Blockchain: Remedy or Poison?

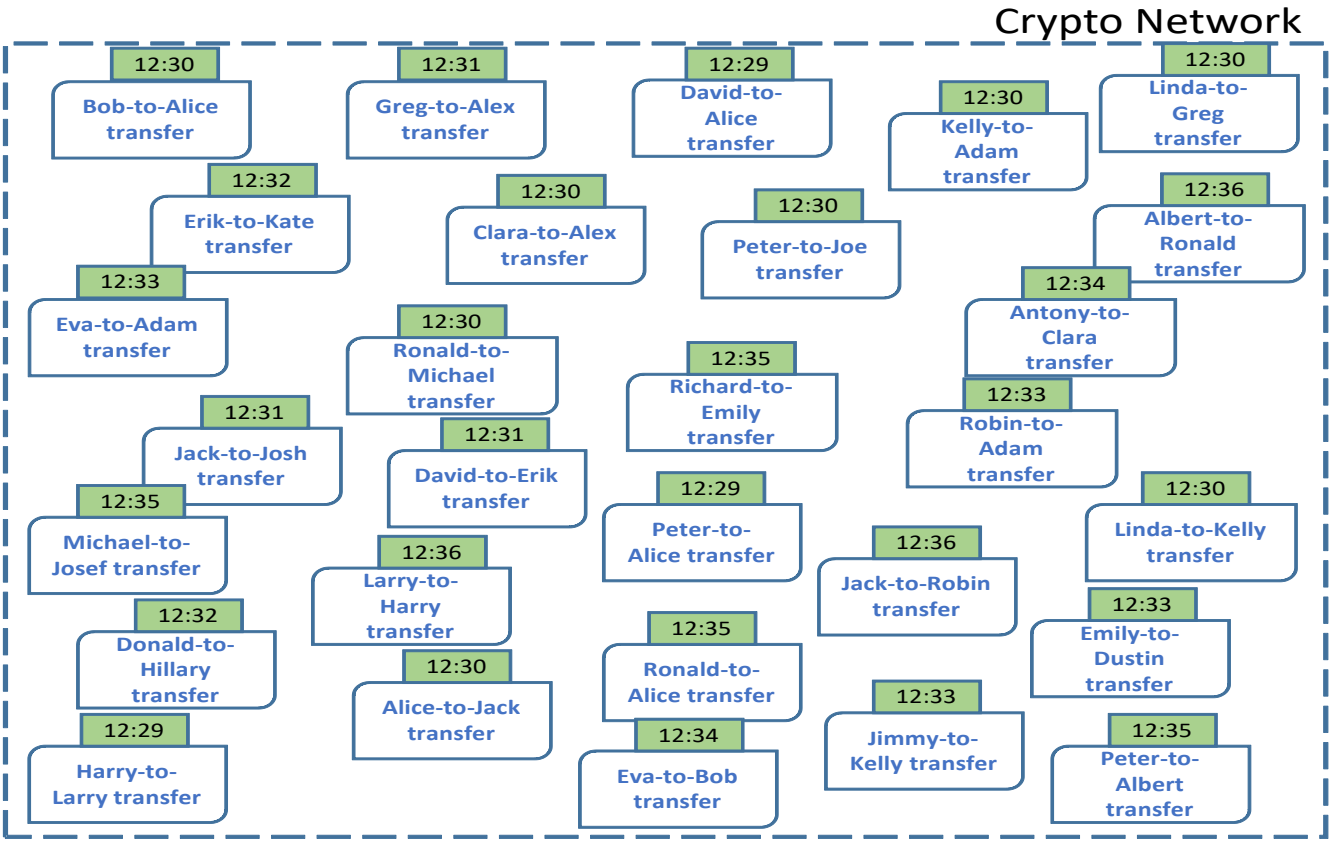
Egger Mielberg
egger.mielberg@gmail.com
31.10.2017

Abstract. We propose a brief analysis of Blockchain technology. Here we try to show as pluses as minuses of this technology in context of storing, intellectual search, analysis and other functionality that is crucial for Big Data System of any kind. We also share our vision of future development of crypto market.

1. Introduction

«Blockchain» — public ledger that stores crypto transactions in a form of blocks. The block transactions are used to be executed at the same time, approximately. The block, meantime, is formed by people, called miners that, *first*, aggregate all the transactions with the same execution time in Crypto Network, *second*, calculate a cryptographic hash value for each block. A given hash value, as for «Bitcoin Network» must satisfy specified criteria.

Further, for better understanding «What Blockchain is?» let's have a look at some pictures below.

