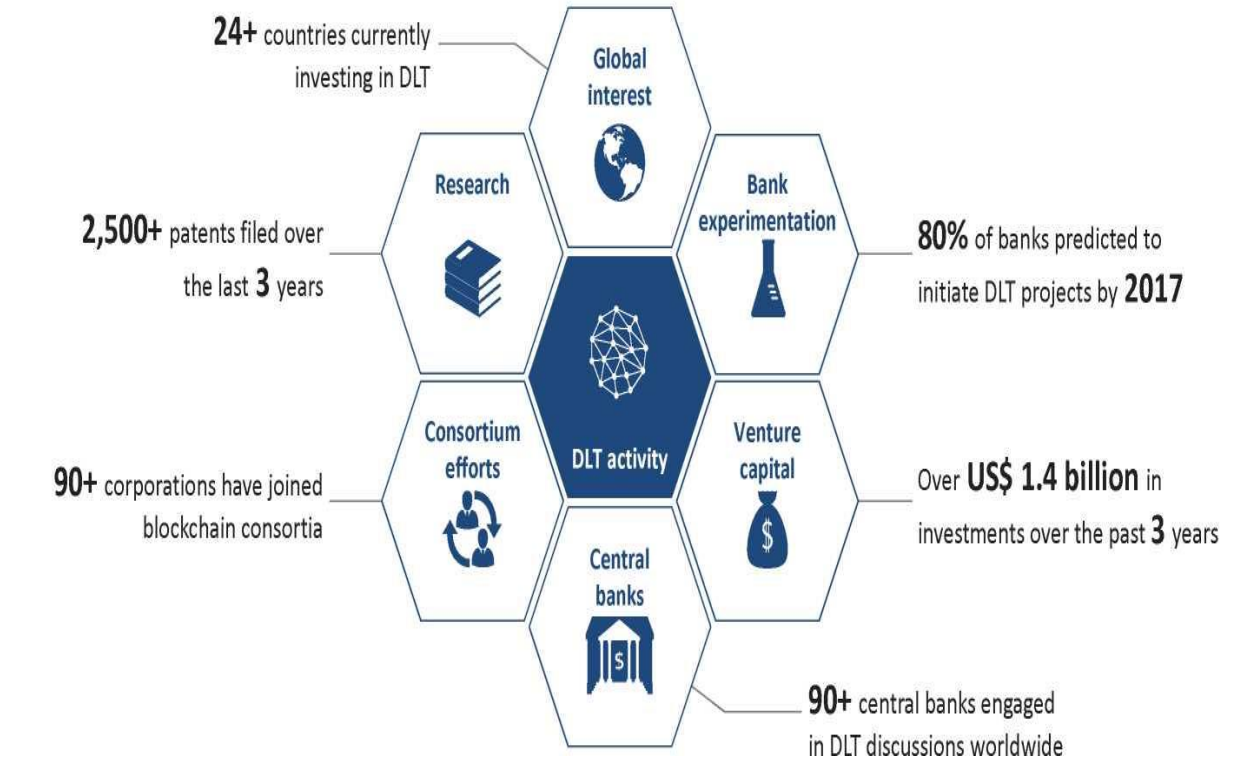
2017

RCieSolution … above digit

Concept Tower
Grzybowska 87
00-844 Warsaw
T.+48 22 4795967

DISTRIBUTED LEDGER TECHNOLOGY AND BITCOIN REVIEW – BASIC CONCEPTS

We believe in the potential of bitcoin and blockchain technology to have a significant, positive social impact.



World Economic Forum ” The future of financial infrastructure” August 2016, p.14

WEF key conclusions on Distributed Ledger Technology (data from a graph as it faces dynamic market may differ significantly from the current):

• DLT has tremendous potential for financial services infrastructure thanks to the simplicity and efficiency it offers.

• DLT is not a panacea; Instead, it should be seen as one of many technologies that in the future can become the leader in the context of the revolutionary evolution of financial services.

• The use of DLT technology will vary from case to case, each using the technology in different ways to differentiate the benefits.

