4. Точність та якість	+	+	+ / -	+	+
5. Відкритість, передача та впровадження	+	-	-	+	+
6. Особиста участь	+	+	+	+	+
7. Відповідальність	+	+	+	+	+
8. Гарантії безпеки	+	+	+	+	+
9. Моніторинг, оцінка та звітність	+ / -	-	+	+	+
10. Попередження шкоди	-	+	-	+	-
11. Треті особи	-	-	+	+	+
12. Управління порушеннями	-	-	-	+	+
13. Безпека та конфіденційність	-	-	-	+	+
14. Вільний потік інформації та законні обмеження	-	-	-	+	+
15. Застосування до країн ЄС	+	+	+	+	-

Виходячи із проведеного дослідження та порівняння міжнародних стандартів, що описують правильність та законність опрацювання ПД в інформаційному просторі, визначено, що не всі стандарти відповідають вимогам ISACA, але всі вони можуть допомогти компаніям точно і якісно визначити, які саме ПД дані компанії потрібно захищати та визначити найкритичніші точки в інформаційному просторі.

Регламент GDPR повністю відповідає принципам конфіденційності ISACA, що відповідає повноцінній захищеності ПД громадян. Тому компаніям, що працюють на ринку України необхідно перевірити власну відповідність нормам Регламенту, де, під час аудиту буде отримано висновок, що допоможе чітко та якісно оцінити захищеність ПД, та допомогти побудувати захищену інфраструктуру для опрацювання ПД громадян України.

Multisignature with double threshold condition in the blockchain

УДК621.395.7
(043.2)

Ruslan Skuratovskii[1], Anastasia Arnautova[2]

National Aviation University, ORCID: 0000-0002-5692-6123.

[1]ruslan.skuratovskii@nau.edu.ua, [2]anastasia.arnautova.bit@stud.nau.edu.ua

Abstract

Improving the reliability of account protection in the blockchain is one of the most important goals of the entire cryptographic arsenal used in the blockchain and cryptocurrency exchange.

We propose a new threshold multisignature scheme with a double boundary condition.

Access to funds stored on a multisig wallet is possible only when two or more signatures are provided at the same time.

A simple analogy is a safe deposit box or safe with two locks and two keys. Maria holds one key, Juan holds the other. They can open the cell only if they present both keys at the same time. Individually, they cannot open a cell without the approval of the other [1].

Thus, multisig wallets provide an additional layer of security. With this technology, users can avoid the problems often encountered with single-key wallets, single point of failure, and vulnerable to attacks from cybercriminals who are constantly developing new phishing techniques.

Since multisig wallets require more than one signature to move funds, they are also suitable for businesses and corporations looking to store funds in shared wallets.

Definition. Multisignature is a technology for signing transactions with multiple private keys to increase security and privacy during the approval process for sending transactions.

A multisignature is a kind of threshold signature, implemented as a check of conditions specified in the basic scripting language of the cryptocurrency. Multisignature technology has become widespread in the world of cryptocurrencies [2].

Definition. A token is a digital certificate that guarantees the company's obligations to its owner, an analogue of shares on the stock exchange in the world of cryptocurrencies [3].

Definition. Threshold signature is a variant of an electronic signature, for the imposition of which the cooperation of at least t members of a group of n participants is required, denoted as. . In essence, it is a special case of the threshold division of a secret according to the scheme (t, n), when the private key is split into n parts, and any t parts are enough to recover it. The public key is used in the usual way. Generation, sharing of a key and distribution of its fragments requires a group manager (dealer).

Note that such a group can be, in particular, a manning pool consisting of n members.

Let's denote – the number of tokens in the wallet of the -th account belonging to a subset of the accounts from the blockchain. Note that one participant can have several accounts, therefore, we consider double indexing where – denotes a wallet in the blockchain network and – this is the owner of the wallet. More generally, cryptocurrency can be used instead of tokens. It is convenient to express the value of a token in cryptocurrency as in monetary terms.

We introduce a double threshold signature condition according to the scheme (t, n), where different t participants from satisfying the inequality where that is, participant really belongs to the group from persons. The this is the boundary number of tokens (or their value in the specified crypto currency) that persons must have in order to be eligible for multisignature.

