CrossRef DOI of original article:

Cryptocurrency based on Blockchain Technology

Dr. Mousa Farajallah

Received: 1 January 1970 Accepted: 1 January 1970 Published: 1 January 1970

Abstract

The state of Palestine does not own national currency, so Palestine loses a lot of money yearly due to the use of foreign currencies and the Paris Protocol agreement prevents Palestinian own currency. For that, the crypto-currencies based on block-chain instead of physical currency will help the state of Palestine to avoid the obstacles that prevent to own currency. In this paper, we will study the cryptocurrency based on Blockchain technology that uses peer-to-peer (P2P) and timestamp server. In additional, exploring the main components of bitcoin currency as an example.

Index terms— blockchain, P2P, timestamp, digital currency, cryptocurrency, bitcoin

1 Introduction

he Palestinians does not have their currency. Therefore, they are using different foreign currencies such as Israeli Shekel (NIS), Jordanian Dinar (JD), United State Dollar (USD), and Euro in small and large payments, this leads to losing tens of NIS millions [1].

According to the Paris Protocol agreement since 1994 which gave the Palestine Monetary Authority (PMA) the functions of a central bank without the ability to issue currency. This agreement obligates the Palestinian to use the NIS in Palestinian territory as main currency [2].

This agreement has several negative influences on Palestinian economic; one important issue was the currency. Azzam Shawwa head of the Palestine Monetary Authority (PMA) said, "If we print currency, to get it into the country you would always need clearance from the Israelis and that could be an obstacle," [2]. This led the PMA to think hard to use the digital currency, and think to create their own official digital currency and the PMA plan to call it as Shawwa said. "It will be called the Palestinian pound." [2].

The PMA planned to see the Palestinian digital pound in the real world after five years since 2017 [2].

One of the important technologies used to create the digital currencies is the blockchain, the bitcoin is considered as one of the first and famous currency used the blockchain.

Blockchain is a set of continuous data records called blocks and linked together as a chain according to creation time, blocks are secured using cryptography tools, the data saved into block are immutable and cannot be changed once it has created. The Blockchain is managed by autonomously using peer-to-peer (P2P) network and distributed time stamping servers. Blockchain is a decentralized, distributed and public digital ledger that used to save all transactions across all nodes in the community of blockchain.

In this paper, we suggest a Blockchain technology that used for cryptocurrency that enables Palestinian people to use their own currency securely and freely without interference of external sides.

The rest of the paper is structured as follows. Section II Blockchain technology. Section III presents the Cryptocurrencies. Section IV presents Literature review. Finally, Section V concludes the paper and points out our future work.

2 II.

3 Blockchain

The Blockchain technology typically includes the four core concepts:

A shared ledger: The shared ledger appends only the distributed transaction record. Any node inside the network could access those transactions. This could control illegal operations.

Cryptography: Cryptography in a blockchain used to ensure authentication and verifiable transactions. By using Hashing function and digital signature (Public/Privet Keys).

Consensus: Trust systems refer to using the power of the network to verify transactions. Trust systems are central to blockchain systems in the authors of book view; "they are at the heart of blockchain applications, and we believe trust system is the preferred term over consensus system since not all validation is done through consensus." [3] Smart contracts: are the business terms that embedded in a blockchain transaction database and executed with each transaction. In addition, this contract needed to define the flow of value and state of each transaction.

Figure 1 illustrate a good idea of these concepts: The Blockchain according to assess the permissions management could be categorized into three types **??**4] [5]. Additional to four-core concepts there are others characteristics make the blockchain technology stronger and stable, such as: Timestamp Server: A timestamp server works by taking a hash of a block of items to be time stamped and widely publishing the hash, such as in a newspaper or Usenet post. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it [6].

4 Proof-of-Work:

The Blockchain data structure used as a mechanism to deal with the problems happened by openness [7]. Therefore, to implement a distributed timestamp server on a peer-to-peer basis, we will need to use a proof-of-work system [6], more information will be discussed in Cryptocurrencies section.

