POLICY PAPER

CRYPTOSYSTEMS AND THEIR POTENTIAL IN THE PRIVATE AND PUBLIC SECTORS

The F. A. Hayek Foundation, 2016

Nadácia F. A. Hayeka

Friedrich Naumann STIFTUNG FÜR DIE FREIHEIT

4LIBERTY.eu ...FREEDOM MATTERS

MATÚŠ POŠVANC (1977)

Matúš Pošvanc is the director of the F. A. Hayek Foundation Bratislava, one of the leading pro-market oriented think tanks in Slovakia. After graduation, he worked on various projects aimed at promoting reforms of the functioning of public sector towards market and free economy. He is a senior advisor for several Slovak business organizations such as the National Union of Employers (one of the leading entrepreneurs association is Slovakia), and Entrepreneurs Association of Slovakia (the oldest entrepreneur's association), in the area of monitoring of the adopted legislation and its impact on the business environment. Regularly he presents his views in Slovak media on economic issues, precious metals and cryptocurrency. He is the author and co-author of numerous publications, articles and studies. Since 2012 he writes a regular blog on the current events on the bullion markets on the web portal www.viagold.sk. Equally he is interested in cryptocurrency – the technology of the future.

KEY WORDS

cryptosystems, cryptocurrencies, Bitcoin, public services, financial services, transparency, effective public administration.

ISSUES ADDRESSED

What are the principles of functionality of cryptocurrencies, or cryptosystems? What kind of technological evolution do they introduce? What are the basic possibilities of their applicability in the private and public sectors?

AUTHORS

Matúš Pošvanc, Andrej Cabaj, Tomáš Havran, Martin Lindák, David Stancel, Andrej Thurzo

EDITOR

Ján Oravec

Contents

1. Abstract

Currently, there is already relatively widespread awareness of the existence of cryptosystems, and/or cryptocurrencies and their applicability in the financial sector. Today, the best-known cryptosystem, i.e. cryptocurrency is Bitcoin. However, not many people recognise the revolutionary potential which cryptosystems entail – the paradigm shift in many social phenomena, not only those of a financial nature.

At present, society has to tackle many problems, especially in the public sector. To name a few: financial transparency, transparency in decision making, the complicated administrative burden of citizens and entrepreneurs, relatively slow and inefficient communication of the public sector with citizens. There are also many issues regarding the interoperability of IT systems within the public sector, the use of public resources for administration and the actual implementation of public policies, the lack of transparency in government procurement, and the common practice of bending the rules. Last but not least is the issue of directness of any form of social assistance by the State (subsidies for transport, welfare, education, culture, etc.).

Technology, which entails cryptocurrencies, allows for the shift of these solutions to a whole new level of operation. Cryptosystems enable society to trust automated activities, which are now carried out by the large public apparatus, without the necessity of this apparatus. They provide immutable and secured data to the users of public databases in an automated way, while ensuring a high level of transparency in public procurement and public decision making. They also allow for the programming of cashflow within the public sector, the addition of further conditions and rights for users of welfare services (transport, education, social services), and predefine the circumstances under which these services are used in an automated way. We may state that, in future, crypto-technologies will enhance the efficiency of the way in which society functions.

2. Description and principles of functions

A cryptosystem, or cryptocurrency, is a technology that exists in the virtual world. Currently, the best-known cryptosystem is called Bitcoin. It is not only the most famous, but also the most advanced and safest cryptosystem of all. Other cryptosystems may be of a similar nature, or directly or indirectly derived from Bitcoin, with slight nuances in the overarching philosophy. We begin our study with a brief description of how Bitcoin functions. This report may serve as an introduction to the understanding of cryptosystems and their functionality.

The Bitcoin network solves the problem of having a trusted third party in transactions between two entities, by replacing it with cryptographic (mathematical eals with transactions, the term "cryptocurrency" has become commonly used for its description.

