New Blockchain Protocol for Partial Confidentiality and Transparency (PPCT)

Salima TRICHNI, Mohammed BOUGRINE, Fouzia OMARY
Faculty of Sciences Mohammed V University in Rabat, Department of Computer Science, Rabat, Morocco

***Abstract*—Running behind new technologies is increasingly becoming a non-circumventable requirement for organisms' survival. This is not only a strategy to gain a competitive advantage in the market but it is a determinant key for their continuity and persistence. The Blockchain is at the heart of this technological revolution for which transparency, accessibility to the public and the sense of sharing are fundamental properties of its design. Despite its importance, leveraging this technology in an ethical and secure manner by ensuring confidentiality and privacy is a top concern. Through this work, we try to design a new approach to validate transactions within the Blockchain. Entitled "Protocol for Partial Confidentiality & Transparency PPCT", this new protocol makes possible to seek a compromise between the two requirements: Confidentiality & Transparency. It allows introducing a new notion of confidentiality that we have named partial confidentiality. Subsequently, it applies it on the transactions exchanged while ensuring the process of their validations by the different nodes of the Blockchain. In addition, and through the use of hashing and digital signature functions, this protocol also ensures integrity and authentication within its validation process. To present this work, we will first discuss the state of the art on the different current privacy approaches and our motivation behind this work. Then we will explain more about the different stages of this process, its benefits and areas for improvement.**

***Keywords*—Blockchain; security; privacy; confidentiality; transparency; integrity; authentication; validation process**

I. INTRODUCTION

Blockchain, the founding technologies of cryptocurrency is very fashionable and on trend recently [1]. Its first use took place in 2009 by Satoschi Nakamoto thus giving birth to Bitcoin [2]. And since then, its fields of application have not stopped expanding to serve different sectors, including banks, insurance, the pharmaceutical industry, supply chains. It is at the heart of the current digital technological revolution and considered by some to be the revolutionary successor to the Internet [3]. Indeed, it allows disintermediation or the renunciation of a trusted third party, thanks to its decentralized architecture coupled with its transparency and its high security. The decentralized architecture of the Blockchain results from its constitution as a distributed P2P (peer-to-peer) network. The latter is made up of a set of nodes through which the exchanges and storage of information present in chained blocks (called a chain of blocks) and linked to each other are carried out. The resulting chain of blocks is incremented as soon as new transactions are validated by a set of network nodes according to a precise consensus algorithm (proof of work or proof of stack or...). With regard to security, it is guaranteed fundamentally in the blockchain by cryptographic processes and in particular asymmetric cryptography [4].

For example, in the cryptocurrency field, if Alice wants to send money to Bob (Alice and Bob are the usual protagonists in the cryptographic context) she will create a transaction specifying the amount to be sent and broadcast it to all nodes. This transaction will be grouped with other transactions in a single block, which will be validated later. All of the nodes in this network verify the transactions in this block using a consensus protocol to obtain network approval. As soon as a group of nodes succeeds in verifying and validating all the transactions contained in the block, this later can be added to the Blockchain. Fig. 1 provides an illustration of this process. Thus, when the "block" containing the transaction is approved by the other nodes and added to the Blockchain that this transfer of money between Alice and Bob will become legitimate [4].

Nevertheless, the adoption of this technology encounters some difficulties and obstacles that prevents the putting in practice and still cause concern among entrepreneurs and investors. Serious problems but which cannot be evaded because this innovation offers much needed potential and assets. These issues can be projected on three essential scales, on the one hand the safety of the technical tools and their ability to guarantee the different properties promised by this technology, on the other hand, the functional aspect linked to the business domains of its application, including financial and economic issues. Then, and finally the legal scope reflecting the reliability claimed by the technology to protect public order, control the consumer and eliminate fraudulent use. As part of this contribution, we focus more on the aspect of transaction confidentiality which is one of the major challenges for the adoption of this protocol. Our goal is to seek a trade-off between transparency and data privacy which is a dilemma of Blockchain adoption [3]. Indeed, although the Blockchain is a transparent and public register, keeping transactions or certain sensitive information confidential is one of the great expectations in this technological context [5], which hinders its adoption in most cases. So, there are many legitimate reasons for conducting private transactions. Reasons may be critical, such as revealing your sources of income to your competitors, your health problems, etc. Other reasons are not necessarily critical, such as keeping a surprise for your spouse secret. In any case, it is a human right that we must absolutely respect. Unfortunately, this property is not supported in today's most popular Blockchains such as Bitcoin. In general, in this type of system, pseudonym tools are often used in order to hide the real identity of the users [6].

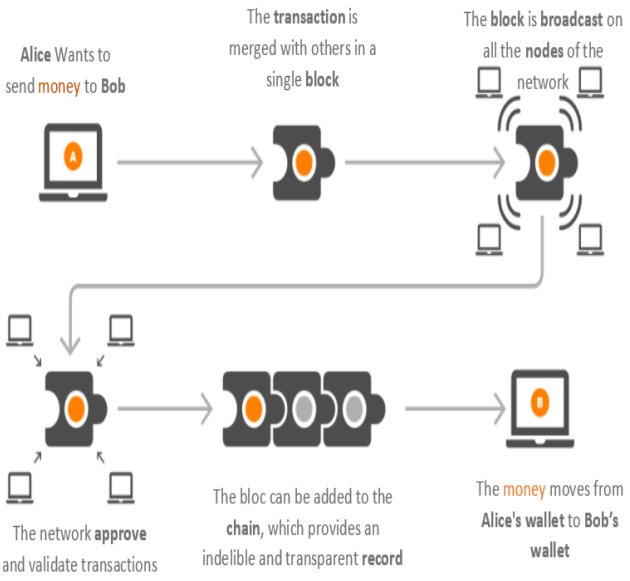

Fig. 1. The Concept of Blockchain Operation.

