International Journal of Information Science and Computing: 4(1): June 2017: p. 27-39

DOI: 10.5958/2454-9533.2017.00004.7

Blockchain Technology: A Revolutionary Bitcoin Technology

Chinmaya Dash* and Prakash Chandra Behera

Department of Computer Science, St. Claret College, Bangalore, Karnataka, India

*Corresponding author: da.chinmaya.sh@gmail.com

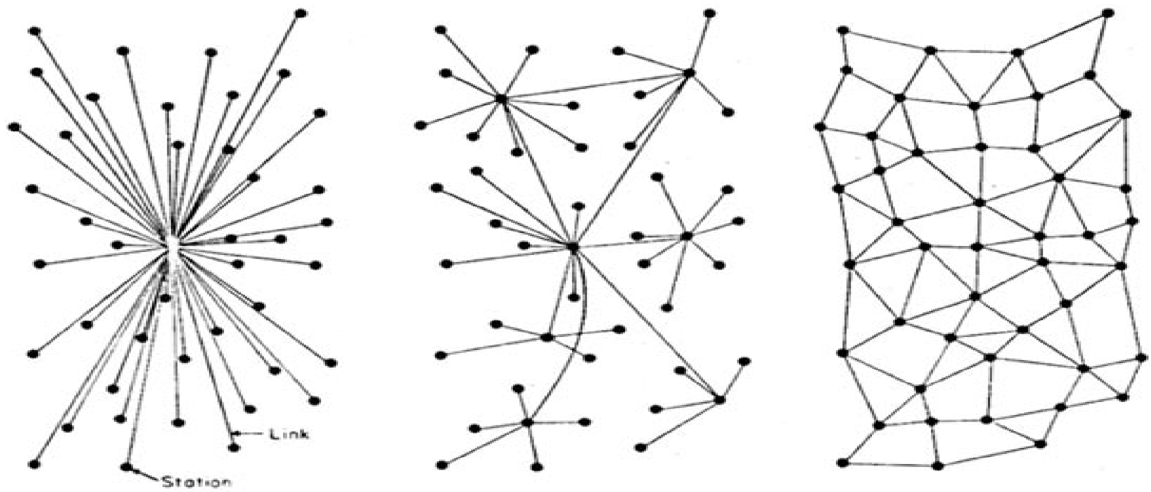
ABSTRACT

Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. The interest in Blockchain technology has been increasing since the idea was coined in 2008. The reason for the interest in Blockchain is its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions, and therefore it creates interesting research areas, especially from the perspective of technical challenges and limitations. This paper highlights the architecture, benefits and applications of Blockchain Technology.

Keywords: Blockchain, bitcoin, cryptocurrency, hash key

Blockchain, mostly known as the backbone technology behind Bitcoin, is one of the hottest and most intriguing technologies currently in the market. Since 2013, Google searches for "blockchain" have risen 1900%. Similar to the rising of the internet, blockchain has the potential to truly disrupt multiple industries and make processes more democratic, secure, transparent, and efficient. Entrepreneurs, start-up companies, investors, global organizations and governments have all identified blockchain as a revolutionary technology.[1][7][10]

The technology concept behind the blockchain is similar to that of a database, except that the way you interact with that database is different. For developers, the blockchain concept represents a paradigm shift in how software engineers will write software applications in the future, and it is one of the key concepts that needs to be well understood. We need to really understand five key concepts, and how they interrelate to one another in the context of this new computing paradigm that is unravelling in front of us: the blockchain, decentralized consensus, trusted computing, smart contracts, and proof of work/stake. This computing paradigm is important because it is a catalyst for the creation of decentralized applications, a next-step evolution from distributed computing architectural constructs.



