEO, Jamie Dimon, stated at a conference that the only people who are better off using Bitcoin as opposed to official currencies are murderers, drug dealers, or people living in places like North Korea (Monaghan 2017). The extent to which this is true is debatable, but there is a currently a heated debate about whether Bitcoin is uniquely situated to promote and support illegal activities such as money laundering, drug dealing and computer virus attacks. The salience of these risks hinges on the (assumed) anonymity Bitcoin provides, as well as the lack of a central monitoring body that would otherwise flag or block suspicious transactions.

In discussing the links between Bitcoin, illicit activity and regulatory efforts, it is helpful to understand two common types of Bitcoin-related services: exchanges and wallets. A Bitcoin exchange is an online marketplace that facilitates

the exchange of Bitcoin into fiat money and vice versa. Today, there are a variety of exchanges that specialise in different currencies. Generally, they offer some baseline of security protections; they also tend to ask for basic personal information from their users, such as a name and an e-mail address. A Bitcoin wallet, on the other hand, is a software service that "stores" a given person's Bitcoin (more accurately stated, it stores the Bitcoin's private key that is shared only with the owner of the Bitcoin). It is not required to have a wallet to collect Bitcoin, but having one offers more security and protection against Bitcoin theft.

Money laundering

There are conflicting perspectives on whether Bitcoin is more likely than other currencies to be used for money laundering. Those who argue that Bitcoin has significant potential to be misused for this purpose tend to focus on three central qualities of Bitcoin and many other cryptocurrencies (Choo 2015):

1. Anonymity: although conducting transactions with Bitcoin via an established online wallet or exchange service generally does require that the account is linked to a personal identity, this is not a requirement to use Bitcoin – it is possible to bypass exchanges and wallet services and participate in mining or transactions without ever having to disclose one's identity (Ludwin 2015). Moreover, the lack of a central authority means that when personal identities are provided, there is no process of identifying suspicious names, for example, the names of known criminals.
2. Flexibility: criminals can easily disperse their bitcoins across multiple accounts to avoid triggering reporting requirements (if they exist at all). They can also obfuscate the origins of the money through layers of multiple transactions that create a complicated web to unravel.
3. Immediacy: Bitcoin transactions are nearly instantaneous (although the actual confirmation of the transaction can take longer). This allows for rapid shifting of money to different locations, again making it difficult to track the flow of funds as well as to stop a transaction if there is suspicion of illegal activity.

Fears of Bitcoin being used for money laundering are widely shared by financial regulators across the world, which is fuelling efforts to extend regulations to cryptocurrencies (see the section on "attempts to regulate" below).

However, others argue that claims of the anonymity Bitcoin provides – and thus its suitability as a means to conduct illegal transactions – are overstated. In particular, it is important to remember that while users can conduct transactions largely anonymously, that does not mean that their actions are not recorded. All Bitcoin transactions are recorded on the blockchain, and these records are freely available to inspect.

Moreover, although transactions do not record the personal identity of the persons involved, they do still log the public keys used by all involved parties (public keys are unique identifiers and, as the name implies, they are publicly visible). These public keys and their associated activities can be tracked, allowing for the possibility of observing bitcoin flows and identifying where the money went (for example, if it was deposited in a specific exchange, or if it is still located at a user's personal address) (Meiklejohn et al. 2013).

Users can have multiple addresses from which they conduct transactions (with an address just being a similar form of unique identifier like a public key), but analyses of transaction histories can identify patterns and attribute these seemingly isolated transactions to a single user (Ludwin 2015).

Importantly, the findings of Meiklejohn et al. (2013) suggest that any Bitcoin tied to illicit activity – either bitcoin acquired as a result of illegal activities or bitcoin used to fund illegal activities or purchases – will eventually find its way to one of the mainstream Bitcoin exchanges. As these exchanges record personal information about account holders, this opens up the opportunity for users to be identified if they are suspected of illegal activity and the exchange in question is put under pressure to disclose pertinent information (for example, via a subpoena).

Despite a preponderance of literature and articles that assert Bitcoin provides full anonymity, this simply is not true. It is far more accurate to think of Bitcoin as pseudonymous rather than truly anonymous. Even Bitcoin.org clearly states on its website that Bitcoin is not anonymous (2018). Criminals can take steps to make their paths hard to follow, but ultimately, if the transactions occur via the blockchain, then they can be tracked.

