UDK 004.89

Nazarov A.[1], Kozel N.[2], Gruzdo I.[3], Kyrychenko I.[4]

[1] Candidate of Technical Sciences, Professor of Software Engineering Department, Kharkov National University of Radio Electronics, oleksii.nazarov1@nure.ua, ORCID iD: 0000-0001-8682-5000

[2] Senior Lecturer at the Department of Software Engineering, Kharkiv National University of Radio Electronics, natalia.kozel1@nure.ua, ORCID iD: 0000-0001-9276-9877

[3] Candidate of Technical Sciences, Associate Professor of Software Engineering, Kharkov National University of Radio Electronics, irina.gruzdo@nure.ua, ORCID iD: 0000-0002-4399-2367

[4] Candidate of Technical Sciences, Assistant of the Department of Software Engineering, Kharkov National University of Radio Electronics, iryna.kyrychenko@nure.ua, ORCID iD: 0000-0002-7686-6439

SECURITY IN DECENTRALIZED DATABASES

Blockchain is a distributed network that records digital transactions on a publicly accessible ledger. This paper explores whether blockchain technology is a suitable platform for the preservation of digital signatures and public/private key pairs. Conventional infrastructures use digital certificates, issued by certification authorities, to declare the authentication of key pairs and digital signatures. This paper suggests that the blockchain's hash functions offer a better strategy for signature preservation than digital certificates. Compared to digital certificates, hashing provides better privacy and security. It is a form of authentication that does not require trust in a third-party authority, and the distributed nature of the blockchain network removes the problem of a single point of failure.

DIGITAL SIGNATURES, BLOCKCHAIN, KEYS, ENCRYPTION, AUTHENTICITY, TRUST.

Introduction

Digital signature (ES) is a special requisite of the document, which allows you to establish the absence of distortion of information in an electronic document since the formation of the ES and confirm that the ES belongs to the owner. The value of the props is obtained as a result of cryptographic transformation of information.

Digital signature allows you to:

- Confirm the authorship of the message sender
- Ensure that no one can forge a message sent and confirmed via an ES

So, with a private key, we sign "letters of transfer of ownership" (transactions), and thus, for example, give our coins to someone else. With the public key (certificate) we verify the authenticity of the transactions of others.

Hashing — transformation of an input array of arbitrary length into a (output) bit string of fixed length. The function that implements the algorithm and performs the conversion is called the "hash function" or "convolution function". The source data is called the input array, "key" or "message". The result of the conversion (output) is called "hash", "hash code", "hash sum", "message summary".

A cryptographic hash function is any hash function that is crypto-resistant, that is, satisfies a number of requirements specific to cryptographic applications.

The fundamental part of Bitcoin are cryptographic algorithms. In particular, the ECDSA algorithm is an Elliptic Curve Digital Signature Algorithm that uses elliptic curves and finite fields to sign data so that a third party can confirm the authenticity of the signature by eliminating the possibility of falsification. ECDSA uses different procedures for signing and verification, consisting of several arithmetic operations[1].

1. Elliptic curves

One form of elliptic curves is Weierstrass curves.

$$y^2 = x^2 + ax + b.$$

For coefficients $a = 0$ and $b = 7$ (used in Bitcoin), the graph of the function takes the following form(Fig.1):

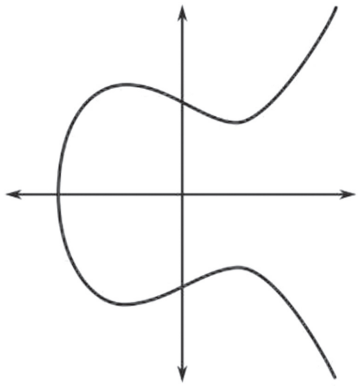

Fig. 1. Elliptic curve

Elliptic curves have several interesting properties, for example, a non-vertical line intersecting two non-tangent points on a curve will cross a third point on the curve. The sum of two points on the $P + Q$ curve is called the R point, which is a reflection of the $-R$ point (constructed by continuing the straight line (P; Q) to the intersection with the curve) relative to the X axis (Fig. 2) [2].

