Annexes

Annex I. - Detailed Description of Blockchain Technology

Blockchain technology manages to overcome the General's Problem by way of complex mathematical problems which the computers participating in the blockchain – the nodes, seek solution for. The solution to these problems requires substantial computing power. The potential traitor or an attacker wishing to corrupt the recorded information would have to possess the majority of the computational power of the entire network of nodes to be successful with its attack. It is easier for the engaged nodes to trust each other, therefore, not requiring assistance of a third trusted party anymore, thus the designation *trustless*.[1]

That also brings us to the difference between a centralized and decentralized ledger. The decentralized or distributed ledger means that all nodes "*are connected with each other and store all data simultaneously, and together constitute the common ledger. [It] requires consensus of those nodes rather than just the confirmation by one hierarchically structured storage device, as with a centralized ledger*."[2] Truly decentralized systems do not differentiate between vertical and horizontal connection, there is no entitled party charged with supervision and control. All participating nodes have equal positions and value in reaching the consensus. There is, however, an exception to this rule. As opposed to the described truly decentralized systems (also called permissionless because not one of the engaged nodes is entitled to give permission), there may also be blockchain systems which are centralized to a certain degree – "permissioned" blockchains. Such blockchain ledgers allow for concentration of power where "*a limited group of actors retain the power to access, check and add transactions to the ledger*".[3] Permissioned blockchains do not need to provide incentives in order to "stay relevant" and functioning; instead, they enable access only to trusted nodes which have other than purely economic interest in the blockchain's functioning.[4] In practice, this approach will be especially interesting to banks or governmental entities wishing to retain some control over the recording process, in particular, in case of

[1] A. Wright, P. de Filippi, op. cit. no. 39, p. 6.

[2] D. A Zetsche and coll., op. cit. no. 188, p. 11.

[3] P. Boucher and coll., op. cit. no. 41, p. 5.

[4] A. M. Puertes, R. Teigland, op. cit. no. 101, p. 300.

very sensitive data. An example of such blockchain protocol of "trusted parties" is Ripple. These trusted parties are then known as "validation nodes"[5].

1. Verification Process

In order to be able to comprehend how the consensus between participating nodes is reached and therefore, how the blockchain technology really works, the process of recording of transactions need to be briefly described from the technical point of view. Due to the fact that Bitcoin was the first successful cryptocurrency project, and so far, is the most widely accepted and used cryptocurrency, the following description of how the crypto transactions are made is based on the Bitcoin system.

Firstly, every computer which wants to engage in a blockchain transaction must download the software containing a full and updated copy of the blockchain ledger. Therefore, every participating computer has access to all data recorded in the blockchain ledger up to the first recorded transaction. The ledger is viewable via the Internet[6], is constantly updated, at regular intervals of 10 minutes[7], and every change of the record is automatically known to all computers participating in this *de facto* network. Consequently, any file which is to be recorded in the ledger is compressed to a 64-character code called the *hash*.[8] The hash is like the file's fingerprint, it is unique for the particular file, i.e. package of information, and no two hashes (made from different files) are the same. Moreover, even though one file can be transformed in multiple copies of hashes, the file's hash cannot be transformed back to the file; it is not reversible. As the next step, the compressed hash of the file is given a time stamp and then inserted to be recorded. Provided that the operation consists in a simple payment transaction without deployment of smart contracts, the file itself is never submitted to the ledger, it stays in the original computer.

To be registered in the ledger, the transaction needs to be firstly accepted as true and validated by a pre-defined number of nodes. The transaction is true or legitimate, if e.g. "*the request comes from the authorized person, the house seller has not already sold the house, and the buyer has not already spent the money*[9]". For this determination, two separate

[5] D. A Zetsche and coll., op. cit. no. 188, p. 12.

[6] M. Swan, op. cit. no. 38, p. 2: blockchains can be viewed via the „*block explorers*", specialized internet sites, such as www.blockchain.info for the Bitcoin blockchain.