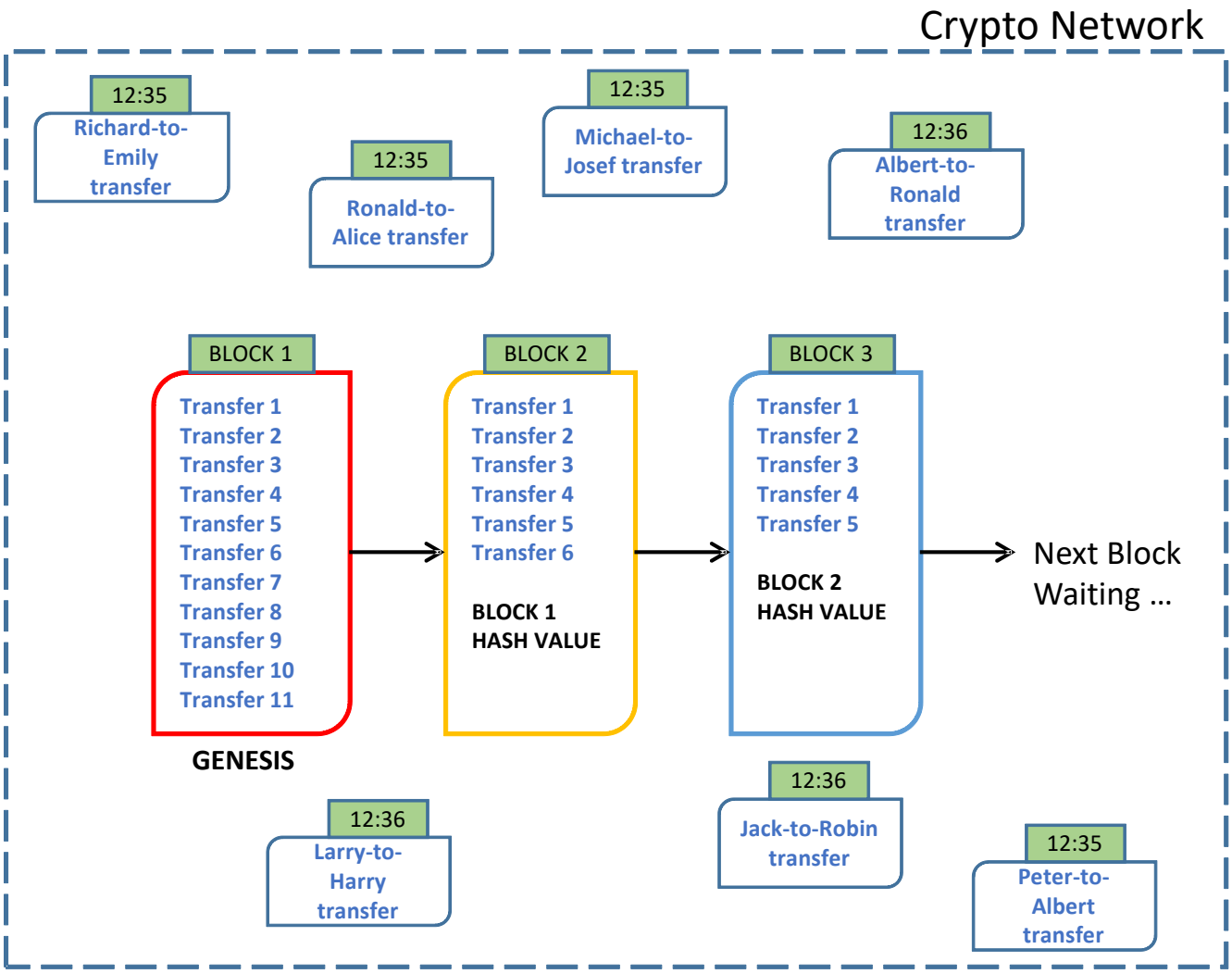


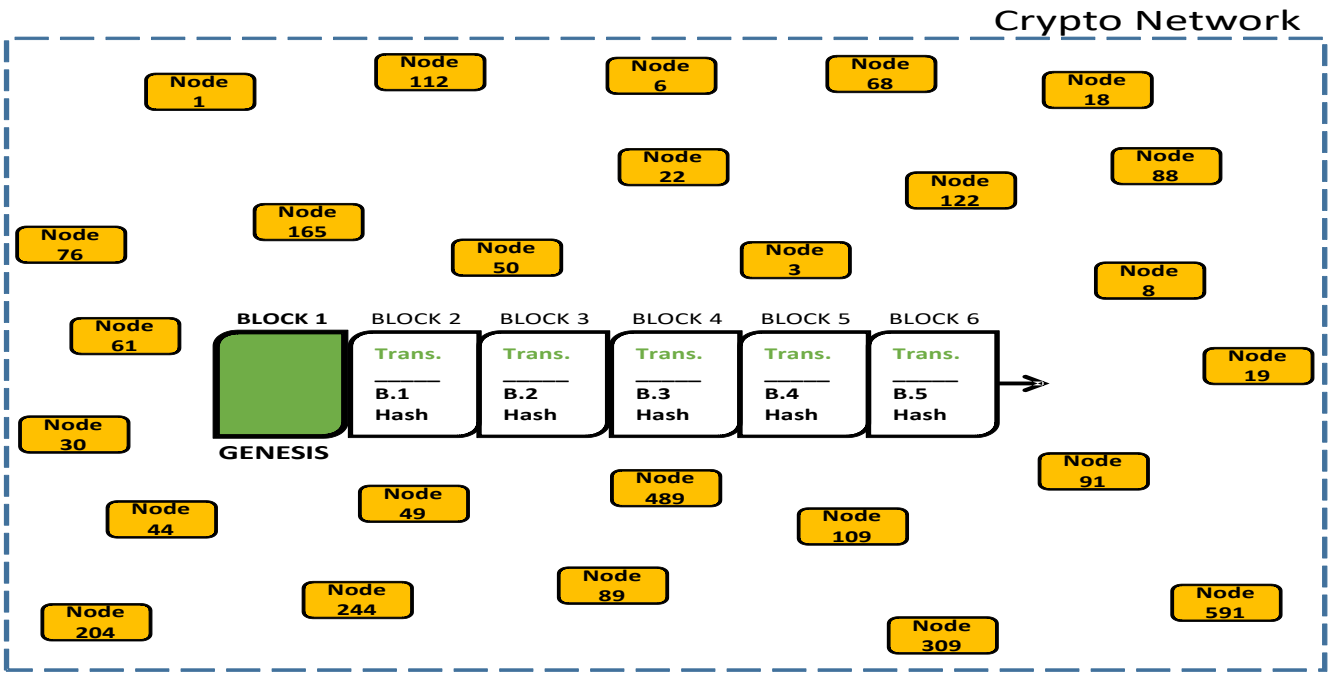
«Crypto Network» - network where each registered user who has a digit wallet can transfer or receive some sum of crypto money (bitcoin, dash, ripple, ether, etc.).

The block consists of a group of transactions which the miner aggregated and hashed for generating a single hash value. For example, the block 2 will consist of own aggregated transactions and hash value of the block 1. *Thus, hash value of any block, besides first block, will always be calculated by using as own transactions as the hash of previous block.* The hash value of the previous block and the current one can be calculated by the same miner or other miner. Two and more blocks form «Blockchain» architecture.

One more time, each subsequent block includes hash value of previous one.

«Genesis block» — first block that initiated «Blockchain». This block doesn't have any hash value of other block.