If we draw a straight line through two points having coordinates of the form $P(a, b)$ and $Q(a, -b)$, then it will be parallel to the ordinate axis. In this case there will be no third intersection point. To solve this problem,

a so-called point at infinity (point of infinity) is introduced, denoted as O. Therefore, if there is no intersection, the equation takes the following form $P + Q = O$.

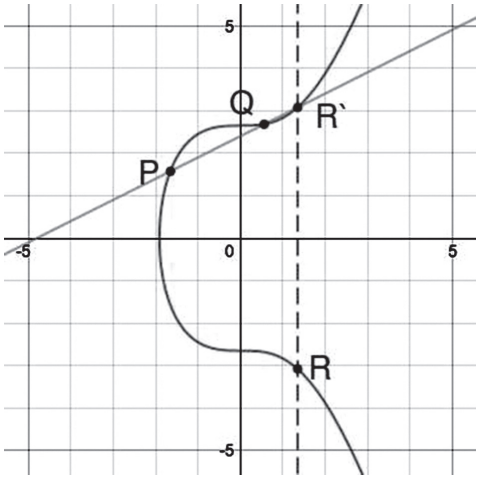

Fig. 2. The sum of two points on the curve

If we want to add the point to itself (double it), then in this case the tangent to the point Q is simply drawn. The resulting intersection point is reflected symmetrically with respect to the X axis (Fig. 3).

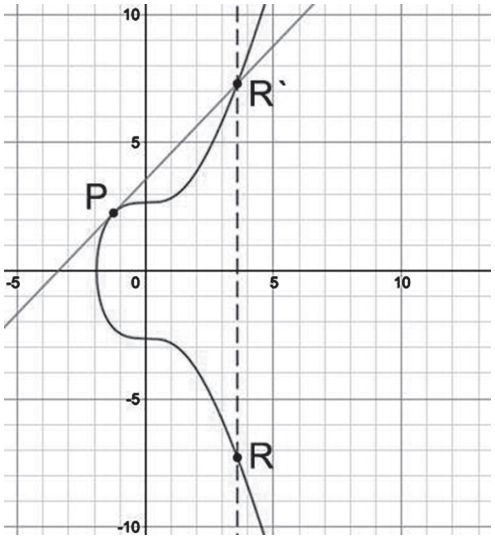

Fig. 3. Double point

These operations allow scalar multiplication of the point $R = k * P$, adding the point P with itself k times. However, note that faster methods are used to work with large numbers [3].

2. Elliptic curve over a finite field

In elliptical cryptography (ECC), the same curve is used, only considered over some finite field. The final field in the context of the ECC can be represented as a predefined set of positive numbers, which should be the result of each calculation.

$$y^2 = x^3 + ax + b \pmod{p}$$

For example, 9 mod 7 = 2. Here we have a finite field from 0 to 6, and all operations modulo 7, no matter how many times they are carried out, will give a result that falls in this range.

All the properties mentioned above (addition, multiplication, point at infinity) for such a function remain in force, although the graph of this curve will not resemble an elliptic curve. The bitcoin elliptic curve, $y^2 = x^3 + 7$, defined on the finite field modulo 67, looks like this (Fig. 4):

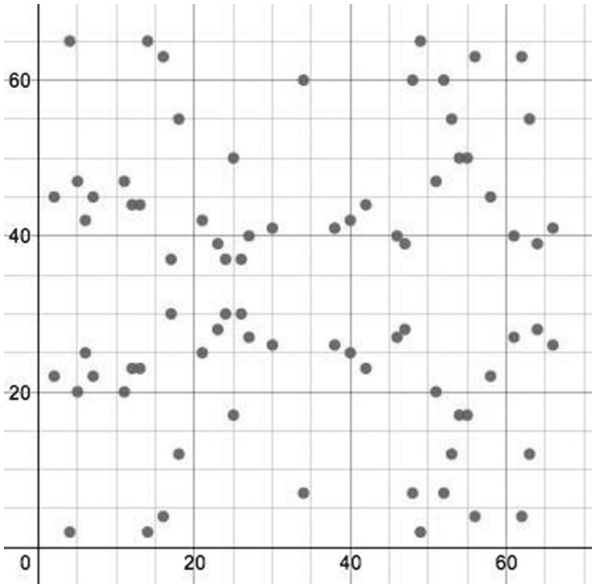

Fig. 4 . Bitcoin elliptic curve defined on a finite field module 67

This is a set of points where all values of x and y are integers between 0 and 66. Straight lines drawn on this graph will now "wrap" around the field as soon as they reach barrier 67 and continue from the other end of it. while maintaining the same slope, but with a shift. For example, the addition of points (2, 22) and (6, 25) in this particular case looks like this (Fig. 5) [4]:

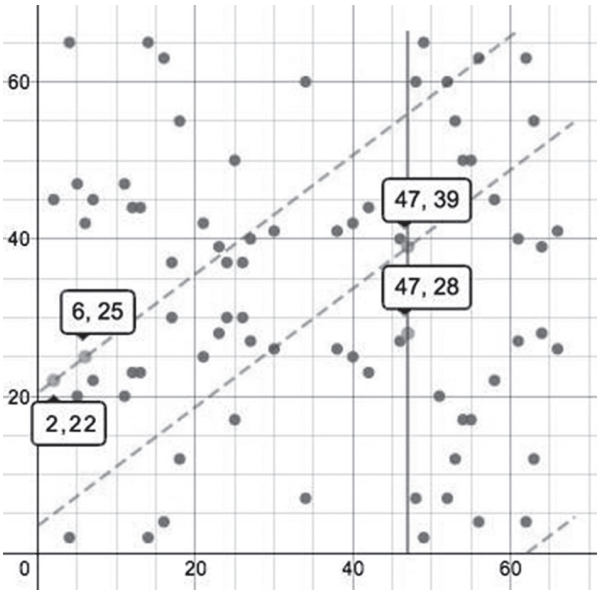

Fig. 5. Addition of points (2, 22) and (6, 25)

3. Bitcoin ECDSA

The Bitcoin protocol contains a set of parameters for an elliptic curve and its finite field, so that each user

uses a well-defined set of equations. Among the fixed parameters, the equation of the curve (equation), the value of the field modulus (prime modulo), the base point on the curve (base point) and the order of the base point (order) are distinguished. About calculating the order of the base point you can read here. This parameter is chosen specifically and is a very large prime number.

In the case of bitcoin, the following values are used:

The equation of an elliptic curve: $y^2 = x^3 + 7$

Simple module: 2256 – 232 – 29 – 28 – 27 – 26 – 24 – 1 = = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE FFFFFC2F

Base point:

04 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798 483ADA77 26A3C465 5DA4FBFC 0-1108A8 FD17B448 A6855419 9C47D08F FB10D4B8

The bold font is the x coordinate in hexadecimal notation. It is immediately followed by the Y coordinate.

Order: FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

This set of parameters for an elliptic curve is known as secp256k1 and is part of the SEC (Standards for Efficient Cryptography) family of standards proposed for use in cryptography. In Bitcoin, the secp256k1 curve is used in conjunction with the ECDSA (elliptic curve digital signature algorithm). In ECDSA, a secret key is a random number between one and an order value. The public key is generated based on the secret: the latter is multiplied by the value of the base point. The equation has the following form:

$$\text{Public key} = \text{private key} * G$$

This shows that the maximum number of secret keys (consequently, Bitcoin addresses) is, of course, equal to the order. However, the order is an incredibly large number, so accidentally or intentionally pick up the secret key of another user is unrealistic.

The public key is calculated using the same doubling and adding points operations. This is a trivial task that an ordinary personal computer or smartphone solves in milliseconds. But the inverse problem (obtaining a secret key publicly) is a problem of discrete logarithmization, which is considered computationally complicated (although there is no strict proof of this fact). The best known algorithms for its solution, like Pollard's ro, have exponential complexity. For secp256k1, in order to solve a problem, you need about 2128 operations, which will require a computation time on a regular computer, comparable to the lifetime of the Universe[5].

When a private / public key pair is obtained, it can be used to sign data. This data can be of any length. Usually, the first step is to hash the data in order to obtain a unique value with the number of bits equal to the bit order of the curve (256). After hashing, the z-signature algorithm is as follows. Here, G is the base point, n is the order, and d is the secret key.

- Some integer k is selected from 1 to n-1
- Calculate the point $(x, y) = k * G$ using scalar multiplication
- Is $r = x \bmod n$. If $r = 0$, then return to step 1
- There is $s = (z + r * d) / k \bmod n$. If $s = 0$, then return to step 1
- The resulting pair (r, s) is our signature.

