Journal of Theoretical and Applied Information Technology
15th December 2021. Vol.99. No 23

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

GDPR-BLOCKCHAIN COMPLIANCE FOR PERSONAL DATA: REVIEW PAPER

[1]YAMAN SALEM, [2]EMAN-YASSER DARAGHMI

[1]Department of Engineering and Technology Sciences, Arab American University, Ramallah, Palestine

[2]Department of Applied Computing, Palestine Technical University, Tulkarm, Palestine

E-mail: [1]y.salem3@student.aaup.edu, [2]e.daraghmi@ptuk.edu.ps

ORCID: [1] https://orcid.org/0000-0002-4737-5112 , [2] https://orcid.org/0000-0001-8986-4232

ABSTRACT

Processing and collecting personal data by third parties poses a big concern to user's privacy. GDPR is a regulation proposed to maintain users' privacy, while blockchain is an innovation technology used in many applications. This research is motivated by the facts mentioned above, and it aims to investigate how to make blockchain complies with the GDPR regulation, a systematic review is conducted to explore the relation between GDPR and blockchain, in addition, this study explores the main compliance issues with the GDPR and blockchain. As a result, it states several suggestions that make a blockchain technology more compliant with GDPR. The suggested solutions may open a new idea to design a novel model for GDPR-Blockchain Compliance for Personal Data.

Keywords: *Blockchain (BC), Privacy, GDPR, Personal Data, Compliance.*

1. INTRODUCTION

Data is considered the most important asset worldwide, this data can be used by organizations to develop several services and for decision making. However, individuals' privacy becomes a big concern in a big data era. A recent survey by [1] indicated that users face challenges regarding protecting and sharing private information over the internet. A huge number of personal and private information are spread over the digital world, consequently, individuals lost the control over their data. Organizations from all around the world are working to make sure they comply with the new regulations because otherwise, they will face hefty fines.

In 2018, a new privacy law which is the GDPR, or General Data Protection Regulation took effect in Europe. It gives EU citizens the control over who is allowed to collect their personal data and over what happens with it [2]. On the other hand, blockchain (BC) technology is one of the innovative technologies that proposed to solve security issues, and it is implemented in many applications. However, it has some challenges and limitations regarding BC privacy. While there are several studies stated data management and privacy of personal data in BC perspective [3], [4], [5], [6]. However, blockchain and its relation to the GDPR regulation is relatively a new topic. There is no GDPR-Blockchain compliance technology but there are some studies stated some applications and case studies related to some aspects such as data management, immutability, transparency, data controller and data processor. In addition, some studies stated the off chain and pseudo-anonymous. Another papers suggested a GDPR compliant blockchain architectures [7].

The GDPR is a great way to protect privacy but it leaves some questions as how it can be applied to blockchains, since the data in a blockchain is recorded in an open and transparent way. In addition, the stored data on a blockchain cannot be changed or erased. These properties are what allows blockchain to be completely distributed without a central authority [3]. But at the same time, these properties do not sound so good when it comes to privacy and GDPR principles. Therefore, this study is motivated by the facts mentioned above, and it aims to focus on blockchain technology in terms of data privacy and explore the GDPR-Blockchain compliance. The following research questions were stated to achieve this aim:

- What is blockchain characteristic?
- What is the GDPR principles and rights that are related to blockchain?

- What are the main compliance conflicts between GDPR and blockchain?
- How to make a blockchain solution more compliant with GDPR?

The rest of the paper is structured as follows: section 2, the background which contains; preliminaries, overview of GDPR, overview of blockchain, Section 3 states related work. This is followed by study framework and method in section 4. In section 5, the research findings and discussions are highlighted. Finally, section 6 contains the conclusion and future work.

2. BACKGROUND

2.1 Preliminaries

2.1.1 Cryptography

Cryptographic algorithms are used to achieve confidentiality, basically, cryptography has two types; symmetric and asymmetric [8]. Symmetric cryptography uses the same key for encryption and decryption, so if A wants to send a message to B, A and B need K1 as a key for encryption and decryption, also if A want to send a message to D, A and D need K2 as a key. Therefore, if the number of users increases then the number of keys increases, so it will be hard to manage all the keys. On the other hand, in asymmetric cryptography each user has two different keys being private and public keys, so if A wants to send a message to B, A encrypts that message with B's public key and B decrypt that message with its private key. In blockchain, each node has a public and private key. A transaction in blockchain is encrypted by asymmetric encryption, and the address of the node in a wallet represents the hash of a public key, while private key is used for authentication [9], [8].

2.1.2 Hashing

Hashing helps in reducing the transmitted data and maintains the integrity. Hash function is a mathematical function which takes data of any length and convert it into a fixed length, see Figure 1. Hash function is a one way function thus, it is very difficult to impossible to get the input data from the output hash value, some of hash algorithms are still weak to resist against collision attacks, in addition, there are different lengths of hash value based on hash function types such as MD versions (MD1, MD2, MD3, MD4, MD5, MD6), SHA versions (SHA0, SHA1, SHA2, SHA3), and many other.