[7] H. M. Botos, '*A Blockchain Intelligence Analysis*' (2017), 13 Res. & Sci. Today 42.

[8] M. Swan, op. cit. no. 38, p. VIII.

[9] P. Boucher and coll., op. cit. no. 41, p. 5.

mathematical methods have been developed. The more usual one is the so-called *proof-of-work* and it basically consists in a mathematical operation, a problem which the computers on the blockchain compete to solve. Each transaction proposes a new problem and the first computer to solve it, is subsequently rewarded, apart from the transaction fee, usually by a sliver of the newly made blockchain's cryptocurrency. The remaining nodes of the system then verify that the solution is correct[10]. Once an adequate number of computers[11] confirm the solution to the problem, the transaction is accepted as true and then recorded in the block of transactions which is linked to previous blocks of transactions. As such, they form a long chain of blocks of transactions going all the way back to the first recorded transaction – the *genesis block*[12]. While the designated amount is transferred immediately, it takes approximately 7 minutes for simple and low-amount transactions to be verified through the described process of problem solving. The process is called *mining* and is used in most blockchain protocols, such as Bitcoin, for example. The miners offer their computing power for the solution of problems and therefore, validation of transactions. In exchange, they obtain a portion of transaction fees and some of them, the one solving the problem first, a portion of the newly created token of cryptocurrency as well. These rewards serve as an incentive to ensure that sufficient number of computers keep performing the necessary mathematical operations. "*Without a community of nodes running the protocol and verifying transactions the system stops working. If all the members have moved to a new system all data stored on the blockchain cease to exist*."[13] Therefore, the lack of interest would inevitably entail the destruction of the whole decentralized system.

The second method of validation, the *proof-of-stake*, is based on the "relevance" of participating computers. The determination of which computer will be charged with confirming and recording the transaction will depend on the computer's previous transactions and its account balance in the blockchain's cryptocurrency. Essentially, computers which have the most traffic (have analyzed and confirmed most transactions) in the past and thus, have been rewarded most of the distributed cryptocurrency, will be likely chosen to perform the recording successfully again, as they have more interest in well functioning of the

[10] M. Atzori, op. cit. no. 229: While the *proof-of-work* itself is difficult to produce, as it requires extensive sources of power and time, it is subsequently not demanding to verify its results by other computers.

[11] D. A Zetsche and coll., op. cit. no. 188, p. 12 „*The number of nodes required for the consensus is set in the code underlying the system and is thus a fundamental aspect of the design of any system. This also provides one of the major known vulnerabilities in many blockchain systems, including Bitcoin*. "

[12] M. Swan, op. cit. no. 38, p. X.

[13] D. A Zetsche and coll., op. cit. no. 188, p. 12.

system.[14] Due to the fact that such method might lead to significant centralization where only few "mighty" computers will effectively perform all actions, more sophisticated protocols were developed which build on the relevance of the computers (their stake) but combine it with various mathematical methods of selection, including randomization. The biggest advantage of this method is that a lot less energy is necessary for the completion of the recording process. As the computers are not required to "waste" enormous computing power for problem solving and subsequent validation, this approach is considered as more energy efficient and economical (for the energy consumptions issues and consequences, please see section **Chyba! Nenalezen zdroj odkazů.** of this thesis). For example, Peercoin protocol is based on the proof-of-stake method and Ethereum is supposed to introduce this method in the near future as well.

