Journal of Cyber Policy

ISSN: 2373-8871 (Print) 2373-8898 (Online) Journal homepage: http://www.tandfonline.com/loi/rcyb20

Blockchain technology for social impact: opportunities and challenges ahead

Walid Al-Saqaf & Nicolas Seidler

To cite this article: Walid Al-Saqaf & Nicolas Seidler (2017) Blockchain technology for social impact: opportunities and challenges ahead, Journal of Cyber Policy, 2:3, 338-354, DOI: 10.1080/23738871.2017.1400084

To link to this article: https://doi.org/10.1080/23738871.2017.1400084

JOURNAL OF CYBER POLICY, 2017
VOL. 2, NO. 3, 338–354
https://doi.org/10.1080/23738871.2017.1400084

Routledge
Taylor & Francis Group

Blockchain technology for social impact: opportunities and challenges ahead

Walid Al-Saqaf[a] and Nicolas Seidler[b]

[a]School of Social Sciences, Södertörn University, Stockholm, Sweden; [b]Internet Society International, Geneva, Switzerland

ABSTRACT

While much has already been written about blockchain applications and prospects in the FinTech industry, little research has been done to explore blockchain technology's user-centric paradigm in enabling various applications beyond banking. This article is an effort to contribute to that body of scholarship by exploring blockchain technology's potential applications, and their limits, in areas that intersect with social impact, including human rights. This article explores whether blockchain technology and its core operational principles – such as decentralisation, transparency, equality and accountability – could play a role in limiting undue online surveillance, censorship and human rights abuses that are facilitated by the increasing reliance on a few entities that control access to information online. By doing so, this article aims at initiating a scholarly curiosity to understand what is possible and what is to be concerned about when it comes to the potential impact of blockchain technology on society.

ARTICLE HISTORY
Received 9 March 2017
Revised 11 October 2017
Accepted 30 October 2017

KEYWORDS
Internet; decentralisation; centralisation; blockchain; rights

Introduction

Barely a day passes without a news article predicting a great future or tragic downfall for cryptocurrencies and their underlying distributed technology, the blockchain.

Originally created by the open-source Bitcoin community to allow reliable peer-to-peer financial transactions, blockchain technology has made it possible to build a globally functional currency relying on code, without banks or any third-party platforms.

Nowadays, the applications of this internet-based distributed ledger technology are ranging all the way from simple verification of digital identities to automating multi-layered payments using complicated smart contracts. The prospect of a future that directly manages services for users and does away with reliance on powerful intermediaries generates great hopes, but also fears, that extend well beyond the domain of the FinTech[1] industry to areas that may impact the livelihood and rights of people.

Building on the permissionless[2] nature of the internet, blockchain technology is one approach that has the potential to enhance decentralisation, transparency, equality and accountability on the internet. Yet, one must also acknowledge that the technology remains relatively untested and may very well hold both familiar and new risks that we will address in this article. Much like other anonymity-based technologies, blockchain

technology can be used both for legitimate uses along with malicious ones, such as the hosting of illicit content and activities.

While much has already been written about blockchain applications and prospects in the FinTech industry, little research has been done to explore blockchain technology's user-centric paradigm in enabling various applications beyond banking. This article is an effort to contribute to that body of scholarship by exploring blockchain technology's potential applications, and their limits, in areas that intersect with social impact, including human rights.

This article explores whether blockchain technology and its core operational principles – such as decentralisation, transparency, equality and accountability – could play a role in limiting undue online surveillance, censorship and human rights abuses that are facilitated by the increasing reliance on a few entities that control access to information online. By doing so, this article aims to initiate a scholarly curiosity to understand what is possible and what one might be concerned about when it comes to the potential impact of blockchain technology on society.

What is the blockchain?

Blockchain technology was first introduced as the underlying structure and mechanism of Bitcoin, a digital cryptocurrency released in 2009 as an open-source system by a person or group of people nicknamed Satoshi Nakamoto.

While the increase in computing power, affordability and global expansion of internet access have set foundations for the growth of cryptocurrencies, their breakout into the public sphere also has to be understood in the context of a strong public reaction to the pitfalls of centralised systems and institutions after the 2008 financial crisis (Ito, Narula, and Ali 2017). This crisis, which some economists consider one of the worst since the Great Depression, shook people's trust in traditional financial intermediaries (Uslaner 2010).

Bitcoin offered a technological response: for the first time ever, people would be able to carry out large monetary transactions without the need to trust or rely on intermediaries. Built on the principles of an interconnected and interdependent chain of blocks – with each block being a record of a cryptographically signed transaction, hence the term 'blockchain' – the trust would shift away from third parties and legacy institutions towards code and a community-based, open-source, peer-to-peer system of transparency and accountability.

So what is blockchain technology exactly?

In very simple terms, the blockchain is a distributed digital ledger or accounting book. Instead of relying on a bank or a lawyer to attest that money was exchanged or that a contract was made, each transaction between members, or nodes, of the blockchain is securely reflected through strong cryptography as an extra *block* in a database, of which all full *nodes* have a copy. Due to how the blockchain works and is designed, no single node can defraud or tamper with its content.[3] To ensure that everyone is using the same version of the blockchain and that no conflicting versions emerge, the design incorporates a system of collective consensus and verification through *mining*, which is a way to establish proof of the work.[4]

What makes blockchain technology unique is its ability to store data immutably without relying on a central authority. This allows it to preserve its integrity and prevent hacking or

other manipulation attempts. As such, it has the potential to replace the intermediary and central entities with code alone that can reliably connect users with each other (Tapscott and Tapscott 2016).

It is important to note that while Bitcoin was the first application of blockchain technology, the term 'Bitcoin' should not be used to mean 'blockchain', which is a much broader term. Cryptocurrencies such as Bitcoin are but one use of blockchain technology, which ranges from finance to record-keeping and from tracking the flow of goods to verifying the identity of citizens. The fundamental common characteristic that all blockchain-based services share is a design that depends on immutability and decentralisation in storing data. Yet, a system based on the community cannot work without the community. Each individual blockchain-based service has its own community that varies depending on how it is designed and operated. While Bitcoin depends on traders, consumers, miners and core developers, each other service has its own community members that collectively create, develop and use it.