SHA-256 hash algorithm is the most commonly used in blockchain [8] [10], each block in blockchain has a hash value and a hash pointer which represents the hash of previous block. Figure 3. If one of block hash is changed then all the hashes in blockchain need to be recalculated and changed, therefore blockchain has an immutability feature [9]. Also, in blockchain, hash function is used in PoW, Merekle tree and for address generator (public key hashing) [8].

Figure 1. Hashing Function

2.1.3 Digital signature

The main aim of digital signature is to achieve the authentication. If A wants to send a message to B, then A signed this message by its private key, and B can verify and authenticate this message by A's public key. ECDSA and EdDSA digital signature schemes are the most commonly implemented in blockchain [8].

Authentication systems is one of the most vital part of any system, it can usually deny unauthorized access, there are three main methods to authenticate users; something you know like password and PIN, something you have such as smart card, and something you have such as biometric [11]. In blockchain private key is considered as a password, a user is authenticated through a digital wallet to manage cryptocurrencies, thus private key is considered the main authentication element [9].

2.1.4 Cryptographic hash functions

Asymmetric encryption associated with hash and digital signature are used in blockchain. The cryptographic hash function is imperative for data security, which guarantees authentication, confidentiality, nonrepudiation and integrity of stored data. Private key is used for decryption and signing while public key is used for encryption and verification. Thus, cryptographic hash algorithms in blockchain are considered a trust factor instead of third party [10].

2.1.5 Private key management

All transactions in blockchain are signed by private keys, if these keys leak, then this will affect the privacy and identity theft could happen, hence the adversary will have a full access to the assets. It is imperative to implement key management system to maintain privacy and prevent identity theft [12].

2.2 Overview of GDPR

GDPR is stands for "General Data Protection Regulation". It is a regulation proposed by European Union in 1995, and it is applied in 2008 in EU countries, The GDPR is only applicable for personal data of EU citizens. However, any company storing any personal information of EU citizens should follow the regulation, even foreign companies like Facebook or Apple must adhere to the law because they have European users [13], [2]. GDPR is interested in protecting personal information which is completely controlled by data owners. In addition, it guarantees that data is gathered for lawful intent under strict terms. All organizations that adhere to GDPR must manage and store data in a good manner to maintain data protection [2].

2.2.1 Key terms in GDPR

According to GDPR (Article 4)[1], there are several definitions for purposes of the regulation, these include the following:

- Personal data: any information that can be used either directly or indirectly to identify natural person this includes ID number, name, email, IP address, home address, date of birth, etc. In GDPR a natural person is termed as a data subject.
- Processing: any operation that is performed on personal data this includes collecting, storing, using, deleting, recording, modification, combining or linking data.
- Profiling: any automated operation that is performed on personal data to analyze or predict certain aspects of data subject, these aspects may be economic situation, health, and behavior.
- Recipient: a natural person, legal entity, or public body to which personal data is disclosed.
- Consent: GDPR mandates the consent that is given to data subject before data processing, the consent must be asked for a clear purpose and must be freely given, it is also must be recorded for future evidence, in addition data subject has the option to withdraw consent at any point of time.
- Data protection officer (DPO): a leadership role required by EU GDPR which is responsible for compliant.
- Supervisor authority: a public authority in an EU county that is responsible for monitoring compliance with the GDPR.
- Pseudonymization: a technique for personal data to make identification of data subject is difficult.
- Anonymization: a technique for personal data to make identification of a natural data impossible.

2.2.2 GDPR components

GDPR defines three main components: data processor, data subject and data controller [2].

- Data subject who owns the data and it has a full control over his personal data, also it has the ability to trace the processed data, force or withdraw consents whenever needed.
- Data controller is a natural person or legal entity that manages personal data and ensures the data subject's rights.
- Data processer is a natural person or legal entity that processes personal data in specific methods on behalf of the data controller for different purposes, processer is called a third party.

2.2.3 GDPR principles

According to GDPR (Article 5)[2], there are several principles related to data processing that must be followed, the following Table 1 concludes GDPR principles.

2.2.4 Transparency and consent through privacy notice

According to (Article 12)[3], the controller should provide the relevant information about data processing to data subjects in an open and transparent manner. Thus, the controller published privacy notice or statement which is a document that describes key aspects of personal data that related to data subject. Privacy notice is usually published on the controller's website or on the internet, it allows data subjects to know what happens to their personal data that they provide to the controller and it should be reviewed regularly. Privacy notice document should be simple, clear, and information provided is easy to understand, in addition, it should be easily accessible to data subjects without having to search the content.

