Chorzowskie Studia Polityczne
Nr 13 rok 2017

Paweł Szewczyk
Wyższa Szkoła Bankowa w Poznaniu
Wydział Zamiejscowy w Chorzowie
e-mail: pszewczyk@chorzow.wsb.pl
tel. 32 22 70 107

Application of the Distributed Ledger Technology in Administration. Blockchain-Based Identity System

Summary. Public administration must be able to keep pace, in the long term, with advances in technology, as well as with the evolution of administrative techniques and changes in the social environment. Technological intervention, the incorporation of new management principles, and an increasing focus on meeting the needs and aspirations of the end customer are just some of the prevalent trends in contemporary public administration. There exists a wide consensus that identity is a fundamental human right. On May 20, 2016 a conference was held under the auspices of the United Nations to discuss the ways of providing a unique digital identity to everyone on the planet. As a most important outcome of the conference, commitments were made by the participants, from individuals pledging their own time, to corporations offering ongoing financial support. Public/private key cryptography and decentralized technologies like blockchain are seen as viable solutions to the problem of universal digital identity. It is hoped that a blockchain-based identity might allow consumption of a number of services in a trusted manner without the need to assert our physical presence, in e.g. remote voting. On the other hand, it must be realized that, promising as it appears, blockchain is just another emerging technology and, like any technology promise, requires time to materialize. The paper employs the latest information available (mostly from Internet sources) to address the objective of providing identity resolution to the world's entire population and describe the earliest attempts at applying the distributed ledger (blockchain) technology to accomplish this objective.

Keywords: public administration, digital identity, distributed computing, blockchain technology

1. Introduction

Experts of the Management Study Guide.com (MSG) defined recently the role of public administration in the modern state in the following way: 1) the critical

role of public administration is governing the society, 2) public administration provides numerous services to the public and serves their interests in many ways, 3) it is the administration which ensures the security and protection of life and property of the members of the society by maintaining proper law and order [managementstudyguide.com 2008].

The economic, cultural and even spiritual progress of society depends on the public administration. The day to day functioning of the government machinery, external affairs and the most important of all, the national defense are the other important functions performed by the public administration of the country.

The current role and functions adopted by public administration owes its origin to the changes which the human history has witnessed in the last couple of centuries. The first important change was the industrial revolution which resulted in the urbanization of the large cities of the world. Secondly, there was a change in the political philosophy from minimalist state intervention (or laissez-fare) and individualism to social welfare. The two World Wars combined with the changing international scenarios with new countries, alliances and organizations like the formation of United Nations, generated a need to reform the goals of administration in the society; not just of within a nation but also with respect to the world. Lastly, the increasing population of the world means tremendous pressure on the available resources. The role of providing for basic amenities like food and shelter has therefore fallen into the lap of the government.

According to MSG experts [managementstudyguide.com 2008] there are three characteristics of an efficient public administration:

– It needs to meet the functional aims for which it has been created.

– It must be able to meet the long term needs which might arise due to change in administrative techniques or the changes in social environment which are more important and influential.

– It needs to conform to a centralized plan but also accommodate the specific and special demand of particular department units.

Thus, the role and functions of public administration has also become quite dynamic in nature and is constantly evolving in response to the changing needs and demands of the society. Technological intervention, incorporation of new management principles, taking into accounts the needs and aspirations of the end customer are some of the new trends in the areas of public administration [managementstudyguide.com 2008].

Taking advantage of the most recent information available (mostly from the Internet sources) in this paper a problem of solving the identity recognition of all members of the world population is approached and first attempts to apply for this purpose the distributed ledger technology (blockchain) is described.

2. Identity – a fundamental human right

One-fifth of the world's population lives without an officially recognized identity [Why identity 2016]. Article 6 of the Universal Declaration on Human Rights stipulates that: „Everyone has the right to recognition everywhere as a person before the law". The Sustainable Development Goals (SDG 2015-2030) [www.un.org 2016] include target 16.9 which aims to „provide legal identity to all, including birth registration, by 2030". Critically, this must include the over 20 million refugees worldwide.

Individuals are required to show identification to access healthcare and education, vote, and access other social assistance programs.

Governments without an accurate system of identification struggle to provide well-coordinated social services, simply because the number of beneficiaries is unknown and precise targeting is impossible. And without clear registries, the risk of leakages and corruption are high. More than 2.5 billion adults do not have a bank account or use formal financial services, making it difficult to move out of poverty or weather a period of hardship [www.un.org 2016]. Connecting people with digitally-based financial tools and services requires accessible, secure and verifiable ID systems.

Women with an official identity are empowered to play a greater role in household decisions and maintain financial independence. Furthermore, identification can be an important defense against child marriage, exploitation and trafficking.

