Volume 7, Issue 6
December 2018

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

A Systematic Review on Evolution of Blockchain Generations

[1,*]Abhishek Srivastava, [2]Pronaya Bhattacharya, [3]Arunendra Singh, [1]Atul Mathur
[1]Naraina College of Engineering and Technology, Kanpur,
Uttar Pradesh, INDIA
[2]Institute of Technology, Nirma University, Ahmedabad,
Gujarat, INDIA
[3]Pranveer Singh Institute of Technology, Kanpur,
Uttar Pradesh, INDIA

E-mail: [1,*]srivastavaabhishek104@gmail.com,[2]pronoya.bhattacharya@nirmauni.ac.in, [3]arun.sachan@gmail.com, [1]hod_cs@narainagroup.net

ABSTRACT

Today world are witnessing a paradigm shift towards distributed applications. This requires applications to be decentralized where data sharing in the form of transactions take place. Thus, security and trust among peer nodes in the network in such environments becomes a critical factor. Blockchain seems to provide a promising solution to such scenarios. Blockchain Technology, which emerged as a digital cryptocurrency since the genesis of Bitcoin, has now transformed as an umbrella solution in decentralizing transactions and providing consensus and trust among participating peers from diverse authoritative domains. This decentralized nature of the blockchain, known as distributed and immutable ledger, has enabled service providers to register, confirm transactions via contracts and transfer credits without the involvement of third parties. In this paper, emergence of Blockchain- starting from Bitcoins to become a solution provider in major domains like finance, Healthcare and Supply Chain Systems is discussed. This paper thoroughly reviews published works on the same and their contributions in form of Blockchain emergence as generations starting from Blockchain 1.0 to Blockchain 4.0.

Keywords: *Blockchain, Cryptocurrency, Smart Contracts.*

1. INTRODUCTION

The new global era has bought a lot of changes in ways we use data. With the shift towards digitalization, new innovations and close customer relations are formed over social networks, smart phones, IoT (Internet of Things), analytics and cloud platforms. New models and architectures are designed to revolutionize this integration of data and customer demands for providing better informed decisions and enrich the user experience. Such huge volume of data in networks brings critical challenges to ensure security fundamentals in a distributed environment. Blockchain, initially introduced as a Bitcoin Cryptocurrency [1] by Satoshi Nakamoto, is today much more than that. It offers a trusted platform for exchange of any service and transaction over a distributed network. Thus, it is revolutionizing the digital economy of today by providing new dimensions to security and efficiency of systems.

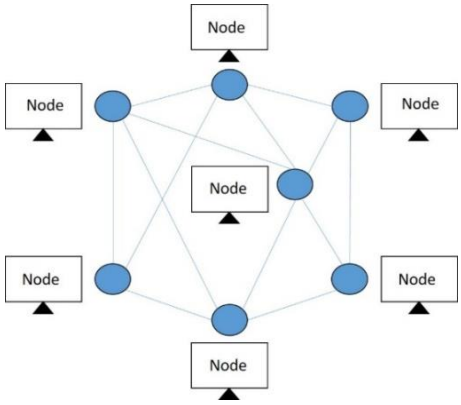

Figure-1: A simplified look of Blockchain architecture

As shown in Figure 1, a blockchain is a distributed ledger over a public or private network that records transactions between peer nodes that do not trust each other. The information or data as transactions are hashed, verified and mined into blocks which are added to the chain by miners based on a consensus mechanism. The addition of blocks is always done to the longest valid chain. This rule of longest chaining allows recorded transactions in blocks to be immutable as any change to the block will change hash value leading to invalidation of blocks. Thus, the valid chain provides a history of transactions as logs which can be verified and created at any moment in the network.

The rapid growth of business processes has led to inevitable requirement of shifting security processes over blockchain networks as they ensure trust and transparency. Today blockchain is gaining more agility as it is integrating in many domains like finance [2-3] in the form of digital assets, remittance and online payments. Also, blockchain is widely used as emerging technology in IoT [4-5], smart contracts [6], healthcare industry [7], voting [8], and verification of educational documents [9].Also, blockchain can be used in a transactional manner in tracking tangible luxury items, intellectual property rights, and many other uses.

The remainder of the article provides a thorough review of evolution of generation of blockchain systems. Section 2 discusses the need and emergence of blockchain in distributed platforms. Section 3 is Blockchain 1.0, which is mainly related to Bitcoin and Cryptocurrency. Section 4 deals with registering and transferring of smart contracts, namely Blockchain 2.0. Section 5 is about extension of Blockchain to various domains like governance and education. This shift is indicated as Blockchain 3.0. Section 6 deals with usage of Blockchain in Industrial sector as a revolution, which is

Volume 7, Issue 6
December 2018

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

named Blockchain 4.0. Section 7 provides the conclusion of the survey and possible research directions.

