Cryptocurrency: Concept and Associated Aspects

Sudhir Singh
Pranveer Singh Institute of Technology, Kanpur

ABSTRACT

A cryptocurrency can be seen as an encoded data string which can be used as a unit of currency or its equivalent. In recent years, we have seen that cryptocurrency has emerged as a buzz word and everybody is talking about it. In this paper, an introductory view of cryptocurrency is given along with basic concepts and associated terms. The knowledge of the above mentioned terms is very important in modern aspects as it is a buzz word today and many jobs are being created in this particular area.

Keywords: **Cryptocurrency, Hash, Cryptography, Security, Market Value**

INTRODUCTION:

Cryptocurrency is not bound to any central authority or verifying agency such as banks or governments. Cryptocurrency does not exist physically and it supports decentralized control. In 2009, Satoshi Nakamoto has developed first cryptocurrency known as Bitcoin based on has functions and proof of work concept. It is still one of the most popular cryptocurrency in the world. There are some other cryptocurrencies exist like Ethereum, Litecoin etc. A comparative view of various cryptocurrencies is given in below table 1.

Cryptocurrency name	Total Market Value (approx)
Bitcoin	$749 billion
Ethereum	$313 billion
Tether	$79.5 billion
Binance Coin	$62.6 billion
USD Coin	$53.2 billion
XRP	$34.4 billion
Terra	$32.9 billion
Solana	$28.5 billion
Cardano	$28.4 billion
Avalanche	$20.6 billion

Table.1. Showing various cryptocurrencies and their respective market values

It is very important to mention here that cryptocurrencies, for example Bitcoin uses SHA-256 which is a hash algorithm. Hash algorithms are also very useful in cryptography and its allied areas [1-9] and also very important to protect wireless communication [10-15] along with vast network security applications [16-20]. A cryptographic hash function exhibits the following properties.

- One way computation
- Pre-image resistance
- Collision resistance
- Avalanche property

The following figures illustrate more about hash functions:

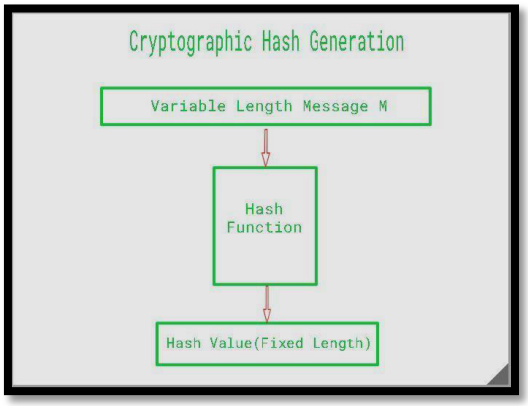

Fig.1. Showing hash value generation of a variable length message

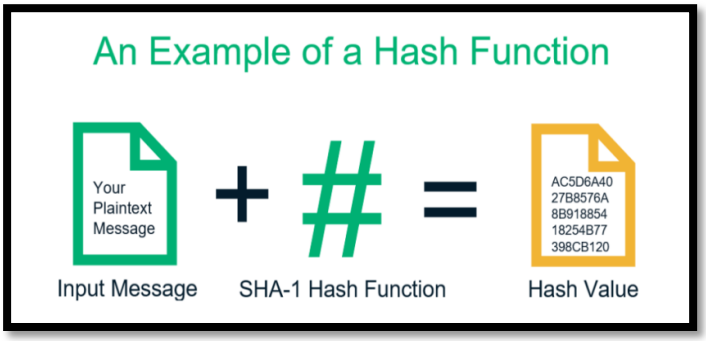

Fig.2. Showing an example of hash computation

Algorithm	Message Size (bits)	Message Digest Size (bits)
SHA-1	$<2^{64}$	160
SHA-224	$<2^{64}$	224
SHA-256	$<2^{64}$	256
SHA-384	$<2^{128}$	384
SHA-512	$<2^{128}$	512
SHA-512/224	$<2^{128}$	224
SHA-512/256	$<2^{128}$	256

Fig.3. Showing SHA variants and the corresponding digest size

ISBN 978-81-931101-3-3 ©2022 Published by Eswar Publications, TN, India

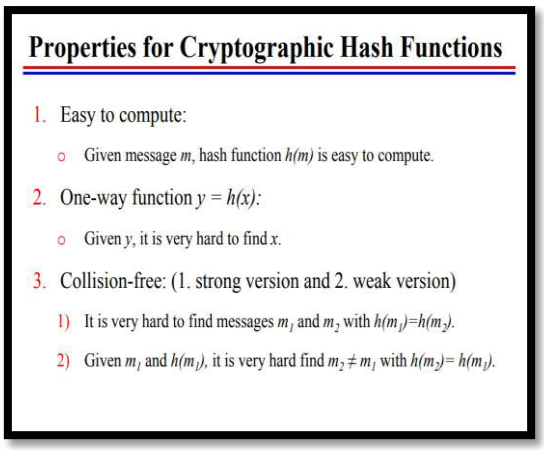

Fig.4. Showing properties of hash functions

POSSIBILITIES IN CRYPTOCURRENCIES:

Many economic agencies and researchers believe that cryptocurrencies will be a very growth full area in the upcoming future [21-23]. The acceptance of cryptocurrencies is increasing day by day worldwide. The below figure illustrates the potential.