Exchanges: A crypto-exchange is a digital marketplace where traders can buy and sell coins using different currencies. A currency exchange is an online platform that acts as an intermediary between buyers and sellers of the Cryptocurrency. More information can be found on [8].

Peer to peer network: There are no servers in a peer-topeer (p2p) computer network, the entire network is includes users running instances of the application on their computers. A small amount of processing and storage resource to the network offered by each running instance, so that it can deliver the services such as privacy, verification, authentication, currency creation and transfer of ownership [9].

5 III.

6 Cryptocurrencies

One of the first and most famous digital currency is bitcoin, a decentralized Peer-to-Peer cryptocurrency [6], this digital coin was and still the source of worry and argue to governments, traders and businessmen. Start dealing with bitcoins in 2009, in Japan. One of the main reasons to widespread of bitcoin is the design of cryptography, which reflects a surprising amount of ingenuity and sophistication [10]. The main purpose of Bitcoin1 is to allow users to transfer currency securely without a third party or a centralized controller, using a publicly very able Blockchain [6]. Bitcoin can generate trustable records of bitcoin transactions, without needing a central owner or manipulator such as banks.

Bitcoin represents a new concept of money, as it is a currency, One of the important specifications is Proof-of-Work, it uses Hashcash-double SHA-256 to generate a unique hash value for each block in the blockchain, Figure 2 depicts an example of block includes a transaction generates around 33,000 BTC [11]. The connectivity of the blockchain is accomplished by linking the hash of a new block to the hash of generating block in the chain [6] [12].

Each block in the blockchain encapsulates one or more transactions. A new block can be linked to the chain if it has a valid proof-of-work. The hash of a block is calculated based on a random nonce value and the block's header data, e.g., previous block hash value, timestamp. For clarifying we can say the calculated hash value should be lower than or equal to the current network target, which makes the probability of finding a valid proof-of-work very low, in addition, the required time and required power consuming process [12]. [13].

IV.

7 Literature Review

Today, several of cryptocurrencies based on blockchain has been widely used. Many works of literature focus on architecture of digital currencies in general and others focus on bitcoin technology. On the other hand, there are several streams of research investigate in optimizing algorithms to improve the characteristics of the technology, such as peer-to-peer.

Nakamoto, Satoshi [6] proposed a solution to the double-spending2 problem by using a peer-to-peer network. The authors are using hashing to hash the network timestamps transactions into an ongoing chain of hash-based proof-of-work, this leads to a record that cannot be modified without redoing the proof-of-work.

The authors review the main blockchain components (Although the blockchain is not explicitly mentioned in the paper, the components mentioned by the authors are the same as the components of the blockchain).

The authors start with transaction as the first component in blockchain; define a digital coin as a chain of digital signatures. Each owner transfers the coin to the next by digitally signing include hash of the previous

transaction and the public key of the next owner and adding these to the end of the chain. One important issue is a payee could verify the signatures to verify the ownership of chain in addition to prevent the double spending.) Figure 3 show the example of linked transactions that could be achieved without a trusted party, transactions must be recorded in a public shared ledger, and use a system for participants to agree on a single history of the order in which they were received (Blockchain). The payee needs proof that at the time of each transaction, the majority of nodes agreed it is the first received.

The authors propose a Timestamp Server used to generate a timestamp, this timestamp includes a block of items. The timestamp proves that the data must have existed at the time, clearly, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, to be like a chain, with each additional timestamp supporting the ones before it.

The author's emphasis that distributed timestamp server on a peer-to-peer basis to be implemented, they need to use a proof-of-work system.

In timestamp network, they implement the proof-of-work by incrementing a nonce in the block until a value is found that give the block's hash the required zero bits. After the CPU effort has been expended to make it satisfy the proof-of-work, the block cannot be modified without redoing the work again, due to that block is chained after it, the work to modify the block would include redoing all the blocks after it.

