Importance of Blockchain technology for the Smart Devices

Sushmita Madishetty[*1] **A. Naveen** [*2] **CH Ramya**[*3]
[*1]BTech Scholar, [*2] Associate professor, [*3]Assistant professor
[*1,2,3]Department of Computer Science & Engineering
[*1,2,3]Nalla Narasimha Reddy Education Society's Group of Institutions

***Abstract*— In today's world, internet applications development demand is very high. So, IoT is a major technology by which we can produce useful internet applications. Some reports on IoT predict that IoT devices will grow to 26 billion by 2020 which is equal to 7.3 billion PC's which are to be expected by 2020. Actually the thought of IoT first became popular in 1999. The versatality of IoT has became very popular in recent times. There are many advantages of having a device based on IoT. Technology has been gaining enormous attention in all the areas.If we name those,we get many. Among those few of them are "blockchain and security, blockchain and finance,blockchain and logistics, blockchain and IoT and so on.**

In this paper, we try to give a clear picture and idea about blockchain and IoT. Both are bigger deals in individual sense.If we combine both, it is biggest deal on internet. In fact, convergence of blockchain and IoT is on the agenda for many companies and there are existing solutions in several areas,outside of IoT too. The goal of this work is to provide detailed description of how blockchains work,pros and cons, the ways in which blockchain and IoT work together.

Keywords*— *Blockchain, IOT, security threat .

I. Introduction

Blockchain is the backbone technology of digital cypto Currency BitCoin. It is a distributed database of records of all transactions. Blockchain technology first came to light when a person or group of individuals name "satoshi nakamoto" published a white paper on "BitCoin: a peer to peer electronic cash system" in 2008.

Usually when many transaction are made or executed,every singke record of each transaction is maintained.Behind all the interactions in network,there is a heavy use of cryptography,blockchain networks etc..so it relates to researchers and developers working in IoT domain.

II. How blockchains work

Technically blockchain is a chain of blocks ordered in anetwork of non-trusted peers.Each block references the previous one and contains data,its own hash and hash of previous block.

BLOCK

A unit of data stored inside a block may be represented by any value depending on type of blockchain.A block can store an amount of money,a share in a company,a digital certificate of ownership,a vote during an election,or any other value.

HASH

Each block has a hash. This hash is value generated from a string of text using a mathematical function. A hash can be compared to a fingerprint,as each hash is unique. Its role is to identify a block and the block's contents. Hash indicates change to block.

HASH OF PREVIOUS BLOCK

If any changes are made to the single hash,then whole chain is invalid.

There are some key features to go through to know the working of blockchain.They are:

1. Blockchain keeps a record of all data exchanges.
2. It utilizes a distributed system to verify each transaction.
3. Once signed and verified,the new transaction is added to blockchain and cannot be altered.

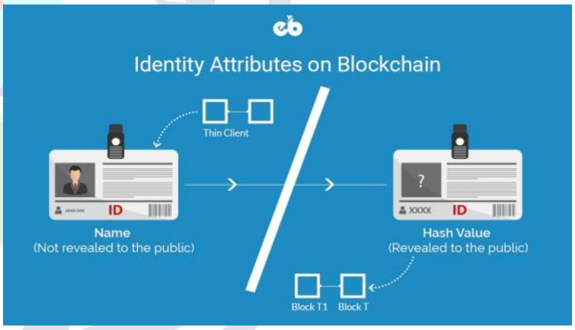

Figure 1: Identity atrributes on blockchain

So,with the set of cryptographic keys,we get a unique identity. Usually keys would be public key and private key which are together combined to give digital signature. Public key defines how others are able to identify you. Private key gives you the power to digitally sign and authorize different actions on behalf of this digital identity when used with your public key.

Also blockchain is a shared public ledger on which the entire BitCoin network relies.All confirmed transactions are included in the blockchain.It allows bitcoin wallets to calculate their spendable balance so that new transactions are verified there by ensuring they are actually owned by spender. The integrity of blockchain is determined by Cryptography.