Illegal transactions

Black market transactions

Bitcoin has gained notoriety for allegedly becoming the currency of choice for illegal transactions. One of the most prominent examples of this is the currently-defunct website Silk Road. This was an online black market that primarily traded goods like narcotics, prescription drugs and counterfeit documents (by one account, 70 per cent of the 10,000 products listed on the marketplace were some sort of drug [Levin at al. 2015]). Importantly, the only currency accepted by the Silk Road was bitcoin.

A 2013 study estimated that the site saw a monthly sales volume equivalent to more than US$1.22 million (Christin 2013). The site has gone through multiple iterations and was shut down by international authorities on two different occasions. It also helped lead to the arrest of Charlie Shrem, generally considered to be Bitcoin's "first felon". Shrem led a Bitcoin exchange known as BitInstant. He was arrested in 2014 for violating anti-money laundering laws through selling bitcoin to users of Silk Road (Spaven 2015). Today, the Silk Road website appears to be non-functional.

Authorities in the UK also claim that Bitcoin is making it easier for drug dealers to hide their actions. In London, police allege that cryptocurrency ATMs give dealers an opportunity to quickly convert cash into bitcoin, providing an alternative to having to make a large cash deposit into their bank accounts that might otherwise arouse suspicion (Corcoran 2017).

Ransomware

Bitcoin has also enjoyed increasing popularity in connection with "ransomware" attacks, whereby cybercriminals take control of computer and block access to its files; users must pay a ransom fee to have the attack lifted. These types of attacks are becoming increasingly common, and Bitcoin is increasingly becoming the preferred currency the attackers ask for, due to its (presumed) anonymity. Some experts even believe the rise of Bitcoin is increasing the frequency of these attacks (Palmer 2016).

Tax evasion

Bitcoin transactions happen "in the absence of government, bank, authorised dealer, payment network, or regulator" (Sapovadia 2015). This means for those interested in declaring their Bitcoin assets to the relevant tax authorities, there tends to be significant confusion about what types of regulations apply and how to declare properly. But it also means that for attempting to evade taxes, the use of bitcoin and other cryptocurrencies presents very real opportunities.

The lack of a central, sovereign jurisdiction that can provide information on transactions means traditional anti-tax evasion strategies, especially those that target tax havens, will not work for Bitcoin. Since transactions occur without divulging personal information and the act of tracing transactions back to individuals is possible but still potentially extremely laborious, tax authorities are highly unlikely to know about Bitcoin-related income unless it is reported (Bal 2015).

It is hard to know just how much potential tax revenue is going uncollected. A lawsuit filed by the Internal Revenue Service (IRS) in the United States against Bitcoin exchange site Coinbase revealed that, in 2015, just 802 individuals reported a Bitcoin transaction (Roberts 2017). To try to combat this issue, the IRS has reportedly purchased specialised software for tracking Bitcoin transactions (Cox 2017).

Attempts to regulate

The European Union

Increasingly, governments are attempting to regulate Bitcoin and other cryptocurrencies as a way to eliminate the loopholes and grey areas in which it operates.

Most recently, both the United Kingdom and the European Union have announced their intention to regulate cryptocurrencies so they adhere to existing anti-money laundering legislation as well as counter-terrorism financial legislation.

A proposed amendment to the EU's anti-money laundering and terrorist financing legislation was first released in July of 2016 and is currently being discussed by member states (European Commission 2016). It proposes to "designate virtual currency exchange platforms as obliged entities" to the EU's Fourth Anti-Money Laundering Directive (4AMLD).

This means exchange platforms as well as wallet providers would be subject to the same regulations as credit and financial institutions. They would be required to implement preventive measures as well as to report suspicious transactions. The proposal also addresses anonymity as one of the problems, stating that "national financial intelligence units (FIUs) should be able to associate virtual currency addresses to the identity of the owner of virtual currencies"; the proposal also says that the possibility of allowing users of virtual currencies to voluntarily disclose their identities to authorities should be assessed.

It is unclear, however, how soon any changes might go into effect. Negotiations have not yet been completed (which also means it is unclear what, if any, changes might be made to the proposal from July 2016), and when they are, member states will still have two years to integrate the directive into their national laws (Meyer 2017).

Worldwide

Looking beyond the EU, French Finance Minister, Bruno Le Maire, has said he intends to ask fellow G20 members to contemplate establishing a joint regulatory framework for Bitcoin, a measure

supported by Germany and Italy (Buergin et al. 2017).