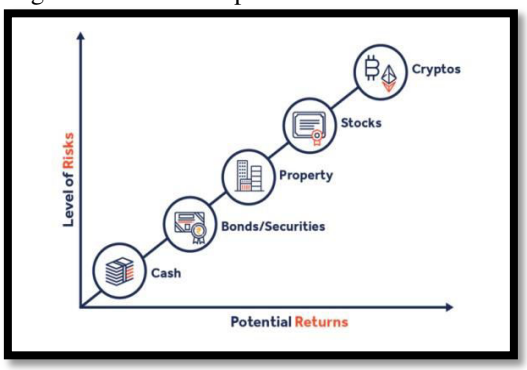

Fig.5. Showing level of risk associated with potential returns

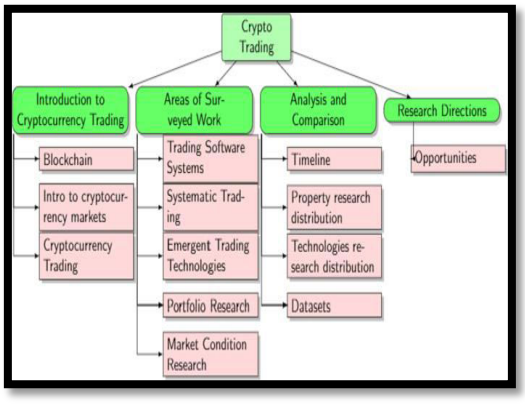

Fig.6. Showing various possibilities and associated applications of cryptocurrencies

CONCLUSION & FUTURE SCOPE:

It can be concluded that cryptocurrencies are emerging as a method of trade now days. Bitcoin is still the most popular cryptocurrency but other cryptocurrencies are also getting popular because of various reasons. Cryptocurrencies use hash functions and involves mining and proof of work concepts. A sound knowledge of hash functions and its properties will help technocrats to understand about cryptocurrencies in a deep fashion. Many traders are accepting payments through cryptocurrencies at various places of world and people are also trading in cryptocurrencies in order to earn high profits. The associated risk with cryptocurrencies provides obstacles in its usage but at the same time, opens the possibilities of high earnings if invested properly. The future scope of cryptocurrencies is also very bright as many countries are preparing various laws regarding it and exploring the possibilities to make it legal and valid completely. Since there is no centralized control in cryptocurrencies, it will be very interesting to see that how governments of various countries deal with it.

REFERENCES

[1]. V. Shukla, A. Chaturvedi, N. Srivastava, Nanotechnology and cryptographic protocols: issues and possible solutions, Nanomaterials and energy, volume 8, issue 1, 2019, 1-6,
DOI: 10.1680/jnaen.18.00006

[2]. M.K. Misra, A. Chaturvedi, S.P. Tripathi, V. Shukla, A unique key sharing protocol among three users using non-commutative group for electronic health record system, Journal of discrete mathematical sciences and cryptography, volume 22, issue 8, 2019, 1435–1451,
DOI: 10.1080/09720529.2019.1692450

[3]. A. Chaturvedi, N. Srivastava, V. Shukla, A secure wireless communication protocol using Diffie-Hellman key exchange, International journal of computer applications, volume 126, number 5, 2015, 35-38,
DOI: 10.5120/ijca2015906060

[4]. V. Shukla, A. Chaturvedi, M.K. Misra, On authentication schemes using polynomials over non commutative rings, Wireless personal communications, volume 118, issue 1, 2021, 1-9,
DOI: https://doi.org/10.1007/s11277-020-08008-4

[5]. V. Shukla, A. Mishra, S. Agarwal, A new one time password generation method for financial transactions with randomness analysis, Innovations in electrical and electronic engineering (Part of the lecture notes in electrical engineering book series (LNEE, volume 661)), 2020, 713-720,
DOI: https://doi.org/10.1007/978-981-15-4692-1_54

[6]. V. Shukla, A. Mishra, A. Yadav, An authenticated and secure electronic health record system, IEEE international conference on information and communication technology, 2019, 1-5,
DOI: 10.1109/CICT48419.2019.9066168

