Blockchain Application on Internet of Things

Ming Lyu

July 26, 2018

Abstract

IoT - Internet of Things - is one of the next biggest evolutions is history, where human-to-human, human-to-machine, and machine-to-machine communications are all supported. Blockchain, an innovative technology, is the key to solve many problems like deficient architecture raised by IoT network. Although most applications of blockchain are around cryptocurrencies, blockchain technology brings the future of IoT in fields like healthcare, finance, transportation and many others to a higher level than the common client-server model due to blockchain's features of security, decentralization, and transparency. In this paper, we will present the current situation of IoT and blockchain technology and how blockchain technology will strength Internet of Things in various aspects.

1 Future of Internet of Things

According to Intel[1], the number of connected IoT devices will reach 50 billion by 2020. With sensor tagged, each connected device is part of the Internet. Data can be collected by these smart devices to be shared, analyzed and exported in real time. Alec Scott[2] mentioned that there are eight ways that Internet of Things can improve our lives including transportation, healthcare and so on. For example, with the development of Internet of Things, autonomous cars are able to receive data like driving speed more frequently and make adjustments on the road more rapidly, reducing traffic and obtaining safety.

At the age of artificial intelligence, IoT will become more powerful. AI-powered IoT help improve operational efficiency as well as reduce cost and time. With billions of devices connected, the volume of data will grow exponentially. It turns out that regular tools cannot handle such large amount of data. Machine learning is one of the tools that open the gate of Internet of things. With huge amount of real-time data, machines are better at analyzing the data and making decisions than human-beings. According to Deloitte, predictive maintenance can reduce the time required to plan maintenance by 20–50 percent, increase equipment uptime and availability by 10–20 percent, and reduce overall maintenance costs by 5–10 percent.[3] AI-powered IoT has huge potential to bring industries to a higher level.

However, there are problems raised by Internet of Things. One of the biggest problems is security. Low-level devices (like home routers) are not the same as personal computers. Malicious party is more likely to target IoT devices rather than computers as IoT business grows. These IoT devices can be infected with malware and used to launch DDoS attacks (Distributed Denial of Services).[4] Centralization is another problem for Internet of Things. Since most of the data are stored in cloud servers, the loss of take-down of a single cloud server is immeasurable.

Blockchain Technology will help solve these problems, which will be mentioned in **Section 3**.

2 Blockchain Technology and DAG (directed acyclic graph)

2.1 Bitcoin and Blockchain

Blockchain technology was introduced in 2008 as a distributed ledger technology, a platform for transactions of a well-known cryptocurrency, Bitcoin. Blockchain allows users to transfer tokens (bitcoin) over a peer-to-peer network (P2P) without regulation and maintenance of a third trust party or central authority.

Proof of work is implemented as a way to reach a consensus over the whole network. Each node in the P2P network competes to solve a puzzle to mine a block using computational power. The first person who solves the puzzle broadcast the solution to the whole network, meanwhile earning the reward for that. The whole network will update the block to their own copies of blockchain, thus creating a blockchain on consensus. There are limited number of bitcoins, and when nodes are not able to get rewards from mining, they are rewarded transaction fees of transactions added to the mined block.

In the blockchain, each block has a hash, which contains the hash of the previous block. This feature makes blockchain immutable. Changing the hash of one block requires changing the hash of all previous blocks, which requires huge amount of computational power to do and it is nearly impossible to succeed when the length of the blockchain is long enough.

The main idea of Blockchain technology is to substitute trust (like a third trust party) with cryptography. Blockchain Technology also achieves the goal of immutability and transparency. Figure 1 is a typical version of Blockchain.