The way it operates is quite simple and is carried out like a regular banking transaction with slight differences. Each participant in the transaction owns a public key – an address that is similar to a bank account – and a private key which is analogous to a password or PIN, entitling the owner to dispose of Bitcoins in a personal account. The difference between a bank and Bitcoin is that, while your bank account and password are assigned by the bank, in the Bitcoin world this pair of interconnected keys (private and public) is generated by the software downloaded from the Internet to your PC or mobile phone.

However, the transaction itself functions in a fundamentally different way from that which we are used to in the banking system. The bank's internal system ensures that the sender's account will be debited with the amount claimed and credited to the recipient. To carry out this operation, the bank needs to know the identity of both parties involved. This makes the transaction itself more costly, along with the necessity of personal data protection. It also extends the time necessary for the transaction's realisation and finally, based on the decision of the bank or other institution, it allows the transaction to be reversed at any time.

In the Bitcoin ecosystem, there is no one to carry out the operation as described above, nor does the Bitcoin system need to know all the identities which are using the addresses. Bitcoin deals with this issue by using a public, and absolutely transparent ledger, called the blockchain.

The blockchain is an accurate record of all transactions in time sequence, indisputably established by cryptographic methods during the process which is known as mining. Mining is a set of operations designed to collect all current transactions, verify whether they are signed by the authorised holders of the relevant addresses (accounts), check the required balances, and confirm transfers to the new addresses.

The whole process is carried out as a set of final transactions collected in a block. This block matches a special digital fingerprint – hash. The hash confirms the validity of ongoing operations and their constancy. Thus, each new block contains a fingerprint – hash – of the previous block and the list of the other new transactions. This means that the blocks form a mutually interdependent chain of blocks.

Anyone who installs the software can become a participant of the Bitcoin network. The system allows the participant to create transactions by generating addresses with associated private keys to transmit the transaction request to the miners in the network to confirm the transaction.

Miners are specialised network associates who provide the confirmation of transactions and immutability of these transactions by finding a unique blockhash. They are motivated by a reward in the form of newly mined Bitcoins and transaction fees. The result must be approved by the absolute majority of the participants in the network, in order to receive the compensation. As the number of Bitcoins is limited (21 million), the reward for miners in the form of new Bitcoins decreases. The compensation comes from an increasing number of transactions, thus the fees for them.

Miners are continually forced, by mutual competition, to confirm the block as quickly as possible. It usually takes approximately 10 minutes. Only the fastest one receives the whole reward. In order to keep a constant rate of this time interval, the network constantly modifies the cryptographic mechanism for finding a blockhash. This process is also called the parameter of network difficulty. If one of the miners manages to find the right hash sooner than in 10 minutes, difficulty in finding the next block would increase exponentially. On the other hand, the time for finding it would extend and the difficulty would decrease proportionally. This automatic process forces miners to invest their resources continually in the new computing power to withstand the competition.

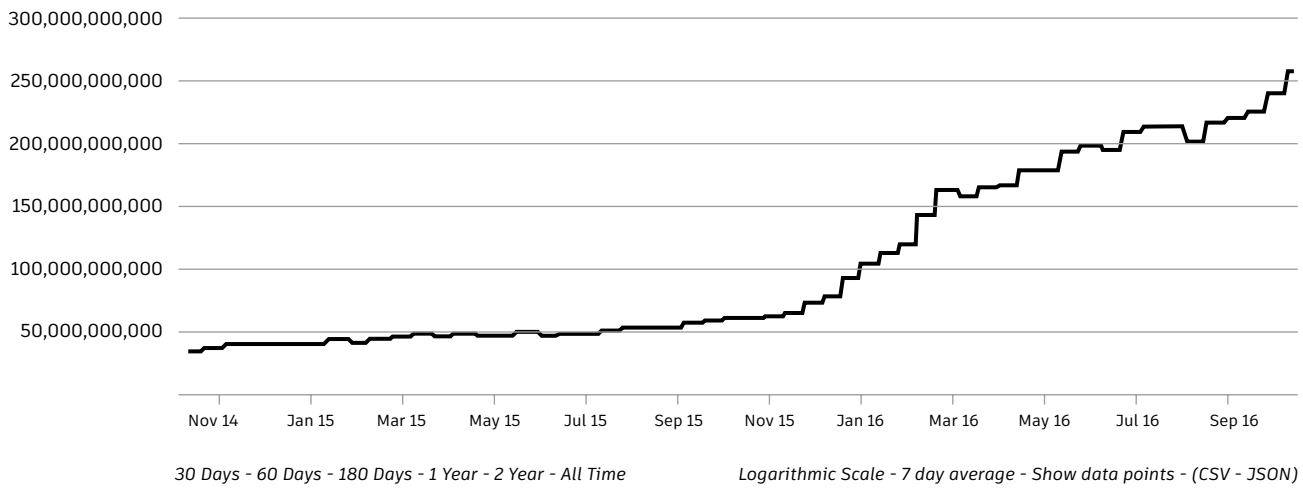
We may state that, through the automated cryptographic blockchain, the Bitcoin network can carry out the transactions transparently without an institutionalised third party or the personal data of subscribers. The process is guaranteed by the democratic power of the absolute computing performance of the participants themselves.

