Possible State Approaches to Cryptocurrencies

Jan Lansky
University of Finance and Administration in Prague
Czech Republic
zizelevak@gmail.com

DOI: 10.20470/jsi.v9i1.335

Abstract: *Cryptocurrencies are a type of digital currencies that are relying on cryptographic proofs for confirmation of transactions. Cryptocurrencies usually achieve a unique combination of three features: ensuring limited anonymity, independence from central authority and double spending attack protection. No other group of currencies, including fiat currencies, has this combination of features. We will define cryptocurrency ownership and account anonymity. We will define cryptocurrency ownership and account anonymity. We will introduce a classification of the types of approaches to regulation of cryptocurrencies by various individual countries. We will present the risks that the use of cryptocurrencies involves and the possibilities of prevention of those risks. We will present the possible use of cryptocurrencies for the benefit of the state. The conclusion addresses the implications of adoption of a cryptocurrency as a national currency.*

Key words: cryptocurrency, Bitcoin, anonymity, risk and prevention, state approaches

1. Introduction

First, we need to distinguish between two basic terms: electronic money and digital currency. Electronic money is a digital equivalent of cash. Electronic money is a payment instrument whereby monetary value is electronically stored on a technical device in the possession of the customer. The amount of stored monetary value is decreased or increased, as appropriate, whenever the owner of the device uses it to make a purchase, sale, loading or unloading transaction. A distinguishing feature of transactions carried out with electronic money is that they do not necessarily involve a bank account (European Central Bank, 2000). Electronic money is not the subject of this article.

Digital (or virtual) currency is an electronically issued currency the transferability of which into fiat currency is not guaranteed by the state (European Banking Authority, 2014). Digital currencies may be divided into centralised and decentralised types. Centralised digital currencies are most often issued by a private actor: *e.g.* E-gold (Grow et. al., 2006), Liberty Reserve (Langlois, 2013), WoW Gold (Debeauvais et. al., 2012), Linden dollars (European Central Bank, 2012).

For purpose of this paper, we created following definition of cryptocurrency. Cryptocurrency is a system that meets all of the following 6 conditions:

(1) The system does not require a central authority, distributed achieve consensus on its state.
(2) The system keeps an overview of cryptocurrency units and their ownership.
(3) The system defines whether new cryptocurrency units can be created. If new cryptocurrency units can be created, the system defines the circumstances of their origin and how to determine the ownership of these new units.
(4) Ownership of cryptocurrency units can be proved exclusively cryptographically.
(5) The system allows transactions to be performed in which ownership of the cryptographic units is changed. A transaction statement can only be issued by an entity proving the current ownership of these units.
(6) If two different instructions for changing the ownership of the same cryptographic units are simultaneously entered, the system performs at most one of them.

Cryptocurrencies are decentralised digital currencies. The decentralization is achieved by the p2p architecture. The cryptography is used for decentralized confirmation of transactions. New cryptocurrency units are usually (but not always) put into circulation as a reward for using the computer's computing power for solving complicated mathematic problems which are used by participants on the system to confirm new transactions among participants. The speed of issuing new money is defined for each cryptocurrency upon creation. Although the speed of issuing can be changed by consensus of community, it happens very unlikely. *e.g.* Dogecoin (Borchgrevink, 2014).

Cryptocurrencies are the only type of currencies with the following three features: ensuring pseudo-anonymity, independence from central authority and double spending attack protection. It has taken 25 years (Narayanan, 2016) to ensure that these three features are available at the same time. The research in this area was launched by Chaum (1983) in his paper “Blind signatures for untraceable payments.” The combination of all of the three features was achieved by Nakamoto (2008) in the paper “A Peer to Peer Electronic Cash System.” The first ever cryptocurrency Bitcoin came into existence on 3 January 2009.

We will describe ensuring anonymity, independence from central authority and double spending attack protection in Bitcoin and from its derived cryptocurencies. Some other cryptocurrencies can work slightly different.

Ensuring pseudo-anonymity – A user who follows the relevant rules (Bonneau et. al., 2014) when executing cryptocurrency transactions cannot be easily identified. However, users may reveal their identity either negligently or knowingly, or outside actors may use external data to identify users, and then the cryptocurrency conversely ensures that their transactions are transparent.

Independence from central authority – Cryptocurrencies are decentralised and independent of central authorities empowered to change the consensus rules of the cryptocurrency system. Any changes to the consensus rules can only be achieved by consensus of the majority (usually 75-95%) of the cryptocurrency operators. However, such changes are intended to be rare.

There are two types of changes: soft forks and hard forks. Soft forks are adding features that make consensus rules stricter. Soft forks restrict the set of valid transactions such that the old version of consensus rules would accept all of the transactions, whereas the new version would reject some. Hard forks introduce new features that were previously considered invalid. That is, the new version of consensus rules would recognize transactions as valid that the old version of consensus rules would reject. (Narayanan et. al., 2016)

Because of its lack of central authority, a cryptocurrency cannot be abolished or regulated by force; a cryptocurrency can only cease to exist by itself, when users of the cryptocurrency lose confidence in it (*e.g.* technical attacks, hacks). Nevertheless, individual users of a cryptocurrency can voluntarily decide for a form of regulation of the transactions executed by them.

Double spending attack protection – The owner of cryptocurrency units cannot use the same cryptocurrency units to pay to two different recipients. Once the cryptocurrency units are sent to one recipient, an attempt at sending them to another one is rejected as an invalid transaction. For fiat currencies this problem is not relevant, as physical fiat money is physically transmitted to the first recipient only. For digital currencies, it was difficult to resolve the double spending problem while protection because the properties of ensuring independence from central authority (Rosenfeld, 2012).

