Data Feeds & Technology
Group Project - Submission 2

- Bosco Keown bosco.keown@gmail.com
- Jeremie Sabban jeremie_sabban@hotmail.com
- Raza Akhtar raza.akhtar@me.com
- Aliaksandr Panko panko.aliaksandr@gmail.com

March 2019
Approx 1540 words

Introduction

Blockchain technology introduced the concept of a digital “ledger” that cannot be corrupted or copied; every record in this ledger is a time-stamped series of transactions called blocks, linked together in a chain using cryptography. Blockchain is truly democratized; there is no central authority controlling it. Blocks are verified by participants in a transparent and visible manner. Falsifying a block would mean falsifying the entire chain. A major benefit is that there is no transaction cost; only the infrastructure on which the blockchain runs costs money.[1]

While Bitcoin[2] is one of the earliest uses of the blockchain, there are other potential uses. We discuss Bitcoin and additional technologies including Ethereum, Hyperledger, and Corda with view to comparing each in terms of scalability, consensus protocol, privacy, degree of decentralization, and settlement finality.

Scalability

Since its introduction in 2009, Bitcoin (BTC) has been the premier cryptocurrency and digital payments system. The biggest problem with Bitcoin has been its inability to scale well. This is - in part - due to the block size limit of 1MB (some claim it is higher) but also because the degree of difficulty of mining BTC has increased over the years with a corresponding increase in computing power and associated energy cost to verify new blocks. Additionally, Bitcoin is “just”

---

[1] "What is Blockchain Technology? A Step-by ...." Accessed March 22, 2019. https://blockgeeks.com/guides/what-is-blockchain-technology/.
[2] "Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org." Accessed March 22, 2019. https://bitcoin.org/bitcoin.pdf.

a cryptographic payments system.[3] This lack of scalability and flexibility was part of the motivation for the creation of Ethereum.

Backed by its own cryptocurrency named Ether (ETH), Ethereum is intended to be a software platform for creating blockchain-based decentralized applications ("dapps") and smart contracts. Even though Ethereum's throughput of 15 transactions per second is double that of Bitcoin, it still falls well short of traditional transaction processing, e.g. Visa's 45,000 per second. Another difficulty for both Bitcoin and Ethereum is the fact that, if block size is allowed to increase, only those who have the resources to run nodes large enough to hold and process larger blocks will be able to participate.[4]

Hyperledger is a blockchain platform that adds scaling capability at the expense of less decentralization (using a "permissioned" model rather than "permissionless" as for Bitcoin and Ethereum). In other words, it is less open. For this reason it uses resources more efficiently by maintaining fewer nodes than a public chain. Additionally, Hyperledger makes extensive use of parallel processing to compute data. The combination of fewer nodes and highly parallel operation enhances scaling far beyond the capabilities of Ethereum.[5]

Corda is similar to Hyperledger, but is created on a specialized platform aimed at the needs of the financial industry. Also a permissioned model, Corda goes a step further - limiting access to only those with a need to know; this helps cut down transaction time. Hyperledger appears to have a clear scaling advantage at present, but Corda is close behind. Care must be taken to compare like with like when measuring transaction scalability.[6]

Consensus

Consensus describes how the blockchain network comes to the conclusion, via a decentralized algorithm, that a block is valid and can be added to the chain or ledger. Bitcoin and Ethereum use the most common algorithm, "Proof of Work", which relies on raw computing power to solve a cryptographic puzzle. The amount of computing power and electrical costs are a serious disadvantage. Ethereum is potentially moving towards a "Proof of Stake" model named Casper in which validators stake some of their coins as "bets" on whether or not blocks are valid, earning a proportionate return on their stake if the block is duly appended to the chain.

---

[3] "On Scaling Decentralized Blockchains - The Initiative For ...." Accessed March 22, 2019. https://www.initc3.org/files/Scaling2016.pdf.
[4] "How Will Ethereum Scale? - CoinDesk." Accessed March 22, 2019. https://www.coindesk.com/information/will-ethereum-scale.
[5] "What Is Hyperledger? The Most Comprehensive Guide ... - Blockgeeks." Accessed March 22, 2019. https://blockgeeks.com/guides/hyperledger/.
[6] "Transactions Per Second (TPS) – Corda – Medium." Accessed March 22, 2019. https://medium.com/corda/transactions-per-second-tps-de3fb55d60e3.

