IBM's New Building Blocks: Blockchain

Simplistically, Blockchain is a decentralized peer to peer ledger network. The blockchain has become synonymous with cryptocurrencies, however, the technology itself has been around for far longer. Leslie Lamport first wrote a research paper in 1998, titled "*The Part Time Parliament"*, which examined the concept of a public ledger used in 11th century Paxos - an Island of Greece. This public ledger was utilized to record decrees passed by lawmakers and was only added to once a consensus was reached. The records could not be erased, and since all parties had a copy of the ledger, a system of in-built trust was established (Lamport, 2000). In the 21st century, Satoshi Nakamoto- a pseudonym, published the first blockchain protocol for an electronic payment system, known as Bitcoin (Nakamoto, 2008). The concept utilized cryptographic algorithms and a decentralized public ledger to record transactions. Validation of records to be added to the ledger would be done by multiple parties, and when a consensus was reached the ledger would be appended. This is known as a permission-less blockchain. The genius behind the concept, is that the ledger is immutable, decentralized, publicly distributed, and pseudo anonymous - any party can view the public address, but no names or identities are viewable. Various measures to counter money laundering and other nefarious activities were introduced, such as KYC (know your customer) laws, which dictate that the company providing the exchange services have to maintain secure records of their customers identities. Blockchain has been widely researched for purposes other than financial products, and the consensus is that blockchain technology may be applied to an almost unlimited number of use case scenarios.

Many companies have begun to invest and develop technologies utilizing blockchain technology, including financial (BBVA and Santander), technology (IBM, Facebook, Amazon), food, supply chain and retail (Nestle, Walmart, Pfizer), insurance (Allianz), car manufacturers (Ford, Toyota), and even entertainment companies such as Disney (Nitish, 2020). IBM has invested over 200 million Dollars and employed over 1000 people for more than 500 blockchain products (Carson *et al.*, 2018) and will be the focus of this review due to their heavy financial investment, interest and development of the blockchain technology.

In 2015, a group of companies including IBM, formed a partnership to create a blockchain for enterprise use, named Hyperledger (placed under the guardianship of The Linux Foundation). Unlike cryptocurrencies which are permission-less – allowing any person to record on or view the blockchain - the Hyperledger was designed to be a permissioned blockchain with a pluggable Byzantine fault-tolerant consensus (pBFT) protocol implemented to prevent malicious actors from controlling the entire blockchain (Cachin *et al*, 2017) with only trusted parties receiving credentials to utilize the blockchain.

The IBM blockchain was released as a “Cloud Based Blockchain service”, which is built on the Hyperledger fabric. IBM has marketed it as being used to enable new revenue streams, reduce and remove redundancies caused by legacy systems, improve efficiencies and increase savings. The IBM Blockchain project contains an important component relating to smart contracts called “chaincode”. This enables the business to automate certain processes once certain criteria are met (Androulaki *et al.*,

2018). As such, the IBM blockchain has claimed a stake in this novel technology, which could revolutionize multiple industries.

Benefits and Real-Life Application

IBM is an early leader in the Blockchain niche and has shown real-life applicability of their technology, giving them a competitive advantage. An interesting use case was tested by Walmart and IBM concerning food traceability. According to the WHO, 10% of the world population suffers from food poisoning annually. The rationale behind the test was to address food contamination and limit outbreaks of food poisoning. In China, pigs were tracked from the farm and slaughterhouse all the way to the distribution centres. Information about temperature, humidity and other data was collected by way of sensors and RFID tags and stored on the blockchain for rapid identification of problems. Patterns were recorded and fixed, and if a recall were needed this could be tracked and completed far more efficiently. Mangoes were also part of the first pilot study - tracked from growth in Central and South America all the way to distribution in North America. Because of the high level of contamination of mangoes, a simple receipt would be enough to identify every stage of the harvest process, from growing to transport, warehousing and distribution. Mangoes in the same harvest or subjected to the same degradation could be analysed and removed from distribution if necessary, thus reducing and limiting food borne disease outbreaks. The pilot study was successful, as the time needed to track mangoes was reduced from 7 days to a phenomenal 2.2 seconds (Kamath, 2018).