2. Literature Review

Cryptocurrency research was started by Chaum (1983), when he drew up the first digital currency system. Chaum et al. (1988) summarises this into several more articles, where various other individual deficiencies of the initial draft of the system were addressed, notably those to ensure anonymity and double spending attack protection. Back (2002) came up with the proof of work concept, which was originally designed to protect email communication against spam. Haber and Stornetta (1997) drew up a data structure that is a predecessor of the blockchain structure, used in cryptocurrencies. The combination of this knowledge gave rise to Bitcoin, the first ever cryptocurrency, which came into existence on 3 January 2009 (Nakamoto, 2008). In January 2016, there were more than 600 cryptocurrencies, of which we regard Factom, designed by Snow et al. (2014), and Ethereum, designed by Buterin (2014), as the most innovative ones (Lansky, 2016). Wolfson (2015) also dealt with the history of cryptocurrencies.

The two following books concern describing Bitcoin and cryptocurrency technologies. The book “Mastering Bitcoin: Unlocking Digital Cryptocurrencies“ by Antonopoulos (2015) is a good tool for programmers who want to implement applications that use cryptocurrencies. The book “Bitcoin and Cryptocurrency Technologies”by Narayanan et al. (2016) also deals with the technical description of the cryptocurrency technology but does not go into such detail. In addition to the technological description itself, the book also marginally addresses social and economic issues.

The European Banking Authority (2014) defined 70 risks related to the use of cryptocurrencies. The New York State Department of Financial Services (2015) has conducted the most comprehensive cryptocurrency regulation for New York to date, called BitLicense. Hansen (2016) updates, on an ongoing basis, a list of individual countries' current positions on cryptocurrencies. Dostov (2014) deals with the options of applying AML to cryptocurrencies. Herrera-Joancomart (2014) deals with the methods of how to reveal the identity of cryptocurrency accounts.

3. Ownership

The functioning principles of cryptocurrencies will be explained with the example of Bitcoin, the oldest cryptocurrency. This explanation is inspired by the Mastering Bitcoin book written by Antonopoulos (2015). For the purposes of this article we have simplified these principles significantly. Cryptocurrencies can be owned through cryptocurrency accounts. A cryptocurrency account consists of a combination of a private key and a cryptocurrency account address. The cryptocurrency account address functions similarly to a bank account number for fiat currencies. The private key is similar to a secret Personal Identification Number (PIN), which can be used to check that the account owner is using the account. Unlike in traditional banking, owner security is weakened because the cryptocurrency account address can be calculated from the private key, and thus the very knowledge of the private key is sufficient to acquire control of cryptocurrency units stored; this is not true of the banking PIN, where the knowledge of the bank account number is also required.

Cryptocurrency technology does not distinguish between the legitimate owner and a successful attacker who has acquired the private key from the owner as a result of the owner's fault. Both the owner and the successful attacker can use the cryptocurrency units stored in the attacked cryptocurrency account for their benefit. The first step of a successful attacker is typically the transfer of all cryptocurrency units stored in the attacked cryptocurrency account to a cryptocurrency account to which only the attacker holds the private keys. The legitimate owner lost cryptocurrency units at this moment. The cryptocurrency technology does not even allow for reversing or cancelling a transaction executed by an attacker.

Private key is a random number within the range of 1 to 2^{256}. There are more possible private keys than atoms in the universe. The security of the stored cryptocurrency units depends on the quality of the random number generating algorithm. It is absolutely inappropriate to create a private key in the same way as a usual password because the potential attacker is not limited at all by the number of attempts at guessing the password, being capable of trying billions of attempts per second. The best option is to create the private key by cryptographically secure pseudo-random number generator (CSPRNG), *e.g.* ISAAC developed by Jenkins (1996).

Private keys can be stored by two different ways: hot wallet and cold wallet. An Internet connected device that stores private keys is called a hot wallet. Hot wallets are exposed to risk of hacking and theft of private keys. Cold wallets (paper, hardware) are offline and more secure. The best option is to have the private key generated and stored by attested software, such as the hardware Bitcoin wallets, *e.g.* Trezor, made by SatoshiLabs (2016) or Ledger Blue, made by Ledger (2017).

4. Anonymity

One individual can even own millions of cryptocurrency accounts for a single cryptocurrency, created by a few seconds. The quantity of cryptocurrency units held by one individual is limited only by the total amount of cryptoccurency units (*e.g.* Bitcoin has 21 milions units).

A newly created account does not include any cryptocurrency units. The creation of a new account initially guarantees the owner's full anonymity. The term anonymity means that nobody (except the owner) can identify the account owner from the account data. It is recommended to use an account for one transaction only, which implies that an individual will have tens to hundreds of thousands of accounts over the course of his or her life.

Account owners may partly lose this anonymity because of their behaviour (Bonneau et. al., 2014). Anonymity is weakened when the cryptocurrency is sent, received and when the identity is voluntarily revealed. The term pseudo-anonymity is used for anonymity in cryptocurrencies. Transacting parties are not identified by their actual proper names or otherwise used identifiers but that those parties still have identifiers (cryptocurrency account addresses).

Account owners who execute a transaction with their accounts (receive or send cryptocurrency units) reveal part of their anonymity to the owner of the other transaction account. If we pay our shopping in a store by cryptocurrency, the merchant knows that the account from which the payment was sent belongs to us. Then the level of the account anonymity depends on the level of our physical anonymity towards the merchant – whether the merchant knows us by name, can recognise us by face.

Account owners can voluntarily reveal their identity. For example, most exchange offices that allow exchanging cryptocurrencies for fiat currencies abide by Know Your Customer (KYC) policies. Exchanges in USA are required (FinCEN, 2017) to implement Banking Secrecy Act (BSA) policies.

Some cryptocurrencies try to achieve full anonymity, not just pseudo-anonymity. Zcash (Sasson et. al., 2014) allows shielded transactions, which do not reveal sender, recipient, and amount of a transaction. Monero and Bytecoin use cryptonote protocol (Saberhagen, 2013), which shows information about transaction (sender, recipient, amount) only to the sender and the recipient of the given transaction. Dash (Duffield, Diaz, 2015) contains function Darksend that mixes cryptocurrency units of different owners.

