BACKGROUND OF BLOCKCHAIN TECHNOLOGY

In the topic context, we face frequently some terms that are related to the blockchain underlying infrastructure. A distributed system is a system, which is built on a collection of distributed components. These components can make decisions in a decentralized manner speedily with high performance and reliability. Nowadays the term is used more broadly in another sense such as cloud-services whose core is a very huge distributed system and for instance, an example is blockchain and its technological background that will be handled in this paper. But while summarizing the properties of these distributed systems we can find the following considered similarities in order to give a classifications for deciding if a system is distributed or not:

- A processing and computational unit or node can be any part of the system for instance a smartphone, tab, server and etc.
-The distributed entities have free decision.
-These entities in such systems should be connected to each other in a defined network
- The entities should be connected in determined paths in order to exchange their information.

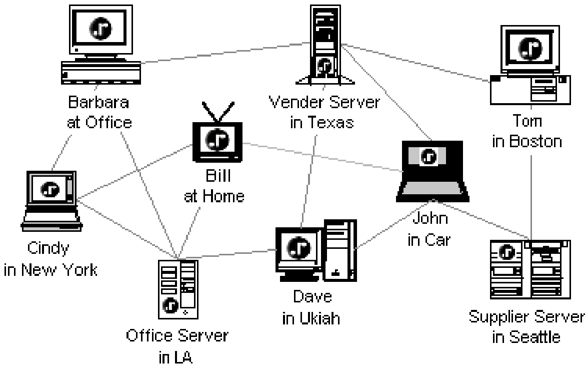

Figure 1 Typical distributed system

Decentralization means distribution of control unit under many parts. Deciding which manner of systems decentralized or centralized to be chosen is a difficult debate nowadays and it comes up to the structure of the departments in an organization. In this summary, we will consider this direction from the decentralized view that is the core structure of our topic blockchain. Now we come to definition of a block. A block is one of the main components of blockchain technology and it can be defined as a container of inputs or transactions. In these containers, the time and sequence of each input will be stored. Moreover, each block is being controlled by the rules of the working network. Implementing a sequence of blocks in succession and in connection builds a so-called blockchain. These sequences of blocks create a secure structure of inputs in each block.

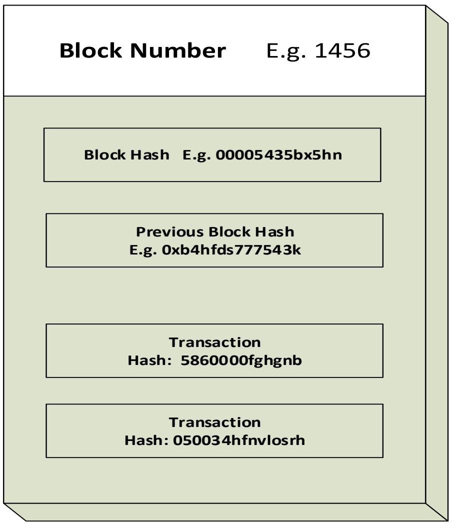

Figure 2. Block

We see in figure 2 the contents of a single block that must be assigned by a unique number. Every block contains the following data: block hash or key includes an accurate code given by each new add of a new block. Previous block hash refers to the block hash of the previous block. Transaction hash is the unique code given to each single transaction saved in a separate part of the block. If we ask at this point, for which reason the previous should be saved, we find in the answer one of strength and security points of blockchains. This topic will be discussed in the next chapter. Therefore, we can imagine a block as well as memory unit that is containing the above determined components. Subsequently, each new generated block is including transactions and it will send them to all network nodes, which will proof the validity of the block and, if necessary, they add it to blockchain as a new element. The result is a distributed trade repository that contains a complete, unchanging history of ownership and transmission relationships of transactions. This register is public, but still allows the confidentiality of individual transaction details, as these can only be viewed with the respective private key of the claimant. The term shared ledger is not a modern term and it comes back to the old centuries and refers to the archiving methods in the libraries. In our current century, the shared blockchain ledgers are being used as a record that can be accessible from all network participants. These ledgers help recording transactions only once and deleting the duplication of effort which is produced for instance in the traditional business networks. Before moving to the next definition, we will see in the following the features and advantages that the shared ledgers can offer to the blockchain network:

- They are the backbone of records inside the business network or the implemented application of blockchain.
- It is shared among the network in order to that each participant keeps a copy of the ledger.
- It has permission accessibility, so each participant has his own privileges to see the transaction which is related to the ledgers

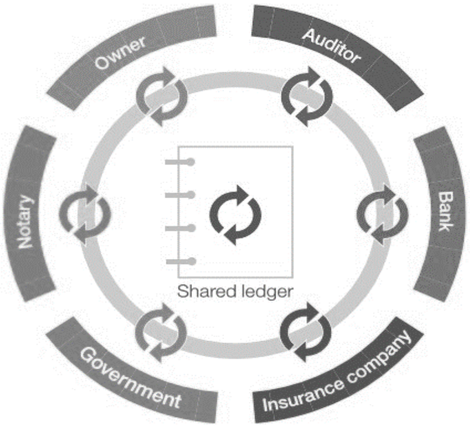

Figure 3, a shared ledger in example of business chain applicate to blockchain

Summarized, a shared ledger is as a type of database that is shared, replicated and synchronized between network participants. The distributed ledger records the transactions, such as the exchange of stocks of data, between the participants in the network. The participants in the network govern and agree on the updates of the records in the records of the ledger.

