Cryptocurrencies: Computational Building Blocks

Frankline Makokha

School of Computing and Informatics University of Nairobi, Kenya

Abstract—**Rapid developments in computational technologies have led to the emergence of various cryptocurrencies riding on key computing technologies, namely cryptology, blockchains and distributed ledgers. These currencies are unregulated and not backed by any government, a fact that has not hindered so far the usage and continued development of new forms of cryptocurrencies. The key impact us for development of cryptocurrencies is ideological innovations. This review paper looks at the enabling technologies for cryptocurrencies the ecosystem of cryptocurrencies, how to mine and spend the cryptocurrencies and factors that impact positively and negatively on the uptake of cryptocurrencies. The paper recommends a laissez faire approach with regards to regulating crytpocurencies.**

Index Terms— **Block Chain, Cyryptocurrency, Distributed Ledgers, Hash Algorithm, Nonce**

I. INTRODUCTION

Cryptocurrencies , also known as Virtual Curencies , Digital Currencies are digital representation of value that can be transferred between parties[1]. They are also defined as digital objects that hold economic value and are functionally similar to fiat currencies that are issued by governments, but are not issued as such and are instead created pursuant to, and governed by, private agreement among a community or users and other network participants [2]. Further virtual currencies could be defined as digital representation of value that can be transferred, stored, or traded electronically and that is neither issued by a central bank or public authority, nor necessarily attached to a fiat currency but is accepted by people as a means of payment [3].

From the above definitions, digital currency could be described as computer-generated units with monetary value of no legal status that could be traded or used as a medium of exchange in a peer-to-peer fashion without intermediaries.

Digital Currencies differ from electronic money (e-money)in that e-money is sovereign monetary value stored electronically in a device such as a chip card or a hard drive in a computer [4]. Examples of this include money in credit and debit cards issued by bank and mobile wallets provided by mobile network operators.

Examples of digital currencies are: Bitcoin, Ethereum, Dash, Maker, Litecoin, Monero, Mixin, Augur, Decred, Clams etc. [5].

Virtual currencies can be broadly classified as open (convertible) or closed(non-convertible). Open virtual currency can be ex-changed back and forth for real currency, while closed virtual currency can only be used in the environment for which it was de-signed [6].

II. CRYPTOCURRENCIES ECOSYSTEM

The Cryptocurrency system is made up of several players namely miners, users, exchangers, and transaction service providers and software developers [2].

The roles played by each player are:

a) Miners: these are entities involved in the creation of digital currency through solving of complex mathematical puzzles and partcipiating in validation of transactions [7]
b) Users: are people who obtain cryptocurrency and use it to purchase goods or services, or to transfer value to another person, or to hold for investment purposes.
c) Exchangers: are persons in the business of exchanging cryptocurrencies for fiat currency.
d) Transaction service providers: are entities that provide online digital currency transaction services, allowing individuals to store and transact Bitcoins without having to run the Bitcoin client on their own computers, e.g wallet and vault providers.
e) Software developers are persons involved in research, design and development of computer software that makes use of cryptocurrencies.
f) Merchants: these are traders that accept cryptocurrencies in exchange for real goods and real services.

III. CRYTOCURRENCY ENABLING TECHNOLOGIES

Digital currencies rely on three main underlying technologies, namely Cryptology, Blockchain technology and Distributed Ledgers technology.

3.1 Cryptology

This is the study of secure communications using cryptography and cryptanalysis [8]. Cryptography deals with the design of algorithms for encryption and decryption, intended to ensure the secrecy and/or authenticity of messages while cryptanalysis involves recovering information from ciphered text.

The main mathematical technique in crytology used by digital currencies is: hash function, encryption and digital signatures.

A Hash function is a directional algorithm that maps a variable length message into a fixed length value called a message digest or hash code. This is used in ensuring the message is not altered (data integrity).

Encryption refers to conversion of plaintext or data into unintelligible form by means of a reversible translation, based on agiven algorithm [8]. The encryption process uses public private key pairs or shared secret keys. Encryption aids in maintaining data confidentiality.

Digital signature refers to a message digest encrypted using the creator's private key and attached to the original message. This is used to ensure Integrity, Authenticy and Non-repudiation of the received message.

3.2 Blockchain technology

A block chain is a series of hashed timestamps, each cryptographically linked to the previous, using a hash digest [9]. It is also defined as a digital ledger that allows parties to transact without the use of a central authority to validate those transactions [10]. It could also be viewed as a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties [11].

From the above definitions a block chain is a set of digital transactions cryptographically linked by hashed content of previous transaction and timespamps.

Block chain technology enables validation of the transactions by participating entries without the need for trusted third parties because the block chains are immutable.

