International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Review: Blockchain and Cryptocurrency: The Future of Digital Transactions

Raghu Raja Mehra[1], Chaitanya Khosla[2]

Department of Information Technology, Ajanta Public School, Amritsar, India
Email: *raghumehra35[at]gmail.com*

Department of Information Technology, Ajanta Public School, Amritsar, India
Email: *chaitanyakhosla21[at]gmail.com*

Abstract: ***Blockchain, the establishment of Bitcoin, has gotten broad considerations. Blockchain fills in as an unchanging record which permits exchanges happen in a decentralized way. Blockchain - based applications are jumping up, covering various fields including financial administrations, notoriety framework and Internet of Things (IoT). There are as yet numerous difficulties of blockchain innovation, for example, versatility and security issues holding back to be survived. This paper displays a far reaching outline on blockchain innovation. We give an outline of blockchain architechture firstly and think about some average agreement calculations utilized in various blockchains. Besides, specialized difficulties and ongoing advances are briefly recorded. We additionally spread out conceivable future patterns for blockchain.***

Keywords: Blockchain, Blockchain architecture, decentralization, consensus, scalability, Bitcoin, Gridcoin, Ethereum coins

1. Introduction

Nowadays cryptographic money has become a popular expression in both industry and the scholarly world. As one of the best digital currency, Bitcoin has delighted in a tremendous accomplishment with its capital market arriving at 10 billion dollars in 2016 [1]. With an exceptionally planned information stockpiling structure, exchanges in Bitcoin system could occur with no outsider and the center innovation to construct. Bitcoin is blockchain, which was first proposed in 2008 and executed in 2009 [2]. Blockchain could be viewed as an open record and every single submitted exchange are put away in a rundown of squares. This chain develops as new squares are annexed to it consistently. Uneven cryptography and circulated agreement calculations have been executed for client security and record consistency. The blockchain innovation by and large has key attributes of decentralization, persistency, namelessness and auditability. With these attributes, blockchain can significantly spare the cost and improve the efficiency. Since it permits installment to be finished with no bank or any go - between, blockchain can be utilized in different financial administrations, for example, advanced resources, settlement and online installment [3], [4]. Furthermore, it can likewise be applied into different fields including keen agreements [5], open administrations [6], Internet of Things (IoT) [7], notoriety frameworks [8] and security administrations [9]. Those fields favour blockchain in multiple ways. First of all, blockchain is unchanging. Exchange can't be altered once it is pressed into the blockchain. Organizations that require high unwavering quality and genuineness can utilize blockchain to draw in clients. Additionally, blockchain is disseminated and can keep away from the single purpose of disappointment circumstance.

With respect to keen agreements, the agreement could be executed by excavators consequently once the agreement has been conveyed on the blockchain. Despite the fact that the blockchain innovation has extraordinary potential for the development of things to come Internet frameworks, it is confronting various specialized difficulties. Right off the bat, adaptability is an immense concern. Bitcoin square size is constrained to 1 MB now while a square is mined about like clockwork. Hence, the Bitcoin arrange is limited to a pace of 7 exchanges for every second, which is unequipped for managing high recurrence exchanging. Be that as it may, bigger squares implies bigger extra room and more slow proliferation in the system.

Blockchain is an arrangement of squares, which holds a total rundown of exchange records like ordinary open record [14]. Figure 1 outlines a case of a blockchain. With a past square hash contained in the square header, a square has just one parent square. It is important that uncle squares (offspring of the square's progenitors) hashes would likewise be put away in ethereum blockchain [15]. The first square of a blockchain is called beginning square which has no parent square. We at that point clarify the internals of blockchain in subtleties.