CENTRALIZED (A) DECENTRALIZED (B) DISTRIBUTED (C)

Fig. 1: Distributed Communications Networks, Paul Baran, 1962 [14][17]

DIFFERENCE BETWEEN BITCOIN & BLOCKCHAIN

Bitcoin is a digital token that lets you send money to any person in the world to pay for goods and services. A large network of computers works 24/7 to check the legitimacy of transactions and process them in real time so that no bank or government needs to be a middle man. The computers also keep track of everyone's bitcoin balance and publish them online as a shared public ledger. The ledger lets anyone check transaction records to make sure they received payments or payments they sent were accepted. Every 10 minutes or so the computers update the ledger with a 'block' of the recent transactions from all bitcoin users worldwide. Once the block is added to the ledger and all computers agree it is legitimate, everyone's bitcoin balance is permanently updated. This long public ledger of transaction blocks is what we call the blockchain. [2][3]

Blockchain technology is simply using a network of computers as a ledger system to keep perfect records. It has mostly been touted as a simple payment system, but it can also be used for a wide range of accounting purposes that could revolutionize how financial services operate worldwide.[5]

FEATURES OF BLOCKCHAIN

Decentralized consensus (on or off bitcoin's blockchain)

A decentralized scheme, on which the bitcoin protocol is based, transfers authority and trust to a decentralized virtual network and enables its nodes to continuously and sequentially record transactions on a public "block," creating a unique "chain": the blockchain. Each successive block contains a "hash" (a unique fingerprint) of the previous code; therefore, cryptography (via hash codes) is used to secure the authentication of the transaction source and removes the need for a central intermediary. The combination of cryptography and blockchain technology together ensures there is never a duplicate recording of the same transaction.[4][6]

With this degree of unbundling, the consensus logic is separate from the application itself; therefore, applications can be written to be organically decentralized, and that is the spark for a variety of system-changing innovations in the software architecture of applications, whether they are money or non-money related.

The blockchain (and blockchain services)

A blockchain is like a place where you store any data semi-publicly in a linear container space (the block). Anyone can verify that you've placed that information because the container has your signature on it, but only you (or a program) can unlock what's inside the container because only you hold the private keys to that data, securely. So, the blockchain behaves almost like a database, except that part of the information stored — its "header" — is public. [2][13]

The data stored can be a token of value, or a crypto money balance. So, the blockchain acts as an alternative value transfer system that no central authority or potentially malicious third party can tamper with (because of the encryption process). The blockchain can also be seen as a software design approach that binds a number of peer computers together that commonly obey the same "consensus" process for releasing or recording what information they hold, and where all related interactions are verified by cryptography.

Smart contracts (and smart property)

Smart contracts are the building blocks for decentralized applications. A smart contract is equivalent to a little program that you can entrust with a unit of value (as a token or money), and rules around that value. The basic idea behind smart contracts is that a transaction's contractual governance between two or more parties can be verified programmatically via the blockchain, instead of via a central arbitrator, rule maker, or gatekeeper. Why depend on a central authority when two (or more) parties can agree between themselves.

Trusted computing (or trust less transactions)

When you combine the concepts behind the blockchain, decentralized consensus, and smart contracts, you start to realize they are enabling the spread of resources and transactions laterally in a flat, peer-to-peer manner, and in doing that, they are enabling computers to trust one another at a deep level.

Proof of work (and proof of stake)

At the heart of a blockchain's operations is the key concept of "proof-of-work," an integral part of Satoshi Nakamoto's original vision for the blockchain's role as the unequivocal authenticator of transactions. The "proof of work" is a "right" to participate in the blockchain system. It is manifested as a "big enough hurdle" that prevents users from changing records on the blockchain without re-doing the proof of work. So, proof of work is a key building block because it cannot be "undone," and it is secured via the strengths of cryptographic hashes that ensure its authenticity.