The block in the blockchain is a pool of digital transactions, and it is the fact that the records are linked cryptographically that forms the blockchain.

3.3 Distributed Ledgers Technology

Distributed ledgers refers to transactions or digital events that have been executed and shared among participating parties where each transaction in the public ledger is verified by consensus of a majority of the participants in the system [11].

They have also been defined as shared databases where all participating nodes have an equal status and thus they can submit, review and verify the records [12].

Distributed Ledger Technology refers to processes and related technologies that enable nodes in a network to securely propose, validate and record state changes (or updates) to a synchronised ledger that is distributed across the network's nodes [13].

IV. MINING OF CRYPTOCURRENCIES

Mining is the process by which new bitcoin is added to the money supply [14]. The miners engage in the mining process and are rewarded by being given crytpocurencies. The value of the Cryptocurrency assigned to a miner incorporates also all transaction fees involved in creating the Cryptocurrency [14].

Mining is done through registration of transactions, which consists of solving a puzzle requiring high computational power [15].

Miners build a list of recent transactions and calculate summary information about the proposed block, which is combined with a number called a nonce to create a block header. The hash of the block header is then calculated to see if it is small enough to win at the current difficulty. If not, the nonce is changed and the new hash is calculated and tested [16].

A nonce (number only used once) is a random string of number added to a hashed block then rehashed [17]. For cryptocurrencies the nonce has to produce a hash value that meets certain difficult restrictions or target value[17]. The miners are required to try different nonces and hash the combination until the produced hash meets the criteria set out in the previous confirmed block.

It is this process of trying different nonces, reharshing them until the correct one is found that is called proof of works. Further depending on the consensus protocol in use by a certain crptocurrency this may also be called proof-of-stake, proof-of-burn, proof-of-elapsed-time or proof-of-capacity [9].

The proof-of-work puzzle is controlled by an adaptive algorithm, which takes into account recent activity in the blockchain's history. The more people join the mining process and dedicate more computing power, the harder the algorithm makes the mining process of new cryptocurrencies [18]

V. SPENDING OF CRYPTOCURRENCIES

For one to acquire and use cryptocurrencies, a digital wallet, either mobile phone based or desktop based is required. A digital wallet is software that stores private and public keys and interacts with various cryptocurrency algorithms to enable users to send and receive digital currency and monitor their balance [19].

Examples of digital wallets include copay, atomic wallet, breadwallet, Airbits etc. Some walletscan be in phyiscal form like USB drives [19]. Different wallets support different cryptocurrencies thus one is required to ensure compartibility before settling on a certain wallet.

The private keys are used to initiate the transcation on the Cryptocurrency, which is validated by a matching public key as-signed to the crytpocurrency being traded.

VI. FACTORS AFFECTING UPTAKE AND HINDRANCE OF CRYPTO CURRENCIES

The uptake in development of various types of cryptocurrencies and crytpocurrency usage has been catalyzed by various factors, namely:

a) Rapid Technological Development: The developments in the encryption algorithms, hash algorithms, rise in the use of blockchains, distributed technologies and rise in the computing power of processing systems has given an impetus into the rise of cryptocurrencies.

b) Design for Anonymity: Due to the fact that conventional currency exchange on the internet goes through a third party, and the fact that there is a mandatory requirement for full identification before one opens a storage for conventional currency like bank account, those who wish to trade anonymously prefer the use of crytpcurrency which does not use a third party and the owners of the transcation are anonymous.

c) Emergence of vendors willing to exchange cryptocurrencies with fiat currencies as well as with goods and services.

d) Ideological motivations: some cryptocurrencies are created as a result of a sheer desire for experimentation and innovation for its own sake and to create an alternative method to existing financial infrastructure [4].

The various factors that hinder adoption of cryptocurrencies include:

a) Lack of a standard value for cryptocurrencies: The value attached to cryptocurrency is based on the perception the users of that currency have and its popularity. For example when the popularity of a virtual currency drops, the value of that particular virtual currency will be devalued [20].

b) Lack of any governments backing, and the consequent lack of any regulaltory frameworks leads to fear among those who may no understand the working of the technology behind the cryptocurrencies.

VII. CONCLUSION

Due to the fact that most cryptocurrencies are spawning out of ideological motivations, it would not be prudent for any government to try and regulate the mining and usage of cryptocurencies.

Further, any attempts to introduce a trusted third party based Cryptocurrency where the trusted third part vets and authenticates the parties to the exchange of cryptocurrencies will defeat the very motivations behind cryptocurrency, namely anonymity and peer to peer network.