The revolutionary potential of Bitcoin and other similar cryptosystems stems from the technology that underpins its form – the blockchain. The blockchain operates as a register or ledger, in which the history of all transactions ever made is recorded. The overarching cryptography protects the immutability of the history. What is important is that the blockchain's properties make it not only public and immutable, but also almost impossible to hack. We can rely on its immutability and accuracy without any assurance from a third party. This set of otential of cryptosystems which we further elaborate on below.

Difficulty

A relative measure of how difficult it is to find a new block. The difficulty is adjusted periodically as a function of how much hashing power has been deployed by the network of miners.

Source: blockchain.info



3. Cryptosystems: the change of paradigm

The above-defined features and potential uses might not seem revolutionary at first glance. However, we dare to claim the opposite. There is a fundamental difference in the way our world operates, when compared with crypto-technologies, which can be more broadly described as follows.

In the current "centralised" world, in many areas, consumers often rely on decisions of third parties, whether of a bank, notarial services, State institutions and administration, public registers, or clearing houses, behind which there are always humans. Users trust them because they have to (public sector), or because of their good reputation. This system has been present in our society for thousands of years. Users have always had to trust a third party. In many cases, this was so only because of insufficient technology that was incapable of sending information, transferring money, or reaching a consensus without having a trusted third party involved.

In the decentralised world of cryptosystems, consumers rely on an automated decision that is kept within the predefined limits by the use of cryptography and mathematical laws. At present, based on the example, the user entrusts money to a bank, which represents the trusted third party. The third party has the full faith of the user, who believes that he or she is transferring money to another client´s account, one who also trusts the third party. In the world of cryptocurrencies, this transfer is carried out directly, for example, between two persons. Mathematical laws and cryptography ensure that no user can deceive anybody else – e.g. copying a Bitcoin twice or spending it twice. It is not the "trusted" third party, but Maths and its laws which guarantee the credibility of transactions and user activities. An important and significant aspect is that cryptosystems may provide consensus among many actors who often have different motivations. This is especially so in the case of someone wanting to attack the given consensus from the outside (e.g. a hacker).

Given the above, a question we should ask is: what are the implications of cryptosystems for the future of our society?

> IT IS NOT THE "TRUSTED" THIRD PARTY, BUT MATHS AND ITS LAWS WHICH GUARANTEE THE CREDIBILITY OF TRANSACTIONS AND USER ACTIVITIES. AN IMPORTANT AND SIGNIFICANT ASPECT IS THAT CRYPTOSYSTEMS MAY PROVIDE CONSENSUS AMONG MANY ACTORS WHO OFTEN HAVE DIFFERENT MOTIVATIONS.

4. The fields of utility

The above-described features explicitly indicate that cryptosystems are clearly useful in financial transfers. They allow equivalent financial value to be sent around the globe; quickly and directly between users, at lower costs compared to the currently existing systems geared to transfer financial value. However, this is not the only possible application.

