Hindawi
Security and Communication Networks
Volume 2021, Article ID 6693726, 6 pages
https://doi.org/10.1155/2021/6693726

Research Article

Fail-Stop Group Signature Scheme

Jonathan Jen-Rong Chen,[1] Yi-Yuan Chiang,[2] Wang-Hsin Hsu,[3] and Wen-Yen Lin[3]

[1]*Department of Information Management, Vanung University, Taoyuan 302, Taiwan*
[2]*Department of Computer Science and Information Engineering, Vanung University, Taoyuan 302, Taiwan*
[3]*Department of Information Management, National Taichung University of Science and Technology, Taichung 404, Taiwan*

Correspondence should be addressed to Wen-Yen Lin; qqnice@nutc.edu.tw

Received 17 December 2020; Revised 25 January 2021; Accepted 29 January 2021; Published 9 February 2021

Academic Editor: Xiaokang Zhou

In this study, a fail-stop group signature scheme (FSGSS) that combines the features of group and fail-stop signatures to enhance the security level of the original group signature is proposed. Assuming that FSGSS encounters an attack by a hacker armed with a supercomputer, this scheme can prove that the digital signature is forged. Based on the aforementioned objectives, this study proposes three lemmas and proves that they are indeed feasible. First, how does a recipient of a digitally signed document verify the authenticity of the signature? Second, when a digitally signed document is under dispute, how can the group's manager determine the identity of the original group member who signed the document, if necessary, for an investigation? Third, how can one prove that the signature is indeed forged following an external attack from a supercomputer? Following an attack, the signature could be proved to be forged without exposing the key. In addition, the ultimate goal of the group fail-stop signature scheme is to stop using the same key immediately after the discovery of a forgery attack; this would prevent the attack from being repeated.

1. Introduction

Electronic documents are being increasingly used instead of paper to conduct official government and private business. Among other advantages, this benefits the environment by reducing the amount of paper being used. However, the use of electronic documents also increases the importance of using digital signatures to guarantee the validity, authenticity, and integrity of electronic documents and reduce the risk of documents being forged.

To cope with the wide range of potential uses for digital signature technology, the concept of group signing was proposed. A real-life example is considered to illustrate the process of using a group fail-stop signature scheme. The chief of Taiwan's Environmental Protection Administration, along with 19 other staff members of the agency, is eligible to digitally sign documents; these staff members include those accusing a subordinate unit of breaking the law. To safeguard the agency members' neutrality and protect them from interference, each staffer is required to activate a digital signature key when they release a statement or document representing the administration. The recipient of the document would be able to verify the authenticity of the digital signature. However, in the event that someone impeaches the integrity or validity of a digitally signed document, the identity of the individual who originally signed the document would remain a secret.

Companies or other entities cited for violations by the Environmental Protection Administration could file a complaint with the agency to deny that they had violated the law. As part of the review process, it might be necessary to determine the identity of the official who signed the original document making the accusation. Under the present scheme, only the manager in the group would have the ability to identify the person who signed the document. The manager, however, cannot pretend to be a member of another group to forge the digital signature.

Chaum and Van Heyst [1] concluded that there are three properties of group signatures. (i) Only members of the group can sign messages. (ii) The recipient can verify that it

is a valid group signature but cannot discover the group member who signed the message. (iii) If necessary, the signature can be "opened," to reveal the person who signed the message.

The group signature scheme also has some favorable features that make it applicable in a range of fields. A digital signature can ensure the validity and authenticity of electronic documents. If the possibility of a document being forged could be reduced, or even if it were possible to prove that the digital signature was forged, the security level of the digital signature could then be enhanced. Another type of fail-stop signature scheme (FSS) can satisfy the aforementioned requirements.

Kitajima et al. [2] showed that an FSS has to have at least two security properties. (i) A scheme based on information-theoretic security has to be secure, even against a computationally unbounded adversary. (ii) If the computational assumption is broken, an honest signer should be able to prove that a signature is a forgery by virtue of information-theoretic security.

In this work, a fail-stop group signature scheme (FSGSS) is proposed. FSGSS combines all the functions and features of two schemes: group signature (GS) and FSS. This algorithm integrates the features of the two types of digital signatures, which strengthens its security level under the GS system. The combination scheme ensures that the group members can prove that a digital signature is indeed a forgery after supercomputer forgery attacks.