Several prominent Asian countries have already moved to regulate Bitcoin exchanges or have expressed intentions to do so.

China was already moving to regulate Bitcoin in some capacity as early as 2013. Originally, the Chinese authorities simply banned financial services companies from working with Bitcoin exchanges, meaning residents could not use their Chinese bank accounts to buy bitcoins on Chinese exchanges (Parker 2017). But in September 2017, China announced an outright ban on cryptocurrency exchanges, which has since taken effect.

Singapore announced in 2014 that it will regulate "virtual currency intermediaries" (for example, exchanges and bitcoin vending machines) located within Singapore, requiring them to verify the identity of customers and to report suspicious transactions to the responsible body (Monetary Authority of Singapore 2014). As of 2017, Singapore's central bank chief said these requirements will be formalised in an upcoming payment services regulation law (Chanjaroen et al. 2017).

In December 2017, the Australian parliament amended its anti-money laundering and counter-terrorism legislation to apply to Bitcoin exchanges. The law makes it illegal for unregistered persons to provide exchange services. It also requires exchanges to maintain anti-money laundering and counter-terrorism financing programmes and to report suspicious transactions (Chau 2017).

Potential applications of blockchain for anti-corruption

Blockchain and distributed legder technology

As highlighted above, blockchain technology must be looked at somewhat separately from different applications of Bitcoin and other digital currencies.

Blockchain is the most common type of distributed ledger technology (DLT) and forms the backbone of the kinds of cryptocurrencies discussed in section 2. Yet, it can also be used for other data storage applications and is increasingly recognised for this potential. There is a large body of research on feasible applications of this technology, yet the number of cases showing its use remains limited (Stinchcombe 2017). Different types of DLT can potentially be used for such purposes and it is important to understand the difference between them (BlockchainHub 2017):

1. Public blockchains are open for everyone to participate in and to send and verify transactions. They are open source and no special permissions are needed. They are based on a proof-of-work consensus algorithm, offer transparency of transactions and can be used with pseudonyms. They form the basis of the most common digital currencies.
2. Federated blockchains are run by consortia of several organisations. Access to them can be public or restricted to participating organisations. Their consensus protocol is typically based in pre-selected nodes. This makes federated blockchain much faster and cheaper to operate. They are used by consortia in the banking, insurance or energy sectors.
3. Private blockchains are restricted to members of a specific organisation. The verification process is restructured to fit the members. Private blockchains are

mainly a different way for an organisation to store data, to simplify document handling and introduce a different compliance mechanism. This can also help to avoid storing the same data on several devices and potentially creating conflicting versions of it. They provide certain advantages and disadvantages with regards to data security.

4. Alternative types of DLT include the recently formed IOTA project, which is based on a network technology titled the tangle. It removes miners from the DLT system and gives each user equal responsibility to add and verify data (Popov 2017).

All applications of DLT are used to store different types of data. As such, they can make data more secure, make changes transparent, support and verify transactions. Once implemented, DLT can be easy to operate and quite efficient, yet not all data storage situations lend themselves to its use.

DLT anti-corruption attributes

DLT is not typically used as a specific anti-corruption tool. Yet, its attributes can make DLT applications more resilient to corruption:

1. Transparency: DLT-based data systems record all changes to stored data. Everyone with access to a blockchain can verify the data stored in this context. Transactions can thus be made more transparent.
2. Immutability: once data is stored on the blockchain, it cannot be altered. It is thus safe from manipulation and illegitimate changes.
3. Security: as data is stored on distributed ledgers, it is secured against fraud and against attacks on a single server.
4. Inclusiveness: public blockchains are open source and accessible to everyone. DLT systems can thus be opened to all citizens, democratising data storage.
5. Disintermediation: DLT systems cut out a third party needed to verify transactions. This reduces transactions costs and makes them potentially less vulnerable to corruption.

To different degrees, these attributes can be assigned to all DLT applications. As such, they can safeguard stored data and transactions administered via DLT against manipulation through corrupt actors.

Immutability and security features make it harder for corrupt actors to manipulate data. The removal of third parties lowers the opportunity for bribery or fraud. Transparency and inclusiveness establish constraints on corruption and make corrupt transactions easier to recognise. Based on these attributes, experts see a lot of potential for DLT to support anti-corruption efforts.

