symmetry

MDPI

Communication

Revisited—The Subliminal Channel in Blockchain and Its Application to IoT Security

Tzung-Her Chen [1], Wei-Bin Lee [2], Hsing-Bai Chen [3] and Chien-Lung Wang [4,*]

[1] Department of Computer Science and Information Engineering, National Chiayi University, 300 University Rd., Chiayi 600, Taiwan; thchen@mail.ncyu.edu.tw

[2] Department of Information Engineering and Computer Science, Feng Chia University, No. 100 Wenhwa Road, Seatwen, Taichung 407, Taiwan; wblee@fcu.edu.tw

[3] Hilltop Information Company Limit, 7F.-3, No. 60, Daxin St., Xitun Dist., Taichung 407, Taiwan; hsingbai@gmail.com

[4] Information Security Research Center, National ChungHsing University, 145 Xingda Rd., South Dist., Taichung 402, Taiwan

* Correspondence: kevinwang@nchu.edu.tw; Tel.: +886-4-22840141 (ext. 373)

Abstract: Although digital signature has been a fundamental technology for cryptosystems, it still draws considerable attention from both academia and industry due to the recent raising interest in blockchains. This article revisits the subliminal channel existing digital signature and reviews its abuse risk of the constructor's private key. From a different perspective on the subliminal channel, we find the new concept named *the chamber of secrets in blockchains*. The found concept, whereby the secret is hidden and later recovered by the constructor from the common transactions in a blockchain, highlights a new way to encourage implementing various applications to benefit efficiency and security. Thus, the proposed scheme benefits from the following advantages: (1) avoiding the high maintenance cost of certificate chain of certificate authority, or public key infrastructure, and (2) seamlessly integrating with blockchains using the property of chamber of secrets. In order to easily understand the superiority of this new concept, a remote authentication scenario is taken as a paradigm of IoT to demonstrate that the further advantages are achieved: (1) avoiding high demand for storage space in IoT devices, and (2) avoiding maintaining a sensitive table in IoT server.

Keywords: authentication; blockchain; digital signature; elliptic curve digital signature algorithm; subliminal channel; IoT

check for updates

Citation: Chen, T.-H.; Lee, W.-B.; Chen, H.-B.; Wang, C.-L. Revisited—The Subliminal Channel in Blockchain and Its Application to IoT Security. *Symmetry* **2021**, *13*, 855. https://doi.org/10.3390/sym13050855

Academic Editor: Basil Papadopoulos

Received: 25 March 2021
Accepted: 10 May 2021
Published: 11 May 2021

1. Introduction

Generally, the digital signature technique is used to demonstrate that a signed message is indeed from the legal signer and unaltered by a villain. Due to the capabilities of authentication, integrity, and nonrepudiation, the related digital signature standards are developed and extensively employed in various applications. Furthermore, the Digital Signature Standard, which specifies a Digital Signature Algorithm (DSA), has been put into the United States government standard for authentication of electronic documents [1]. In addition, the encryption technique is an individual process to agree on confidentiality. In order to guarantee the authentication, integrity, nonrepudiation, and confidentiality, two processes—signature and encryption—are involved in common designs.

For more efficiency, the ordinary digital signature process did not possess confidentiality until Simmons introduced the so-called "subliminal channel" to hide a message within an authentication code [2]. Sequentially, Simmons demonstrated the existence of a subliminal channel in the DSA and the ElGamal signature schemes, which allows a message, named subliminal information, to be secretly hidden into a digital signature.

The elliptic curve digital signature algorithm (ECDSA) [3], accepted as ANSI, IEEE, NIST, ISO standards, is the elliptic curve analogue of DSA. It is intuitive that ECDSA also exists in its subliminal channel [4].

In such a way, only the intended receiver will be able to notice its presence and then recover it. If the signer and the receiver are not the same, there is the risk that the receiver can forge a signature sealed with the signer's private key. Thus, the potentially catastrophic impact on treaty verification on the national security of the USA has been disclosed by Simmons many years later [5]. In response to this threat, more complete discussions were garnered in [6], to name a few, which indicates that mutual trust between the signer and the receiver in all subliminal channels is absolutely necessary. This security risk restricts wide uses of subliminal channel in commercial applications.