In this article we draw up a classification of accounts into four groups by level of their anonymity. The highest – full – anonymity is provided by anonymous account. Pseudo-anonymous account also provides a high level of anonymity. The state administration (of at least one state) knows the identity of a semi-transparent account owner. The identity of a transparent account owner is publicly traceable.

Transparent account: The owner has revealed his or her identity in credible manner, e.g. on his or her website registered in the owner’s name. A debatable question occurs if the owner’s identity is revealed, for example, in a discussion forum user’s profile – i.e. the question is whether such identity can be trusted.

Semi-transparent account: The account owner’s identity is traceable for the state administration. For example, the account owner has bought cryptocurrency for fiat currency at an exchange office that abides by KYC policies.

Pseudo-anonymous account: Only the account owner’s business partners can know the owner’s identity. This may not necessarily include knowing the name but also knowing the information that can help ascertain the identity. A merchant who is personally selling an expensive article may remember the customer’s face while merchants in ordinary sales may keep their Closed Circuit Television recordings and online stores may keep the customer’s Internet Protocol (IP) address.

Anonymous account: Nobody but the owner knows the account owner’s identity. This applies to newly opened accounts. This category also includes accounts that were initially pseudo-anonymous but all business partners have already forgotten all information to reveal the account owner’s identity.

5. State approaches to cryptocurrencies

Our aim is to analyse and classify public authorities’ approaches to cryptocurrencies in individual countries of the world. For the purposes of this article we created a classification composed of 6 levels referred to as levels 0 to 5: Level 0 – ignoring, Level 1 – monitoring, Level 2 – recommendation, Level 3 – guidance, Level 4 – regulation, Level 5 – ban or integration. Within certain levels we also created groups. States are always included in a single level only – the highest achieved by the state. States may be included in several groups within a single level.

As the basis for creating this classification we used Hansen’s list (2016), updated on an ongoing basis. This list includes alphabetically sorted countries of the world that deal with cryptocurrencies. For each country a chronological development of its relationship to cryptocurrencies is described. More information is also available in an article about the history of cryptocurrencies by Wolfson (2015).

Level 0 – ignoring: The state does not deal with the existence of cryptocurrencies. The reason may be the small importance attached by the state to cryptocurrencies. The market capitalisation of all cryptocurrencies altogether was approximately $6 billion in January 2016 according to CoinMarketCap

(2016). Originally this level included all countries in the world and, with the growing importance of cryptocurrencies, individual countries are moving to higher levels. Approximately 150 countries currently remain in this level.

Level 1 – monitoring: A state authority, usually an institution responsible for supervising financial institutions, has issued a statement that it is aware of the existence of cryptocurrencies and will deal with them in the future. At the same time, no recommendation for an approach to cryptocurrencies has been issued. This level includes 3 countries only: Croatia, Ireland and Japan. Individual countries usually skip this level.

Level 2 – recommendation: A state authority has recognized cryptocurrencies and issued a recommendation for an approach to cryptocurrencies for its citizens. Most recommendations view cryptocurrencies negatively (see 25 countries in group 2A), except for a report by the European Banking Authority (2014), which cites possible benefits in addition to risks.

Group 2A – warning against risks: The most comprehensive summary of risks can be found in a report by the European Banking Authority (2014). The most serious warnings include those against a possible rapid decline in the cryptocurrency exchange rate and the irreversibility of the transactions made. These two risks are often misused for various types of criminal activities. To date approximately 25 countries have issued warnings against risks independent of this report (Hansen, 2016): Belgium, Brazil, Cyprus, Denmark, France, Greece, Hungary, India, Indonesia, Israel, Italy, Lebanon, Lithuania, Malaysia, Mexico, Netherlands, New Zealand, Philippines, Portugal, Serbia, South Africa, South Korea, Taiwan, Turkey and Vietnam.

Group 2B – presentation of the cryptocurrency potential: According to a statement by the European Banking Authority (2014), cryptocurrencies are suitable for micro-transactions, international payments and for use in developing countries with instable currencies. The statement also recognized that cryptocurrencies do not retain personal data of their owners, thus preventing the risk of misusing such personal data.

Level 3 – guidance: A state authority has issued guidance to govern the method of using cryptocurrencies. Such guidance is usually accompanied by a warning against cryptocurrency risks. This level includes numerous groups, depending on the type of guidance issued, with a single country very often included in several groups.

Group 3A – AML: Cryptocurrency transactions are subject to restrictions similar to those applicable to financial transactions in terms of anti-money laundering (AML) laws. Usually a greater level of risk is attributed to transactions executed by cryptocurrencies than to those executed by fiat currencies. This group includes 5 countries (Hansen, 2016): Argentina, Czech Republic, Canada, Singapore and USA. In addition, this group should also include European Union countries soon, as the European Banking Authority is planning to issue binding guidence. Given the nature of cryptocurrencies, the AML application is not easy and sometimes it is even impossible; Dostov (2014) deals with this in detail.

Group 3B – not VAT: Cryptocurrencies are not goods and cannot be subject to value added tax (VAT). This group includes European Union countries, according to Perez (2015), and Switzerland. The following 3C group may also be seen as a sub-group of 3B.

Group 3C – assets: Cryptocurrencies are considered to be a sort of assets, with gains from holding or selling them being subject to the existing tax legislation applicable to assets. This group includes 9 countries (Hansen, 2016): Australia, Bulgaria, Canada, Estonia, Germany, Norway, Singapore, Sweden and USA (IRS, 2014).

Group 3D – VAT: Cryptocurrencies are goods and ought to be subject to value added tax. This group includes Hong Kong and the United Kingdom (Hansen, 2016). The United Kingdom is likely to review its position soon because, being a member of the European Union, the UK should be included in the group of countries where VAT is not applied to cryptocurrencies.