In general, there is an ongoing discussion about the application of cryptosystems in areas other than just in finance. Many small IT companies are contributing to this debate within their "Bitcoin 2.0" projects. At present, it is assumed that technology will disrupt many sectors, both in business and the everyday lives of people.

In the following text, we outline five areas in the private sector, and broader five areas in the public sector, where the use of cryptosystems can dramatically change the methods of operation.

4.1 POTENTIAL USE OF CRYPTOSYSTEMS IN THE PRIVATE SECTOR

There are various possibilities for the utilisation of cryptocurrencies in the private sector. It is most likely that the private sector will start to use this technology sooner than the public sector. So which areas seem to be the most interesting in terms of the application of the technology?

4.1.1 Financial clearing

One of the possible options that is being strongly debated is the application for financial clearing within global trade – a replacement for the already "old-fashioned" SWIFT mechanism. One company is already taking up this challenge, with its crypto-currency called Ripple. Although not very popular in the Bitcoin community due its partly centralised nature, some banks have already decided to implement it.

4.1.2. Use of sidechains in financial services

The Bitcoin cryptosystem is relatively slow for contemporary trading of instruments on stock exchanges. The verification time – 10 minutes – is not fast enough for today's high-frequency trading system that takes place in milliseconds. However, there is already an emerging concept of what is called "sidechains" being considered. Sidechains are independently operating registers that will not be hampered by the relatively slow Bitcoin infrastructure. They would allow different types of trading and the Bitcoin – as the most trusted system – would only be used as a clearing function among traders where the 10-minute frequency is sufficient.

4.1.2 The Internet of Things

Imagine a user arriving at a cinema and paying for the ticket with cryptocurrency, by placing a mobile phone on the turnstile that allows him entrance. He goes to the seat he has paid for, attaches the phone, and the seat automatically reclines. And finally, he can watch the movie. Or let us imagine a drone flying in through a customer's window (or directly to the customer, wherever he is). It delivers a package, a pizza or any other product. The customer attaches the mobile phone, which scans a confirmation of payment in the given cryptocurrency, and the drone subsequently delivers the product to the customer.

When dealing with the Internet of Things, the execution of a transaction and its detection can be set up by automated pre-set instructions, which may serve to manage almost everything that can be connected to electricity or another energy source. Cryptosystems ensure that the management of these facilities will not be misused by third parties' adverse actions.

4.1.3 Subscription of shares

Currently, it is very difficult to realise the subscription of shares or any other instruments on the stock exchange. Of course, it is not impossible, but the action is often a financially and resource-intensive

process. This problem does not apply in the world of cryptosystems. Share subscription, its property records and trading on decentralised marketplaces, is probably one of the other areas in which cryptosystems will be used very soon. Systems such as Omni and Counterparts are already trying to develop this kind of service.

4.1.4 Decentralised data repositories/decentralised Internet

Everyone has already encountered the problem of leaked personal data of the clients of some companies. Decentralised applications would avoid such issues. Some of the projects intend to move security of the Internet on to a whole new level—not only to securely store and automatically encrypt data–, but also to retrieve data almost instantly. This can be useful for securing websites, electronic communication within the financial system, and electronic communication in general. Projects like MaideSafe aim to acquire these and similar features.

4.2 POTENTIAL USE OF CRYPTOSYSTEMS IN THE PUBLIC SECTOR

At present, the use of information technologies in the public sector is very frequent. Information technologies reduce the administrative burden on business, facilitate communication with citizens and increase the transparency of the public sector. Besides the traditional use of cryptocurrencies for clear, efficient and auditable payment of taxes and duties (ranging from Income Tax, VAT in the whole chain of payments, to any kind of fees), cryptosystems may be implemented in other areas with the effect of saving resources, improving transparency and the practical usage of public resources.

4.2.1 Public procurement

The area of public procurement is one good example of the adoption of crypto-technology. Government contracts usually include public works, services, and supplies performed by public institutions. At the same time, this is one of the most criticised fields in Slovakia. Experts mention the lack of transparency, and the circumvention and illegal adaptation of the rules.