One of the latest features of blockchain technology is called 'smart contracts', which can be described as automated computer programs that can be triggered to transfer digital assets automatically within the same blockchain, upon meeting certain triggering conditions. A smart contract, which itself is immutable since its code is on the blockchain, makes it possible to do a host of transactions without any human intervention (Fairfield 2014). Ethereum, which in 2016 became the second most widely used permissionless blockchain cryptocurrency system, was the first to introduce a smart contract ecosystem. Some enthusiastic entrepreneurs and governments have started looking into smart-contract-based applications ranging from decentralised voting to identity verification and from global money transfers to decentralised fundraising (Pilkington 2016).

The applications of blockchain technology are numerous since they allow disintermediation in ways that can potentially empower people in trade, expression, democratic participation, social interaction and financial freedom. Yet as we will see later, there are challenges and risks that need to be considered and addressed for the technology to yield an overall positive outcome for society.

A reaction to increased centralisation on the internet

The increased interest in and use of distributed ledger technologies such as the blockchain need to be understood in contrast with the high concentration of user interactions and data at the internet's application layer, such as on search engines, social networks and content platforms (Internet Society 2014).

Aided by the rise of smartphones and cheaper, easier telecommunication access, the internet has witnessed tremendous growth since 2000. At the same time, internet users have gradually turned to a relatively small set of aggregating platforms to retrieve information and communicate with one another (Clark et al. 2017). Over time, the internet became more centralised, which is rather counter-intuitive since decentralisation is the basis on which the internet was founded.

This development can be observed by the fact that the wealth amassed in the last dozen years or so mainly benefited a small number of global corporations, whose strategy was to link internet users to each other by serving as a customer interface.

> Uber, the world's largest taxi company, owns no vehicles. Facebook, the world's most popular media owner, creates no content. Alibaba, the most valuable retailer, has no inventory. And Airbnb, the world's largest accommodation provider, owns no real estate. (Goodwin 2016)

Billions of people from all parts of the world have become dependent on the digital products and services of a small number of global corporations that serve, whether they want to or not, as choke points for individuals' personal data, speech and more (MacKinnon 2017). While internet users remain highly distributed on a global network of networks, the data these users produce are very much concentrated in the hands of a few companies.

This interconnectedness is helpful to users since it reduces the time and effort it takes to access their data or use other online services. It also allows many small businesses to flourish on such platforms and gives some internet users, such as video bloggers, the opportunity to generate income by monetising content through advertisements and other methods (Marsden 2010).

However, having such a degree of centralisation is the antithesis of the original promise of the internet as an open-source and interoperable network with the ability to endure massive losses to its underlying physical network (Leiner et al. 2009).

The creator of the World Wide Web, Tim Berners-Lee, has publicly called for a return to some of the earliest ideals of decentralisation:

> The web is already decentralised, […] The problem is the dominance of one search engine, one big social network, one Twitter for microblogging. We don't have a technology problem, we have a social problem. (Tim Berners-Lee, as cited in Hardy 2016)

Several examples of cyberattacks and technical failures in recent years have illustrated that the centralised model is vulnerable to different forms of abuse or malfunction that can harm individuals, including the right to privacy and freedom of expression.

For example, the Snowden revelations exposed how the U.S. government had direct access to data from Google, Facebook and other U.S. companies (Landau 2013). Another example is the 2012 hack of LinkedIn, which compromised over 100 million user accounts (Paul 2012). On the side of freedom of expression, data from Freedom House suggests that internet restrictions – including censorship, filtering of content and harassment of bloggers, to name a few – have been on the rise since at least 2012 (Freedom House 2016).

It is important to consider that in the early 2000s, some attempts to dial back the severity of centralisation of online content services were made using peer-to-peer (P2P) applications such as Napster and protocols such as BitTorrent, which helped combat centralisation by using overlay networks such as Freenet, a unique method of limiting surveillance and control (Clarke et al. 2010). But using such tools also resulted in legal challenges, mainly in the domain of copyright infringements (Vincents 2007).

Some other technologies focused more on limiting surveillance by internet service providers (ISPs) and governments. They did so by avoiding the use of companies and instead by relying on other users as proxies. Among such initiatives is the Tor Project, which was among the most ambitious open-source projects aimed at creating a blocking-resistant web experience (Fairfield 2014). Each of those, however, still had their limitations in terms of man-in-the-middle attacks or exposing some of the users in the network (Chaabane, Manils, and Kaafar 2010).

Furthermore, a reaction from the powerless against powerful intermediaries cannot alone explain the early adoption and current uses of blockchain or other distributed technologies. There are several examples where illegal activities were a factor in using such technologies. For instance, BitTorrent was found to have been used to exchange child pornography (Greenemeier 2011), Tor was attributed with helping create marketplaces for human trafficking and other crimes (O'Neill 2017) and Bitcoin was the cryptocurrency used by hackers to extort funds from victims in return for restoring access to valuable data (Ali, Clarke, and McCorry 2015). In other words, it is important to keep in mind that technology is not inherently good or bad; rather it creates a set of potentials that are informed by its core architecture and principles.

Against this backdrop, let us dive in in more detail with some of the promises and pitfalls of blockchain technology when it comes to its impact on society at large.

Individual autonomy, but for how long?

The Universal Declaration of Human Rights states: 'Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers' (Article 19, Universal Declaration of Human Rights).

While the internet came a long way in making this a reality, it fell short because a significant portion of content and speech are either hosted or routed by intermediaries, who have de facto power to restrict and control speech and contents. The blockchain technology offers to eliminate the need for a central platform altogether, giving individuals the ultimate power of sending and receiving information without oversight or central control.

In a permissionless blockchain, i.e. one that is open to anyone to participate, individuals are fully autonomous and can act on their own to send and receive information. As will be described in a later section, however, this does involve certain consequences such as the impossibility of enforcing laws or regulations on individual members without having to affect the whole infrastructure of the blockchain itself. Nonetheless, blockchain technology is arguably the first ever innovation where the end users are both at the centre as well as the periphery of the network. In fact, they are the network.