Group 3E – tax from mining: Cryptocurrency mining is subject to income tax. This group includes Poland and Slovenia (Hansen, 2016).

Group 3F – tax from gambling: Cryptocurrencies are subject to gambling tax. This group includes Spain only (Hansen, 2016).

Level 4 – regulation: Provision of cryptocurrency-related services requires an explicit authorisation from the relevant state authority. Predefined conditions must be met to obtain the authorisation. This group includes Jersey, New York (USA) and Luxembourg (Hansen, 2016). The most comprehensive regulation is the BitLicence issued by the New York State Department of Financial Services (2015).

Level 5 – ban or integration: The last level is the refusal or the full adoption of the cryptocurrency concept. The refusal can be implemented through various forms of prohibition. Conversely, a state can recognise a cryptocurrency as a currency equivalent to its national fiat currency or even replace its national fiat currency with a cryptocurrency. An interesting approach is being pushed by Ecuador (Yanez, 2015), which applies a combination of a ban on existing cryptocurrencies and preparations for issuing its own cryptocurrency.

Group 5A – ban for banking institutions: Banking institutions are prohibited from providing cryptocurrency-related services, in particular exchanging them for fiat currencies. The execution of cryptocurrency transactions among people is not restricted. This group includes 4 countries (Hansen, 2016): China, Colombia, Iceland and Jordan.

Group 5B – complete ban: The execution of cryptocurrency transactions is prohibited not only for banking institutions but also for people. The ban can be enforced under the threat of imprisonment. The ban can be accompanied by censoring the websites providing cryptocurrency information and services. This group includes 5 countries (Hansen, 2016): Bangladesh, Bolivia, Kyrgyzstan, Russia and Thailand.

Group 5C – integration: The state will enact a cryptocurrency as its national currency, which can be a cryptocurrency created by that state. Or the state will use the cryptocurrency technology for operating the state administration services. The state can also invest its central bank's money in cryptocurrencies. At present, this category includes two countries only: Ecuador (Yanez, 2015) and Isle of Man (Caffyn, 2015), which are working on the integration of cryptocurrencies into their respective state administrations.

6. Risks and their prevention

The European Banking Authority (2014) defined 70 risks, divided into several categories based on who or what is threatened by them. The threatened groups include: (A) users of cryptocurrencies for business transactions, (B) users of cryptocurrency repository services or cryptocurrency exchange offices, (C) financial integrity, including money laundering and other crime, (D) existing payment systems, (E) regulatory authorities.

In this article we will view the risks from the perspective of their causes rather than consequences. We will divide the risks into categories, depending on what cryptocurrency feature causes these risks. For each risk category we will specify the possible actions to reduce those risks. We have divided the risks into the following categories: (R1) low market capitalisation, (R2) private key knowledge equals ownership, (R3) transaction irreversibility, (R4) account anonymity, (R5) infrastructure distributed all over the world. Chapter 7 of this article presents a comprehensive state approach to cryptocurrencies that would curb all of these risks.

R1 – low market capitalisation: Given the limited number of users and its capital, the market capitalisation of cryptocurrencies is low. Any one user's trade would have a disproportionate impact on market price. Hence exchange rates of cryptocurrencies against fiat currencies may change quickly. Such exchange rate changes may result from a release of new information about the cryptocurrency at issue, or from a targeted attack by speculators. Speculators are able to buy or sell large portion of existing units of the given cryptocurrency, because the market capitalisation of the cryptocurrency is low. This leads to significant exchange rate changes.

Some cryptocurrencies may even be created directly by speculators for their later enrichment. As a result of this risk a user may lose 100% of invested funds over a few months. Police in London investigate OneCoin Ponzi scheme (Higgins, 2016). OneCoin is presented by its founders as a centralised cryptocurrency (OneCoin, 2017).

The best situation is that of Bitcoin while the worst is that of newly created cryptocurrencies. In the past, it was normal for Bitcoin, the most stable cryptocurrency, to fall in value by 50% or rise in value by 100% in a week. However, most cryptocurrencies are even less stable, e.g. Paycoin lost more than 99.7% of its value in 2015 (Lansky, 2016).

This can be addressed by making users aware of the risk of rapid exchange rate fluctuations, which may even occur with well-established cryptocurrencies such as Bitcoin, Litecoin, Ripple, Dash, Dogecoin and Peercoin. Users must be consistently warned from investing in newly created cryptocurrencies, which have existed for days or weeks.

The growing expansion of cryptocurrencies will gradually eliminate this problem (Short, 2014). The market capitalisation of well-established cryptocurrencies such as Bitcoin will increase, making them resistant to rapid exchange rate fluctuations. One investor or speculator will control smaller portion of existing units of the cryptocurrency. In addition, user awareness of the risks involved in buying newly arising cryptocurrencies will improve. When buying cryptocurrencies, users will consider the reputation of the creators and promoters of those cryptocurrencies.

R2 – private key knowledge equals ownership: If a user divulges a private key to his or her cryptocurrency account to another person, this person can take full control of the account. Combined with the irreversibility of transactions made (the R3 risk), this may lead to an irrecoverable loss of funds in this account. Chapter 2 of this article deals with ownership in greater detail.

Users may divulge their private keys involuntarily, *e.g.* if hackers attack the electronic device in which the user's private key is stored. Users can voluntarily hand over their private keys to a service that stores cryptocurrencies, *e.g.* the online wallet Blockchain.info (2017). More often, users voluntarily transfer units of cryptocurrency to a service that stores cryptocurrencies (online wallets, exchanges) who provides them with the ability to recover those units of cryptocurrency later. In that event, all that the hackers need to do is successfully attack the server of that service and then they will acquire the cryptocurrencies stored there in hot wallets.