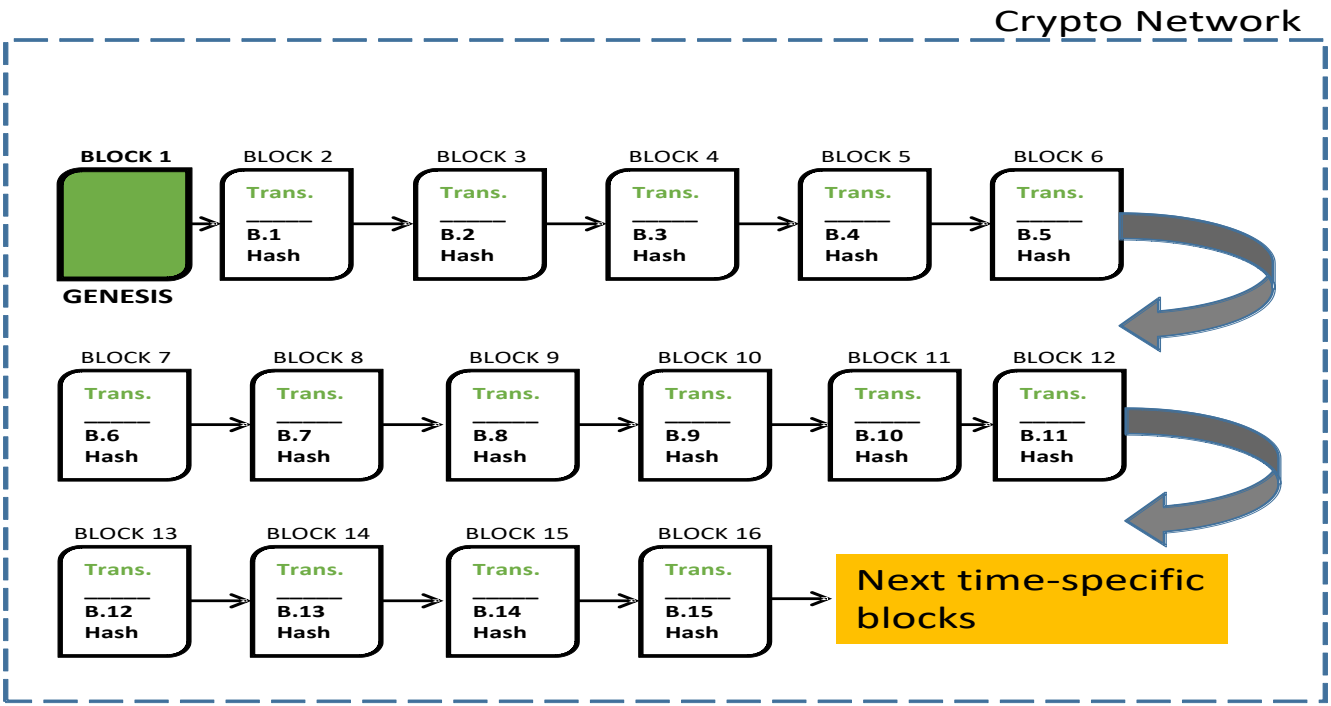
2. Pluses

In order to get clear presentation about necessity of usage of Blockchain technology let's go over its pluses:

- *Complexity in changing data of blocks.*

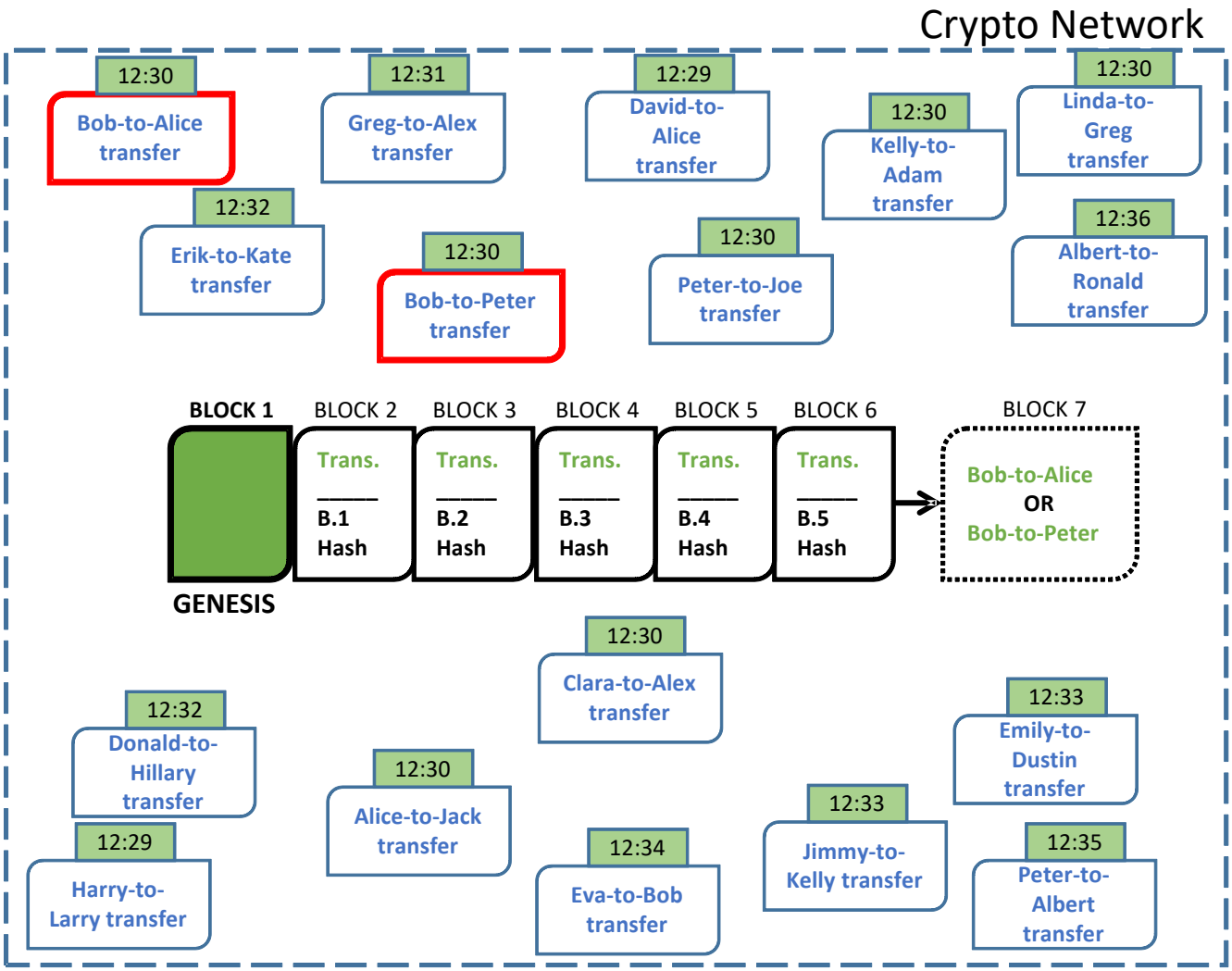
For example, if a criminal wants to change data of, say, block 2 he will need to recalculate hash values of all successive blocks, block 3, block 4, block 5, etc. That is unlikely possible as a formation of new blocks takes place each 7-9 minutes, approximately. It is always less than 10 minutes.