The remainder of this paper is organized as follows: Section 2 describes studies related to the present work. Section 3 presents our scheme, and Section 4 provides an analysis of the scheme and a discussion thereof. Finally, Section 5 concludes the paper and provides directions for future research.

2. Related Work

Desmedt proposed a group-oriented cryptosystem concept in 1987. In his dissertation [3], he noted that, in addition to entities that exist as individuals, there are entities comprising groups of several individuals, such as hospitals, schools, public institutions, and private companies. When these entities issue signed electronic documents, such as certificates, the concept of a digital signature becomes a mechanism to replace signatures on paper documents. Digital signatures could be placed on electronic diplomas, electronic medical records, and other official documents released by governmental agencies. The documents that carry digital signatures must have the following features: certainty of identity, nonrepudiation, and unforgeability.

Therefore, the design of the way keys are exchanged, the parameters of the exchanges become particularly important. Although each member in a group has a secret key, the group password must be reused. In other words, individuals in the group cannot exchange their keys during an operation. Instead, they exchange secondary keys derived from their main keys. This ensures the security of the main keys. In addition, members cannot export the group's master key. This ensures that this key remains secure. Chen and Yuanchi [4] developed a new and fast anonymous digital signature system by linking the LUC function with the complexities of discrete logarithms and factorization.

Conversely, multiple studies have focused on the security of conventional digital signature schemes that rely on a computational assumption. FSSS provide security for a sender against a forger with unlimited computational power by enabling the sender to provide a proof of forgery if it occurs. FSSs have been proposed in [5–10]. Chain [11] proposed that a fail-stop scheme could assert a victim's innocence, without exposing the $n = p \times q$ secret, and would guard against malicious behavior. More recently, Kitajima et al. [2] proposed a framework for FSS operating in a multisigner setting and called for a primitive fail-stop multisignature scheme. In other words, they combined threshold and fail-stop signatures. After the first aggregate signature scheme was proposed, several researchers attempted to propose more efficient versions of FSS by combining various schemes.

Recently, blockchain technology was used to realize the calculation and verification of the original GS algorithm. The calculation of the group certificate and signature recognition should be completed by the corresponding smart contract. This reduces the possibility of a joint attack. The newly added signature node no longer needs the approval of the center and only requires the approval of the majority node, realizing the true decentralization of signatures [12]. However, the decentralized GS scheme, based on blockchain, requires more calculation and is more expensive to implement smart contracts and applications without a decentralized network. Conversely, the blockchain-based smart contract is visible to all blockchain users. This leads to a situation where bugs, including security holes, are visible to all, yet may not be quickly fixed [13–15]. In particular, issues in Ethereum smart contracts include ambiguities and easy-but-insecure constructs in its contract language solidity, compiler bugs, Ethereum virtual machine bugs, attacks on the blockchain network, and the immutability of bugs; moreover, there is no central source documenting known vulnerabilities, attacks, and problematic constructs [14].

3. Proposed Scheme

3.1. Initialization. The system center (SC) chooses a primitive element g over the Galois field p_0, satisfying the following equation:

$$p_0 = 4p_1q_1 + 1, \tag{1}$$

where p_1, q_1 are large primitive. Let

$$n = p_1q_1. \tag{2}$$

Then, SC chooses a number $g_2 \in Z_n^*$, satisfying

$$g_2^{p_1} \equiv 1 \left(\mathrm{mod} p_0\right), \tag{3}$$

where $\{g_2, p_0, n\}$ and $\{p_1, q_1\}$ are the public key and secret key of the SC, respectively. The details of the initialization process are shown in 0 (Figure 1).