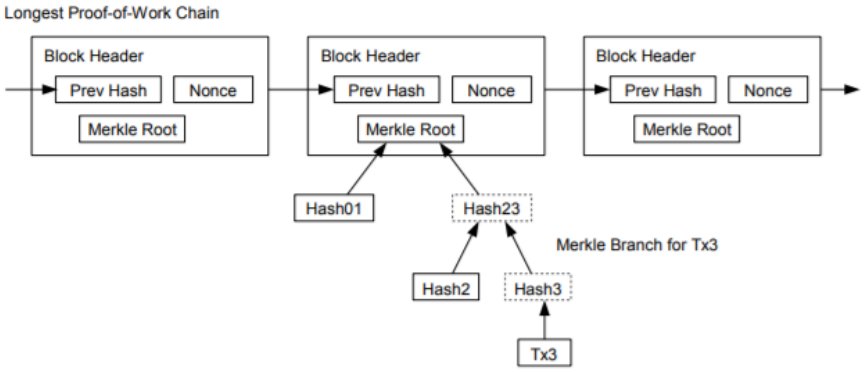

Figure 1: Blockchain Breakdown[5]

2.2 IOTA and DAG (directed acyclic graph)

IOTA is a new type of DLT, using directed acyclic graph instead of a single chain. IOTA's incentive algorithm works differently than Bitcoin. In the P2P network, when a node wants to add a transaction to the graph, it needs to verify another two transactions in the tangle and link the new transaction to those two. It gets rids of mining reward, allowing micropayments since there is no transaction fee involved.

Efficiency is IOTA's another feature. Blockchain right now can handle a max of 7 transactions per second. It is relatively slow comparing to average 2000 transactions handled by Visa per second.[6] IOTA right now can handle about 500 transactions per second. With more users participating in the network, IOTA is able to handle more transactions per second. With more users' verifications on transactions, nodes are able to verify them faster and add new transactions faster as well. Blockchain cannot break its bottleneck since there is 10-minute-gap before a new block can be added to the blockchain.

IOTA scales better than Blockchain. When a transaction is verified directly or indirectly enough times, the network will think them as valid transactions. Then, these transactions can be "buries down" as a layer and become immutable. IOTA will start a new snapshot, saving space for new transactions.

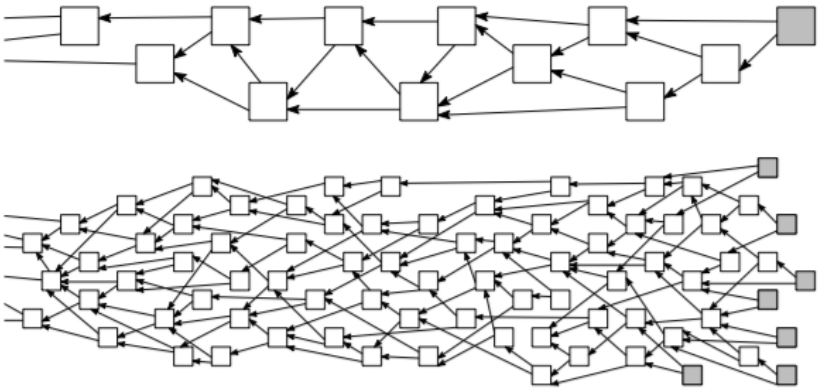

Figure 2: DAG Breakdown[7]

2.3 Conclusion

Here is a comparison between bitcoin and IOTA.

Comparison Table among Bitcoin, Ethereum, EOS, IOTA and PAYMON

Features	Bitcoin	Ethereum	EOS	IOTA	Paymon
Ticker	BTC	ETH	EOS	MIOTA	PMNC
TPS (Transaction per second)	7 tps	13-15 tps	100 000 tps (on testnet)	★Unlimited (2,5mil TPS on mainnet)	★Unlimited
Transaction confirmation	~30 minutes-16 hours	~1 minute	<1,5s	★Instant	★Instant
Block time	10 minutes	15 seconds	3-40 seconds	★No Block	★No Block
Transaction fee	Dynamic	Dynamic	★Free	★Free	★Free
Gas price		20 gwei	2 gwei	★Free	★Free
Blocksize	1Mb	Dynamic	Dynamic	★No Block	★No Block
Blockchain type	Public, decentralized	Permission less, public, private, non-systematic	Permissioned, Private Decentralized	Permission less Decentralized	Permission less-Decentralized

Figure 3: Bitcoin and IOTA Comparison[8]

3 How Blockchain Technology will Strengthen IoT

3.1 Data Security and Availability

As we mentioned in **Section 1**, one of the problems of Internet of things is its security. The immutability of Blockchain provides IoT business a way to store the data securely and reliably. In order to prevent the attack like DDoS, we could use blockchain-based identity and access management systems.[4] Every valid device is added to the system. Once the device is registered to the system, it is hard to tamper with them due to blockchain's immutability.[9] The traditional way of security IoT devices is to implement security software into them and connect them through Internet. Then we have the problem of how to update them fast and efficiently. Besides, implementing such software to IoT devices might cause them to run slower.