In addition to the intrinsic benefit of identity, it is a necessary prerequisite for achieving many of the other sustainable development goals. International goals will be difficult to reach or measure without a way to identify beneficiaries.

The United Nations created ID2020 – a hub, that will harness emerging digital technologies, to create the world's largest innovation platform in support of SDG goal 16.9; providing legal identity for all, including birth registration.

It serves as a bridge between governments and public-sector organizations working on the ground and technology companies who understand technical possibilities. This ensures that solutions developed are appropriate and implementable, while also bringing the best technological innovation to bear [id2020.org 2016a].

On May 20th, 2016 the hub ID 2020 organized an Inaugural Summit at the United Nations [id2020.org 2016b].

The summit brought together over 400 people to discuss how to provide a unique digital identity to everyone on the planet, including the 1.5 billion people living without any form of recognized identification.

Participants included over 150 private sector companies, 11 UN agencies, diverse non-profits, governments, and representatives from academia. This

collaborative, multi-sectoral forum explored both the human challenges of life without identity, explored relevant technological innovations, and highlighted opportunities and constraints for scaling up.

The following outcomes were reached [id2020.org 2016b]:

– Widespread consensus among ID2020 attendees that identity is both a fundamental human right and a necessary prerequisite for the success of the Sustainable Development Goals.

– Recognition that the private sector has significant expertise and technology that could be transformative in accelerating access to digital identity.

– Broad understanding that no single organization or government can „own" identity, but instead, that a public-private partnership is needed to bring together the broad group of stakeholders, provide coordination, and ensure that the best technological innovations are implemented in ways that are appropriate, secure and sustainable.

– Sweeping commitments from conference attendees to contribute towards the shared goal of universal digital identity. These commitments ranged from individuals pledging their time to corporations offering ongoing financial support.

3. Achieving trust in the digital age

According to the opinions of Don Tapscott and Alex Tapscott [2016: 10-26] trust in business is the expectation that the other party will behave according to the four principles of integrity:

– honesty,
– consideration,
– accountability, and
– transparency.

Honesty has become an economic issue. Organizations must be truthful, accurate, and complete in communications. **Consideration** in business often means a fair exchange of benefits or detriments that parties will operate in good faith. **Accountability** means making clear commitments to stockholders and abiding by them. **Transparency** means operating out in the open, in the light day.

In the world, trust in transactions derived from individuals, intermediaries, or other organizations acting with integrity. In the emerging blockchain world, trust derives from the internet network and even from the objects on the network.

Throughout history, each new form of media has enabled mankind to transcend time, space, and mortality. That ability raises the existential question of identity. The above mentioned authors use the word **identity** to describe the self,

the projection of the self to the world, and all these attributes that are associated with that self or one of its projections. These may come from nature, from the state, from private organizations.

In the early days of the Internet most corporations and institutions view people by their data contrail across the Internet. They aggregate ones data into a virtual representation of that person and they provide this „virtual person" with extraordinary new benefits.

This „ virtual person" could in fact be owned by the person as a personal avatar and „lived" in the black box of the person's identity, so she could monetize own data stream and reveal only what would be needed. One can imagine a new era of the Internet where the personal avatar manages and protects the contents of her black box. This trusty software servant could release only the required detail or amount for each situation.

The black box may include information such as a government-issued ID, social security number, medical information, service accounts, financial accounts, diplomas, practice, licenses, birth certificate, various other credentials.

In order to achieve prosperity, an individual must possess, at minimum, access to some form of basic financial services to reliably store and move value, communication, and transactional tools to connect to the global economy, and security, protection, and enforcement of the title to land and other assets they possess legally. This is the promise of the blockchain technology [Tapscott 2016: 17].

4. Blockchain technology explained

Blockchain technology can be a confusing concept to understand [Definitions and Explanations... 2016]. It is a relatively new concept and rapidly growing industry. Similar data structures have existed long before the popular bitcoin cryptocurrency was conceived, however, principal theories of blockchain architectures used today were first outlined and defined in the original bitcoin white paper written and published by Satoshi Nakamoto in 2008 [Nakamoto 2008].

As this nascent technology is ripe with ongoing innovations, it is best to keep an open mind and expect new related-technologies to continue to emerge. Below key definitions and concepts to understand of this basic pillars behind this revolutionary technology are explored.

A **distributed ledger** is a consensus of replicated, shared, and synchronized digital data geographically spread across multiple sites, countries, and/or institutions. Users of Distributed Ledger Technology (DLT) significantly benefit from

the efficiencies and economics by creating a more robust environment for real-time and secure data sharing.

A **blockchain** is a type of distributed ledger, comprised of unchangeable, digitally recorded data in packages called **blocks**. These digitally recorded „blocks" of data is stored in a linear **chain**. Each block in the chain contains data (e.g. bitcoin transaction), is cryptographically hashed. The blocks of hashed data draw upon the previous-block (which came before it) in the chain, ensuring all data in the overall „blockchain" has not been tampered with and remains unchanged.