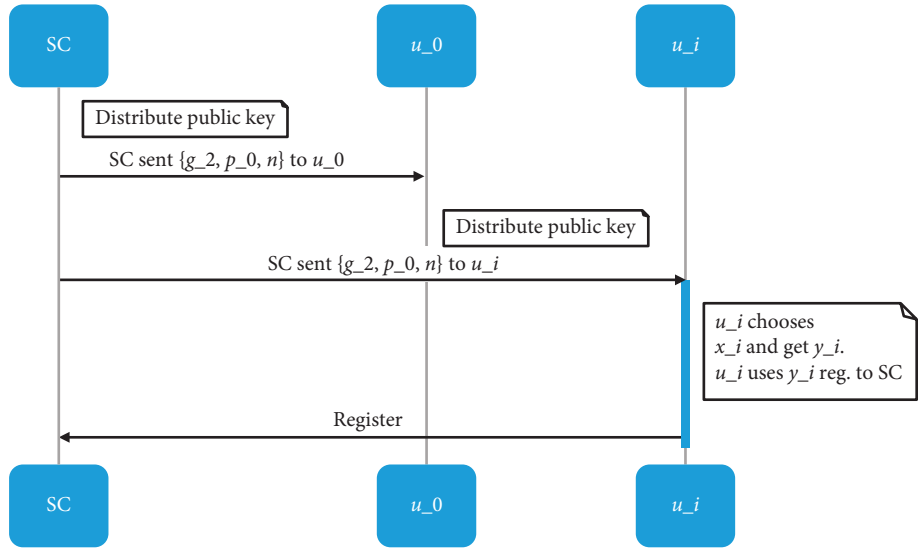

Figure 1: Initialization of GFSS.

3.2. Group and Its Members. Without loss of generality, we assume a group and its members $u_i, 0 \le i \le l$, where u_0 is the manager of a group. The member registers to SC individually as follows:

u_i chooses a number x_i and calculates

$$g_2^{x_i} \equiv y_i \pmod{p_0}, \tag{4}$$

u_i uses the y_i to register.

3.3. Parameters Exchange. Example 1: $u_i, 0 \le i \le l$, requests a part of the parameter from u_0; and then, u_0 chooses a number k and calculates

$$g_2^k \equiv r_1 \pmod{p_0}, \tag{5}$$

$$u_0 \longrightarrow u_i\colon r_1. \tag{6}$$

This means that u_0 sends r_1 to u_i. u_i chooses a number b' and calculates

$$g_2^{b'} \equiv b \pmod{p_0}, \tag{7}$$

$$r_1^b \equiv r_3 \pmod{p_0}, \tag{8}$$

$$r_2 \equiv \frac{r_3}{b} \pmod{n}, \tag{9}$$

$$u_i \longrightarrow u_o\colon r_2, \tag{10}$$

u_0 chooses a number a, satisfying the following equation:

$$a \equiv x_0 r_2 + ks \pmod{n}, \tag{11}$$

$$u_0 \longrightarrow u_i\colon a, s. \tag{12}$$

After the aforementioned procedure is performed, if manager u_0 knows the parameters, k, a, x_0, and r_2, then s is known. It is to be noted that y_0, r_1 is the public key of u_0, where $g_2^{x_0} \equiv y_0 \pmod{p_0}$, based on equation (4). The detailed process of GFSS is shown in 0 (three-way handshake for exchange parameters) (Figure 2).

3.4. Signing Message m. Multiplying both sides of equation (11) with b, we obtain

$$ba \equiv x_0 (br_2) + (kb)s \pmod{n}. \tag{13}$$

Multiplying both sides of equation (9) with b, we obtain

$$r_3 \equiv br_2 \pmod{n}. \tag{14}$$

Using equations (13) and (14), we obtain

$$ba \equiv x_0 r_3 + (kb)s \pmod{n}. \tag{15}$$

Then, we choose two numbers c, e and calculate

$$g_2^c \equiv r_5 \pmod{p_0}, \tag{16}$$

$$g_2^e \equiv E \pmod{p_0}. \tag{17}$$

Let

$$r_4 \equiv r_3 r_5 \pmod{p_0}, \tag{18}$$

and

$$s_1 \equiv r_5 s \pmod{n}. \tag{19}$$

Adding cs on both sides of equation (15), we acquire

$$ba + cs \equiv x_0 r_3 + (kb)s + cs \equiv x_0 r_3 + (kb + c)s \pmod{n}. \tag{20}$$