> PUBLIC TENDERS ORGANISED BY GOVERNMENT AGENCIES CAN BE MORE TRANSPARENT, AUTOMATISED AND SELF-ENFORCEABLE BY USING WHAT ARE KNOWN AS "SMART CONTRACTS" WHICH ARE IN CHARGE OF THE WHOLE PROCESS.

Public tenders organised by government agencies can be more transparent, automatised and self-enforceable by using what are known as "smart contracts" which are in charge of the whole process. Transparency could be achieved by blockchain technology (Bitcoin or its specialised derivative), used in the announcement of government contracts. In this way, everyone would be able to verify that the best offer has actually won the tender. At the same time, it would not be necessary to publish the identity of all those involved, if undesirable. All offers for bids can be pseudo-anonymous, because the addresses in blockchain do not have to be connected to real identities behind them. Despite this fact, any participant in the tender would be able to provide unequivocal evidence of the interconnection of his or her actual and virtual identity by using digital signatures.

Automatisation of procurement could be increased up to the point when the smart contract will automatically select the most advantageous tender (i.e. less costly) after the expiration period specified for the receipt of bids. Subsequently, another conditioned (Escrow) contract can deal with the remu-

neration payment after the fulfilment stated in the previous contract. Compensation would be released after receiving input from the credentials. In the event that a supplier does not deliver the agreed services or goods, the funds would be automatically returned to the contracting authorities. In the event of the realisation of the order, an applicant could automatically receive references that would automatically refer him or her to other public procurements (e.g. following § 34 of the current Act n.343 / 2015 Coll. about Public Procurement).

Under such operations of public procurement, demonstration of the fulfilment of the other conditions (e.g. regarding §26) could be facilitated for candidates. The system would automatically control the fulfilment of conditions.

4.2.2 Notarial records

We have classified the notarial area as a public service, due to the fact that a Notary is a person who is State-licensed to carry out notarial activities. The set of these responsibilities is granted by the State for an indefinite period.

Transfer of assets, ownership titles, confirmations, agreements, testaments – for the implementation of all these types of records, blockchain technology can be used. The result is a safe record without the possibility of change. There is thus the maximum security rate of authenticity, with a sufficient degree of transparency. Notarial recorded data based on cryptosystems can be used for further operations and their application in the automation of payments, transfer of assets or automatisation of actions without human intervention.

Examples include the automatic fulfilment of conditions in a testament, a transfer of ownership of property based on predefined performance conditions (e.g. the implementation of payments for purchased assets), and the automatic realisation of sanctions in the case of failure to meet contractual conditions.

4.2.3 Registers

We can envisage the implementation of blockchain technology in the creation and use of any public register. Applying data will meet the criteria of inalterability, guaranteed authenticity and non-vulnerability, all with a sufficient degree of privacy and transparency. The data will also be accessible at anytime by any electronic device. This solves many problems which current IT solutions bring about.

The “National Concept of Public Administration in Slovakia” points to the usefulness of cryptosystems in dealing with actual problems in this area. It is aimed at the rationalisation of the running of an information system by government cloud and enhances the protection and security of the data. The result should be the rationalisation and streamlining of public administration for the State, citizens and businesses.

This is the area where it is meaningful to consider the use of cryptosystems in future. One of the projects dedicated to this issue is “Factom”.

Example of decentralised register. The Factom project.

The Factom project has existed since September 2015. It is focused on the creation and maintenance of registers and databases. The name Factom comes from the Latin word “factum” which means “what is stated is true.” Factom is a cryptosystem which uses Bitcoin blockchain and recently Ether (another cryptocurrency) for secure storage of records and data. The data entries can be realised by public or private institutions. The data embedded in Factom are inerasable and immutable. They are not at risk by any third party in the form of an attacker (hacker), and are credible.

Factom system utilisation

The system is easiest to describe regarding its users. On one hand, there is the perspective of the State institution that is interested in, for example, keeping track of its citizens, with the data being secured and user-accessible, editable or erasable. On the other hand, there will be people who use the database for its interoperability with other databases, which simplifies the administration associated with verifying and using the data in question, while making them accessible only to the rightful data owners.

