Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (1-5), Month: May - August 2023, Available at: www.noveltyjournals.com

The blockchain as a cryptographic system

Professor KABEYA TSHISEBA Cedric

National Pedagogic University(DRC)

DOI: https://doi.org/10.5281/zenodo.7886035

Published Date: 02-May-2023

Abstract: **This article on the presentation of the Blockchain as a cryptographic concept, started from the observation that the majority of articles, discussions, forums that talk about it, always tend to present it simply as an algorithmic concept at the base of the operation of most current cryptocurrencies, that is not wrong. Except that, after having been in contact with this matter, we found that the Blockchain deserves a much better presentation beyond a simple algorithm, either as a cryptosystem in its own right, at the base of the security of several systems of 'information. We have in this research developed what is said above, talking about the different details that make this system a crypto system worthy of the name.**

Keywords: **Authentication, Bitcoin, Blockchain, One Way Functions.**

1. INTRODUCTION

Cryptography and Blockchain Cryptography seen as a mathematical discipline is today at the center of the process of validation and verification of information exchanged within a network, this is what ensures trust. In the following lines, we will describe the blockchain not simply as an algorithm at the base of a certain number of cryptocurrencies as most scientists working in this field have always presented it, but rather as a cryptographic and therefore mathematical concept, like others at the base of several cryptosystems currently in use. Historically, cryptography has been associated with issues allowing the creation and analysis of encryption schemes (which authorizes the exchange of secret information through insecure communication channels). However, from the 1970s, the construction of tamper-proof electronic signatures and the development of error tolerance protocols were included in the discipline of cryptography. In this case, cryptography concerns any system that needs to deal with abuse or malicious attacks. Our definition of cryptography makes essential and necessary the use of certain mathematical tools, such as one-way functions, pseudo-random generators and zero-knowledge proofs, which will be covered in this article.

It is important to emphasize that cryptography is based on a very important assumption which is the existence of one-way functions. These functions capture the computational difficulties that are inherent in cryptography and capitalize on these computational limitations. Without computational limitations, this approach to cryptography becomes ineffective. The difficulties generated by these problems constitute an opportunity for cryptography, but an additional difficulty for the algorithms making it possible to generate the one-way functions.

2. ENCRYPTION SCHEMES

The exchange of secret information over public communication channels represents the most basic and traditional problem in cryptography. This consists of two parties communicating secretly without a third party exploiting this information. Typically, an encryption scheme consists of a pair of algorithms. The first algorithm is the encryption algorithm applied by the sender of the message and the second is the decryption algorithm used by the recipient in order to read the original message. In this configuration, only the ciphertext passes through the communication channel. To guarantee the secrecy of this type of exchange, the two parties must share information that they alone hold. This additional information or “extra knowledge” can take the form of a decryption algorithm or an auxiliary parameter used by the encryption algorithm. This

additional information is called the decryption key. We can note that the decryption algorithm can be known to everyone, since it is necessary to have the decryption key in one's possession in order to decrypt the content. It is also important to point out that the decryption key must always be kept secret.

Assessing the degree of security of this kind of scheme is a task that is not easy, and in some cases it turns out to be very complicated or even impossible. It is important to define the notion of security and its perimeter. Two approaches are possible.

The first derives from information theory, it concerns the information on the source text contained in the ciphertext. If source text information is contained in the ciphertext, then the ciphertext is considered insecure. It has also been shown that, to have a high level of security, an encryption key at least as long as the source text was needed. This drastic condition represents a limitation for this scheme, especially when the amount of information to be encrypted is high.

The second approach is more modern and is based on the degree of complexity of the calculation (complexity theory). In this case, it is not important whether or not the ciphertext contains information about the source text. The only question to ask is related to the feasibility of extracting information from this text. In other words, we are interested in the degree of complexity to decipher the encrypted information. It turns out that in this situation the length of the encryption key is not a "key" element in encryption security. For example, we could use a pseudo-random generator of encryption keys as long as possible from shorter keys.

The first derives from information theory, it concerns the information on the source text contained in the ciphertext. If source text information is contained in the ciphertext, then the ciphertext is considered insecure. It has also been shown that, to have a high level of security, an encryption key at least as long as the source text was needed. This drastic condition represents a limitation for this scheme, especially when the amount of information to be encrypted is high.