- *Decentralization of Crypto Network.*



In Crypto Network, there is no central chief node (computer) that would have any «Read/Write/Update» privileges compared to other ones.

- *Tracking «double spend».*

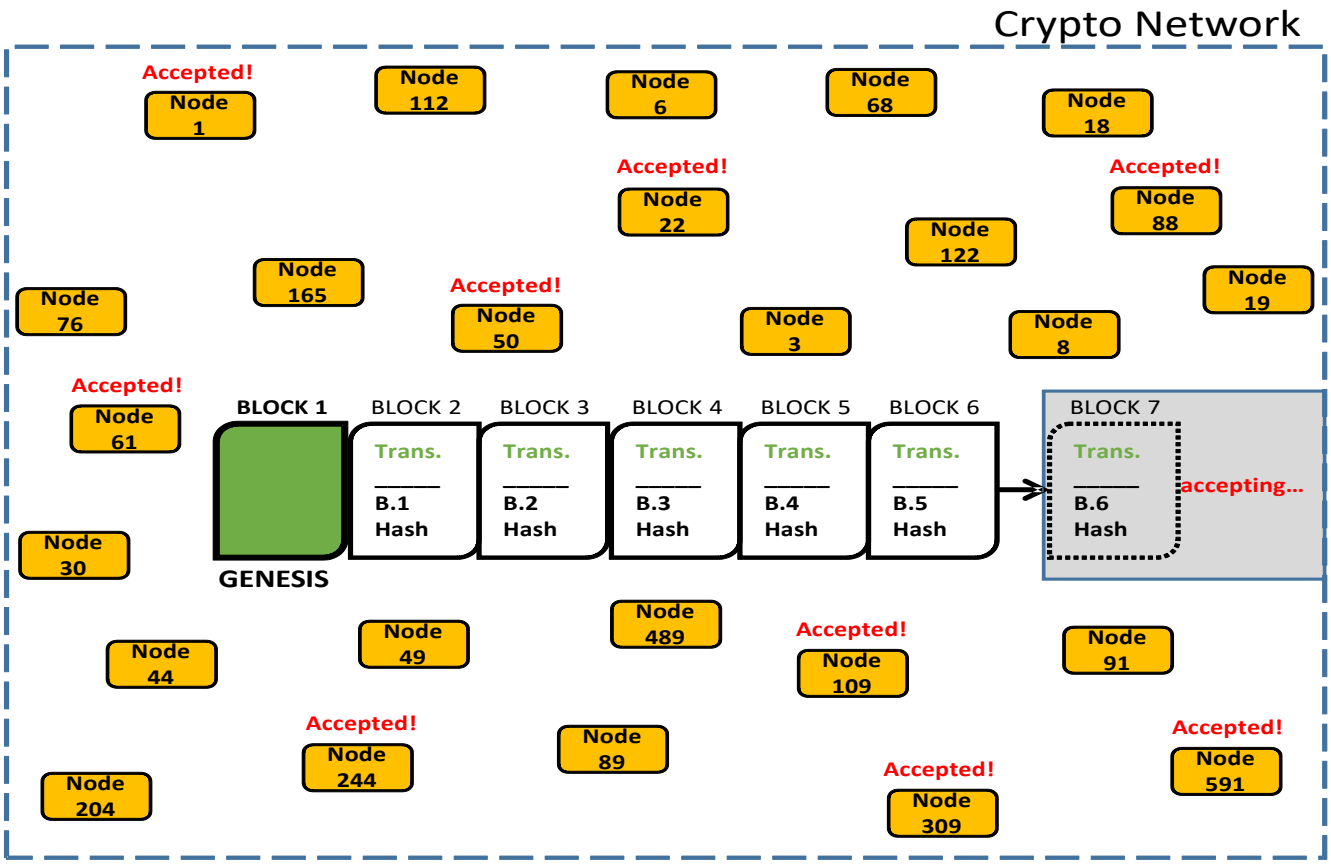


For example, if, say, Bob has 5 crypto units (bitcoins, ethers, etc.) that he decides to send to both Peter and Alice at the same time. As soon as one of the following events being happened first, «Peter or Alice receives 5-crypto-units-transfer» or «one or many of Crypto Network participants check Bob's income/outcome crypto units», time second transfer will immediately be blocked.

- *Constancy of blocks data.*

At any time, data of blocks will be permanent. In other words, if you have generated hash value of, say, block 765, so that value would have been valid at the time of generating, say, block 1 678 543.

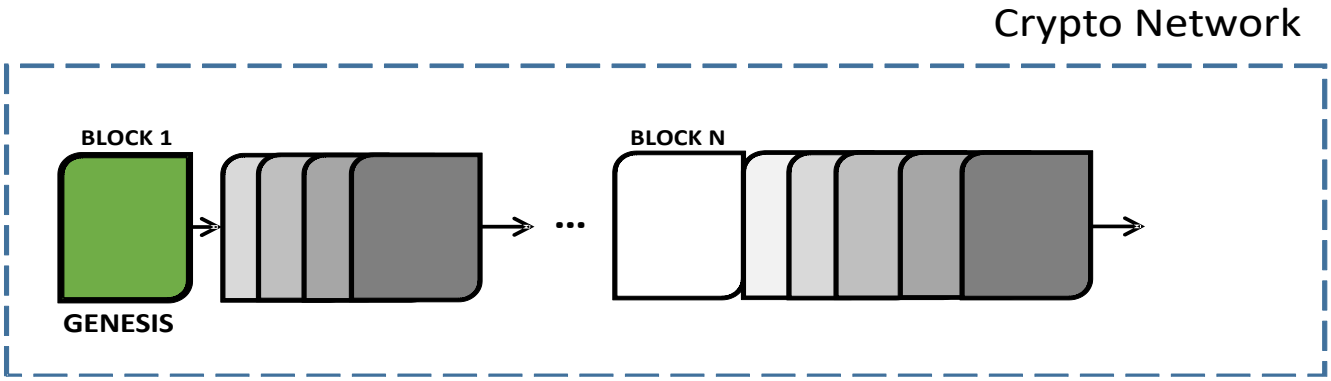
- *Independence of Crypto Network participants.*



Before inclusion of «just-formed» block into «Blockchain» the participants check correctness and consistency of the block data. The participants are independent of the block transactions being accepted.

