GODINA 2, BROJ 2 (2019)

ISSN 2566 - 4514

VISOKA ŠKOLA
"INTERNACIONALNA POSLOVNO-INFORMACIONA AKADEMIJA" TUZLA

ZBORNIK RADOVA

Book of Proceedings

2. MEĐUNARODNA NAUČNA KONFERENCIJA O DIGITALNOJ EKONOMIJI DIEC 2019

2nd INTERNATIONAL SCIENTIFIC CONFERENCE ON DIGITAL ECONOMY DIEC 2019

TUZLA, APRIL 2019.

Izdavač / Publisher

Internacionalna poslovno - informaciona akademija

ISSN 2566 - 4514 (Print)
ISSN 2566 - 4522 (Online)

SADRŽAJ

Domagoj Sajter, Associate Professor[1]

Keynote paper

UNBLOCKING BLOCKCHAIN POTENTIALS

Abstract

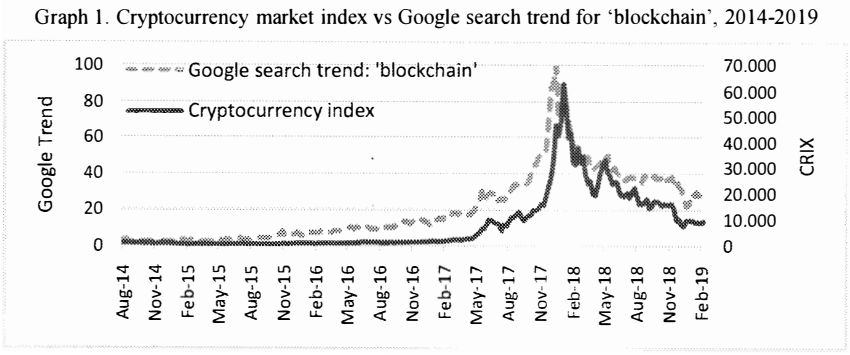
The goal of this paper is to research and present the current developments and future prospects of the blockchain technology throughout economy. Since it was introduced within the Bitcoin, blockchain became a buzzword repeated everywhere, often a proposition of panacea for the global problems. However, in the meantime the world of cryptocurrencies experienced a typical boom-bust cycle which many left wandering if blockchain technology was anything more than a hype. This paper aims to establish a brief overview of the possible implementations of distributed ledger (blockchain) technology in the context of the fast growing information society: blockchain may be the essential tool in the economy based upon Internet-of-things, new mobile connectivity standards and big(ger) data.

Keywords: *Blockchain, distributed ledger, information society*

1. Introduction

Blockchain is among the top buzzwords of the economy in the past couple of years. Worldwide interest for the term 'blockchain' on the Google search engine strongly correlates with the cryptocurrency index CRIX, which is not surprising given the stellar growth of the Bitcoin, Ether and other major cryptocurrencies (Graph 1). The impressive progression of cryptocurrencies during 2017 drew attention for the technology and architecture behind them and fuelled interest to the innovative concept of writing, storing and sharing data.

Graph 1. Cryptocurrency market index vs Google search trend for 'blockchain', 2014-2019



Notes:Google Trends line represents search interest for the term 'blockchain' relative to the highest point on the chart worldwide during the last five years (2014-2019); a value of 100 is the peak popularity for the term, while 50 means that the term is half as popular.

The CRIX is a cryptocurrency market index where the number of constituents is determined by analysing Akaike and Bayesian information criterions for multiple alternatives of the index, and where each cryptocurrency is weighted with its market capitalization.

Sources: Google Trends and CRIX.de

Those who reflect on the blockchain with (some) knowledge of its peculiarities argue in favour of its potentials; many others who are unacquainted with hashes, nonces, public-key cryptography and

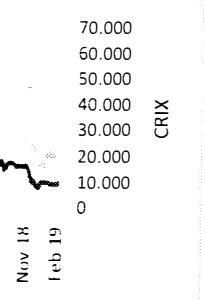
[1]Associate Professor at Faculty of Economics in Osijek, Croatia, e-mail: sajter@efos.hr, phone: +385 91 2244 102; web: http://www.efos.unios.hr/sajter

IALS

ments and future prospects of
roduced within the Bitcoin,
tion of panacea for the global
perienced a typical boom-bust
hing more than a hype. This
tations of distributed ledger
n society: blockchain may be
nobile connectivity standards

couple of years. Worldwide
strongly correlates with the
growth of the Bitcoin, Ether
on of cryptocurrencies during
n and fuelled interest to the

ckchain', 2014-2019



' relative to the highest point on
popularity for the term, while 50

ents is determined by analysing
d where each cryptocurrency is

culiarities argue in favour of
ublic-key cryptography and

: phone: +385 91 2244 102;

other similar "oddities" believe it to be just another passing fad, ripe for oblivion together with the cryptocurrencies' spectacular crash of 2018. It is a trigger-word often inciting emotive reactions, especially with those that gained and/or lost considerable amounts of money with cryptocurrencies.

Regardless of the stance towards the crypto-universe it is only natural to be fascinated by the spectacle of the 01/2017 - 01/2019 crypto boom-bust cycle. What remains, if anything? Eurostat[2] and Fred[3] were queried in February 2019; both sides of the Atlantic had no available data on the keyword 'blockchain'. Is it that the new technology has not yet settled and supplied enough documented statistics, or is digital static all that' s left?

The purpose of this paper is to present the novelty of blockchain technology and to discuss both its present merits and its faults from a non-attached, independent standpoint, away from the emotive reactions of crypto-evangelists and Bitcoin obituaries' writers[4]. Will it really change everything or will it go down in history? As always with such radically opposing and borderline alternatives the road is somewhere in the middle – of course – but to which border is it closer? This paper chooses its risks wisely and halts at the epistemological frontier of knowledge about the society in the future.

After the introduction, the next – second – chapter defines and explains the main pillars of blockchain and the disambiguation between blockchain and distributed ledger, as well as the blockchain as a trust-building mechanism. The third chapter sets the stage for possible implementations and developments of the blockchain technology by providing wider context of the information society we live in, together with the new developments of the information communication technology. Finally, fourth chapter concludes.

2. Blockchain and trust

Deloitte surveyed 1053 respondents knowledgeable of blockchain across seven countries globally, from ten industries, and two thirds of them said that their company will spend more than 1 million USD investing in the blockchain technology during the next year (Deloitte, 2018, p. 18). This is an indication of the non-triviality of the momentum cryptocurrencies have made.

On the other hand, it is sometimes difficult to assess whether the investment into blockchain is a "true" venture into new technology or a covert marketing expenditure trying to implant an image of a corporation willing to explore cutting-edge ideas. This adds to list of reasons why it is important to understand what blockchain is and what it proposes.

Oxford Dictionary defines blockchain as "*a system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network*" (Oxford Dictionaries, 2019). Acknowledging that every definition is always a trade-off between brevity and accuracy, the previous explanation provides only indications of what blockchain is, does, and could be. The most cited article on both Web of Science and Scopus databases regarding blockchain (199 and 324 citations in February 2019, respectively) portrays it as "*a distributed data structure that is replicated and shared among the members of a network*"; "*a log whose records are batched into timestamped blocks*" (Christidis & Devetsikiotis, 2016, p. 2293).