A blockchain is just one type of distributed ledger, not all distributed ledgers necessarily employ blocks or chain transactions. Although the term „blockchain" is used more frequently than „distributed ledger" in discussions, a block chain is only one of the many types of data structures that provide secure and valid achievement of distributed consensus. The Bitcoin blockchain, which uses „The proof-of-work mining" [Krawisz 2016], is the most publicly proven method used to achieve distributed consensus. However, other forms of distributed ledger consensus exist such as Ethereum, Ripple, Hyperledger, MultiChain, Eris, and other private enterprise solutions.

4.1. Distributed Ledger Technology: beyond block chain

A recent report by the UK Government Chief Scientific Adviser: „Distributed Ledger Technology: beyond block chain" contains the following astute description of the potential applications of this technology [UK Government Chief Scientific Adviser 2016]. A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds. The assets can be financial, legal, physical or electronic. The security and accuracy of the assets stored in the ledger are maintained cryptographically through the use of „keys" and signatures to control who can do what within the shared ledger. Entries can also be updated by one, some or all of the participants, according to rules agreed by the network.

Underlying this technology is the „block chain", which was invented to create the peer-to-peer digital cash bitcoin in 2008. Block chain algorithms enable Bitcoin transactions to be aggregated in „blocks" and these are added to a „chain" of existing blocks using a cryptographic signature. The Bitcoin ledger is constructed in a distributed and „permission less" fashion, so that anyone can add a block of transactions if they can solve a new cryptographic puzzle

to add each new block. The incentive for doing this is that there is currently a reward in the form of twenty five bitcoins awarded to the solver of the puzzle for each „block". Anyone with access to the internet and the computing power to solve the cryptographic puzzles can add to the ledger and they are known as „Bitcoin miners" [wikipedia.org 2016]. The mining analogy is apt because the process of mining bitcoin is energy intensive as it requires very large computing power.

Bitcoin is an online equivalent of cash. Cash is authenticated by its physical appearance and characteristics, and in the case of banknotes by serial numbers and other security devices. But in the case of cash there is no ledger that records transactions and there is a problem with forgeries of both coins and notes. In the case of Bitcoins, the ledger of transactions ensures their authenticity. Both coins and bitcoins need to be stored securely in real or virtual wallets respectively – and if these are not looked after properly, both coins and bitcoins can be stolen. A fundamental difference between conventional currency and bitcoins is that the former are issued by central banks, and the latter are issued in agreed amounts by the global „collaborative" endeavor that is Bitcoin. Cash as a means of exchange and commerce dates back millennia and in that respect there is a lineage that links hammered pennies and bitcoin.

So the basic block chain approach can be modified to incorporate rules, smart contracts, digital signatures and an array of other new tools.

Distributed ledger technologies have the potential to help governments to collect taxes, deliver benefits, issue passports, record land registries, assure the supply chain of goods and generally ensure the integrity of government records and services. For the consumer of all of these services, the technology offers the potential, according to the circumstances, for individual consumers to control access to personal records and to know who has accessed them.

Existing methods of data management, especially of personal data, typically involve large legacy information technology (IT) systems located within a single institution. To these are added an array of networking and messaging systems to communicate with the outside world, which adds cost and complexity. Highly centralized systems present a high cost single point of failure. They may be vulnerable to cyber-attack and the data is often out of sync, out of date or simply inaccurate.

In contrast, distributed ledgers are inherently harder to attack because instead of a single database, there are multiple shared copies of the same database, so a cyber-attack would have to attack all the copies simultaneously to be successful. The technology is also resistant to unauthorized change or malicious tampering, in that the participants in the network will immediately spot a change to one part of the ledger. Added to this, the methods by which information is secured and

updated mean that participants can share data and be confident that all copies of the ledger at any one time match each other [wikipedia.org 2016].

But this is not to say that distributed ledgers are invulnerable to cyber-attack, because in principle anyone who can find a way to „legitimately" modify one copy will modify all copies of the ledger. So ensuring the security of distributed ledgers is an important task and part of the general challenge of ensuring the security of the digital infrastructure on which modern societies now depend.

Governments are starting to apply distributed ledger technologies to conduct their business. The business community has been quick to appreciate the possibilities. Distributed ledgers can provide new ways of assuring ownership and provenance for goods and intellectual property. For example, Everledger [2017], a fraud detection system overlaying big data from closed sources like insurers and law enforcement, provides a distributed ledger that assures the identity of diamonds, from being mined and cut to being sold and insured. In a market with a relatively high level of paper forgery, it makes attribution more efficient, and has the potential to reduce fraud and prevent 'blood diamonds' [wikipedia.org 2017a] from entering the market.