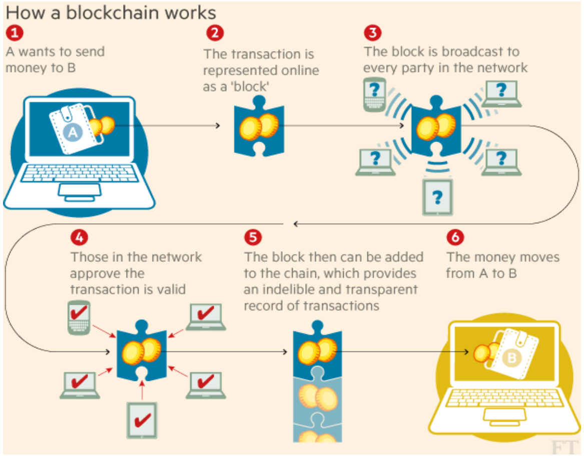
How a blockchain works
1
A wants to send money to B
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
A
B
FT

Figure 2: working process of blockchain

III. PROOF- OF-WORK

It is a process of producing data that’s hard to get but easy to verify. In the context of blockchain, proof-of-work is about solving mathematical problems added to the blockchain.On average, performing proof-of-work calculations and adding a new block to the chain takes about 10minutes.

Proof-of-stake(PoS) is an alternative of Proof-of-work(PoW)

which requires far fewer CPU computations for mining. In PoS, the chances of a node mining the next block are proportional to node’s balance. PoS has their own strengths and weaknesses and its very complex.

Proof-of-work solves a puzzle in which the node can have its assembled block to be its next mining block on the network and also if they find right random number in that blocks header leading to no of zeros that network would never expect. Also if two forks compete, there might be a chance of generating next block simultaneously. So in order to resolve this, proof-of-work tells us to adopt a fork which has greatest amount of work.

There are few algorithms to discuss. They are PBFT, BFT, RIPPLES CONSENSUS ALGORITHM etc..So starting with PBFT-practical byzantine fault tolerance is one of the algorithm to solve byzantine generals problem which occurs in internet. It is a three phase protocol where primary node acts as block miner.View change mechanism is used when it exhibits byzantine faults. Next, BFT-byzantine fault tolerant which provides tighter guarantee that if results at client side are almost faulty by using round robin manner or other techniques related.

And the last.. RIPPLE’S CONSENSUS ALGORITHM uses UNL(unique node lists). It deals with BFT tolerant systems.In order to reach consensus, a node requires to query its own UNL instead of whole network.

IV. BIOT APPLICATIONS

There are many versions of block chain. Blockchain 1.0 (first blockchain application started with this). Blockchain 2.0 (smart contracts). BlockChain 3.0 (related to efficiency,justice etc). So,beyond cryptocurrencies and smart contracts,few of the blockchain technologies where IoT applications are involved are.. sensing, data storage,identity management, timestamping services, smart living applications, intelligent transport systems, wearables, supply chain management, mobile crowd sensing, cyber law and security in mission critical scenarios.

The concept called Etherium which is the most popular blockchain based platform for smart contracts.The system stores public keys in Etherium and private keys are saved on each IoT device.

BIoT applications related to agriculture are tracking Chinese agri-food supplies which is based on RFID (radio frequency identification) and also blockchain related to logistics.Related to healthcare, IOT sensors are used where we check public accessibility to temperature records in the pharmaceutical supply chain. Also used in clinical trials, precision medicine,generic smart health care system.

V. BLOCKCHAIN TAXONOMY

The diversity of blockchain research and development provides an opportunity for cross-fertilization of ideas and creativity, but it can also result in fragementation of the field and duplication of efforts. One solution is to establish standarised architectures to map the field and promote coordinated research and development initiatives. However in terms of blockchain software architecture design, little has been proposed so far and the problem of consistently engineering large and complex blockchain systems remains largely unsolved. We approach this problem by proposing a component based blockchain taxonomy starting from a coarse-grained connector-component analysis.The taxonomy compartmentalizes the blockchain components and establishes relationships in a hierarchical manner. We adopt reverse engineering approach to unbundle the blockchains and divide them into main components.If necessary,each main component is divided into sub and sub sub components. By deriving the logical derivation or elationship between main and sub components,the study helps to clarify the alternative modus operandi of the blockchains and helps to develop conceptual blockchain design.