Blockchain technology makes it possible to evade forms of repression by authorities that control online content through ISPs or content platforms. This feature allowed the creation of a censorship-resistant, Twitter-style social media platform called Twister, and Namecoin, which is a totally decentralised domain-name registry (Peck 2015). New app platforms such as Blockstack[5] promise full control for users over their data and identity through secure and decentralised communications. Blockchain technology could also be valuable for music producers to independently sell their music to end users without having to rely on middlemen such as agencies or music production companies (Joshi 2017).

Risks of re-centralisation

Yet, one thing we can learn from the internet's evolution is that a decentralised and distributed network can be overtaken by market forces and corporations, as was demonstrated by the likes of Google, Facebook and Amazon. Blockchain technology is not immune to a similar fate partly because users often prefer convenience to the ability to

serve as peers in a global blockchain system. This convenience could be provided through proprietary software in the form of apps on smartphones and computers that can interact with various blockchains. Some of the biggest IT corporations have already started investing in blockchain technology (Microsoft n.d.; IBM Corporation 2017).

Furthermore, the practical realities of blockchain-based transactions have led to centralisation mechanisms which are prone to failure and vulnerability. For example, the fact that cryptocurrencies are traded over exchanges[6] seems to shift the role of intermediaries from traditional banks to such exchanges. In fact, unlike banks, which are mostly fortified with strict security, exchanges are vulnerable and prone to potential theft through hacking and malware infection. One example is what happened in February 2014 when MtGox, which was the largest Bitcoin exchange in the world at the time, reported that 850,000 Bitcoins belonging to customers were stolen (Decker and Wattenhofer 2014). As of September 2017, that would have amounted to a loss exceeding USD 3.5 billion.

Government resistance

When the internet first emerged, governments initially did not pay much attention. But as it became a fundamentally impactful force affecting trade, media and communication, some governments started to resist by imposing restrictions and regulations to limit how the internet was used (Schneier 2013).

The same may be assumed for blockchain technology, which is still in an early developmental stage comparable to the internet of the early 1990s. Some governments are exploring blockchain and its applications (IBM Corporation 2017) with a view to make government services more efficient, while others may not be so keen on the range of economic and social activities potentially taking place on an unregulated and decentralised system, as demonstrated by the U.S. regulators' rejection of a Bitcoin exchange traded fund (Hunnicutt and Chavez-Dreyfuss 2017). In particular, the peer-to-peer functionality highlighted previously will likely not be welcomed by governments who are committing or sanctioning human rights abuses or those who wish to maintain a grip on the financial and information sectors.

It is important, however, not to discount the legitimate concerns that many governments may have when it comes to possible uses of cryptocurrency transactions to launder money (Stokes 2012), evade taxes (Torpey 2014) and carry out illegal activities in the black market. While there have already been proposals for ways to mitigate such abuses (Barber et al. 2012), the risk remains real and could have a substantial negative impact on societies.

Equality in design, divides in practice

Individuals are often negatively impacted when a particular group or person abuses power to the detriment of other members of the community. In a permissionless blockchain ecosystem, code is written in a way that does not favour certain individuals or groups over others. Permissionless blockchains typically rely on open-source code that does not differentiate between users based on social status, ethnicity or any other non-technical characteristics. They do not give particular nodes special privileges or impose conditions before verifying and executing transactions. This neutrality ensures that all are treated equally and are not abused by a central or more powerful element.

Furthermore, blockchains rely on the automated execution of code when agreed conditions are met, giving no room for subjective human interpretation. This comes in stark contrast to traditional legal frameworks, where the judiciary holds the power to interpret the law and issue sanctions or remedies. In the offline world, citizens can claim their rights in courts on the basis of legal provisions. But the judicial system also has its limits: it also tends to be slow, costly (see also 'New efficiencies and risks of fragmentation' section), territorial and can sometimes be subject to political influence or control.

A start-up called CrowdJury is using this feature by creating a blockchain-enabled online platform that crowdsources judicial proceedings from the moment of filing a complaint through the process of evaluation of evidence, and all the way to a virtual trial and jury verdict (Schiller 2016). Every single member of the blockchain is given equal rights and obligations in this virtual courtroom.

So, can automated, transparent code execution lead to a more equalitarian justice system? Not necessarily. First, there is no guarantee that pre-agreed conditions set in the code would be free from bias or discrimination. Second, the legal system purposefully leaves a little room for a limited amount of judicial interpretation in some instances, which can be necessary in complex cases that involve a wide range of variables. Human judgement can sometimes lead to mistakes, but also to fair assessments of complex legal situations.

Unequal access

What makes blockchain technology challenging to deploy and use effectively in some parts of the world is the fact that it requires fast and reliable internet access. The mining activity to verify blockchain transactions also requires significant processing power. The reality is that parts of the world still suffer from tremendously weak telecommunication infrastructures (Mlot 2015). Even developed countries can have inequities that favour one societal group or location (Riddlesden and Singleton 2014).

The fact that blockchains require distribution of data across various nodes exacerbates the problem due to the high bandwidth, processing power and storage demands to be an active node. This divide would naturally result in having some individuals, groups and regions less likely to reap the benefits of the technology for national services.

Additionally, there is a knowledge divide when it comes to creating and using blockchains. Looking at the major blockchain companies and start-ups around the world, it becomes apparent that the majority are based in Western countries (*Blockchain Daily News* 2017). The code and interfaces created for the blockchain software would therefore be likely to favour certain cultures and countries. The code would also be optimised to environments that assume a high degree of resourcefulness such as high bandwidth, storage and processing capacities, which are often unavailable in many developing countries.

Trust in code and coders

As with the case of any open-source software, there is always a community of core developers. While blockchains generally do not need to have trusted parties to operate, there is indeed an element of trust in the code and the people who write it. This may create an imbalance between the developer community and everyday users.