These tools are based on sender and recipient address type information and solve this problem by relying on the principle of sharing information without being visible to the public. On the other hand, if an adversary has key information about one of the two parties, he can acquire links or relations leading to the true identity and so decrypt the pseudonym of this user [7]. Although the techniques of anonymization and pseudonym are more and more complex and sophisticated; the risks of privacy leakage due to various inference attacks [8] are also well developed [9]. Therefore, it is essential to implement stronger protection mechanisms.

We will dedicate the following section to discuss key techniques that can help improving data confidentiality and transaction privacy on the Blockchain.

II. Related Work

Most of the work that aims to solve the problem of privacy in the Blockchain, is more focused on what is called by "secure computing". Indeed, this type of solution is based on techniques allowing the realization of calculations on data without revealing the secret part of each transaction. To do this, these works are essentially based on one or two of the following encryption approaches:

- The Attribute-Based Encryption (ABE) approach.
- The Secure Multipart Calculation (SMPC) approach.
- The Homomorphic Encryption (HE) approach.
- The Non-interactive zero-knowledge proof (NIZK).

In this section, we will try to address these approaches by describing some of the work done under each approach.

A. Attribute-Based Encryption (ABE)

Proposed in 2005, the concept of attribute-based encryption (ABE) was first introduced based on a single authority [7]. It represents a new encryption policy that builds on the same principle of asymmetric encryption by adding an additional layer to include user-specific attributes. This is a recent and promising approach to provide both data privacy and access control to that data through the integration of private attributes into all the tools of this protocol. The policy for the use of these attributes must be defined in advance by the appropriate authority [10] [11] in order to be able to cryptographically combine decryption keys with data access permissions. The data thus encrypted does not need to be transmitted over a secure channel or stored in a trusted server. To decrypt encrypted data, users must now meet the access policy that is defined based on the attributes that can be associated with data users, data elements, and the environment. Despite their power, these algorithms are not very widespread because of the difficulty associated with their design and implementation. Little is done using this type of encryption [5].

In blockchain, for example, the first proposal for the use of ABE was published in 2011 in [12], it is a decentralized ABE scheme that is based on access tokens assigned according to the rights of each node. Token tracking automatically goes through the processes that are in place. The distribution of tokens no longer relies on a central authority [4], several nodes can be elected through witnesses to play this role. Another ABE-based encryption proposal was patented in [13] and published in 2018. It consists of an encryption solution based on a pre-calculation phase that does not require exchanges with trusted servers and that significantly reduces the cost of computing encryption on devices with limited resources. This encryption is based on CP-ABE "Ciphertext-Policy Attribute-Based Encryption" and defines an access policy for encryption by referring to an access structure in the form of a tree. Encryption goes through 2 steps, the first performs a multiplication between random elements defined by a randomly generated polynomial on each root of the tree and the elements of a cyclic group. The second step is based on the results of the pre-calculation performed previously and stored in a memory to accomplish the encryption task.

B. Secure Multi-party Computing

The Multiparty Computing Model (MPC) is a generic cryptographic scheme for performing secure calculations between two or more parties without revealing their private data inputs. The first variants of this type of encryption were proposed by Andrew Yao [9] [14], the first in 1982 concerns just two parts while the second in 1986 and is generalized on several parts. Other designs of this scheme have been successfully realized and applied on a variety of issues such as distributed voting, private auctions and lately in the Blockchain. In [15], Andrychowicz and all built an MPC protocol for Bitcoin to be used in the lottery field to ensure honest behavior within this Blockchain. This type of algorithm was also used in a work published in [16]. Ce Last offers a secure computing solution for Blockchain networks, it uses the MPC calculation protocol by separating the ownership of the data and the use of this data and allows to reduce the burdens of the computational work to a few nodes by using a layer 2 solution, then it uses the message authentication code (MAC) to verify the accuracy of the calculation carried out. We thus conclude with another work in this same context; this is the

Enigma platform that is also based on SMPC and hardware privacy technology TEE (Trusted Execution Environment) to provide computation over encrypted data and guarantee confidentiality [17].

C. Homomorphic Encryption (HE)

Homomorphic encryption (HE) is a new family of cryptographic tools. It adds a verifiable compute layer while maintaining the confidentiality of source data [4]. Indeed, homomorphic encryption must be able to evaluate encrypted data by performing certain arbitrary functions directly on the ciphertext [18]. On the other hand, when deciphering the results found we end up with values identical to those performed by the same operations on the plaintext. The application of this type of encryption within the Blockchain is of great use to ensure the confidentiality of data. It makes it possible to store the encrypted data in the distributed ledgers of the Blockchain [19], and then execute the validation process on this encrypted data without proceeding to its decryption. Y.Wang and A.Kogan proposed in [20], a new design of a transaction processing system based on the Blockchain and dedicated to accounting and auditing. This design aims to ensure the confidentiality of transactions by using on the one hand the Homomorphic algorithms and on the other hand the approach of the non-interactive proofs with zero knowledge NIZK and more precisely its variant zk-SNARK.