The original bitcoin blockchain technology had limitations as we started to push its limits outside of money-related services and into the software applications realm, so we shouldn't be surprised that the way forward is a world of multiple blockchains. Some of them will be working together, some competing with one another, and others just being benevolent to each other.[8][9][13][14]

SEGMENTS OF BLOCKCHAIN APPS

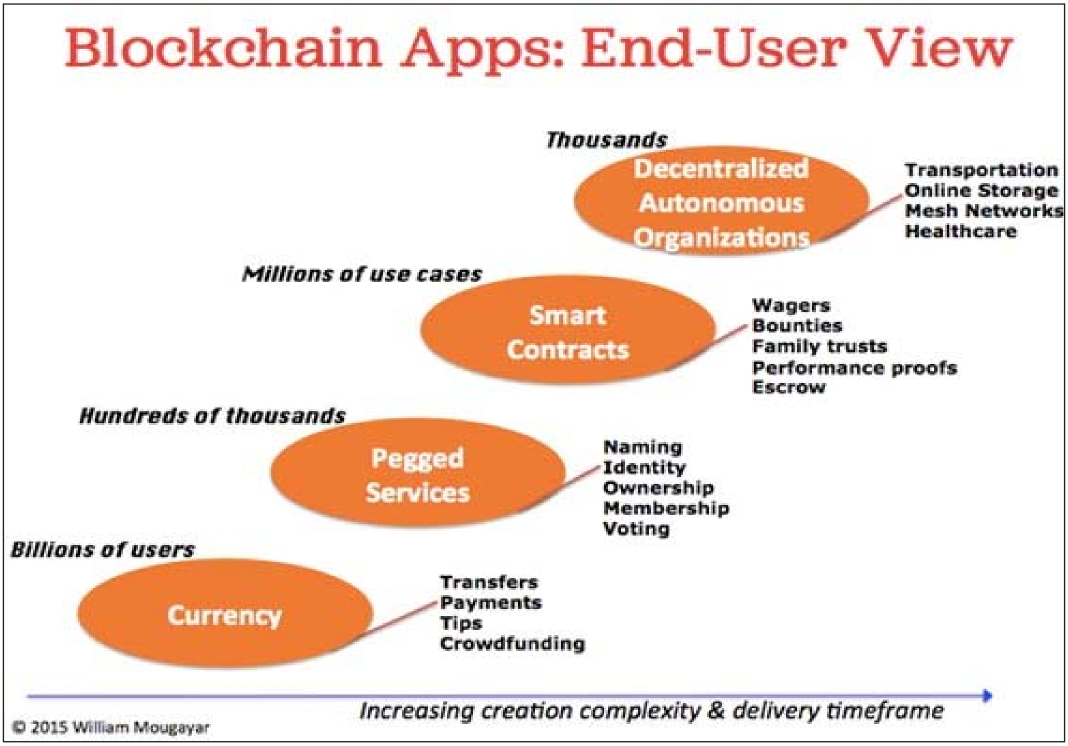


Fig. 2: Segment of Blockchain (Courtesy of William Mougayar) [3][11][12]

The *currency*-related segment targets money transfers, payments, tips, or funding applications. The end-user typically goes to an exchange or uses their own wallet to conduct such transactions, benefiting from transaction cost reductions, speeds in settlements, and freedom from central intermediaries. Today's exchanges are centralized, but it's likely we'll see another generation of decentralized trusted exchanges. And although the current bitcoin wallets today are "dumb" wallets, they could become smarter, via an ability to launch smart contracts.

Pegged services to the blockchain represent an interesting segment because these apps utilize the blockchain's atomic unit, which is a "value store" capability, but they also build on top of that with their unique off-chain services. For example, decentralized identity or decentralized ownership is a horizontal blockchain service, but it can be applied to any other vertical segments, such as for videos, music, or photography, just to name a few.

Smart contracts are small programs or scripts that run on a blockchain and govern legal or contractual terms on their own. They represent a simple form of decentralization. They will become available in a variety of application areas, such as for wagers, family trusts, escrow, time stamping, proofs of work delivery, etc. In essence, they are about moving certain assets or value from one owner to another, based on some condition or event, between people or things. Smart contracts represent an “intermediate state” between parties, and we will trust these smart programs to verify and take action based on the logic behind these state changes.