[1] Art. 4 GDPR – Definitions | General Data Protection Regulation (GDPR) (gdpr-info.eu)
[2] Art. 5 GDPR – Principles relating to processing of personal data | General Data Protection Regulation (GDPR) (gdpr-info.eu)
[3] Art. 12 GDPR – Transparent information, communication and modalities for the exercise of the rights of the data subject | General Data Protection Regulation (GDPR) (gdpr-info.eu)

2.2.5 Data subject rights

GDPR empowers the data subject with certain rights, the following Table 2 summarize data subjects' rights in GDPR.

Table 1. GDPR Principles

GDPR Principle	Summary
Lawfulness, fairness and transparency	Personal data processes should be fair where controller do not perform processing that is not legitimate, and data subjects can be sufficiently informed regarding processing of their data. Hence, personal data is processed lawfully, anonymized and in a transparent manner.
Purpose limitation	Processing of personal data must be limited to the legitimate purpose for which the personal data was originally collected.
Data minimization	When collecting data, only the personal data absolutely required for that purpose should be collected, this means that no data other than what is necessary should be requested or stored.
Accuracy	Personal data must be up to date and controllers are asked to ensure that data is kept accurate, in addition, data subjects have the opportunity to update their data when required.
Integrity and confidentiality	Personal data must be processed in a way that ensures security including protection against unauthorized processing, moreover, controllers must ensure that data cannot be modified by unauthorized users.
Storage limitation	Personal data should be retained when necessary and should be deleted once the purpose for which it was collected has been fulfilled.
Accountability	Data controller must be responsible and adhere to all previous principles.

Table 2. Rights of Data Subject

GDPR right	Description	Article Number
Right to information	Provide the data subject with the ability to ask information about what is being processed and the rationale for such processing.	Article 13
Right to access	Provides the data subject with the ability to get access to personal data that is being processed.	Article 15
Right to rectification	Provide the data subjects with the ability to ask for modifications to their personal data incase that it is not accurate, or it needs up to date.	Article 16
Right to withdraw consent	Provide the data subjects with the ability to withdraw previously given consent for the processing of their personal data.	Article 7
Right to object	Provide the data subjects with the ability to object to the processing of their personal data.	Article 21
Right to be forgotten	Provides the data subjects with the ability to ask for deletion of their data.	Article 17
Right to data portability	Allows the data subjects to transfer their personal data.	Article 20

2.3 Overview of Blockchain

In 2008, an unknown identity author called Satoshi Nakamoto was the first one who introduced the bitcoin, which is a digital cryptocurrency based on blockchain technology. Nakamoto clarifies the problem of currency transactions which depends on third parties and needs fees. In addition, all individuals' data are controlled by centralized banks and organizations, thus he comes with the idea of bitcoin as it is a digital cryptocurrency that solves the previous mentioned problems, bitcoin was the first peer to peer digital currency with the most famous and successful one [14], [9].

Blockchain depends on decentralized system with distributed database of information records that are continuously keep increasing and verified by the participated nodes without relying on third party, all nodes have a copy of a public ledger which contains every completed transaction, this creates the transparency and decentralization in the system. All the participated nodes are anonymous which increase the privacy. Further, a computational power based on asymmetric cryptography algorithms are used in blockchain technology to confirm transactions which increases the integrity and the security of systems, in addition to using digital signature algorithm to solve

non repudiation, integrity and authentication issues [9], [15].

2.3.1 Blockchain applications

Blockchain started with the bitcoin application, then digital cryptocurrencies became more popular. In 2018, the number of cryptocurrencies reached to 1591 as many entities proposed new cryptocurrencies. Blockchain technology has different advantages, it is not only used for cryptocurrency applications, also, it is applied in several applications such as, IoT, intelligent transport systems, smart cities, healthcare, digital assets, social services and cloud services [10], [4], [16] [16]–[18].

Blockchain is improved using smart contracts and modified consensus protocols to develop blockchain-based platforms such as Hyperledger and Ethereum. In 2016, IBM developed blockchain as a service (BaaS). Furthermore, Google, Microsoft and Amazon joined the (BaaS) business [10].

2.3.2 Blockchain challenges

There are several challenges in blockchain technology, for instant this study [9] stated some of them, such as bandwidth, versioning, 51% attack, multiple chains, selfish mine attack, hard forks, transaction data malleability problems, throughput and deanonymization by transaction linking, furthermore, some issues related to security and privacy.

Further, wasted resources and computational power are considered one of the main challenges. When the size of Blockchain grows the computational process becomes more complex, it also requires more power to confirm and validate more blocks. In addition to latency, as a transaction block needs a round ten minute to be completed and validated [9].

2.4 Blockchain Architecture

2.4.1 Transaction

The transaction is simply data recorded or saved in a block.