In the case of the Factom cryptosystem, the public institution in the development of the database must follow the next steps. First of all, it has to purchase Factum currency – known as Factoids. Factoids may be compared with Bitcoin. It is perceived as a financial unit – the system´s token. The

purchased Factoids are held in an electronic wallet. Subsequently, the government institution buys the rights to collect data into the system. These rights are called "entry credits".

A subscription of one gigabyte of data into the Factom system currently costs approximately $2 000. On one hand, the price is several times higher than the price of secured cloud services as it depends on the cloud provider, the quantity of data stored, and especially on the time for which they are saved (data storage is paid for annually). On the other hand, the Factom cryptosystem provides the possibility of establishing a highly secure database, with the practical impossibility of changing the data without notification to the user (e.g. the State), whose inscription is practically perpetual. Within the cryptosystem, it is also possible to link individual registers, for example, personal data with medical or criminal records.

Description of how Factum works

The absolute smallest unit is called the "entry file" (in our specific case – specific data about a citizen), which the user (the State) inserts into the generated database (i.e. chain).

The databases (chains) may be imagined as folders containing the data. Each folder is designated for different data. One folder would only include the data about the population, and another folder would include only medical records. It can never happen that the data with medical records get into the folders with population data. On one hand, it would not get through the rules which could be defined by every user at the beginning. On the other hand, each inserted entry has its "ID chain". This is an identification number of entered data, based on which of the data are stored in individual objects of databases (chains).

The government could, for instance, define a database which would also take into account legislative or other criteria. Of course, legislative changes could be reflected in the database by incremental actualisation. The potential utilisation of such databases is massive, depending on the user and nature of the data.

Security

The system is secured by a high level of cryptography. Every minute the chains (databases) are assigned to the upper layer, which is a block of chains consisting of several chains. Those are stored in the top layer – called the "direct block". A single direct block is created at the end of every minute, where the blocks of chains are collected. This process is repeated 10 times. After assembly of the 10th direct block, i.e. at the end of the 10th minute, the whole hash of these blocks is created and 10 direct blocks are placed into the Bitcoin blockchain. Thus, all saved data, as well as individual levels of data are protected cryptographically.

It should be noted that Factom is not an ordinary database where a user merely records something. The first entry which the user inserts into Factom is the properties of the database (e.g. the register of citizens in the form of the name, surname, birth number, address, nationality, date of birth, social security number, etc.). The public institution can define the parameters, based on which data will or will not be collected in the system.

Benefits to database users of the Factom system

The first and principal benefit of the Factom system is its safety. This means that no one, except the actual creator of the chain (or database), is able to manipulate it. The second advantage is the aforementioned first input (Entry), the application which may vary in the context of the requirements for the data structure and their functionality. The third benefit is that the system can save the costs associated with security, data leakage and similar. As the fourth advantage, we should mention the possible interoperability between databases.

This may be demonstrated by the following example. Consider a situation when a citizen is applying for a job in the army or police. In this case, it may be necessary to have no criminal record, no serious illness, specific education, possess some proven skills and a driving licence. Government institutions can develop a system which will automatically retrieve the following data from various databases. More precisely, from the criminal and medical records databases, from the driving licence database, the database of educational attainment and certificates of acquired skills. If the system finds that the applicant meets the required criteria, it automatically recommends his or her approval. The system can be applied to other areas, for example, the actual issuing of driving licences, passports, visas, etc.

A potential implementation of the Factom technology encompasses other areas, such as the field of land registers, records of patents, commercial or trade licence register, population records, vehicle register, register of defaulters, etc.

4.2.4 Databases of e-health

As previously mentioned, cryptography has enabled crypto-technologies to become a significant innovation. The encryption provides protection in the electronic virtual world. The highest priority will remain the protection of the data and processes in the health sector regarding their current digitalisation. Digitalisation without online access is only a half measure. However, online accessibility entails particular risks. Some discreet medical data might be more strictly protected than money. Currently, their protection requires patients' trust in the State/hospital/ or another intermediary that stores sensitive data. Crypto-technologies allow for operation in an environment which is not based on trust in a middleman.