D. Non-Interactive Zero-Knowledge Evidence (NIZK)

Proposed in the early 1980s [21], the ZK zero-knowledge interactive proof system is the first version of this approach that allows a certifier to prove to a verifier that a statement is accurate without providing any useful information to the verifier, in other words, it allows, from a formal proof applied to a secret entry, generate an exit open to the public without disclosure of any other information [22]. This variant then became Non-Interactive in the sense that it no longer requires direct interaction between the certifier and the verifier. It is enough that the latter two share a common reference chain to achieve the same objective, which is zero knowledge. This is called NIZK. The use of this type of algorithm in the Blockchain is in great demand. It has been used in several cryptocurrencies in order to prove the validity of the transfer of the currency between the different entities without having any knowledge about the balance of each entity. Several other versions of this same protocol have been proposed in the context of the Blockchain, the best known of which are currently:

- Zcash [23] a cryptocurrency based on the Bitcoin code and integrates zk-SNARK [24] in order to be able to verify transactions while keeping user information confidential.
- Zerocash over Ethereum (ZoE), applied on Ethereum, it allows a user to store Ether (ETH) in a discreet manner by adding a "serial number" as a commitment in a Merkel tree, which is maintained by the contract [4].

Admittedly, all the approaches just mentioned offer very innovative solutions for ensuring the confidentiality of sensitive data, however, as we can see from the description of each one, these approaches nevertheless remain limited to specific cases and cannot be applicable on any type of consensus [6]. They are more applicable in cases where the process of validating a transaction requires the calculation of one or more operations [16]. So, in the case of a consensus based on a procedural and purely functional smart contract, the application of this type of solutions will not be possible otherwise it will be expensive [17].

Other disadvantages can hinder the use of this type of algorithm such as their slowness and cost in terms of consumption of physical resources [16]. This is due to the fact that the calculations/checks they use are not done directly on the raw data. On the other hand, these algorithms consider a limited amount of data and cannot support a large input volumetric [20]. And finally, these approaches still suffer from their lack of maturity and complexities related mainly to the difficulty of their implementation and implementation [13].

The encryption approach proposed in this work is generic and applicable on any type of consensus. In contrast to the solutions presented above, our model offers more fluidity and makes it possible to exploit the symmetric encryption algorithms that have largely proven their robustness and performance in the field. In addition, it integrates other security tools such as hash functions and digital signatures [25]. The flexibility of this protocol does not only concern the security tools put in place, but also at the level of the distribution of roles at each transaction, something that prevents the vulnerability of the system.

III. Methodology

The new PPCT protocol proposes to keep some of the information confidential and leave other non-sensitive information transparent and readable by everyone. It aims to use the principle of partial confidentiality in order to be able to share transactions in a public way while keeping sensitive data secret except in the eyes of authorized nodes. This solution promotes parallelization of the transaction verification activity to ensure the security of the system by separating the tasks between the different participants of the distributed network.

To further explain the system, below are all the definitions and steps put in place under this protocol.

A. Definition: Partial confidentiality

This work presents a new concept of confidentiality which is partial confidentiality. As its name suggests, this concept aims to ensure the ownership of confidentiality just on a part of the data deemed to be sensitive. To do this, the partial confidentiality algorithm requires prior identification of sensitive information, then it proceeds to ordinary encryption processes to encrypt this data and reintegrate it at the end of the algorithm into its original context, Fig. 2.

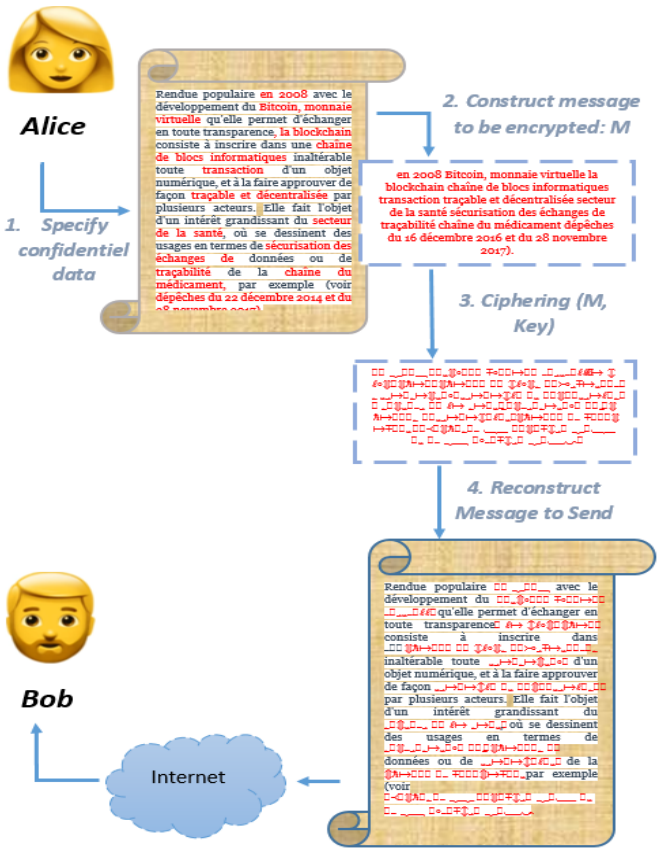

Fig. 2. Principle of Partial Confidentiality.