2. NEED AND EMERGENCE OF BLOCKCHAIN

A. Problems with current centralized and distributed systems

Suppose we want to edit a document over a network. In traditional classical system, we make the required changes and forward it to other person who downloads the copy over network and makes his own changes. This may lead to multiple copies of same data as redundancy and also makes it difficult for us to locate the most recent copy. Also, we have to wait for the other person to make changes and then only we can proceed with our modifications. This is shown in Figure 2.

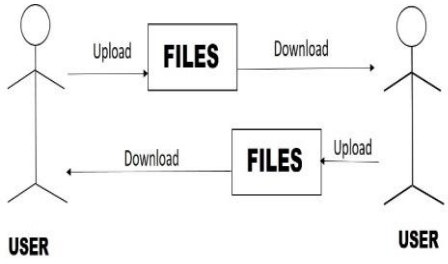

Figure 2: Traditional way of sharing documents

Later a centralized shared system was proposed in which both parties which want to edit the document can share the same space simultaneously as in Figure 3. The shared document in normally on a server called cloud which resolves the issue of recent updated version and waiting time.

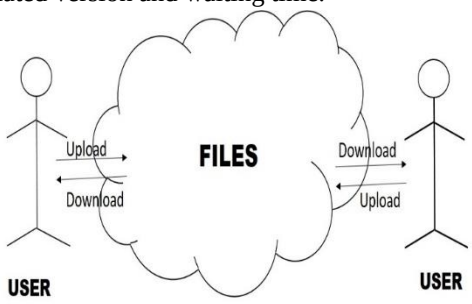

Figure 3: Shared Centralized System

The problems with the current approach are that all data is on a central server and operations are performed based on network connectivity. Thus, cloud based systems faced many challenges. According to a survey conducted by Information Data Centers (IDC) in 2008 [10], the major challenges are identified in cloud based systems are listed in Table 1.

Table 1: Major Challenges in Cloud Based Systems

Parameters	Challenges	Reason
Bandwidth	Insufficient bandwidth with high amount of jitter[11]	Heterogeneous Networks, Low Quality-of-Service(QoS)
Load Balancing and Scalability	Server Crash over encrypted tunnels	Excessive Security Headers, wrong tunnels to route data
Security Attacks	Difficult to maintain CIA(Confidentiality, Integrity and availability) triad.	Central Servers are more prone to hijacks and Denial of Service(DoS) attacks.

Thus, such centralized shared databases are then replaced with distributed databases as they are more robust in event of network failures. However, distributed databases have the following challenges.

Challenges:

1. They mainly operate over synchronous and asynchronous networks, hence packet delivery guarantees is based on remote node which might experience congestion, may fail, or message might wait in queue.
2. The application-specific system might overlook consistency using weak enforcement of ACID properties over scalability normally in case of replication systems.
3. All nodes might not be working as intended, known as a security attack known as byzantine attack, hence the consensus achieved might not be the correct one.
4. Even in cases of highly scalable distributed databases like MongoDB which achieves eventual consistency using a leader election protocol, multi document transactions in parallel are not allowed leading to more waiting times.

B. Emergence of Blockchain as a Solution Provider

Blockchain achieves consistency in transactions by accounting for auditability, atomicity and integrity of data over distributed autonomous platforms, where peer nodes do not trust each other. They are similar to distributed systems where nodes continuously check other nodes integrity using a consensus protocol to agree on a common state of the chain. They chains are cryptographically auditable as they rely on Merkle root value and order-execute architecture in which blockchain network orders the transactions first using a consensus protocol and then executes them in the listed order in all peer nodes in a sequential manner.

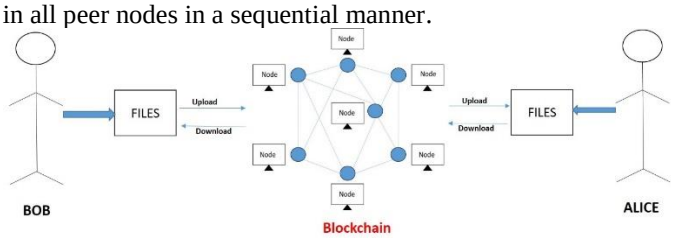

Figure 4: A distributed architecture using Blockchain Network

As shown in Figure 4, the entities (Alice and Bob) involved in the transaction performs update to their local copy of the

Volume 7, Issue 6
December 2018

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

document which is then added by computing the hash value of the document which could be digitally signed using users' private/public key pairs and added to the chain. The validation of the transactions is done by miners which add a block to a chain. This logical chaining is done by the process of hashing of data blocks, where any block B_i stores the hash of its previous block B_{i-1}. The hash in any i^{th} block is computed as $H_i = f(input_i, ID_i, Timestamp, H_{i-1})$ where $input_i$ is the input document, ID_i is the digital identifier associated with the document, *Timestamp* is the current timestamp value and H_i and H_{i-1} are the hashes of current and previous blocks respectively. The blocks link to form a trace back to the genesis block, thus allowing consensus in a blockchain network.