Therefore, a paradigm shift in healthcare does not occur only due to virtual reality applications, 3D-printing and bio-printing, but also through the awareness of digitalisation and working with big and valuable data. Already existing applications of blockchain technologies indicate that their primary dominance is decentralisation. Alternative blockchain design provides higher security and lower costs compared to the centralised governmental, often overpriced, e-health solutions with a much lower level of data protection. In the summer of 2016, it was no coincidence when the US government agency decided to apply crypto-technologies to the healthcare sector and announced a public tender for the design of these applications.

In 2015, Health Nautica company joined forces with the above-mentioned Factom project. The main objective was to connect medical record management with the benefits of crypto-technologies. The feature of immutability is of particular importance to medical data. This is a principle which is now, within existing databases, a serious problem. Data modification, or annulment of any part of the records because of any other reason than an existential one means an eternal loss of credibility in that database or system. Nowadays, modification of data by third parties in a generated centralised system may put a patient´s life at risk.

> IF THE SYSTEM FINDS THAT THE APPLICANT MEETS THE REQUIRED CRITERIA, IT AUTOMATICALLY RECOMMENDS HIS OR HER APPROVAL. THE SYSTEM CAN BE APPLIED TO OTHER AREAS, FOR EXAMPLE, THE ACTUAL ISSUING OF DRIVING LICENCES, PASSPORTS, VISAS, ETC.

Let us take the example of encrypted electronic records, part of which the owner/patient has intentionally left partially public (e.g. blood type in case of emergency). This may even be the "Emergency Care Data Set" (ECDS), a broader data set – a unique biometric identifier of the owner/patient which is readily available to ambulance staff. Immutability of the data, at least without majority consensus, is a key aspect of data security. And immutability is what is implied by the nature of cryptosystems. Imagine that a patient him- or herself decides (voluntarily) to whom his or her own securely stored data should be made available. And it may not even be necessary that the State or another centralised institution has to develop this kind of application.

Another example of crypto-technology implementation could be a simple automated, anonymous and rapid procedure in a case when it is necessary to validate a personal competency to grant consent for a particular operation or to exclude the presence of some highly infectious disease, etc. For example, the automated IT system in a turnstile where a per-

son attempts to enter a public swimming pool, children's playground or airport, identifies a particular item in the health records (which are noted on the blockchain of the particular cryptosystem) based on his or her biometric identification, a scan of the fingerprints, etc. The system checks whether there is a specific biosafety threat to others in a given protected area, and according to this validation, will allow or forbid entrance. Safety is ensured without any interaction with a third party or non-encrypted identification, without the necessity to record a given automated demand or revelation of accurate information to the third party (as in the case of centralised systems, e.g. a person who controls the data).

Therefore, the implementation of crypto-technologies into the existing processes in the health sector is logical. This does not only concern the online storage and disclosure of medical records, but also working with big data and dynamic analyses and response to information, for example, at the time of the spread of an epidemic.

Crypto-technologies permit the phasing out of intermediaries from the existing processes which previously required a mediator, whether it was a bank, the State or a healthcare institution which centrally stores data on the health conditions of its patients in the "trust-based" age. If centralised systems were to collapse, there is a technology available that can reliably operate without the precondition of confidence in a third party. In this kind of world, the main implication is that security of the patient´s data will be based on the preferences.

4.2.5 Smart contracts for public services

One of the problems which is presented in the provision of public services and which is often discussed, is directness in the use of any form of social assistance from the State. Social benefits, as well as the access to education, transport services, or any other support policies may be considered as social support. Crypto-technology can partially alleviate this problem, while ensuring that the process is not bureaucratically challenging.

The potential use of cryptosystems in public social support, in combination with protocols such as "coloured coins" will make it possible to construct "smart contracts" and to automatise cashflow in the economy or in some of its sections. It will allow the defining of the purposes and services on which the money will be spent. In principle, it will be possible to create conditional financial contributions that will be spent on a precisely predefined specific purpose – such as healthcare, medicine, food and other goods provided by authorised service providers.