A comprehensive description of blockchain includes (at least) four elements: it defines it as (1) a data structure, (2) an algorithm, (3) a collection of technologies, and (4) a generalization of distributed peer-to-peer systems with a common application area (Drescher, 2017, p. 33).

Data structure relates to the concept of arrangement of data within entities named as *blocks*, whereas blocks are connected between themselves in an ordered sequence (*chain*). Linking blocks

[2] https://ec.europa.eu/eurostat/
[3] https://fred.stlouisfed.org
[4] Reference to https://99bitcoins.com/category/bitcoin-obituaries/.

is done via cryptography which ensures immutability of the data within. In simple terms, cryptography is here used primarily for two purposes: (a) to "lock" the data within the blocks (to make the data unchangeable and/or private, hidden to outsiders), and (b) for trustworthy and reliable assignment of identities behind the data (digital signatures). The data of the first blockchain – Bitcoin – consists of transactions, where one party sends valuable information (which crypto-proponents equate to money[5]) to the other, through internet, where every malevolent person could alter or steal the contents of that transaction.

Having seen that the Bitcoin system functions the idea evolved with the notion that the data within blocks can be something other than transactions – whichever "valuable information" (Dujak & Sajter, 2019, p. 26) that may be. The data structure is also described as a *ledger*; 'distributed ledger technology' is often used as a synonym to 'blockchain technology', especially with those who seek to distance themselves from the cryptocurrency subculture and its worldviews[6].

Closely related to the data structure, an 'algorithm' refers to an unambiguous sequence of commands, which as an output frequently builds up aforementioned data structures – blocks. Developing and maintaining blockchain requires a common set of rules which users abide by; these rules are encoded in the algorithm which is often referred to as "the law" (Lessig, 2000).

Combining data structure with the algorithm and underlying cryptographic models broadens the concept of blockchain and extends it to a collection of technologies with similar traits.

Lastly, a blockchain can be viewed as a generalization of distributed, decentralized systems with a [illegible] application. The keywords here are distribution and decentralization: in a globalized economy founded upon the information flows one of the vital actual questions is how to reach a consensus without a common authority. Internet is by itself a global network without a main, central [illegible] continental or even regional core points. It is a collection of dispersed nodes, open for communication, which makes them vulnerable to all kinds of attacks. Conceiving both a data structure and a protocol for sending and receiving, storing and changing valuable information on such a flat, level playing field is an innovation worthy of its "buzz".

Given that the main pillar of the blockchain is its ability to attain agreement on a peer-to-peer level much of the confusion and controversy regarding the notion of blockchain stems from abandonment of aforementioned proposition, a proposition which was central to crypto-enthusiasts. Evolution of blockchain lead it to the crossroad at which the basic, rudimentary typology emerged: blockchains can be public or private (Bashir, 2018).

Public blockchains are "classic, traditional" systems open to everyone, where no permission needs to be given from the existing participants to the admission of the newcomer; he only needs to adhere to the established protocol in order to join. This also means that the identity is irrelevant since anyone can participate –screening individual traits is pointless as there are no gatekeepers. The only prerequisite is adherence to "the law" – the software code within the protocol.

Private blockchains are the opposite: they are permissioned (only selected entities can be members) which means that a blockchain only enhances certain pre-existing level of trust. As such, private

[5] One can notice a reluctance in calling Bitcoin "money". This is because even though it is an innovative and promising concept it only anecdotally fulfils three main functions of money: Bitcoin is not a widely accepted medium of exchange, nor it is a unit of account, and it certainly is not a stable depository of value over time. This could however change in the future, but that would require large scale adoption and a redesign of current payment systems.

[6] The origins of Bitcoin are embedded in the cypherpunk movement, which could be correlated to cyber-anarchy (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016, p. 247). One of the predecessors of Bitcoin is *b-money*, concept developed by Wei Dai in 1998. Dai starts his essay with the following statements: "*I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary.*" (Dai, 1998) If we would maintain that ideas and beliefs are the essential drivers of human actions, if the cryptocurrencies were to become mainstream the ideas and beliefs behind them would also need to become mainstream. With cypherpunk this is certainly not the case.

blockchains lack the fun
the very notion of priva
widespread. Without de
private blockchain, beca
shared database, saved
logins and changes to it.

There is also a third p
permissioned and permi
proofing, upgrading prot
can be given to certain g
its potential.

The essential innovation
"glue" that holds the e
anything, but not trust[8].
basic proficiency in ma
calculus is easily prova
3325548 equals 749840
where the following prin
it takes much more time
to find which two sever
Cryptography uses powe
advance, but are practica
in the context of maint
securely over unsafe com

However, "trust" here ha
the context of blockchai
variables, parameters an
world trust also has an
indefinite set of variabl
algorithm) will be equal
also forward looking: it
future consequences of t
which is only party simu
is with is (somewhat sim
data locked/signed with t
that the blockchain syste
intermediaries will surviv
provide service, that regu
the civilization could s
edger technology.

For instance, public could be
proofing. and group C could gr
an entrepreneur somehow
previous state. Money can mer
change beliefs.
Scheier provides a vivid exa
[1 J to 10^-7 joules]. *If all o*
be cycled through all of
maximums that thermodyna
infeasible until compute
Scheier. 2015, pp. 157–158

ta within. In simple terms, he data within the blocks (to) for trustworthy and reliable ata of the first blockchain – information (which crypto- ery malevolent person could

he notion that the data within able information" (Dujak & s a *ledger*; 'distributed ledger pecially with those who seek dviews[6].

unambiguous sequence of ed data structures – blocks. s which users abide by; these " (Lessig, 2000).

graphic models broadens the h similar traits.

decentralized systems with a ntralization: in a globalized questions is how to reach a twork without a main, central of dispersed nodes, open for ks. Conceiving both a data ging valuable information on

ement on a peer-to-peer level ain stems from abandonment pto-enthusiasts. Evolution of ology emerged: blockchains

where no permission needs newcomer: he only needs to hat the identity is irrelevant as there are no gatekeepers. hin the protocol.

ted entities can be members) el of trust. As such, private

it is an innovative and promising ely accepted medium of exchange, This could however change in nt systems.
rrelated to cyber-anarchy sers of Bitcoin is *b-money*, nts *"I am fascinated by Tim anarchy". in a crypto-anarchy* h unnecessary." (Dai, 1998) If the cryptocurrencies were to nstream. With cypherpunk this is

blockchains lack the fundamental novelty of its Bitcoin predecessor, which is why many oppose to the very notion of private blockchain and why the phrase "distributed ledger technology" became widespread. Without decentralization it becomes difficult to find the unique selling point of a private blockchain, because a simple (and free) Google Sheet (e.g.) does almost all the work: it is a shared database, saved online, with dedicated passwords for viewing and editing, recording all logins and changes to it.

There is also a third path: somewhere in between. A blockchain-based system can have both permissioned and permissionless sub-zones where different permissions (for reading/writing data, proofing, upgrading protocol, as well as granting and revoking authorities for these activities, etc.) can be given to certain groups, even to the public[7]. This is where presently blockchain hold most of its potential.