Discussion

The developed taxonomy serves as a bridge between blockchain technology and blockchain application areas. The taxonomy constitutes a tool to connect technical blockchain characteristics across a range of foundational application cases. There are five principal findings. First, application areas in the taxonomy are at different maturity levels. Financial transactions constitutes the most mature application area and is supported by existing proofs of concept. Smart contracts have found much attention because of the idea to execute agreements on blockchains instead of third parties. Data management gains momentum because of emerging application cases. Storage, communication, and ranking on blockchains are less prevalent. Blockchain scalability issues prevent storage of data on blockchains. The value of applying blockchains for communication and ranking is specific to each application case. In particular, it is challenging to support mobile devices when energy-consuming consensus mechanisms and the transfer of the whole transaction history are required.

Second, application cases inside one application area vary in the dimensions reading access, writing access, main consensus mechanism, and anonymity level. The characteristics in these dimensions depend on the required levels of decentralization for application cases. The more centralization is required, the more private reading access and the more permissioned writing access is required. Main consensus mechanism and anonymity level follow the required level of decentralization so that the more centralization is required, the less energy-consuming are consensus mechanisms and the less anonymous are nodes.

Third, to classify application areas, we reveal new technical dimensions that are overlooked in extant technical classifications on blockchains due to its predominant focus on the financial sector. The new dimensions are event handling, data exchange type, encryption, and history retention. Custom event handling specifies smart contracts. Data exchange type allocates whether data is stored on or off blockchains. Encryption is different between application cases that require to store content or transactions on blockchains. History retention is different for application cases that store blockchains on small-capacity external devices and have to remove old information from blockchains.

Fourth, not all and different technical blockchain characteristics are suitable for different application areas. For example, communication systems based on private permissioned blockchains do not appear to create additional value compared to peer-to-peer messengers such as Telehash, which are used by many decentralized services (e.g., IBM Adept). However, this statement requires further investigation.

Fifth, the taxonomy purposefully avoids the classification of poorly developed blockchain-based systems because blockchain application cases are identified and related to unique and effective combinations of technical characteristics. Therefore, blockchain-based systems that are not captured by the taxonomy might represent application areas that are unsuitable for blockchains. Combinations of technical characteristics that contradict the taxonomy can lead to inefficient technical designs. Inconsistencies between application areas and technical designs may indicate a lack of compliance with technical and application requirements. However, the taxonomy is only based on extant knowledge in research and practice and this assertion requires further research.

There are three promising areas for future research. First, research that replicates our research approach with more or different scientific and business sources will be useful to falsify or corroborate our findings. Second, further analysis of theoretical findings allows to hypothesize about the relationships between application areas and technical blockchain characteristics. Third, research that focuses on socio-economic concepts different from application areas, for example, market regulations in different countries will be useful to contextualize the taxonomy for different industries and domains.

This study is not without limitations. First, the taxonomy cannot identify application areas that may emerge in the future. The rapidly evolving nature of the blockchain domain will necessitate an extension of the taxonomy with new application cases. Second, the identified application areas do not directly capture more complex services, such as prediction markets or crowdsourcing platforms; instead, we decided to break complex application cases down into the basic functionalities that can be performed by blockchains.

This research contributes to the scientific literature on blockchain in three ways. First, allocation of blockchain application cases based on technical blockchain characteristics reduces the hype around blockchain application possibilities. A classification of application areas that, along with semantic differences, is based on technical characteristics make the identification of application areas more meaningful. The well-studied financial sector can serve as a good example for how to leverage blockchains in less studied application areas and the other application areas may reveal opportunities that have been overlooked in the financial sector. Second, we identified additional technical dimensions of importance in the blockchain domain. While some of the taxonomy dimensions (reading access, writing accesses, main consensus mechanisms, and anonymity level) align with previous taxonomies, the remaining dimensions (event handling, data exchange type, encryption, and history retention) represent specific application areas and complement previous taxonomies by offering more comprehensive insights into the technical nature of blockchains. Therefore, technical research can go beyond the Bitcoin blockchain and focus on other areas, for example, development of a blockchain-based protocol for data transmission in healthcare. Third, previous taxonomies consider technical knowledge [17] or application knowledge [12] separately. Our taxonomy combines the knowledge, which allows to bridge the gap between extant technical and application research streams on blockchain. Linking application areas and technical characteristics informs step-by-step guidelines for leveraging blockchains across application areas. Such guidelines might be useful for further development of successful blockchain-based systems.