Algorithm 1 ?????? ?!???? ???? ????? ???????? ????? ?????? ??????? presents steps to run the network: Algorithm 1 Steps of run network (Source [6]) 1 New transactions are broadcast to all nodes 2 Each node collects new transactions into a block. 3 Each node works on finding a difficult proof-ofwork for its block. 4 When a node finds a proof-of-work, it broadcasts the block to all nodes. 5 Nodes accept the block only if all transactions in it are valid and not already spent. 6 Nodes express their acceptance of the block by working on creating the next block in the Chain, using the hash of the accepted block as the previous hash.

Network nodes always consider that longest chain is the correct one and will keep working on extending that chain. If two nodes broadcast different versions of the next block at the same time, some nodes may receive the block or the other first. In that case, they work on the first one received, but keep the other branch in case it becomes longer.

The authors clarify the Simplified Payment Verification process, by keeping a copy of the block headers of the longest proof-of-work chain the, payment verification could be done without running a full network node.

In the end, the verification becomes more reliable as long as honest nodes control the network, but there is more risk vulnerable if the network is overpowered by attackers. While network nodes can verify transactions for themselves, the simplified method can be fooled by an attacker's fabricated transaction for as long as the attacker can continue to overpower the network. The authors suggest a strategy to protect against such attack would be to accept alerts from network nodes when they detect an invalid block, prompting the user's application to download the full block and alerted transactions to confirm the inconsistency.

The authors suggest to combining and splitting value using multiple inputs and outputs for transactions as illustrated in Figure 4. By default, there will be either a single input from a larger previous transaction or multiple inputs combine smaller amounts. Mostly the output will be two amounts in two blocks, the first block for the payment, the second block for returning the change, if any, and this block back to the sender's chain. The Authors did not forget to mention privacy, they maintain the privacy by breaking the flow of information in another place: by keeping public keys anonymous. Someone could send an amount to someone else, this transaction the public can see it, but without information linking the transaction to anyone. To achieve that the authors suggest using a key pair, this new key pair should be used for each transaction to avoid linked transaction to the owner.

Simon, Boyen, Shi, and Uzun [10] perform an in-depth investigation to understand why bitcoin is so successful, compared with cryptographic e-cash. In addition to that, the authors asking how bitcoin could become a better candidate for a long-lived stable currency.

Authors addresses the most vital problems most expeditiously as below: 1. No central point of trust. Therefore, Bitcoin architecture is completely distributed. Actually, "bitcoin assumes that the majority of nodes in its network are honest, and resorts to a majority vote mechanism for double-spending avoidance, and dispute resolution." 2. Incentives and the economic system. Bitcoin's ensures that users have economic motivations to participate. In fact, "bitcoin miners" solve computational puzzles to generate new bitcoins, and this process is closely coupled with the verification of transactions previously created. Furthermore, miners also gain optional transaction fees for their effort of vetting said transactions. 3. Predictable money supply, new coins will be minted at a fixed rate. 4. Divisibility and fungibility. One of the most advantages of Bitcoin is the ease of dividing and recombining the coin to create essentially any denomination possible. Decker et. Al., [7] provide a new system (called PeerCensus), built on the Bitcoin blockchain to enable strong consistency. The system acts as a certification authority, manages node identities in a peer-to-peer network so that enhance Bitcoin and similar systems with strong consistency.

The authors [7] mention that the main objective of the provided system is to enable the creation of a cryptocurrency that provides forward security and supports fast confirmations. They do that by using the techniques from Bitcoin, resulting in strong consistency guarantees. They mention three reasons for Known agreement protocols are not applicable to a peer-topeer environment in which Bitcoin operates.

Algorithm ???????.2? ?????? ????? ???????? ????? ???? ????!? is described in [7] in order to illustrate integral tool used in the Blockchain protocol called Proof-of-Work, they expressed how the protocol maintains a

list of functions triggered when a new block join the chain, starting creating the hash through the mining until Chain Agreement (CA) accept the block.

Decker concludes that the digital cryptocurrency "Discoin", which builds on top of the new PeerCensus system, is easier to analyze and implement than the current Bitcoin system, additional to that, it provides a stronger guarantees and faster confirmations.