One way to completely eliminate the risk of involuntarily divulging the private key is to use the hardware Bitcoin wallet, *e.g.* Trezor by SatoshiLabs (2016) or Ledger Blue by Ledger (2017). However, the risk of voluntarily divulging the private key, may be reduced but not wholly eliminated. Users must be warned that they should only entrust an amount of a cryptocurrency to a third party cryptocurrency repository or exchange service to the extent that the loss of that amount will not financially threaten them.Users should consider the reputation of the owners of the service concerned and how the service is secured.

Consumer risk of loss can be further reduced through regulation (Coleman, 2017) e.g. by the BitLicence issued by the New York State Department of Financial Services (2015). The service provider cannot be compelled to implement regulation because, given the electronic nature of these services, they can easily leave or change their jurisdictions. Bitlicense is expensive and time consuming (Reuters, 2016), so many cryptocurrency companies left New York jurisdiction, *e.g.* Poloniex (Redman, 2015). Nevertheless, the service providers can decide to adopt regulation if they determine it is beneficial. Users may prefer a service that is regulated over a service that is not.

R3 – transaction irreversibility: Most cryptocurrencies do permit transactions to be reversed. If a user remits a payment to a non-existing account by mistake, the amount remitted is lost forever. If a user remits a payment to a business partner who will not meet the agreed terms of contract, the law in many countries (*e.g.* Europe Union) enables the user to request that the business partner return the amount remitted but the business partner can refuse such a request. The cryptocurrency technology does not allow a transaction to be reversed, even when subject to a court order. It is also impossible to compel the withdrawal of funds gained through criminal activity unless the perpetrator surrenders the private key to his or her account – see the R2 risk: private key knowledge equals ownership.

There is only one possible (but very rare) way. Community can execute a hard fork of the cryptocurrency. After The DAO hack, Ethereum community executed hard fork (Castilo, 2016). In the new chain were stolen funds returned to original owners, but 10% of community disagree and follow original chain Ethereum Classic.

To resolve potential future business disputes, it is possible, prior to the commencement of the transaction, to agree on appointing a third party who will decide a possible dispute as an arbitrator. The money will be sent to a special type of account – multiple signature, usually called "multisig". Three private keys to this account exist. Each business party holds one private key and one is held by the arbitrator. Two of the three private keys are required to transact the cryptocurrency from this account.

It is very difficult to withdraw funds gained through criminal activity. In non-democratic countries this could happen by means of torture. In some democratic states can be torture used in cases of suspected terrorism. *e.g.* Patriot Act in the USA (2001). In other democratic countries this may only happen if the private key is insufficiently secured by the perpetrator or if the perpetrator decides to surrender the funds voluntarily.

R4 – account anonymity: Chapter 3 dealt with account types distinguished by anonymity. Users can direct payment of cryptocurrency to a fully anonymous account. Users can also keep the anonymity of such an account by spending the money from it cautiously. If users spend their money incautiously, their accounts will change into pseudo-anonymous ones. It is difficult for state authorities to trace the owner of a pseudo-anonymous account, especially if the transactions take place in a different country. Herrera-Joancomart (2014) deals with the methods of how to reveal the identity of a pseudo-anonymous account owner based on analysing the executed transactions.

If the account contains funds from criminal activity, the account anonymity is a serious problem for investigating the crimes such as financial thefts, abductions, extortions and bribery. If the perpetrator is cautious, it is even impossible to prove that the perpetrator owns the funds concerned.

Existing AML and KYC mechanisms can make it much more difficult for the perpetrator to spend the money. These mechanisms may even lead to the identification of the perpetrator. This solution does not address the situation where the perpetrator is spending the money in countries that do not apply such mechanisms or is spending only small amounts to which such mechanisms are not applied. The perpetrator can avoid AML and KYC mechanisms by using direct exchange between users - Local Bitcoins.

R5 – distributed infrastructure: Cryptocurrencies are used across the globe. Regarding Bitcoin, Higgins (2015) writes that there is even a plan to launch 24 nanosatellites into space in 2016. Thus no country has the option of achieving an extinction of a specific cryptocurrency by prohibiting it.

Using its laws, a state can prohibit using a cryptocurrency for business transactions within its territory. Citizens of such a country can still use the cryptocurrency in countries where it is not prohibited. Citizens can also trade with other people from the same country who decide to breach the ban.

A state has the option of blocking the web services that accept cryptocurrencies. Nevertheless, technically skilled people can continue to use such web services by connecting to foreign proxy servers. The only reliable solution would be a separation of that country's Internet from the rest of the world, which is unlikely.

7. Utilisation

There are currently several areas where using cryptocurrencies may be superior to fiat money. According to the European Banking Authority (2014), this includes micropayments, international payments and payments in countries with unstable currencies.

Micropayments: Cryptocurrencies can express very small financial amounts. For example, Bitcoin can express an amount equal to 0.001 US cents. Fees for cryptocurrency transactions are very low. The fee for a Bitcoin transaction corresponds to $0.80 (Voorhees, 2017) and there are cryptocurrencies with fees several orders of magnitude lower, *e.g.* Dogecoin's fee corresponds to 0.03 US cents. Both of these features predetermine cryptocurrencies for micropayment use. In practice, fees must be significantly smaller than the amounts to be conveyed. Although Bitcoin fees impose a practical barrier, the technology permits micropayments

Foreign payments: International payments by conventional fiat currencies take days and are delayed by bank holidays, for instance. Cryptocurrency transactions usually take minutes to tens of minutes. Fees per cryptocurrency transaction (as stated in the foregoing paragraph) are negligible. Use of cryptocurrencies for foreign payments saves both money and time. Cryptocurrency users (who do not use fiat) avoid value fluctuation risk, marketability risk and AML/KYC reporting risk.

Payments in countries with unstable currencies: According to Hanke and Kwok (2009), the month-on-month inflation rate in Zimbabwe was above 100% in 2007 to 2008. Although cryptocurrencies are affected by instable exchange rates against fiat currencies, the use of Bitcoin instead of the local fiat currency may be a better alternative for people in certain African and South American countries with high inflation rate (Vega, Singh, 2016). The withdrawal of 500 and 1000 rupee notes from circulation in India has sparked interest in Bitcoin among India's consumers (Graham, 2016). Chinese use Bitcoin to funnel money out of the country, regardless of restrictions (Schmid, 2015).