The success of the food traceability project may also be applied to vaccine distribution. The recent Covid-19 crisis around the world has necessitated a vaccine to be rolled out effectively all over the world, under strict conditions. Pfizer mRNA vaccines are to be stored below -70°C, and Moderna's RNA vaccine below -20°C at all times. The IBM blockchain can adequately monitor all stages of transport and handling using IOT sensors to ensure that they are tamper-proof and suitable for use. If a batch recall is necessary, this can be done almost instantaneously. A simulated recall study was done by the FDA, IBM, Merck, and KPMG, wherein a recall and notification could take up to 3 days based on current procedures. Conversely, utilizing the blockchain for the same simulated recall takes 10 seconds for all parties involved to be notified, thus improving patient and pharmaceutical safety (FDA DSCA, 2020),

Critiques and Challenges

a) Consensus

Generally, the blockchain is verified by a consensus algorithm – similar to proof of work (Bitcoin) and proof of stake (Ethereum). This prevents malicious parties from altering or appending the blockchain. Unlike Hyperledger, IBM does not intend utilizing the pBFT at this time due to it being a resource-intensive process, and as the blockchain is protected by laws and regulations, litigation would be more effective than prevention. The introduction of pBFT would also decrease scalability, thus potentially hampering future business prospects (Frantzell, 2019).

In the IBM Blockchain, an alternative ordering system utilizing Apache Kafka is used (Bhuvana, R. & Aithal, 2020). In this Kafka ordering system, the orderers are the Kafka clients and the Kafka cluster is the data centre. The diagram below explains the Kafka ordering system

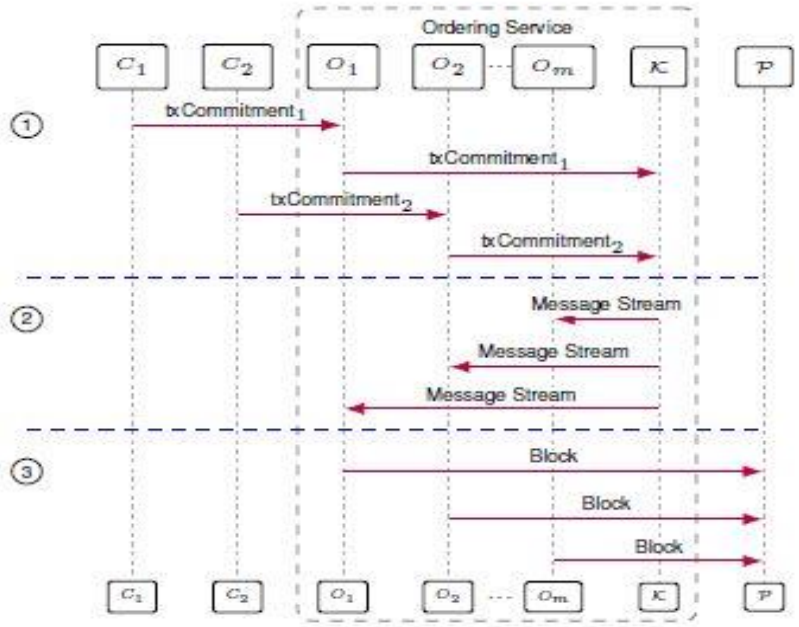

Figure 1. A diagrammatic representation of the Kafka ordering system (Reproduced from Graf et al, 2020).

Analysis and evaluation of this system led to underwhelming conclusions. Graf *et al.* analysed the Kafka ordering system and found that it fails the security tests for consistency and accountability. Sousa *et al.* found that while robust, it is only able to withstand crash faults, leading to a single point of failure.