2.4.2 Block

Each block has two main parts, the block header which contains the hash of previous block, its hash value, time stamp and nounce, while the block body consists of a set of transactions. The structure of block may differ based on the type of blockchain. See Figure 2.

2.4.3 Blockchain

It constructed from a set of blocks that linked to each other by hash values, the first block is called a Genusis block with previous zero hash value. A blockchain is stored in multiple nodes, every node has a copy of the same state of blockchain. The term blockchain refers to the technology or to chain of blocks which represents a database [15], See Figure 2.

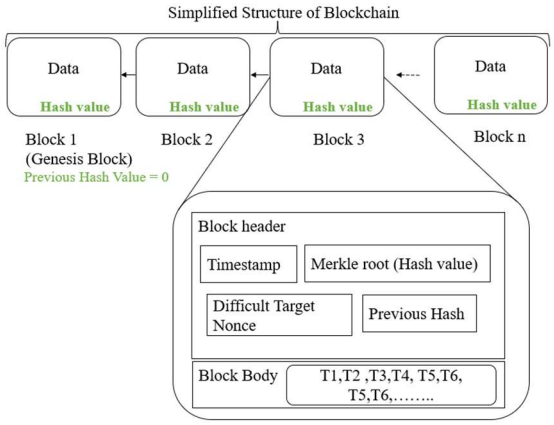

Figure 2. Simplified Structure of Blockchain

2.4.4 Ledger

A database that stores and synchronizes all transactions over the network, also, it is referred to the chain of blocks.

2.4.5 Merekle Tree

Blockchain is constructed from lots of blocks and these blocks are connected with the help of hash value, Merekle tree is used to find the hash of each block as it contains one transaction or thousands of transactions, Figure 3 clarifies a Merekle tree of one block that has 6 transactions.

2.4.6 Nodes

A blockchain network contains nodes, these nodes can be a computer or a mobile phone. There are two types of nodes being full nodes and partial nodes. A full node is basically a device which has the entire blockchain and it is also verifies the new blocks to add them into the blockchain, a full node can also be a miner which involved in transactions and mining. These nodes need a huge amount of storage to store blockchain, in addition to a huge computing power as well as electricity to run that machine. On the other hand, partial nodes or light nodes have a software wallet for bitcoin transactions, these nodes cannot download the entire blocks and did not involve in mining.

2.4.7 Mining

A cryptocurrency or a bitcoin unit is represented by a number which is a result of well-defined equation, the bitcoin network is secured by individuals called miners. Miners are rewarded newly generated bitcoins for verifying transactions. The transaction is verified by the winner miner who solved a complicated equation; thus, he found a new block or a bitcoin which added then to the chain.

Transactions are digitally signed to guarantee integrity and avoid nonrepudiation. After transactions are verified, they are recorded in a transparent public ledger [15].

2.4.8 Blockchain Network

It is a peer-to-peer network that lets each node or miner to contact with each other.

2.4.9 Smart Contract

It was proposed in 1994 by Nick Szabo, smart contract is a transaction protocol executed by a piece of code when predetermined conditions are met, the transactions can be verified by executed smart contract [15].

2.4.10 Wallets

Blockchain wallet is a digital wallet that stores all transactions history and allows users to transfer and manage the transactions. Once the wallet is installed on the node, a wallet ID is created which is a unique id (hashed public key) similar to a bank account number, a user can log into wallet by email and password (private key).

Bitcoins are kept in a digital wallet on a computer or a mobile device, private key is simply the password that let user to spend bitcoins in a wallet. There are three main types of wallets (software wallet, hardware wallet, paper wallet); software wallets that can be downloaded in a phone or a computer. Hardware wallet, which is portable, convenient and can support multiple cryptocurrencies. While paper wallet is printed with two QR code, one code for private key and the other code for public key.

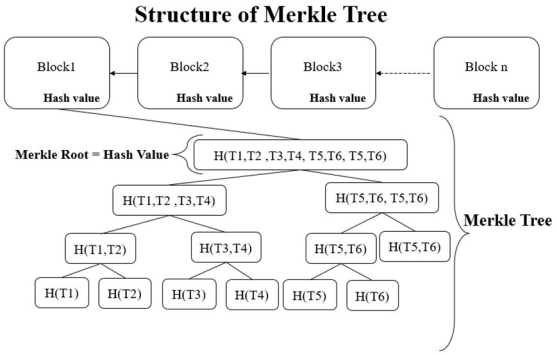

Figure 3. Merkle Tree in Blockchain

3. RELATED WORK

Many studies have introduced the relation between GDPR and blockchain technology, for example [19] investigated the relation between processing of personal data in GDPR and blockchain principles, it stated the blockchain type for two scenarios which were chosen based on decision model from this study [20], the first scenario was processing data in healthcare, it was concluded that permissioned consortium BC is suitable for this scenario. While the second scenario was processing data for identity management where permissioned consortium BC or permissioned private BC is suitable. In addition, the study result showed that storage limitation and accuracy principles in GDPR are conflicts all BC types because of immutability of BC characteristic. Furthermore, the right of erasure and the right to be forgotten are also conflicts BC immutability, thus BC is not compliant with GDPR regarding personal data processing.