Distributed Autonomous Organization is “kind of” incorporated on the blockchain because its governance is very dependent on the end-users who are part-owners, part-users, and part-nodes on that decentralized network. Key aspects of a DAO are that each user is also a “worker,” and by virtue of their “work,” they contribute to the value appreciation of the DAO via their collective participation or activity levels. Arguably, bitcoin itself is the “uber DAO.”

Table 1: Segments of Blockchain[16][17]

Category	Protocol User	Frequency	Benefits	Examples
Currency	Exchanges, payment processors, miners, wallets.	Sporadic	Cost, speed.	Coinbase ChangeTip *any wallet* *any exchange*
Pegged Services	Web business	Chronic	Openness, flexibility, new business models, network effects, empowered users.	OneName Mine Swarm Streamium OpenBazaar Assembly
Smart Contracts	Contracts service provider, web apps, or end-user with self-service tools.	Episodic	Autonomy, cost, speed, irrefutability.	Mist (by Ethereum) SmartContract Secure Asset Exchange
Decentralized Autonomous Organizations	DAO itself	Habitual	User protection, user voice, user governance, transparency, self-regulation, sovereignty.	La’Zooz, Storj MaidSafe OpenGarden Bitnation

PUBLIC VS PRIVATE BLOCKCHAINS

Bitcoin allows anyone to write to its ledger. **B**itcoin is designed as a ‘anyone-can-write’ blockchain, where participants aren’t vetted and can add to the ledger without needing approval, it needs ways of arbitrating discrepancies (there is no ‘boss’ to decide), and defence mechanisms against attacks (anyone can misbehave with relative impunity, if there is a financial incentive to do so). These create cost and complexity to running this blockchain.[6][11][15]

Public blockchains

Ledgers can be 'public' in two senses:

- ❖ Anyone, without permission granted by another authority, can write data
- ❖ Anyone, without permission granted by another authority, can read data usually
- ❖ When people talk about public blockchains, they mean anyone-can-write.

Private Blockchains

- ❖ A 'private' blockchain network is where the participants are known and trusted: for example, an industry group, or a group of companies owned by an umbrella company
- ❖ Many of the mechanisms aren't needed – or rather they are replaced with legal contracts. This changes the technical decisions as to which bricks are used to build the solution.

HOW DOES BLOCKCHAIN WORK?