With the bloom of cryptocurrency, such as Bitcoin [7] since 2009, and Ethereum [8] since 2013, the blockchain technologies, providing a trusted mechanism without centralized and trusty parties, have captured more and more attention in either academia or the IT industry. A blockchain is a growing list of blocks that are continuously linked by a one-way hash technology and secured using a digital signature technology. Each block contains a couple of transactions Tx which consist of a group of data including the messages of account addresses *from* and *to*, etc., and the signatures *r* and *s*. Table 1 illustrates an instance of a transaction Tx in the block number 10941440 in the Ethereum blockchain. Some fields of an Ethereum transaction are described as follows.

- *from*: the sending account address which, also, implies the signer of this transaction.
- *to*: the destination account address.
- *value*: the amount of ether to transfer.
- *input*: an arbitrary message or the code to create a smart contract.
- *nonce*: the count of the number of outgoing transactions.
- *gas*: the maximum amount of gas that can be spent to process the transaction.
- *r* and *s*: the ECDSA signature for this transaction.
- *v*: to make up the ECDSA signature along with r and s.

Table 1. The structure of one transaction in the Ethereum blockchain.

Fields	Value
blockHash	0x9d505654f898ac399265ab19263a005c8cde246e7cbbc7131367d1ab59522600
blockNumber	10941440
transactionIndex	0
from	0xF21B66afa206a3Dd5FD263B30708851d0B8BC418
to	0x8D4192005ed871056F53df7840c3B6D5866e3339
value	0
gas	100000
gasPrice	171600000000
input	0xfa09e630000000000000000000000000f21b66afa206a3dd5fd263b30708851d0b8bc418
nonce	53
hash	0x752c353be538865b4708e39f63c6c85a60f81025a38d08ccd432855dc7cfa492
r	0x807afb686424b39e546847e9fc42449fe8bc2f01a54f2379f1e9250a5ae60bee
s	0x624df310a0972d275d531db2ab9323997ad8056fd679ea334ea268b24a95af57
v	38

It is worth noting that ECDSA is adopted to sign a transaction in both Bitcoin and Ethereum. The signature fields *r* and *s* in each transaction, as shown in Table 1, are proven. Without loss of generality, a transaction is denoted *Tx* = <*from*, ..., *r*, *s*>.

For a user in a blockchain, his private key is regarded as his identity and security credential. Notably, the private key is generated and maintained by the user himself, not a trusted third party, and it is used to sign outgoing transactions.

1.1. Motivation

In traditional asymmetric cryptography, if Alice intends to verify Bob's signature, she must confirm the validation of Bob's public key first by verifying Bob's certificate. That is, Alice needs to verify the corresponding certificate that is issued by another upper issuer called the intermediate certificate authority (CA). This implies that the signatures of the certificates in the certificate chain should be verified up continuously to the root CA certificate. This is the so-called overhead of public key infrastructure (PKI).

1.2. Contribution

Based on these observations, we revisit the subliminal channel from a different perspective that the message sealed in the subliminal channel is later recovered by the signer. This different perspective helps us to discover a new concept, named *the chamber of secrets in blockchains*. Differing from the application which adopts the Simmons's subliminal channel, the signer has no need to leak his/her own private key to anyone, and thus the abuse risk of private keys disappears. Additionally, four charming characteristics are found in this new concept: natural camouflage, confidentiality, integrity, and efficiency. Furthermore, the following advantages are achieved.

(1) *Avoiding the high maintenance cost of CA or PKI.* Generally speaking, a blockchain technology has no mechanism to publish users' public keys, which can be extracted from their related transactions instead. In such a way, the public key extraction operation can reach the goal of the authentication of public keys from transactions directly.