However, multiple potential solutions were identified each with their own advantages and disadvantages. Graf *et al.* proposed two solutions in order to achieve individual accountability.

1. Utilise the PeerReview programme on top of the Hyperledger Fabric with Kafka system in order to achieve accountability for the protocol. Researchers found that this method, while effective, comes with a few downsides, namely: the program runs in an additional layer on top of Kafka, producing a communication overhead, as well as requiring auditors to identify malicious parties(Graf *et al*, 2020).

2. A modified version of Kafka was proposed, which utilizes Merkle Trees. Merkle trees are a type of encoding, that is more efficient and secure. Each pair of transactions in a block are hashed and then concatenated with the adjacent transactions hash, until only the root hash is present. This saves time to verify transactions, as the entire blockchain need not be verified, only the root hash of the previous block. Additionally, this modified version of Kafka requires that “orderers cut blocks by including a complete consecutive section of the Kafka message stream, including all message IDs and valid signatures, without dropping any messages. In particular, there may be no gaps (according to the message IDs, which must be consecutive) within one block and across consecutive blocks”(Graf *et al*, 2020).

Sousa *et al*. proposed the use of a BFT-SmaRT replication library. Their results show an increased throughput and decreased latency, however, there was no mention of security improvements. Scalability of this solution was also poor (Sousa *et al*, 2018). Feng *et al*. proposed a scalable modified pBFT consensus algorithm called scalable dynamic multi-agent hierarchical PBFT algorithm (SDMA-PBFT). The system utilized a hierarchical design approach and builds sub-groups, after which an agent is elected as a primary node in each sub-group. This method addresses the scalability issue, but suffers from a major drawback in which new nodes cannot easily join the blockchain network, and if a non-loyal node is designated as an agent, the number of consensus nodes will be subsequently decreased (Feng *et al.*, 2018).

IBM themselves touted the development and deployment of a replacement ordering service called Raft. A comparison by Yusuf *et al*. suggested that while similar, the Kafka service was not designed for large networks. Raft is superior in that it is easier to use; and each organization has its own ordering services node, making the network more decentralized. However, while Raft is superior in speed and success, Kafka is better in querying transactions (Yusuf & Surjandari, 2020).

Seo *et al*. proposed an innovative coordination technique for Scalabel BFT consensus. Their technique consists of 4 steps (Seo *et al*., 2020):

1. “The prime node is elected among all participating nodes.
2. The coordinator collects all transactions that existed in the transaction pool of each node.
3. The coordinator checks the equality of transactions and classifies transactions into common and trouble transactions. For trouble transactions,

the coordinator requests a prime node to execute a consensus algorithm and obtains agreed transactions.

4. The coordinator merges common and agreed transactions and requests the controller of all nodes to execute block generation with merged transactions."