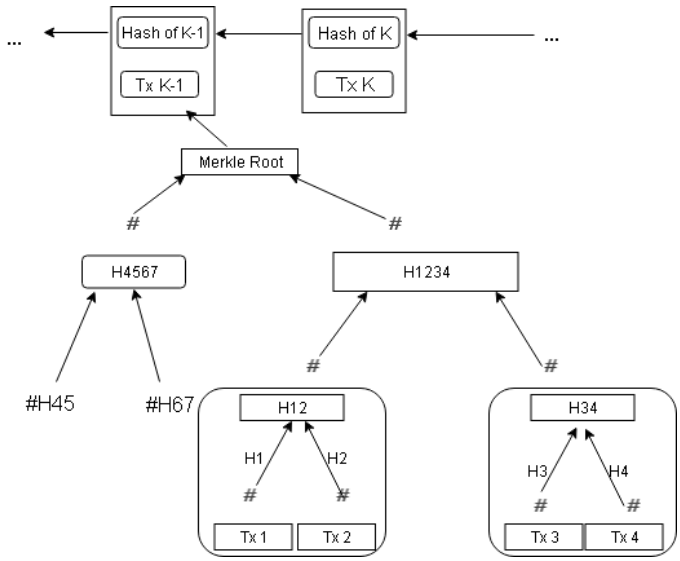

Figure 5: Overview of Blockchain Transactions and Merkle Root

Also as shown in Figure 5, all the hash are computed and used to form the hash at the next higher level in the chain. This is the concept of Merkle tree and the final Merkle value is stored in a block, hence even there is a tamper in one of the blocks, it leads to complete invalidation of all blocks in the path, to the genesis block. This makes the blockchain system 'tamper-proof and secure.

To add a block, a miner must solve a puzzle in a challenge-response environment by guessing starting bytes of the block in such a way that the hash of the block is smaller than the acceptable target hash value. Each block acts a puzzle for a miner which is termed as nonce or difficulty value. Once the nonce is solved by a miner, the block gets appended to the existing validated chain by appending the hash value of the chain to the block. The above concept is also known as "Proof-of-Work (PoW)" in a blockchain network. The copies of the new block are added to all nodes in the network maintaining consensus.

Sometimes, it may happen that miners can unintentionally generate different blocks of same transactions which fork the chain. Thus, forking creates a problem, so as one branch becomes longer, all the miners prefer adding blocks to that branch. This rule of longest chaining increases security in the system as an attacker has to create a branch of the same length of the longest chain in a very short span of time, which requires a lot of computational power and resources. So even if the nodes in the chain do not trust each other or behave in an arbitrary manner, sometimes referred to as Byzantine manner [12], then also at any instant, the state of the chain is considered to be valid. The only possibility is that the blocks are added in a slow manner or there are many fork operations in a chain, which makes it more time consuming to elect the longest chain. In such a case, an attacker can form his chain to be the longest and force the miners to add blocks to his chain making it look like a legitimate chain. Although this is a limitation, the propagation latency of adding of blocks in a network is small, hence the probability of such an attack is almost zero, making the blockchain network very secure in a distributed environment to achieve common consensus. Hence, the blockchain network solves the current limitations of the database system and achieves consistency in a shared and distributed platform.

3. BLOCKCHAIN 1.0: BITCOIN AND CRYPTOCURRENCY

A. Fundamentals of Bitcoin

The emergence of Blockchain defined the state of the distributed ledger as virtual coin, known as Bitcoin Blockchain [1]. This virtual currency allowed users to do financial transactions and is also called the Internet Cash. The currency is named as cryptocurrency as each coin defines an electronic signature where the private key is used for signing the transaction and public key is used for verification. The Bitcoin ledger is a Finite State Transition Automaton, which consists states as ownerships of all existing bitcoin users and their transactions in form of transitions between the states. The output of any particular state is a transactional value if the transaction is successful, which means enough bitcoins (BTC) are present, or error, otherwise. The state transition function takes us to a new state. Every node in the network keeps a copy of this finite state transition system as a ledger record [13].The PoW was carried out using hashing scheme Bitcoin based on HashCash[14] and SHA-256 hash function[15]. Thus, third parties were eliminated in a decentralized anonymous system where a user can control his funds and do transactions.