Information retention: Cryptocurrencies retain the full history of all executed transactions in a data structure called blockchain (Satoshi, 2008). The transaction history is retained in such a form that it can not be practically changed and consequently forged in the future. There are ways to add additional information, which is retained in this unforged way, to the individual transactions. Special type of transaction (OP_RETURN) do not transfer cryptocurrency units but is used for store information. Snow et. al. (2014) created the Factom system, which is an example of this concept.

In this way it is possible to verify the existence of a document at a given time in an unforged manner and at very low cost. The authenticity of an agreement and signatures can be verified in this way. This can be used for the record-keeping purposes currently in state control: property register, vehicle register, etc. It can also replace the services of notaries in certifying documents and the services that maintain vital records about the population.

Colored coins: Cryptocurrencies allow for assigning a specific attribute to some of its payment units in order to distinguish them from the other payment units of the same cryptocurrency. This procedure is called coin colouring. Numerous cryptocurrencies currently focus on this. Mizrahi (2012) created ChromaWay, which use colored coins for identify the current owner of high-value property (real estate, cars, art). ColoredCoins (2013) community is building a universal framework for digital currencies on top of a Bitcoin blockchain. Ethereum, a cryptocurrency presented by Buterin (2014) is focused on smart contracts, but colored coins are supported too. Waves (2016) allows users to trade colored coins (called tokens) representing USB, BTC, gold, pieces of companies, physical or intellectual property.

With coin colouring it is possible, anonymously and at low cost, to hold elections, operate state lotteries. Coin colouring enables each citizen to start issuing his or her own shares at no cost, which could give a lift to economic growth.

8. Cryptocurrency as a national currency

This chapter will deliberate over the implications that establishing a cryptocurrency as a national currency would have. To this end, an existing cryptocurrency such as Bitcoin can be used, or a new cryptocurrency can be created. Ecuador applies a combination of a ban on existing cryptocurrencies and preparations for issuing its own cryptocurrency (Yanez, 2015). Moore and Stephen (2015) analysed impact of inclusion cryptocurrencies into portfolio of international reserves held by the Central Bank of Barbados. Barrdear and Kumhof (2016) analysed the macroeconomics of central bank (Bank of England) issued digital currencies.

Chapter 5 of this article presented the risks involved in cryptocurrencies. To a certain extent, these risks can be mitigated, for example, by user awareness or by applying AML and KYC approaches. However, the risks cannot be eliminated. A ban on cryptocurrencies is no solution either because, given the decentralised nature of cryptocurrencies, such a ban would be difficult to enforce even in the territory of the state that has issued it.

We expect that introducing a national cryptocurrency with open mining protocol or adopting an existing cryptocurrency as a national currency might significantly reduce the risks brought about by cryptocurrencies, although a complete elimination of those risks is impossible.

If a state adopted a cryptocurrency as legal tender within its jurisdiction, it would be appropriate if the state engaged itself in the infrastructure operating the cryptocurrency concerned. Hence the state ought to invest in the equipment for mining that cryptocurrency. Nevertheless, these costs would be counterbalanced by the revenues from the mined cryptocurrency. The amounts of the mining costs and mining revenues would be much the same (Valfells, Egilsson, 2016). If the state morally supported a cryptocurrency by investing in it, the general confidence in that cryptocurrency would increase, as would its market capitalisation. We expect that this would curb the risk of rapid fluctuations in value of that cryptocurrency as well as other problems caused by the low market capitalisation – the R1 risk.

The transaction irreversibility (R3 risk) makes it impossible for the state administration to seize illegally gained (or mistakenly send) money. This is augmented by the risk of easy loss of the funds if the private key is divulged (R2 risk). If the state engages itself in cryptocurrency mining, there is a solution. Miller (2013) presented a feather forking attack, which makes it possible, if the mining power is large enough (at least 10% of the total mining power), to block the execution of transactions from selected accounts. A state that wants to enforce blacklisting transactions from a particular address, might refuse to build block on any chain containing a transactions it does not like. A miner who decides include the blacklisted transaction into his block is risking that his valid block will be ignored in small percentage of cases and this miner will lose mining reward. While perpetrators could gain their money, they could not spend it. This would significantly reduce their motivation to commit crimes.

Through the feather forking attacks the state could also enforce users giving up their anonymity and reporting their identity to the state (semi-transparent account). The state could block transactions from accounts with a higher level of anonymity than that allowed by the state. This blocking would apply globally. Use of the Feather Forking Attacks would curb the anonymity of accounts (R4 risk).

The greatest challenge would be to curb the R5 risk, caused by the global distribution of the network. This risk can be partially curbed by means of Feather Forking Attack. This risk would only be eliminated if most countries in the world adopted a single approach to cryptocurrencies.

So far we have only presented the advantages of introducing a cryptocurrency as a national currency: this would reduce the risks caused by cryptocurrencies. At the same time, however, the state would give up its powers to regulate its currency through the central bank, thus influencing the country's economy. The question is whether this disadvantage offsets the aforementioned advantages.

Another solution will be a national "cryptocurrency" with closed mining protocol and a central point of control. This solution will be close to current fiat currencies, only in a fully digital form. It will break cryptocurrency rule about decentralisation. The confidence in that "cryptoccurency" will depend on confidence in the given state. The state can decide which transactions will be valid. The state will have information for tax collection. The state can easy do blacklisting, even more the state can executed judicial decisions – the state can sign transaction instead of regular owners.

9. Conclusion

Cryptocurrencies are a revolutionary invention among digital currencies. Since first of them (Bitcoin) being created in 2009, they have attracted enough users to draw attention of state authorities in certain countries. Compared to conventional currencies, cryptocurrencies involve a different approach to ownership and anonymity. These differences pose numerous risks but also numerous opportunities.