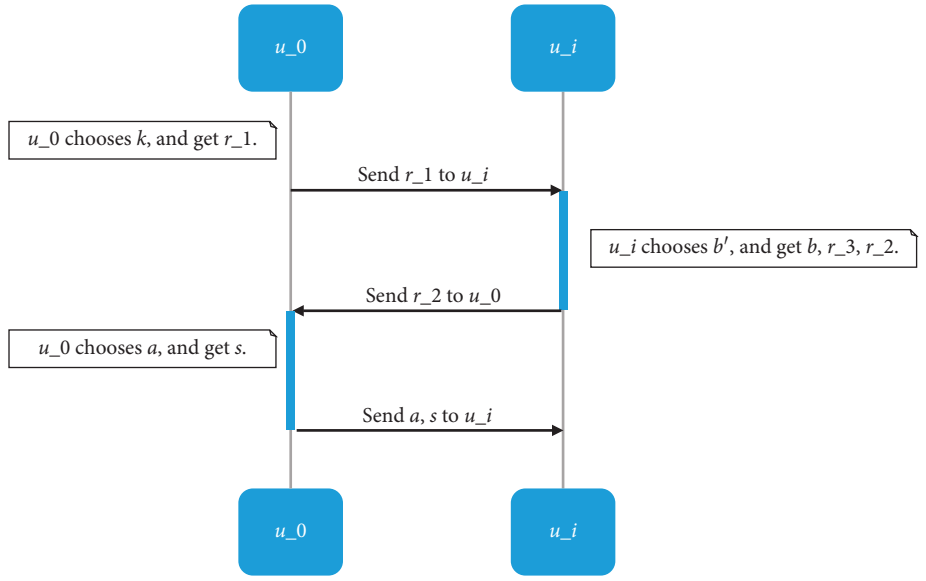

Figure 2: Three-way handshake for parameter exchange.

Using r_5 from equations (18) and (19) to multiply both sides of equation (20), we obtain

$$\begin{aligned}(ba+cs)r_5 &\equiv x_0\left(\frac{r_4}{r_5}\right)r_5+(kb+c)\left(\frac{s_1}{r_5}\right)r_5\\ &\equiv x_0r_4+(kb+c)s_1\,(\mathrm{mod}n).\end{aligned}\tag{21}$$

Let

$$r_6=(ba+cs)r_5\,(\mathrm{mod}n),\tag{22}$$

and

$$m+r_6=cE+es_2\,(\mathrm{mod}n).\tag{23}$$

Assuming that the recipient of the message is R, u_i sends messages to R. It is to be noted that

$$u_i\longrightarrow R\colon\{m,c,E,r_4,r_6,s_1,s_2\},\tag{24}$$

where R is used in the equations as follows:

$$g_2^{r_6}\equiv y_0^{r_4}r_4^{s_1}\,(\mathrm{mod}n),\tag{25}$$

$$g_2^{m+r_6}=g_2^{cE}E^{s_2}\,(\mathrm{mod}p_0).\tag{26}$$

The receiver accepts this digital signature if both equations (25) and (26) are valid. Otherwise, this digital signature is denied (Table 1).

4. Analysis and Discussion

In this section, we first introduce Lemma 1 to check the validity of a digital signature. Lemma 2 verifies whether a digital signature is activated by a group member. Lemma 3 shows that the attack method, mentioned by Susilo [7], will not succeed. There are several parameters after these procedures. We created a list of members holding parameters, as shown in 0. In this scheme, the members share partial parameters and maintain a few parameter(s). For example, manager u_0 holds only parameter k; member u_i only holds parameter b. In this case, someone creates a digital signature of u_0 and passes the verification; however, she/he is unaware of parameter b. That is, this person is a forger.

Lemma 1. *If u_0 and u_i are trusted authorities, then both equations (24) and (25) are valid.*

Proof. Using equation (22), we have

$$g_2^{r_6}\equiv g_2^{(ba+cs)r_5}\equiv g_2^{x_0r_4+(kb+c)s_1}\equiv g_2^{x_0r_4}g_2^{(kb+c)s_1}\,(\mathrm{mod}n).\tag{27}$$

There are two parts of the last term of the aforementioned equations; considering the first part and using equation (4), we have

$$g_2^{x_0r_4}\equiv\left(g_2^{x_0}\right)^{r_4}\equiv y_0^{r_4}\,(\mathrm{mod}n).\tag{28}$$

Considering the second part,

$$\begin{aligned}g_2^{(kb+c)s_1}&\equiv g_2^{(kb)s_1}g_2^{cs_1}\equiv\left(\left(g_2^k\right)^b\right)^{s_1}g_2^{cs_1}\equiv\left(\left(r_1\right)^b\right)^{s_1}g_2^{cs_1}\ \text{via equation (5)}\\ &\equiv r_1^{bs_1}\left(g_2^c\right)^{s_1}\equiv r_1^{bs_1}r_5^{s_1}\ \text{via equation (17)}\\ &\equiv r_3^{s_1}r_5^{s_1}\equiv\left(r_3r_5\right)^{s_1}\ \text{via equation (8)}\\ &\equiv r_4^{s_1}\,(\mathrm{mod}n)\ \text{via equation (18).}\end{aligned}\tag{29}$$

By combining equations (28) and (29), we obtain

$$g_2^{r_6}\equiv y_0^{r_4}r_4^{s_1}\,(\mathrm{mod}n).\tag{30}$$

Hence,

$$g_2^{m+r_6}=g_2^{cE}E^{s_2}\,(\mathrm{mod}p_0).\tag{31}$$

Therefore, both equations (25) and (26) are valid.