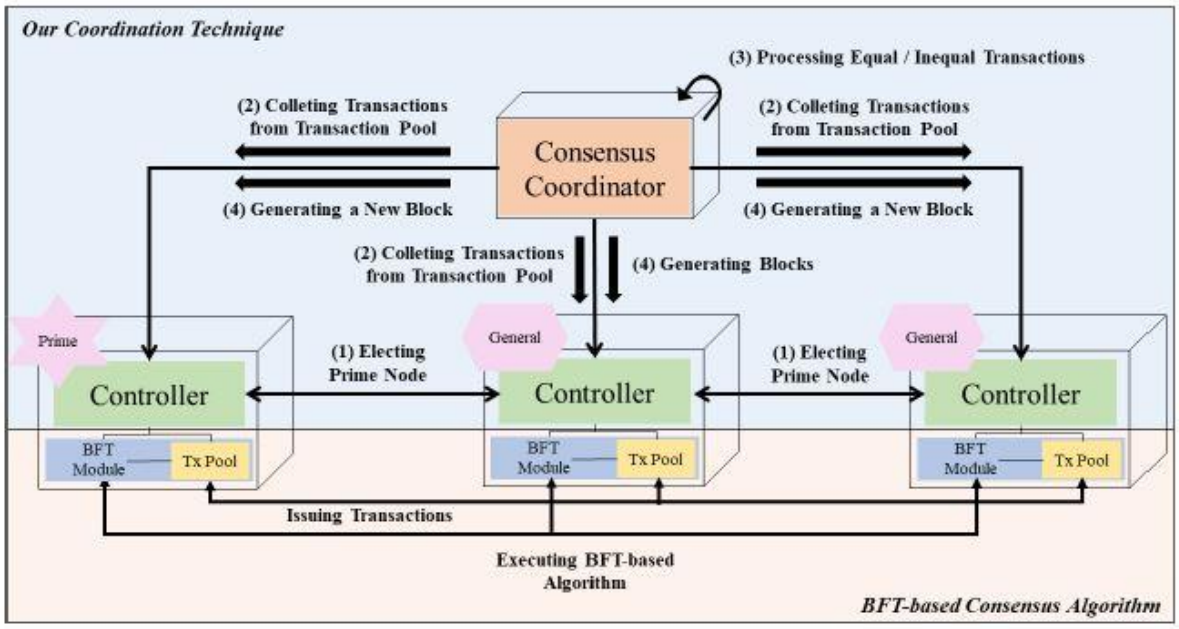

Figure 2. A diagrammatic representation of how the BFT consensus algorithm works (Reproduced from Seo et al., 2020).

Results from testing this coordination technique shows that when using 4 nodes, performance was improved by 3.77 times compared to standard pBFT, and when using 80 nodes, performance was improved by 5.56 times compared to standard pBFT. Seo *et al*. tested their technique on the Hyperledger Besu blockchain with IBFT consensus and similar improvements were noted, thus concluding that their technique successfully improves scalability issues (Seo *et al.*, 2020).

Ultimately, IBM needs to improve their consensus protocol, as Bhuvana *et al.* concluded, “IBM is selling and calling blockchain as Hyperledger fabric by sacrificing the truly important feature of blockchain with more complex architecture than any blockchain platform while also being less secure against tampering and attacks” (Bhuvana & Aithal, 2020). In my opinion, the proposed solution by Seo *et al*. is the most promising with regards to scalability and implementation of a successful and efficient consensus protocol to improve security.

b) GDPR Concerns

Due to the everchanging nature of technology, countries’ privacy policies have also had to be improved accordingly, and this has provided a hurdle for companies with products operating in various regions. One of these policies has been the release of the GDPR (General Data Protection Regulation) – the primary regulation on data protection and privacy in the European Union. Interestingly, IBM themselves released a report into how their blockchain platform abides by the GDPR. The blockchain and GDPR are aligned on the principles of users in charge of their own data. The cardinal rule for blockchain being that no personal data should be stored on the blockchain (due to its immutable nature) and should be stored on off chain storage in order to comply with the ‘right to erasure’ clause in the GDPR, and this is sufficiently satisfied by the IBM blockchain. Additionally, due to the pseudo anonymous and encryption properties that blockchain is built on, it automatically fulfils the data protection clause in the GDPR (Compert, 2018), and thus manages to fall within the data protection scope laid out by the GDPR.

Conclusion and Future Recommendations

The World Economic forum predicts that by 2023, tax collection by a government will be done on the blockchain and that by 2027, 10% of global GDP will be stored on the blockchain (WEF, 2015). This means that businesses such as IBM offering cloud based blockchain solutions will thrive. Scalability of the IBM blockchain is of vital importance for growth and access to future revenue streams, as is resolution of its consensus vulnerabilities. There are, however, multiple issues which may help or hinder blockchain technology development, depending on their approach, including: government regulations, other technological advances, ability to digitize assets and cooperation. It may be necessary for a regulatory or industry body to take the reins to guide policy and regulation, so that cooperation may be achieved (Carson *et al.*, 2018). IBM is fortunate, in that it has already been established as a leader of the blockchain enterprise solutions and has displayed its competency and reliability. By building strategic alliances, improving security and use case solutions, IBM will be at the forefront of the blockchain boom, predicted to be in three to five years' time (Carson *et al.*, 2018).