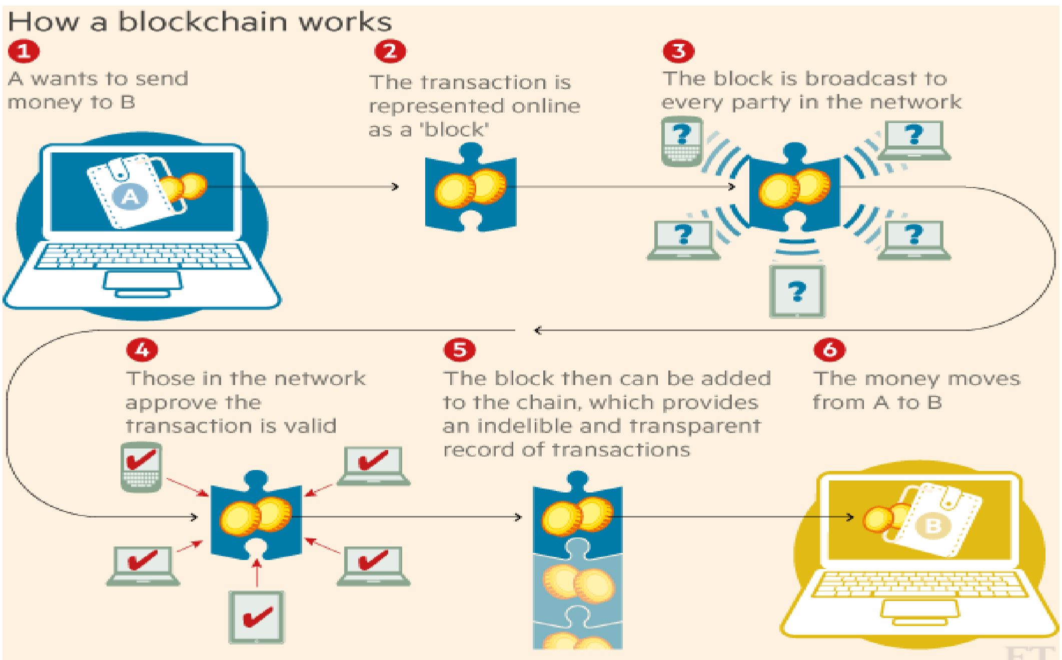


Fig. 3: Blockchain Working Model

When someone wants to add a transaction to the chain, all the participants in the network will validate it. They do this by applying an algorithm to the transaction to verify its validity. What exactly is understood by "valid" is defined by the blockchain system and can differ between systems. Then it is up to a majority of the participants to agree that the transaction is valid. A set of approved transactions are then bundled in a block, which gets sent to all the nodes in the network. They in turn validate the new block. Each successive block contains a hash, which is a unique fingerprint, of the previous block.[4][7][10]

BLOCKCHAIN ARCHITECTURE

When one examines the architecture of Blockchain, a few important design aspects need to be discussed.

- The **Blockchain platform** itself
- The role of **Nodes** in constituting the overall blockchain & the Node discovery process
- **Transactions** that make up the **blocks** running in the Nodes
- **Security** implementation that generates the **Blocks**
- The process of adding newer blocks to the **Chain**

Blockchain Platform

The Blockchain itself is an application that runs on a network of distributed servers. The core application is a transaction database modeled as a secure ledger, that is shared by all nodes (servers) that run the full stack install. It is thus a 100% decentralized transaction system that acts as a highly transparent ledger. Any node running the Blockchain software can run the entire Blockchain locally. While the Blockchain client uses Google's LevelDB database to store metadata internally – the Blockchain data can be stored in a flat file or in a relational DB depending on user preferences.

Once installed on a server, the full Blockchain client syncs up with other nodes in the network. From then onwards the particular server maintains all and any transaction records conducted using bitcoins (or any other application running on the Blockchain). The integrity and chronological order of the transactions (& the addresses owning the currency) are enforced by strong cryptographic rules. As stated above, the Blockchain software operates at such a massive scale which makes it virtually impossible (and cost prohibitive) to hack or otherwise break into bitcoin or any other application running on it. Thus there is no need for a central 3rd party to an issue, authenticate and validate ownership of the currency.The nodes in the overall network use the peer-to-peer IP network to process and verify transactions. When several nodes all have the same blocks in their individual databases, they are considered to be in consensus.[15]

Network Protocol Stack

Once nodes are booted up, they perform a peer discovery to contact any other valid node using a given port over TCP. The Blockchain stack is depicted below and is layered on the OSI stack. The Blockchain Message Exchange specifies the handshake logic between nodes as well as the serialization format for messages exchanged over the wire. The Blockchain Overlay Network provides higher level semantics that allow multiple types of blockchains (public, vertical specific & private blockchains) to co-exist as well as provides management abstraction for the same. Developers will essentially use this layer to extend vanilla blockchain to support other kinds of applications which can leverage the existing bitcoin blockchain to validate their transactions. E.g. Other kinds of virtual currency, sidechains etc.

Transactions and Blocks

Applications, the first among them being Bitcoin use blockchain to timestamp transactions. The blockchain implementation consists of two kinds of records: transactions and blocks.