In [21], focused on the right to be forgotten which is the main challenge for GDPR-Blockchain compliance, this study presented a model for GDPR compliance, it was concluded that the right to be forgotten depends on central data controller. In addition, the study proposed using cryptographic principles along with smart contracts to improve its model.

In [22], three approaches were suggested to comply blockchain with GDPR which are central authority, shared responsibility and pseudonymization, furthermore, it stated some recommendations for making blockchain comply with GDPR which are the following:

- Personal data should be stored outside blockchain this guarantees modification and deletion data.
- A private and permissioned blockchain should be used for processing personal data.

Another study [23] proposed blueprints for compliance by focusing on Privacy by Design principle (Article 25) and data subject's consent (Article 6). Further, a study by [7] pointed two challenges for GDPR compliant blockchain which are;

- Blockchain is a decentralized system while GDPR recommends that data subject should have a control over its data and a controller should manage data subject consent.
- Blockchain is immutability, however GDPR recommends that data should be modified or deleted when needed.

A systematic review study [7] stated six groups for the relevant of GDPR to blockchain, see Table 3.

Previous studies have focused on specific areas for blockchain-GDPR compliance, while this study is difference where the researchers stated all the characteristics of BC and all the GDPR principles

and rights in order to find the compliance issues and make blockchain technology more GDPR-compliant, in addition, limited studies investigated blockchain-GDPR compliance in a holistic approach, thus, this study helps researchers to continue in this topic and develop new models to solve BC-GDPR compliance issues.

Table 3. The Relevant GDPR Articles to Blockchain

Group Title	Article Title	Article Number
Territorial scope	Territorial scope	Article 3
Data processing principles and lawfulness	Principles relating to processing of personal data	Article 5
	Lawfulness of processing	Article 6
	Transparent information, communication and modalities for the exercise of the rights of the data subject	Article 12
Consent management	Conditions for consent	Article 7
Data deletion and modification	Right to rectification	Article 16
	Right to erasure ('right to be forgotten')	Article 17
	Right to restriction of processing	Article 18
Protection by design by default	Data protection by design and by default	Article 25
Responsibilities of controllers and processors	Responsibility of the controller	Article 24
	Joint controllers	Article 26
	Processor	Article 28

4. METHODLLOGY AND STUDY FRAMEWORK

The main aim of this study is to make a review and identify study areas related to GDPR compliant blockchain, in addition to explore the possible research gaps, this study started with an overview of GDPR, overview of blockchain, and then, the related work of GDPR compliant blockchain were stated. The study questions were stated to find the relation between both items (blockchain and GDPR). The following Figure 4 clarifies the study framework.

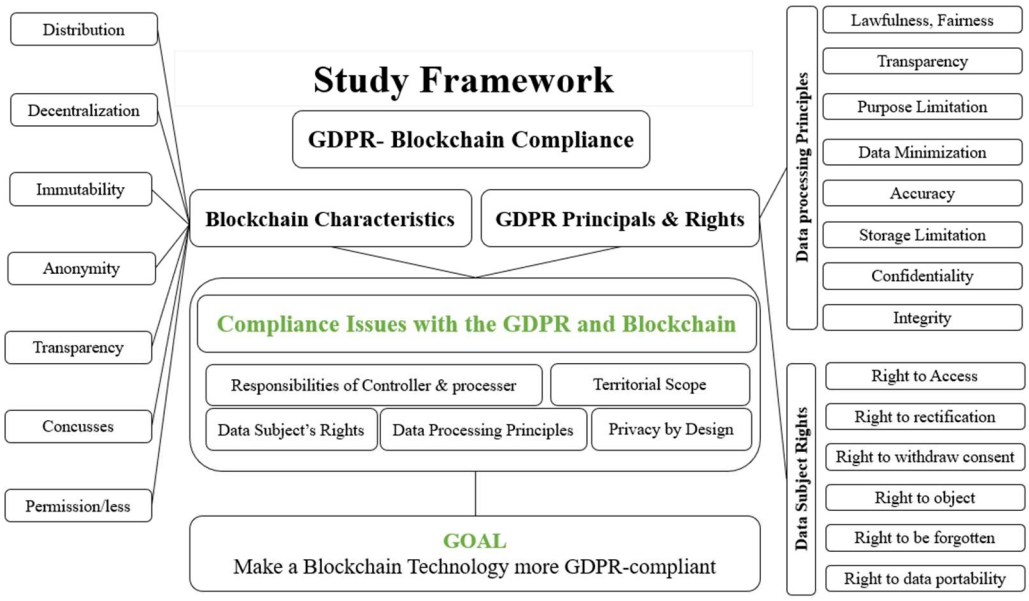

Figure 4. Study Framework

4.1 What is Blockchain Characteristics?

Distribution: In distributed networks, all nodes work together, the same database is distributed on each node. A distributed system could have a centralized or decentralized structure.