To better assimilate this algorithm, below are the details of the operations performed at the level of each step:

- Step 1 – Identification: The first step of this system is to identify the sensitive information in the text to be shared using a separation mechanism before and after each part.
- Step 2 - Extraction: The second step is to extract sensitive information from the text to be shared by referring to the separator used for this protocol. Then, they are grouped in an apartment block called black-blocks (BBs) and which will be encrypted in the next step.
- Step 3 – Encryption: Encryption is performed on the black blocks (BBs) containing the sensitive data using a symmetric encryption algorithm whose secret key is that of the entities authorized to validate the transaction or part of the smart-contract.
- Step 4 – Reconstruction: The reconstruction step consists of integrating the different bytes of the encrypted BBs into their initial positions of the clear text by referring another time to the separator set up during the identification step.

B. Transaction Trust Group: TTG

Each participant /organization shall identify in advance its trusted group with which it must ensure the validity of the information exchanged in full transparency. This trusted group can be considered as a private subnet of our distributed network whose cryptographic key exchange is previously carried out outside the Blockchain.

C. Transaction Base

In a Blockchain several types of transactions can circulate and exchange between the different nodes of the network, each transaction reflects a specific functionality in the process to be digitized. It can present a purchase, a transfer, a contract verification, the result of a diagnosis, or others. Regardless of the type of transaction, in our system we require to specify the structure of all possible transactions and give them a well-defined base. The Pillar of each transaction must distinguish between public information and information that must remain secret.

D. Partial Confidentiality

As we have presented before, partial confidentiality is a technique that has just been defined to ensure the privacy of a set of information included in a data model intended for the public. To do this, it is necessary to go through the separation of these two categories of data, encrypt the sensitive part based on a cryptographic encryption tool and finally reintegrate this part into the model in question, Fig. 3.

E. Private Validation

In order to validate the current transaction, each node in the trusted group partially decrypts the model, calculates the hash of the content in clear and then proceeds to the realization of their tasks necessary for their validation.

Validators send their signed and encrypted responses using the hashed of clear text as the encryption key, it is also called the "public validation key" (kv).