As with most new technologies, the full extent of future uses and abuses is only visible dimly. And in the case of every new technology the question is not whether the technology is „in and of itself" a good thing or a bad thing. The questions are: what application of the technology? for what purpose? and applied in what way and with what safeguards?

In summary, distributed ledger technology provides the framework for government to reduce fraud, corruption, error and the cost of paper-intensive processes. It has the potential to redefine the relationship between government and the citizen in terms of data sharing, transparency and trust. It has similar possibilities for the private sector [UK Government Chief Scientific Adviser 2016].

4.2. How blockchain works

In the January-February 2017 issue of Harvard Business Review, Marco Iansiti and Karim R. Lakhani [2017: 118-127] described the characteristics of the blockchain technology.

They assumed that there are five basic principles underlying the technology:

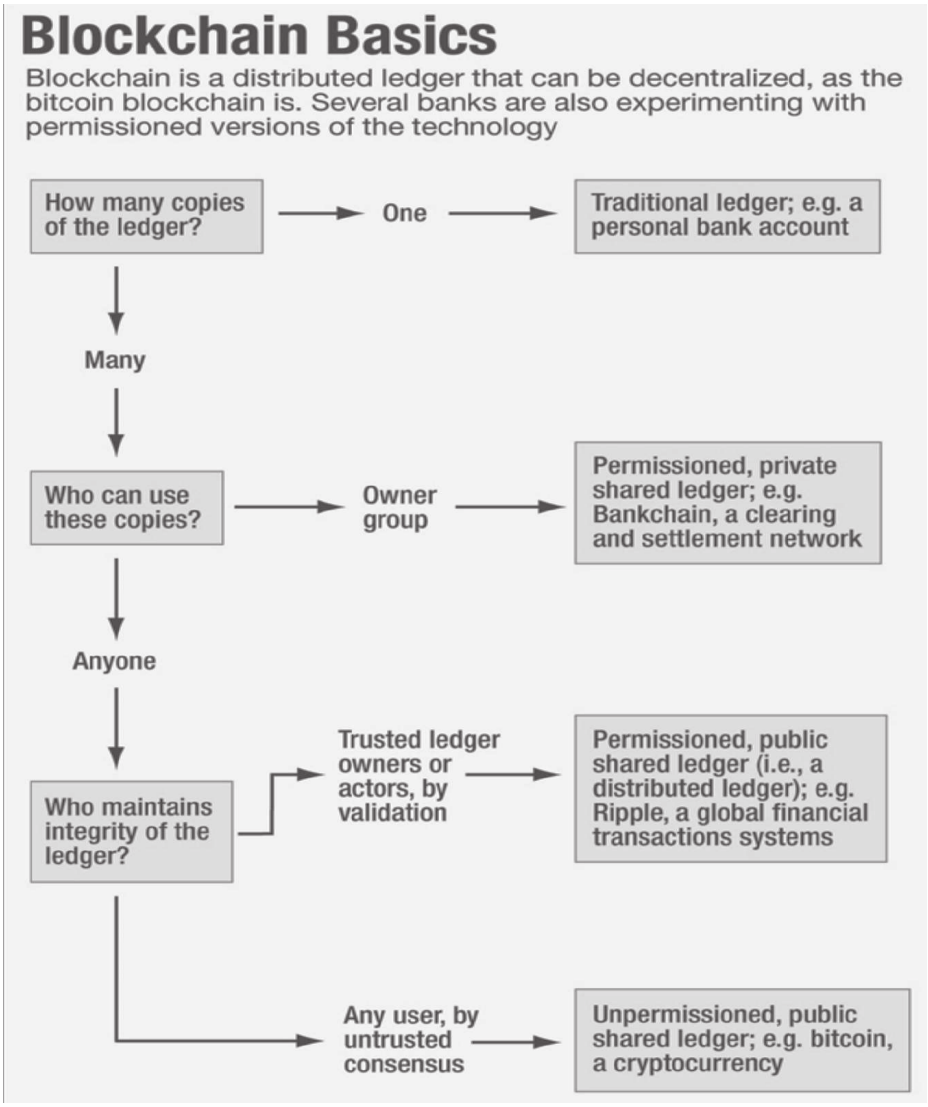
1. Distributed Database. Each party on a blockchain has access to the entire database and its complete history. No single party controls the data or the information. Every party can verify the records of its transaction partners directly, without an intermediary.

2. Peer-to-Peer Transmission. Communication occurs directly between peers instead of through a central node. Each node stores and forwards information to all other nodes.

3. Transparency with Pseudonymity. Every transaction and its associated value are visible to anyone with access to the system. Each node, or user, on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others. Transactions occur between blockchain addresses.

4. Irreversibility of Records. Once a transaction is entered in the database and the accounts are updated, the records cannot be altered, because they are linked to every transaction record that came before them (hence the term "chain").