Once IoT devices are guaranteed to be valid, transactions can be added to another layer of blockchain protocol. When transactions are added to this layer, they can never be altered. Data integrity is achieved. In IoT applications, data integrity is essential, usually provided by third-parties.[10] Use of blockchain-based IoT business eliminates the need for third-party, avoiding such dependency. Although there are situations like 51 percent attack, it is nearly impossible because of the huge amount of computational power needed.

Data availability is implemented directly by blockchain technology. Since it is a distributed system, every node owns a copy of the blockchain. They can work on their own copies regardless of what happened to the other nodes (nodes being attacked,etc.) While the node is under consensus with the whole network, it is more convenient to work locally rather than retrieving data from cloud servers or central databases. Besides, blockchain technology allows users to search for data that they are interested without the restraints of central cloud servers. IOTA's tangle has the potential to become smart applications' data providers. Bogdan Cristian FLOREA[11] uses Raspberry Pi as a sensor to collect data. The data is formed into JSON (JavaScript Object Notation) messages, which is assigned a tag. Then, the message is attached to the tangle system. The tag acts like an identification, allowing end users to search for data that they want. It is a simple and successful case of using blockchain technology for Internet of things Business. Furthermore, IOTA's team has launched a data market program, which is, in my perspective, a bigger version of the model I mentioned above. They are all bases for Internet of Things.

3.2 Centralization vs Decentralization

Cloud server is the common model to store data nowadays. However, with the rapid growth of Internet of Things business, the space required is beyond expectation. With centralized cloud servers, single point failure at any time causes big problems. It could the problem mentioned in **Section 1** due to cyber attacks, or cloud servers are sometimes down due to software bugs, power, cooling, or other problems.[4] This makes services of cloud server unavailable. Decentral-

Table 1. How blockchain can address Internet of Things (IoT) challenges.

Challenge	Explanation	Potential blockchain solution
Costs and capacity constraints	It is a challenge to handle exponential growth in IoT devices: by 2020, a network capacity at least 1,000 times the level of 2016 will be needed.	No need for a centralized entity: devices can communicate securely, exchange value with each other, and execute actions automatically through smart contracts.
Deficient architecture	Each block of IoT architecture acts as a bottleneck or point of failure and disrupts the entire network; vulnerability to distributed denial-of-service attacks, hacking, data theft, and remote hijacking also exists.	Secure messaging between devices: the validity of a device's identity is verified, and transactions are signed and verified cryptographically to ensure that only a message's originator could have sent it.
Cloud server downtime and unavailability of services	Cloud servers are sometimes down due to cyberattacks, software bugs, power, cooling, or other problems.	No single point of failure: records are on many computers and devices that hold identical information.
Susceptibility to manipulation	Information is likely to be manipulated and put to inappropriate uses.	Decentralized access and immutability: malicious actions can be detected and prevented. Devices are interlocked: if one device's blockchain updates are breached, the system rejects it.

Figure 4: IoT challenge and Blockchain solution[4]

ization of validating transactions prevents a single point of failure mentioned above. When validating transactions comes to a large scale (about 1000 times than today by 2020), it is hard to believe that they can be all handled by third parties.

After Edward Snowden's leakage on PRISM, the public realizes that central authorities cannot be fully trusted. If Internet of Things business is based on a cloud-server architecture, privacy will be fully exposed. Decentralization prevents data from being controlled by a small party, giving public opportunity to decide how to use their own data. Imagine a house full of sensors. While all these sensor's data is stored in a cloud server, where the government can access them at any time. "You are being watched." A sentence from *Person of Interest* could be the reality of tomorrow. For instance, consider the water crisis in the city of Flint, Michigan, which began in 2014. The Michigan officials were suspected to change the sample data. They indicated that the water was safe to drink. The truth is that the water lead concentration is above the safety line and is not suitable to drink. We do not know how many of these are happening but with blockchain, it is impossible to do that. Centralization is good to the most part, and I think we still need decentralization as a part to prevent such problems.