Decentralization: In centralized systems, each transaction is validated through a central entity (third party), while in decentralized system each transaction conducted by any node without need a central entity. Figure 5 clarifies the difference between centralized and decentralized system's structure [24].

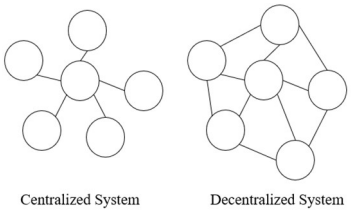

Figure 5. Centralized and Decentralized Systems

Immutability: Each transaction is validated before recorded in blocks, all nodes have a copy of database, therefore, it is impossible to modify the recorded data, thus, any tamper could be detected easily, this guarantees the integrity [24].

Anonymity: All users in blockchain are anonymous, since user's address is represented by the hash of a public key, this guarantees the anonymity [9].

Transparency: Each transaction is validated with timestamp, thus it is easy to trace the previous transactions through the distributed stored database [24].

Consensus: Blockchain technology employs consensus algorithms which ensures all nodes participate in the agreement in blockchain network [10], consensus protocols are needed in blockchain to avoid any disruption action from adversary, besides to decide which node has a permission to add a new block to get a reward, consequently the rest nodes verify that block and update their ledger accordingly [9]. Several consensus protocols have proposed such as:

Proof of Work (PoW): The most common algorithm used which depends on the work (computational power) done by node to obtain a new block, the block has to be validated before making change, it takes at least 10 minutes to add a block in the chain.

Proof-of-Stake (PoS): The permission for verification depends on the node with the less vulnerability to attacks.

Delegate Proof of Stake (DPoS): Permissions for verification are controlled by selected delegates.

Proof of Capacity (PoC): The proof depends on the storage capacity.

4.2 Types of Blockchain

There are three main types of blockchain; public, hybrid and private blockchains [10]. Bitcoin cryptocurrency is an example of public blockchain which is fully decentralized system and anyone can be part of this public blockchain, while Hyperledger lies in hybrid blockchain which is partially distributed, thus at least five of the ten consensus nodes verify the generated blocks. The private blockchain is a centralized system and it is controlled by specific entities like governance and healthcare management [10].

Permission and permissionless blockchains are another category. Permissionless blockchain, where any node can participate in consensus and join to the blockchain without any permission, on the other hand, nodes must be permissioned and granted access to participate in consensus in permissioned blockchain [4]. The following Table 4 states a comparison between blockchain characteristics and types.

Table 4. Comparison Between Blockchain Types

Characteristic	Public Blockchain	Private Blockchain
Consensus participation	All nodes	Organization/ selected nodes
Read permission	Public	Public or restricted
Centralized	No	Yes
Efficiency	Low	High
Consensus	Permissionless	Permissioned

5. RESEARCH FINDINGS AND DISCUSSION

5.1 What are the main compliance conflicts between GDPR and blockchain?

There are three articles in the GDPR that are conflict with Blockchains; article 16 which is about the right to rectification[4], article 17 which about the right to be forgotten[5] and article 18 which about the restriction of processing data[6]. Table 5 clarifies the main conflicts between GDPR and blockchain.

Table 5. Main Conflicts Between GDPR and Blockchain.

[4] https://gdpr-info.eu/art-16-gdpr/
[5] https://gdpr-info.eu/art-17-gdpr/
[6] https://gdpr-info.eu/art-18-gdpr/

GDPR	Blockchain
Article 16 gives the right to correct and modify the existing personal data, even add new data if the current data is inaccurate or incomplete.	Adding new data to a blockchain is not a problem, but changing data is.
Article 17 gives the right to forget and delete the data.	It is not being able to remove data from blockchain, therefore they cannot store personal data in blockchain.
Article 18 which gives the right to prevent companies from doing something with users' data.	completely open, allowing anyone to grab a copy of all the data. Hence, there is no control over who is processing data.

5.2 How to make a blockchain technology more compliant with GDPR?

The following suggestions state how can a blockchain get around the previous mentioned issues.

Suggestion 1: Encryption

The first possible solution would be to encrypt personal data before storing it on a blockchain using strong encryption means that only the person or company with the decryption key can process that data. To delete the data, it is suggested to destroy that key and then the encrypted data becomes useless, but strong encryption is still reversible. As computers get faster over time, it is more likely that the encryption can be broken and reveal the personal data again. Maybe not such a good solution after all.