In blockchain, we can explore a distributed structure. This structure consists of individual computational units called nodes. These nodes give allowance for using their computational resources for all legal members of the network under determined rules without existing of centralization.

Again as mentioned above, when a new node joins to peer-to-peer system, it has to concern and understand its rights and roles inside the system. Moreover, without forgetting to mention that all nodes (users, consumers or suppliers of the resources) in the whole system acquire privileges and responsibilities. Now and before finishing this definition, we should clarify the relation between distributed peer-to-peer systems and the blockchain. As clarified in the previous definitions, the sequence of blocks can be determined as far as a tool for reaching and maintaining the integrity in distributed systems and at the same time, the peer-to-peer systems might use the blockchain to reach a good result of maintaining system integrity. The importance of a distributed peer-to-peer system can be seen while implementing it in the business fields and through replacing of the traditional centralized systems. This implementation will change the whole industry and business aspect. The most amazing mix is when these type of distributed peer-to-peer systems use the blockchains in order to achieve a good result

of achieving and maintaining of integrity inside the system as well as the disintermediation in the system. The famous worldwide definition of blockchain from Vitalik Buterin (programmer and co-founder of Ethereum Cryptocurrency): *’’ the blockchain is a magic computer that can upload anonymously programs to and leave the programs in self-execute, where the current and all previous states of every program are always publicly visible, and which carriers a very strong crypto-economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies[*Marc Pilkington, Université Bourgogne Franche Comté, “Blockchain Technology: Principles and Applications,” 15 Apr., 2016*]’’*.
A blockchain can be determined in this context as an obvious instance, which is structured technologically on shared digital distributed ledgers (databases in programmatic sense).These ledgers record transactions either in a public or in a private shared peer-to-peer network. These ledgers are built in sequential cryptographic hashed blocks that should be distributed to all members of the network simultaneously at the same time.
For a good understanding of the meaning of the term ‘’chain’’ here, we have to analyze the building structure of blockchain. Hence, each block should be linked to the next one and so on reaching to the current last block in the chain. Respectively, this sequential order of blocks is named a chain and as a result, it will produce a blockchain

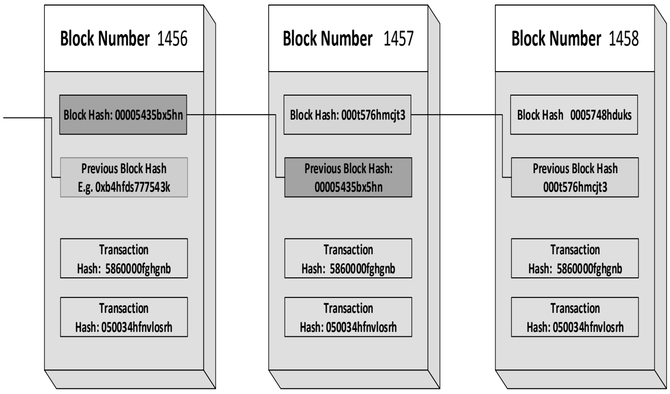

Figure 4. Blockchain figuration

We see in Figure 4, each block contains a block unique number in addition to a block hash and timeline of recent authorized transactions. The previous hash prevents from altering or adding of blocks between the current existing blocks. This method produces strengthens by verification of each previous block and so on till the end of the entire chain. Without forgetting it that blockchain technology ensures a double time spend, with enhancement of public-key cryptography, whereby every node in the network is determined by a private-key and public-key should be shared with all other nodes.

TYPES OF BLOCKCHAIN NETWORKS

After the revolutionary concept of blockchain came to technical implementation, the research works classified the blockchain networks into two types public and private. Some other researches added an advanced type whose name is hybrid. In the public blockchains and in most cases, every anonym user in the network (such as in the internet) has access to the chain and to its decentralized ledgers. This participation of the users is unconditional and subjects to the four main core keys .These blockchain-keys will be described and detailed in the next section. The another private type where the write and read-permission are fairly restricted. The participants in this case are known and trusted. The third type of blockchain is partially hybrid that contains a mixed model between high-trust and low-trust.
A highlight of public blockchains is the high performance capacity of transaction agreement maintained and agreed between the participants on the network. The space for blocks of transactions written by everyone to the blockchains (distributed ledgers) who creates transactions. In addition to the ability to send such transactions over the network. Besides, all these processes do not require the approval of a third party or intermediate center or authority. On the other hand, the limitations of accessibility and privileges in the private blockchains depend the flexibility of the implemented rules inside the network. The pattern of the private blockchains can be executed in such a way that only known and trusted users can insert data into the blockchain. Thus, private blockchains do not allow unknown and untrusted participants to read or write data on the chain.

Public Blockchains	Private Blockchains
Participants are not necessarily known	Participants are known and trusted
Participants are not necessarily trusted	Participants are trusted
Anyone without permission granted by another authority	Only permitted participants can write data

Table 1 The differences between Public Blockchains and Private Blockchains