3.3 Cost and Efficiency

Although in terms of data storage, blockchain type technology does not do well as the traditional database. The reason is that every node in the P2P network has a copy of the blockchain, which overall increases the space for data storage. However, blockchain allows real-time control and supervision with the help of smart contracts. There is an unbalance between energy production and energy demand.[12] Blockchain-based solution reduces the surplus of energy

production. According to [12], the decentralized management system is capable of timely adjustments of the energy demand in near real-time by enacting the expected energy flexibility levels and validating all the DR agreements. In my perspective, this strategy can be applied to many other fields, where there is a surplus of energy production.

Talking about efficiency, IOTA does a better job than Blockchain technology. Although IOTA right can handle about 500 transactions per second, which is inefficient compared to 2000 transactions of major trust third party like Visa. However, Figure 4 shows how transaction time will vary based on the number of transactions for IOTA's tangle. The more transactions the system has, the more efficient tangle will be. The reason is that nodes in the P2P network are working on its own part of tangle, thus expanding the tangle while more users participate in the network. In Internet of Things, suppose that all the machines are users in the P2P network of tangle and transaction time is almost neglectable. It turns out that machine-to-machine payments can be made in an instant.

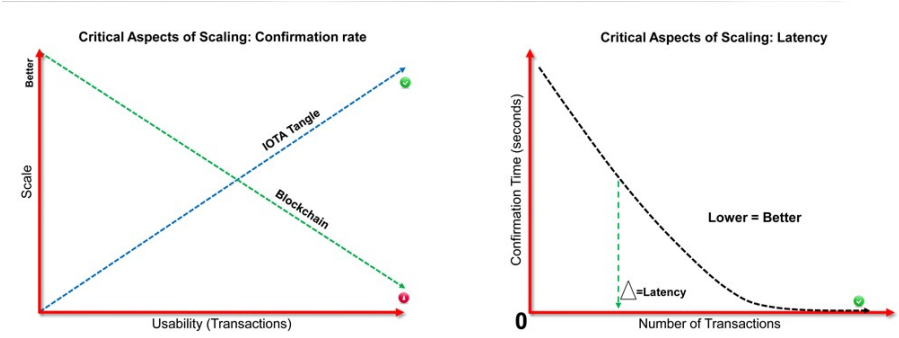

Figure 5: Tangle vs Blockchain Scalability and Transaction Time[13]

3.4 Common Platform

Blockchain Technology is suitable for a common platform for different types of smart devices. Although devices are connected in some sort of way, there is a need for common protocol. For example, different manufacturers have different types of sensors. It results that the consumer's devices are limited to their manufacturers' network. It sounds weird when Ford's vehicles can only use Ford's charging station. Blockchain and Tangle especially Tangle make cross-connection possible.

IOTA's tangle allows micropayments as well. Without mining, IOTA's support transactions without fees. "You are waiting at a red traffic light; your car is being recharged automatically via a smart recharging solution under the surface of the street. After only 10 seconds, the light turns green and you drive

on. If you wanted to pay this with other crypto coins, fees would be higher than the charged power. With IOTA, you can even pay these tiny amounts without having to pay any fees. And it can be done in seconds without any scaling problems."[14] There could other sceneries like parking for few minutes and so on.

4 Independent Study

Before I started the research, I have heard about Bitcoin and studied a little bit about blockchain and cryptocurrency. I am pretty new in this field. The first article I read is Michael Nielsen's *How the Bitcoin protocol actually works.*[15] It is a great article for beginners to learn about Bitcoin and reasons behind design. It connects hash function, cryptography, proof of work and double spend problem. Michael Nielsen starts from nothing, building a new cryptocurrency called "infocoin" based on needs as a simulation of how Bitcoin is created. A transaction is not considered confirmed until: (1) it is part of a block in the longest fork, and (2) at least 5 blocks follow it in the longest fork. Combination of such rules and proof of work tend to prevent double-spend problems. However, Michael Nilsen omits the details of Merkle Tree, which is a data structure used to store transactions.