• Digital identity is an important factor for expanding the use of technology

• The most influential DLT applications require close cooperation between current operators, innovators and regulators

• The new DLT-based financial services infrastructure will overhaul business processes while questioning some of the existing ones

• Operational simplification DLT reduces / eliminates the manual efforts required to settle and resolve disputes

• Improving Regulatory Efficiency DLT enables real-time monitoring of financial activity between regulators and regulated entities

• Reduction of the counterparty risk DLT reduces the counterparty's risk in fulfilling obligations as the contracts are codified and executed in a common, unchanging environment.

• Liquidity and improved capital DLT reduces capital blocked and ensures transparency in acquiring liquidity assets

• Minimizing DLT scams allows to set up a resource base and complete transaction history in one real source

Blockchain, a cryptographic technology associated with the virtual bitcoin currency, is becoming an area of interest for investors, banks, consulting and technology companies, and governments. It has a chance to become a new foundation of the infrastructure of the global financial system and to change the balance of power. This technology is seen as a tremendous opportunity to reduce transaction costs, accelerate transactions, make them clearer and safer, and a great challenge, as it eliminates intermediaries, such as banks and clearing houses. The concept of decentralized databases - or the so-called blockchain - captures the financial services sector by storm, with venture capital investing in startup ventures. The debate on the possible use of Blockchain technology and its limitations continues for good. Next to anyone who believes that blockchain is the most revolutionary technological platform since the Internet, skeptics of this technology have come up against it by seeing it as a next tulip mania. The widespread consensus that blockchain is an innovative discovery with broad possibilities of

implementation in the area of financial and banking services is a growing phenomenon. There has been a genuine influx of market participants and initiatives, including startups and emerging consortia focusing on technical standards and promoting cooperation in the area. Consistent recording of data in an invariant manner causes that the network consensus is a continuous process, the books are updated with the same data in the same order, and the data entered can not be modified by a single participant. Databases are replicated by network participants, and their correctness is verified using a defined algorithm. Data input is transparent and comprehensive, and market participants have access to real-time data. Data is authorized by "fingerprint" using one-way encryption. Data integrity in approved books, identities and permissions are checked against each transaction. The so-called "smart contracts" allow to implement business logic and workflows into database structures with the option of updating the book on contractual terms. Robust and flexible data environment provides greater capabilities in the area of data analysis and reporting. Some analysts believe that the impact of the blockade will be limited to services and processes called facilities. Early efficiency gains are most evident in the middle and back office areas through data standardization, trade facilitation and simplified infrastructure. However, when real assets - digitally represented by tokens or smart contracts - can instantly change the owner, there is a moment to talk about innovation. Flexibility of settlements will allow new pricing models and new service offerings. In addition to better data management, the ability to verify assets using a database creates new opportunities against a traditional database. The account of such defined digital assets will significantly reduce the risk of collateral management and the continuous valuation of underlying assets will improve the valuation of the assets-backed securities. The question of whether the decentralized nature of the distributed database will be the key to adoption in the traditional market still remains. It seems that the blockchain will change the structure of the market, the possibilities offered by the products, the experience and perception of customers, thus changing the image of the global economic market.

Bank industry representatives (JP Morgan) expect the following three waves in the next 15 years of the blockchain technology development :

2016-2019: Blockchain used for sharing and transmitting data

• Used internally and between trusted external organizations

• Distributed Ledger Technology solutions tested as proof of concept parallel to current workflows

• Extension of existing processes

2017-2025: Blockchain provides an environment for storing and controlling data

• Incorporation of existing Distributed Ledger Technology into existing solutions, supporting efficiency in operations and workflows

• First pilots may run in parallel with existing processes until the user trust is high enough to start migrating volumes.