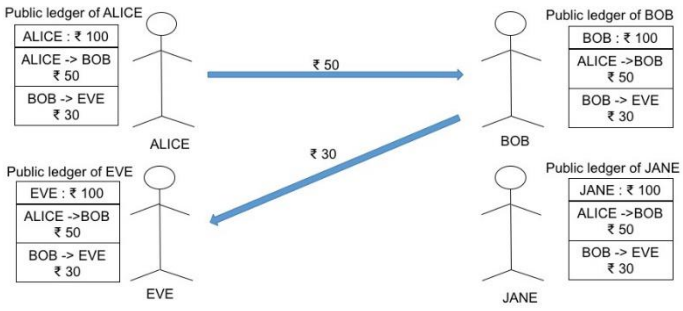

Figure 6: View of Public Ledger to all Peers in a Bitcoin Network

As shown in Figure 6, the users can make transactions by BTC, where the user refers the purchaser to his signature, which is a 16 digit encrypted code. The purchaser decodes the

Volume 7, Issue 6
December 2018

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

code at his receiving device to get the BTC. Thus, the digital currency becomes medium to buy and sell goods and services over anonymous and permission less network. The states of all transactions are reflected to all peers in the network as form of public ledger.

Advantages:

1. Lower transactional cost in comparison to other electronic payment channels.
2. Secure and Transparent transactions with tracking cash, so counterfeiting is not possible.
3. There is a finite supply of Bitcoins, just like gold markets.
4. Relative anonymity in transactions.

Disadvantages:

1. The approvals of transactions are slow in comparison to other electronic channels.
2. Various fraud schemes are launched over Bitcoin wallets like Ponzi Schemes [22], Bitcoin Mining Scams [23], Bitcoin exchange scams and wallet scams[24].

B. Challenges and Limitations in Bitcoin Environment

Bitcoin, with a block size of 1 MB, has scalability issues as only 7 transactions per second can be supported. In comparison, a Visa Network averages hundreds of transactions per second. Thus, Bitcoin, it has to match to this rate, it would require a throughput of 8GB per bitcoin block every ten minutes, leading to data requirements of over 400TB per year [16]. Thus, nodes with high storage capacities will survive in the network, making the scheme centralized. Some solutions like Soft and Hard Forks [17], SegWit [18], Lightning Network [19] were proposed to alleviate the scalability issue. Also, the PoW algorithm is now changed to Equihash [20]. This makes it more scalable and makes mining possible on heavy graphic processors. The nonce is adjusted per block, instead of every 2016 blocks of Bitcoin [21].

4. BLOCKCHAIN 2.0: SMART CONTRACTS AND ETHEREUM

A. Beyond Bitcoin: Ethereum and Smart Contracts

With the shift towards decentralization, the limited capabilities of Bitcoin could not suit the needs of a general purpose application. Thus, a requirement of general purpose development platform was felt. In 2013, Ethereum[25] was introduced which addressed several limitations in Bitcoin Scripting. Ethereum is a blockchain with built in Turing Complete programming language. Thus, it supports all type of transactions, including loops. Ethereum provides a virtual abstraction and anyone can create their own instructions for ownership, the format of the transactions, and define the state transition function.

Ethereum thus paved the way for Smart Contracts, which are small computer programs that live and execute on the blockchain. The work autonomously and execute automatically, based on specific predefined conditions for validation of a transaction. Thus smart contracts reduce the cost of verification, arbitration and fraud prevention and allow transparency.

As shown in Figure 7, a smart contract code is shown on an Ethereum Blockchain which consists of accounts, a 20-byteaddress and a state transition function. Two types of accounts are possible- externally owned (using private key) and contract account (using smart contracts). Smart Contract accounts are further classified into two categories- smart contract code and smart legal contracts [26]. The smart contract code is stored, verified and executed on a blockchain where each transaction consists of nonce, ether balance, contract code hash, and storage root [27-28].

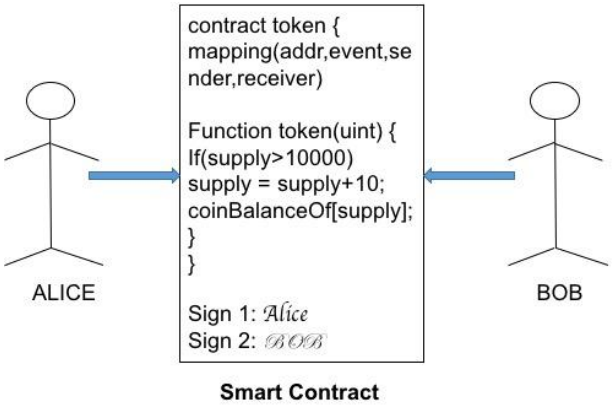

Figure 7: A sample Smart Contract between two entities

Advantages:

1. Smart contracts are accurate and records all terms and condition to minutest explicit detail.
2. Terms and conditions of the contract are fully visible to all transactional involved peers.
3. Smart contracts are interpreted, thus the scripts are executed live on the server, thus transaction executes fast.
4. Businesses are now paper-free, thus smart contracts allow go-green initiative.
5. It eliminates a vast chain of intermediaries as only transaction parties are involved in the contract.