The areas where utilisation may be considered include: educational allowances, public transport (trains, bus transportation, road networks, etc.), government subsidies of various kinds, and social benefit commitments to fulfil other conditions (e.g. property, salary, etc.). An important factor is that the bureaucratic apparatus to monitor and enforce the rules would no longer be necessary, because all the rules can easily be pre-programmed into the token properties of the given cryptosystem. It is even possible to program a feature ensuring that the money is to be returned to the provider, in this case, the State if it is not used by a certain date.

However, that is not all. A public organisation can relatively easily program wage costs, material, and maintenance into its budget. Such a definition of the purpose precludes the use of money for undesired purposes. In addition to this, automatisation of these processes leads to a dramatic reduction of bureaucracy and saves both financial and human resources, as well as time.

5. Brief description of the technical implementation of database entries

The information which can be used directly for entry into the blockchain must meet two essential conditions. The first is precise measurability. This condition corresponds, for example, with the exact number of square metres in Slovakia vs. an exact number of tokens, e.g. Bitcoin tokens (21 million). From this point of view, for example, the Land Register is a good example of direct utilisation of the blockchain. The second condition for immediate implementation is the relationship between the blockchain tokens and e.g. a precisely defined number of square metres in the cadastre. After a complementary pairing of inputs and outputs, the result must be equal to zero, while the unmatched outputs are inputs for future transactions at the end of the chain.

Other types of information cannot be clearly calculated or are constantly growing (e.g. medical history of the population). In these cases, the information cannot be directly written into the blockchain. Given the size of the database, it could grow to infinity, while there would not exist any direct connection allowing annihilation of inputs and outputs. Technically, the absurdity of such a kind of obligation is demonstrated by the impossibility of the checksum execution. The checksum is known from accounting, when assets have to be equal to liabilities. Otherwise, the accounting is not correct and is unreliable. In cryptosystems, the potential non-compliance could be followed by a loss of confidence in the blockchain and its subsequent collapse.

However, the technology of the crypto-world can be adapted to the unlimited records. A medical file may serve as illustration. As we know, it has potentially unlimited information size ("the thickness of a medical record" is different for every person). This digitized record will be encrypted, and can safely be distributed to the users of the whole health system (e.g. insurance companies, hospitals, doctors, etc.) or other potential users (e.g. family, employer, government institutions, etc.). The record might have various degrees of decryption, and assigned access rights.

The cryptosystem´s blockchain can be re-used to access the encrypted files. From a technical point of view, the "multi-signature" transaction allows for the generation of an access key to the present level of encrypted data. Only the owner/citizen (using e.g. a Master Private Key) will have access to all the records. However, in the event of an accident, invited participants, e.g. an emergency service, could generate access rights to the blood type of the patient, according to predefined rules and practical situations. In this case (and similar cases of above–unbounded data), it would be appropriate to have a robust and particularly reliable blockchain (e.g. a specialised derivate of a Bitcoin blockchain) which safely stores records about the time and level of generated access rights.

6. Conclusion

Scarcely anyone can imagine using crypto-technologies in everyday life. However, it is apparent that they are of potential use, not only in the private but also in the public spheres. Crypto-technologies would result in greater safety, transparency, public controllability and automation of many activities, in both the private and public sectors that today require human intervention. These automated actions could be achievable, based on the trust in data and storage registration and their utilisation by means of blockchain technology.

4Liberty.eu is a platform where experts and intellectuals representing the liberal environment from Central and Eastern Europe can share their opinions and ideas. Representatives of 15 think-tanks from various countries, including Poland, Hungary, Slovakia, Czech Republic, Germany, Slovenia, Bulgaria, Estonia, Lithuania, Ukraine and Georgia regularly publish comments, analysis and polemics concerning politics, economy, social and cultural life, as well as the subjects of heated debates in the media shown from a Central European perspective.

http://4liberty.eu/

facebook.com/4liberty.eu

@4LibertyEu