Table 1 - Simple overview of main consensus protocols

CONSENSUS PROTOCOL	OVERVIEW
Proof of Work	Uses computational power to validate new blocks of data. To participate in this scheme, participants are required to collate transactions within single block and then apply a hash function with the use of some additional metadata.
Proof of Stake	Validators (special nodes) voting on valid blocks whilst posting collateral in order to be able to participate in the validation process. Unlike Proof of Work, Proof of Stake relies on proving the user is invested in the underlying token of value of the network being mined rather than being the owner of a large amount of computing power.
Ripple Protocol	In order to validate new transactions servers amalgamate outstanding transactions into a "candidate list". All participants then vote on valid transactions then be included in the ledger. Transactions that meet the 80 % threshold of "yes" votes are included within the following last closed ledger state.
Proof of Elapsed Time	As part of its Intelledger proposal, Intel has devised a means of establishing a validation lottery that takes advantage of the capability of its CPUs to produce a timestamp cryptographically signed by the

[14] L. Lee, op. cit. no. 154, p. 29.

	hardware. Whoever in the chain has the next soonest timestamp will be the one to decide which transactions will be a part of the next block in the chain. This consensus method is extremely energy efficient compared to Proof of Work and therefore more adapted to IoT devices.

Source: ENISA (2016), op. cit. no. 265, p. 10, own table processing

After the hash is recorded in the ledger, it is permanent. Unless some unpredictable and unusual circumstances arise, such as a hacker attack, the data can never be amended or erased from the blockchain ledger. All other nodes in the network use the updated version of the blockchain for verification of new transactions which makes the ledger *transparent*. Later, when a stakeholder wishes to prove that the file has not been changed and therefore, is subject to the particular transaction recorded in the blockchain, it is sufficient to make a new 64-character hash of the file and compare it with the one recorded in the ledger. If the code is exactly the same, the file has not been tempered with.

2. Forks and Rule of the Longest Chain

In terms of addition of new blocks to the chain of transactions, each node within the network follows the principle of the longest chain, meaning that the node verifying the transaction will always accept a new block which it considers as the continuation of the longest chain. Nonetheless, it is theoretically possible that two different transactions are completed at exactly same time which effectively leads to a split of the chain, also called a fork. This issue is resolved when another node within the network accepts and adds a new block to the end which it deems the longest (for example due to the fact that it adds the block before it receives information that the chain was split). Therefore, upon this moment one split end becomes longer and all other nodes verifying the following transactions are bound by the longest chain rule and only add blocks to the one longer end of the chain. Blocks of transactions which are set aside and abandoned due to the split resolution are usually referred to as "*orphan blocks*". Nodes whose blocks became orphan blocks eventually lose the right to a reward. The rate of forks and orphan blocks is regarded as one of factors for determination of the level of security of the whole network, as they often occur at the times of "*double-*

spend attacks"[15] when the relevant node attempts to spend the same tokens of cryptocurrency twice, i.e. for two separate transactions. "*A node can decide to broadcast a transaction in one block, and if the transaction value is high enough, it can try to broadcast another transaction spending the same Bitcoins in another block. To invalidate the first transaction, it needs to create a chain of blocks that is longer than the chain that already contains the first transaction. This in turn creates an increase in orphaned blocks independent of the success of the attack. Furthermore, a system that naturally has a high rate of orphan blocks is more vulnerable to double-spend attacks. This is due to the fact that a forked chain reduces the number of blocks that the attacker needs to create in order to invalidate one of its own transactions.*" Such attacks are, however, immensely energy consuming.[16]

On the other hand, some forks of the chain may be intentional and legitimate. The particular design of the ledger system and all its properties, including the requirements for consensus, are set up by a group of core code developers who *de facto* represent administrators of the system. They are constantly developing and improving the software, similar to internet applications. Each major update of the blockchain system (namely but not limited to cryptocurrencies such as Bitcoin) is referred to as "*hard fork*" and all users are requested to download the latest version of the software[17]. Due to the fact that the majority of blockchain-based software is open source, the entire community of blockchain enthusiasts is allowed to participate in further improvement of the software. What's more, each node may independently decide on the version of software (the particular fork) it supports and follows which it signals to other nodes when connected to the network.[18] Due to the fact that each upgrade of the network by way of a hard fork needs support of the majority, otherwise it is "doomed to fail", this has been referred to as a *de facto* type of direct democracy.[19] However, even though the core developers usually do take into account suggestions and complaints of individuals and entities, the decision-making regarding the development rests with them. This aspect of so-called "*key personnel*" can potentially have negative effects, in particular with respect to the security of the system[20] (please see section **Chyba! Nenalezen zdroj odkazů.** of this thesis).