Figure 1. Basic features of the blockchain technology



Source: Yurcan 2016.

Various computational algorithms and approaches are deployed to ensure that the recording on the database is permanent, chronologically ordered, and available to all others on the network.

5. Computational Logic. The digital nature of the ledger means that blockchain transactions can be tied to computational logic and in essence programmed. So users can set up algorithms and rules that automatically trigger transactions between nodes.

In Figure 1 the main characteristics of blockchain technology are presented graphically.

5. Blockchain-based identity system

Blockchain technologies.com [www.blockchaintechnologies.com 2016] is a free resource to help entrepreneurs, investors and consumers learn about the rapidly emerging field of blockchain technologies. With use cases in all fields from finance to identity, the stage is set for blockchain technologies to forever change the way we transfer, store and handle data. As far as blockchain applications in Identity are concerned blockchain technologies make tracking and managing digital identities both secure and efficient, resulting in seamless sign-ons and reduced fraud [www.blockchaintechnologies.com 2016].

Be it banking, healthcare, national security, citizenship documentation, online retailing or walking into a bar, identity authentication and authorization is a process intricately woven into commerce and culture worldwide. Due to the lack of common comprehension and often-unchecked cyberspace of personal information, identity in the context of technology is facing significant hurdles. Events such as hacked databases and breached accounts are shining light on the growing problems of a technologically advanced society, without outpaced identity-based security innovations. Alongside biometrics, blockchain technology offers a solution to many digital identity issues, where identity can be uniquely authenticated in an irrefutable, immutable, and secure manner. Current methods use problematic password-based systems of shared secrets exchanged and stored on insecure systems. Blockchain based authentication systems are based on irrefutable identity verification using digital signatures based on public key cryptography. In blockchain identity authentication, the only check performed is whether or not the transaction was signed by the correct private key. It is inferred that whoever has access to the private key is the owner and the exact identity of the owner is deemed irrelevant.

Blockchain technology can be applied to identity applications in the following areas [www.blockchaintechnologies.com 2016]:

– Digital Identities,
– Passports,
– E-Residency,
– Birth Certificates,
– Wedding Certificates,
– IDs,
– Online Account Logins,
– Many More.

5.1. The Relationship between blockchain and digital identity

According to Gautam Hazari [Hazari 2016], technical director of GSMA [1982], „Identity" is a word often used to mean subtly different things. The Oxford English Dictionary defines it succinctly as „*The fact of being who or what a person or thing is*"; The ISO Standard 29115 [ISO/IEC 2013] prefers the broader „*Set of attributes related to an entity*". Identity, therefore is not a singular characteristic but rather a set of attributes that vary by relationship and moreover the plurality of these relationships can enhance the confidence level that the identity being asserted is genuine through corroboration.

In the physical world this is fairly straightforward. A government institution for example, can attest the photograph, name and address of a citizen; these can then be corroborated through identity checks conducted by banks or telecommunication providers, who are regulated to „know their customers" hence enhancing the confidence level of the attributes associated with a given identity and hence the identity itself.

Digital identities need to function in a similar way, but the nature of the digital world makes it much harder. In particular, some of the key challenges that digital identity faces include:

– Establishing **trust** in the trustless digital world,
– **Decentralization**: control and ownership of the identity attributes,
– **Immutability** of the operations related to the digital identity.

These requirements are also the fundamental building blocks behind blockchain. Here, the user's identity starts its journey into the blockchain as a self-asserted block, containing the user's identity attributes (hashed) and the user's public key, all signed with the user's private key. At this stage, the level of confidence in the user's identity is at base level.

Other entities, such as a bank or electricity provider, with which the user has a relationship, are also represented within the blockchain, with their own sets of hashed attributes and public keys. These entities can establish relationships with the user by signing the particular hashed attributes of the user that are relevant to that relationship. For example, the Passport Office could sign the hashed address, name, and photograph of the subject if the attribute values asserted by the user match those on record at the Passport Office.

As more and more relationships are established for the user within the blockchain, confidence in the accuracy of the attributes – and hence the identity itself – grows organically. In addition, as more transactions take place involving the user (with other users or entities verifying or trusting the hashed attributes of the user), the „reputation capital" of the identity also grows. In other words, confidence in the identity's accuracy increases as does confidence in the trustworthiness of the person behind it, based on what they do online – all of which is transparent, and visible to anyone via the blockchain. If any of the relationships change between the user and the entities, the change can be established within the blockchain as a separate block with a cryptographically signed timestamp hence enabling any new verifier to observe both previous and current relationships in a cryptographically protected sequence.

The block representing a digital identity in the blockchain is identified using the public key associated with the user, and the corresponding private key is the credential that the user needs to keep protected. In a sense, therefore, the public key can be considered equivalent to a user ID and the private key equivalent to a "password" or biometric [Hazari 2016].