Bitcoin, for example, has a core group of developers, originally led by a person or group of people nicknamed Satoshi Nakamoto. This group is passionate and dedicated enough to improve the software and apply patches when necessary. The group effort to identify and quickly address patches through platforms such as the Bitcoin Wiki[7] has increased trust in the system. This did not prevent the exploitation of some vulnerabilities, however, such as a bug that led to over 184 billion Bitcoins being generated in a transaction and sent to two addresses. The bug was soon addressed and the blockchain was forked[8] without those false transactions. Yet, even the new clean version has built-in limitations in terms of scaling, since it can only deal with seven transactions per second. This is a major scalability limitation if it is to compete with other payment methods such as VISA, which can have as many as 4000 transactions per second (Scalability n.d.) . New initiatives such as SegWit and the Lightning Network are meant to help resolve this deficiency, but there is no consensus within the Bitcoin community as to which solution to use. Yet users have no choice but to trust in the developers and their decisions.

Another demonstration of the seemingly blind trust that some investors and blockchain enthusiasts put in the technology was the attack on the first Decentralised Autonomous Organisation (DAO) project in June 2016. The attack exploited buggy smart contract code resulting in the loss of over $60 million worth of Ether, the currency used in Ethereum (Morris 2016). This was followed by other thefts in 2017 that exploited bugs in popular software used by the Ethereum community leading to the loss of $34 million worth of Ether (Reiff 2017).

Transparency, accountability and the limits of anonymity

Corruption and human rights violations often thrive in environments of secrecy, information asymmetry and opaque communication channels. In stark contrast, blockchains are designed to bring total transparency to nodes in the system so that every single piece of information can be traced to its source and followed through with ease.

According to the World Bank, about 1.1 billion people do not have an official recognised document to prove their identity (Desai 2017). This makes victims of abuse invisible to society, making it difficult to help them effectively. This is also an issue for refugees seeking asylum and participation in society.

There are many possible blockchain applications of transparency. For example, just as it is possible to track a particular good from the producer to the consumer through blockchain-enabled supply chain applications, it is theoretically possible to identify if there are missing individuals based on the shared information that exists on a broad network of nodes connected to the same blockchain or even interoperable blockchains. Provided that ethical and privacy considerations are taken into account, which are essential conditions here so as to avoid a scenario of unwanted surveillance, it could be beneficial to track movements of refugees and asylees to facilitate knowing their whereabouts and providing them with the help they need. Evidently, another condition related to this is the ability of refugees to connect to the network, which is an important challenge.

Concrete blockchain-enabled applications have been created to improve transparency and traceability to help in fighting human trafficking in the fish (Provenance 2016) and diamond mining (Gadnis and Cronen 2017) industries, tackling child

exploitation (Forrest 2016) and verifying refugees' identities using apps installed on their smartphones in order to enable them to access basic services such as education and healthcare (Bindi 2017).

The domain of self-sovereign identity has been one of the most hyped in the realm of non-bitcoin applications of distributed ledger technology. While it holds a lot of potential, it is important to remember that this is a domain where there are challenges, including the extent to which personal information would be exposed and possibly subject to attacks (Miller 2017). To avoid such attacks, efforts such as the DIACC/SecureKey effort in Canada shows real promise of combining the benefits of the technology with more identifiable external trust anchors for users (SecureKey 2017).

Another relevant case is the protection of people's ownership rights of property, with real estate being one of the most viable areas of application. There are numerous cases in many countries where land grabs have caused tremendous loss to many lawful owners since ownership documents can be forged. In a fully transparent and mutually trusted blockchain-based public distributed ledger of land ownership, it is not possible to defraud the system and claim land ownership without taking over the blockchain itself. A demonstration of this application has been under way in the Republic of Georgia since 2016 and is often referred to as a solid proof of concept demonstrating the potential of blockchain technology to protect citizens' property (Bindi 2017). Sweden is also testing blockchain smart contracts for land registry (Rizzo 2016).

Similarly, it is possible to use blockchains to ensure free and fair elections as votes would be accounted for and defrauding elections would be very difficult, if not virtually impossible. In early 2017, an experiment by Nasdaq and e-Residency, a Japanese platform of electronic citizenship, made a successful experiment using blockchain technology in carrying out an e-voting process for shareholders (Nasdaq 2017).

Blockchain technology could also be used to detect corruption in government circles and limit abuses of power in ways that traditional bookkeeping methods cannot. By allowing journalists and other public interest groups open access to public data on the blockchain, human rights could be a major beneficiary. The data could be used as irrefutable evidence to expose criminal practices within the state, and hence protect vulnerable community members.

It is important to note that the degree and implementation of transparency may vary from one blockchain to another. In permissioned blockchains, it is possible to keep parts of the data transparent to some nodes while keeping the rest hidden. This can be crucially important for some businesses and services that rely on confidentiality in transaction data. The Hyperledger Fabric[9] is one of the blockchain platforms that allows the creation of permissioned blockchains in which the nodes can be configured to have different roles and permission settings. Such platforms provide the possibility of covering a wide variety of blockchain applications with varying degrees and levels of transparency.

From transparency to accountability

When it comes to accountability, smart contracts can take the features of blockchain technology to the next level. Smart-contract-based projects have been implemented in the fields of real estate, financial services, predictive markets, privacy and identity, insurance, entertainment and infrastructure (Cummings 2016).

Along with other supply-chain-focused use cases, blockchains could also help fight the spread of counterfeit drugs. To prevent pharmaceutical fraud from victimising millions of unsuspecting victims, the technology could inform the relevant authorities when counterfeit medical products are detected at selling points at any pharmacy that has the smart-contract-enabled software in place (Bajpai 2016). In essence, the blockchain would provide a single, un-tampered picture of all transactions happening in typically complex supply chains (including multiple suppliers, vendors and distributors).

Similarly, taking into account privacy considerations, health records of patients kept on the blockchain could eliminate potential misdiagnosis and identify forms of malpractice by medical doctors while streamlining the treatment process across medical institutions and practitioners (Molteni 2017).

It is also easy to imagine a world where detection of corruption at a particular level could trigger the suspension of a financial transaction or the blocking of a particular account. The fact that blockchains are immutable makes it possible to preserve evidence and hold corrupt individuals to account in a court of law.