---

[15] For detailed description of double-spending please see M. Rosenfeld, '*Analysis of hashrate-based double-spending*' (2012), Cornell University Library, available at: https://arxiv.org/abs/1402.2009, last accessed 19.8.2018.

[16] H. Holmberg op. cit. no. 287, p. 313.

[17] D. A Zetsche and coll., op. cit. no. 188, p. 21.

[18] H. Holmberg op. cit. no. 287, p. 319.

[19] Ibid, pp 319, 321.

[20] D. A Zetsche and coll., op. cit. no. 188, p. 19.

3. Cryptography

Nonetheless, another piece of the puzzle is crucial for mainstream acceptance of blockchain and that is the encryption. The encryption ensures pseudonymization, i.e. separation of identifiers which are the data that identify or may identify a natural person. For these reasons, every person that opens an account with cryptocurrency and wants to perform a blockchain transaction is automatically assigned two pieces of information: (i) public key, or more precisely public address, and (ii) private key. Only the public key is registered in the ledger and unless the private key is leaked or openly connected to the public key by the particular person, no one can identify the concerned person (for more details regarding the encryption, please see **Annex II. - Cryptocurrencies and Financial Services**).

Annex II. - Cryptocurrencies and Financial Services

For the sake of completeness, cryptocurrencies based on Bitcoin and Satoshi's manual are usually called alt-coins (derived from the word *alternative*). Further, some authors differentiate between different alt-coins based on their inherent purpose.[21] Firstly, alt-coins which have been designed for the same purposes as Bitcoin, that is to serve as a means of payment in a decentralized transaction system are referred to as pure alt-coins, or simply alt-coins. Secondly, cryptocurrencies with focus on privacy can be referred to as anonymous coins and thirdly, cryptocurrencies which only use blockchain transaction systems as an underlying layer which they build on for additional purposes can be referred as Appcoins.

Although the Bitcoin is not the first digital currency project in history, the Satoshi's paper presents a first solution to the above mentioned *Byzantine General's Problem* by creating a decentralized network which does not require trust towards an intermediary. Furthermore, it solves the previously unsolvable *Double-Spend Problem.* "*Until blockchain cryptography, digital cash was, like any other digital asset, infinitely copiable (like our ability to save an email attachment any number of times), and there was no way to confirm that a certain batch of digital cash had not already been spent without a central intermediary*."[22] It follows that an intermediary was not only necessary to establish trust between the involved parties but also to prevent fraudulent activities consisting in transferring the digital cash intended for the payment several times to several individuals.

For ensuring that one token of digital currency is not used twice at the same time Satoshi combines the BitTorent protocol for peer-to-peer file sharing and encryption technology based on unique private key solely known and available to the users themselves.[23] What should be emphasized is that no special account needs to be opened in order to be able to participate in a decentralized transaction system, such as the Bitcoin. Every user is given a public address which serves as an identificator of the particular person when another person sends them digital money. In the traditional transaction system the public address corresponds to the bank account number. For example in the Bitcoin system, the public address is composed of 26 to 34 alphanumeric characters, such as 1JDQ5KSqUTBo5M3GUPx8vm9134eJRosLoH which can also have the form of a QR

[21] J. Baron and coll., op. cit. no. 45, pp15-16.

[22] M. Swan, op. cit. no. 38, p. 2.