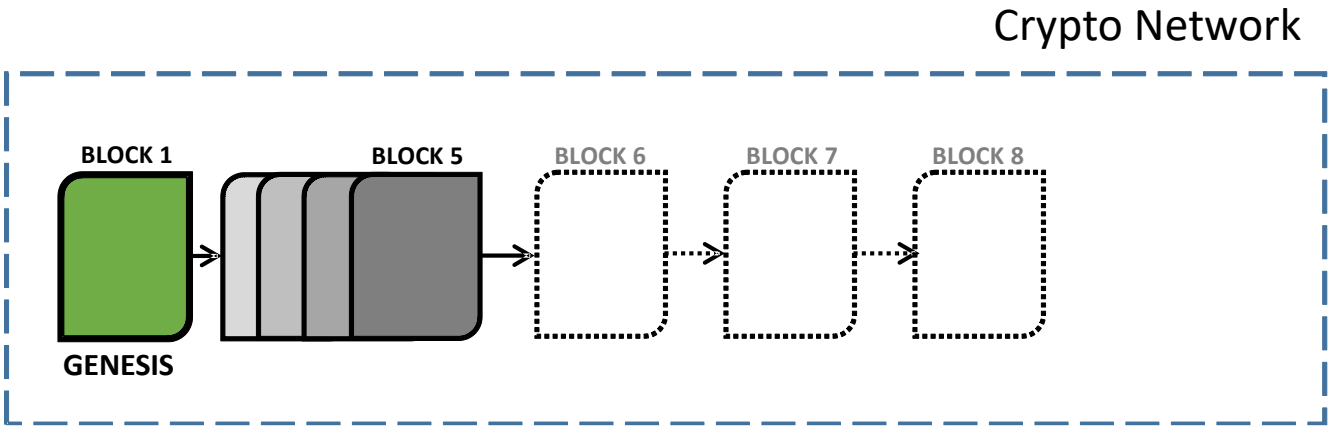
3. Minuses

- *Extremely inefficient storing, searching and extracting of Big Block Data.*

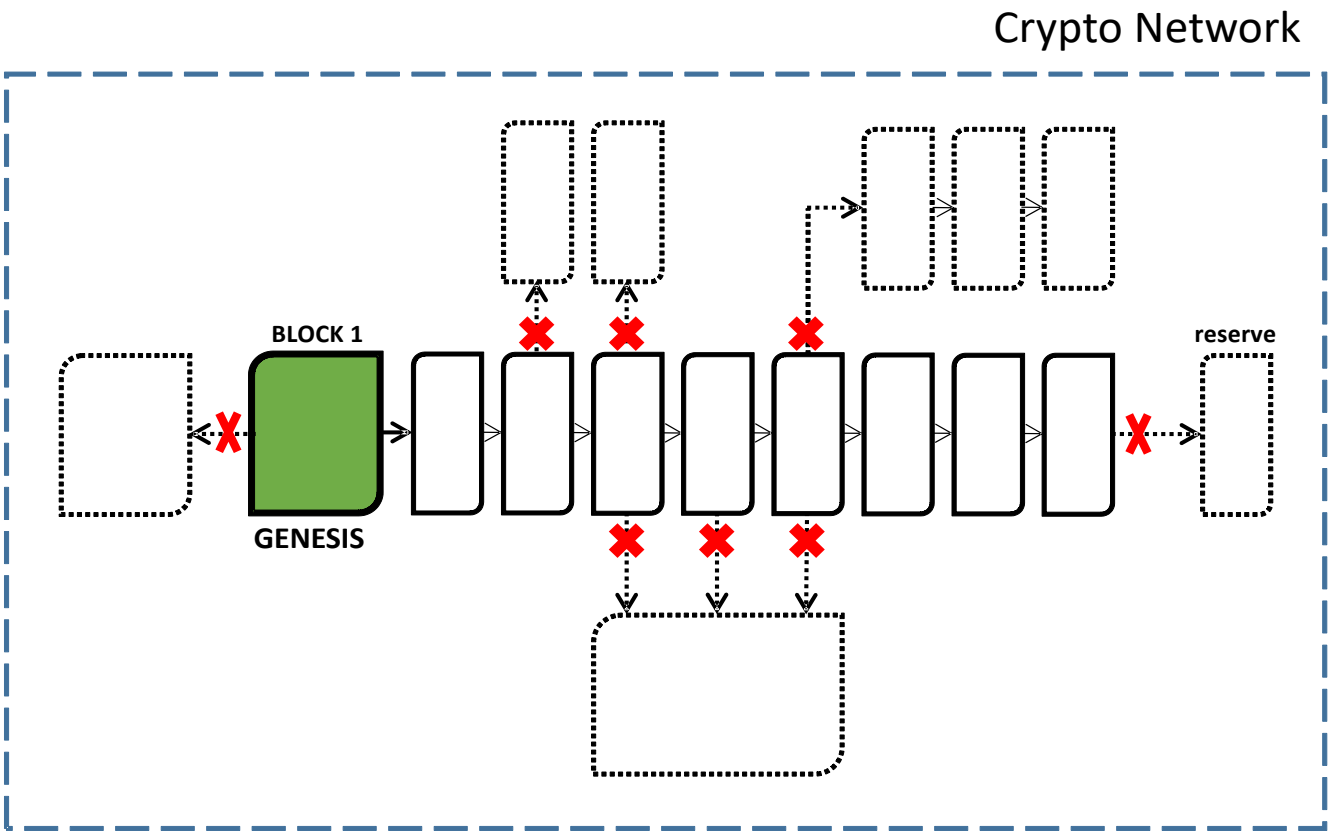


For data extraction from, say, block N any «Blockchain» system will first need to step-by-step iterate all the blocks from the left (right). Then, the block N must be deciphered. Moreover, the blocks don't have metadata, short data description for a quick and qualitative search.