The following section discusses DLT applications in government services. There as yet, however, hardly any successful cases of DLT being used in this context. Blockchain technology has potential for anti-corruption, but is far from being an easily applicable and transferable anti-corruption instrument (Kim & Kang 2017).

Securing government data

At its core, DLT provides a different way of storing data that brings both advantages and disadvantages. Storing data on the blockchain can have positive effects for anti-corruption, if safeguards against corruption are considered in the design process. Data audits need to be built in.

It must be ensured that transparency of transactions also leads to more accountability. This needs consideration in the application design process and in expectation management. Blockchain has real potential to improve data management in the public sector. It might be able to increase trust in governments in contexts which are affected by corruption and thus often show low levels of trust. Its implementation, however, also presents considerable challenges (Cheng et al. 2017). These challenges are discussed in the final part of this paper.

Land registries

Some of the most advanced conceptualisations of using blockchain for storing government data come from land governance initiatives. DLT can be used to store land registry entries and land titles on the blockchain to protect them against fraud and corruption. Several countries run such pilot projects:

1. In Honduras, Factom is building a land registry database on the blockchain to empower citizens to fight for land titles in court. The project has been in development since 2015 and has not yet been fully deployed, but is considered promising (Collindres et al. 2016)
2. In Sweden, ChromaWay is developing a similar concept to test the possibility of running housing purchases using DLT and smart contracts (see below). The project is still in its exploratory phase (ChromaWay 2017).
3. In Ghana, Bitland aims to protect and secure land titles by putting them on the OpenLedger blockchain (Bates 2016). It has provided its proof-of-concept, but has not yet been fully implemented.
4. In Georgia, Exonum (2017) is used to transfer the Georgian land registry onto a blockchain. The project was launched in 2017 by the Georgian government together with Bitfury. Having completed its first phase, Georgian land titles are currently hashed on the blockchain, securing them from tampering and providing a time-stamped and sealed copy of data, akin to Bitcoin transactions described earlier. Longer term objectives include running changes to land titles via the blockchain, a project that remains to be implemented.

Voting

In societies that show high corruption levels, voting processes are often subject to fraud and corrupt practices. This seriously undermines the operation of electoral democracies and citizens' trust in democratic systems. Several projects look at using DLT in the context of voting. They go as far as claiming that blockchain could revolutionise the way that democracies operate.

FollowMyVote describes a way that electronic voting could be secured via a blockchain. Voters install a digital voting booth, submit their identify information for verification and get verified with voter registries. They can then submit their ballot to a blockchain-based ballot box while remaining anonymous using private keys. Similarly, an app called Sovereign offers blockchain-based voting solutions, using tokens that voters can send as votes via the blockchain. This enables more complex voting situations with, for example, separation of votes between different candidates or voting for or against certain aspects of a treaty (Leary 2017).

Securing transactions

In its original conception as the underlying technology of Bitcoin, DLT is used to secure and record transactions of digital currencies. Increasingly, people are using the blockchain to store and verify other transactions as well. This can include international money flows, the movement of goods and the implementation of contracts. Blockchain is already used by several bank consortia and has potential in cross-border payments as these are often difficult to process and need third parties to verify transactions. (Higginson 2016).

In the context of anti-corruption, there are several applications in which DLT might secure transactions.

Financial transactions

Many international development organisations provide budget support or financing for specific projects to recipient countries. These payments are often vulnerable to corruption. In 2017, German development bank KfW initiated TruBudget, a pilot project to provide budget support and project management based on a private blockchain. All stakeholders involved in a project can access the TruBudget. Requests, submissions of documents and approvals can all be processed in real time through the platform and by all the stakeholders involved. These can include a donor organisation, national governments, local governments, implementing agencies, banks and others. Basing the platform on the blockchain can establish trust between the different partners as data is hosted in a decentralised manner and secured against subsequent alteration. TruBudget is currently in development and is scheduled for testing soon (Aldane 2017).

In 2017, the World Food Programme (WFP) began a pilot programme to distribute food vouchers in one of Jordan's refugee camps using the Ethereum blockchain. Food vouchers are assigned to refugees, who can access them in supermarkets in refugee camps using biometric data. The project uses a private "fork" of the Ethereum database, so that it does not need miners to verify transactions and that the data is not stored openly on all nodes of the Ethereum network. So far, the WFP has transferred over US$1.4 million in food vouchers to 10,500 Syrian refugees and it plans to extend the programme to 100,000 refugees in 2018. The implementation using the blockchain runs more efficiently and provides better security against fraud (Wong 2017).