Suggestion 2: Permissioned Blockchain

A better solution would be to store the personal data in a permissioned blockchain instead of a public one. Public blockchains allow anyone to see the data that is stored inside of them and to put new data on the chain. while in permissioned blockchains the access is controlled and restricted to only a few known and trusted parties. By doing this it will be complied with article 18 of the GDPR: the right to restrict who can process your data. But a permissioned blockchain is still immutable, meaning data cannot be deleted or edited, this does not comply with article 16 and 17.

Suggestion 3: Hash and Central Server for off-chain storage

A real solution would be an off-chain storage which is simply store the personal data somewhere else, where it can be accessed such as a secure server. A reference can be stored to that data on blockchain. Almost like a shortcut or pointer. To create this link, a digital fingerprint of the data using a hash function is used. And then that hash is stored on the blockchain.

Hash has two interesting properties. First, hashes work in one way, meaning the hash of some data can be created, but cannot take the hash and turn it back into that data. And secondly, a hash function allows to verify that the files on the central server have not been tampered with.

An important property if moving to this model is that the hash stored inside the blockchain is just a string of random letters and numbers, but it qualifies as personal data because it can be linked to the data on the server. Hence, to exercise the right to be forgotten, just the actual data is removed from the central server. Therefore, the hash in blockchain becomes useless and is no longer considered personal data, because it points towards nothing. However, this solution is not perfect because blockchains are decentralized and with a system like this you would partially centralize it again.

Suggestion 4: Zero-Knowledge Proof

This is a technology that allows to prove that something is true, without revealing the actual data. In case of a cryptocurrency, it can be proved that a transaction happened without disclosing how much money is transferred or to whom. This technology is used by Zcash to let users completely hide their transactions [8].

The following Table 6 clarifies suggested solutions for making GDPR-blockchain compliance [7].

Table 6. suggested solutions for GDPR-blockchain compliance

Group Title	Article Title	Article No.	Suggested Solutions
Territorial scope	Territorial scope	Article 3	Private BC
Data processing principles and lawfulness	Principles relating to processing of personal data	Article 5	Smart contracts

	Lawfulness of processing	Article 6	Smart contracts
	Transparent information, communication and modalities for the exercise of the rights of the data subject	Article 12	Smart contracts
Consent management	Conditions for consent	Article 7	Smart contracts
Data deletion and modification	Right to rectification	Article 16	Permissioned BC
	Right to erasure ('right to be forgotten')	Article 17	Hash and Central Server for off-chain storage
	Right to restriction of processing	Article 18	Smart contract
Protection by design by default	Data protection by design and by default	Article 25	Zero knowledge proof for anonymity
Responsibilities of controllers and processors	Controller	Article 24	Miners in private BC
	Joint controllers	Article 26	Miners in private BC
	Processor	Article 28	Miners in BC or developers of smart contracts

6. CONCLUSION AND FUTURE WORK

This study explored BC features, all GDPR principles and GDPR rights, it investigated the relation between GDPR and blockchain, additionally, it stated the main issues related to GDPR-Blockchain compliance, it is concluded that there are several conflicts that make blockchain not compatible with the GDPR such as distribution, decentralization, immutability, processing data, consent management, and responsibilities of nodes. However,these conflicts can be solved by the suggested solutions such as using private-permissioned blockchain, smart contracts, and off-chain storage that make blockchain more compliant with the GDPR principles and rights. For future work it is suggested to develop a GDPR-Blockchain compliance model that gathered all the suggested solutions in this study.

ACKNOWLEDGMENT

We would like to thank Arab American University and Palestine Technical University for their support.

REFERENCES

[1] Y. Salem, M. Moreb, and K. S. Rabayah, "Evaluation of Information Security Awareness among Palestinian Learners," pp. 21–26, 2021, doi: 10.1109/icit52682.2021.9491639.

[2] A. P. Guide, *Data Protection Regulation*.

[3] B. K. Mohanta, D. Jena, S. S. Panda, and S. Sobhanayak, "Blockchain technology: A survey on applications and security privacy Challenges," *Internet Things*, vol. 8, p. 100107, 2019, doi: 10.1016/j.iot.2019.100107.

[4] J. Bernal Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. Torres Moreno, and A. Skarmeta, "Privacy-Preserving Solutions for Blockchain: Review and Challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019, doi: 10.1109/ACCESS.2019.2950872.

[5] G. Zyskind, O. Nathan, and A. S. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," *Proc. - 2015 IEEE Secur. Priv. Workshop SPW 2015*, pp. 180–184, 2015, doi: 10.1109/SPW.2015.27.

[6] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Comput. Surv.*, vol. 52, no. 3, 2019, doi: 10.1145/3316481.