(2) *Seamlessly integrating with blockchains*. The proposed scheme utilizes the ECDSA private/public keys without any modification of blockchains. The chamber appears as a common transaction of blockchains. In this way, the proposed scheme does seamlessly comply with a state-of-the-art blockchain.

This new concept is adopted in the applications in which the secrets must be kept safe and retrieved accurately on demand. Taking the remote authentication as a paradigm of Internet of Things (IoT), this article shows that the paradigm alters the benefits to include both efficiency and security, including (1) *avoiding high demand for storage space in IoT devices*, and (2) *avoiding maintaining a sensitive table in IoT server*.

2. A New Concept: The Chamber of Secrets

Herein, a new observation for the subliminal channel is presented. Let us first consider the following scenario borrowed from Harry Potter [9]:

In this popular novel, the characters believe *the chamber of secrets* to be fictive. However, the chamber is opened when the person who has the power to do so appears, thus proving its existence. The chamber was constructed because a person made preparations concealed from others for finishing his expected work at some other time. The person, called the constructor, built the castle, which contains *the chamber of secrets*, a covert room within the castle to house a scheme executor which would finish the constructor's expected work. *The chamber of secrets* is well-hidden and looked upon by others as a fictive part of the castle. It requires someone to have the clue to open its entrance, and this is a power which only very few have. Furthermore, in the story, the expected work would be accomplished when the constructor opens the chamber and releases the executor.

2.1. Property of the Chamber of Secrets

From this scenario, there are many superior characteristics, described as follows, that fascinate us. First, for hiding a secret well, it must be a good idea that the secret is covered within a common object to attract less attention. As *the chamber of secrets* is wrapped as a common object, the castle is a camouflage to confuse the public. Second, nobody can find the chamber because only the constructor has the clue that can open its entrance. Under this scenario, the abuses and the debates on trust indeed disappear in *the chamber of secrets*. Third, according to this scenario, everyone should possess the ability to detect a falsified legend because the legend is circulated throughout the people. However, there is no way for anyone to assure whether the legend is true to determine the existence of *the chamber of secrets* except the constructor. No doubt the reality of the legend is the key to successfully deal with the chamber. Finally, because the chamber is constructed together with the castle, there is no extra cost for building.

Thus, the expected properties of the chamber can be summarized as follows.

- The chamber appears as a common object to lower the attention of potential attackers.

- The chamber cannot be opened by anyone but the constructor.
- The reality of the legend is the key to successfully discover the chamber of secrets.
- The chamber is constructed together with the common object and therefore no extra cost for the construction of the chamber is required.

2.2. How to Construct the Chamber of Secrets in Blockchain

To demonstrate the concept of *the chamber of secrets in blockchains*, the ECDSA scheme, adopted in the blockchains of Bitcoin and Ethereum, is exploited as an example.

Assume that the elliptic curves E over prime finite field F_p, where p be a prime. An elliptic curve equation $y^2 = x^3 + ax + b\ (mod\ p)$ where $a, b \in F_p$ with $4a^3 + 27b^2 \neq 0\ (mod\ p)$. The points on $E(F_p)$ including a special point O called the point at infinity form a group $G = \{(x, y) : x, y \in F_p\ and\ (x, y)\ \in E(F_p)\}\ \cup\ \{O\}$.

The particular elliptic curve specified in Bitcoin and Ethereum is $secp256k1$ [10]. The $secp256k1$ refers to the parameters of the elliptic curve used in Bitcoin's and Ethereum's asymmetric cryptography. The elliptic curve domain parameters over F_p are specified by:

- $p = 2^{256} - 2^{32} - 2^9 - 2^8 - 2^7 - 2^6 - 2^4 - 1$ where finite field modulus (p) was close to 2^{256} and there are still a lot of primes between p and 2^{256}.
- $a = 0$.
- $b = 7$.
- The base point (P) is recommended as $P =$ 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0E1108A8 FD17B448 A6855419 9C47D08F FB10D4B8.
- The order n of P is n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141.