• Users have a choice of many infrastructures developed by the vendors

2020-2030: Blockchain adopted by market participants as the main infrastructure for critical functions

• Centralized authority (supervision) still needed to execute administrative functions (granting access rights, setting industry standards)

• Replacement of existing infrastructure assets, transactions and payments

• Participants are forced to adopt and integrate with a new infrastructure based on blockchain technology

*

The Wall Street Journal

"No digital currency will detoxify the dollar quickly, but bitcoin is more than just currency. It is a radical new decentralized management system, a way of exchanging wealth in society. To put it simply, it is one of the most powerful innovations in the financial world over the past 500 years. "

*

"In my opinion, it's amazing that in the bitcoin world, the algorithm takes over the functions typical of the government." - Al Gore, former US vice president, Nobel Peace Prize laureate

July 2016: Bank of America, Merrill Lynch, HSBC and the Singapore-based Infocomm Technology Regulatory Commission have announced total digitization of a key foreign currency settlement instrument - a letter of credit.

Jaimie Dimon: In a letter addressed to the shareholders, "In many areas, blockchain will replace the current centralized business model in financial services."

June 2017: The Singapore Diamond Investment Exchange (SDiX) announced a partnership with Kynetix and Everledger to complete the first stage of Proof-Of-Concept block authorization and secure document storage service for diamonds on the global commodity exchange.

Some banks are involved in consortia that try to test new technological possibilities. The New York R3CEV consortium brings together 40 banks and financial institutions led by Goldman Sachs and the Linux Foundation. Its purpose is to create a financial infrastructure to serve the SME sector. Similar agreements have been concluded by BNP Paribas Securities Services, Caisse des Dépôts, Euroclear, Euronext, S2iEM and Société Générale. Other banks such as USAA and BBVA have invested millions of dollars in Coinbase and Circle startups to test the use of blockchain technology. Barclays and Fidelity, in turn, have created technological accelerators. While in the United States, Depository Trust & Clearing Corp. proposes to completely change the reporting infrastructure and the terms of the Credit Default Swap Instrument (CDS), the Australian Securities Exchange (ASX) is introducing a pilot project based on blockchain technology. The Bank of England and the European Securities and Markets Authority (ESMA) have published a commentary on the feasibility of digital cash and distributed ledger technology (DLT). The tone of talks with "Is it worth to develop?" (Blockchain) evolves toward "How best can we get involved?" Santander Bank participates in the Ripple project and tests DLT technology in corporate banking and settlements. Julio Fara, vice president of research and development, "... if the banks are working to develop a comprehensive DLT technology plan, they will not move forward. It is more about solving problems, demonstrating the benefits and thus developing the whole organization. " The most promising uses of blockchain technology, according to the Bain & Company and World Economic Forum (WEF) analyzes, are the areas of international payments (correspondent banking), trade finance settlements and domestic payments. There are three criteria to be considered: value of revenue, ability to automate operations by digitizing paper processes and eliminating intermediaries.

Will blockchain technology be the foundation of a new global finance infrastructure?

For this to happen, not only technical problems (efficiency and capacity issues) must be solved, but also macroeconomic and legal issues. Establishing

common standards so that many distributed solutions create a common system requires transnational regulation, as the development of new technologies often takes place in a precarious legal environment. The issue of digital identity and so called smart contracts that play a key role in the automation of transactions. Smart contracts carried out using blockchain should, in principle, include a set of conditions to which the parties agree, and the circumstances in which the action must take place. Smart contracts are not based on new technology, they are rather "stored procedures" that initially appeared in SQL databases. The most basic level of smart contracts can be considered in relation to the provisions of commercial law. It is practically impossible to commit fraud as an unauthorized change of ownership of assets, not only because of cryptography - it would also involve the change of all the blocks that preceded the transaction. This aspect, in turn, means a completely different philosophy of AML and Know Your Customer politics. DLT technologies are still undergoing testing and experimenting for the time being. However, there are some examples of practical solutions. The Ripple Company, invited by the Federal Reserve to the Fast Payments Working Group, has developed a digital platform that enables financial institutions to real-time trade in currency, commodity and other assets without the help of traditional intermediaries.

Faced with the presence of pilot projects, many of the challenges ahead of the technology of distributed registers can be considered ready for use by companies. Security, privacy and scalability remain one of the biggest technical challenges that must be addressed and legal and regulatory feasibility remain a major obstacle to further technological development. Blockchain technology, in all its forms, evolves very quickly. Problems that seemed difficult a year ago, such as single digit, transaction bandwitch per second, today are seen differently.