2. Blockchain Architecture

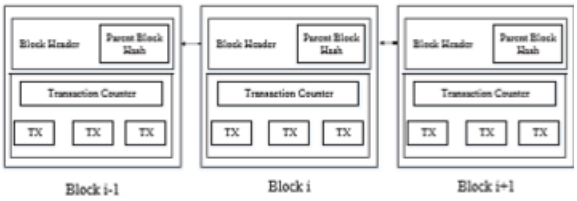

Figure 1: An example of blockchain which consists of a containing sequence of blocks

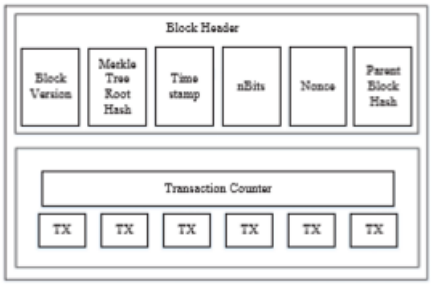

Figure 2: Block structure

a) BLOCK

A block comprises of the square header and the square body as appeared in Figure 2. Specifically, the square header incorporates:

- Block rendition: shows which set of square approval rules to follow.
- Merkle tree root hash: the hash estimation of the considerable number of exchanges in the square.
- Timestamp: current time as seconds in all inclusive time since January 1, 1970.
- nBits: target edge of a substantial square hash.
- Nonce: a 4 - byte field, which for the most part begins with 0 and increments for each hash estimation.
- Parent square hash: a 256 - piece hash esteem that focuses to the past square. The square body is made out of an exchange counter and exchanges. The most extreme number of exchanges that a square can contain relies upon the square size and the size of every exchange. Blockchain utilizes an uneven cryptography system to approve the verification of exchanges [13]. Computerized signature dependent on deviated cryptography is utilized in a conniving domain. We next briefly outline advanced mark

b) Computerized Signature

Each client possesses a couple of private key and open key. The private key that will be kept in confidentiality is utilized to sign the exchanges. The computerized marked exchanges are communicated all through the entire system. The common computerized mark is engaged with two stages: marking stage and verification stage. For example, a client Alice needs to send another client Bob a message.

- In the marking stage, Alice scrambles her information with her private key and sends Bob the encoded outcome and unique information.
- In the verification stage, Bob approves the incentive with Alice's open key. In that manner, Bob could without much of a stretch check if the information has been altered or not. The commonplace advanced mark calculation utilized in blockchains is the elliptic bend computerized signature calculation (ECDSA) [16].

c) Characteristics Key of Blockchain

In rundown, blockchain has following key attributes:

- **Decentralization**- In traditional unified exchange frameworks, every exchange should be approved through the focal confided in office (e. g., the national bank), definitely coming about to the expense and the exhibition bottlenecks at the focal servers. Difference to the unified mode, outsider is never again required in blockchain. Accord calculations in blockchain are utilized to keep up information consistency in disseminated arrange.
- **Persistency:** Exchanges can be approved rapidly and invalid exchanges would not be conceded by fair excavators. It is about difficult to erase or rollback exchanges once they are remembered for the blockchain. Hinders that contain invalid exchanges could be found right away.
- **Anonymity**: Every client can cooperate with the blockchain with a created address, which doesn't uncover the genuine character of the client. Note that blockchain can't ensure the ideal security.

d) Scientific categorization of blockchain frameworks

Current blockchain frameworks are classified generally into three sorts**: open blockchain, private blockchain and consortium blockchain** [17]. In open blockchain, all records are obvious to the general population and everybody could participate in the accord procedure. In an unexpected way, just a gathering of pre - chosen hubs would take an interest in the accord procedure of a consortium blockchain. With respect to private blockchain, just those hubs that originate from one specific association would be permitted to join the accord procedure.

- **Consensus assurance:** In open blockchain, every hub could partake in the agreement procedure. Furthermore, just a chose set of hubs are liable for approving the square in consortium blockchain. Concerning private chain, it is completely constrained by one association and the association could decide the final accord.
- **Read authorization:** Exchanges in an open blockchain are unmistakable to the general population while it depends with regards to a private blockchain or a consortium blockchain.
- **Immutability:** Since records are put away on an enormous number of members, it is almost difficult to alter exchanges in an open blockchain. In an unexpected way, exchanges in a private blockchain or a consortium blockchain could be altered effectively as there are just set number of members
- **Efficiency:** It requires some investment to proliferate exchanges and squares as there are countless hubs on open blockchain organize. Subsequently, exchange throughput is constrained and the idleness is high. With less validators, consortium blockchain and private blockchain could be more efficient.
- **Centralized:** The fundamental contrast among the three kinds of blockchains is that open blockchain is decentralized, consortium blockchain is halfway brought together and private blockchain is completely concentrated as it is constrained by a solitary gathering.