The chamber constructor selects a private key $d \in\ [1, n-1]$, and computes a public key $Q = d * P$. The chamber of secrets scheme consists of three phases: the cryptographic key generation phase, the construction phase, and the unsealing phase.

Phase 1: The cryptographic key generation

A chamber constructor creates a cryptographic key CK as a secret and houses it in the chamber. The cryptographic key is generated as follows.

- Prepare a chamber $k \in\ [1, n-1]$.
- Generate a cryptographic key

$$CK = h(L||\ k) \tag{1}$$

where $h(.)$ denotes a one-way hash function, such as $SHA-256$ [11] in Bitcoin or $SHA-3$ [12] in Ethereum, and "||" represents a concatenation.

Here, L is treated as the legendary fable possibly known by everybody where L denotes all the transaction fields given in Table 1 except for the fields about digital signature. The cryptographic key CK is the secret housed in the chamber, and only the constructor can release the secret by following the clue dropped by the legend L.

Phase 2: The construction

To attract less attention, it must be a good idea that *the chamber of secrets* is wrapped as a common transaction in blockchains. This phase is used to seal the chamber in an ordinary digital signature on the legend L. *The chamber of secrets* is constructed as follows.

- Compute r by using the chamber k as

$$R = k * P =\ (x_1, y_1) \tag{2}$$

$$r = x_1\ mod\ n \tag{3}$$

$$s = k^{-1} *\ (h(L) + d * r)\ mod\ n \tag{4}$$

- Solve s from the equation

In this phase, the appearance of the signature (r, s) provides a well-camouflaged service for k and the integrity of the legend L can be verified through the constructor's public key as follows.

- Compute $w = s^{-1} \ \ mod\ n$, $u_1 = h(L) * w \ \ mod\ n$, and $u_2 = r * w \ \ mod\ n$.
- Compute $X = u_1 * P + u_2 * Q$ and choose $x - coordinate$ of X as v. If

$$v = r \ \ mod\ n \tag{5}$$

holds, the signature is valid.

Phase 3: The unsealing

Whenever the secret housed in the chamber is demanded, the common signature (r, s) for a transaction and the legend L are required by the chamber constructor. Only the constructor with the knowledge of the private key d can uncover the chamber as follows.

- Open the chamber with the knowledge of d as

$$k = s^{-1} * \ (h(L) - d * r) \ \ mod\ n \tag{6}$$

- Discover the secret cryptographic key

$$CK = h(L||\, k) \tag{7}$$

Since the integrity of the legend L is confirmed in Equation (4), this implies that the reconstructed cryptographic key CK is genuine. The cryptographic key housed into the chamber is further used to accomplish the expected work of the constructor.

3. Discussion

In this section, the characteristics of *the chamber of secrets in blockchains* are examined. The characteristics of the chamber of secrets can be examined to derive the corresponding security as follows. Prior to demonstrating the security of the proposed scheme, some definitions are given below.

Definition 1. (one-way hash function). *A one-way hash function is defined as the hash function, the output value is defined as $h(x)$, where x is a variable-length value, and the output $h(x)$ is the fixed-length value. A secure one-way hash function $y = h(x)$, where given x to compute y, is easy, but given y to deduce x is hard.*

Definition 2. (ECDLP). *Elliptic curve discrete logarithm problem (ECDLP): If $a \in F_p^*$ is unknown, compute a by giving P, and $a * P$.*

Theorem 1. *Confidentiality: The chamber cannot be opened by anyone but the constructor.*

Proof. The chamber k s protected within the digital signature constructed in Equations (2)–(4). If someone intends to retrieve k from Equations (2) and (3), a well-known elliptic curve discrete logarithm problem computationally infeasible to be solved [3] will occur by Definition 2. When someone attempts to recover k from Equation (4), there is no feasible way because of two unknown secrets, k and d, by Definition 2, which are involved in one equation. Only the signer who possesses the knowledge of d has the power to discover k and further retrieves the secret cryptographic key $CK = h(L||\, k)$. Hence, the confidentiality of the chamber is assured. It also implies that the confidentiality of the content encrypted with the cryptographic key is guaranteed when the underlying cryptosystem is proved to be secure enough. □