8 H

Israa Alqassem, Davor Svetinovic [12], provide an up-to-date protocol specification and architectural analysis of the system of the first cryptocurrency called bitcoin. The authors perform that analysis as the first step towards the specification of the cryptocurrency reference architecture. The described architecture will consider as a starting architectural point for the development process of new systems that influence on Bitcoin protocol in different contexts and for different purposes. In addition, the authors discuss whether the current architecture satisfies the system's primary purpose, for example, providing a pure decentralized version of the cryptocurrency.

The authors emphasize that in order to develop an architecture model. it should achieve the below goals to make it modifiability, maintainability, reusability, and comprehensibility [12]:

1. Provide a basis for eliciting additional requirements and constraints by evaluating the system's technical feasibility. 2. Help in understanding and evaluating the rationale behind the Bitcoin design and implementation, hence paving the way towards alternative design approaches that improve and refine the current architecture. 3. Alleviate potential security risks when integrating further components or extending the system. 4. Map the quality attributes such as scalability, security, and performance onto advanced modular architectures. Their work examines the high priority aspects of Bitcoin architecture3, for example, the main components and the required interactions between the components; Figure 5 shows the Bitcoin transaction domain Model, and bellow ?????? ????? ???????? ????? ???? ???????.???!? the description of components. The authors cover both structure (static architecture) and behavior (dynamic behavior) aspects of the system [12].

Transactions: Transactions serve as a payment verification system, as a mechanism to transfer money from one entity to another.

Memory Pool: In each node, there is a local storage of unconfirmed transactions.

Wallet and Coin Selection: All information about user's accounts is saved in Bitcoin wallet, i.e., addresses and the transitions related to them. Moreover, the user has to decide which previous transaction outputs should be selected from the wallet as inputs to the current transaction.

Blockchain: Blockchain serves: first, facilitates the coordination between network's nodes to process transactions. Second, encapsulates the values of proofof-work which it responsible for maintaining network's security. Finally, helps in verifying the ownership of transferred coins. The authors describe the Bitcoin initialization and running processes, Figure 6 illustrates a flowchart of the processes that take place once the Bitcoin application starts.

The authors recommend finding alternative design approaches that enhance and improve the current architecture and decrease potential security risks when integrating further components or extending the current system architecture.

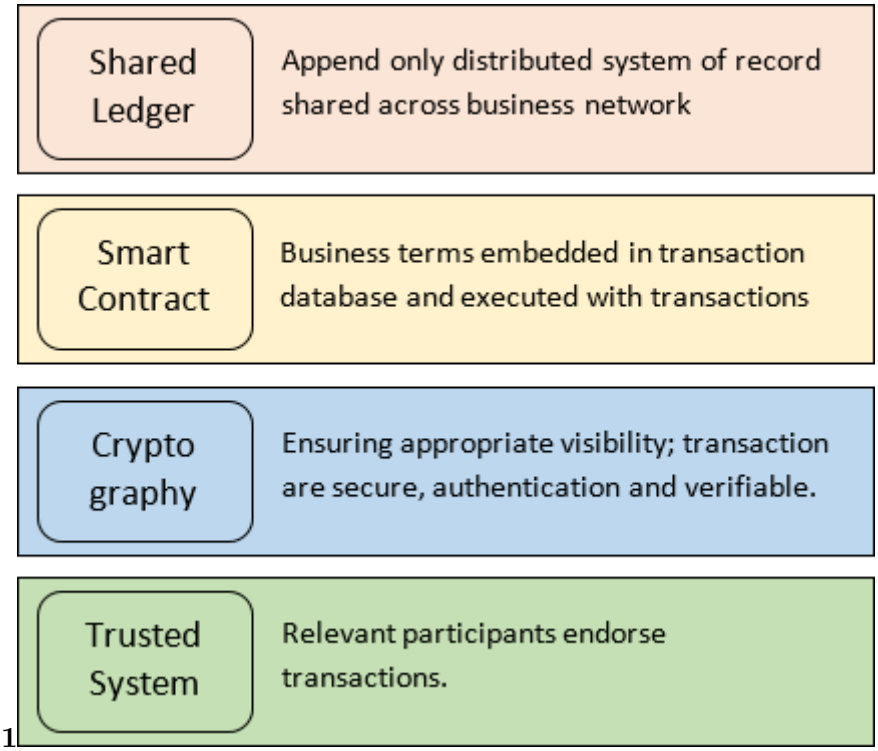
Figure **??** show the initialization process of the bitcoin from the parameters step load till the GUI step.