Industry convergence on the desire to get approval, opened the door for registers for faster consensus on the algorithm and the possibility of more transactions per second. Challenges such as privacy, security and regulatory transparency still remain. Implementing smart contracts still requires robust security solutions for audit techniques and a code of good practice for blockchain developers as well as the enterprise system. Promising is, that regulators and legal experts are increasingly involved in publishing documents and submitting proposals. Most of them concern legal issues related to the use of digital property rights. There is still much work to be done to bridge the gap between conceptual evidence and real production systems. The convergence of technologists, stakeholders and goverment agencies can lead to consensus.

The biggest challenge will be the rapid implementation of these issues, following the pace dictated by the evolution of technology.

The Bitcoin system transfers the amounts between public accounts using public key cryptography. Transactions are public and stored in a distributed database. In order to prevent double spending, the network implements a type of distributed time server, using the string of mathematical proofs of the actions performed (Proof of Work). The transaction history must be stored in the database, and the tree of the hash function is used to limit the size of the database. Every Bitcoin user installs on their computer a client program that generates a wallet (Bitcoin Wallet) containing any number of cryptographic keys. Public keys, also known as bitcoin addresses, act as source and destination for all payments. The corresponding private keys authorize payments only for the user who owns them. Addresses do not contain any information about their owner and are usually anonymous. Addresses that correspond to classic bank account numbers are alphanumeric strings of approximately 34 characters, excluding the 0, the capital letter O, the capital letter I, and the lowercase letter i. You may have multiple addresses, even for each transaction. It can generate new addresses without any restrictions. Generating a new address is quick - it actually boils down to the client program designating a new public-key pair, which does not require contact with the rest of the network. Creating single-use addresses used for a single purpose increases the degree of anonymity of the user. Transfers are made directly without the use of financial operators run by third parties and can not be refunded. Transactions are similar to those of electronic signature technology. Each Bitcoin coin is digitally signed by the ECDSA (Elliptic Curve Digital Signature Algorithm) of its owner. When he transfers a number of bitcoins to the other user of the system, he renounces their possession by adding the public key of that user by signing it with his own private key. Then he announces his transaction in a message sent to a peer-to-peer network. When the new owner wants to pay his coin to someone else, he re-signs his private key using the new owner's public key. The system creates a register of all transactions from the beginning of the existence of the network in the form of the so called block chain (Blockchain), which is made public by saving it to a publicly accessible registry. Each block consists of a header that distinguishes it from other blocks, and a list of transactions. The block chain is formed by combining it: block n points to block n-1 by activating the hash function of n-1 block contents. Since this block contains the function of the shortcut of the n-2 block, the shortcut of the last block in the chain is dependent on the shortcut of each previous block of the chain. If two nodes recognize the indicated block shortcut in the chain, they simultaneously agree to all other blocks. With this property it is impossible to fake a single block - it would invalidate all previous ones. Bitcoin uses the shortcut function RIPEMD-160 on the public part of the ECDSA key to serve as a unique identifier for the location to which the bitcoins are sent. The network

checks the correctness of digital signatures and the number of coins used before accepting them. A transaction sent to other nodes does not immediately become valid until it is placed in the chain of blocks, labeled with a time stamp and acknowledged. To this end, each generating node (issuer) collects all unacknowledged transactions. Then it tries to calculate the hash of this block with certain features, which requires a predictable number of trials and errors. When it finds a solution, it announces it to the rest of the network. Nodes receiving the newly resolved block, check its correctness before accepting and adding to the chain. Ultimately, the chain of blocks contains a cryptographic history of changes in the possession of all coins, starting with the address of their issuer, up to the address of the current holder. That is why if a user tries to reuse a previously issued coin, the network rejects the attempt to execute the transaction. Bitcoin's creator (creators) proposed using the so called hashcash (CPU cost-function) that can be used as the proof of work (Proof of Work). Work is being performed by some system users in a heavily-enforced transaction verification process that requires high-performance computing in specialized workstations configured with the most powerful CPUs, CPUs, FPGAs, and so on. This process is called mining, and the open-source program for this service is Miner. Workstations for "digging" are "diggers". The proof of work procedure consists of calculating the SHA-256 shortcut function for a new block created by excavators that listens to all new transactions (purchase, sale, donation) that have occurred since the creation of the previous block. On this block, the diggers run a hash algorithm based on the preceding shortcut, and a randomly selected nonce value so that you can create different hashes from the same data. When the smallest possible hash is found, the software announces that it "won the race to the next major block". Then it is rewarded with 25 new (now) branded bitmaps.