In a very long-term and maybe hyperbolic vision of the true potential of blockchain technology, one could go so far as to imagine a world where governments and various other entities have their full legislations enforced automatically via smart contracts. This could be possible due to the rapid developments in artificial intelligence, machine learning, cloud storage, bandwidth and processing power, as well as the proliferation of billions of devices in the Internet of Things (IoT) communicating among themselves securely and automating many traditionally manual processes (Huckle et al. 2016).

The limits of anonymity

People often think that Bitcoin or other blockchain-based applications are anonymous, but as we have seen from many examples already covered in this article, this is not always the case.

Even in permissionless blockchains that normally do not require the provision of any ID or personal information to create a wallet and make transactions, personal information might be exposed when, for example, the owner of cryptocurrency needs to dispense it for a service or a product. Due to legal and practical requirements, providing personal information to those wishing to buy services or products with cryptocurrencies is often necessary. At that point, the anonymity of the person involved would be jeopardised.

Even in the case of ATM machines that exist in several countries as a way to easily purchase Bitcoin using cash or credit cards, there are some precautionary measures taken by the ATM operators to identify the person using the service. In the case of an ATM machine in Geneva, for example, a Swiss mobile phone number along with personal information are required to buy Bitcoins (Guélat 2016). At that point, the wallet in which the Bitcoins are stored will be linked in the service provider's database to that particular person. Additionally, CCTV cameras are expected to be installed at ATMs for security purposes.

The main exception to the lack of anonymity may be in the underground criminal world, often referred to as the darknet, where transactions can take place without linking personal information to the individual. This explains why the WannaCry ransomware hackers demanded payments by Bitcoin (Symantec 2017). Nonetheless, the addresses of those hackers can be tracked using any Bitcoin block explorer, which may lead to the criminals when those Bitcoins are used (Tech Wire Asia 2017).

New efficiencies and risks of fragmentation

During times of humanitarian disasters or military conflicts, financial aid to buy medication and other urgently needed supplies often takes too long to reach the victims. Delays caused by bureaucracy, paperwork or political barriers can potentially lead to irreversible loss of property, injuries and even death. But by using smart-contract-enabled blockchain technology, remittances can be sent automatically in a pre-programmed fashion. This could also be used to help activists receive emergency funds through a rapid response smart contract. An instantaneous trigger of a transaction to send an emergency fund anywhere around the world is one major advantage that blockchains could provide, and thereby contribute to humanitarian causes.

While the remittance of instant funds is a straightforward process, there are several other use cases that could utilise the efficiency of blockchain technology, for example carrying out nationwide elections that are fraud resistant and can return prompt, verifiable results without significant delays. This is possible because of the way data is stored and optimised to ensure records are kept intact and in order, consistent across nodes without the need for any extra actions or privileges.

As mentioned earlier, redress mechanisms in response to abuses tend to be slow, influenced by political agendas and generally not accessible to poor and uneducated people. While legal interpretation might still be needed in many cases, blockchain could be a more efficient way to track abuses and match them with applicable law.

Fragmentation and limited liquidity

Yet, as blockchain technology generates new efficiencies, some challenges have emerged regarding interoperability across distributed systems.

The proliferation of blockchains in a rather hype-driven trend has resulted in fragmentation of this space with none of the blockchains able to communicate with any others. The lack of standards and interoperability within this sector is a major obstacle that prevents the wide adoption of the technology, particularly as each of the blockchains has its own addressing and transaction mechanism. Work has started in this space including with Interledger, an open protocol suite developed under the umbrellas of W3C and IETF – which are open standards development bodies for the web and internet layers – that aim to bring interoperability across different ledgers used for payments.[10]

This challenge plays out clearly when attempting to acquire cryptocurrencies since each of the exchange services is confined to one of a small subset of blockchains. The ability to exchange tokens is currently only possible by exchanging one cryptocurrency with traditional fiat money and then back to the other cryptocurrency. While some services such as ShapeShift[11] are starting to offer limited crypto-to-crypto exchange opportunities for small fees, this enforces the dependency on third-party software as an intermediary, which is contrary to the fundamental benefits of blockchains.

Since those difficulties hinder wider adoption of the technology, it leads to fewer users, which in turn results in lower levels of liquidity and frequent massive swings in price. Price instability driven from sudden surges in demand or rushed sales can have a detrimental effect on the trust of users and investors since currencies are most useful when they

can be exchanged for day-to-day purchases without having to worry too much about price fluctuations (Houser 2017).

Disruption effects

While much of the hopes and discourse around blockchain technology focus on its empowering and efficiency effects, there is also a view that the potential trigger of the next financial crisis could come from the rapidly growing and relatively unchecked and unregulated blockchain-based FinTech industry that has contributed to the rising market cap of cryptocurrencies reaching well over USD 140 billion as of September 2017 (Magnuson 2017).

It is already well established that technology, through computerisation and automation, is resulting in the loss of many occupations that rely on low-skilled labour (Frey and Osborne 2016). One could argue that blockchain technology will drive automation to unprecedented levels, which would inevitably lead to the further elimination of jobs in many new areas such as those relying on intermediary companies. The repercussions of eliminating the need for banks, insurance companies and even giant social media companies, for example, may have enormous economic implications for the employees of those companies. This may have serious negative implications for companies that are unable to quickly adapt to the coming wave of blockchain technologies. This perhaps explains the frantic and rapid adoption of blockchain technologies by major global IT corporations and financial institutions.

History has taught us that it is not possible to prevent automation technologies from replacing jobs. Instead, major changes in educational and training programmes need to be in place to allow the acquirement of the skills needed to develop, use and maintain present and future blockchain-enabled systems that are expected to replace the intermediaries of today.

Conclusion

Blockchain technology, while only in its infancy, offers the promise of a return to some of the earlier spirit of the internet; interactions that are peer-to-peer, by the community, with a strong do-it-yourself culture that does away with the convenience, and downsides, of centralised commercial services.

As we have seen in this article, a few principles of blockchain technology have relevance in several domains that could impact society at large. Transparency, equality and autonomy are a few of the characteristics of blockchain technology that could facilitate progress in areas such as online identity, human trafficking, corruption, fraud, democratic participation and freedom of expression. Beyond the application of blockchains to cryptocurrency, practical use cases have demonstrated the potential to harness code and provide the community with a new architecture that can bring crowdsourced accountability in many domains. Distributed architectures offer a glimpse at a possible future shifting away from commercial communication platforms, where business models are based on the non-transparent monetisation of user data.