3. Research Methodology

To provide a transparent, reproducible and scientific literature review of blockchain based applications the process suggested by Briner and Denyer (2012) as well as some features of the PRISMA statement (Moheretal., 2009) have been adopted. The overall methodological approach includes the following steps:

1. Identify the need for there view, prepare a proposal for there view, and develop the review protocol.

2. Identify the research select the studies, assess the quality, take notes and extract data, synthesise the data.

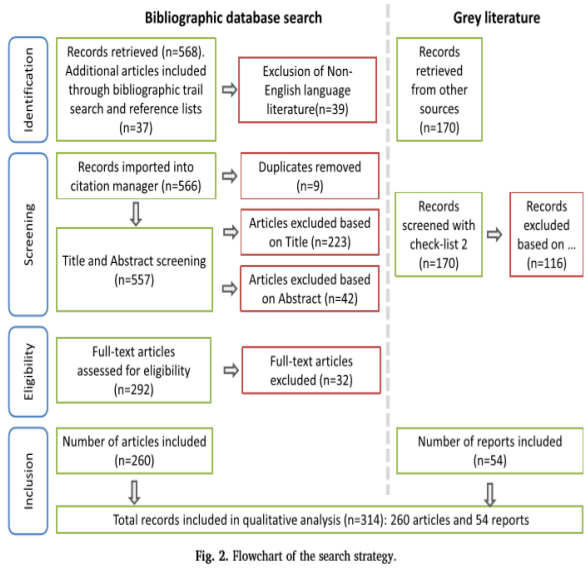

Figure 3: Flowchart of search strategy

A Primer on Blockchain Technology

The Crypto - economy

Cryptographic techniques draw on the science of cryptography, and allow for the protection of sensitive information (organizational, institutional or personal), either in storage or in communication. Initially devised for information security systems (Saper, 2013, p.673), they are now moving into

Blockchain technology ensures the elimination of the double - spend problem, with the help of public - key cryptography, whereby each agent is assigned a private key (kept secret like a password) and a public key shared with all other agents. A transaction is initiated when the future owner of the coins (or digital tokens) sends his/her public key to the original owner.

The coins are transferred by the digital signature of a hash. Public keys are cryptographically generated addresses stored in the blockchain. Every coin is associated with an address, and a transaction in the crypto - economy is simply a trade of coins from one address to another. The striking feature of the blockchain is that public keys are never tied to a real - world identity.

Transactions, although traceable, are enabled without disclosing one's identity; this is a major difference with transactions in fiat currencies that, with the exception of (non - traceable) cash transactions, are related to specific economic agents endowed with legal personality (whether physical or juridical).

Payment finality is "the discharge of an obligation by a transfer of funds and a transfer of securities that have become irrevocable and unconditional" (Committee on Payment and Settlement Systems, 2003, p.496). In a world of fiat money, payment finality is conceptualized in relation to bank money within a triangular payment structure involving a payer, a payee, and a bank acting as a 'go between' (Rossi, 2004, p.3). This 'go between' is in fact the trusted third party required in all payments until the advent of cryptocurrencies. Yet, the latter are trustless protocols that dispense with the trusted third party