After every 210,000 verified blocks (roughly every 4 years), the prize awarded is reduced by half. In the history of the Bitcoin system, such reductions have already taken place once and the initial award of 50 bitcoins per block dropped to 25 bitcoins. Such a reduction of the prize approximately every four years will continue until about 2136 (16.08.2017: 16 510 513 bitcoins mined with respectively no more than 21 million in the future). The value of the last prize will fall below 10-8 bits per block, which is below the smallest bitcoin, called satoshi (1 satoshi - 0.00000001 bitcoin).

Calculating a shortcut for a given data is relatively simple, but the algorithm requires that the shortcut meets the specified condition, eg to have a certain number of zeros at the beginning. It is impossible to predict in advance what the value of nonce variable will give the correct result. The shortcut functions must be calculated until the result is correct. Anyone on the network can see if the creator of the block has actually created it, whether it has placed only significant transactions in the block and

whether it has made 25 coins for itself. This information is available at blockexplorer.com. It is worth noting that the calculation of the SHA-256 shortcut function is needed primarily to authorize transactions made on the Bitcoin network by other users, thus confirming the transactions that took place. The described solution combines the authorization and emission procedures, because in essence, the issue of currency is rewarding the work of the authorizing persons. The probability that a given digger will receive a lot of coins depends on the ratio of the computational power contributed to the network through it to the sum of computational power contributed by all nodes. Miners can also generate bitcoins acting as a group, respectively dividing the spoil. Nodes in the network evaluate every two weeks how many blocks have been created, and independently modify the difficulty of such digging operations so that, on average, a block is generated every 10 minutes on the entire network. In this way, the money supply is reduced without the central server. According to the procedure in the software, the number of possible "dug" bits will decrease from zero to a total of no more than 21 million. This will happen in 2136. Existing transfer money in the Bitcoin network may already have a small transaction fee. This is not mandatory, but it speeds up transaction authorization as it encourages diggers. To run the generating software, especially since the difficulty of digging is generally increasing and the dredge is decreasing with time. Nodes collect transaction fees associated with all transactions included in their block. The minimum transaction fee for low priority transactions is currently 0.0005 BTC. It is assumed that after the issue of the issue, the verification nodes will be maintained solely from the collection of transaction fees. Unlike other electronic currencies such as WebMoney or e-gold, Bitcoin is a currency in itself. There is no guaranteed price or value by any issuer. Many believe that Bitcoin was used as a currency by accident, saying that without a global crisis, its use would be completely different, because the protocol alone gives unlimited possibilities and functionality. It is unknown what the true intent of Satoshi Nakamoto (who is considered to be the creator of the system) was. Bitcoin can equally well be used as an integrated voting system in the presidential or parliamentary elections. In essence Bitcoin is a tool for keeping a synchronized and decentralized public global database.

Is Bitcoin the currency? Tony Gallippi (co-founder and CEO of BitPay, Inc.) responds as follows: "... yes, sometimes; so most people think nowadays. However, Bitcoin may equally well perform other functions. Can Bitcoin be treated as an accounting register? Definitely yes. Is Bitcoin a barter system? Perhaps. Is Bitcoin a specific database of property rights? Yes, it is. Bitcoin can also be used for many other purposes. "

Persons and institutions wishing to explore cryptocurrencies and distributed ledger technology knowledge for investment purposes, please write: contact@rciesolution.pl

or call +48 22 4795967.

Rafał Ciepielski