This optimistic outlook, fuelled by a set of use cases, puts an important pressure on the blockchain to deliver more and more services in a manner that is better for society.

Yet, blockchain technology remains hampered by a set of challenges and risks that currently prevent it from being more broadly adopted.

Often portrayed as a 'trustless' technology, blockchains actually shift the trust from intermediaries to code and coders. The technology is also not immune to governments stepping in to regulate its use, or to big companies turning the technology into centralised commercial services, potentially raising risks for expression and privacy. Some of the most radical and creative applications of blockchain technology, such as those related to eliminating a large set of intermediaries, would require a change of mindset that goes beyond a simple technological shift and requires long-term commitments to equip future generations with the knowledge and skills needed to remain relevant in what will be an increasingly automated future.

To a large extent, the success of blockchain technology will rely as much on us as users, as a community, as on the technology itself. Technology, after all, is developed for humans by humans:

> Software – like all computer code – is an evolving product of the human mind, and its deployment is vulnerable to human frailties and divergent ideals. (Popper 2016)

At this stage, blockchain technology is very much about potential, and this is why much of this article's content is about start-ups and ideas, some of which may fail. To make its most promising features to empower people a reality, it is important to have all relevant stakeholders understand and shape its evolution. An open mind and a readiness to embrace radical change is key to a broader understanding of the technology and its potential.

It will be a bumpy ride but the blockchain journey has definitely begun and it is moving forward rather rapidly. Whether the journey succeeds will depend on how well the disruptive blockchain technology is utilised and how well-prepared society is to receive its blessings and deal with its curses.

Notes

1. FinTech can be defined as software and other technologies that are used to facilitate and assist in carrying out financial and banking services.
2. Permissioned blockchains, on the other hand, would be restricted to those that have prior permission to use the blockchain. Examples involve private companies, banking systems, regulatory agencies, etc.
3. In the case of Bitcoin, however, a '51% attack' may result in manipulating the public ledger, although this is highly unlikely without the concentrated power of miners. See https://learncryptography.com/cryptocurrency/51-attack.
4. A full description of how proof-of-work functions for Bitcoin can be found in Krawisz (2013).
5. See https://blockstack.org.
6. Websites where people can sell, buy or exchange cryptocurrencies against other digital currencies of fiat money (EUR, USD, etc.)
7. See https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures.
8. Forks occur when a copy of source code from one software package is copied into a new independent software development project, leading to the creation of new and distinct software.
9. See https://hyperledger-fabric.readthedocs.io/en/latest/.
10. See https://interledger.org.
11. See https://shapeshift.io.

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Walid Al-Saqaf is Yemeni, a software developer, an Internet rights advocate and a postdoctoral researcher at Stockholm University with a passion for promoting a strong and open Internet that netizens can use to promote democratisation and free speech.

As a computer engineering undergraduate student in the mid-1990s at the Middle East Technical University in Turkey, Walid designed YemenTimes.com as the first news website in his home country Yemen. In 2007, he launched YemenPortal.net as the first news aggregator and search engine of its kind in the Arab world to provide Internet users with the ability to get a wide spectrum of perspectives from various news sources on Yemen in Arabic and English. When the website was blocked by the Yemeni government in 2008 due to its open platform that allowed dissident voices to be heard, he developed Alkasir website censorship mapping circumvention solution, which was initially used to access YemenPortal.net, but which soon became widely used by Internet users in many states such as Iran, Syria, China and Saudi Arabia to bypass website filtering in those countries.

Featured by CNN, the Guardian, the Huffington Post and other media, Walid's work was particularly useful during the Arab Spring when some authoritarian Arab regimes practised pervasive Internet filtering of news and social media websites. He has also been active in supporting open Internet access and online free speech in developing countries through non-technical means such as advocacy campaigns and training. His efforts have earned him recognition through several awards including a TED 2012 senior fellowship and Örebro University's 2010 Democracy Award.

Walid is also engaged in several initiatives to promote innovation and creativity in technology among the youth as he organised TEDxSanaa 2012 and 2013, founded Sanaa Hub as part of the Global Shapers Community of the World Economic Forum and co-founded and led Yemen's Internet Society Chapter for which he built a robust core team that was able to make ISOC-Yemen one of the most active chapters in the Middle East. Walid's unique position as a scholar based in Sweden as well as a pro-free speech cyber activist and software developer of Arab background have jointly helped him develop a wide a range of skills and expertise to contribute to technical and policy discussions around Internet-related issues on several platforms such as ICANN, RIPE, IGF and the World Wide Web Foundation. This helped him build bridges between developing and developed countries when it comes to addressing key issues that concern Internet users around the world.

Nicolas Seidler is Senior Policy Advisor at the Internet Society. He joined the organisation in February 2010 and currently leads ISOC's work on Internet and Human Rights issues. He also engages in key global Internet governance issues and processes.

Nicolas works with a broad spectrum of international partners, global policy-makers and non-governmental stakeholders on a range of Internet issues. In this role, he contributes to ISOC's engagement with a variety of international and regional organisations such as the ITU, UNESCO, the Human Rights Council or the Council of Europe. He also plays a key role in coordinating the Internet Technical Advisory Committee (ITAC) to the OECD.

Nicolas holds a Master's degree in International Relations from the Graduate Institute of International and Development Studies (Geneva). He also holds a Master's degree in Communication and Media Sciences from the University of Geneva.

Nicolas is based in Geneva, Switzerland.

References

Ali, S. T., D. Clarke, and P. McCorry. 2015. "Bitcoin: Perils of an Unregulated Global P2P Currency." In *Security Protocols XXIII*. Lecture Notes in Computer Science, edited by B. Christianson, P. Švenda, V. Matyáš, J. Malcolm, F. Stajano, and J. Anderson, 9379. Cham: Springer. https://link.springer.com/chapter/10.1007/978-3-319-26096-9_29.