[23] Ibid, p. 2.

code.[24] It is practically impossible that two individuals are generated the same public address.[25]

On the other hand, the private key paired to the public address represents a secret code, which is never given away by the user and its sole purpose is identification of the user, i.e. to assign the particular digital cash balance to the particular person. The private key is usually a 256-bit number and is even longer than the public address shown above as an example.[26] Without the private key the user cannot access its digital finances and cannot proceed with transacting a sum to another person's public address.[27]

In addition to this information, a person must have a computer and internet access to either become a full node within the network or to use SPV software relying on other nodes; nothing else is necessary for a blockchain transaction. Nevertheless, the private key represents an extremely sensitive piece of information – there is "*no customer service number to call for password recovery or private key backup*"[28]. If it is lost, there is no way it can be recovered, and thus, all digital cash is lost as well. As a consequence, other software has been developed to ensure safe-keeping of private keys. This software is usually referred to as *eWallet*[29] and apart from the public address and private key, it may also include a part of the blockchain database relating to the user's past transactions, similar to a statement of account. One eWallet may keep access information to more than one transaction system and more than one cryptocurrency. Examples of eWallets include ChromaWallet, Counterwallet or OneWallet. The eWallets also help to make the blockchain system more user-friendly, as instead of remembering the complicated public address and private keys numbers, a person can set up a personalized, sufficiently safe password. However, as shown in section **Chyba! Nenalezen zdroj odkazů.** of this thesis, they can also represent concentration and centralization to a certain degree which may consequently result in formation of new "honeypots" – hackers' targets.

---

[24] Ibid, p. 97.

[25] Ibid, pp 98-99: Upon registration, the pair of public and private key is generated first, on the basis of the current standard which is the Elliptic Curve Digital Signature Algorithm. Additional steps are taken for the public address to be generated. Essentially the public key is transformed into a shorter format with assistance of encryption protocols like SHA-256 and RIPEMD-160. While it is technically possible that the same public address is generated for two separate individuals, the odds of such possibility are less than 0,0001 %. Furthermore, potential derivation of the private key based on the public key or public address would be either impossible (one-way hashing operation) or would require extreme computing power and thus, would be extremely expensive.

[26] Ibid, p. 99.

[27] Ibid, p. 3.

[28] Ibid.

[29] Ibid.

In regard to mainstream acceptance of Bitcoin and other virtual currencies, a vendor wishing to accept cryptocurrencies must dispose with a particular payment processing solution (as it is not reasonable to expect usual consumers to pay for a cup of coffee via Internet). In the traditional sense of payment this solution corresponds to a credit card terminal, as an interface capable of reading the customer's public address and interacting with his eWallet.[30]. Some of the most common merchant solutions include BitPay and Coinbase in the United States. Coinbase has also recently started to provide an eShop, i.e. eCommerce, solution for integration of Coinbase payment option in the checkout process[31]. In Europe, e.g. BitcoinPay enables operation with many traditional currencies, including CZK. Another solution, CoinGate also offers mobile processing of payments.[32]

While it is definitely useful that the above mentioned payment processing solutions provide for immediate exchange of Bitcoins into traditional currency, such as euros, for most small businesses it will probably rather pose an obstacle than a convenience to install additional forms of payments, even more so if we take into account the current instability of the majority of virtual currencies (for more details on the issue if instability of altcoins, please see section **Chyba! Nenalezen zdroj odkazů.** of this thesis). For these reasons, one of the foremost areas of focus for future development might be providing a solution capable of combining traditional and decentralized payment processing solutions.[33] Among first steps in this direction is BitPay VISA Prepaid Card project which enables the consumer to pay in Bitcoins at every vendor place accepting VISA credit and debit cards.[34] This solution

[30] As follows from the Bitcoin's official website, "*some Bitcoin merchant solutions also provide invoices and easy to use Point-Of-Sale (POS) applications that run on a smart phone or tablet. Many merchant processors instantly convert the Bitcoin payment to your local currency at the current exchange rate. There are also a number of stand-alone tools available online for merchants to identify the current conversion rate quickly if needed*". Please see '*Merchant Solutions*', available at: https://www.bitcoin.com/merchant-solutions/, last accessed 19.8.2018, for further description and list of merchant solutions.