Access to funds stored on a multisig wallet is possible only when two or more signatures are provided at the same time. At its core, a user's account can be identified with his wallet. But one person can have several accounts (for example, this happens during a CB-attack). Therefore, if person j proves that she has in the aggregate at least the threshold amount necessary to satisfy the inequality of the threshold amount for multisignature, then the sums of tokens or currency equivalents on all her wallets are summed up and included in the total amount of the group. To install accounts on a node, each of the participants can use the BIP 39 algorithm. Even on one node, one person can have several accounts. Therefore, we will summarize each wallet -th the participant indexing it by its index and then we summarize the amounts available to different participants in the external amount by . Then we construct multisignature with sheme, where number of wallets of participant denoted by and is sum of taken in -th wallet of -th participant of blochain

The method of proving that -th a person has a certain amount in the wallet can be a simple contract, where the money is transferred back to the same -th user. Thus,the -th participant shows in the contract that he has this amount explicitly, but then transfers it back to himself (possibly by paying for the transaction). In most cases, for example, in the Effirium currency, the amount in the wallet is visible inside the blockchain. In addition, such an amount can be counted as the sum of incoming money from records inside blockchain transactions and the amount of outgoing spending from this wallet visible in blockchain transactions. Thus, in any case, the total amount of tokens or currency of the -th participant can be calculated without cost.

We will divide the entire blockchain into domains, each of which has its own digital signature. Only those domain entities whose wallets have the number of tokens in excess of a percentage of the critical number of tokens of the entire blockchain domain have the right to sign. The persons who has the authority to sign in the -th domain will be denoted by. If a domain member does not have a number of tokens that exceed the percentage of critical tokens of the entire domain i, it can apply for the right to sign to the authorized person of his domain S. It should be noted that S can be located at the intersection of domains, then the process of transferring the key is simplified due to the fact that an authorized person acts as a surety of two parties at once.

References:

1. Funds stored on a multisig wallet is possible only when two or more signatures are provided at the same time. [Electronic resource] / According to the general edition «Multisignature»

Access mode: https://www.okex.com/academy/ru/%D0%BC%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%BF%D0%BE%D0%B4%D0%BF%D0%B8%D1%81%D1%8C

2. Multisignature is a technology for signing transactions with multiple private keys to increase security and privacy during the approval process for sending transactions. [Electronic resource] / According to the general edition «What is multisignature? What is a ring signature?»

Access mode: https://forklog.com/chto-takoe-multipodpis/

3. A token is a digital certificate that guarantees the company's obligations to its owner, an analogue of shares on the stock exchange in the world of cryptocurrencies. [Electronic resource] / According to the general edition Karpova K.

Access mode: https://secretmag.ru/enciklopediya/chto-takoe-token-obyasnyaem-prostymi-slovami.htm

Напрямки підвищення ефективності та якості підготовки кадрів для сфери захисту інформаційної безпеки

УДК 331.5.024.

Мельник Сергій

Кандидат економічних наук, доцент, заслужений економіст України, завідувач сектору професійної освіти відділу освітньої статистики і аналітики ДНУ «Інститут освітньої аналітики», член Національного агентства кваліфікацій, к.е.н., доц., Заслужений економіст України, Київ, Україна

s.melnik@iea.gov.ua

Ключовим питанням якісної та ефективної підготовки кадрів для будь-якої країни виступає система їх оцінювання. Багато країн це питання уже давно та успішно вирішили. Напрямків реалізації оцінювальної діяльності безліч, це й Інформаційна мережа занять США (Occupational Information Network (O'net)[1] та американська мережа центрів з видання ліцензій на професійну діяльність [2], національні бази інформаційних матеріалів з оцінювання, мережі центрів з незалежного оцінювання та присвоєння професійних кваліфікацій у більшості країн ЄС, у Великій Британії та Канаді, в основу яких покладено ключові положення Міжнародної стандартної класифікації занять 2008 року (ISCO-08)

[1] Інформаційна мережа занять США.- URL: https://www.onetonline.org/

[2] Національна база даних з професійного ліцензування.- URL: https://www.ncsl.org/research/labor-and-employment/occupational-licensing-statute-database.aspx