Bajpai, P. 2016. "Blockchain Technology Can Help Reduce the Flow of Counterfeit Drugs." December 14. http://www.nasdaq.com/article/blockchain-technology-can-help-reduce-flow-of-counterfeit-drugs-cm721230.

Barber S., X. Boyen, E. Shi, and E. Uzun. 2012. "Bitter to Better – How to Make Bitcoin a Better Currency." In *Financial Cryptography and Data Security. FC 2012*. Lecture Notes in Computer Science, edited by A. D. Keromytis, 7397. Berlin: Springer. https://link.springer.com/chapter/10.1007/978-3-642-32946-3_29#citeas.

Bindi, T. 2017. "Microsoft and Accenture Develop Blockchain ID System for Refugees." June 20. http://www.zdnet.com/article/microsoft-and-accenture-develop-blockchain-id-system-for-refugees/.

Blockchain Daily News. 2017. "Top 250 Blockchain Companies & Startups." July 6. http://www.blockchaindailynews.com/Top-250-blockchain-companies-startups_a24712.html.

Chaabane, Abdelberi, Pere Manils, and Mohamed Ali Kaafar. 2010. "Digging into Anonymous Traffic: A Deep Analysis of the Tor Anonymizing Network." In *2010 4th International Conference on Network and System Security (NSS)*, IEEE, 167–174.

Clark, J., R. Faris, R. Morrison-Westphal, H. Noman, C. Tilton, and J. Zittrain. 2017. "The Shifting Landscape of Global Internet Censorship." June 29. https://thenetmonitor.org/research/2017-global-internet-censorship#results.

Clarke, I., O. Sandberg, M. Toseland, and V. Verendel. 2010. *Private Communication Through a Network of Trusted Connections: The Dark Freenet*. Vancouver: Network.

Cummings, D. 2016. "Use Cases of Ethereum in Different Sectors 2016." December 15. https://www.ethnews.com/use-cases-of-ethereum-in-different-sectors-2016.

Decker, C., and R. Wattenhofer. 2014. "Bitcoin Transaction Malleability and MtGox." In *Computer Security – ESORICS 2014. ESORICS 2014*. Lecture Notes in Computer Science, edited by M. Kutyłowski and J. Vaidya, 8713. Cham: Springer. https://link.springer.com/chapter/10.1007/978-3-319-11212-1_18.

Desai, V. 2017. "Counting the Uncounted: 1.1 Billion People Without IDs." June 6. https://blogs.worldbank.org/ic4d/counting-invisible-11-billion-people-without-proof-legal-id.

Fairfield, J. 2014. *Smart Contracts, Bitcoin Bots, and Consumer Protection*, 71 Wash. & Lee L. Rev. Online 36. http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3.

Forrest, C. 2016. "Microsoft Believes Blockchain Tech Could Help Fight Human Trafficking, Child Exploitation." May 31. http://www.techrepublic.com/article/microsoft-believes-blockchain-tech-could-help-fight-human-trafficking-child-exploitation/.

Freedom House. 2016. *Freedom on the Net 2016*, November. https://freedomhouse.org/sites/default/files/FOTN_2016_Full_Report.pdf.

Frey, C. B., and M. Osborne. 2016. "The Future of Employment: How Susceptible Are Jobs to Computerisation?" *Technological Forecasting and Social Change* 114 (2017): 254–280. http://www.sciencedirect.com/science/article/pii/S0040162516302244.

Gadnis, A., and K. Cronen. 2017. "Unchaining Modern-Day Slavery: Blockchain Offers a Real Solution." January 24. http://blog.chemonics.com/unchaining-modern-day-slavery%3A-blockchain-offers-a-real-solution.

Goodwin, T. 2016. "The Battle is for the Customer Interface." *TechCrunch*. https://techcrunch.com/2015/03/03/in-the-age-of-disintermediation-the-battle-is-all-for-the-customer-interface/.

Greenemeier, L. 2011. "Cops Enlist Data-Tracking Software in the Fight Against Child Predators." *Scientific American*, November. https://www.scientificamerican.com/article/software-against-p2p-bittorrent-abuse/.

Guélat, J. 2016. "Switzerland: How the World's Densest Bitcoin ATM Network is Doing." December 15. https://news.bitcoin.com/switzerland-densest-bitcoin-atm-network/.

Hardy, Q. 2016. "The Web's Creator Looks to Reinvent It." June 7. https://www.nytimes.com/2016/06/08/technology/the-webs-creator-looks-to-reinvent-it.html.

Houser, K. 2017. "In the Age of Blockchain, Crypto Has a Major Problem." July 10. https://futurism.com/the-age-of-blockchain-crypto-has-a-major-problem/.

Huckle, S., R. Bhattacharya, M. White, and N. Beloff. 2016. "Internet of Things, Blockchain and Shared Economy Applications." http://www.sciencedirect.com/science/article/pii/S1877050916322190.

Hunnicutt, T., and G. Chavez-Dreyfuss. 2017. "U.S. Regulators Reject Bitcoin-ETF, Digital Currency Plunges." March 10. http://uk.reuters.com/article/us-bitcoin-etf-idUKKBN16H2NU.

IBM Corporation. 2017. *Building Trust in Government: Exploring the Potential of Blockchains*. January. https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=GBE03801USEN.