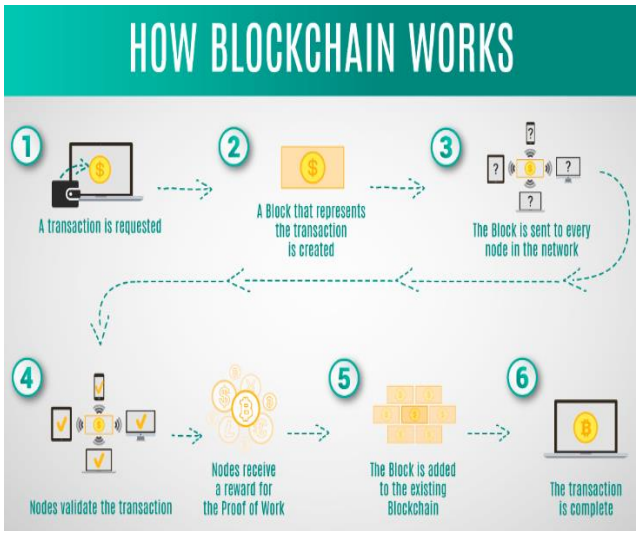

Figure 4: Working of blockchain

Miners and Computational Problem Solving

The blockchain is a chain of transactional records that a subset of network participants (also known as 'miners') enriches by solving difficult computational problems. Miners fiercely (and anonymously) compete on the network to solve the mathematical problem in the most efficient way, thereby adding the next block to the blockchain. The block reward (i. e. newly minted coins) is sent to the miner's public address.

If the miner wants to spend these coins they must sign with the corresponding private key. When mining power increases, so does the difficulty of the computational problems required to mine a new block (Böhme et al, 2015, p.218). This difficulty level is adjusted to keep the block - generation pace constant, roughly ten minutes (Dwyer, 2014, p.5). In the early days, mining was primarily done by individuals on home computers through central (or graphics) processing units BitShare, a mining chip, potentially embedded into millions of Internet devices, works collectively to mine new currency.

These new streams of crypto - currency both solve the problem of bearing the cost of Micropayments, and bring to the fore a new crypto - business model by helping finance the chips themselves (Niccolai, 2015). The technical details remain unclear, but if the latter innovation were to be replicated and widely adopted, it would be a game changer for the whole crypto - economy.

Hashes and Hash Functions

The essence of the blockchain is informational before being economic or monetary, conducive to many emerging and increasingly popular token - free blockchains. It relies extensively on hashes and hash functions. A hash (output) is the result of a transformation of the original information (input). A hash function is a mathematical algorithm that takes an input and transforms it into an output. A cryptographic hash function is characterized by its extreme

difficulty to revert, in other words, to recreate the input data from its hash value alone. This is called the collision resistance. Proof - of - work and Proof - of - stake. The hash cash proof - of - work function is at the heart of block generation in the Bitcoin protocol.

Proof - of - stake is a proposed alternative to proof - of - work already implemented for certain altcoins (other than Bitcoin), whereas others rely on a hybrid protocol (Graydon, 2014). Instead of splitting blocks across proportionally to the relative hash rates of miners (i. e. their mining power), proof - of - stake protocols split stake blocks proportionally to the current wealth of miners. Buterin (2014b) argues that proof - of - stake has a number of distinct advantages over proof - of - work (non - wasteful protocol, decreased likelihood of a 51% attack, potentially faster blockchains.)

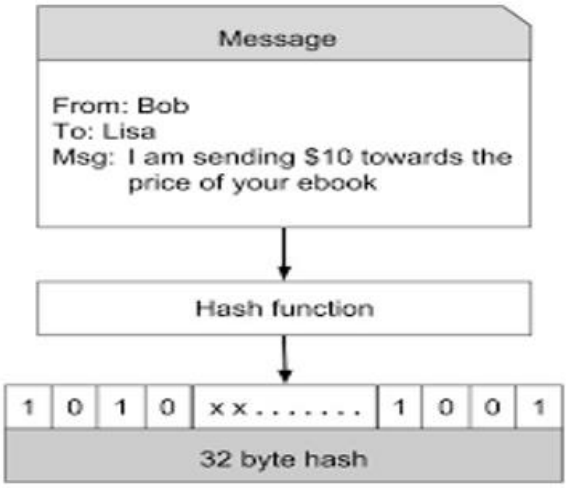

Figure 5: The basic hash function model

A Holistic View of Blockchain Technology

Vitalik Buterin's Definition of the Blockchain

We have previously exposed the core concepts of the blockchain, and alluded to Bitcoin, which is today one blockchain - based platform amongst others, although it still is the most famous worldwide. For Vitalik Buterin (2015a), the blockchain is a magic computer that anyone can upload programs to and leave the programs to self - execute, where the current and all previous states of every program are always publicly visible, and which carries a very strong crypto economically secured guarantee that programs running on the chain will continue to execute in exactly the way that the blockchain protocol specifies.