Theorem 2. *Integrity: The reality of the legend is the key to successfully discover the chamber of secrets.*

Proof. For the signature, it is impossible to forge a legend fable L to pass the signature verification. That is, once the integrity of L is guaranteed by verifying its digital signature, it also implies that the chamber k embedded in the signature is genuine. The correctness of L and k implies that the fidelity of the cryptographic key $CK = h(L|| \, k)$ is also assured. □

Theorem 3. *Known-key security: The proposed scheme does provide the service of known-key security.*

Proof. The cryptographic key generated in the proposed scheme is independent and should not be exposed if other cryptographic keys are compromised. Notedly, if a chamber sealed in an ordinary digital signature on the legend L is not only used one time, the cryptographic key may be further defined as $CK = h(L|| \, k||id)$ instead, where the parameter id indicates some session. Assume the cryptographic key CK is compromised for some reason. To deduce k from CK is infeasible by **Definition 1**. Hence, if one cryptographic key is disclosed, it is still hard to know the cryptographic key with different id in another session. □

Next, the two characteristics are highlighted as follows.

Proposition 1. *Natural camouflage: The chamber appears as a common transaction to lower the attention of potential attackers.*

Proof. The chamber appears as an ordinarily digital signature (r,s) for the legendary fable L. The chamber is indeed constructed during the generation of a digital signature so that others have no idea where/whether it exists. In other words, the digital signature in a blockchain plays the role of logical camouflage to confuse the public. It also reduces the attention of the malicious attackers. This implies that the chamber may store without using any particular protection mechanisms but blockchains. □

Proposition 2. *Efficiency: The chamber is constructed together with the common transaction and therefore no extra cost is required.*

Proof. It is obvious that k is an already-existing step within the construction process of an ordinary signature (r,s) for a transaction in blockchains such as Equations (2), (3), and (4). Hence, no extra cost is necessary for the constructor to construct and maintain the chamber. □

According to these analyses, the chamber of secrets indeed exists in current blockchain mechanisms such as well-known Bitcoin and Ethereum and, therefore, has no cost at all. Additionally, as the characteristics of the chamber of secrets in blockchains satisfies the expectation investigated above, they will definitely benefit the applications adopted this new concept.

4. Performance of Implementing an Ordinary Signature

Next, the implementation cost for the signature generation is also discussed. According to Proposition 2, discussing the cost of constructing the chamber is necessary because the construction is indeed a necessary step while generating the signature. Therefore, the focus is shifting to the cost of the signature generation.

Accordingly, Equations (3) and (4) used for the signature construction, and Equation (6) used to unseal the chamber, are all ECDSA-based operations. Among three state-of-the-art algorithms including RSA, DSA, and ECDSA, it is well-known that the ECDSA achieves not only the same level of security with a smaller key size, but it also achieves higher computational efficiency than those of the RSA and DSA. For example, 256-bit ECDSA with the standard elliptic curve defined in $secp256k1$ provides comparable security to 3072-bit RSA [13]. Thus, the proposed scheme also provides the same level of security as that in either Bitcoin or Ethereum.

5. The Application of the Chamber of Secrets to IoT

IoT has been a topic of much interest in academia and industry and, in the last decade, security of the IoT systems has become a field of immense research activities. There are a couple of published surveys on IoT security issues focusing on authentication, confidentiality, and so on [14,15]. Mutual identity authentication between IoT servers and IoT devices plays an important role in secure IoT systems.

In this section, a remote authentication scenario between IoT server and IoT devices is illustrated to show the superiority of the new discovery. To remotely authenticate a client, i.e., IoT device, is a very important issue in such an information-networked world. Accordingly, there are many research results that can be found [16,17]. No matter what method is concerned, the underlying idea is very similar, where a client IoT device must register at the IoT server to have a secret-shared token and the token can later be used to generate the challenge–response to verify whether or not the communication partners are genuine.