Ito, J., N. Narula, and R. Ali. 2017. "The Blockchain Will Do to the Financial System What the Internet Did to Media." March 09. https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media.
Joshi, P. 2017. "How Blockchain Can Revolutionise the Music and Media Industries." https://yourstory.com/2017/10/how-blockchain-can-revolutionise-the-music-and-media-industries/.
Krawisz, D. 2013. "The Proof-of-Work Concept." June 24. http://nakamotoinstitute.org/mempool/the-proof-of-work-concept/.
Landau, S. 2013. "Making Sense From Snowden: What's Significant in the NSA Surveillance Revelations." *IEEE Security & Privacy* 11 (4): 54–63.
Leiner, B. M., V. G. Cerf, D. D. Clark, R. E. Kahn, L. Kleinrock, D. C. Lynch, J. Postel, L. G. Roberts, and S. Wolff. 2009. "A Brief History of the Internet." *ACM SIGCOMM Computer Communication Review* 39 (5): 22–31.
MacKinnon, R. 2017. "The Internet Has a Dark Side. We Need a Plan for Taming it." *World Economic Forum*. January 16. https://www.weforum.org/agenda/2017/01/internet-freedom-censorship-regulation.
Magnuson, W. 2017. "The Next Crisis Will Start in Silicon Valley." September 18. https://www.bloomberg.com/view/articles/2017-09-18/the-next-crisis-will-start-in-silicon-valley.
Marsden, P. 2010. *Social Commerce: Monetizing Social media*. London: GRIN Verlag. https://digitalintelligencetoday.com/documents/Syzygy_2010.pdf.
Microsoft. n.d. "What is Blockchain?" https://azure.microsoft.com/en-us/solutions/blockchain/.
Miller, R. 2017. "The Promise of Managing Identity on the Blockchain." September 10. https://techcrunch.com/2017/09/10/the-promise-of-managing-identity-on-the-blockchain/.
Mlot, S. 2015. "Global Broadband Access Still Lacking." September 23. http://uk.pcmag.com/internet-products/71341/news/global-broadband-access-still-lacking.
Molteni, M. 2017. "Moving Patient Data Is Messy, but Blockchain Is Here to Help." January 2. https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/.
Morris, D. 2016. "Blockchain-Based Venture Capital Fund Hacked for $60 Million." June 18. Fortune. http://fortune.com/2016/06/18/blockchain-vc-fund-hacked/.
Nasdaq. 2017. "Is Blockchain the Answer to e-Voting? Nasdaq Believes So." January 23. http://business.nasdaq.com/marketinsite/2017/Is-Blockchain-the-Answer-to-E-voting-Nasdaq-Believes-So.html.
O'Neill, P. H. 2017. "Tor's Ex-Director: 'The Criminal Use of Tor has Become Overwhelming'". May 22. https://www.cyberscoop.com/tor-dark-web-andrew-lewman-securedrop/.
Paul, I. 2012. "Update: LinkedIn Confirms Account Passwords Hacked." *PC World*, 6. https://www.pcworld.com/article/257045/security/6-5m-linkedin-passwords-posted-online-after-apparent-hack.html.
Peck, M. 2015. "The Future of the Web Looks a lot Like the Bitcoin Blockchain." July 1. http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin.
Pilkington, M. 2016. "Blockchain Technology: Principles and Applications." In *Handbook of Research on Digital Transformations*, edited by F. Xavier Olleros and Majlinda Zhegu, 225–253. Cheltenham: Edward Elgar.
Popper, N. 2016. "A Bitcoin Believer's Crisis of Faith." *New York Times*, January 14. https://www.nytimes.com/2016/01/17/business/dealbook/the-bitcoin-believer-who-gave-up.html.
Provenance. 2016. "From Shore to Plate: Tracking Tuna on the Blockchain." July 15. https://www.provenance.org/tracking-tuna-on-the-blockchain.
Reiff, N. 2017. "Second Major Ethereum Hack in a Week Leads to $34 Million Theft." July 24. http://www.investopedia.com/news/second-major-ethereum-hack-week-leads-34-million-theft/.
Riddlesden, D., and A. Singleton. 2014. Broadband Speed Equity: A New Digital Divide? August. http://www.sciencedirect.com/science/article/pii/S0143622814000782.
Rizzo, P. 2016. "Sweden Tests Blockchain Smart Contracts for Land Registry." June 16. http://www.coindesk.com/sweden-blockchain-smart-contracts-land-registry/.
Internet Society, Robachevsky, A. 2014. "The Danger of the New Internet Choke Points." February 18. https://www.internetsociety.org/blog/2014/02/the-danger-of-the-new-internet-choke-points/.
Scalability. n.d. In *Bitcoin wiki*. 11 October, 2017, https://en.bitcoin.it/wiki/Scalability.

Schiller, B. 2016. "Can Crowdsourced Jury Trials on the Blockchain Deliver Justice for All?" August 6. https://www.fastcompany.com/3060524/can-crowdsourced-jury-trials-on-the-blockchain-deliver-justice-for-all.

Schneier, B. 2013. "The Battle for Power on the Internet." *The Atlantic*, October 24. https://www.theatlantic.com/technology/archive/2013/10/the-battle-for-power-on-the-internet/280824/.

SecureKey. 2017. "SecureKey and the Digital ID and Authentication Council of Canada Awarded Grant to Create Privacy Enhancing Cloud Ecosystem." February 12. http://securekey.com/press-releases/securekey-digital-id-authentication-council-canada-awarded-grant-create-privacy-enhancing-cloud-ecosystem/.

Stokes, R. 2012. "Virtual Money Laundering: The Case of Bitcoin and the Linden Dollar." *Information & Communications Technology Law* 21 (3): 221–236. December. http://www.tandfonline.com/doi/pdf/10.1080/13600834.2012.744225.

Symantec Security Response. 2017. "What You Need to Know About the Wannacry Ransomware." May 12. https://www.symantec.com/connect/blogs/what-you-need-know-about-wannacry-ransomware.

Tapscott, D., and A. Tapscott. 2016. *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*. New York: Portfolio / Penguin.

Tech Wire Asia. 2017. "Ransomware Bitcoins Might Lead Authorities to Cybercriminals." May 19. http://techwireasia.com/2017/05/ransomware-bitcoins-might-lead-authorities-cybercriminals/#m7j6×8vVkUWjdmfe.99.

Torpey, K. 2014. "Bitcoin and Tax Evasion: Are the Possibilities Overstated?" October 28. http://insidebitcoins.com/news/bitcoin-and-tax-evasion-are-the-possibilities-overstated/25805

Uslaner, E. 2010. "Trust and the Economic Crisis of 2008." July 21. https://link.springer.com/article/10.1057/crr.2010.8.

Vincents, Okechukwu Benjamin. 2007. "When Rights Clash Online: The Tracking of P2P Copyright Infringements vs. the EC Personal Data Directive." *International Journal of law and Information Technology* 16 (3): 270–296.