The complexity theory leads us to introduce certain concepts such as the public key encryption scheme. Before describing this method, it should be emphasized that it is possible to add an auxiliary parameter to an encryption algorithm, which is the encryption key. Which means that, to encrypt a message, we must also provide the encryption key to the encryption algorithm. Most encryption schemes use equal encryption and decryption keys. This raises the issue of key distribution. This is why a new encryption scheme based on complexity theory has been proposed, where the encryption key (public key) can be known to everyone and is different from the decryption key which is kept secret. It is impossible to trace the decryption key from the encryption key. This scheme solves the key distribution problem and makes it possible to make encryption keys (identifiers) public.

This type of encryption scheme is used in distributed systems such as the blockchain, in order to control access and the validity of information circulating within the network.

3. PSEUDO-RANDOM GENERATORS

Pseudo-random generators play a central role in the construction of encryption schemes. In particular, they make it possible to generate private encryption keys. However, it should be noted that the term "pseudorandom generator" is also used in other contexts, such as probabilistic procedures. Therefore, it is essential to give a clear and precise definition because of their importance in cryptography.

Pseudo-random generators are deterministic algorithms which make it possible to lengthen a sequence of "seed" random numbers, in order to obtain a longer sequence of bits which appears random even though it is not. Pseudo-randomness and complexity theory are fundamentally linked, as these generators are built on the intractability assumption. The hypothesis of the existence of the pseudorandom generator is related to the existence of one-way functions, since it is constructed from particular one-way functions.

4. THE FUNDAMENTALS OF PROBABILITY THEORY

In this section, we will define one-way functions with emphasis on their mathematical descriptions. We will also provide examples of these functions and their applications.

Before presenting these one-way functions, we will make a few reminders about probability calculations. These fundamentals are the bedrock of one-way functions and complexity theory.

Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (1-5), Month: May - August 2023, Available at: www.noveltyjournals.com

Probabilities play a key role in cryptography. In particular, they are essential for processing information or the lack of information (the secret). In this part, we discuss some relevant concepts and inequalities in cryptography.

In what follows, we will only refer to discrete probability distributions. In our case, the probability space consists of a sequence of characters of a certain length l and which are uniformly distributed. This is a sample with a total character length of l bits, and each character is assigned a probability of 2-l.

Random variables are functions that assign a value from the sample space to the real space. The random variable represents the set of outcomes defined over the set of eventualities.

4.1 One-way function

4.1.1 Introduction

A one-way function is a mathematical function that is significantly easier to compute in one direction (the forward direction) than in the opposite direction (the inverse direction). It might be possible, for example, to compute the function in the forward direction in seconds but to compute its inverse could take months or years, if at all possible.

Informally, a function f is a one-way function if

The description of f is publicly known and does not require any secret information for its operation.

Given x, it is easy to compute f(x).

Given y, in the range of f, it is hard to find an x such that f(x) = y. More precisely, any efficient algorithm solving a P-problem succeeds in inverting f with negligible probability.

The existence of one-way functions is an open conjecture. In fact, their existence would imply P = NP, resolving the foremost unsolved question of computer science. This is easy to show by showing the contrapositive: if P = NP, then FP = FNP, and so any function that can be computed in polynomial time can be inverted in polynomial time, since there is a simple FNP algorithm that inverts it by nondeterministically enumerating all possible inputs. However, it is not known whether P = NP implies the existence of one-way functions, mainly because of the worst-case hardness vs. average-case hardness distinction.

For example, it is conjectured, but not proved, that the following are one-way functions:

Factoring problem: f(p,q) = pq, for randomly chosen primes p,q.

Discrete logarithm problem: f(p,g,x) =< p,g,gx(modp) >for g a generator of Z_p∗ for some prime p.

Discrete root extraction problem: f(p,q,e,y) =< pq,e,ye(modpq) >, for y in Z(pq)∗, e in Z_(pq) and relatively prime to (p − 1)(q − 1), and p,q primes. This is the function commonly known as RSA encryption.

Subset sum problem: f(a,b) =< sum (i = 1)(n)a ib i,b >,for a_i in 0,1, and n-bit integers b_i.

Quadratic residue problem.