After reading this article, My advisor Dr.Chenette talked with me about what functions Bitcoin uses for its protocol. There are several hash function families – SHA-1, SHA-2, and SHA-3. SHA-2 is most widely used. Since it is a one-way encrypted, it can not be decrypted unless using brutal force. Hash function SHA-2 is also fast and strong collision-free. Bitcoin right now uses SHA-2 as the hash function for its Merkle tree. Dr.Chenette also mentioned how digital signature works in the Bitcoin protocol. Public keys are used to encrypt data and message and on matching private keys can be used to decrypt them.

After knowing some parts about Bitcoin, I decide to read about Bitcoin original white paper.[5] The first thing that interests me is how Merkle Tree works. The Merkle Tree's root is a hash of all the hashes of the transactions. While some old transactions are not often used, only the root of the tree is saved for the purpose of saving disk space. Satoshi also simulates what is the probability of malicious party catching up from different numbers of blocks behind. The result showed that the possibility is quite low and thus proves that blockchain is secure enough. There is one exception, where the attack owns 51 percent of the computational power.

Then, I started to look at attacks that could be applied to Bitcoin\Blockchain. The most famous one is 51 percent attack. This attack has nearly 100 percent success rate. The attacker can hard fork the blockchain even after 6-block-confirmation rule mentioned above. The reason is that after the honest transaction is confirmed by 5 other transactions, the attack can choose to add blocks to the diverging transaction and create a new longest chain. The new longest chain contains the double-spend transaction. The attacker owns 51 percent of

the computational power of the whole network and he will likely always to be the first one to solve the hash and then own the block. The next one is Finney attack. The attack is quite costly because there is a time gap between the generation of the block by the attacker and completing transaction A, during which someone else on the network could generate a valid block and broadcast it, thus invalidating the valid block generated by the attacker. I not sure I understand it right. If the premined block is not broadcast to the rest of the network, the miners do not know someone solved the puzzle. (They will keep on working to solve the puzzle). If the second person solves the puzzle and broadcast it to the rest of the network, the attacker is not able to put "evil" transactions into the block since the block is controlled by the second person who solved the puzzle. (the second person broadcast it). Or the block does not have to be the attacker's specific one. It could be other ones that are valid. (makes the attacker's one invalid since he has to resolve the puzzle to get the new hash). So suppose the time gap from he generates the block to completion of the good transaction is t. The average time to find a new block is T. Then we have a probability of t/T that attacker fails. The logic here feels right as t increases, the attacker is more likely to fail and t/T increases.[16]

After a thorough research on Bitcoin, we decided that we can look into other kinds of cryptocurrency. Ethereum is another good option. Instead of using Proof of Work, Ethereum uses Proof of Stake as its consensus algorithm. In general, a proof of stake algorithm looks as follows. The blockchain keeps track of a set of validators, and anyone who holds the blockchain's base cryptocurrency (in Ethereum's case, ether) can become a validator by sending a special type of transaction that locks up their ether into a deposit. The process of creating and agreeing to new blocks is then done through a consensus algorithm that all current validators can participate in. Comparing to Proof of Work, Proof of Stake saves so much energy and is more secure to some extent. The algorithm will randomly select a validator based on the size of their stakes. To form a 51 percent attack, the attacker needs to hold 51 percent of the currency and it is nearly impossible. Besides, Ethereum allows developers to write their own smart contracts. The network of nodes will only validate transactions if certain conditions are met through smart contracts. However, there are limitations to smart contracts in terms of regulation. Since smart contract cannot be changed once it is created, there is no guarantee that the smart contract created does not have a loophole. It is hard to detect those loopholes.