The essential innovation of the blockchain technology is its proclaimed ability to generate the "glue" that holds the economy together: trust. In a capitalist economy money can buy almost anything, but not trust[8]. The core element of trust building within any blockchain is math; at the basic proficiency in math language 2254789 x 3325548 either is or isn't 7498409049372. The calculus is easily provable, and after proofing "trust" is established that indeed 2254789 times 3325548 equals 7498409049372. Cryptography could be regarded as a branch of mathematics where the following principle is heavily used: it is very easy to determine as true that $a \times b = c$, but it takes much more time and effort to start backwards, with the product (c = 7498409049372), and to find which two seven-digit numbers (a, b) were multiplied in order to provide that solution. Cryptography uses powerful functions which are very easy to prove if one has the information in advance, but are practically impossible to solve backwards[9]. This property allows them to be used in the context of maintain data integrity, proofing ownership over data and exchanging data securely over unsafe communication channels, which are crucial in the internet today.

However, "trust" here has only one necessary component because it is only ex-post maintained: in the context of blockchain it merely declares that the outcome of an algorithm with known set of variables, parameters and rules is true or false, which hardly qualifies as trust. In the non-virtual world trust also has an ex-ante notion: it is a belief that under unknown future circumstances (indefinite set of variables and parameters, but known rules) the outcome of a series of events (algorithm) will be equal to anticipated. The trust as a prerequisite for the functioning economy is also forward looking; it is a consciously accepted risk (under condition of uncertainty) that the future consequences of the risk acceptance will not be disappointing. It is a leap into unknown which is only party simulated in the crypto domain, where the sole trust cryptography can provide us with is (somewhat simplified) that in the future only the holder of the right keys can handle the data locked/signed with that keys. However, the trust is needed beyond that: one needs to believe that the blockchain system will persist and be active, that developers will maintain the code, that intermediaries will survive (presuming that the user is not skilled as a blockchain developer) and provide service, that regulation will not change radically, etc. Hence, the core assumption that trust in the civilization could somehow be coded into software is only partially established with the novel ledger technology.

[7] For instance, public could be given right to read the data, group A could write to database, group B could do the proofing, and group C could give subsections of both groupa A and B right to update the protocol.

[8] If an entrepreneur somehow cheats its business partner no money in the world can restore their relationship to its previous state. Money can mend superficial relationship and be a component of the restoration, but money alone cannot change beliefs.

[9] Schneier provides a vivid example: „*A typical supernova releases something like 10^51 ergs* [erg is an unit of energy equal to 10^−7 joules]. *If all of this energy could be channelled into a single orgy of computation, a 219-bit counter could be cycled through all of its states. These numbers have nothing to do with the technology of the devices; they are the maximums that thermodynamics will allow. And they strongly imply that brute-force attacks against 256-bit keys will be infeasible until computers are built from something other than matter and occupy something other than space.*" (Schneier, 2015, pp. 157–158)

3. Information society and leaps in the development of ICT

In 2018 worldwide each minute, every day, approximately 160 million of emails are sent, 13 million SMS (text) messages are delivered, and Google conducts 3,9 millions of searches; by 2020 it's estimated that for every person on earth 1,7 MB of data will be created every second (Domo Inc., 2018). Handling the enormous and growing amounts of data will require novel systems, and blockchain stands here as a potential framework – a blueprint for the future data management technologies.

It could be argued that people created vast amounts of data since the beginning of civilization, but that data was not (for the most part) stored anywhere and it was lost either immediately, or over time. Nowadays Wi-Fi passwords are stored even in lightbulbs (see Table 1.), and people leave digital traces in whatever they do and wherever they go. Most of the digital services regarded as "free" (because they are not paid with money directly; e.g. browsing the web, e-mail communication, social networks, etc.) are funded indirectly by the data we leave behind while using these services. Even though the data created could be seen as merely noise, powerful AI systems can detect patterns within, which makes them potentially valuable. Since almost no one actually reads the contracts we sign when we register for these services and that they are in fact unreadable (Benoliel & Becher, 2019), it shouldn't come as a surprise that our private data gets leaked, sold and resold, and used in ways we never could foresee.

With the purpose of giving illustration to the previous statements, a miniature ad-hoc "research" has been performed. News was collected from well-known and widely used internet outlets regarding issues of consumer privacy. The extent of the research spans over three months (from the beginning of November 2018 to end of January 2019); 26 articles during that period were found which expose various malfeasances with user data (Table 1.). Many blockchain enthusiasts intend to take back control of both the underlying data and the systems which create and manage that data.The processes of data creation and high-speed communication are expected to escalate to a new level. Among others, two noticeable (and intertwined) advancements are anticipated. The one is the proliferation of a new category of data creators in the realm of internet-of-things – devices and objects packed with sensors, cameras, microphones, machine learning / artificial intelligence software, etc., connected to internet and communicating between themselves. The ability to collect real-time data could provide businesses and consumers with a number of benefits, allowing automation of processes, rising productivity and enhancing customer service. The second is the new standard of mobile communication which will serve as a highway for distribution of all the new (and "old") data. Fifth generation of mobile infrastructure (5G), expected to be perfected in 2020, will expectedly provide a massive leap in not only speed, but also capacity, cost reduction, and traffic. Expectations are very high and even if the providers under-deliver the change could still be substantial. These leaps will most likely indicate a new era of ICT and data management.

However, one of the difficult tasks will be to provide proper levels of security and privacy: creating and sharing all that data could easily become disturbing if confidentiality controls were not put in place. One of the main contributions of Bitcoin and blockchain in general is in directing attention to powerful cryptographic tools which can protect both privacy and security – values which are in high demand lately:

"*The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data.*[...] [T]*rusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger.*" (Zyskind, Nathan, & Pentland, 2015, p. 180)

Farsighted but concrete projects such as Hyperledger, IBM's Blockchain World Wire, Microsoft's Azure Blockchain Workbench, Alibaba Cloud's Blockchain as a Service. Amazon's Quantum

Ledger Database, JP M
could be here to stay, reg

Table 1. N

Publisher of the news*	Sh
Washington Journal of Law, Tech and Arts	ht
Business Insider	ht
Financial Times	ht
New York Times	ht
Techcrunch	ht
35th Chaos Communication Congress	ht
Ars Technica	ht
The Verge	ht
Wired	ht b
Business Insider	ht m
Deutsche Welle	ht
Techcrunch	ht
Medium	ht
Medium	ht
The Intercept	ht
Business Insider	ht
Search Engine Journal	ht
Bruce Schneier	ht
Wired	ht
Fair	ht
Motherboard	ht s
Boing Boing	ht
Bloomberg	ht
Business Insider	ht
Bleeping Computer	ht
Techcrunch	ht

News published during the t

4. Conclusion

The concept of blockcha
with the aim of increasi
tool with whom all nail
delivering babies (Awod

An example: a company tha
price Rapier. 2018).

illion of emails are sent, 13
millions of searches; by 2020
created every second (Domo
ll require novel systems, and
the future data management

beginning of civilization, but
t either immediately, or over
Table 1.), and people leave
e digital services regarded as
browsing the web, e-mail
we leave behind while using
noise, powerful AI systems
Since almost no one actually
at they are in fact unreadable
rivate data gets leaked, sold

niature ad-hoc "research" has
ed internet outlets regarding
months (from the beginning
od were found which expose
thusiasts intend to take back
and manage that data.The
d to escalate to a new level.
anticipated. The one is the
rnet-of-things – devices and
ning artificial intelligence
selves. The ability to collect
mber of benefits, allowing
rvice. The second is the new
r distribution of all the new
ted to be perfected in 2020,
apacity, cost reduction, and
ver the change could still be
lata management.

ecurity and privacy: creating
lity controls were not put in
al is in directing attention to
y – values which are in high

ity breaches compromising
parties collect and control
outing is possible using a
skind, Nathan, & Pentland,

in World Wire, Microsoft's
rvice, Amazon's Quantum

Ledger Database, JP Morgan's Coin – among many others – signal that blockchain technology could be here to stay, regardless of the cryptocurrency haze.