Table 1: List of members holding parameters.

	SC	u_o	u_i	R		SC	u_o	u_i	R
g_2	v	v	v	v	s		v	v	
p_o	v	v	v	v	m			v	v
n	v	v	v	v	c			v	v
y_i	v	v	v		E			v	v
r_1		v	v		r_4			v	v
b'			v		r_6			v	v
b			v		s_1			v	v
r_2		v	v		s_2			v	v
a		v	v						

Certain parameters are required to check whether message m has been sent by u_i. Hence, we obtain the following lemma: □

Lemma 2. *If u_0 and u_i are trusted authorities, then it implies that message m was sent from u_i by equation (8).*

Proof. The following should be noted:

(a) $r_1^b \equiv r_3 \pmod{p_0}$ from equation (8)
(b) $u_i \longrightarrow R$: $\{m, c, E, r_4, r_6, s_1, s_2\}$ from equation (24)
(c) $u_0 \longrightarrow u_i$: a, s from equation (12)
(d) $r_4 \equiv r_3 r_5 \pmod{p_0}$ from equation (18)
(e) $ba \equiv x_0 r_3 + (kb)s \pmod{n}$ from equation (15)
(f) $g_2^k \equiv r_1 \pmod{p_0}$ from equation (5)
(g) $g_2^{r_6} \equiv y_0^{r_4} r_4^{s_1} \pmod{n}$ from equation (25)
(h) $g_2^{m+r_6} = g_2^{cE} E^{s_2} \pmod{p_0}$ from equation (26)

Considering equation (19), $s_1 \equiv r_5 s \pmod{n}$, s_1 and s can be determined because of equations (12) and (24). Hence, we can obtain r_5 and r_3 via equations (18) and (24). Finally, b must be calculated (only u_i knows this parameter) because u_0 is unaware of b.

Considering equation (15), a, x_0, r_3, k, and s are known. It is not easy for anyone to obtain b; only the manager of group u_0 knows this value. In fact, it is a discrete logarithm problem when someone knows r_1, r_3 only by equation (8).

We conclude that u_0 can obtain b because u_0 already knows parts of parameters from u_i and has their own parameter k. Therefore, after checking equations (25) and (26), we can say that the message is sent by u_i. □

Lemma 3. *An attacker intercepting the message passed by the digital signature to adapt the method of Susilo et al. will not succeed.*

Proof. The following is to be noted:

(a) $u_i \longrightarrow R$: $\{m, c, E, r_4, r_6, s_1, s_2\}$ from equation (24)
(b) $g_2^{r_6} \equiv y_0^{r_4} r_4^{s_1} \pmod{n}$ from equation (25)
(c) $g_2^{m+r_6} = g_2^{cE} E^{s_2} \pmod{p_0}$ from equation (26)

If an attacker A intercepts the message as shown in equation (24) because A is unaware of parameters x_0, r_4, we assume that

$$g_2^{x_0'} \equiv y_0 \pmod{p_0}, \quad g_2^{r_4'} \equiv r_4 \pmod{p_0}. \tag{32}$$

Attacker A can easily forge m^* for suitable parameters $\{c', E', s_2'\}$ such that both equations (25) and (26) are valid. In other words, the digital signature passes the test of Lemma 2. After the procedure of Lemma 2 is performed, a nontrivial factor of n can be found by computing $GC\ D(b, b^*, n)$. We note that the probability of b being equal to b^* is $(1/q_0)$. Therefore, it is proved that m^* is not sent by the group members. □

5. Conclusions and Future Work

In this study, we propose a novel FSGSS. This algorithm integrates the features of two types of digital signature, which strengthens its security level under the GS system. The proposed FSGSS ensures that the group members can prove that a digital signature is indeed a forgery after supercomputer forgery attacks. In addition to discussing the integration of these two digital signatures, this dissertation highlights three proposed Lemmas and proves that they are feasible. Lemma 1 verifies an FSGSS digital signature. Lemma 2 is used by the group manager, when needed, to determine the identity of the group member who originally created the digital signature. Finally, this dissertation proposes Lemma 3. When the digital signature is found to be forged, members of the group can prove this fact.