After searching for several cryptocurrencies, IOTA came into my mind. IOTA uses DAG instead of a traditional blockchain. When a new transaction arrives, it must approve two previous transactions. The advantage of tangle over blockchain is that it is much faster than blockchain, and it allows micro-transactions. I think it is an All for one and one for all situation. In order to get your transaction to be approved, you have to approve others' transactions. If you do not work hard to approve others', they will not help you approve your transaction. Tangle also uses MCMC tip selection algorithm to avoid double-spend attack.[7] The white paper is long, and I spent several days reading that paper and tried to understand them. There are no miners and so there is no

reward. Microtransactions will be considered equally as other transactions. For bitcoin, it is not logical to give transaction fees for microtransactions like a 0.01 bitcoin transaction when the fees are equal or almost equal to the amount of the transaction. I see great potential for IOTA and think IOTA's tangle is a better DLT overall.

During that time period, I read news on IOTA and Volkswagen – IOTA and Volkswagen Present Proof of Concept for Autonomous Cars.[17] It seems that Internet of Things and IOTA's tangle is tightly connected. Below is a table for IOTA's features that are suitable for Internet of Things.

#	Feature	Description
1	Scalability for High Throughput	> Built upon a Directed Acyclic Graph > Transaction validation and data acquisition can run in parallel in the network
2	Resource-Lite for IoT Devices	> Low resource requirements designed for IoT devices such as sensors / actuators > Small and big IoT devices can run an IOTA client
3	Nano Payments	> No mining required > Nano-transactions without transaction fees > Real-time payment streaming > Enables machines to effectively transact among each other
4	Data Security Layer	> Focus on data authenticity and integrity > Transports data in a secure way
5	Partition-tolerant	> Multiple IOTA tangles can exist in disconnected clusters > Support of clusters of cyber-physical systems > Enables offline transactions

Figure 6: IOTA's Features for IoT[18]

Then, I began to search for projects that IOTA foundation participate in. Volkswagen's proof of concept for autonomous car using IOTA's tangle is quite fascinating. However, there are no details about how specifically it works.

There are other projects that use IOTA's tangle as well. The list includes Tokyo Metropolitan Government Program, Netherlands's experiment on implementing IOTA (MIOTA) for administrating legal documents, Taipei's partnership with IOTA to become a blockchain-powered smart city and more. I realized that maybe IOTA is more than a technology for cryptocurrency unlike blockchain and Bitcoin but have applications in real life. Since IOTA's tangle is originally designed as a backbone for Internet of Things, I start to explore on that field.

Blockchain is not the solution for all problems.[19] The public is doubtful of whether blockchain technology is secure enough and if it can scale as indicated. I hope that with the hype of Blockchain, we can optimize the technology and

Figure 7: Volkswagen and IOTA Proof of Concept for interconnected vehicles

make it in good use. That is why I am excited about those projects that IOTA participated in. Below is the Proof of Concept using IOTA's Tangle for

interconnected vehicles.

5 Conclusion

In conclusion, Blockchain Technology has great potential for Internet of Things. Although it is new and has its own drawbacks, Blockchain Technology is still at the first stage and nowhere near optimization. Blockchain Technology improves Internet of Things's security, eliminating the need for the third party and is suitable for a common platform for different types of IoT devices. However, there is no one-size-fits-all solution for a Blockchain-based IoT application. Blockchain-based IoT model still needs additional technological research advances to address the specific demands and technical issues like scalability.

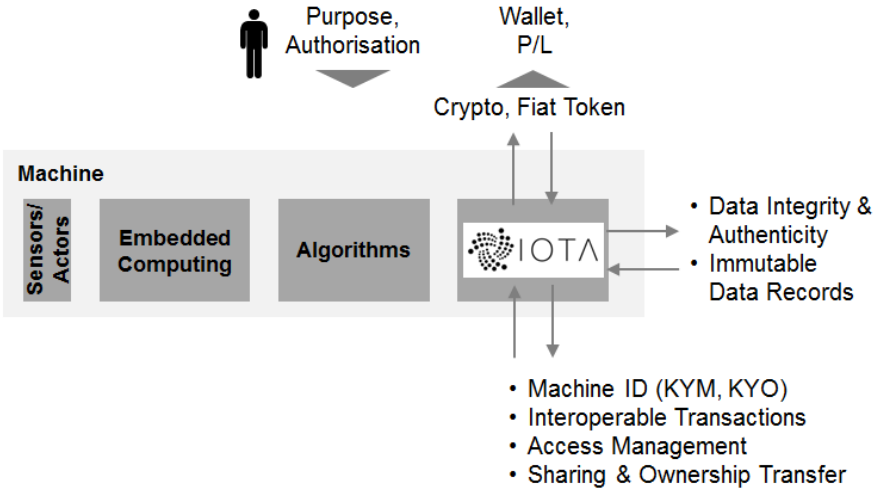

Figure 8: IOTA's tangle model for IoT[18]