[7] A. B. Haque, A. K. M. N. Islam, S. Hyrynsalmi, B. Naqvi, and K. Smolander, "GDPR compliant blockchains-a systematic literature review," *IEEE Access*, vol. 9, pp. 50593–50606, 2021, doi: 10.1109/ACCESS.2021.3069877.

[8] L. Wang, X. Shen, J. Li, J. Shao, and Y. Yang, "y," *J. Netw. Comput. Appl.*, vol. 127, pp. 43–58, 2019, doi: 10.1016/j.jnca.2018.11.003.

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on Blockchain technology? - A systematic

review," *PLoS ONE*, vol. 11, no. 10, pp. 1–27, 2016, doi: 10.1371/journal.pone.0163477.

[10] Y. Lu, "Blockchain and the related issues: a review of current research topics," *J. Manag. Anal.*, vol. 5, no. 4, pp. 231–255, 2018, doi: 10.1080/23270012.2018.1516523.

[11] M. H. Barkadehi, M. Nilashi, O. Ibrahim, A. Zakeri Fardi, and S. Samad, "Authentication systems: A literature review and classification," *Telemat. Inform.*, vol. 35, no. 5, pp. 1491–1511, 2018, doi: 10.1016/j.tele.2018.03.018.

[12] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K. K. Raymond Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, no. February, p. 102731, 2020, doi: 10.1016/j.jnca.2020.102731.

[13] M. Goddard, "Viewpoint: The EU general data protection regulation (GDPR): European regulation that has a global impact," *Int. J. Mark. Res.*, vol. 59, no. 6, pp. 703–706, 2017, doi: 10.2501/IJMR-2017-050.

[14] M. Monti and S. Rasmussen, "RAIN: A Bio-Inspired Communication and Data Storage Infrastructure," *Artif. Life*, vol. 23, no. 4, pp. 552–557, 2017, doi: 10.1162/ARTL_a_00247.

[15] M. DI Pierro, "What Is the Blockchain?," *Comput. Sci. Eng.*, vol. 19, no. 5, pp. 92–95, 2017, doi: 10.1109/MCSE.2017.3421554.

[16] E. Y. Daraghmi, Y. A. Daraghmi, and S. M. Yuan, "MedChain: A design of blockchain-based system for medical records access and permissions management," *IEEE Access*, vol. 7, pp. 164595–164613, 2019, doi: 10.1109/ACCESS.2019.2952942.

[17] Daraghmi, Daraghmi, and Yuan, "UniChain: A Design of Blockchain-Based System for Electronic Academic Records Access and Permissions Management," *Appl. Sci.*, vol. 9, no. 22, p. 4966, Nov. 2019, doi: 10.3390/app9224966.

[18] E.-Y. Daraghmi, M. Abu Helou, and Y.-A. Daraghmi, "A Blockchain-Based Editorial Management System," *Secur. Commun. Netw.*, vol. 2021, pp. 1–17, May 2021, doi: 10.1155/2021/9927640.

[19] F. Zemler and M. Westner, "Blockchain and GDPR: Application scenarios and compliance requirements," *PICMET 2019 - Portland Int. Conf. Manag. Eng. Technol. Technol. Manag. World Intell. Syst. Proc.*, vol. 0, 2019, doi: 10.23919/PICMET.2019.8893923.

[20] K. Wust and A. Gervais, "Do you need a blockchain?," *Proc. - 2018 Crypto Val. Conf. Blockchain Technol. CVCBT 2018*, no. i, pp. 45–54, 2018, doi: 10.1109/CVCBT.2018.00011.

[21] A. Bayle, M. Koscina, D. Manset, and O. Perez-Kempner, "When Blockchain Meets the Right to Be Forgotten: Technology versus Law in the Healthcare Industry," *Proc. - 2018 IEEEWICACM Int. Conf. Web Intell. WI 2018*, pp. 788–792, 2019, doi: 10.1109/WI.2018.00133.

[22] A. Rieger, J. Lockl, N. Urbach, F. Guggenmos, and G. Fridgen, "Building a blockchain application that complies with the EU general data protection regulation," *MIS Q. Exec.*, vol. 18, no. 4, pp. 263–279, 2019, doi: 10.17705/2msqe.00020.

[23] C. Wirth and M. Kolain, "Privacy by BlockChain Design: A Blockchain-enabled GDPR-compliant Approach for Handling Personal Data," *Proc. 1st ERCIM Blockchain Workshop 2018 Eur. Soc. Socially Embed. Technol. EUSSET*, p. 6, 2018.

[24] X. Chen, "Blockchain challenges and opportunities : a survey Zibin Zheng and Shaoan Xie Hong-Ning Dai Huaimin Wang," *IEEE Int. Symp. High Perform. Distrib. Comput. Proc.*, vol. 14, no. 4, pp. 352–375, 2018.