Supply chain management

Global supply chains involve a large number of transactions and a complex system of documentation that is vulnerable to corruption due to the myriad of actors involved. Currently a lot of information in supply chains is still recorded on paper. It is thus vulnerable to potential alterations or to information being lost. In any case, a paper-based system is not the most efficient solution.

Several organisations are thus working to digitalise supply chains and using blockchain technology in this context. Storing data on products on a blockchain makes transaction data instantly available and traceable in real time. It makes transactions safer and more transparent as time stamps make it possible to audit transactions (Heinen 2017).

IBM is running several projects aimed at creating blockchain-based supply chain management systems. Everledger is a global registry for diamonds that is run on the blockchain. It registers a unique ID for each diamond and traces its ownership, starting in the mine. This system is

meant to combat counterfeiting and, crucially, the spread of conflict diamonds (Volpicelli 2017).

Smart contracts

One of the most cited blockchain applications are smart contracts. These are contracts which are written in code instead of paper. They are signed by digital signatures and automatically implemented. This means that conditions that are written in the contract determine the execution of the contract. If the conditions are met and verified, the contract will be executed automatically. This procedure, similar to other blockchain transaction, cuts out middle men.

Audits and safeguards can be coded into a smart contract, which could in theory limit the scope for fraud and corruption. Smart contracts, as they are saved on the blockchain, are transparent but cannot be altered without consent. If properly coded, opportunities for corruption are thus limited. This makes smart contracts potentially applicable to several areas of government contracting, especially with regards to the potential to limit manipulation during public procurement processes.

One company advancing the idea of smart contracts is Ethereum, which has made such contracts a major part of its business model (Buterin 2017). While there is a lot of enthusiasm behind smart contracts, they are still far from being practicable due to the reasons discussed in the final section below.

Challenges and open questions

As many observers hail the advent of the blockchain revolution, there remain many challenges to the use of blockchain technology for securing government data, formulating smart contracts, managing supply chains or keeping track of cross-border money flows. So far, there are very few successful cases of DLT being used in this context (Stinchcombe 2017). While the potential for using blockchain in this context is significant, it will probably still take years for the technology to mature to widespread use (Banker 2017). Several challenges are still ahead.

Legal questions

DLT is still very new. Many applications are thus still lacking an appropriate legal and regulatory framework in which to operate. Public blockchains pose a particular challenge. Their nodes, and therefore the data that is stored on the blockchain, can be located in any country. This poses several legal questions (McKinley et al. 2017):

1. Which jurisdiction applies to transactions conducted using the blockchain?
2. Who is liable for malfunctions of the distributed ledger system?
3. What happens to government data that legally cannot be taken out of a given country?

Furthermore, privacy legislation can be cause for concern, notably the “right to be forgotten” which will be applied as part of the EU’s General Data Protection Regulation (GDPR). As old data on the blockchain cannot be deleted or altered, a user’s request to erase personal data could provide a serious challenge (McKenzie & Taylor 2017).

Smart contracts on their own provide several legal challenges. Currently it is unclear if and to what extent they are legally enforceable and if they would be accepted by contracting authorities (McKinley et al. 2017). Additionally, in some jurisdictions, more complex smart contracts might need some sort of verified digital identity to be signed and to be legally binding.

Infrastructure challenges

Blockchain promises secure, fast and efficient transactions. However, it is not always the case that blockchain transactions are fast. Public blockchains in particular can be slowed down through their proof-of-work verification mechanism; by design, all nodes are processing all transactions. Transactions can often not be verified for several minutes, which is much slower than traditional database solutions.

Fees for performing transactions on the Bitcoin blockchain have recently also soared, making it less attractive for smaller transactions (Lee 2017). These problems can partially be circumvented using private or federated blockchains, or by other DLT applications such as IOTA. Yet, they are to be considered when thinking about the merits of DLT, some of which are not as pronounced when implemented in the form of a private blockchain (Buterin 2015). The infrastructure for a wide use of public blockchains is not fully implemented, and scalability remains an issue (McKinlay et al. 2017) – at least, for now.