After receiving the data and signing it, a third party, knowing the public key, can verify it. The steps to verify the signature are (Q — public key):

- Check that both r and s are in the range from 1 to n-1
- Calculated $w = s - 1 \bmod n$
- Calculated $u = z * w \bmod n$
- Calculated $v = r * w \bmod n$
- Calculate the point $(x, y) = uG + vQ$
- If $r = x \bmod n$, then the signature is true, otherwise it is invalid.

Indeed,

$$uG + vQ = u + vdG = (u + vd)G = (zs - 1 + rds - 1)G = (z + rd)\, s - 1\, G = kG$$

The last equality uses the definition of s at the stage of creating a signature.

ECDSA security is related to the complexity of the secret key search task described above. In addition, the security of the original scheme depends on the "randomness" of choosing k when creating a signature. If the same k value is used more than once, then the secret key can be extracted from the signatures, which is what happened with the Therefore, modern implementations of ECDSA, including those used in most bitcoin wallets, generate k determinedly based on the secret key and the message being signed[6].

4. Other security features

In addition, there are also other elements that protect the blockchain.

More than two users confirm and ensure the security of the transaction. Even in most modern processing systems, only a few levels of verification are involved in verification — as a rule, it is the seller, the buyer, and some third parties (most often a bank or a credit agency).

However, there are from several hundred to several thousand different nodes in the blockchain system, each of which contains a complete copy of the registry of records. Therefore, any of these nodes can also participate in the verification of the transaction, and if the node for some reason does not accept the transaction, it will be canceled. Such an alignment almost to a minimum reduces the possibility of creating a false or fraudulent transaction[7].

The cryptographic keys used by the system in exchange processes are also a miracle of modern cybersecurity. Each encrypted key is a long, complex sequence of data that is practically undecipherable. And if you consider that for confirmation, two such unique keys are required, the system begins to look almost like an impregnable fortress. At the same time, the blockchain is considered to have a unique security system, because with such a level of protection it is possible to retain almost complete transparency of transactions.

5. The most vulnerable places

But, as already mentioned, even the blockchain is not perfect. He, like any other system, has weak spots. So, if you plan to use cryptocurrency and invest your funds in it, or if you have to deal with the blockchain in the future, then you just need to know and understand the potential vulnerabilities of the technology. Therefore, try to remember the following features related to the safety of this technology:

System complexity

If you decide to create a system based on blockchain technology from scratch, then one small mistake can be fatal and "put" all your development. Of course, this cannot be considered a disadvantage of the blockchain itself — rather, it concerns the features of its use. In addition, the average person is much more difficult to understand the blockchain because of its complexity, which, in turn, means that many do not fully understand the risks associated with the use of the system, and do not fully use the available functionality.

Network size

The work of the blockchain requires at least several hundred, or even better, several thousand nodes that work in concert. It is because of this that the system is extremely vulnerable to attacks in the initial stages of work. For example, if a user can gain control over 51% of the system nodes, he will be able to fully control the result of work. And if there are only 20 nodes in the system, then such a scenario is more than possible.

Network speed and efficiency

The blockchain structure is also one of the reasons why the normal functioning of the system can be disrupted. So, if the system becomes too widespread, and the blockchain's infrastructure is not ready for this volume of transactions, as a result, the speed of transactions may decrease, data storage problems may occur, and this will not affect the network efficiency in the best way [8].

Usage policy

Although it cannot be said that this item is directly related to the security of the blockchain, but the policy of the system may affect its application and further development. Considering that the currency in the blockchain system is international and decentralized, this, in essence, devalues the national currency controlled by the state. And, of course, at the moment the governing bodies of some states are seeking to impose more stringent restrictions on the use of the blockchain. Governments of different countries hope to bring the system under control before it becomes a serious competitor and threatens their economy. Indirectly, this is also a significant security threat to the blockchain, which can significantly slow down the spread of technology.

Third Party Systems

For example, NiceHash — a third-party market for Bitcoin mining — was recently cracked, as a result of which cryptocurrencies worth more than $ 60 million were stolen. As it turned out, this platform was unsafe. That is, it is not a security bug of the blockchain system itself. Rather, on the contrary, cybercriminals gained access to the NiceHash system using the blockchain.