Now the individual countries tend to realise the risks in particular because these risks threaten them. Most risks can be curbed by awareness among cryptocurrency users and by using AML and KYC policies. The impossibility for public authorities to withdraw funds from a cryptocurrency account, in combination with the irreversibility of transactions made, can be seen as the greatest risks. The perpetrator's cooperation (i.e. the perpetrator's fault or good will) is required in democratic countries for illegally gained funds to be returned.

Many states do not pay much attention to opportunities that cryptocurrencies offer. These opportunities tend to be embraced by private businesses, with some of them starting to operate services that used to be primarily provided by the state.

Acknowledgement

This research was supported by the Czech Science Foundation as part of the project New Sources of Systemic Risk on Financial Markets (GA ČR 16-21506S).

References

Back, A., 2002: *Hashcash - A Denial of Service Counter-Measure*. Available from http://www.hashcash.org/papers/hashcash.pdf

Antonopoulos, A. M., 2015: *Mastering Bitcoin: Unlocking Digital Cryptocurrencies*. O'Reilly Media, Sebastopol, CA, USA

Barrdear, J. & Kumhof, M., 2016: The macroeconomics of central bank issued digital currencies. Staff Working Paper No. 605. Bank of England. Available from http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf

Blockchain.info, 2017: *Bitcoin Wallet - Blockchain*. https://blockchain.info/wallet/#/

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A., Felten, E., W. 2014: Mixcoin: Anonymity for Bitcoin with Accountable Mixes. *International Conference on Financial Cryptography and Data Security*. pp 486-504.

Borchgrevink, J., 2014: Dogecoin Forks to Avoid Multipool Exploit, Mandatory Update! Cryptocoinsnews. Available from https://www.cryptocoinsnews.com/dogecoin-forks-again-to-avoid-multipool-exploit/

Buterin, V.: 2014: Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform. *Bitcoin Magazine.* Available from http://bitcoinmagazine.com/9671/ethereum-next-generation-cryptocurrency-decentralized-application-platform/

Caffyn. G., 2015: Isle of Man Trials First Government-Run Blockchain Project. *CoinDesk*. Available from http://www.coindesk.com/isle-of-man-trials-first-government-run-blockchain-project/

Castilo, M., 2016: *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*. *CoinDesk.* Available from http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/

Chaum, D., 1983: Blind signatures for untraceable payments. Advances in *Cryptology Proceedings of Crypto* 82 (3): 199–203

Chaum, D., Fiat, A., Naor, M., 1988: Untraceable electronic cash. *CRYPTO 88 Proceedings on Advances in Cryptology*, pp. 319-327, Springer-Verlag New York, Inc. New York, NY, USA.

CoinMarketCap, 2016: *Crypto-Currency Market Capitalizations*. Available from http://coinmarketcap.com/

Coleman, L., 2017: Bitfinex's Lesson: Has the Time for Regulation Arrived?. Cryptocoins News. Available from https://www.cryptocoinsnews.com/bitfinexs-lesson-has-the-time-for-regulation-arrived/

ColoredCoins, 2013: *Coloredcoins Codex*. Available from http://coloredcoins.org/documentation/

Debeauvais, T., Nardi, B. A., Lopes, C. V., Yee, N., Ducheneaut, N., 2012: 10,000 Gold for 20 Dollars*: An exploratory study of World of Warcraft gold buyers*. FDG '12, Raleigh, NC, USA. pp. 1-8

Dostov, V., Shust, P., 2014: Cryptocurrencies: an unconventional challenge to the AML/CFT regulators? *Journal of Financial Crime*, Vol. 21 No. 3, pp. 249-263

Duffield, E., Diaz. D., 2015: *Dash: A Privacy-Centric Crypto-Currency*. Available from https://www.dash.org/wp-content/uploads/2015/04/Dash-WhitepaperV1.pdf

European Banking Authority, 2012: *Virtual currency schemes.* Available from https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf

European Banking Authority, 2014: *EBA Opinion on virtual currencies*. EBA/Op/2014/08.

European Central Bank, 2000: *Issues arising from the emergence of electronic money*. ECB Monthly Bulletin. November 2000

FinCEN, 2017: *Bank Secrecy Act Requirements - A Quick Reference Guide for MSBs*. Financial Crimes Enforcement Network. United States Department of the Treasury. Available from https://www.fincen.gov/sites/default/files/shared/bsa_en_bank_reference.pdf

Graham, L., 2016: *India's rupee restrictions are boosting demand for bitcoin*. CNBC. Available from http://www.cnbc.com/2016/11/15/india-rupee-restriction-boost-bitcoin-digital-currency.html

Grow, B., Cady, J., Rutledge, S., Polek, D., 2006: *Online payment systems like e-gold Ltd. are becoming the currency of choice for cybercrooks*. BusinessWeek. Available from https://www.bloomberg.com/news/articles/2006-01-08/gold-rush

Haber, S., Stornetta, W. S., 1997: Secure names for bitstrings. *Proceedings of the 4th ACM Conference on Computer and Communication Security*

Hanke, S. H., Kwok, A. K. F., 2009: On the Measurement of Zimbabwe's Hyperinflation. *Cato Journal*, 29 (2)

Hansen, J. D., 2016: *Virtual Currencies: International Actions and Regulations*. Perkins Coie Available from https://www.perkinscoie.com/en/news-insights/virtual-currencies-international-actions-and-regulations.html

Herrera-Joancomart, J., 2014: *Research and Challenges on Bitcoin Anonymity*. Keynote Talk: 9th International Workshop on Data Privacy Management, Wroclaw, Poland.