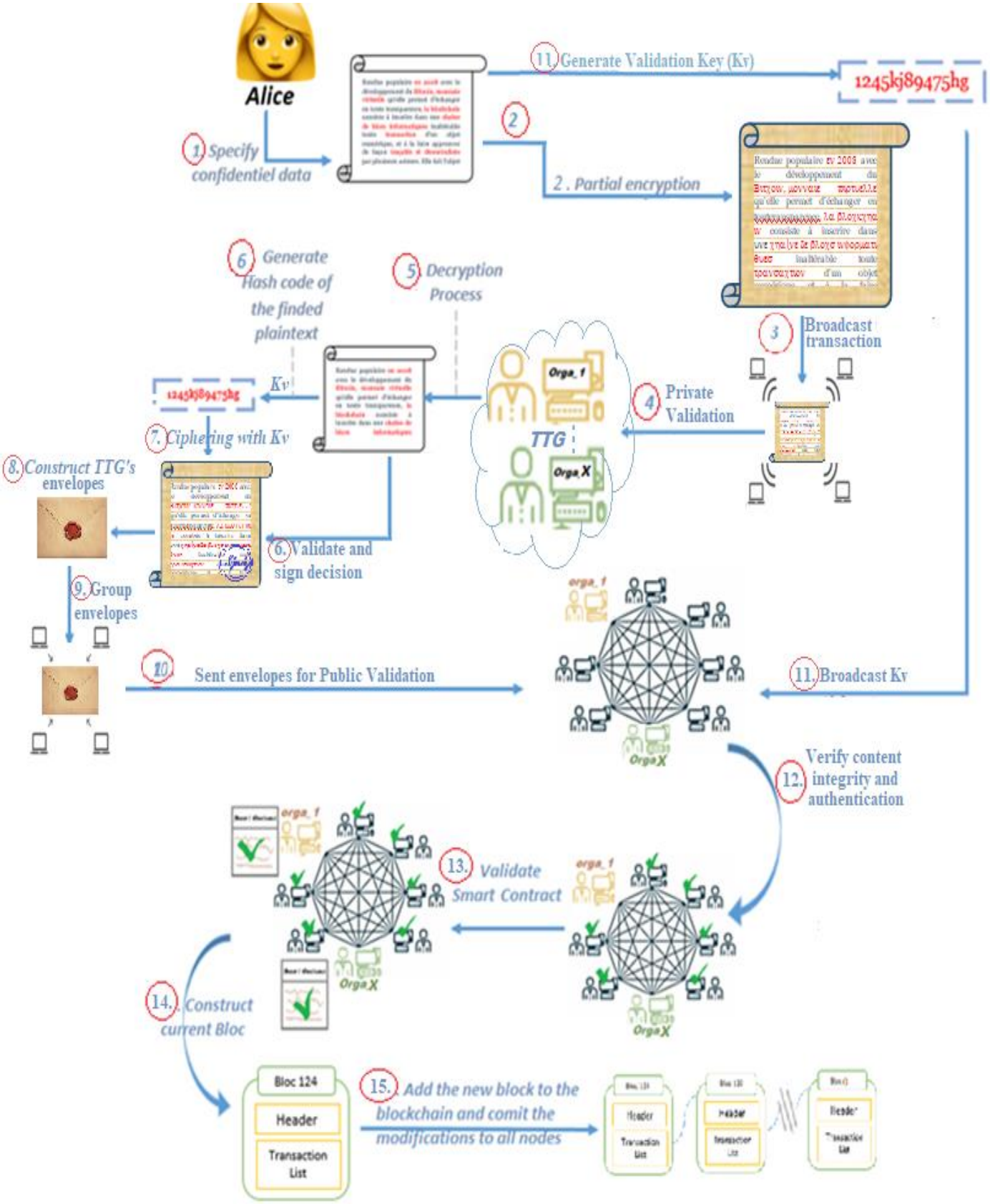

Fig. 3. Protocol Preserving Confidentiality and Transparency (PPCT).

It should be noted that each validator node also has a base for its response and uses its own signature to sign its decision. The whole thing is encrypted using the hash of the clear. This encryption operation has a very important role in this security protocol. On the one hand, it ensures the credibility of the validator's decision because he had the right hash code and therefore was able to rely on the right information contained in the plaintext model. On the other hand, through this encryption we manage to protect the group against the infiltration of malicious nodes so as not to impact the final decision of the transaction, and therefore, we ensure the neutrality of this decision. This operation is considered a closed envelope intended to be broadcast on the network.

F. Public Validation

Once you receive the envelopes from the various validators of the trusted group, a notification is sent to the initiator of the transaction in order to send the hashed clear in the Blockchain. The final transaction is built based on the model, hash and envelopes of the trusted group.

The transaction is added to the Blockchain block and sent to the public network for final validation. The public network opens the envelopes of each validator by performing the decryption operation with the key the hashed of the clear, then compares the results and performs its global checks to validate the operation.

If the public validators manage to decipher the message with the hashed of the clear it means that the private validator had the right content of the model that the initiator of the transaction and therefore on the basis of the different answers the public validates the final transaction.

Once the final validation consensus is passed, the block is stored and added to the ledger via the ordinary mechanisms of the Blockchain.

IV. USE CASE: REIMBURSEMENT FOR CARE

For example, in the field of health where trust holds a dominant and decisive place, the application of the Blockchain can open up very promising horizons and prospects. The desire for perfect traceability in an environment where information is shared and stored in a fairly transparent manner, while ensuring a reasonable degree of security for a real control of the data circulating there. This field of application, which requires the coexistence of these two seemingly antagonistic qualities, is very favorable for the production of our solution. Understanding this health process in a Blockchain is of great use. In fact, it reduces their complexity by facilitating the management of relationships between different heterogeneous information systems while ensuring a secure and transparent exchange of information. This Blockchain brings together the entire medical profession, patients, insurance companies, radiology centers, laboratories, pharmacies, physiotherapy centers.... In short, all professionals in the field of health must come together around this Blockchain, each from its own angle, to ensure the smooth running of different standards put in place in the service of health. These contributions in terms of: trust, security, simplification, and parallelization of verification procedures are immediately and not only in an economic gain in time and money but also in a huge improvement in the quality of life of the populations.

We can imagine a simple and very recurrent use case in our daily life and it is the procedure of reimbursement of care by health insurance. Automating the reimbursement of care is a rather complex task because it depends on the credibility and commitment of all entities in the field of health. The normal course of this reimbursement process requires a complete medical record containing all the supporting documents on the consultations, diagnoses, care and treatments carried out. This proof must be signed and validated by the various interlocutors in the field. All these papers are then deposited with the insurer who in turn carries out its checks and validates the file for reimbursement according to the insured's health insurance contract. Communication between the different interlocutors of a medical file is carried out by the patient. We start from this same principle and we propose the scenario modeled in the sequence diagram in Fig. 4.

Patient

- Identifies its interlocutors in the blockchain.
- Completes their medical file.
- Request for the validation of his file.

Healthcare Professional

- Validation of the medical file by the interlocutors.

Insurance:

- Validation of the medical record by the insurance.
- Reimbursement of the file.
- Validation of the refund transaction by the network.
- Transaction storage.