B. Challenges and Limitations in Smart Contracts and Ethereum

Ethereum and Smart Contracts are very popular as they can be extensively applied in many areas, still some serious challenges and limitations are present which makes usage of smart contracts vulnerable. First of all, it is difficult to write smart contracts [29-32]. A smart contract, once it is executing, it is very difficult to modify and terminate the contract [33]. Also, under-optimized smart contracts have little support [34] as programming languages are normally complex[35] to understand and comprehend. Smart Contracts also suffers from Transaction-ordering dependency vulnerability, Timestamp dependency vulnerability, Exception vulnerability and Re-entrance vulnerability [36-37]. Finally, criminals can also leverage smart contracts [38] and privacy issues like transactional privacy [39], data feeds privacy[38,40] and sequential execution of contracts[41] makes the usage of contracts limited. Although, recently Zeppelin Operating System[42], Solcover [43] for Code Coverage for Solidity, ConsenSys [44] for providing list of recommended platforms for development of smart contracts. Security Tools include

Volume 7, Issue 6
December 2018

ITEE Journal
Information Technology & Electrical Engineering

ISSN: - 2306-708X

Oyenete [45], F* Framework for runtime security [46] and Gasper [47] for identifying gas costly programming patterns in the contract. Usage of above systems and tools minimize the effects of vulnerabilities in the contract.

5. BLOCKCHAIN 3.0: CONVERGENCE TOWARDS DECENTRALIZED APPS

As smart contracts are growing every day, the current technology cannot support such volume of micro-transactions. Although, Ethereum improved the transaction rate to 15 tps over bitcoin 7 tps, still it is not sufficient to support today's economy. Hence, Blockchain is currently shifting towards decentralized internet, which will integrate data storage, communication Networks, Smart Contracts and Open standards platforms. Thus, there is need of DApp- which is abbreviation of Decentralized Applications. DApp have their backend running on a Blockchain Network and can have a frontend code and user interfacing in any programming language that can call the backend for functionality support. DApp have the following properties [53]: Open Source platforms for coding support, Internal Cryptocurrency Support, a token that quantifies all credits and transfer in transactions within the system, and Decentralized Consensus mechanisms.

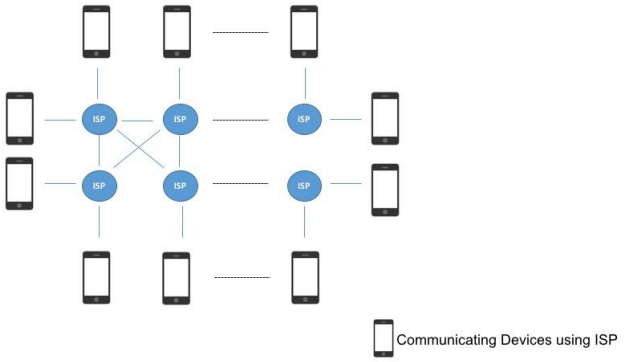

Figure 8: DApp- A Decentralized autonomous Blockchain Governance

The frontend is supported on decentralized storage platforms like mesh network Tangle[48], which is based on Direct-Acyclic Graph(DAG) for validation, EOS[49], an open source platform that provides horizontal and vertical scaling of DApps, NANO [50] for block lattice structures, Andrena [51] open source Internet, ArcBlock [52] to provide a scalable platform for building DApps and many others. Thus, an ultimate blockchain application should be DApp hosted on a peer network as it requires no maintenance and governance, thus enabling no human intervention. This allows for the formation of Decentralized Autonomous Organizations (DAO) [54], in which profit is shared by all members by simply recording their activities on the Chain. The following is shown in Figure 8.

Advantages:

1. No single point of failure as there is no single node controlling the transaction.
2. No central authority owing the DApps Network, even if any intruder tries to manipulate data, it is not possible as the app does not lie on any particular Internet Protocol(IP) address, hence trust on the system is enhanced.
3. The transactional speed is increased about 100 times in distributed environment system.

Disadvantages:

1. Updations and bug fixes are difficult as all copies in the network need to be updated.
2. User Verification is not the governance of any single entity, so Know Your Customer (KYC) process is difficult in comparison to centralized apps.
3. To achieve consensus, complex protocols needs to be implemented to achieve data validation, thus restricting the network scalability.
4. Communication of DApp via third party Application Programming Interface (API) for user information makes communication ecosystem less flexible.

6. BLOCKCHAIN 4.0: SEAMLESS INTEGRATION WITH INDUSTRY 4.0.

The unbounded parallel growth of decentralized applications, we require an umbrella platform that can integrate various services and architectures by allowing cross-chain communications. This will allow users from different platform to work together as one unit, thus making a seamless integration towards business needs and demands of Industry 4.0. The current specifications of Industry 4.0 require an enterprise resource planning platform which can provide automation and integration of different execution platforms as a single coherent unit. This demands for an increasing degree of trust and privacy, thus a scalable Blockchain network is required. This is where Blockchain 4.0 fits, allowing the IT systems to do business integration, operating on Cross-Blockchain business processes like allowing for autonomously placing an order via smart contract as well as ensuring safety to machines. This will support Supply-Chain Managements, Financial management systems, Health and IoT Workflow Management and asset management. Thus, in short Blockchain 4.0 is decentralizing Blockchain 3.0 to operate in real-life industry and business logics to satisfy the requirements of Industry 4.0. This is shown in Figure 9.