Table 1. Malfeasances with user data: online news from Nov-2018 to Feb-2019

Publisher of the news*	Shortened link to the news	"Perpetrator/-s"	Deed
Washington Journal of Law, Tech and Arts	tinyurl.com/yxqrjnul	Amazon	Consumer generated mass surveillance
Business Insider	tinyurl.com/y3be8jk6	Amazon	Spying/tracking users
Financial Times	tinyurl.com/y2yzzh2n	At least 34 apps (games, etc.)	Selling user data to Facebook
New York Times	tinyurl.com/y7lry8rw	At least 75 companies	Spying/tracking users
Techcrunch	tinyurl.com/y9h3ky78	Facebook	Spying/tracking users
35th Chaos Communication Congress	tinyurl.com/y3ja6w83	Facebook	Tracking and selling user data even if user doesn't have FB account or app
Ars Technica	tinyurl.com/y3yby6ya	Facebook	"Knowingly violated" privacy laws
The Verge	tinyurl.com/yckq85tt	Facebook	Spying/tracking users
Wired	tinyurl.com/y7o9muqb	Facebook, Instagram, WhatsApp, Messenger	Sharing user data
Business Insider	tinyurl.com/y7e9gbcm	Google	Creating "bubbles" by filtering search results
Deutsche Welle	tinyurl.com/yyazassz	Google	Privacy breach
Techcrunch	tinyurl.com/yaopxlop	Google	Spying/tracking users
Medium	tinyurl.com/ydfmnbpe	Google	Spying/tracking users
Medium	tinyurl.com/yyjwzjh7	Google	Spying/tracking users
The Intercept	tinyurl.com/yagqxlh7	Google	Spying/tracking users
Business Insider	tinyurl.com/y3jb37ac	Google	Secretly putting microphones in devices
Search Engine Journal	tinyurl.com/y4uayhns	Google, Facebook, Twitter	Disrespecting the "Do Not Track" setting on web browsers
Bruce Schneier	tinyurl.com/y8yy9eh9	Government/-s	Placing surveillance cameras in streetlights
Wired	tinyurl.com/y7r24mel	Governments	Spying/tracking citizens
Fair	tinyurl.com/yye47urs	Governments	Potential misuse of face recognition
Motherboard	tinyurl.com/ya25y9wx	Hundreds of free apps	Tracking and selling user data
Boing Boing	tinyurl.com/yadybxyy	Lifx	Passwords saved insecurely (in a lightbulb)
Bloomberg	tinyurl.com/y9jzrjmf	Private DNA testing company	Leaking DNA data to FBI
Business Insider	tinyurl.com/ybjldmrg	Smart TVs	Tracking and selling user data
Bleeping Computer	tinyurl.com/y49o9jr5	Thousands of apps	Violating policies
Techcrunch	tinyurl.com/ycr4m3o5	Unknown	24 million financial and banking documents published online

**News published during the three month period from the beginning of November 2018 to end of January 2019*

Source: Author

4. Conclusion

The concept of blockchain seems to be an interest-inciting idea often thrown around ostentatiously with the aim of increasing brand and or company valuation[10]. It is also frequently perceived as a tool with whom all nails could be hammered: dealing with issues from corruption in Africa to delivering babies (Awodipe, 2019).

[10] An example: a company that sells ice tea renamed to "Long Blockchain" which was enough to quadruple its stock price (Rapier, 2018).

One of the main promises of the blockchain technology is establishing trust: it suggests that trust – as a main building block of finance (and economy in general) – could be coded within software. Indeed, paradigms shifted with the advent of internet and other communication technologies: relationships between humans, institutions and systems now primarily take place in the virtual, online sphere. We produce, interact, buy and sell all sorts of things without ever seeing each other or shaking hands. When most of our activities transpire within this realm we find ourselves in need of a robust framework for our virtual relations: from proving identity and ownership to establishing lasting business partnerships. Blockchain promises a platform where trust can be "programmed" – obtained by software code which is undisputable, concise, consistent and stable – opposite to human relationships which are often completely opposite.

However, one would be wrong to believe that trust issues are completely resolved by blockchain. Trust (similar to risk in finance) cannot be removed or deferred, it can only be transferred[11]. While it seems easier to trust technology (which is complex but low-dimensional) than humans (which are inseparably both rational and emotional, and prone to exogenous influences – unlike software which does not react differently if the sun is shining[12]), behind every technology ultimately there is always a person. While no one can bribe an algorithm, and while software cannot change its opinion and suddenly slide with the competition, algorithms do not produce themselves ex nihilo: humans make them. Since most people are not experts in coding and cannot review nor audit the source code, ultimately we are dependant to those who provide the technology: we either trust or do not trust them. Furthermore, if the providers are anonymous even larger scope of trust needs to be laid out in order to establish a functioning system.

On the other hand, if nothing else, blockchain provided a new label for the increased yearning for more transparency and individual power in today's ever more interconnected, but simultaneously distant and alienated, big data world, where only a few American companies (Google, Microsoft, IBM, Facebook, Apple) govern and control almost entire digital domain. It expressed a desire for the democratization of information management (creation, storing, sharing, (re)selling, etc.) processes, and that is an impetus worth following.

References:

1. Awodipe, T. (2019). Can Blockchain be used to check corruption in Africa? Retrieved from: https://qwenu.com/2019/03/01/can-blockchain-be-used-to-check-corruption-in-africa/Accessed: 1/3/2019.
2. Bashir, I. (2018). Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained (2nd revised). Packt Publishing.
3. Benoliel, U., Becher, S. I. (2019). The Duty to Read the Unreadable (SSRN Scholarly Paper No. ID 3313837). Retrieved from: https://papers.ssrn.com/abstract=3360200.
4. Christidis, K., Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. Ieee Access.4.pp. 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
5. Dai, W. (1998). b-money. Retrieved from: http://www.weidai.com/bmoney.txt Accessed: 12/3/2019.
6. Deloitte. (2018). Breaking blockchain open: Deloitte's 2018 global blockchain survey. Retrieved from:https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf
7. Domo Inc. (2018). Data never sleeps. Retrieved from: https://www.domo.com/solution/data-never-sleeps-6. Accessed: 12/3/2019.
8. Drescher, D. (2017). Blockchain Basics: A Non-Technical Introduction in 25 Steps. Apress.
9. Dujak, D., Sajte
   Maryniak (Eds.)
   91668-2_2
10. Heyes, A., Saber
    Cases. Americ
    https://doi.org 10
11. Lessig, L.
    https://www.harv
12. Narayanan, A.,
    Cryptocurrency
    https: lccn.loc.g
13. Oxford Dictiona
    Retrieved fro
    19 2 2019.
14. Rapier, G. (2018
    shares to b
    https: finance.ya
    Accessed: 1 3 20
15. Schneier, B. (20
    2th ed.). John V
16. Zyskind, G., Na
    Blockchain to Pr