V.

9 Conclusion and Future Work

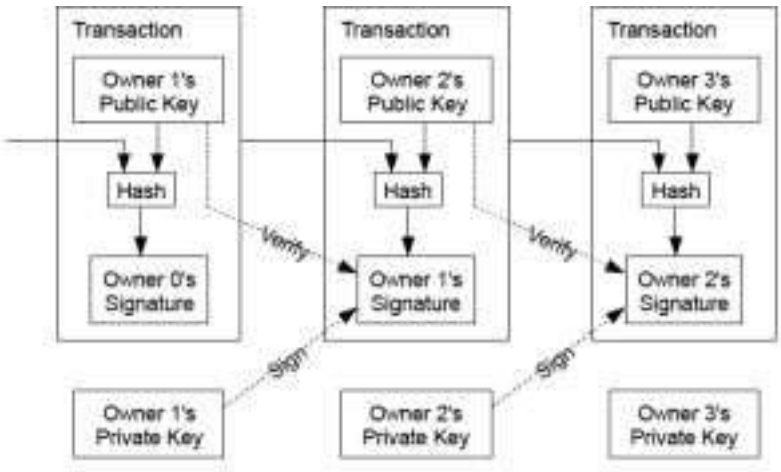
The purpose of this review was to view the trends in cryptocurrencies studies and see how the blockchain technology concept used in order to create cryptocurrencies and solve cryptocurrencies problems. It is clear from the research reviewed that the blockchain solving many problems such as double spending and avoid using a trusted third party to do the transactions. Along with this, it is also clear that there are some factors in Bitcoin protocol need to be improving like consistency. Current research supports the use of blockchain, as discussed above; however, we recommend the cryptocurrencies based on blockchain technology as a good solution to replace the existing physical currencies.

Future work might take a closer look at how to customize blockchain to be using as Palestinian currency and building the mathematical model of this currency. [1]



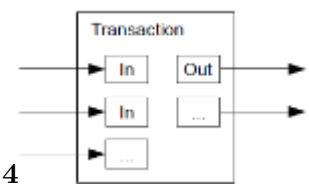
1

Figure 1: Figure 1 :