The definition arguably lacks scientific rigor ('a magic computer' is a debatable term). It is nevertheless useful to discuss, and highlight the features it omits. By not referring to the terms 'ledger', 'money' or 'transactions', Buterin makes the point that the essence of the blockchain is informational and processual, and does not relate directly to the monetary sphere. In this sense, blockchains may exist without an underlying token.

The blockchain is structured around a network, which is evolutionary in essence (Pilkington, 2016, forthcoming). This evolutionary process may be mapped by a state transition function, describing what state to move to, on receiving a given input in a given state.

Again, Buterin rightly refrains from specifying any state transition function.

We find Buterin's definition useful in the sense that amongst the previously discussed core concepts, 'crypto - economy' and 'payments finality' are not definitional features per se, but rather fundamental characteristics of major blockchain applications, extended to the monetary and economic sphere.

Figure 6: The symbolic Bitcoin as a cryptocurrency

Private, Public and Hybrid Blockchains

Public decentralized ledgers are accessible to every Internet user. The public nature stems from the free and unconditional participation of everyone in the process of determining what blocks are added to the chain, and what its current state is (Buterin, 2015b). These fully decentralized blockchains rest on a consensus mechanism of proof - of - work (or proof - of - stake) for validation purposes: "in the case of Bitcoin, the "longest chain – the chain with the most proof - of - work – is considered to be the valid ledger" (Swanson, 2015, p.4).

In a fully private ledger, write - permissions are monitored by a central locus of decision - making. Read - permissions are either public or restricted (Buterin, 2015b). A private blockchain amounts to a permissioned ledger, whereby an organizational process of Know - Your - Business (KYB) and Know - Your - Customer (KYC) enables the white listing (or blacklisting) of user identity. The difference between public and private blockchains is the extent to which they are decentralized, or ensure anonymity. Between the two extremes, there exists a continuum (Brown, 2015, Allison, 2015) of "partially decentralized" blockchains (Buterin, 2015b), rather than a strict public/private dichotomy. Partially decentralized, also called "consortium blockchains" (Buterin, 2015b), constitute a hybrid between the low - trust (i. e. public blockchains) and the single highly - trusted entity model (i. e. private blockchains).

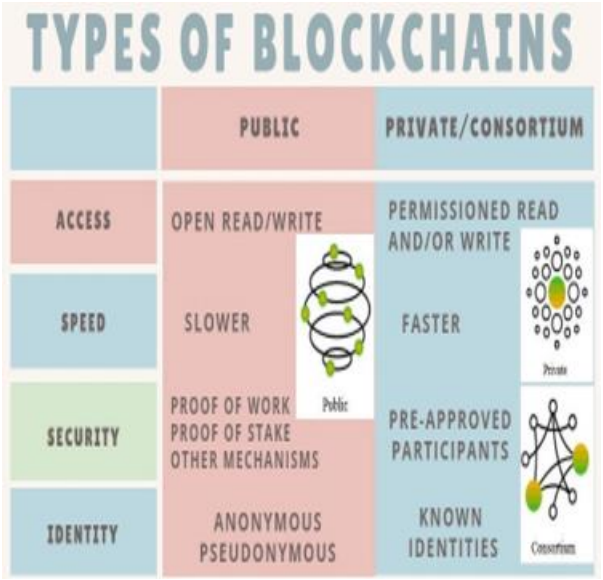

Figure 7: Types of Blockchain

Features of Decentralized Public Ledger Platforms

Bitcoin was the first decentralized public ledger, and has acquired a global status since 2013 - 2014. Although we are still far away from mass adoption, the success of Bitcoin is to be credited to the underlying innovation called the blockchain.

What is the blockchain?