[31] Please see L. Shen, '*Meet 'Paypal for Crypto,' a New Way to Pay With Bitcoin and Litecoin*' (2018), available at: http://fortune.com/2018/02/15/bitcoin-paypal-coinbase-commerce/, last accessed 19.8.2018 and '*Coinbase Commerce –the Easiest Way for Merchants to Accept Digital Currency*' [2018], available at: https://medium.com/@coinbasecommerce/coinbase-commerce-the-easiest-way-for-merchants-to-accept-digital-currency-54ba64966f8d, last accessed 19.8.2018.

[32] In respect of mobile processing by way of an application for iOS or Android, some of the most common, apart from CoinGate, are European XBTerminal and Coinify.

[33] M. Swan, op. cit. no. 38, p. 4.

[34] However, the BitPay card itself does not process the payment in Bitcoins. It is a two-step process. Firstly, the BitPay card is directly connected to the individual's BitPay eWallet and can be "loaded" with Bitcoins via said eWallet. However, it can also be loaded with US dollars. Secondly, the payment is made in US dollars. All Bitcoins which were transferred to the BitPay Card are exchanged to US dollars under current exchange rate. The balance is subsequently always kept in US dollars and the consumer is free to use the card like a usual payment card or even withdraw US dollars in cash from an ATM machine. For further information on BitPay Visa Prepaid Card please see: '*Load dollars using your Bitcoin wallet, spend anywhere*', available at: https://bitpay.com/card/, last accessed 19.8.2018.

definitely represents one of the first steps of "rapprochement" of traditional and decentralized payment systems.

With respect to purchase of Bitcoins, the Bitcoin's official website provides a list of "*places to buy Bitcoin in exchange for other currencies*". Some of the prominent international exchanges include Kraken or Bitstamp while others, such as BitPanda or BL3P are focused on the European market.[35]

While not technically an exchange, Bitcoin trading places, such as Coinbase, provide exchange services as well. Their customers can buy and sell Bitcoins and other virtual currencies. For these purposes Coinbase has enabled transferring of funds via credit and debit cards and even PayPal[36], however only within the US market. PayPal, with more than 227 million active users[37], was prohibiting usage of their payment processing services for the purposes of *de facto* exchange operation in the past, however they have since then changed their stance and are now cooperating with Coinbase so that the users of Coinbase can now sell Bitcoin and receive payments via their PayPal accounts.[38] PayPal has even acquired a subsidiary Braintree for the purpose of enabling their users to pay for Uber rides or Airbnb rentals with Bitcoin.[39] As of March 2018, there have been reports that the company even filed for a patent with the US patent office with the objective of speeding up the decentralized transaction processing time.[40] The long processing time of transactions remains an obstacle to mainstream acceptance and use of cryptocurrencies, for more details please see section **Chyba! Nenalezen zdroj odkazů.** of this thesis.

[35] Please see '*Bitcoin exchanges*', available at: https://bitcoin.org/en/exchanges, last accessed 19.8.2018.

[36] Please see '*Coinbase adds support for PayPal and Credit Cards*' (2016), available at: https://blog.coinbase.com/coinbase-adds-support-for-paypal-and-credit-cards-21968661d508, last accessed 19.8.2018.

[37] Numbers for 2017, reports from '*PayPal Reports Fourth Quarter and Full Year 2017 Results*' (2018), https://investor.paypal-corp.com/releasedetail.cfm?ReleaseID=1055924, last accessed 19.8.2018.

[38] Please see I. Kar, '*PayPal is warming up to bitcoin*' (2016), available at: https://qz.com/713528/paypal-is-warming-up-to-bitcoin/, last accessed 19.8.2018.

[39] M. Swan, op. cit. no. 38, p. 11.

[40] Please see J. Wilmoth, '*PayPal Files Patent to Improve Cryptocurrency Transaction Times*' (2018), available at: https://www.ccn.com/paypal-files-patent-improve-cryptocurrency-transaction-times/, last accessed 19.8.2018.