- *Long period of waiting time for getting transaction status «Protected».*



In other words, if your transaction was included in block 5, for security reason, you will be strongly recommended to wait for another consecutive blocks.



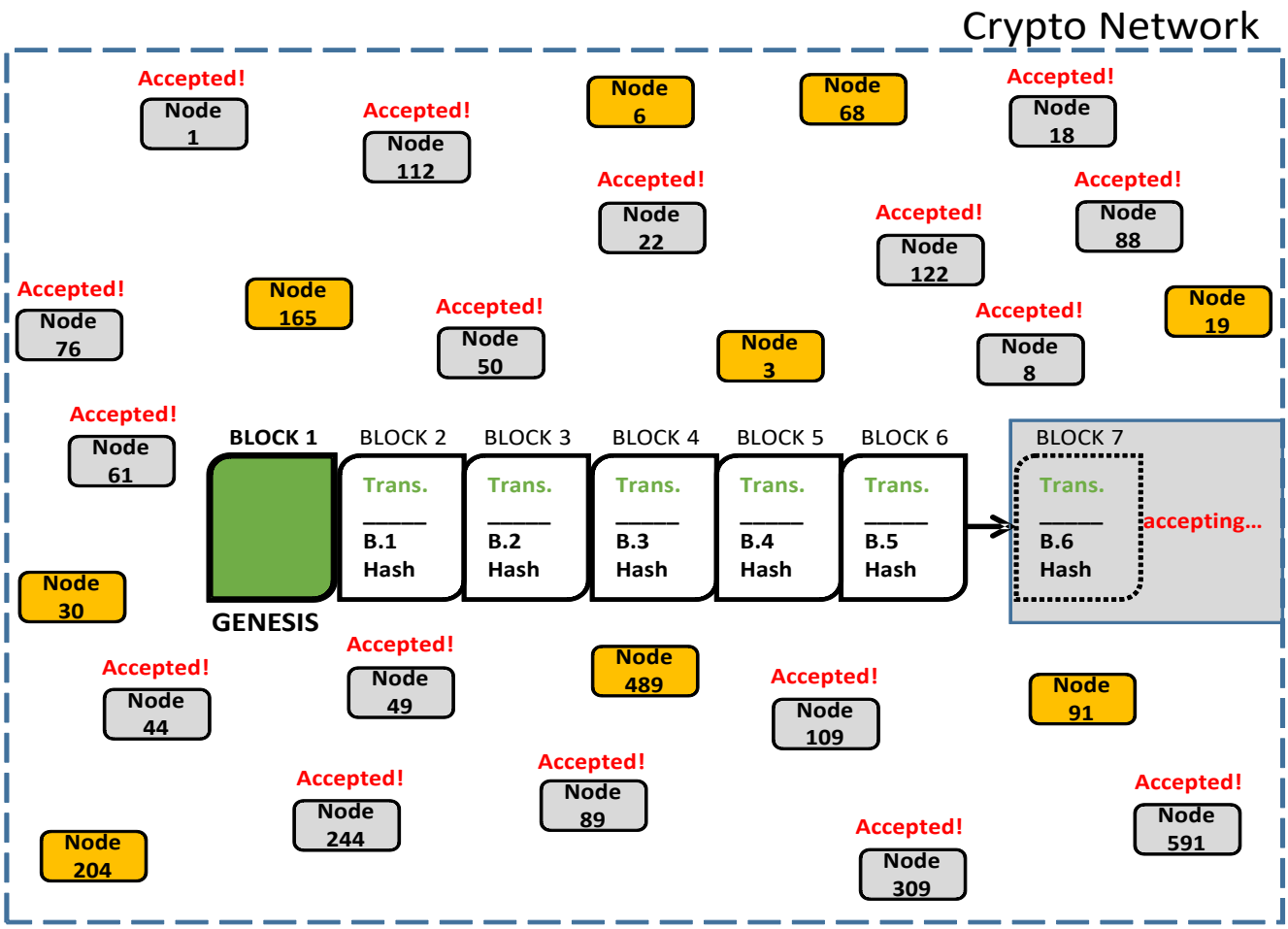
- *Linear architecture of «Blockchain».*

Scalability is not supported by nature of «Blockchain». *First*, data of one block can not be split into pieces and store in an other block. *Second*, addition of an empty block ahead is impossible.

- *Impossibility of realization of intellectual blocks-data analysis.*

In order to find a relevant information in any blocks, the ones must be deciphered and then indexed. «Decipher-Then-Index» procedure has to be executed on each block of «Blockchain» until the relevant information is found.

- *Direct dependence on miner's honesty.*



For example, if number of criminal nodes (computers) exceeds the number of trusty nodes then the task of accepting of a new block may be under question.

- *Exponential growth of complexity of forming a new block in case of increasing total number of miners in Crypto Network.*

In other words, if you are not a millionaire you won't have a chance to form even a single transaction block as your computer even super up-to-date would need years to get this block formed.

4. «Blockchain» as a remedy.

«**YES**» – One record, one immutable origin.

«**YES**» – No chance for changing block data.

«**YES**» – No central management node.

«**YES**» – Tracking transaction's correctness.

«**YES**» – Safety and time invariant storage for transaction data.

5. «Blockchain» as a poison.

«**NO**» – Data classification.

«**NO**» – Intellectual data analysis.

«**NO**» – **Fast transaction processing.**

«**NO**» – **Scalability.**

«**NO**» – Data defragmentation.

«**NO**» – **Smart search.**

«**NO**» – Minimum of needed energy.

«**NO**» – **Peer mining.**

«**NO**» – Functional superiority over fiat IT market.