Salient features of transactions :

- ❖ Transactions can be created on the behalf of any client using a Mobile Wallet or any other client application
- ❖ Transactions contain the actual business data to be stored in the blockchain
- ❖ Blocks record the sequence of transactions in the blockchain. Transactions are journaled into the blockchain based on specific sequences
- ❖ Miner nodes create blocks as discussed in the above section

BENEFITS OF BLOCKCHAIN TECHNOLOGY

- ❖ **Disintermediation & trust less exchange**
- ❖ Two parties are able to make an exchange without the oversight or intermediation of a third party, strongly reducing or even eliminating counterparty risk.
- ❖ **Empowered users**
- ❖ Users are in control of all their information and transactions.
- ❖ **High quality data**
- ❖ Blockchain data is complete, consistent, timely, accurate, and widely available.
- ❖ **Durability, reliability, and longevity**
- ❖ Due to the decentralized networks, blockchain does not have a central point of failure and is better able to withstand malicious attacks.
- ❖ **Process integrity**
- ❖ Users can trust that transactions will be executed exactly as the protocol commands removing the need for a trusted third party.
- ❖ **Transparency and immutability**
- ❖ Changes to public blockchains are publicly viewable by all parties creating transparency, and all transactions are immutable, meaning they cannot be altered or deleted.
- ❖ **Ecosystem simplification**
- ❖ With all transactions being added to a single public ledger, it reduces the clutter and complications of multiple ledgers.
- ❖ **Faster transactions**
- ❖ Interbank transactions can potentially take days for clearing and final settlement, especially outside of working hours. Blockchain transactions can reduce transaction times to minutes and are processed 24/7.
- ❖ **Lower transaction costs**
- ❖ By eliminating third party intermediaries and overhead costs for exchanging assets, blockchains have the potential to greatly reduce transaction fees.

CHALLENGES OF BLOCKCHAIN TECHNOLOGY

- **Nascent technology**
- Resolving challenges such as transaction speed, the verification process, and data limits will be crucial in making blockchain widely applicable.
- **Uncertain regulatory status**
- Because modern currencies have always been created and regulated by national governments, blockchain and Bitcoin face a hurdle in widespread adoption by pre-existing financial institutions if its government regulation status remains unsettled.
- **Large energy consumption**
- The Bitcoin blockchain network's miners are attempting 450 thousand trillion solutions per second in efforts to validate transactions, using substantial amounts of computer power.
- **Control, security, and privacy**
- While solutions exist, including private or permissioned blockchains and strong encryption, there are still cyber security concerns that need to be addressed before the general public will entrust their personal data to a blockchain solution.
- **Integration concerns**
- Blockchain applications offer solutions that require significant changes to, or complete replacement of, existing systems. In order to make the switch, companies must strategize the transition.
- **Cultural adoption**
- Blockchain represents a complete shift to a decentralized network which requires the buy-in of its users and operators.
- **Cost**
- Blockchain offers tremendous savings in transaction costs and time but the high initial capital costs could be a deterrent.

APPLICATION OF BLOCKCHAIN

- *Blockchain Money*: Cryptocurrencies provide people across the globe with instant, secure, and frictionless money. Blockchains provide the permanent record storage for every cryptocurrency transaction taken place. Blockchain based cryptocurrencies work because only *verified* transactions are permitted to be recorded in the blockchain. Current systems require users to trust a central authority that the monetary supply and payment transfer will not be tampered with. Blockchain technologies obsolete this previous method of payment transfer by providing a *trustless* environment so that there is no longer a need to rely on a third-party to ensure your payment transfers, thus creating a Person-to-person(Peer-to-peer) environment. [1][3][6]
- *Blockchain Financial services*: Blockchain financial services are redefining the existing rails of our current financial markets infrastructure. Areas of this sector experiencing significant activity range from backend clearing and settlement, to global capital markets architecture. Distributed

ledger systems in some of these cases do not need to be entirely decentralized, and several financial institutions are looking at creating their own "private blockchains".[2][12]

Blockchain technology can be applied to financial services in the following areas:

- Smart Securities via Smart Contracts
- Post Trade Processing and Settlement
- Loan Origination and Servicing
- Foreign Exchange Markets
- Derivatives Markets
- Record-Keeping Processes
- Auditing and Corporate Compliance
- Corporate Shareholder Voting
- Reducing Counterparty Risk
- Cross-Border Payment