[11] Proverbial "kicking the can down the road".
[12] Reference to Heyes and Saberian (2019).

g trust: it suggests that trust –
ld be coded within software.
communication technologies:
ily take place in the virtual,
ithout ever seeing each other
alm we find ourselves in need
and ownership to establishing
trust can be "programmed" –
nd stable – opposite to human

etely resolved by blockchain.
n only be transferred[11]. While
onal) than humans (which are
ences – unlike software which
ogy ultimately there is always
annot change its opinion and
elves ex nihilo: humans make
w nor audit the source code,
ve either trust or do not trust
of trust needs to be laid out in

for the increased yearning for
onnected, but simultaneously
mpanies (Google, Microsoft,
ain. It expressed a desire for
g. sharing, (re)selling, etc.)

on in Africa? Retrieved from:
k-corruption-in-

technology, decentralization,

dable (SSRN Scholarly Paper
act=3360200.
Contracts for the Internet of
.CCESS.2016.2566339
.i.com/bmoney.txt Accessed:

bal blockchain survey.
: cz Documents/financial-

.ww.domo.com/solution/data-

duction in 25 Steps. Apress.

9. Dujak, D., Sajter, D. (2019). Blockchain Applications in Supply Chain. In A. Kawa & A. Maryniak (Eds.).SMART Supply Network. pp. 21–46. https://doi.org/10.1007/978-3-319-91668-2_2
10. Heyes, A., Saberian, S. (2019). Temperature and Decisions: Evidence from 207,000 Court Cases. American Economic Journal: Applied Economics.11(2). pp. 238–265. https://doi.org/10.1257/app.20170223
11. Lessig, L. (2000). Code Is Law. Retrieved from: https://www.harvardmagazine.com/2000/01/code-is-law-html Accessed: 12/3/2019.
12. Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S. (2016). Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Retrieved from: https://lccn.loc.gov/2016014802
13. Oxford Dictionaries. (2019). Definition of blockchain in English by Oxford Dictionaries. Retrieved from: https://en.oxforddictionaries.com/definition/blockchain Accessed: 19/2/2019.
14. Rapier, G. (2018). The iced tea company that pivoted to blockchain is selling $8.4 million of shares to buy bitcoin mining machines (LTEA). Retrieved from:: https://finance.yahoo.com/news/iced-tea-company-pivoted-blockchain-151100889.html Accessed: 1/3/2019.
15. Schneier, B. (2015). Applied cryptography: protocols, algorithms, and source code in C (20th ed.). John Wiley and Sons.
16. Zyskind, G., Nathan, O., Pentland, A. "Sandy." (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. New York: Ieee.

Unblocking Blockchain Potentials

Domagoj Sajter
Associate Professor at Faculty of Economics in Osijek, Croatia
e-mail: sajter@efos.hr, phone: +385 91 2244 102; web:
http://www.efos.unios.hr/sajter

Abstract:

The goal of this paper is to research and present the current developments and future prospects of the blockchain technology throughout economy. Since it was introduced within the Bitcoin, blockchain became a buzzword repeated everywhere, often a proposition of panacea for the global problems. However, in the meantime the world of cryptocurrencies experienced a typical boom-bust cycle which many left wandering if blockchain technology was anything more than a hype. This paper aims to establish a brief overview of the possible implementations of distributed ledger (blockchain) technology in the context of the fast growing information society: blockchain may be the essential tool in the economy based upon Internet-of-things, new mobile connectivity standards and big(ger) data.

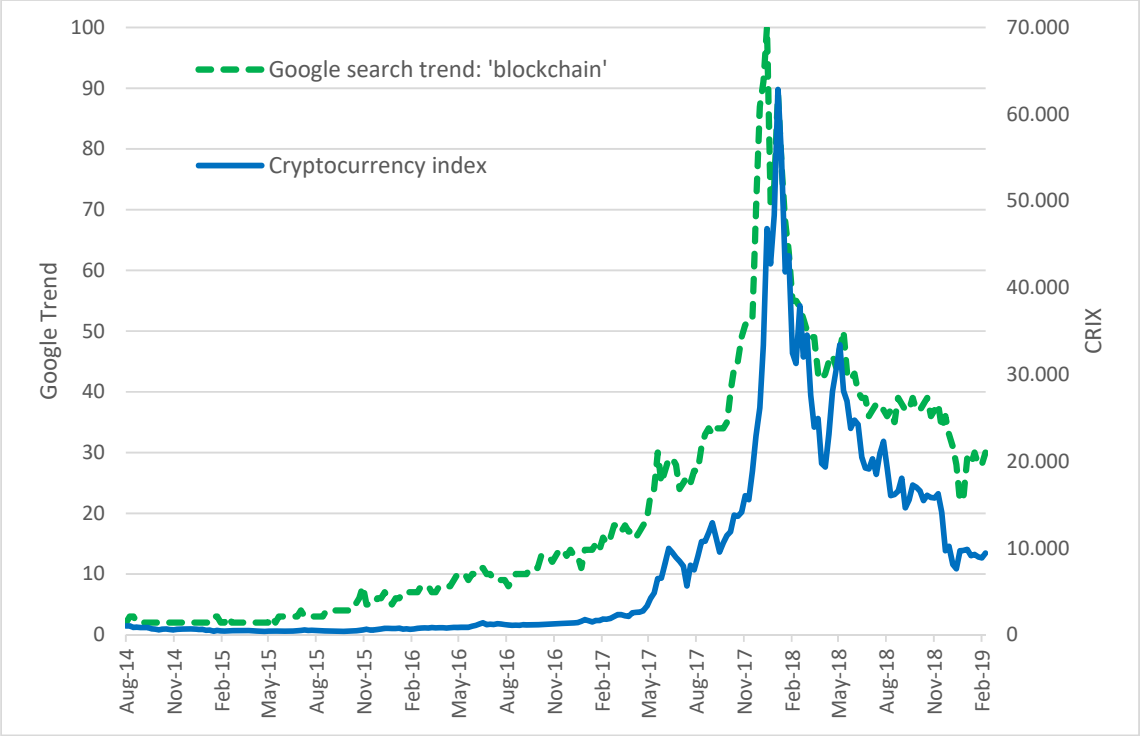
Keywords:
Blockchain, distributed ledger, information society

JEL Codes:
L86, M15, O33, O35, Z0

1. Introduction

Blockchain is among the top buzzwords of the economy in the past couple of years. Worldwide interest for the term 'blockchain' on the Google search engine strongly correlates with the cryptocurrency index CRIX, which is not surprising given the stellar growth of the Bitcoin, Ether and other major cryptocurrencies (Graph 1). The impressive progression of cryptocurrencies during 2017 drew attention for the technology and architecture behind them and fuelled interest to the innovative concept of writing, storing and sharing data.

Graph 1. Cryptocurrency market index vs Google search trend for 'blockchain', 2014-2019



Notes:

Google Trends line represents search interest for the term 'blockchain' relative to the highest point on the chart worldwide during the last five years (2014-2019); a value of 100 is the peak popularity for the term, while 50 means that the term is half as popular.

The CRIX is a cryptocurrency market index where the number of constituents is determined by analysing Akaike and Bayesian information criterions for multiple alternatives of the index, and where each cryptocurrency is weighted with its market capitalization.