The ultimate goal of the group fail-stop signature scheme is to stop using the same key immediately after the discovery of a forgery attack; this would prevent the attack from being repeated. That is, the "key" considered in this study is parameter b used by u_i. If the parameters need to be changed each time an entity is under attack, the process of replacing the parameters is equivalent to reexecuting the exchange parameter program. Therefore, in future work, we plan to design a scheme wherein we need not directly expose key b; we can then prove that a certain number of

signatures are forged, which will enhance the efficiency of GFSS.

Data Availability

No data were used to support the findings of this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

Wang-Hsin Hsu passed away in March 15, 2020. We would like to express our gratitude to him for his contribution to this paper. We will always miss you and continue your unfinished wishes. Hope you rest in peace. This research is partially supported by the "Higher Education Sprout Project," Ministry of Education, Taiwan.

References

[1] D. Chaum and E. Van Heyst, "Group signatures," in *Workshop On the Theory And Application Of Cryptographic Techniques*, Springer, Berlin, Germany, 1991.

[2] N. Kitajima, N. Yanai, T. Nishide, G. Hanaoka, and E. Okamoto, "Constructions of fail-stop signatures for multi-signer setting," in *Proceedings of the 2015 10th Asia Joint Conference On Information Security*, IEEE, Kaohsiung City, Taiwan, May 2015.

[3] Y. Desmedt, "Society and group oriented cryptography: a new concept," in *Proceedings of the Conference On the Theory And Application Of Cryptographic Techniques*, Springer, Amsterdam, The Netherlands, April 1987.

[4] J. J.-R. Chen and L. Yuanchi, "A traceable group signature scheme," *Mathematical Computer Modelling*, vol. 31, no. 2-3, pp. 147–160, 2000.

[5] T. P. Pedersen and B. Pfitzmann, "Fail-stop signatures," *SIAM Journal on Computing*, vol. 26, no. 2, pp. 291–330, 1997.

[6] K. Schmidt-Samoa, "Factorization-based fail-stop signatures revisited," in *Proceedings of the International Conference On Information And Communications Security*, Springer, Malaga, Spain, October 2004.

[7] W. Susilo, "A new and efficient fail-stop signature scheme," *The Computer Journal*, vol. 43, no. 5, pp. 430–437, 2000.

[8] E. Van Heyst and T. P. Pedersen, "How to make efficient fail-stop signatures," in *Workshop On the Theory and Application of Cryptographic Techniques*, Springer, Berlin, Germany, 1992.

[9] X. Zhou, W. Liang, S. Shimizu, J. Ma, and Q. Jin, "Siamese neural network based few-shot learning for anomaly detection in industrial cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 1, 2021.

[10] X. Zhou, Y. Hu, W. Liang, J. Ma, and Q. Jin, "Variational LSTM enhanced anomaly detection for industrial big data," *IEEE Transactions on Industrial Informatics*, vol. 1, 2020.

[11] K. Chain, "An improved fail-stop signature scheme based on dual complexities," *International Journal of Innovative Computing, Information and Control*, vol. 10, no. 2, pp. 535–544, 2014.

[12] Y. Cao, "Decentralized group signature scheme based on blockchain," in *Proceedings of the 2019 International Conference On Communications, Information System And Computer Engineering (CISCE)*, Haikou, China, July 2019.

[13] M. E. Peck, "Ethereum's $150-million blockchain-powered fund opens just as researchers call for a halt," 2016, https://spectrum.ieee.org/tech-talk/computing/networks/ethereums-150-million-dollar-dao-opens-for-business-just-as-researchers-call-for-a-moratorium.

[14] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *Proceedings of the International Conference on Principles of Security and Trust*, Springer, Uppsala, Sweden, April 2017.

[15] X. Zhou, W. Liang, K. I.-K. Wang, H. Wang, L. T. Yang, and Q. Jin, "Deep-Learning-Enhanced human activity recognition for internet of healthcare things," *IEEE Internet of Things Journal*, vol. 7, no. 7, pp. 6429–6438, 2020.