- *Blockchain Property*: Smart property allows ownership of both physical and non-physical property to be verified, programmable and tradeable on the blockchain. Physical examples of smart property include vehicles, phones and houses which can be activated, deactivated, tracked, and maintained. [2][9]
- *Blockchain IOT*: Blockchain technology provides the ideal engine to power a fairly new concept regarding our new connected world: *Internet-of-Things.* Spending on the internet-of-things market is expected to top the $1 Trillion mark in the coming years. This opportunity is poised for Blockchain Internet-of-Things to step in and provide the ultimate system to track the unique histories of the billions of smart-devices coming online over the next few years. The following areas are used by Blockchain:

  - Connected Vehicles
  - Smart Appliances
  - Supply Chain Sensors

- *Blockchain Law*: In blockchain law applications, smart contracts are verified on the block chain, allowing for programmable, self-executing and self-enforcing contracts. Blockchain law also encompasses the idea of "Smart Corporations" which includes concepts such as Decentralized Autonomous Corporations (DAC) or Decentralized Autonomous Organization (DAO). [10][14]
- *Blockchain Music*: Applying blockchain technology to music applications allows for a paradigm shift in the way artists can control their musical work. From ownership rights, to royalty payments and first edition rights, blockchain technology applications empower artists to extend ownership of their works.
- *Blockchain Real Estate*: Blockchain technology will inevitably become a foundational pillar of the real esate industry. In a mostly paper-record based industry, block chain real estate allows for an unparralled upgrade in how records are stored and recorded. Utilizing blockchain applications

in essential functions such as payment, escrow, and title can also reduce fraud, increase financial privacy, speed up transactions, and internationalize markets.

- *Blockchain Identity*: Blockchain technology provides the ideal engine to power digital identities. While digital identities are emerging as an inevitable part of our connected world, how we secure our online information is coming under intense scrutiny. Blockchains based identity systems can provide a solution to this issue with hardened cryptography and distributed ledgers.

  Blockchain technology can be applied to identity applications in the following areas:

  - Digital Identities
  - Passports
  - E-Residency
  - Birth Certificates
  - Wedding Certificates
  - IDs
  - Online Account Logins

CONCLUSION

A blockchain is a public ledger of all Bitcoin transactions that have ever been executed. It is constantly growing as 'completed' blocks are added to it with a new set of recordings. The blocks are added to the blockchain in a linear, chronological order. Each node (computer connected to the Bitcoin network using a client that performs the task of validating and relaying transactions) gets a copy of the blockchain, which gets downloaded automatically upon joining the Bitcoin network. The blockchain has complete information about the addresses and their balances right from the genesis block to the most recently completed block.

ACKNOWLEDGEMENTS

We are also grateful to Dr. P.K. Paul, Raiganj University who moderated this paper and in that line improved the manuscript significantly.

WE have to express out appreciation to Dr. Anil Bhumali, Vice-Chancellor, Raiganj University for sharing his pearls of wisdom with us during this research. We are also immensely grateful to Dr. Anil Bhumali and Dr. P K Paul for their comments on an earlier version of the manuscript, although any errors are our own and should not tarnish the reputations of these esteemed professionals.

REFERENCES

1. Raval, Siraj 2016. "What Is a Decentralized Application?". *Decentralized Applications: Harnessing Bitcoin's Blockchain Technology*. O'Reilly Media, Inc. pp. 1–2. ISBN 978-1-4919-2452-5. OCLC 968277125. Retrieved 6 November 2016 – via Google Books.

2. Nian, Lam Pak, Chuen, David LEE Kuo 2015. “A Light Touch of Regulation for Virtual Currencies”. In Chuen, David LEE Kuo. *Handbook of Digital Currency: Bitcoin, Innovation, Financial Instruments, and Big Data*. Academic Press. p. 319. ISBN 978-0-12-802351-8

3. Nakamoto, Satoshi 2008. “Bitcoin P2P e-cash paper”. *The Cryptography Mailing List* (Mailing list). Gmane. Archived from the original on 2016-12-13. Retrieved 2016-12-09.