In such a scenario, the secret token no doubt is very critical. How to protect the token is the major issue in the remote authentication scenario. From the lifetime of the token, these issues can be categorized as follows.

- The token generation: A secure token should be generated to perform a challenge–response mechanism.
- The token prevention: The generated token must be protected to assure the confidentiality and the integrity.
- The token recovery: The token must be retrieved to perform a challenge–response mechanism.
- The token renewing: The token should be updated periodically to assure the higher security.

In the following, the scheme based on the chamber of the secrets is illustrated.

5.1. Registration Phase

The phases 1 (cryptographic key generation) and 2 (construction) demonstrated in the abovementioned section can be used for the registration because the IoT device will have a secret token CK and the corresponding signature (r, s) for L from the IoT server, where L denotes a public statement about what access rights the remote IoT device is authorized by the IoT server. Precisely, the IoT sever generates and broadcasts the transaction where the "$from$" field is the IoT server's identity, and the "to" field is the registered IoT device's identity. Thus, the secret token CK can be deduced by the IoT server later.

5.2. Authentication Phase

Whenever login to the IoT server occurs, the IoT device sends the authorization $\{L, (r, s)\}$, i.e., the transaction issued by the IoT server in the registration phase, back to the IoT server or indicates where the transaction is on the blockchain. The IoT server can recover the token CK by processing the abovementioned Phase 3 (unsealing). Once the secure token is obtained, a challenge–response mechanism is able to be used to authenticate each other. Notedly, since the transaction $\{L, (r, s)\}$ is well-protected by blockchain techniques, the IoT sever needs not verify the validation of the transaction.

This scheme demonstrates a scenario based on the concept of the chamber of secrets, and the issues of this scenario are answered by the characteristics of the concept as follows.

- The token generation: A secure token is generated with very light overhead, a hash function computation, for the underlying signature scheme, according to Proposition 2.
- The token prevention: According to Theorem 1 and 2, the token CK is secure against any disclosure and any malicious modification. Therefore, the generated token is protected under the guarantee of the confidentiality and the integrity.
- The token recovery: According to Theorem 1, only the server has the ability to retrieve the token to verify whether the client is genuine.

- The token renewing: According to Proposition 1, the token is sealed in the signature to be a camouflage object. To update the token, re-signing the authorized agreement L by the server is performed, and the corresponding secure token will be updated easily.

During the lifetime of the secure token, it is confirmed that the concept of the chamber of secrets provides a very efficient way to implement the challenge–response mechanism in the IoT remote authentication scenario. Additionally, it is worth mentioning that all merits are gained in only one single equation of the ordinary signature equation, rather than a complex combination of the cryptographic primitives.

Upon introducing *the chamber of secrets in blockchains* into IoT remote authentication systems, the following benefits are further highlighted.

(1) *Avoiding high demand for storage space in IoT devices*. Whenever logging in the IoT server, the IoT device sends the authorization $\{L, (r, s)\}$ back to the IoT server by indicating the transaction on the blockchain instead of storing $\{L, (r, s)\}$ locally.
(2) *Avoiding maintaining a sensitive table in IoT server*. Generally speaking, if the IoT server privately maintains the sensitive table that stores the shared secret between the IoT server and the specific IoT device, it will be an attractive target resulting in potential server compromise. By the design of chamber of secrets, the proposed scheme needs no sensitive table stored in the IoT server.
(3) *Benefiting integrity of secure token from seamlessly integrating blockchains*. The presented model not only satisfies the common criteria analysis but also highlights some seldom-mentioned merits, including the integrity of the secure token.

6. Conclusions

This article has revisited the subliminal channel in a digital signature and has discovered and presented the new concept *the chamber of secrets in blockchains* from a different perspective. Under this concept, four charming characteristics are found: natural camouflage, confidentiality, integrity, and efficiency. We have shown a remote authentication scenario in IoT systems with a challenge–response mechanism to understand and believe the superiority of the proposed concept, as well as a new way of encouraging implementing various applications to benefit efficiency and security.