References

1. Androulaki, E. *et al.* (2018) ‘Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains’, *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, 2018-January. doi: 10.1145/3190508.3190538.
2. Bhuvana, R. & Aithal, P. S. (2020) ‘Blockchain based Service: A Case Study on IBM Blockchain Services & Hyperledger Fabric’, *International Journal of Case Studies in Business, IT, and Education (IJCSBE)*, Vol. 4(May 2020), p. 94.
3. Cachin, C., Schubert, S. and Vukolić, M. (2017) ‘Non-determinism in Byzantine fault-tolerant replication’, *Leibniz International Proceedings in Informatics, LIPIcs*, 70, pp. 24.1-24.16. doi: 10.4230/LIPIcs.OPODIS.2016.24.
4. Carson, B. *et al.* (2018) ‘Blockchain beyond the hype: What is the strategic business value? | McKinsey&Company’, *Digital McKinsey*, (June), p. p.1-13. Available at: https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value.
5. Compert, C. M. L. (@MauLui) B. P. (@lebertrand) (2018) ‘Blockchain and GDPR’, 1(1), pp. 8–23.
6. FDA DSCA (2020) ‘Fda dscsa’, pp. 0–34.
7. Feng, L. *et al.* (2018) ‘Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain’, *Applied Sciences (Switzerland)*, 8(10). doi: 10.3390/app8101919.
8. Frantzell, L. (2019) *Best practices: Creating a successful blockchain application – IBM Developer*. Available at:

https://developer.ibm.com/technologies/blockchain/articles/from-vision-to-reality-creating-a-successful-blockchain-application/ (Accessed: 11 December 2020).

9. Graf, M., Kusters, R. and Rausch, D. (2020) ‘Accountability in a Permissioned Blockchain: Formal Analysis of Hyperledger Fabric’, *Proceedings - 5th IEEE European Symposium on Security and Privacy, Euro S and P 2020*, (i), pp. 236–255. doi: 10.1109/EuroSP48549.2020.00023.
10. Kamath, R. (2018) ‘Food Traceability on Blockchain: Walmart’s Pork and Mango Pilots with IBM’, *The Journal of the British Blockchain Association*, 1(1), pp. 1–12. doi: 10.31585/jbba-1-1-(10)2018.
11. Lamport, L. (2000) ‘The Part-Time Parliament The Part-Time Parliament’, 2(August).
12. Nakamoto, S. (2008) *Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute*. Available at: https://nakamotoinstitute.org/bitcoin/.
13. Nitish, S. (2020) *Companies Investing in Blockchain | 101 Blockchains*. Available at: https://101blockchains.com/companies-investing-in-blockchain/ (Accessed: 10 December 2020).
14. Seo, J. *et al.* (2020) ‘A coordination technique for improving scalability of Byzantine fault-tolerant consensus’, *Applied Sciences (Switzerland)*, 10(21), pp. 1–20. doi: 10.3390/app10217609.
15. Sousa, J., Bessani, A. and Vukolic, M. (2018) ‘A byzantine Fault-Tolerant ordering service for the hyperledger fabric blockchain platform’, *Proceedings - 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2018*, (1), pp. 51–58. doi: 10.1109/DSN.2018.00018.

16. WEF (2015) ‘Deep shift: technology tipping points and societal impact’, *World Economic Forum*, (September), pp. 1–44. Available at: http://www3.weforum.org/docs/WEF_GAC15_Technological_Tipping_Points_report_2015.pdf.
17. Yusuf, H. and Surjandari, I. (2020) ‘Comparison of Performance Between Kafka and Raft as Ordering Service Nodes Implementation in Hyperledger Fabric’, *International Journal of Advanced Science and Technology*, 29(7), pp. 3549–3554.