[7]. A. Chaturvedi, V. Shukla, M.K. Misra, Three party key sharing protocol using polynomial rings, 5th IEEE Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), 2018, 1-5,
DOI: 10.1109/UPCON.2018.8596905

[8]. V. Shukla, A. Chaturvedi, N. Srivastava, Secure wireless communication protocol: to avoid vulnerabilities in shared authentication, Communications on applied electronics, volume 7, number 6, 2017, 4-7,
DOI: 10.5120/cae2017652680

[9]. V. Shukla, M.K. Misra, A. Chaturvedi, Journey of cryptocurrency in India in view of financial budget 2022-23, Cornell university arxiv, 2022, 1-6,
DOI: https://doi.org/10.48550/arXiv.2203.12606

[10]. V. Shukla, N. Srivastava, A. Chaturvedi, A bit commitment signcryption protocol for wireless transport layer security (wtls), IEEE international conference on electrical, computer and electronics engineering , 2016, 83-86, DOI: 10.1109/UPCON.2016.7894629

[11]. V. Shukla, A. Chaturvedi, N. Srivastava, A new secure authenticated key agreement scheme for wireless (mobile) communication in an EHR system using cryptography, Communications on applied electronics, volume 3, number 3, 2015, 16-21,
DOI: 10.5120/cae2015651903

[12]. A. Chaturvedi, N. Srivastava, V. Shukla, S.P. Tripathi, M.K. Misra, A secure zero knowledge authentication protocol for wireless (mobile) ad-hoc networks, International journal of computer applications, volume 128, number 2, 2015, 36-39,
DOI: 10.5120/ijca2015906437

[13]. V. Shukla, A. Chaturvedi, N. Srivastava, Authentication aspects of dynamic routing protocols: associated problem & proposed solution, International journal of recent technology and engineering, volume 8, issue 2, 2019, 412-419,
DOI: 10.35940/ijrte.B1503.078219

[14]. V. Shukla, A. Kushwaha, S.S. Parihar, S. Srivastava, V. P. Singh, Authenticated wireless information display system using GSM module, Communications on applied electronics, volume 5, number 3, 2016, 7-11,
DOI: 10.5120/cae2016652251

[15]. V. Shukla, A. Chaturvedi, N. Srivastava, Double layer cryptographic protocol for mobile ad-hoc networks (MANETs) by commitment scheme, Communications on applied electronics, volume 7, number 9, 2017, 32-36,
DOI: 10.5120/cae2017652716

[16]. V. Shukla, A. Chaturvedi, N. Srivastava, A secure stop and wait communication protocol for disturbed networks, Wireless personal communications, volume 110, 861-872, 2019,
DOI: https://doi.org/10.1007/s11277-019-06760-w

[17]. V. Shukla, A. Mishra, A new sequential coding method for secure data communication, IEEE international conference on computing, power and communication technologies, 2020, 529-533,
DOI: 10.1109/GUCON48875.2020.9231252

[18]. A. Chaturvedi, V. Shukla, M.K. Misra, A random encoding method for secure data communication: an extension of sequential coding, Journal of discrete mathematical science and cryptography, volume 24, issue 5, 2021, 1189-1204,
DOI: https://doi.org/10.1080/09720529.2021.1932902

[19]. V. Shukla, A. Chaturvedi, N. Srivastava, A new one time password mechanism for client-server applications, Journal of discrete mathematical sciences and cryptography, volume 22, 2019, 1393-1406,
DOI: 10.1080/09720529.2019.1692447

[20]. V. Shukla, M.K. Misra, A. Chaturvedi, A new authentication procedure for client-server applications using HMAC, Journal of discrete mathematical sciences and cryptography, volume 24, issue 5, 2021, 1241-1256,
DOI: https://doi.org/10.1080/09720529.2021.1932908

[21]. M.A. Fauzi, N. Paiman, Z. Othman, Bitcoin and cryptocurrency: challenges, opportunities and future works, Journal of asian finance, economics and business, volume 7, number 8, 2020, 695-704,
DOI: https://doi.org/10.13106/jafeb.2020.vol7.no8.695

[22]. F.J.G. Corral, J.A.C. García, J.D.P. Valenciano, J.U. Toril, A bibliometric review of cryptocurrencies: how have they grown, Financial innovation, volume 8, article number 2, 2022, 1-31,
DOI: https://doi.org/10.1186/s40854-021-00306-5

[23]. N. Gowda, C. Chakravorty, Comparative study on cryptocurrency transaction and banking transaction, Global transitions proceedings, volume 2, issue 2, 2021, 530-534,
DOI:https://doi.org/10.1016/j.gltp.2021.08.064