For transactions in the blockchain system, public and private cryptographic keys are used.

By themselves, such keys are almost impossible to crack, but a cybercriminal can get them in a simpler and more familiar way. For example, keys can be obtained if you store them on an unsafe or weakly secured platform. So, if someone hacks your mailbox, he will be able to get access to all your letters, and therefore to the keys of your profile in the blockchain. In this case, the attacker will be able to seize your funds, posing as you. And this is one of the main issues concerning the security of the system.

Traditional fraudulent tricks

Users of the system can also fall for other, more traditional tricks scam. In fact, such fraudulent schemes are not considered a weak point in the blockchain security system. So, for example, you can receive an e-mail in which a stranger to you will convince you that it was you who became the lucky one who won something significant. Alternatively, fraudsters may offer you to spend your cryptocurrency on some product or service that you will never receive.

6. The main risks and threats to information security of technology blockchain

At the moment, the main threat to the blockchain, relatively hypothetical, is the "51% attack", when an attacker can roll back transactions by printing alternative blocks on a side chain (branch) and is guaranteed to refute what happens in the main chain of the blockchain. In fact, it looks like a shuttle run. However, taking into account the resource-intensiveness of the hash function solution and the emission of new bitcoins, so far this option seems unlikely. The collusion of the owners of the largest mining pools also looks unconvincing (if you do

not take into account the statistics of the largest producers of bitcoins). But there were already similar examples: one of the pools — ghash.io — gained power close to 50%, after which the owners stopped accepting new users in order not to create a compromising situation.

Consider a scenario where an attacker tries to generate an alternative chain faster than honest nodes. Even if it succeeds, he will not be able to make any changes in the system, for example, to create coins from the air or take coins that no one has transferred to him. Nodes will not accept an incorrect transaction as a payment, and honest nodes will never accept a block with an incorrect transaction. The attacker can only change one of his own transactions by returning to himself the payment he recently made. The race between the honest chain and the attacker's chain can be described in terms of a binomial random walk. A successful event is an increase in the honest chain by one block with an approach to the goal by +1, an unsuccessful event is an increase by one block in the attacker's chain with a decrease in the gap by –1. The possibilities of an attacker in a race under restrictions are similar to the description of the Gambler's Ruin problem (the ruin of a gambler). And so, a gambler with unlimited credit starts the game under conditions of restriction and can potentially hold an unlimited number of games to try to achieve break-even. We can calculate the likelihood of them achieving a break-even point or the same thing that an attacker will overtake honest chain builders [9].

Let: p – the likelihood that an honest host will find the next block; q – the likelihood that the attacker will find the next block; qz – the likelihood that an attacker will win the race if he falls behind by z blocks.

Then:

$$q_z = \begin{cases} 1 & \text{if } p \le q \\ (q/p)^z & \text{if } p > q \end{cases}$$

Suppose that $p>q$, then the probability decreases exponentially with an increase in the number of blocks that the attacker is behind. Thus, if he fails to get ahead at the very beginning, then his chances of winning in the future will become vanishingly small. Consider now how long the payee must wait to be sure that the sender will not be able to change the transaction. Suppose the sender is an attacker who wants the recipient to believe that the payment has been made, but after a while to return the payment to himself. The recipient will be notified when this happens, but the sender hopes that it will be too late. The recipient generates a new key pair and gives the public key to the sender shortly after signing it. This does not allow the sender to prepare a block chain in advance working on it ahead of time to complete the transaction at the moment. Only when a transaction is sent, can a dishonest sender begin to work in secret on a parallel chain containing an alternative version of this transaction. The recipient waits until the transaction is added to the block and the Z blocks are added after that. He does not know at what stage of construction the attacker is, but assuming that honest blocks were built with the same average time per block, the expected value of the attacker's gain can be found through the Poisson distribution[10]:

$$\lambda = z\frac{q}{p}$$

To get the probability with which the attacker can still come forward, multiply the Poisson distribution of each value of the attacker's progress by the probability that he will come forward from this point:

$$\sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \cdot \begin{cases} (q/p)^{(z-k)} & \text{if } k \le z \\ 1 & \text{if } k > z \end{cases}$$

Or after regrouping:

$$1 - \sum_{k=0}^{z} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - (q/p)^{(z-k)}\right)$$

By analyzing the resulting expression numerically, one can easily verify that the probability decreases exponentially with increasing z.