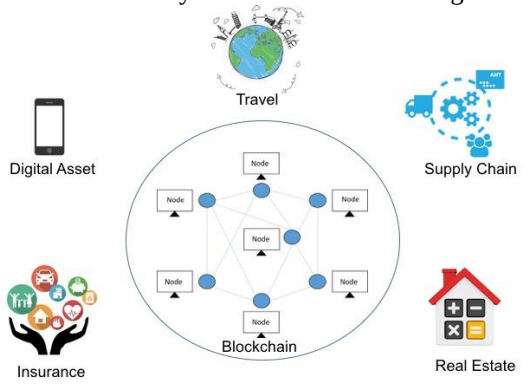

Figure 9: Umbrella Trust and Privacy Solutions provided via Blockchain 4.0

The first platform to support Industry 4.0 is Unibright [55] which allows a unified integration for blockchain business models. Now days, SEELE Platform [56] is providing the unity in blockchain space by enabling cross communication between different blockchain protocols across various services. It allows individual chains within the complex structure to harmonize connection while they themselves operate independently. It operates on a neural consensus algorithm which allows linear scalability and operates both on on-chain and off-chain computing. It also allows transactional speed up to 1M TPS which currently seems impossible in a public blockchain.

7. CONCLUSIONS

The use of Blockchain is not only limited to provide trust and privacy as a means of crypto currency, but be a business provider in current industry and market demands. In this paper, we discussed the need and emergence of blockchain and then we did a systematic and detailed review of various generations of blockchain and how they are eventually shaping out organizational needs. Blockchain is the biggest disruptive technology that has hit the markets and most industries are gradually shifting to blockchain platforms. According to the Global Blockchain Survey 2018 by Deloitte [57], almost 74% of use cases are being implemented and nearly 40% organizations are going to adopt blockchain. In future, we may seem integration of Artificial Intelligence and Blockchain to automate and secure business processes. Thus, the following research areas are proposed that will shape blockchain in near future:

1. Convergence of Blockchain and Machine Learning in providing solutions to business demands in Healthcare, Supply-Chain, Finance, and Maintenance operations.
2. Providing secure approaches to practical solutions of scalability issues in Blockchain in Cloud and Fog Nodes.
3. Providing security for low powered enabled IoT nodes, mainly in Vehicular communication and Healthcare.
4. Development of more secure and powerful cryptocurrency and efficient mining standards.
5. Providing Consensus Protocols for Secure communication in pervasive and Social Networks.

REFERENCES

[1] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008), https://bitcoin.org/bitcoin.pdf.(Accessed on November 2018).

[2] Foroglou, G., Tsilidou, A.L.: Further applications of the blockchain (2015)

[3] Peters, G.W., Panayi, E., Chapelle, A.: Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective (2015), http://dx.doi.org/10.2139/ssrn.2646618

[4] Christidis, K., Devetsikiotis, M., "Blockchains and Smart Contracts for the Internet of Things", in IEEE Access, vol. 4, pp. 2292-2303, May 2016.

[5] Zhang, Y., Wen, J.: An iot electric business model based on the protocol of bitcoin. In: *Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN)*. pp. 184–191. Paris, France (2015).

[6] Kosba, A., Miller, A., Shi, E., Wen, Z., Papamanthou, C.: Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In: *Proceedings of IEEE Symposium on Security and Privacy (SP)*. pp. 839–858. San Jose, CA, USA(2016)

[7] Peterson, K., Deeduvanu, R., Kanjamala, P., & Mayo, K.B. (2016). A Blockchain-Based Approach to Health Information Exchange Networks.

[8] L. Wang, W. Liu and X. Han, "Blockchain-Based Government Information Resource Sharing," In *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, Shenzhen, 2017, pp. 804-809.doi: 10.1109/ICPADS.2017.00112

[9] Srivastava A., Bhattacharya P., Singh A., Mathur A., Prakash O., Pradhan R. "A Distributed Credit Transfer Educational Framework based on Blockchain" In: *IEEE 2018 2nd International Conference on Advances in Computing, Control and Communication Technology(IA3CT 2018)*, Allahabad, Uttar Pradesh, India, 2018(***Article in Press***).

[10] Popovic, Kresimir & Hocenski, Zeljko. (2010). Cloud computing security issues and challenges. 344 - 349.

[11] Zhang Yhing: "Method and System to allocate bandwidth based on task deadline in cloud computing network" in United States Patent Patent No: US 9,923,837 B2 March 20, 2018

[12] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," in *IEEE Transactions on Knowledge and Data Engineering*, vol. 30, no. 7, pp. 1366-1385, 1 July 2018. doi: 10.1109/TKDE.2017.2781227.