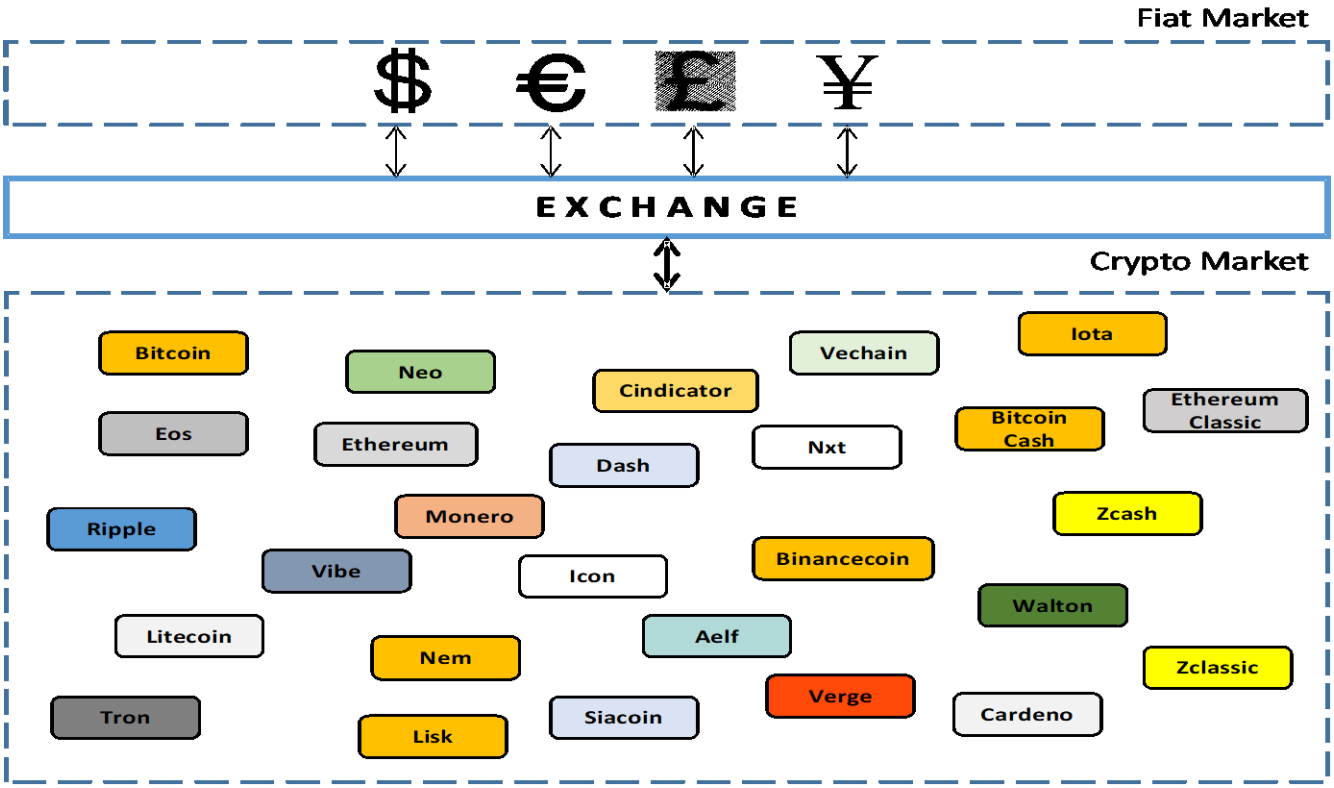
«**NO**» – Transparency.

«**NO**» – **Replacement of current financial (bank) technologies.**

In spite of the fact that «Blockchain» has many minuses, there are also many businesses' fields where it may be extremely useful.

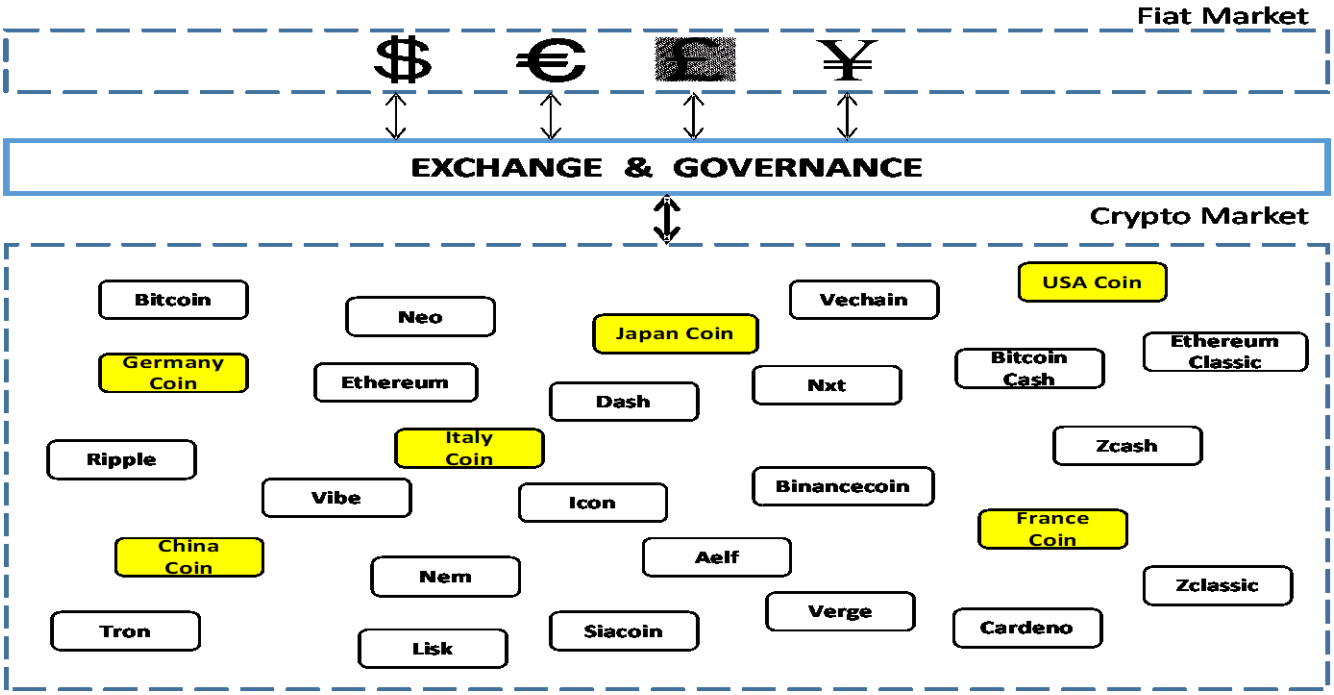
In conclusion, I would like to stop on, as it seems to me, the most important moment of «Blockchain» technology, namely its *integration into current fiat IT market*. Our experience tells us that there are three main ways of that integration:

Number 1.