Annex III. – Ripple

Bitcoin is not the only representative of cryptocurrencies. In order to describe the differences between centralized and decentralized transaction systems, this section will briefly focus on Ripple (i.e. Ripple Protocol Consensus Algorithm) as a representative of semi-centralized transaction systems[41].

Ripple shares some basic features and setting with Bitcoin. It is also based on a decentralized ledger, public and private keys and very similar encryption. However, a node does not have to download the whole content of the ledger. Ripple tries to prevent "bloating" and capacity issues by implementing two ledgers – one contains all transactions in Ripple currency (XRP), similarly to Bitcoin (referred to as "state tree"), the other, however, contains only most recent transactions confirmed by the network (called "transaction tree").

In 2004, when the Ripple system was first presented, it had yet not acquired features of blockchains as per Bitcoin's design and was essentially based on limited trust. Each node had to trust at least one other node which then had its own mini network of trusted nodes (frequently compared to Facebook friends network). Transactions were then processed even between complete strangers connected by chain of "friends". The currency was created as corresponding to debts resulting from nodes' interaction.[42] Nonetheless, the system did not grow as expected and in 2012 the network got "blockchainized". As a result, users can chose from two ways of transaction processing: either they know the sender and thus can transact directly, or they do not know or trust the sender and use a gateway. Gateways, while not necessary required, are usually exchanges/trading places which have earned the trust of the network and ensure safe processing.

The most interesting part is that Ripple does not require mining because the consensus is not reached by a proof. Instead each node in the network has a list of trusted nodes "*that are not likely to collude against them*" which is called a UNL ("unique node list"). A consensus is reached by voting – nodes compare the latest version of the ledger and then vote which transaction was received soonest, which is true etc. Due to the fact that nodes vote only when one of their UNL nodes is involved, the majority (80 %[43]) and consensus are reached very quickly, in a matter of few seconds. This gives Ripple a major edge over Bitcoin and

[41] The description of the Ripple network is primarily based on V. Buterin, '*Introducing Ripple: A Detailed Look at Cryptocurrency's New Kid on the Block*' (2013), available at: https://bitcoinmagazine.com/articles/introducing-ripple/, last accessed 19.8.2018.

[42] For more detailed explanation see Ibid.

[43] A. M. Puertas, R. Teigland, op. cit. no. 101, p. 286.

other similar systems – validation of transactions is a lot more energy efficient. From another point of view, there might also be certain consequences. For instance, as Ripple does not need mining and does not provide incentives, its total supply of XRP 100 billion is owned by the founder and will be slowly distributed firstly among users and then among the general public, probably on the basis of auction.[44] This entails significant deflationary effect.[45] Also, while Ripple is well adapted for currency exchange services[46] and payment services and cooperation with financial institutions, such as the example of *Fidor Bank* in Germany, as the network imposes a minimal transaction value threshold (XRP 50, for creation of address XRP 200), the system is not suitable for micropayments, e.g. in connection with IoT. This only proves the vast versatility of the blockchain technology and the fact that not every blockchain is the same.

[44] Ibid, p. 286: "*As of 2017, Ripple has sold XRP 40billion. In May 2017, Ripple announced that they would place XRP 55 billion in an escrow account with a precise schedule to eliminate the fear of an unexpected shock in the money supply. The escrow account contains 55 contracts of XRP 1 billion that expire on the first day of every month. The amount that is not sold is returned to the escrow account and offered after the original 55 contracts have expired.*"

[45] V. Buterin, op. cit. no. 410: "*Unlike BTC, where the total number of currency units in existence increases more and more slowly with every passing year until eventually stabilizing at a permanent 21 million in 2140, the number of XRP starts off at an all-time maximum of 100 billion and then immediately starts permanently decreasing as transaction fees are paid.*"

[46] L. Lee, op. cit. no. 154, p. 32.