This paper therefore recommends a laissez-faire approach where technological advancements are left to chart their own course to maturity. It is at this maturity stage that self-regulatoty and non-intrusive regulatory frameworks could be designed.

REFERENCES

[1]. Dong H., Karl H., Ross L., Vikram H., Yasmin A., Mikari K., Kyriakos-Saad N., Hiroko O., Tahsin S. S.,, Natalia S., and Verdugo-Yepes C.(2016) . Virtual Currencies and Beyond: Initial Considerations. The International Monetary Fund. (https://www.imf.org/external/pubs/ft/sdn/2016/sdn1603.pdf)

[2]. L. W. Jonathan (2015) A Facilitative Model for CryptocurrencyRegulation in Singapore, in: L. K. C. David (Ed.) Hand-book ofDigital Currency: Bitcoin, Innovations, Financial Instruments and Bid Data . Amsterdam: Elsevier/ AP.

[3]. Baron, J., O'Mahony A., Manheim D. and Dion-Schwarz, C. (2015) National Security Implications of Virtaul Currency: Examining the potential for non-state Actor Deployment. Santa Monica, CA: Rand Coprora-tion.https://www.rand.org/pubs/research_reports/RR1231.html

[4]. Committee onPayments and MarketInfrastructure (2015) Digital Currencies. Basel, Switzerland: Bank for International Settlements.https://www.bis.org/cpmi/publ/d137.pdf

[5]. CoinMarketCap [online] Top 100 Cryptocurrencies by Market Capitalizationhttps://coinmarketcap.com/(accessed on 22nd May 2019).

[6]. Toms, S., Zdrowski, M. and Hall, R.(2015) Virtual Currencies . London: Allen&Overy LLP.http://www.allenovery.com/SiteCollectionDocuments/Virtual%20Currencies.pdf

[7]. Narayanan, A., Bonneau, J., Felten, E., Miller A., and Goldfeder, S.(2016) Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. New Jersy: Pricnceton Universuty Press.

[8]. William, S. (2001) Cryptography And Network Security: Principles And Practice. 5th Edition. New York: Prentice Hall.

[9]. Arim, S., Umar, R. and Rubina L. (2018) Conceptualizing Blockchains:Characteristics & Applications. 11th IADIS International Conference Information Systems 2018.

[10]. Congress (2018) Beyond Bitcoin: Emerging Applications forBlockchain Technology. inHearing before aCommittee on Science, Space and Technology Subcommittee on Oversight & Subcommittee on Research and Technology U.S. House of Representatives. 2018(Statement by Chris JaikaranAnalyst in Cybersecurity Policy).

[11]. Crosby, M., Nachiappan, Pattanayak, P. , Verma, S. andKalyanaraman, V. (2016) BlockChain Technology: Beyond Bitcoin. Applied Innovation Review (AIR), Issue 2.

[12]. Global System for Mobile Communication (GSMA, 2017) Blockchain for Development: Emerging Opportunities for Mobile, Identity and Aid. https://www.gsma.com/mobilefordevelopment/resources/blockchain-development-emerging-opportunities-mobile-identity-aid/

[13]. Committee on Payments and Market Infrastructures (2017) Distributed ledger technology in payment, clearing and settlement: An analytical framework. Basel, Switzerland: Bank for International Settle-ments.https://www.bis.org/cpmi/publ/d157.pdf.

[14]. Antonopulous, M. A. (2010) Mastering Bitcoin: Unlocking Digital Cryptocurrencies .CA, O'Reilly Media, Inc.

[15]. Dmitry, N. (2017) Bitcoin Mining as a Contest. Ledger Vol 2. University of Pittsburgh: University Library System.

[16]. Sterry, D. R. (online 2012) Introduction to Bitcoin Mining :A Guide For Gamers, Geeks, and Everyone Else.http://euro.ecom.cmu.edu/resources/elibrary/epay/IntroductiontoBitcoinMiningSterry.pdf [accessed on 28th May 2019].

[17]. Frankenfild, J. (Online) Nonce.https://www.investopedia.com/terms/n/nonce.asp [accessed on 28th May 2019].

[18]. Peng, S. (2013) BITCOIN: Cryptography, Economics, and the Future. BAS, University of Pennsylvania.

[19]. Rosic, A. (online) Cryptocurrency Wallet Guide: A Step-By-Step Tutorial. https://blockgeeks.com/guides/cryptocurrency-wallet-guide/ [accessed on 30th May 2019] .

[20]. Guo, J. and Chow, A.(2008) Virtual Money Systems: a Phenomenal Analysis, 2008. E-Commerce Technology and the Fifth IEEE Conference on Enterprise Computing, E-Commerce and E-Services.Washington, DC, USA.