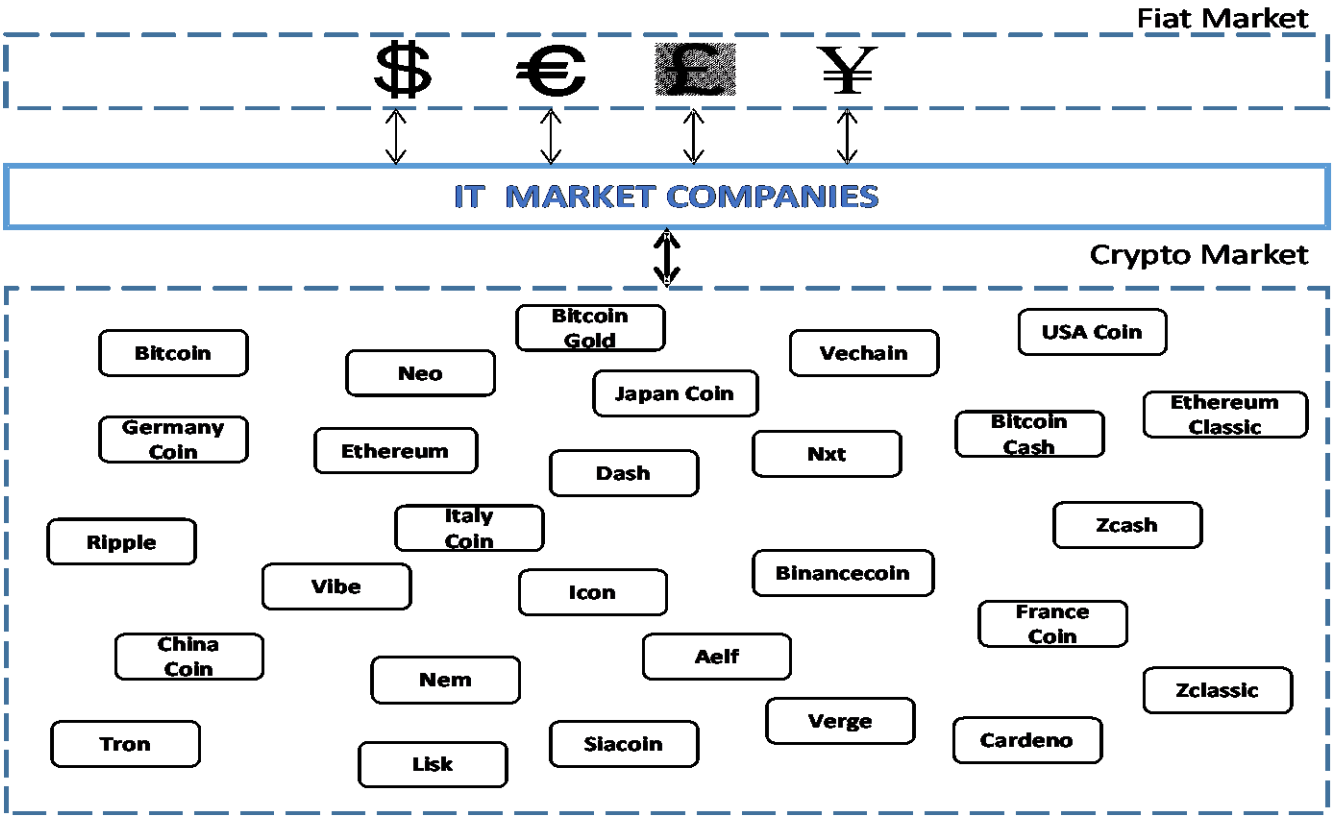
On the first way, all cryptocurrencies will only be supported by doubtful guarantees of its emitters. Volatility will stay on a high level because of absence of direct dependence on fiat IT market.

Number 3.



On the third way, besides private emitters the Crypto Market will have countries with its own cryptocurrencies. The main purpose of that countries will govern as private cryptocurrencies as crypto market as a whole.

Number 2.



On the second way, ***more perspective and favorable***, the fiat IT companies will be integrated by one of two following approaches:

1. Emission of own cryptocurrency.
2. Addition of payment method by using any cryptocurrency.

Perspective of the second way is that the crypto market will directly depend on current fiat IT market. And level of volatility will totally depend on IT market development.

References

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2008

[2] " Understanding Blockchain Technology - DBS Bank", DBS Group Research, https://www.google.ru/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwia7JPL-P3aAhWFVSwKHRF7AUUQFggnMAA&url=https%3A%2F%2Fwww.dbs.com.sg%2Ftreasures%2Faics%2FpdfController.page%3Fpdfpath%3D%2Fcontent%2Farticle%2Fpdf%2FAIO%2FAIO_2016%2FSECTOR-19-001-blockchain-lowres.pdf&usg=AOvVaw2pPJbt-wvfeFJyqityyItC, 2016

[3] Philip Boucher, Susana Nascimento, Mihalis Kritikos, "How blockchain technology could change our lives", http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf,

2017
[4] "DEMYSTIFYING BLOCKCHAIN", Cognizant, https://www.cognizant.com/whitepapers/demystifying-blockchain-codex2199.pdf, 2017
[5] Marco Iansiti, Karim R. Lakhani, "The Truth About Blockchain", https://hbr.org/2017/01/the-truth-about-blockchain, 2017
[6] "The Developing Role of Blockchain", World Energy Council, https://www.pwc.se/sv/pdf-reports/energi/the-developing-role-of-blockchain.pdf, 2017
[7] Karl Wüst, Arthur Gervais, "Do you need a Blockchain?", https://eprint.iacr.org/2017/375.pdf, 2017
[8] Jun Kogure, Ken Kamakura, Tsunekazu Shima, Takekiyo Kubo, "Blockchain Technology For Next Generation ICT", https://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol53-5/paper09.pdf, 2017
[9] Roman Matzutt, Jens Hiller, Martin Henze, Jan Henrik Ziegeldorf, Dirk Mu¨llmann, Oliver Hohlfeld, Klaus Wehrle, "A Quantitative Analysis of the Impact of Arbitrary Blockchain Content on Bitcoin", https://fc18.ifca.ai/preproceedings/6.pdf, 2017