References

[1] G. Abramovich, "15 mind-blowing stats about the internet of things," Apr 2015. [Online]. Available: https://www.cmo.com/features/articles/2015/4/13/mind-blowing-stats-internet-of-things-iot.html#gs.1vlwOmo

[2] A. Scott, "Eight ways the internet of things will change the way we live and work," Jun 2017. [Online]. Available: https://www.theglobeandmail.com/report-on-business/rob-magazine/the-future-is-smart/article24586994/

[3] W. Insider, "Bringing the power of ai to the internet of things," May 2018. [Online]. Available: https://www.wired.com/brandlab/2018/05/bringing-power-ai-internet-things/

[4] N. Kshetri, "Can blockchain strengthen the internet of things?" *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," http://bitcoin.org/bitcoin.pdf."

[6] J. Vermeulen, "Bitcoin and ethereum vs visa and paypal – transactions per second," Apr 2017. [Online]. Available: https://mybroadband.co.za/news/banking/206742-bitcoin-and-ethereum-vs-visa-and-paypal-transactions-per-second.html

[7] S. Popov, "The tangle," Oct 2017. [Online]. Available: http://iotatoken.com/IOTA_Whitepaper.pdf

[8] nguyenthithuha, "[review ico] what is paymon? what's new? blockchain hive? payment messenger?" Apr 2018. [Online]. Available: https://bitcointalk.org/index.php?topic=3424682.0

[9] Y. Gupta, R. Shorey, D. Kulkarni, and J. Tew, "The applicability of blockchain in the internet of things," in *2018 10th International Conference on Communication Systems Networks (COMSNETS)*, Jan 2018, pp. 561–564.

[10] T. M. Fernández-Caramés and P. Fraga-Lamas, "A review on the use of blockchain for the internet of things," *IEEE Access*, vol. 6, pp. 32 979–33 001, 2018.

[11] B. C. Florea, "Blockchain and internet of things data provider for smart applications," in *2018 7th Mediterranean Conference on Embedded Computing (MECO)*, June 2018, pp. 1–4.

[12] C. Pop, T. Cioara, M. Antal, I. Anghel, I. Salomie, and M. Bertoncini, "Blockchain based decentralized management of demand response programs in smart energy grids," *Sensors*, vol. 18, no. 1, p. 162, 2018.

[13] D. Observer, "Iota: Part 2 of real world use cases cryptocurrency decentral market headlines," Apr 2018. [Online]. Available: https://decentral.market/2018/04/13/iota-2-of-real-world-use-cases/

[14] C. Meuller, "Volkswagen and iota build the future," Jul 2018. [Online]. Available: https://helloiota.com/volkswagen-and-iota-build-the-future/

[15] M. Nielsen, "How the bitcoin protocol actually works," Dec 2013. [Online]. Available: http://www.michaelnielsen.org/ddi/how-the-bitcoin-protocol-actually-works/

[16] M. Rosenfeld, "What is a finney attack?" Oct 2014. [Online]. Available: https://bitcoin.stackexchange.com/questions/4942/what-is-a-finney-attack

[17] M. Huillet, "Cebit '18: Iota and volkswagen present proof of concept for autonomous cars," Aug 2018. [Online]. Available: https://cointelegraph.com/news/cebit-18-iota-and-volkswagen-present-proof-of-concept-for-autonomous-cars

[18] C. Stöcker, "Automating machine transactions and building trust in the 4th industrial revolution," Feb 2017. [Online]. Available: https://blog.iota.org/automating-machine-transactions-and-building-trust-in-the-4th-industrial-revolution-d3219a157396

[19] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaría, "To blockchain or not to blockchain: That is the question," *IT Professional*, vol. 20, no. 2, pp. 62–74, Mar 2018.