Sources: Google Trends and CRIX.de

Those who reflect on the blockchain with (some) knowledge of its peculiarities argue in favour of its potentials; many others who are unacquainted with hashes, nonces, public-key cryptography and other similar "oddities" believe it to be just another passing fad, ripe for oblivion together with the cryptocurrencies' spectacular crash of 2018. It is a trigger-word often inciting emotive reactions, especially with those that gained and/or lost considerable amounts of money with cryptocurrencies.

Regardless of the stance towards the crypto-universe it is only natural to be fascinated by the spectacle of the 01/2017 - 01/2019 crypto boom-bust cycle. What remains, if anything? Eurostat[1] and Fred[2] were queried in February 2019; both sides of the Atlantic had no available data on the keyword 'blockchain'. Is it that the new technology has not yet settled and supplied enough documented statistics, or is digital static all that' s left?

The purpose of this paper is to present the novelty of blockchain technology and to discuss both its present merits and its faults from a non-attached, independent standpoint, away from the emotive reactions of crypto-evangelists and Bitcoin obituaries' writers[3]. Will it really change everything or will it go down in history? As always with such radically opposing and borderline alternatives the road is somewhere in the middle – of course – but to which border is it closer? This paper chooses its risks wisely and halts at the epistemological frontier of knowledge about the society in the future.

After the introduction, the next – second – chapter defines and explains the main pillars of blockchain and the disambiguation between blockchain and distributed ledger, as well as the blockchain as a trust-building mechanism. The third chapter sets the stage for possible implementations and developments of the blockchain technology by providing wider context of the information society we live in, together with the new developments of the information communication technology. Finally, fourth chapter concludes.

2. Blockchain and trust

Deloitte surveyed 1053 respondents knowledgeable of blockchain across seven countries globally, from ten industries, and two thirds of them said that their company will spend more than 1 million USD investing in the blockchain technology during the next year (Deloitte, 2018, p. 18). This is an indication of the non-triviality of the momentum cryptocurrencies have made.

On the other hand, it is sometimes difficult to assess whether the investment into blockchain is a "true" venture into new technology or a covert marketing expenditure trying to implant an image of a corporation willing to explore cutting-edge ideas. This adds to list of reasons why it is important to understand what blockchain is and what it proposes.

Oxford Dictionary defines blockchain as "*a system in which a record of transactions made in bitcoin or another cryptocurrency are maintained across several computers that are linked in a peer-to-peer network*" (Oxford Dictionaries, 2019). Acknowledging that every definition is always a trade-off between brevity and accuracy, the previous explanation provides only indications of what blockchain is, does, and could be. The most cited article on both Web of Science and Scopus databases regarding blockchain (199 and 324 citations in February 2019, respectively) portrays it as "*a distributed data structure that is replicated and shared among the members of a network*"; "*a log whose records are batched into timestamped blocks*" (Christidis & Devetsikiotis, 2016, p. 2293).

[1] https://ec.europa.eu/eurostat/

[2] https://fred.stlouisfed.org

[3] Reference to https://99bitcoins.com/category/bitcoin-obituaries/.

A comprehensive description of blockchain includes (at least) four elements: it defines it as (1) a data structure, (2) an algorithm, (3) a collection of technologies, and (4) a generalization of distributed peer-to-peer systems with a common application area (Drescher, 2017, p. 33).

Data structure relates to the concept of arrangement of data within entities named as *blocks*, whereas blocks are connected between themselves in an ordered sequence (*chain*). Linking blocks is done via cryptography which ensures immutability of the data within. In simple terms, cryptography is here used primarily for two purposes: (a) to "lock" the data within the blocks (to make the data unchangeable and/or private, hidden to outsiders), and (b) for trustworthy and reliable assignment of identities behind the data (digital signatures). The data of the first blockchain – Bitcoin – consists of transactions, where one party sends valuable information (which crypto-proponents equate to money[4]) to the other, through internet, where every malevolent person could alter or steal the contents of that transaction.

Having seen that the Bitcoin system functions the idea evolved with the notion that the data within blocks can be something other than transactions – whichever "valuable information" (Dujak & Sajter, 2019, p. 26) that may be. The data structure is also described as a *ledger*; 'distributed ledger technology' is often used as a synonym to 'blockchain technology', especially with those who seek to distance themselves from the cryptocurrency subculture and its worldviews[5].

Closely related to the data structure, an 'algorithm' refers to an unambiguous sequence of commands, which as an output frequently builds up aforementioned data structures – blocks. Developing and maintaining blockchain requires a common set of rules which users abide by; these rules are encoded in the algorithm which is often referred to as "the law" (Lessig, 2000).

Combining data structure with the algorithm and underlying cryptographic models broadens the concept of blockchain and extends it to a collection of technologies with similar traits.

Lastly, a blockchain can be viewed as a generalization of distributed, decentralized systems with a common application. The keywords here are distribution and decentralization: in a globalized economy founded upon the information flows one of the vital actual questions is how to reach a consensus without a common authority. Internet is by itself a global network without a main, central hub, without continental or even regional core points. It is a collection of

---

[4] One can notice a reluctance in calling Bitcoin "money". This is because even though it is an innovative and promising concept it only anecdotally fulfils three main functions of money: Bitcoin is not a widely accepted medium of exchange, nor it is a unit of account, and it certainly is not a stable depository of value over time. This could however change in the future, but that would require large scale adoption and a redesign of current payment systems.

[5] The origins of Bitcoin are embedded in the cypherpunk movement, which could be correlated to cyber-anarchy (Narayanan, Bonneau, Felten, Miller, & Goldfeder, 2016, p. 247). One of the predecessors of Bitcoin is *b-money*, concept developed by Wei Dai in 1998. Dai starts his essay with the following statements: "*I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary*." (Dai, 1998) If we would maintain that ideas and beliefs are the essential drivers of human actions, if the cryptocurrencies were to become mainstream the ideas and beliefs behind them would also need to become mainstream. With cypherpunk this is certainly not the case.

dispersed nodes, open for communication, which makes them vulnerable to all kinds of attacks. Conceiving both a data structure and a protocol for sending and receiving, storing and changing valuable information on such a flat, level playing field is an innovation worthy of its "buzz".

Given that the main pillar of the blockchain is its ability to attain agreement on a peer-to-peer level much of the confusion and controversy regarding the notion of blockchain stems from abandonment of aforementioned proposition, a proposition which was central to crypto-enthusiasts. Evolution of blockchain lead it to the crossroad at which the basic, rudimentary typology emerged: blockchains can be public or private (Bashir, 2018).

Public blockchains are "classic, traditional" systems open to everyone, where no permission needs to be given from the existing participants to the admission of the newcomer; he only needs to adhere to the established protocol in order to join. This also means that the identity is irrelevant since anyone can participate – screening individual traits is pointless as there are no gatekeepers. The only prerequisite is adherence to "the law" – the software code within the protocol.

Private blockchains are the opposite: they are permissioned (only selected entities can be members) which means that a blockchain only enhances certain pre-existing level of trust. As such, private blockchains lack the fundamental novelty of its Bitcoin predecessor, which is why many oppose to the very notion of private blockchain and why the phrase "distributed ledger technology" became widespread. Without decentralization it becomes difficult to find the unique selling point of a private blockchain, because a simple (and free) Google Sheet (e.g.) does almost all the work: it is a shared database, saved online, with dedicated passwords for viewing and editing, recording all logins and changes to it.