Threat 2. Control Package

Different products of the blockchain technology use different methods of block confirmation. For example, in Bitcoin, the proof-of-work method is used — block confirmation by computing power. Another option for closing blocks is proof-of-stake, when blocks are printed not with computing power, but with the help of money held by people in their hands. In this case, in order to conduct a "51% attack", you must have 51% of the coins wrapped around the system. As in the case of the "shuttle run", if the attacker owns more than 51% of the coins, he will also be able to create an alternative chain, which will become the main one. This situation is reminiscent of a vote at a shareholders meeting, when one of the owners has a controlling stake in his hands, blocking the votes of other holders[11].

Threat 3. Key to all doors

If the security of the blockchain causes a minimum of concern, then the safety of Bitcoins, on the contrary, raises many questions, because, like ordinary paper money, cryptocurrency can also be stolen. The key of the blockchain entry is a hash function of the public key. Uncertain or negligent storage of a private key can lead to theft or loss of bitcoins. According to the Harvard Business Review, the cost of lost bitcoins is already about $ 950 million. The easiest way to protect yourself is to create a wallet password. But if a hacker kidnaps both your wallet and your password, it will be almost impossible to recover the stolen Bitcoins, since the transactions represented with the stolen keys seem to be checking nodes indistinguishable from legitimate

transactions. Some skeptics claim that hackers will be able to crack the key using services that calculate passwords by hash. However, given the current computing power, this seems unlikely. But if suddenly an algorithm appears that allows for the effective factorization of elliptic curves, then there will be a possibility that it will be easy to find private keys to the wallet addresses from which the money was spent.

Threat 4. Exchange attacks

The reliability of cryptocurrency exchanges raises no less questions. In August 2016, 119,756 bitcoins (about $ 65 million) were stolen from the Hong Kong Stock Exchange Bitfinex, one of the four largest cryptocurrency trading sites in the world. Bitfinex has a reputation as one of the most reliable and secure organizations: most user funds were stored in multi-signature wallets and in "cold stores". Despite this, the attackers managed to bypass Bitgo protection, including two-factor authentication and a multi-signature mechanism, and to commit mass theft from individual users' wallets. The details of the hacking were never conveyed to the general public, but the media replied that the Bitfinex employees might be involved in hacking, which again raises the question of the human factor.

Conclusions

Can we now, having considered all these points, say with confidence that the blockchain is a secure and safe system?

Rather, it is worth concluding that the system will function properly if used correctly and accurately. It is also worth bearing in mind that its security depends on the presence of a sufficient number of users, and many security gaps appear trite due to the human factor. Therefore, we should not forget that any system has weak spots, and the blockchain is not an exception to this rule[12].

References

[1] http://www.blockchain4innovation.it/wpcontent/uploads/sites/4/2017/05/Blockchain-

[2] https://www.coindesk.com/information/who-created-ethereum

[3] https://www.coindesk.com/information/how-ethereum-works

[4] A Survey of blockchain security issue and challenges(Iuon-Chang Lin1,2 and Tzu-Chun Liao2)[jan-12- 2017]

[5] Public standares and patients controll:how to keep electronic medical records accessible but private(Kenneth D Mandl, Peter Szolovits, Issac S Kohane)[3 february 2001]]

[6] https://blockgeeks.com/guides/smart-contracts/

[7] *A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman,* Medrec: Using blockchain for medical data access and permission management, in 2016 2nd International Conference on Open and Big Data (OBD), Aug 2016, pp. 2530.

[8] *G. Zyskind, O. Nathan, and A. Pentland.* Decentralizing privacy:Using blockchain to protect personal data, in Security and Privacy Workshops (SPW), 2015 IEEE, May 2015

[9] https://www.researchgate.net/publication/319058582 Blockchain Challenges and Opportunities A Survey

[10] http://www.meti.go.jp/english/press/2016/pdf/053101f.pdf

[11] https://www.dotmagazine.online/issues/innovation-in-digital-commerce/what-can-blockchain-do/securityand-privacy-in-blockchain-environments

[12] https://www.business2community.com/tech-gadgets/issues-blockchain-security-02003488

The article was delivered to your editory stuff on the 20.05.2019