[13] Ethereum Community, "A next-generation smart contract and decentralized application platform," White Paper, availableat: Ethereum Community, "A next-generation smart contract and decentralized application platform," White paper, available at: https://github.com/ethereum/wiki/wiki/White-Paper (Accessed on November 2018)

[14] A. Back, "Hashcash – a denial of service counter-measure," 2002,available at: http://www.hashcash.org/papers/hashcash.pdf

[15] D. Eastlake, 3rd and T. Hansen, "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)," RFC 6234 (Informational), May 2011, available at: http://www.ietf.org/rfc/rfc6234.txt.

[16] J. Poon and T. Dryja, "The bitcoin lightning netwiork: scalable off-chaininstant payments,", 2016, available at:https://lightning.network/lightning-network-paper.pdf

[17] A. Castor, "A short guide to Bitcoin forks," March 2017, available at: https://www.coindesk.com/short-guide-bitcoin-forks-explained/(Accessed on November 2018)

[18] Cointelegraph, SegWit explained, available at:https://cointelegraph.com/explained/segwit-explained, (Accessed on November 2018)

[19] S. Sundararajan, "Blockstream launches micropayments processing system for Bitcoin apps," January 2018, available at: https://www.coindesk.com/blockstream-launches-micropaymentsprocessing-system-for-bitcoin-apps/, (Accessed on November 2018).

[20] A. Biryukov, D. Khovratovich, "Equihash: asymmetric proof-of-work based on the generalized birthday problem," Ledger, vol. 2, pp. 1-30,April 2017

[21] Bitcoin Gold Roadmap, available at: https://bitcoingold.org/wpcontent/uploads/2017/10/BitcoinGold-Roadmap.pdf, (Accessed on November 2018).

[22] Bartoletti, Massimo & Pes, Barbara & Serusi, Sergio. (2018). Data Mining for Detecting Bitcoin Ponzi Schemes. 75-84. 10.1109/CVCBT.2018.00014.

[23] N. Hajdarbegovic, Bitcoin miners ditch ghash.io pool over fears of 51% attack, 2014. URL https://www.coindesk.com/bitcoin-miners-ditch-ghash-io-pool-51-attack/, (Accessed on Novemeber 2018).

[24] A. Sraders "Pay Attention to These 7 Bitcoin Scams in 2018", July 2018, available at: https://www.thestreet.com/investing/bitcoin/bitcoin-scams-14640202 , (Accessed on November 2018).

[25] V. Buterin, "Ethereum white paper: a next generation smart contract & decentralized application platform," 2013, available at: http://www.theblockchain.com/docs/Ethereum_white_papera_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, (Accessed on Novemeber 2018).

[26] J. Stark, "Making sense of blockchain smart contracts," Available online at: http://www.coindesk.com/making-sense-smart-contracts/(Accessed on November 2018).

[27] Y. Sompolinsky and A. Zohar, "Secure high-rate transaction processingin Bitcoin," Financial Cryptography, pp. 507-527, 2015.

[28] G. Wood, "Ethereum: a secure decentralised generalised transactionledger, Byzantium version," 2018, available at:https://ethereum.github.io/yellowpaper/paper.pdf, (Accessed on November 2018).

[29] K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, "Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in *International Conference on Financial Cryptography and Data Security*, pp. 79-94, Springer, 2016.

[30] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N.Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, et al., "Formal verification of smart contracts:Short paper," in *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysisfor Security*, pp. 91-96, ACM, 2016.

[31] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, "Validation of decentralised smart contracts through game theory and formal methods," in *Programming Languages with Applications to Biology and Security*, pp. 142-161, Springer, 2015.

[32] C. K. Frantz and M. Nowostawski, "From institutions to code: Towards automated generation of smart contracts," in *2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS*W)*, pp. 210-215, IEEE, 2016.

[33] B. Marino and A. Juels, "Setting standards for altering and undoing smart contracts," in *International Symposium on Rules and Rule Markup Languages for the Semantic Web*, pp. 151-166, Springer, 2016.

[34] T. Chen, X. Li, X. Luo, and X. Zhang, "Under-optimized smart contracts devour your money," in *2017 IEEE 24th International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pp. 442-446, IEEE, 2017.

[35] F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, "Evaluation of logic-based smart contracts for blockchain systems," in *International Symposium on Rules and Rule Markup Languages for the Semantic Web*,167-183, Springer, 2016.

[36] C. Natoli and V. Gramoli, "The blockchain anomaly," in *15th International Symposium on Network Computing and Applications (NCA), 310-317, IEEE*, 2016.

[37] 19.L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16*, pp. 254-269, ACM, 2016.

[38] A. Juels, A. Kosba, and E. Shi, "The ring of gyges: Investigating the future of criminal smart contracts," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, CCS '16*, pp. 283-295, ACM, 2016.

[39] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in 2016 IEEE Symposium on Security andPrivacy (SP),839-858, IEEE, 2016.