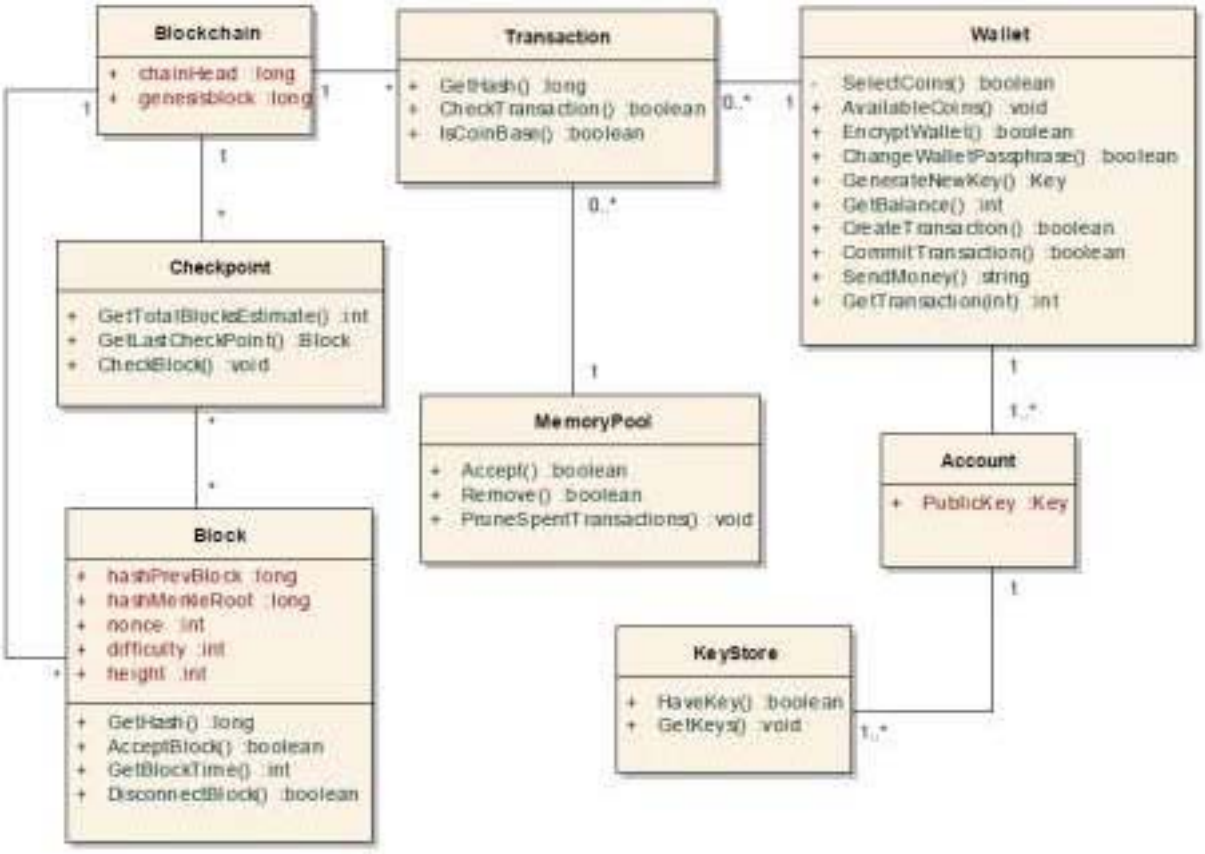
3

Figure 2: Figure 3 :



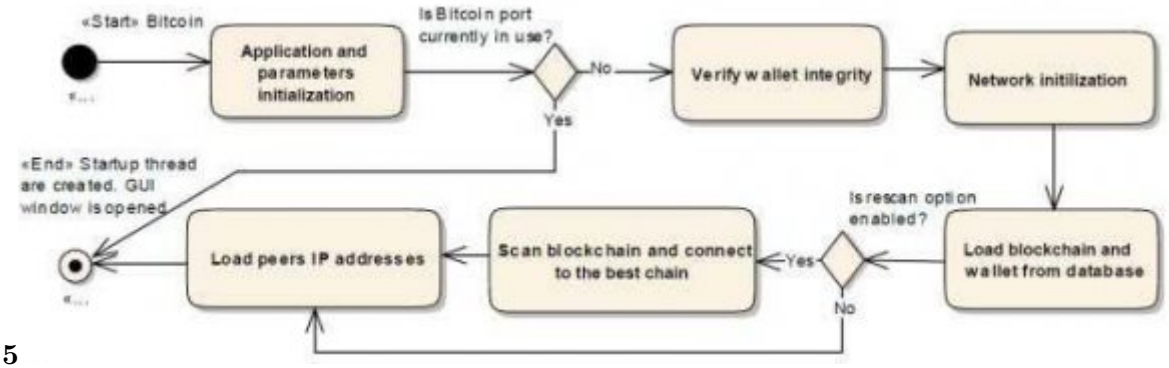
4

Figure 3: Figure 4 :



2

Figure 4: Algorithm 2 The



5

Figure 5: Figure 5 :

1

	Public	Consortium	Private
Participation	Free Anonymous	Permissioned Identified and Trusted	
Consensus Mechanisms	Mining (Prof-of-Work) No Finality 51% attack	Coting/Multi-party Consensus Algorithm Lighter, Faster Enable finality	
energy consumption	Large	Low	
Transaction Approval time	Long (e.g. 10 min)	Short (100x msec)	
Uses Case Cryptocurrency		Transaction in financial and business sectors, e.g. Documents archive.	