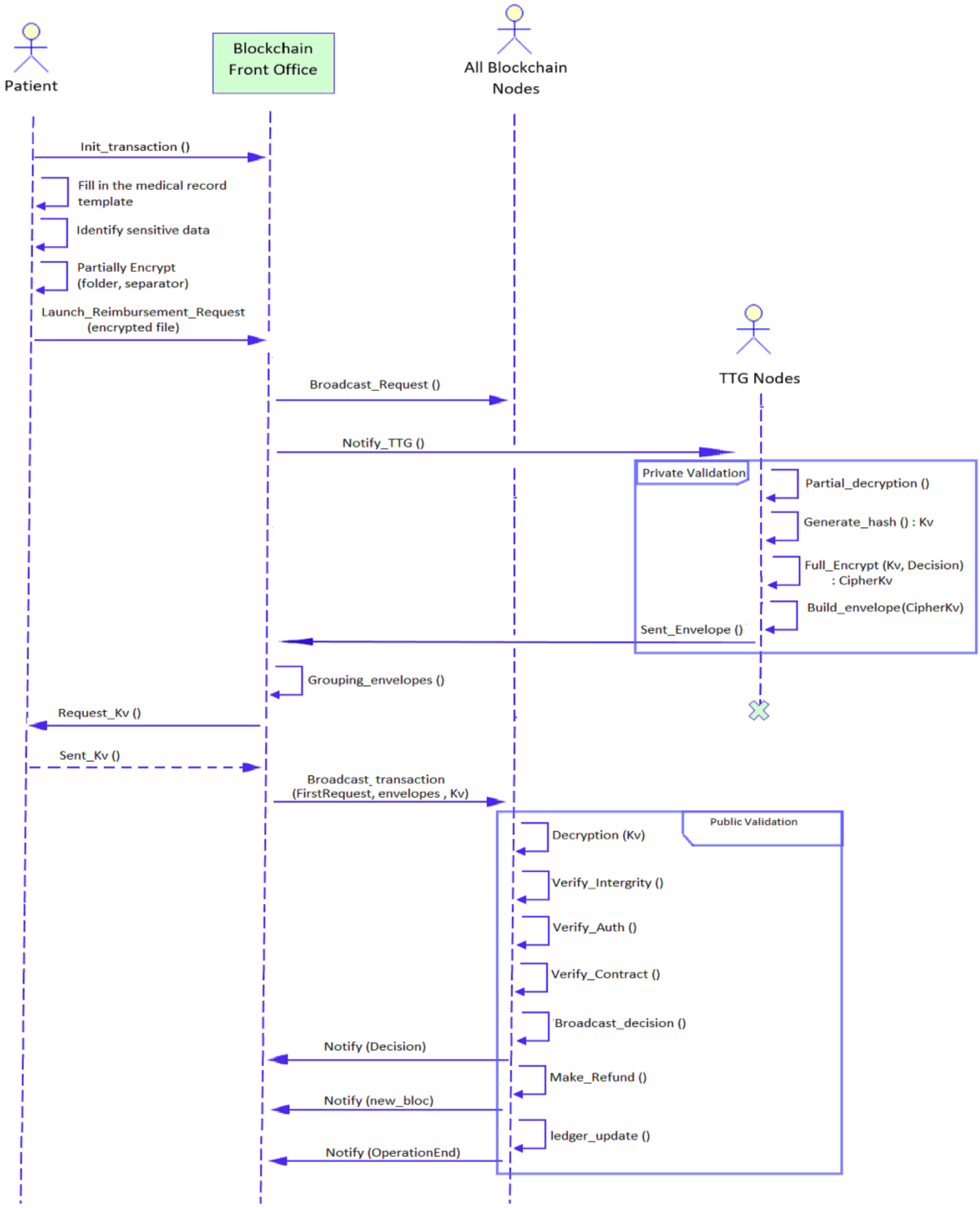

Fig. 4. Sequence Diagram for Healthcare Reimbursement.

V. Result and Discussion

As Blockchain technology is based on a distributed network, the notion of a central authority no longer exists. As a result, all members of this network are invited to execute the consensus in question in order to validate the transactions of this network. Nevertheless, with the immense evolution of the size of current Blockchains, collective intervention becomes more expensive whether in terms of quantity of calculations or transaction fees [26]. Thus, it causes real latency and performance issues on the network [27]. In addition, the security aspect is also impacted and is becoming increasingly difficult to ensure. Our protocol responds to this problem and offers advantages to keep the potential of the blockchain to the maximum while promoting its scalability and security. These benefits can be discussed in the following points:

A. Confidentiality

Confidentiality is ensured based on the process of partial confidentiality using ciphering algorithm [28] . This process makes it possible to encrypt sensitive data not necessary for the public validation of the transaction and then reintegrate it into the overall base of the transaction containing other public clauses. In this way, the public clauses as well as the basis of this type of transaction will be validated in public. On the other hand the trusted group of this transaction guarantee the validation of the private elements as a whole by performing the partial decryption and thus verifying the overall content of the current transaction.

B. Integrity

In addition to the confidentiality of sensitive data, the PPCT protocol also ensures the integrity of this data based on the hash of the clear part [25] [29]. The latter is designated in our protocol by the Kv validation key. This key is the same for all participants in the TTG group. It is used by each member of this group to encrypt all the elements of its envelope and distribute it within the distributed network. Once all envelopes are retrieved, the nodes in the public network ask the initiator to reveal the Kv validation key by distributing it to the network, and then they verify the integrity of the committed transaction. They decipher different envelopes of the TTG group. If the decryption of each envelope passes well it means that the hashed of the clear was the right one for this participant and its validation can be considered in the public validation.

C. Authentication

Ensuring authentication is also one of the advantages of this solution. Indeed, adding the signature [25] [29] of the validator of the TTG group makes it possible to verify his identity and to ensure that the decision sent in the network concerns the right person designated in the TTG group.