[40] F. Zhang, E. Cecchetti, K. Croman, A. Juels, and E. Shi, "Town crier: An authenticated data feed for smart contracts," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, CCS '16, pp. 270-282, ACM, 2016.

[41] M. Vukolić, "Rethinking permissioned blockchains," in Proceedings of the *ACM Workshop on Blockchain, Cryptocurrencies and Contracts, BCC '17*, pp. 3-7, ACM, 2017.

[42] Araoz, M. July 2017. Introducing zeppelinos: the operating system for smart contract applications. https://blog.zeppelin.solutions/introducing-zeppelinos-the-operating-system-for-smartcontract-applications 82b042514aa8, (Accessed on November 2018).

[43] Solcover Link: https://github.com/sc-forks/solidity-coverage,(Accessed on November 2018).

[44] ConsenSys. Recommendations for smart contract security in solidity-ethereum smart contract best practices. https://consensys.github.io/smart-contract-best practices/recommendations/,(Accessed on November 2018).

[45] Luu, L., Chu, D.-H., Olickel, H., Saxena, P., & Hobor, A. 2016. Making smart contracts smarter. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 254–269. ACM.

[46] Bhargavan, K., Delignat-Lavaud, A., Fournet, C., Gollamudi, A., Gonthier, G.,Kobeissi, N., Rastogi, A., Sibut-Pinote, T., Swamy, N., & Zanella-Beguelin, S.2016. Formal verification of smart contracts. In *Proceedings of the 2016 ACMWorkshop on Programming Languages and Analysis for Security-PLAS'16*, 91–96.

[47] Chen, T., Li, X., Luo, X., & Zhang, X. 2017. Under-optimized smart contracts devour your money. In *Software Analysis, Evolution and Reengineering (SANER), 2017 IEEE 24th International Conference* on, 442–446. IEEE

[48] Tangle-IOTA- One Idea Creates Tow Others, URL-https://thinktangle.com, (Accessed on November 2018)

[49] EOSIO- The most powerful infrastructure for decentralized applications URL-https://developers.eos.io (Accessed on November 2018).

[50] NANO- Create Your Own Nano WebWallet, URL-https://nanowallet.io, (Accessed on November 2018)

[51] ANDRENA- Welcome to your new Internet, High-speed Internet, at a fraction of the cost URL-https://andrena.com, (Accessed on November 2018)

[52] ArcBlock- The World's first blockchain ecosystem for building and deploying decentralized application URL-https://www.arcblock.io/, (Accessed on November 2018)

[53] S. Raval, Decentralized applications : harnessing Bitcoin's blockchain technology. O'Reilly Media, 1 ed., 7 2016.

[54] H. Green, "Introducing the DAO: The organisation that will kill corporations," City A.M., May 2016.

[55] Unibright- The Unified Framework For Blockchain based Business Integration, 2018, URL-https://unibright.io, (Accessed on November 2018).

[56] SEELE- All ICO Information about Seele URL-https://icodrops.com/seele/, 2018(Accessed on November 2018).

[57] 2018 Global Blockchain Survey by Deloitte-URL-https://www2.deloitte.com/global/en/pages/energy-and-resources/articles/gx-innovation-blockchain-survey.html, 2018, (Accessed on November 2018).

AUTHOR PROFILES

Abhishek Srivastava is currently pursuing his M.Tech in Computer Science and Engineering from Naraina College of Engineering and Technology, Kanpur, Uttar Pradesh affiliated to Dr. A. P. J Abdul Kalam Technical University, Lucknow, Uttar Pradesh. He has done his B.Tech. in Information Technology from Pranveer Singh Institute of Technology, Kanpur, Uttar Pradesh. His areas of interest includes Network Security and Artificial Intelligence.

Pronaya Bhattacharya is presently working as an Assistant Professor in Department of Computer Science and Engineering at Nirma University, Ahmedabad, Gujarat. He is pursuing his PhD in Computer Science and Engineering from Dr. A. P. J Abdul Kalam Technical University, Lucknow, Uttar Pradesh. He has a teaching experience of more than 8 years as an Assistant Professor in various universities. He has authored papers in various reputed journals and conferences like IEEE and ACM. His areas of interest include Network Security, Machine Learning and Optical Communications.

Arunendra Singh is presently working as an Assistant Professor in Department of Information Technology at Pranveer Singh Institute of Technology, Kanpur. He is Pursuing his Ph.D. in Computer Science and Engineering from Dr. A. P. J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh. He received his M.Tech. from Motilal Nehru National Institute of Technology(MNNIT), Allahabad in 2011 and B.Tech. from Harcourt Butler Technological Institute(HBTI), Kanpur, Uttar Pradesh in 2005. He has published several research papers in highly reputed Journals and conferences like, Springer, IEEE, and ACM. His area of interest includes Network Security, Optical Communications, Computer Networks etc.