References

Aldane, J. 2017. KfW Tests Blockchain Software to Track Funding in Africa. https://www.devfinance.net/blockchain-track-public-spending-africa/

Bal, A. 2015. How to Tax Bitcoin? in *Handbook of Digital Currency (*Lee Kuo Chen, D. ed.*)*. Academic Press. pp. 267-282.

Banker, S. 2017. Blockchain In the Supply Chain: Too Much Hype. https://www.forbes.com/sites/stevebanker/2017/09/01/blockchain-in-the-supply-chain-too-much-hype/#3dd26393198c

Bitocin.org. 2018a. Running A Full Node. https://bitcoin.org/en/full-node

Bitcoin.org. 2018b. FAQ. https://bitcoin.org/en/faq

BlockchainHub. 2017. Blockchains & Distributed Ledger Technology. https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/

Buergin, R., Jennen, B. & Follain, J. 2017. Germany Joins French-led Moves to Regulate Bitcoin at G-20 Level

Buterin, V. 2015. On Public and Private Blockchains. https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

Buterin, V. 2017. Ethereum White Paper. https://github.com/ethereum/wiki/wiki/White-Paper

Chanjaroen, C., Tan, A., & Amin, H. 2017. Singapore Won't Regulate Cryptocurrencies, Central Bank Chief Says

Chau, D. 2017. Bitcoin One Step Closer to Being Regulated in Australia Under New Anti-Money Laundering Laws. http://www.abc.net.au/news/2017-10-23/bitcoin-one-step-closer-to-being-regulated-in-australia/9058582

Cheng, S., Daub, M., Domeyer, A. & Lundqvist, M. 2017. Using Blockchain to Improve Data Management in the Public Sector

Choo, K. 2015. Cryptocurrency and Virtual Currency: Corruption and Money Laundering/ Terrorism Financing Risks? in *Handbook of Digital Currency (*Lee Kuo Chen, D. ed.*)*. Academic Press. pp. 283-307.

Christin, N. 2013. Traveling the Silk Road: A Measurement Analysis of a Large Anonymous Online Marketplace. Proceedings of the World Wide Web Conference 2013.

ChromaWay. 2017. Blockchain and Future House Purchases Second Phase Completed in March 2017. https://chromaway.com/landregistry/

Coinmarketcap.com. 2018. Cryptocurrency Market Capitalizations. https://coinmarketcap.com/all/views/all/

Collindres, J.C., Regan, M. & Panting, G.P. 2016. Using Blockchain to Secure Honduran Land Titles. https://s3.amazonaws.com/ipri2016/casestudy_collindres.pdf

Corcoran, K. 2017. Drug Dealers Are Laundering Cash at Bitcoin ATMs, London Police Say. http://www.businessinsider.de/drug-dealers-laundering-their-money-at-bitcoin-atms-london-police-say-2017-12

Cox, J. 2017. IRS Now Has a Tool to Unmask Bitcoin Tax Cheats. https://www.thedailybeast.com/irs-now-has-a-tool-to-unmask-bitcoin-tax-cheats

European Commission. 2016. COM (2016) 450: Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing and amending Directive 2009/101/EC. http://eur-lex.europa.eu/procedure/EN/2016_208

Exonum. 2017. Blockchain Land Registry. https://exonum.com/napr

Hackett, R. & Wieczner, J. 2017. How High Can Bitcoin's Price Go in 2018. http://fortune.com/2017/12/21/bitcoin-price-value-prediction-bubble/

Heinen, D. 2017. Blockchain in Supply Chain Management – In the Future, Trust Must Be Earned Rather than Paid. https://www.capgemini.com/consulting/2017/07/blockchain-in-supply-chain-management-in-the-future/

Higginson, M. 2016. How Blockchain Could Disrupt Cross-Border Payments. https://www.theclearinghouse.org/research/2016/2016-q4-banking-perspectives/blockchain-cross-border-payments

Kim, K. & Kang, T. 2017. Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology. The 2017 OECD Global Anti-Corruption & Integrity Forum. https://www.oecd.org/cleangovbiz/Integrity-Forum-2017-Kim-Kang-blockchain-technology.pdf

Kroll, J. A., Davey, I. C., & Felten, E. W. 2013. The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Proceedings of WEIS (Vol. 2013).