D. Off-chain Processing on a Small, Private and Dynamic (Cyclical) Network

The PPCT makes it possible to move part of the work outside the public network. It allows you to create a verifiable property in the outsourced calculation task [6]. This property is ensured by the Kv (Validation Key) which is carried out according to the sensitive data of each transaction. The Kv Key is an effective way for the public to confirm their validation without resorting to sensitive data from that transaction. The network delegates this task to the TTG while maintaining control over the work of this small private network. This solution is very useful in that it applies the principle of off-chain calculation [30] [16] in order to be able to solve this problem effectively. So, he

- does not depend on the size of the blockchain [16];
- promotes the scalability of the blockchain [27];
- reduces calculation costs [16];
- reduces overall transaction validation time [16].

E. Independent Treatment of Public Network Trust

The PPCT does not manage access to the Blockchain in a strict and permanent way, it is only at the time of the creation of the transaction that the initiator of the transaction designates his trusted group. This increases the security of the protocol for two reasons, the TTG group represents entities that are concretely trusted in reality and not defined in a procedural way. The second related to the dynamism of this group so even if one of the malicious nodes manages to integrate the TTG group of the current transaction, it will not necessarily be able to be in the other time. And so, the attack can only concern a single transaction and for which it can be well identified in the public validation stage.

- Permissions are not fixed and change from one transaction to another by favoring the choice of the initiator of the transaction.
- The initiator of the transaction designates his trusted group.

F. Efficient and Secure Processing Capacity

For the PPCT protocol, the calculation and validation time passes faster because it is realized after the decryption of sensitive information by the trusted group. Thanks to decryption [31], validation calculations do not represent any complexity and do not require any requirements in terms of computing power.

G. Independence of Data Type and Size

Digital or literal, Log file or raw data, the PPCT can be applied easily on the different types of transaction unlike other confidentiality protocols that are restricted to numerical data to perform calculations or to some private data to represent identity [32]. In our case, just choose the right Symmetric Encryption algorithms that perform better on the volume and types of data to be exchanged to improve the performance of the protocol [33].

H. Flexibility of Cryptographic Tools

Cryptographic tools can be appropriated according to the constraints of the entities that come into play in this Blockchain [33].

The following table (Table I) summarizes the advantages and disadvantages that we have been able to identify, in order to conclude a static comparison with our work.

TABLE I. COMPARATIVE SUMMARY

Technique	*Advantage*	*Disadvantage*	*Application*
HE	It can perform confidentiality-preserving calculations by performing calculations directly on the ciphertext.	Only certain types of operations, such as addition and multiplication, can be implemented effectively. The computational efficiency of complex functions is very low.	Etherium
MPC	It allows multiple parties to perform calculations jointly on their private data entries without violating their input confidentiality.	Only certain simple functions can be supported, and complex functions are less efficient.	Enigma
ABE	It can simultaneously ensure data confidentiality and precise access control.	Issuing and revoking the attribute certificate in a distributed environment has yet to be resolved.	SO
NIZK	The user can easily prove that he has a sufficient balance for the transfer with NIZK, without revealing the account balance.	Less effective	Zcash
PPCT	Ensures partial confidentiality while maintaining transparency on transaction.et also integrity and authentication	Latency to improve	SO

VI. CONCLUSION

The work presented in this paper has opened a new compromise track between transparency and privacy within the blockchain. First, through the introduction and after giving a general overview on blockchain technology, we have exposed the problem studied during this work as well as the main objective of our proposal which is: the confidentiality of sensitive data while preserving transparency within the blockchain infrastructure. We then presented the various related works in this context that are generally designed at the basis of secure calculation algorithms namely: ABE, SMPC, Homomorphic encryption and NIZK algorithms. Then we gave the detailed description of our solution entitled "Protocol for Partial Confidentiality & Transparency (PPCT)" by discussing, at the end of the article, its advantages over other equivalent systems. In summary, and through this work, it can be concluded that the PPCT protocol proposed here, was able to solve the problem of privacy by exploiting the conventional tools of cryptography and adapting them to the concepts of the blockchain in a new perspective. We defined a new notion of confidentiality that is partial confidentiality and then we integrated hash functions and signature algorithms at the heart of the validation process. The integration of the latter ensures the increase in the level of security of the system by guaranteeing the other two pillars of security, namely: integrity and authentication. Thus, the PPCT protocol makes it possible to ensure the confidentiality of the sensitive data of each transaction via the partial encryption of it, then the integrity of this data using its hash, then the authentication of the first validators' decision-makers of this transaction via their signatures. As presented in the discussion section, the performance of this protocol is well in line with other privacy solutions that rely on secure calculation tools. In our next work, we want to focus more on the latency time between the initial validation and the final validation of the transaction while studying ways to improve this criterion by adding the aspect of parallelism in this process. We also want to carry out comparative experiments between the different possible combinations and proposing a clearer scheme of use on each type of need.

REFERENCES

[1] R. a. C. M.-B. Beck, "Blockchain as Radical Innovation: A Framework for Engaging with Distributed," in Proceedings of the 50th Hawaii International Conference on System Sciences, 5390-5399, 2015.

[2] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," https://bitcoin.org/bitcoin.pdf, 2009.

[3] L. F. Frédéric Lau, Blockchain : passer de la théorie à la pratique. Les enjeux de la transformation pour l'adoption, Cigref, octobre 2018.

[4] I. Bashir, Mastering Blockchain-deeper insights into decentralization, cryptography, Bitcoin and popular Blockchain frameworks, Packt, 2017.