Author Contributions: Conceptualization, W.-B.L. and T.-H.C.; methodology, T.-H.C. and C.-L.W.; validation, H.-B.C.; formal analysis, C.-L.W.; data curation, H.-B.C.; writing—original draft preparation, H.-B.C.; writing—review and editing, T.-H.C.; funding acquisition, C.-L.W. and T.-H.C. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported in part by the Ministry of Science and Technology of Taiwan under grant MOST 107-2221-E-415-001-MY3.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. NIST, FIPS 186-2. Digital Signature Standard. October 2001. Available online: http://csrc.nist.gov/publiscations/fips/fips186-2/fips186-2-change1.pdf (accessed on 11 May 2021).
2. Simmons, G.J. The Prisoners' Problem and the Subliminal Channel. Available online: https://link.springer.com/chapter/10.1007/978-1-4684-4730-9_5 (accessed on 11 May 2021).
3. Johnson, D.; Menezes, A.; Vanstone, S. The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* **2001**, *1*, 36–63. [CrossRef]
4. Hu, J. The improved elliptic curve digital signature algorithm. In Proceedings of the 2011 IEEE International Conference on Electronic & Mechanical Engineering and Information Technology, Harbin, China, 12–14 August 2011; Volume 1, pp. 257–259.

5. Simmons, G.J. The history of subliminal channels. In Proceedings of the First International Workshop on Information Hiding, Cambridge, UK, 30 May–1 June 1996; LNCS 1174. Springer: Berlin/Heidelberg, 1996; pp. 237–256.
6. Desmedt, Y. Simmons' protocol is not free of subliminal channels. In Proceedings of the 9th IEEE Computer Security Foundations Workshop, Kenmare, Ireland, 10–12 June 1996; pp. 170–175.
7. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: https://bitcoin.org/bitcoin.pdf (accessed on 11 May 2021).
8. Buterin, V. Ethereum White Paper. 2013. Available online: https://ethereum.org/en/whitepaper/ (accessed on 11 May 2021).
9. Rowling, J.K. *Harry Potter and the Chamber of Secrets*; Bloomsbury: London, UK, 1998.
10. Qu, M. *Sec 2: Recommended Elliptic Curve Domain Parameters*; Tech. Rep. SEC2-Ver-0.6; Certicom Research: Mississauga, ON, Canada, 1999.
11. NIST, FIPS PUBS 180-2. Secure Hash Standard. August 2002. Available online: http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf (accessed on 11 May 2021).
12. NIST, FIPS 202. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. August 2015. Available online: https://www.nist.gov/publications/sha-3-standard-permutation-based-hash-and-extendable-output-functions?pub_id=919061 (accessed on 11 May 2021).
13. Fernández-Caramès, T.M.; Fraga-Lamas, P. Towards Post-Quantum Blockchain: A review on Blockchain Cryptography Resistant to Quantum Computing Attacks. *IEEE Access* **2020**, *8*, 21091–21116. [CrossRef]
14. Santacà, K.; Cristani, M.; Rocchetto, M.; Viganò, L. A topological categorization of agents for the definition of attack states in multi-agent systems. In Proceedings of the Multi-Agent Systems and Agreement Technologies, Valencia, Spain, 15–16 December 2016; Springer: Cham, Switzerland; pp. 261–276.
15. Yang, Y.; Wu, L.; Yin, G.; Li, L.; Zhao, H. A survey on security and privacy issues in Internet-of-Things. *IEEE Int. Things J.* **2017**, *4*, 1250–1258. [CrossRef]
16. Almuhaideb, A.M.; Alqudaihi, K. A Lightweight Three-Factor Authentication Scheme for WHSN Architecture. *Sensors* **2020**, *20*, 6860. [CrossRef] [PubMed]
17. Xu, Z.; Li, F.; Deng, H.; Tan, M.; Zhang, J.; Xu, J. A Blockchain-Based Authentication and Dynamic Group Key Agreement Protocol. *Sensors* **2020**, *20*, 4835. [CrossRef] [PubMed]