Annex IV. – Ethereum

Ethereum is based on a blockchain ledger which works similarly to the one of Bitcoin with the rule of the longest chain and currently deployed proof-of-work mechanism for confirmation of transactions and creation of blocks. It might be worth to mention that Ethereum is planning to switch to proof-of-stake with its upgrade called *Casper*.[47] Ethereum ensures adoption of new confirmation mechanism by making the proof-of-work exponentially more difficult, until it becomes virtually impossible.[48] The miners are rewarded in Ether which is the platform's currency, also similarly to Bitcoin. But that is where the similarities end.

Firstly, transaction fees are not just based on the size of a block. Ethereum comes up with a more sophisticated solution, in order to mitigate or make up for the amounts of computational energy that are wasted for the proof-of-work mechanism. In particular, users have to pay for that energy upfront by way of a fee called gas. Gas is like a fuel for processing of the transaction and is paid in Ether. Due to the fact that Ethereum is primarily intended for self-executing contracts, the more complicated the execution of contract, the more gas is needed during its life-cycle. If a smart contract runs out of gas, the contract is not executed. On the other hand, if some amount of gas is left after all actions in a smart contract have been completed the rest is given back to the originator of the transaction. This is why gas has also been referred to as *execution fee*.[49] Furthermore, the amount of gas can also affect the speed of processing, namely, if the transaction fees are higher, the likelihood that it will be picked up by one of the miners is higher as well.[50]

Secondly, the processing time in Ethereum can be measured in seconds, i.e. the problems which miners have to solve are not as difficult as in Bitcoin.[51] This raises doubts in relation to orphan blocks and double-spend attacks. The higher orphan rates were resolved by implementation of stale blocks which are added to calculations to ensure that longest chains are the true ones.[52]

---

[47] I. Bashir, op. cit. no. 157, p. 249: "*An Algorithm named Casper has been developed, which will replace the existing Proof of Work in Ethereum. This is a security deposit based on the economic protocol where nodes are required to place a security deposit before they can produce blocks. Nodes have been named bonded validators in Casper, whereas the act of placing the security deposit is named bonding.*"

[48] Ibid, p. 244

[49] Ibid, pp 214-245.

[50] Ibid, p. 245.

[51] A. M .Puerstas, R. Teigland, op. cit. no. 101, p. 293.

[52] I. Bashir, op. cit. no. 157, p. 214. The stale blocks are referred to as Uncles or Ommers in Ethereum.

Thirdly, due to Ethereum's focus on smart contracts, the network has two kinds of accounts: (i) so-called externally owned accounts which can only send transactions, similarly to Bitcoin, and cannot execute a code of smart contract, and (ii) contract accounts which can execute smart contracts. However, the distinction should be removed in the near future and all accounts should be enabled to execute smart contracts.[53]

Fourthly, it uses a Turing-complete protocol on top of the blockchain layer. Turing-completeness refers to an "*ability to run any coin, protocol, or blockchain*"[54] and is ensured by Ehtereum's programming language called Solidity which has been often compared to JavaScript, the basis of many applications, such as Gmail or Facebook.[55] The language is stack-based, not binary like Bitcoin which is what enables creation and execution of smart contracts, as it enables unlimited number of contract stages. "*With Bitcoin, the transactions are binary – the Bitcoins are either spent or not spent. With Ethereum, the contract does not have to be fulfilled or not fulfilled, but can be in stage one pre-negotiation, stage two offer, etc.*"[56] Another thing which makes Solidity well-suited for smart contracts is that it is contract-oriented (as opposed to object-oriented) which enables it to understand "*concepts such as identity, ownership, and protection forms*."[57]

[53] Ibid, p. 236.

[54] M. Swan, op. cit. no. 38, p. 21.

[55] L .Lee, op. cit. no. 154, p. 114; also A. M. Puertas, R. Teigland, op. cit. no. 101, p. 292.

[56] L. Lee, op. cit. no. 154, p. 115.

[57] A. M. Puerstas, R. Teigland, op. cit. no. 101, p. 292.