Leary, K. 2017. Blockchain Might Be About to Change the Way We Vote. https://www.weforum.org/agenda/2017/09/blockchain-could-be-about-to-change-how-you-vote

Levin, R.B., O'Brien, A.A. & Zuberi, M. M. 2015. Real Regulation of Virtual Currencies. In *Handbook of Digital Currency* (Lee Kuo Chen, D. ed.). Academic Press. pp. 327-360.

Ludwin, A. 2015. How Anonymous is Bitcoin? A Backgrounder for Policymakers. https://www.coindesk.com/anonymous-bitcoin-backgrounder-policymakers/

McKenzie, I. & Taylor, M. 2017. An Introduction to Blockchain: The Key Legal Issues. http://www.osborneclarke.com/insights/an-introduction-to-blockchain-the-key-legal-issues/

McKinlay, J., Pithouse, D., McGonagle, J. & Sanders, J. 2017. Blockchain: Background, Challenges and Legal Issues. https://www.dlapiper.com/en/uk/insights/publications/2017/06/blockchain-background-challenges-legal-issues/

Meiklejohn, S.; Pomarole, M.; Jordan, G.; Levchenko, K.; McCoy, D.; Voelker, G.; & Savage, S. 2013. A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. Proceedings of the 2013 Internet Measurement Conference. pp. 127-140. https://cseweb.ucsd.edu/~smeiklejohn/files/imc13.pdf

Meyer, D. 2017. Here's When Europe's New Bitcoin Rules Will Come into Effect. http://fortune.com/2017/12/04/eu-bitcoin-anti-money-laundering-uk/

Monaghan, A. 2017. Bitcoin is a Fraud that Will Blow Up, Says JP Morgan Boss. https://www.theguardian.com/technology/2017/sep/13/bitcoin-fraud-jp-morgan-cryptocurrency-drug-dealers

Monetary Authority of Singapore. 2014. MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://people.eecs.berkeley.edu/~raluca/cs261-f15/readings/bitcoin.pdf

Palmer, D. 2016. How Bitcoin Helped Fuel an Explosion in Ransomware Attacks. http://www.zdnet.com/article/how-bitcoin-helped-fuel-an-explosion-in-ransomware-attacks/

Parker, E. 2017. Can China Contain Bitcoin? https://www.technologyreview.com/s/609320/can-china-contain-bitcoin/

Popov, S. 2017. The Tangle. http://iota.org/IOTA_Whitepaper.pdf

Roberts, J. 2017. Only 802 People Told the IRS About Bitcoin. http://fortune.com/2017/03/19/irs-bitcoin-lawsuit/

Sapovadia, V. 2015. Legal Issues in Cryptocurrency. in *Handbook of Digital Currency* (Lee Kuo Chen, D. ed.). Academic Press. pp. 253-266.

Spaven, E. 2015. Bitcoin's 'First Felon' Charlie Shrem Begins 2-Year Sentence. https://www.coindesk.com/bitcoins-first-felon-charlie-shrem-begins-2-year-sentence/

Stinchcombe, K. 2017. Ten Years in, Nobody Has Come Up with a Use for Blockchain. https://hackernoon.com/ten-years-in-nobody-has-come-up-with-a-use-case-for-blockchain-ee98c180100

Volpicelli, G. 2017. How the Blockchain is Helping Stop the Spread of Conflict Diamonds. http://www.wired.co.uk/article/blockchain-conflict-diamonds-everledger

Wong, J. I. 2017. The UN is Using Ethereum's Technology to Fund Food for Thousands of Refugees

Yermack, D. 2013. Is Bitcoin a Real Currency? An Economic Appraisal. National Bureau of Economic Research. http://centerforfinancialstability.org/research/DavidYermack-Bitcoin.pdf

TRANSPARENCY INTERNATIONAL
the global coalition against corruption

"Anti-Corruption Helpdesk Answers provide practitioners around the world with rapid on-demand briefings on corruption. Drawing on publicly available information, the briefings present an overview of a particular issue and do not necessarily reflect Transparency International's official position."

Transparency International
International Secretariat
Alt-Moabit 96
10559 Berlin
Germany

Phone: +49 - 30 - 34 38 200
Fax: +49 - 30 - 34 70 39 12

tihelpdesk@transparency.org
www.transparency.org

blog.transparency.org
facebook.com/transparencyinternational
twitter.com/anticorruption

Transparency International chapters can use the Helpdesk free.
Email us at ***tihelpdesk@transparency.org***