Higgins, S., 2015: Bitcoin Nanosatellites Could Orbit Earth in 2016. *Coindesk.* Available from http://www.coindesk.com/bitcoin-nanosatellites-orbit-earth-2016/

Higgins, S., 2016: London Police Investigate OneCoin Cryptocurrency Scheme. *Coindesk*. Available from http://www.coindesk.com/london-police-investigate-onecoin-cryptocurrency-scheme/

IRS, 2014: Notice 2014-21. *Internal Revenue Service,* USA. Available from https://www.irs.gov/pub/irs-drop/n-14-21.pdf

Jenkins, R. J. Jr. (1996). *ISAAC*. Fast Software Encryption, pp. 41–49.

Langlois, J. (2013). *Liberty Reserve digital money service shut down, founder arrested. GlobalPost*. Available from https://www.pri.org/stories/2013-05-27/liberty-reserve-digital-money-service-shut-down-founder-arrested

Lansky, J., 2016: Analysis of Cryptocurrencies Price Development. *Acta Informatica Pragensia*, Vol. 5, No. 2, pp. 118-137. DOI: 10.18267/j.aip.89

Ledge, (2017: *Ledger Wallet - Hardware wallets - Smartcard security for your bitcoins*. Available from https://www.ledgerwallet.com/

Miller, Andrew, 2013: Feather-forks: enforcing a blacklist with sub-50% hash power. *Bitcointalk*. Available from https://bitcointalk.org/index.php?topic=312668.0

Mizrahi, A., 2012: A blockchain-based property ownership recording system. *ChromaWay*. Available from http://chromaway.com/papers/A-blockchain-based-property-registry.pdf

Moore, W., Stephen, J., 2015: Should Cryptocurrencies be included in the Portfolio of International Reserves held by the Central Bank of Barbados? *CBB Working Paper* No. WP/15/16. Central Bank of Barbados. Available from http://www.centralbank.org.bb/news/article/8827/should-cryptocurrencies-be-included-in-the-portfolio-of-international-reserves

Nakamoto, S., 2008: *Bitcoin: A Peer-to-Peer Electronic Cash System*. Available from https://bitcoin.org/bitcoin.pdf

Narayanan, A., Bonneau, J., Felten, E., Miller, A., Goldfeder, S., 2016: *Bitcoin and Cryptocurrency Technologies*. Draft, Princeston, USA

New York State Department of Financial Services, 2015: *New York codes, rules and regulations.* Title 23. Department of Financial Services. Chapter I. Regulations of the superintendent of financial services. Part 200 Virtual Currencies

OneCoin, 2017: *OneCoin offers borderless and affordable financial services*. Available from https://www.onecoin.eu/en/about

Perez, Y. B., 2015: *Bitcoin is Exempt from VAT, Rules European Court of Justice*. Available from http://www.coindesk.com/bitcoin-is-exempt-from-vat-says-european-court-of-justice/

Redman, J., 2015: *Poloniex Leaves New York Due To BitLicense.* Available from https://news.bitcoin.com/poloniex-leaves-new-york-due-to/

Reuters, 2016: New York's bitcoin hub dreams fade with licensing backlog. Available from http://www.cnbc.com/2016/10/31/new-york-bitcoin-hub-dreams-fade-with-licensing-backlog.html

Rosenfeld, M., 2012: *Analysis of hashrate-based double-spending*. Available from https://bitcoil.co.il/Doublespend.pdf

Saberhagen, N. v., 2013: *CryptoNote v 2.0* Available from https://cryptonote.org/whitepaper.pdf

Sasson, E. B., Chiesa, A., Garman, C., Green, M., Miers, I., Tromer, E., Virza, M., 2014: Zerocash: Decentralized Anonymous Payments from Bitcoin. *Security and Privacy (SP) 2015 IEEE Symposium on*, pp. 287-304

SatoshiLabs, 2016: *Hardware Bitcoin Wallet Trezor*. Available from http://satoshilabs.com/trezor/

Schmid, V., 2015: Markets How Chinese Use Bitcoin to Funnel Money Out of the Country. *Epoch Times*. Available from http://www.theepochtimes.com/n3/1891021-how-chinese-use-bitcoin-to-funnel-money-out-of-the-country/

Schwartz, D., Youngs, N., Britto, A., 2014: *The Ripple Protocol Consensus Algorithm*. Available from https://ripple.com/files/ripple_consensus_whitepaper.pdf

Short, J. H., 2014: *The Future of Cryptocurrency*. Available from http://www.harkell.com/TFOC-30-03-14.pdf

Snow, P. et. al., 2014: *Factom: Business Processes Secured by Immutable Audit Trails on the Blockchain*. Github. Available from https://github.com/FactomProject/FactomDocs/blob/master/Factom_Whitepaper.pdf

USA, 2001: *USA Patriot Act*. Available from https://www.gpo.gov/fdsys/pkg/BILLS-107hr3162enr/pdf/BILLS-107hr3162enr.pdf

Valfells, S., Egilsson, J. H., 2016: Minting Money With Megawatts. *Proceedings of the IEEE*, Vol. 104, No. 9, pp 1674 - 1678

Vega, A., Singh, S., 2016: Why Latin American economies are turning to bitcoin. *Crunch Network.* Available from https://techcrunch.com/2016/03/16/why-latin-american-economies-are-turning-to-bitcoin/

Voorhees, E., 2017: *The True Cost of Bitcoin Transactions*. Available from http://bitcoin.xyz/erik-voorhees-true-cost-bitcoin-transactions-2/

Waves, 2016: *Waves Platform - Blockchain for the people*. Available from https://wavesplatform.com/

Wolfson, S. N., 2015: Bitcoin: The Early Market. *Journal of Business & Economics Research*, Volume 13, Number 4, pp. 201-214

Yanez, P. R., 2015: *La junta de poliflca y regulacion y financiera*. Resolucion No. 064-2015-M. Ecuador minstry of finance. Available from http://www.juntamonetariafinanciera.gob.ec/PDF/resolucion64m.pdf?dl=0

JEL Classification: E50, N20