Figure 6: Table 1 :

.1 Acknowledgement

I would like to make this a useful document, updating it as I receive comments. Please take a moment to email me any comments or suggestions for improvement. Thanks to Dr. Fadi Shrouf for supporting me.

[Sulabi ; Entercoin et al. (2018)] , N Sulabi ; Entercoin , ?????????? ??????? ?????? ?" , Carlo ??????? Monte , Doualiya . https://www.mc-doualiya.com 15 March 2018. 10 February 2019.

[Gaur et al. ()] , N Gaur , L Desrosiers , V Ramakrishna , P Novotny , D S A Baset , A O'dowd . *Hands-On Blockchain with Hyperledger* 2018. Packt Publishing Ltd.

[Meqdad et al. ()] *? ???????????? The Islamic University Gaza*, S Meqdad , M Meqdad , ??????? ??????? ???????? " ??????????? ????????? ?????????? ??????? ???????? ? , ???????? ????????? . 2007.

[Binance] *Binance*, https://www.binance.com

[Decker et al. ()] 'Bitcoin Meets Strong Consistency'. C Decker , J Seidel , R Wattenhofer . *ICDCN '16 Proceedings of the 17th International Conference on Distributed Computing and Networking*, (Singapore) 2016.

[Nakamoto ()] *Bitcoin: A Peer-to-Peer Electronic Cash System*, S Nakamoto . 2008.

[Barber et al. ()] 'Bitter to better-how to make bitcoin a better currency'. S Barber , X Boyen , E Shi , E Uzun . *International Conference on Financial Cryptography and Data Security*, (Berlin) 2012. p. .

[Blockchain (2019)] *Blockchain*, https://www.blockchain.com/btc/block-height/572068 Blockchain, 17 April 2019. 17 April 2019.

[Gipp et al. ()] 'Decentralized Trusted Timestamping using the Crypto Currency Bitcoin'. B Gipp , N Meuschke , A Gernandt . *Proceedings of the iConference 2015*, (the iConference 2015) 2015. (to appear)

[MOLD Comparison of Several Types of Blockchains (Public?Private?Consortium) (2018)] 'MOLD'. https://medium.com/mold-project/blockchain-comparison-51f881c8399f *Comparison of Several Types of Blockchains (Public?Private?Consortium)*, 14 June 2018. 29 April 2019. (MOLD project)

[P2P Foundation wiki ()] *P2P Foundation wiki*, http://wiki.p2pfoundation.net/Bitcoin Jauary 2016. 15 April 2019. (Bitcoin)

[Jones (2017)] 'Palestinian officials hope to launch ecurrency in 5 years'. M Jones . https://www.reuters.com *Reuters* 12 May 2017. 15 February 2019.

[Bela et al. ()] 'Securing video integrity using decentralized trusted timestamping on the bitcoin blockchain'. G Bela , J Kosti , C Breitinger . *Proceedings of the 10th Mediterranean Conference on Information Systems (MCIS)*, (the 10th Mediterranean Conference on Information Systems (MCIS)Cyprus) 2016.

[Alqassem and Svetinovic ()] 'Towards Reference Architecture for Cryptocurrencies: Bitcoin Architectural'. D Alqassem , Svetinovic . *IEEE International Conference on Internet of Things (iThings), and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber*, 2014. 10 p. .

[Types of Blockchain - Public, Private, and Consortium Blockchain (2018)] *Types of Blockchain - Public, Private, and Consortium Blockchain*, https://medium.com June 2018. 11 February 2019.

[Gipp et al. ()] 'Using the Blockchain of Cryptocurrencies for Timestamping Digital Cultural Heritage'. B Gipp , N Meuschke , J Beel , C Breitinger . *IEEE Technical Committee on Digital Libraries (TCDL)* 2017. 13 (1) .