This research contributes to practice in three ways. First, we present further evidence that blockchains are not only applicable to the financial sector, which is the focus of the majority of blockchain projects but also for other promising areas. Thus, other industries can use blockchain advantages for resolving their challenges. For example, in the media industry blockchain-based data management may be useful to monitor the use of media content to prevent copyright infringements. Second, we highlight other blockchain characteristics besides the widely-known public blockchains that can be useful if public blockchains cannot be employed. Businesses may consider implementation of private blockchains that store information in a more reliable way. Third, we have proposed the taxonomy of blockchain applications to guide development of more successful blockchain-based systems. The taxonomy establishes an overview of blockchain applications, organizes them in application areas, and relates them to technical blockchain characteristics. Furthermore, the taxonomy can be used to avoid poorly designed blockchain applications. This might be useful for practitioners to identify the more promising blockchain projects and assess risks during blockchain implementation. For example, chief information officers could learn which modules in the enterprise information systems landscape can be realized on blockchains and developers could learn which peer-to-peer system prototypes are worth to be develop on blockchains.

VI. Deployment

Unlike a software application created for an individual company, a blockchain network based application involves a potentially large number of parties all coming together to collaborate and compete within the network. As such,it requires careful considerations before deployment.

Considerations are:

1. how will the governance of the network operate?
2. what policies need to be set?
3. how will participants manage keys?
4. what happens if keys are lost or stolen?
5. how will participants host nodes?
6. how will the pricing work?

VII. CONCLUSION

Blockchain is a new name in the world of technologies but it is definitely the one to last. Even in the early stages, the technology has gained huge popularity starting with their very first application of cryptocurrencies. More areas of applications are being discovered and tested with each passing day. Once the technology is adopted and accepted on a global level, it'll transform the way we live today.

REFERENCES

[1] Singh, Dhananjay, Gaurav Tripathi, and Antonio J. Jara. &quot;A survey of Internet-of-Things: Future vision, architecture, challenges and services.&quot; Internet of Things (WF-IoT), 2014 IEEE World Forum.

[2] Atzori, and Morabito, "The internet of things: A survey", Computer Networks, 54(15), 2787–2805, 2010.

[3] Humayed, Abdulmalik, &quot;Cyber-Physical Systems Security—A Survey.&quot; arXiv preprint arXiv:1701.04525 (2017).

[4] Meinel, Holger, and Wolfgang Bösch, &quot;Radar Sensors in Cars.& Automated Driving. Springer International Publishing, 2017. 245-261.

[5] Uden, Lorna, and Wu He, &quot;How the Internet of Things can help knowledge management: a case study from the automotive domain,& Journal of Knowledge Management 21.1 (2017).

[6] Sot iriadis, Stelios, Kostantinos St ravoskoufos, and Euripides GM Pet rakis, & Future Internet Systems Design and Implementation: Cloud and IoT Services Based on IoT-A and FIWARE.&quot; Designing, Developing, and Facilitating Smart Cities, Springer International Publishing, 2017. 193-207.

[7] http://www.informationsecuritybuzz.com/expert-comments/symantec-report-hijacked-iot-devices-ddos/

[8] On Public and Private Blockchains, "https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/,"2017

[9] IOTA http://iotatoken.com/

[10] Machine-to-Machine, https://en.wikipedia.org/wiki/Machine_to_machine

[11] Madhusudan Singh, "Perspective, Challenges, and Future of Automotive Security Enriched with Blockchain Technology", IEEE Transportation Electrification Community Webinar-Abstract,06 Dec, 2017. https://register.gotowebinar.com/register/6157413934050745602

[12] Understanding Autonomous Organizations on the Blockchain https://www.linkedin.com/pulse/understanding-autonomous-organizations-blockchain-paul-kohlhaas

[13] C. Decker and R. Wattenhofer, "A fast and scalable payment network with bitcoin duplex micropayment channels," In Stabilization, Safety, and Security of Distributed Systems pages 3–18. Springer, 2015

[14] Das, Manik Lal, &quot;Privacy and Security Challenges in Internet of Things,& Distributed Computing andInternet Technology. , pp 33-48, 2015.

[15] Joseph Bonneau, "Research Perspectives and Challenges for Bitcoin and Cryptocurrencies," IEEE SECURITY AND PRIVACY (forthcoming May 2015), http://www.jbonneau.com/doc/BMCNKF15-IEEESP bitcoin.pdf.