[5] "Rui Zhang and Rui Xue and Ling Liu, Security and Privacy on Blockchain,2019,zhang2019security,arXiv:1903.07602".

[6] P. J. T. C. X. L. a. Q. Xiaoqi Li, "A Survey on the security of blockchain systems," Future Generation Computer Systems, 2017.

[7] "Amit Sahai and Brent Waters. [n. d.]. Fuzzy Identity-Based Encryption. 457–473".

[8] H. C. Y. Z. M. H. M. S. Z. C. Yourong Chen, "A survey on blockchain systems: Attacks, defenses, and privacy preservation," High-Confidence Computing , vol. 2, no. 100048, 2022.

[9] "A. C. Yao. [n. d.]. Protocols for secure computations. In SFCS 1982. 160–164.".

[10] "Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, and BrentWaters. [n. d.]. Attribute-Based Encryption for Circuits from Multilinear Maps. 479–499.".

[11] "Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. [n. d.]. Attribute-based Encryption for Circuits. In Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing (STOC 2013). 545–554.".

[12] "Allison Lewko and Brent Waters. [n. d.]. Decentralizing Attribute-based Encryption. In EUROCRYPT 2011. 568–588.".

[13] "OUALHA, Nouha et Janneteau, Christophe, Méthode De Chiffrement Basée Sur Les Attributs Comprenant Une Phase De Pré-Calcul , Brevet Européan "EP3371929B1"".

[14] "Andrew Chi-Chih Yao. [n. d.]. How to Generate and Exchange Secrets. In SFCS 1986. 162–167".

[15] "Marcin Andrychowicz, Stefan Dziembowski, Daniel Malinowski, and Lukasz Mazurek. [n. d.]. Secure Multiparty Computations on Bitcoin. In SP 2014. 443–458.".

[16] "Zhang, Derek & Su, Alex & Xu, Felix & Chen, Jiang. (2018). ARPA Whitepaper".

[17] O. N. a. A. P. Guy Zyskind, "Decentralized Computation Platform with Guaranteed Privacy.," Computer Science., 2015.

[18] "Craig Gentry. [n. d.]. Fully Homomorphic Encryption Using Ideal Lattices. In STOC 2009. 169–178".

[19] "Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. [n. d.]. Fully Homomorphic Encryption over the Integers. In EUROCRYPT 2010. 24–43".

[20] "Yunsen Wang, Alexander Kogan,Designing confidentiality-preserving Blockchain-based transaction processing systems,International Journal of Accounting Information Systems,Volume 30,2018,Pages 1-18,ISSN 1467-0895,".

[21] "S Goldwasser, SMicali, and C Rackoff. [n. d.]. The Knowledge Complexity of Interactive Proof-systems. In STOC 1985. 291–304.".

[22] "Manuel Blum, Paul Feldman, and SilvioMicali. [n. d.]. Non-interactive Zero-knowledge and Its Applications. In STOC 1988. 103–112.".

[23] "Eli Ben Sasson, Alessandro Chiesa, Christina Garman, Matthew Green, Ian Miers, Eran Tromer, and Madars Virza. [n.d.]. Zerocash: Decentralized Anonymous Payments from Bitcoin. In SP 2014. 459–474.".

[24] "Jens Groth. [n. d.]. Short Pairing-Based Non-interactive Zero-Knowledge Arguments. 321–340".

[25] F. G. E. N. S, "Techniques Of Cryptography," CNAM, 2002.

[26] H. L. J. H. X. W. Q. Miao, "An intelligent and privacy-enhanced data sharing strategy for blockchain-empowered Internet of Things," Digital Communications and Networks, no. doi: https://doi.org/10.1016/j.dcan.2021.12.007, 2022.

[27] A. A.-A. H. K. Yehia Ibrahim Alzoubi, "Blockchain technology as a Fog computing security and privacy solution: An overview," Computer Communications, vol. 182, no. https://doi.org/10.1016/j.comcom. 2021.11.005, p. 129–152, 2022.

[28] S. F. M.Bougrine, "Improving Performance of the Symmetrical Evolutionary Ciphering System SEC," InternationalJournal of High Performance Systems Architecture, vol. 10, no. 1, pp. 12-19, 2021.

[29] O. P. V. E. V. S. Menezes A.J., Handbook Of Applied Cryptography, Crc Press, 1997.

[30] U. Kumar, "Understanding Ethereum — Pertinent problems,Scalability, and Possible Solutions.," Coinmonks, 01 06 2018. [Online]. Available: https://medium.com/coinmonks/understanding-ethereum-pertinent-problems-scalability-and-possible-solutions-eb4fec0405be.

[31] S. a. O. F. a. I. A. a. B. M. a. A. M. Trichni, "New intelligent strategy for encryption decisional support system," International Journal of High Performance Systems Architecture, vol. 9, no. 4, pp. 173-181, 2020.

[32] R. P. M. Patel, "Improved Identity Based Encryption System (IIBES): A Mechanism for Eliminating the Key-Escrow Problem," Emerging Science Journal, vol. 5, no. 1, 2021.

[33] F. O. a. M. B. Salima TRICHNI, "New Smart Encryption Approach based on Multidimensional Analysis Tools," New Smart Encryption Approach based on Multidimensional Analysis Tools, vol. 12, no. 5, 2021.