There is also a third path: somewhere in between. A blockchain-based system can have both permissioned and permissionless sub-zones where different permissions (for reading/writing data, proofing, upgrading protocol, as well as granting and revoking authorities for these activities, etc.) can be given to certain groups, even to the public[6]. This is where presently blockchain hold most of its potential.

The essential innovation of the blockchain technology is its proclaimed ability to generate the "glue" that holds the economy together: trust. In a capitalist economy money can buy almost anything, but not trust[7]. The core element of trust building within any blockchain is math; at the basic proficiency in math language 2254789 x 3325548 either is or isn't 7498409049372. The calculus is easily provable, and after proofing "trust" is established that indeed 2254789 times 3325548 equals 7498409049372. Cryptography could be regarded as a branch of mathematics where the following principle is heavily used: it is very easy to determine as true that a x b = c, but it takes much more time and effort to start backwards, with the product (c = 7498409049372), and to find which two seven-digit numbers (a, b) were multiplied in order to provide that solution.

[6] For instance, public could be given right to read the data, group A could write to database, group B could do the proofing, and group C could give subsections of both groupa A and B right to update the protocol.

[7] If an entrepreneur somehow cheats its business partner no money in the world can restore their relationship to its previous state. Money can mend superficial relationship and be a component of the restoration, but money alone cannot change beliefs.

Cryptography uses powerful functions which are very easy to prove if one has the information in advance, but are practically impossible to solve backwards[8]. This property allows them to be used in the context of maintain data integrity, proofing ownership over data and exchanging data securely over unsafe communication channels, which are crucial in the internet today.

However, "trust" here has only one necessary component because it is only ex-post maintained: in the context of blockchain it merely declares that the outcome of an algorithm with known set of variables, parameters and rules is true or false, which hardly qualifies as trust. In the non-virtual world trust also has an ex-ante notion: it is a belief that under unknown future circumstances (indefinite set of variables and parameters, but known rules) the outcome of a series of events (algorithm) will be equal to anticipated. The trust as a prerequisite for the functioning economy is also forward looking; it is a consciously accepted risk (under condition of uncertainty) that the future consequences of the risk acceptance will not be disappointing. It is a leap into unknown which is only party simulated in the crypto domain, where the sole trust cryptography can provide us with is (somewhat simplified) that in the future only the holder of the right keys can handle the data locked/signed with that keys. However, the trust is needed beyond that: one needs to believe that the blockchain system will persist and be active, that developers will maintain the code, that intermediaries will survive (presuming that the user is not skilled as a blockchain developer) and provide service, that regulation will not change radically, etc. Hence, the core assumption that trust in the civilization could somehow be coded into software is only partially established with the novel ledger technology.

3. Information society and leaps in the development of ICT

In 2018 worldwide each minute, every day, approximately 160 million of emails are sent, 13 million SMS (text) messages are delivered, and Google conducts 3,9 millions of searches; by 2020 it's estimated that for every person on earth 1,7 MB of data will be created every second (Domo Inc., 2018). Handling the enormous and growing amounts of data will require novel systems, and blockchain stands here as a potential framework – a blueprint for the future data management technologies.

It could be argued that people created vast amounts of data since the beginning of civilization, but that data was not (for the most part) stored anywhere and it was lost either immediately, or over time. Nowadays Wi-Fi passwords are stored even in lightbulbs (see Table 1.), and people leave digital traces in whatever they do and wherever they go. Most of the digital services regarded as "free" (because they are not paid with money directly; e.g. browsing the web, e-mail communication, social networks, etc.) are funded indirectly by the data we leave

[8] Schneier provides a vivid example: „*A typical supernova releases something like 10^51 ergs* [erg is an unit of energy equal to 10^−7 joules]. *If all of this energy could be channelled into a single orgy of computation, a 219-bit counter could be cycled through all of its states. These numbers have nothing to do with the technology of the devices; they are the maximums that thermodynamics will allow. And they strongly imply that brute-force attacks against 256-bit keys will be infeasible until computers are built from something other than matter and occupy something other than space.*" (Schneier, 2015, pp. 157–158)

behind while using these services. Even though the data created could be seen as merely noise, powerful AI systems can detect patterns within, which makes them potentially valuable. Since almost no one actually reads the contracts we sign when we register for these services and that they are in fact unreadable (Benoliel & Becher, 2019), it shouldn't come as a surprise that our private data gets leaked, sold and resold, and used in ways we never could foresee.

With the purpose of giving illustration to the previous statements, a miniature ad-hoc "research" has been performed. News was collected from well-known and widely used internet outlets regarding issues of consumer privacy. The extent of the research spans over three months (from the beginning of November 2018 to end of January 2019); 26 articles during that period were found which expose various malfeasances with user data (Table 1.). Many blockchain enthusiasts intend to take back control of both the underlying data and the systems which create and manage that data.

The processes of data creation and high-speed communication are expected to escalate to a new level. Among others, two noticeable (and intertwined) advancements are anticipated. The one is the proliferation of a new category of data creators in the realm of internet-of-things – devices and objects packed with sensors, cameras, microphones, machine learning / artificial intelligence software, etc., connected to internet and communicating between themselves. The ability to collect real-time data could provide businesses and consumers with a number of benefits, allowing automation of processes, rising productivity and enhancing customer service. The second is the new standard of mobile communication which will serve as a highway for distribution of all the new (and "old") data. Fifth generation of mobile infrastructure (5G), expected to be perfected in 2020, will expectedly provide a massive leap in not only speed, but also capacity, cost reduction, and traffic. Expectations are very high and even if the providers under-deliver the change could still be substantial. These leaps will most likely indicate a new era of ICT and data management.

However, one of the difficult tasks will be to provide proper levels of security and privacy: creating and sharing all that data could easily become disturbing if confidentiality controls were not put in place. One of the main contributions of Bitcoin and blockchain in general is in directing attention to powerful cryptographic tools which can protect both privacy and security – values which are in high demand lately:

"*The recent increase in reported incidents of surveillance and security breaches compromising users' privacy call into question the current model, in which third-parties collect and control massive amounts of personal data.* […] [T]*rusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger*." (Zyskind, Nathan, & Pentland, 2015, p. 180)

Farsighted but concrete projects such as Hyperledger, IBM's Blockchain World Wire, Microsoft's Azure Blockchain Workbench, Alibaba Cloud's Blockchain as a Service, Amazon's Quantum Ledger Database, JP Morgan's Coin – among many others – signal that blockchain technology could be here to stay, regardless of the cryptocurrency haze.