It is simply a secure public ledger platform shared by all parties through the Internet or an alternative distributed network of computers. With the notable exception of token - free applications, the tour de force of the blockchain is to remove the need for a trusted third party to guarantee a transaction. Here after, we list five important features of public ledgers. Protocol for Sending, Receiving and Recording Value. When extended to the (crypto) monetary sphere, the blockchain is nothing less than the continuation of the value transfer system, a technological innovation patented in the USA in 1998 (Jones & Higgins, 1998). Early value transfer systems embodied the concepts of value storage, encryption, and cryptographic public/private key pairing, at the heart of modern crypto - currencies. The main difference between blockchain technology and these crude predecessors is the level of decentralization of the network.

As defined by Benkler (2006, p.62), "' [d]ecentralization' describes conditions under which the actions of many agents cohere, and are effective despite the fact that they do not rely on reducing the number of people whose will counts to direct effective action". Most payment platforms, such as Visa, rely on private secure communication networks, although "VISANet connects to both wired, wireless and also the Internet for processing"., p.4).

Hence, the blockchain is purely Internet - based, and the Bitcoin's blockchain is decentralized. The level of decentralization is far greater in the blockchain than in the first value transfer systems, thanks to the immense network effect of the Internet. However, the current level of decentralization is increasingly questioned by the emergence and adoption of private blockchains by organizations.

Internet - based Value Containers: Coins or Tokens

The "crypto - currency" blockchain set (Byrne, 2015), which does not encompass all the "distributed application/ledger" blockchain set (ibid.), is a modern value transfer system, namely a protocol for sending, receiving and recording value on a public ledger. No transmission of value would ever be possible without the existence of a value container.

This is what economists, who emphasize the unit of account function, call money (Schmitt, 1984, Keynes, 1930, Innes, 1913).

The use of money does not necessarily imply the physical presence of a metallic currency, nor even the existence of a metallic standard of value. We are so accustomed to a system in which the dollar or the sovereign of a definite weight of gold corresponds to a dollar or a pound of money that we cannot easily believe that there could exist a pound without a sovereign or a dollar without a gold or silver dollar of a definite known weight (Innes, 1913, p.377).

Today's blockchain model works the same way: the public ledger or database is simply a more modern way to map out the actual transfer and ownership of crypto - currency. The value container is called a coin, a terminology reminiscent of the currency lexical field, and in fact the primary purpose of a coin (whether tangible or virtual) is precisely to carry value between members of a community of payments. However, the value container may contain instead a fiat currency unit or a financial instrument, which would undermine its full - fledged virtual currency status. Strictly speaking, value containers (or tokens) and currencies are thus not synonymous. 3

.

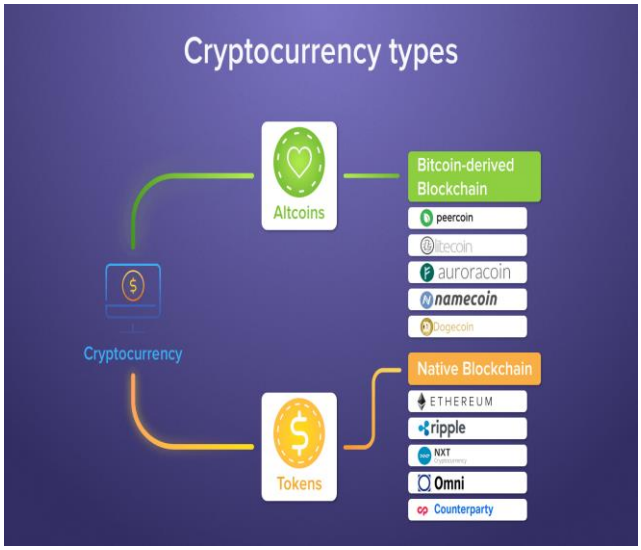

Figure 8: Coins Vs Tokens

Immutability of the System

Immutability is a characteristic of blockchain technology (Coletti, 2015). Derose (2015b) argues that immutability, or resistance to tampering, is what confers its intrinsic value to crypto - currencies, thanks to a revolutionary feature, namely "the ability to declare a truth, globally and without a centre of authority, regardless of what anyone else does to change this truth".