The existence of a one-way function implies the existence of many other useful cryptographic primitives, including:

Pseudorandom number generators;

Pseudorandom function families;

Bit commitment schemes;

Private-key encryption schemes secure against adaptive chosen-ciphertext attack;

Message authentication codes;

Digital signature schemes (secure against adaptive chosen-message attack.

A trapdoor one-way function is a one-way function for which the inverse direction is easy given a certain piece of information (the trapdoor), but difficult otherwise.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 10, Issue 2, pp: (1-5), Month: May - August 2023, Available at: www.noveltyjournals.com

4.1.2 Types of One Way Functions

There are two types of one way functions namely weak one way functions and strong one way functions

4.1.2.1 Strong One Way Function

A Strong One-Way function is a function which is easy to compute and can be inverted only with a negligible probability on a random input or it is hard to invert on all but a negligible fraction of inputs.

Definition 1. A function f : $\{0,1\}* \rightarrow \{0,1\}*$ is called strongly one way if two condition hold

easy to compute: There exists a polynomial-time algrithm, A, so that on input x algorithm A outputs f(x) (i.e f(x)=A(x)).

hard to invert: For every probabilistic polynomial-time algorithm A ,every polynomial p() , and all sufficently large n's

$Pr(A^{'}(f(x)) \in f^{-1}f(x)) < \frac{1}{p(n)}$

4.1.2.2 Weak One Way Function

A Weak One-Way function is a function which is easy to compute and slightly hard to invert for random inputs or easy to invert on some non-negligible fraction of the inputs.

Definition 2. A function f: $\{0, 1\}n \rightarrow \{0,1\}n$ is called weak one-way, if f is a polynomial-time computable function

there exists a polynomial p(.), for every probabilistic polynomial-time algorithm A, and all sufficiently large n s

$Pr(A^{'}(f(x)) \in f^{-1}f(x)) < 1 - \frac{1}{p(n)}$

where x is chosen uniformly in 0,1n and the probability is also over the internal coin flaps of A flops

Example Integer Factoring

Consider f(x,y) = x.y

Easy to compute Is it one-way?

No: if f(x,y) is even can set inverse as (f(x,y)/2,2)

If factoring a number into prime factors is hard

Specially given N = P.Q, the product of two random large (n-bit) primes, it is hard to factor

Then somewhat hard - there are a non-negligible fraction of such numbers 1//n2 from the density of primes.

Hence a weak one-way function.

5. CONCLUSION

We believe we have achieved our goal, which was to present the Blockchain differently, contrary to the qualification of most others. We have therefore, beyond the presentation of the Blockchain as a simple algorithm at the basis of the operation of certain cryptocurrencies, addressed the essential mathematical concepts making it a system on which organizations can base their confidence in the security of their information system.

REFERENCES

[1] Bellare, Mihir; and Rogaway, Phillip. (September 21, 2005). "Introduction." In Introduction to Modern Cryptography (p. 10). web.cs.ucdavis.edu/~rogaway/classes/227/spring05/book/main.pdf.

[2] Oded Goldreich (2001). Foundations of Cryptography: Volume 1, Basic Tools, (draft available from author's site). Cambridge University Press. ISBN 0-521-79172-3.

[3] Russell, A. Necessary and Sufficient Conditions for Collision-Free Hashing. Journal of Cryptology vol. 8, no. 2., pp. 87-99. 1992.

[4] Template:Cite journal

[5] Further reading

[6] Jonathan Katz and Yehuda Lindell (2007). Introduction to Modern Cryptography. CRC Press. ISBN 1-584-88551-3.

[7] Template:Cite book Section 10.6.3: One-way functions, pp. 374–376.

[8] Template:Cite book Section 12.1: One-way functions, pp. 279–298.

[9] hackernoon.com/stablecoins-designing-a-price-stable-cryptocurrency-6bf24e2689e5

[10] medium.com/@argongroup/stablecoins-explained-206466da5e61

[11] medium.com/coinmonks/asset-tokenization-on-blockchain-explained-in-plain-english-f4e4b5e26a6d

[12] www.nasdaq.com/article/how-tokenization-is-putting-real-world-assets-on-blockchains-cm767952

[13] www.investopedia.com/terms/f/fungibility.asp

[14] www.w3.org/Protocols/Design/Interevol.html