4. Tapscott, Don, Tapscott, Alex 2016. *The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*. ISBN 978-0-670-06997-2.

5. Franco, Pedro 2014. *Understanding Bitcoin: Cryptography, Engineering and Economics*. John Wiley & Sons. p. 95. ISBN 978-1-119-01914-5. Retrieved 6 November 2016 – via Google Play

6. Franco, Pedro 2014. *Understanding Bitcoin: Cryptography, Engineering and Economics*. John Wiley & Sons. p. 9. ISBN 978-1-119-01916-9. Retrieved 4 January 2017 – via Google Books.

7. *Virtual Currencies and Beyond: Initial Considerations*. IMF Discussion Note. International Monetary Fund. 2016. p. 23. ISBN 978-1-5135-5297-2. Retrieved 12 November 2016 – via Google Play.

8. Swan, Melanie 2015. *Blockchain: Blueprint for a New Economy*. O’Reilly Media, Inc. p. 16. ISBN 978-1-4919-2047-3. Retrieved 12 November 2016 – via Google Books.

9. Extance, Andy, 2015. “The future of cryptocurrencies: Bitcoin and beyond”. *Nature*. **526** (7571): 21–23. doi:10.1038/526021a. ISSN 0028-0836. OCLC 421716612.

10. Rizun, Peter R., Wilmer, Christopher E., Burley, Richard Ford, Miller, Andrew 2015. “How to Write and Format an Article for Ledger” (PDF). *Ledger*. **1** (1): 1–12. doi:10.5195/LEDGER.2015.1 (inactive 13 March 2017). ISSN 2379-5980.

11. Herrera-Joancomart J. Research and Challenges on Bitcoin Anonymity. In: Garcia-Alfaro J, Herrera-Joancomart J, Lupu E, Posegga J, Aldini A, Martinelli F, *et al.,* editors. Data Privacy Management, Autonomous Spontaneous Security, and Security Assurance. vol. 8872 of Lecture Notes in Computer Science. Springer International Publishing; 2015. p. 3–16. Available from: http://dx.doi.org/10.1007/978-3-319-17016-9_1.

12. Housley R. In: Public Key Infrastructure (PKI). John Wiley & Sons, Inc.; 2004. Available from: http://dx.doi.org/10.1002/047148296X.tie149.

13. Paul G, Sarkar P, Mukherjee S. 2014. Towards a More Democratic Mining in Bitcoins. In: Prakash A, Shyamasundar R, editors. Information Systems Security. vol. 8880 of Lecture Notes in Computer Science. Springer International Publishing; p. 185–203. Available from: http://dx.doi.org/10.1007/978-3-319-13841-1_11.

14. Mann C, Loebenberger D. 2015. Two-Factor Authentication for the Bitcoin Protocol. In: Foresti S, editor. Security and Trust Management. vol. 9331 of Lecture Notes in Computer Science. Springer International Publishing; p. 155–171. Available from: http://dx.doi.org/10.1007/978-3-319-24858-5_10.

15. Bamert T, Decker C, Wattenhofer R, Welten S. BlueWallet 2014. The Secure Bitcoin Wallet. In: Mauw S, Jensen C, editors. Security and Trust Management. vol. 8743 of Lecture Notes in Computer Science.

Springer International Publishing; p. 65–80. Available from: http://dx.doi.org/10.1007/978-3-319-11851-2_5.

16. Ateniese G., Faonio A., Magri B., de Medeiros B. and Certified Bitcoins. 2014. In: Boureanu I, Owesarski P., Vaudenay S, editors. Applied Cryptography and Network Security. Vol. 8479 of Lecture Notes in Computer Science. Springer International Publishing; p. 80–96. Available from: http://dx.doi.org/10.1007/978-3-319-07536-5_6.