5.2. Problems with the current state of identity systems

In a recently published *White paper* on the creation of a platform for identity Christian Lundkvist, Rouven Heck, Joel Torstensson, Zac Mitton and Michael Sena [Lundkvist et al. 2016] described the many problems with the current state of identity systems and proposed the creation of an identity system that aims to be a flexible and easy-to-use method of interacting with decentralized applications as well as off-blockchain identity related tasks.

Digital identity is fragmented and siloed between various service providers, prohibiting a holistic view, and delivering poor user experience necessitating repetitive registrations and logins with usernames and passwords. This results in insecure systems where people use the same password for many of their sites. The centralized servers of identity providers like Google and Facebook are honeypots of data, so they're economically valuable for hackers to attempt to

crack. The upcoming reliance on billions of internet-of-things devices makes it untenable to have all those devices controlled by a centralized identity provider, since a breach of this provider would prove catastrophic to not only digital but also physical infrastructure.

Public/private key cryptography and decentralized technologies like blockchains offer a promising solution to the problems mentioned above. These technologies push ownership of identity away from centralized services to the edges – to individuals – so that the identities themselves are in control. This is commonly referred to as self-sovereign identity. This approach decentralizes data and computation and pushes them to the edges, where it is less economically valuable to hackers because it would require a lot of effort to hack many individual identities one-by-one. However, introducing new technologies to end-users is difficult. Public-key cryptographic tools like PGP [2017] have been around for 25 years, but their use in digital identity systems have seen little use due to their unintuitive and complex user experience, and the fact that usernames and passwords work well enough for most people.

Blockchain technologies are interesting in that they require the use of cryptographic keys to sign messages for each interaction of the blockchain. Thus the rise of cryptocurrencies like bitcoin and general blockchain architectures like Ethereum [Buterin 2017] have sparked new interest in making public key cryptography usable to regular consumers and users in order for them to interact with these systems.

Interactions with blockchain based systems necessitate usable public-key cryptography, and up to this point the key management solutions (commonly called „wallets") have been difficult to use for non-technical users. Interestingly the blockchain can itself help make public-key cryptography more usable and secure by acting as a decentralized public key infrastructure (PKI). The blockchain can be viewed as a decentralized certificate authority that can maintain the mapping of identities to public keys. Smart contracts [wikipedia.org 2017b] can furthermore add sophisticated logic that helps with key revocation and recovery, lessening the key management burden for the end user.

This whitepaper has presented uPort, an identity system that aims to be a flexible and easy-to-use method. The system aims to abstract away the public key cryptography from the end user to make the user experience intuitive. A mobile app holds the user's private key and a smart contract address acts as their identifier. A novel identity recovery mechanism is used to let the user select friends from their contact list which gives a quorum of these friends the ability to recover the identity of the user if their mobile device is lost.

5.3. Recent initiatives of Azure.microsoft and Deloitte UK

Yorke Rhodes III [Rhodes III 2017] of Azure.microsoft explained that the ID2020 forum (compare p. 1) has provided an opportunity to bring together the technology sector with those who best understand the social and cultural challenges in question. While they do not profess to have solutions to these overwhelming problems today, they can start where the open source community is best: collaboration. To progress toward these goals they have been working with partners to address identity using the self-owned or self-sovereign qualities of blockchain technology.

Microsoft is collaborating with partners and developers across the globe on an open source, self-sovereign, blockchain-based identity system that allows people, products, apps, and services to interoperate across blockchains, cloud providers, and organizations. Their goal in contributing to this initiative is to start a conversation on blockchain-based identity that could improve apps, services, and more importantly, the lives of real people worldwide by enabling self-owned or self-sovereign identity. An implementation of self-sovereign identity can be established using the qualities of blockchain based systems and Microsoft has chosen to start collaborating with two partners with considerable blockchain identity expertise. It is working with Blockstack Labs and ConsenSys to leverage their current Bitcoin and Ethereum-based identity solutions, Blockstack [Blockstack… 2017] and uPort. Through this open source collaboration they intend to produce a cross-chain identity solution that can be extended to any future blockchains or new kinds of decentralized, distributed systems.

There are many questions that remain unanswered, but Microsoft can imagine a world where an individual can register their identity in a cross blockchain fashion, providing a single namespace for lookup regardless of blockchain of choice. The self-sovereign nature of the solution enables many scenarios and becomes an asset owned by the individual, with attributes doled out on a time bounded basis only to parties with a need to know. An open source framework will be made available on Azure, where developers will be able to quickly set up an instance and begin exploring how an open source identity layer can benefit their applications.