Table 1. Malfeasances with user data: online news from Nov-2018 to Feb-2019

Publisher of the news*	Shortened link to the news	"Perpetrator/-s"	Deed
Washington Journal of Law, Tech and Arts	tinyurl.com/yxqrjmul	Amazon	Consumer generated mass surveillance
Business Insider	tinyurl.com/y3be8jk6	Amazon	Spying/tracking users
Financial Times	tinyurl.com/y2yzzh2n	At least 34 apps (games, etc.)	Selling user data to Facebook
New York Times	tinyurl.com/y7lry8rw	At least 75 companies	Spying/tracking users
Techcrunch	tinyurl.com/y9h3ky78	Facebook	Spying/tracking users
35th Chaos Communication Congress	tinyurl.com/y3ja6w83	Facebook	Tracking and selling user data even if user doesn't have FB account or app
Ars Technica	tinyurl.com/y3yby6ya	Facebook	“Knowingly violated” privacy laws
The Verge	tinyurl.com/yckq85tt	Facebook	Spying/tracking users
Wired	tinyurl.com/y7o9muqb	Facebook, Instagram, WhatsApp, Messenger	Sharing user data
Business Insider	tinyurl.com/y7e9gbcm	Google	Creating "bubbles" by filtering search results
Deutsche Welle	tinyurl.com/yyazassz	Google	Privacy breach
Techcrunch	tinyurl.com/yaopxlop	Google	Spying/tracking users
Medium	tinyurl.com/ydfmnbpe	Google	Spying/tracking users
Medium	tinyurl.com/yyjwzjh7	Google	Spying/tracking users
The Intercept	tinyurl.com/yagqxlh7	Google	Spying/tracking users
Business Insider	tinyurl.com/y3jb37ac	Google	Secretly putting microphones in devices
Search Engine Journal	tinyurl.com/y4uayhns	Google, Facebook, Twitter	Disrespecting the “Do Not Track” setting on web browsers
Bruce Schneier	tinyurl.com/y8yy9eh9	Government/-s	Placing surveillance cameras in streetlights
Wired	tinyurl.com/y7r24mel	Governments	Spying/tracking citizens
Fair	tinyurl.com/yyg47urs	Governments	Potential misuse of face recognition
Motherboard	tinyurl.com/ya25y9wx	Hundreds of free apps	Tracking and selling user data
Boing Boing	tinyurl.com/yadvbxyv	Lifx	Passwords saved insecurely (in a lightbulb)
Bloomberg	tinyurl.com/y9jzrjmf	Private DNA testing company	Leaking DNA data to FBI
Business Insider	tinyurl.com/ybjldmrg	Smart TVs	Tracking and selling user data
Bleeping Computer	tinyurl.com/y49o9jr5	Thousands of apps	Violating policies
Techcrunch	tinyurl.com/ycr4m3o5	Unknown	24 million financial and banking documents published online
**News published during the three month period from the beginning of November 2018 to end of January 2019*			

Source: Author

4. Conclusion

The concept of blockchain seems to be an interest-inciting idea often thrown around ostentatiously with the aim of increasing brand and/or company valuation[9]. It is also frequently perceived as a tool with whom all nails could be hammered; dealing with issues from corruption in Africa to delivering babies (Awodipe, 2019).

One of the main promises of the blockchain technology is establishing trust: it suggests that trust – as a main building block of finance (and economy in general) – could be coded within software. Indeed, paradigms shifted with the advent of internet and other communication technologies: relationships between humans, institutions and systems now primarily take place in the virtual, online sphere. We produce, interact, buy and sell all sorts of things without ever seeing each other or shaking hands. When most of our activities transpire within this realm we find ourselves in need of a robust framework for our virtual relations: from proving identity and ownership to establishing lasting business partnerships. Blockchain promises a platform where trust can be "programmed" – obtained by software code which is undisputable, concise, consistent and stable – opposite to human relationships which are often completely opposite.

However, one would be wrong to believe that trust issues are completely resolved by blockchain. Trust (similar to risk in finance) cannot be removed or deferred, it can only be transferred[10]. While it seems easier to trust technology (which is complex but low-dimensional) than humans (which are inseparably both rational and emotional, and prone to exogenous influences – unlike software which does not react differently if the sun is shining[11]), behind every technology ultimately there is always a person. While no one can bribe an algorithm, and while software cannot change its opinion and suddenly slide with the competition, algorithms do not produce themselves ex nihilo: humans make them. Since most people are not experts in coding and cannot review nor audit the source code, ultimately we are dependant to those who provide the technology: we either trust or do not trust them. Furthermore, if the providers are anonymous even larger scope of trust needs to be laid out in order to establish a functioning system.

On the other hand, if nothing else, blockchain provided a new label for the increased yearning for more transparency and individual power in today's ever more interconnected, but simultaneously distant and alienated, big data world, where only a few American companies (Google, Microsoft, IBM, Facebook, Apple) govern and control almost entire digital domain. It expressed a desire for the democratization of information management (creation, storing, sharing, (re)selling, etc.) processes, and that is an impetus worth following.

5. Bibliography

Awodipe, T. (2019, March 1). Can Blockchain be used to check corruption in Africa? Retrieved March 1, 2019, from Qwenu website:

[9] An example: a company that sells ice tea renamed to "Long Blockchain" which was enough to quadruple its stock price (Rapier, 2018).

[10] Proverbial "kicking the can down the road".

[11] Reference to Heyes and Saberian (2019).

https://qwenu.com/2019/03/01/can-blockchain-be-used-to-check-corruption-in-africa/
Bashir, I. (2018). *Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained* (2nd revised). Packt Publishing.
Benoliel, U., & Becher, S. I. (2019). *The Duty to Read the Unreadable* (SSRN Scholarly Paper No. ID 3313837). Retrieved from Social Science Research Network website: https://papers.ssrn.com/abstract=3360200
Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *Ieee Access*, *4*, 2292–2303. https://doi.org/10.1109/ACCESS.2016.2566339
Dai, W. (1998). b-money. Retrieved March 12, 2019, from Wei Dai's Homepage website: http://www.weidai.com/bmoney.txt
Deloitte. (2018). *Breaking blockchain open: Deloitte's 2018 global blockchain survey*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf
Domo Inc. (2018). Data never sleeps. Retrieved March 17, 2019, from See how data's connecting everyone to everything across the world, every minute website: https://www.domo.com/solution/data-never-sleeps-6
Drescher, D. (2017). *Blockchain Basics: A Non-Technical Introduction in 25 Steps*. Apress.
Dujak, D., & Sajter, D. (2019). Blockchain Applications in Supply Chain. In A. Kawa & A. Maryniak (Eds.), *SMART Supply Network* (pp. 21–46). https://doi.org/10.1007/978-3-319-91668-2_2
Heyes, A., & Saberian, S. (2019). Temperature and Decisions: Evidence from 207,000 Court Cases. *American Economic Journal: Applied Economics*, *11*(2), 238–265. https://doi.org/10.1257/app.20170223
Lessig, L. (2000, January 1). Code Is Law. Retrieved March 12, 2019, from Harvard Magazine website: https://www.harvardmagazine.com/2000/01/code-is-law-html
Narayanan, A., Bonneau, J., Felten, E., Miller, A., & Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*. Retrieved from https://lccn.loc.gov/2016014802
Oxford Dictionaries. (2019). Definition of blockchain in English by Oxford Dictionaries. Retrieved February 19, 2019, from Oxford Dictionaries | English website: https://en.oxforddictionaries.com/definition/blockchain
Rapier, G. (2018, January 5). The iced tea company that pivoted to blockchain is selling $8.4 million of shares to buy bitcoin mining machines (LTEA). Retrieved March 1, 2019, from Yahoo Finance website: https://finance.yahoo.com/news/iced-tea-company-pivoted-blockchain-151100889.html
Schneier, B. (2015). *Applied cryptography: protocols, algorithms, and source code in C* (20th ed.). John Wiley and Sons.
Zyskind, G., Nathan, O., & Pentland, A. "Sandy." (2015). *Decentralizing Privacy: Using Blockchain to Protect Personal Data*. New York: Ieee.