Certain features of the blockchain concept might be relaxed (see infra), but not immutability, which remains crucial: “a blockchain does not need to be a shared ledger, nor does it need to have a distributed consensus. It can be completely centralized as long as its data/state is externally verifiable and all data is immutable” (anonymous reviewer cited by Swanson, 2015, p.59). So if immutability is what ultimately makes a cryptocurrency intrinsically worth trading, this must be the most essential feature of all. Hasn’t the Bitcoin’s blockchain ever experienced failure since its inception? On March 11, 2013, the network proved dysfunctional, with the appearance of a fork resulting in two concurrent Bitcoin networks with two distinct blockchains running in parallel, before one of them was eventually abandoned by the community of miners a few hours later (Buterin, 2013). Buterin (ibid.) describes a more serious bug that shook the network in August 2010, yet without any serious consequence. He explains the technical details of the incident akin to an integer overflow bug3 that required the Bitcoin software to be republished resulting in a fork of the blockchain with a new valid chain overtaking the old one. Notwithstanding these two incidents, the Bitcoin distributed ledger remains immutable to date.

4. Conclusion

Blockchain has shown its potential for transforming traditional industry with its key characteristics: decentralization, persistency, anonymity and auditability.

In this paper, we present a comprehensive overview on blockchain. We have exposed the core concepts at the heart of blockchain technology as well as some of the most significant features of public decentralized ledger platforms. After showing why the blockchain is a foundational and disruptive technology, with the potential to revolutionize the nature of the interface between economic agents, we have presented a non - exhaustive list of existing applications of blockchain technology. These applications range from Blockstream sidechains and Ethereum to digital identity providers and blockchain - based voting systems, as well as Ripple. And we have highlighted the societal relevance of these wide - ranging technological evolutions, which could effectively contribute to social inclusion in the developing world.

Blockchain enthusiasts, surfing on a wave of euphoria set in motion by scores of innovative start - ups (Shubarth, 2015) currently seem to outnumber the sceptics.

The fundamental blockchain question is ultimately that of trust. Yet, as Seabright (cited by Harford 2010), “ [f]actors which increase trust in society are not necessarily a good thing, because they can increase the bonds between gang members, whose main economic success comes from extorting or coercing other people”. This opinion is corroborated by Kaminska (2014), who thinks that blockchain technology has been mired in paradox from the onset. Without an inbuilt payoff mechanism, the cost of participation is dissuasive, and leaves aside all agents who do not have a direct interest in the projected consensus.

References

[1] “State of blockchain q1 2016: Blockchain funding overtakes bitcoin, ” 2016. [Online]. Available: http: //www.coindesk. com/ state - of - blockchain - q1 - 2016/
[2] S. Nakamoto, “Bitcoin: A peer - to - peer electronic cash system, ” 2008. [Online]. Available: https: //bitcoin. org/bitcoin. pdf
[3] G. W. Peters, E. Panayi, and A. Chapelle, “Trends in crypto - currencies and blockchain technologies: A monetary theory and regulation perspective, ” 2015. [Online]. Available: http: //dx. doi. org/10.2139/ssrn.2646618
[4] L. Tsilidou, “Furtherapplicationsoftheblockchain, ” 2015.
[5] Y. Zhang and J. Wen, “An iot electric business model based on the protocol of bitcoin, ” in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp.184–191.
[6] M. Sharples and J. Domingue, “The blockchain and kudos: A distributed system for educational record, reputation and reward, ” in Proceedings of 11th European Conference on Technology Enhanced Learning (EC - TEL 2015), Lyon, France, 2015, pp.490–496.
[7] C. Noyes, “Bitav: Fast anti - malware by distributed blockchain consensus and feedforward scanning, ” arXiv preprint arXiv: 1601.01405, 2016.
[8] Eyal and E. G. Sirer, “Majority is not enough: Bitcoin mining is vulnerable, ” in Proceedings of International Conference on Financial Cryptography and Data Security, Berlin, Heidelberg, 2014, pp.436– 454.
[9] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: A technical survey on decentralized digital currencies, ” IEEE Communications Surveys Tutorials, vol.18, no.3, pp.2084–2123, 2016.
[10] NRI, “Survey on blockchain technologies and related services, ” Tech. Rep., 2015. [Online]. Available: http: //www.meti. go. jp/english/press/ 2016/pdf/0531 01f. pdf