Another initiative was mentioned in May 2016 at the conference in New York [The Blockchain Team... 2016] where the Blockchain team of Deloitte UK announced the development of its Smart Identity prototype. Smart Identity is a solution which will allow users to create a universal digital identity powered by blockchain technology. The solution is at proof of concept stage and Deloitte will call for greater collaboration to work towards standardized identity protocols.

The Smart Identity solution will allow users to create and control all aspects of their digital identity within a highly structured and accessible environment.

Smart Identity will function as a digital account containing the information and credentials needed for trusted digital interaction.

Deloitte is developing a number of initial applications for Smart Identity, including [The Blockchain Team... 2016]:

– **Access management**, using a single digital key to access any identity-restricted location, from website single sign-on, to physical buildings, smart vehicles and ticketed locations such as event venues or airplanes.

– **Automated identification and verification of customers**, including people, organizations, and robots, either at sign-up or on a real time transactional basis.

– **Identification and tracking of assets of any form**, from vehicles and property to pharmaceutical products and commodities such as oil or farming produce.

– **Transactions**, empowering devices or „Things" to obtain and transact using recognizable and standardized identity, enabling them to manage assets and to securely interact with other devices, people, or organizations.

– **Digitization of traditional identity components** such as driving licenses and passports, into a single, versatile digital record.

Stephen Marshall [2016], head of financial services technology at Deloitte UK, said: „Our analysis and experimentation into the capabilities and applications of blockchain technology has led us increasingly to the question of identity. New distributed platforms are set to rewire our digital economy and in order to make the most of this opportunity, we must first solve the problem of digital identity".

„The Smart Identity solution will take the first step in evolving digital identity from a disparate record-set into an empowered and verifiable digital entity. However, it is early stages and there are many obstacles that must be overcome before we see a standardized identity solution in place. At the conference, we are calling on businesses to collaborate with us to help develop a solution that works across all industries and sectors".

6. Conclusions

At the United Nations a hub named ID2020 was created that should harness emerging digital technologies to create the world's largest innovation platform in support of Sustainable Development Goals (SDG) providing legal identity for all, including birth registration. Presently:

– 1.5 billion people are without proper identification, that's one-fifth of the world's population,

– One in three children under the age of five does not officially exist because their birth has not been recorded,

– Cumulatively, 230 million children under the age of five have no birth certificate; this number is growing,

– 50 million children are born without legal identity each year.

As is well known, without legal identification, children and people are invisible to society which makes them most vulnerable to trafficking, prostitution and child abuse.

The May 20th, 2016 Summit on Identity and alignment to the UN's Sustainable Development Goals – ID2020 forum has provided an opportunity to bring together the technology sector with those who best understand the social and cultural challenges in question. While there are not yet solutions to these overwhelming problems today, collaboration should be started where the open source community is best. To progress toward these goals a common work was initiated with partners to address identity using the self-owned or self-sovereign qualities of blockchain technology. Blockchain identity should be primarily an enabler to applications and services that we could not conduct previously online, or at least they should provide a tangible benefit that is an improvement to something else we were doing prior. Of course, there are many obstacles that must be overcome before one can see a standardized identity solution in place. Nevertheless, finally the public administration will have a new digital opportunity to ensure the security and protection of life and property of the members of the society by maintaining proper law and order.

Literature

Blockstack – a New Decentralized Internet, 2017, https://blockstack.org [access: 21.09.2017].

Buterin V., 2017, *Ethereum, Platform Review; Opportunities and Challenges for Private and Consortium Blockchains*, https://en.wikipedia.org/wiki/Ethereum [access: 15.06.2017].

Definitions and Explanations to Understand Blockchain Technologies, www.blockchaintechnologies.com/about [access: 6.12.2016].

Everledger, 2017, www.everledger.io [access: 15.06.2017].

GSMA, 1982, *GSMA-formed in 1982 by the Confederation of European Posts and Telecommunications as a Pan-European Mobile Technology Organization*, www.gsma.com [access: 15.06.2015].

Hazari G., 2016, *The Relationship Between Blockchain and Digital Identity*, November 10, 2016 Blog, www.gsma.com/personaldata/the-relationship-between-blockchain-and-digital-identity [access: 10.11.2016].

Iansiti M., Lakhani K.R., 2017, The Truth about Blockchain, *Harvard Business Review*, January-February 2017 issue, pp.118-127, https://hbr.org/2017/01/the-truth-about-blockchain [access: 12.12.2017].

id2020.org, 2016a, http://id2020.org/partnership [access: 10.12.2016].

id2020.org, 2016b, http://id2020.org/news/2016summit [access: 10.12.2016].

ISO/IEC, 2013, *ISO/IEC 29115:2013: Information Technology – Security Techniques – Entity Authentication Assurance Framework*, www.iso.org/iso/catalogue_detail.htm?csnumber=45138 [access: 5.09.2016].
Krawisz D., 2016, *The Proof-of-Work Concept*, Satoshi Nakamoto Institute, http://nakamotoinstitute.org/mempool/the-proof-of-work-concept [access:10.12.2016].
Lundkvist C., Heck R., Torstensson J., Mitton Z., Sena M., 2016, *Uport: A Platform for Self--Sovereign Identity*, Draft version White paper, https://uport.me/library/pdf/whitepaper.pdf [access: 10.12.2016].
Marshall S., 2016, *Blockchain Enigma. Paradox. Opportunity*; Forward, p. 1, deloitte-uk-blockchain-full-report.pdf [dostęp: 10.12.2016].
Nakamoto S., 2008, *Bitcoin: A Peer-to-Peer Electronic Cash System*, www.bitcoin.org/en/bitcoin--paper [access: 5.06.2016].
PGP, 2017, www.pgpi.org/doc/pgpintro [access: 10.12.2016].
Rhodes Y. III, 2017, *What Does Identity Mean in Today's Physical and Digital World?*, https://azure.microsoft.com/en-us/blog/what-does-identity-mean-in-today-s-physical-and-digital-world [access: 10.12.2016].
Tapscott D., Tapscott A., 2016, *Blockchain Revolution*, New York: Portfolio/Penguin Random House.
The Blockchain Team of Deloitte UK, 2016, *Blockchain Enigma. Paradox. Opportunity*, Deloitte LLP 2016, www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk--blockchain-full-report.pdf [access: 10.12.2016].
UK Government Chief Scientific Adviser, 2016, *Distributed Ledger Technology: beyond Block Chain* (GS/16/1), a report, www.gov.uk/government/organisations/government-office-for--science [access: 10.12.2016].
Why Identity, 2016, http://id2020.org [access: 10.12.2016].
wikipedia.org, 2016, https://en.wikipedia.org/wiki/Bitcoin_network#Bitcoin_mining [access: 15.09.2017].
wikipedia.org, 2017a, https://en.wikipedia.org/wiki/Blood_diamond [access: 15.09.2017].
wikipedia.org, 2017b, https://en.wikipedia.org/wiki/Smart_contract [access: 15.09.2017].
www.blockchaintechnologies.com, 2016, www.blockchaintechnologies.com/blockchain-identity [access: 10.12.2016].
www.managementstudyguide.com[1], 2008, www.managementstudyguide.com/role-of-public-administration-in-modern-state.htm [access: 10.12.2016].
www.un.org, 2016, www.un.org/sustainabledevelopment/sustainable-development-goals [access: 10.12.2016].
Yurcan B., 2016, *How Blockchain Fits into the Future of Digital Identity*, American Banker, Bank Technology, Dec 24, www.americanbanker.com/bank-technology [access: 28.12.2016].

Zastosowanie w administracji technologii rozproszonej księgi. System identyfikacji oparty na technologii *blockchain*

Streszczenie. Administracja publiczna musi być w stanie spełniać długoterminowe zapotrzebowania, które mogą wyniknąć ze zmian w technikach administracyjnych lub zmian w środowisku społecznym. Wpływ technologii, włączenie nowych zasad zarządzania, z uwzględnieniem rachunków

[1] An educational portal launched in 2008 with the vision of providing students and corporate workforces worldwide with access to rich, easy to understand, frequently updated instruction on many management related topics.

potrzeb i aspiracji klienta końcowego, to tylko niektóre z nowych trendów w dziedzinie administracji publicznej. Istnieje powszechne przekonanie, że tożsamość jest podstawowym prawem człowieka. W dniu 20 maja 2016 r. na konferencji zorganizowanej przez Organizację Narodów Zjednoczonych uczestnicy zastanawiali się, jak zapewnić indywidualną tożsamość cyfrową dla każdej osoby na naszej planecie. Główne zobowiązania uczestników konferencji, to przyczynienie się do osiągnięcia wspólnego celu cyfrowej tożsamości. Publiczne i/lub prywatne klucze kryptograficzne i zdecentralizowane technologie, takie jak *blockchain*, oferują obiecujące rozwiązania problemów związanych z tożsamością cyfrową. Tożsamość oparta na technologii *blockchain* ma umożliwić skorzystanie z wielu usług w poufny sposób, bez konieczności obecności fizycznej. Z drugiej strony, *blockchain* jest zasadniczo technologią obiecującą i, jak każda obietnica, do urzeczywistnienia się potrzebuje czasu. Korzystając z najnowszych dostępnych informacji (głównie ze źródeł internetowych), w tej pracy przybliżono proces rozwiązywania problemu przyznania tożsamości wszystkim członkom populacji światowej oraz opisano pierwsze próby zastosowania w tym celu technologii rozproszonych – *blockchain*.

Słowa kluczowe: administracja, tożsamość cyfrowa, technologia *blockchain*