Hyperledger instead uses PBFT (Practical Byzantine Fault Tolerance) voting-based consensus broken down into three phases: Endorsement, Ordering and Validation. First of all, X out of N participants endorse a transaction, then the order in which the transaction(s) are committed is agreed upon, and finally the block of ordered transaction(s) is validated.[7] However, Hyperledger is working towards pluggable consensus models - i.e. the consensus algorithm can be changed depending on the use case. Corda already supports this idea - for example: "*a high value asset might be tagged with a multi-part byzantine fault-tolerant consensus pool. And updates to an ephemeral document being managed by several firms who trust each other might be just fine to be confirmed by a crash-fault tolerant cluster operated by those firms themselves.*" [8]

In our opinion, the pluggable consensus model is the ideal solution. Apart from flexibility, it also affects scalability and transaction speed depending on the level of consensus required and the complexity of reaching it.

Privacy

A major factor in any decentralized application is privacy. Bitcoin transactions are stored on a public ledger and are traceable by address, even though most users only use an address (typically generated by a wallet per transaction) once.[9] Ethereum is in some ways even more transparent than Bitcoin, but that may change mainly due to negative sentiment surrounding Facebook and Cambridge Analytica, and the introduction of GDPR. There is a move towards "data security" rather than "privacy" per se. To this end, a number of projects are under way to enhance privacy on Ethereum.[10]

Hyperledger and Corda are designed more for business; privacy is a design feature with them. Hyperledger has more of a wider privacy setting using permissions on "channels" which are like mini blockchains - this becomes a scaling and control issue when you have thousands of customers and thousands of channels. Corda is a lot more granular in that privacy settings can be narrowed down to a particular smart contract, only sharing data between counterparties to a deal and, possibly, any regulatory bodies.[11]

---

[7] "The Ultimate Guide to Consensus in Hyperledger Fabric - Skcript." Accessed March 22, 2019. https://www.skcript.com/svr/consensus-hyperledger-fabric/.
[8] "Corda Top Ten Facts #8: Pluggable Consensus – Corda – Medium." Accessed March 22, 2019. https://medium.com/corda/corda-top-ten-facts-8-pluggable-consensus-447545e6cb0d.
[9] "Protect your privacy - Bitcoin.org." Accessed March 22, 2019. https://bitcoin.org/en/protect-your-privacy.
[10] "4 Projects Seeking to Solve Ethereum's Privacy Paradox - CoinDesk." Accessed March 22, 2019. https://www.coindesk.com/four-projects-seek-solve-ethereums-privacy-paradox.
[11] "Blockchain-for-Banks Startup Switches From Hyperledger ... - CoinDesk." Accessed March 22, 2019. https://www.coindesk.com/blockchain-for-banks-startup-switches-from-hyperledger-to-r3s-corda.

Decentralization

As mentioned earlier, Bitcoin and Ethereum run on very public blockchains and are thus very decentralized and democratized. This may be at risk due to the cost of validating blocks in terms of computing power and electricity. Those with financial resources to mine intensively with specialized ASIC hardware components may end up having more control.[12] A major threat to decentralization is regulation, China being one example. There is a school of thought that believes that corporate giants using blockchain technologies for their own ends - particularly Hyperledger and Corda - are themselves a threat to the decentralized nature of blockchain in general. Hyperledger and Corda, being permissioned platforms, are not truly decentralized in any case except to a typically limited group of participants. Where solving a cryptographic puzzle is not required, but voting - or indeed some other method such as Proof of Stake - is the consensus algorithm and the blockchain is permissioned rather than permissionless, there is a risk of bad actors (the Byzantine Generals Problem). Hyperledger allows other nodes to make decisions on behalf of “bad” nodes, but we have yet to see how this might be exploited in the future. Corda is not as decentralized as Bitcoin and Ethereum - or even Hyperledger for that matter, but it allows businesses to work in a decentralized fashion.

Settlement Finality

Bitcoin and Ethereum transactions, once validated in blocks, are final and irrevocable; if a transaction was for the wrong amount, it has to be corrected with another transaction or a hard fork. However, this does not mean that all blockchain-based transactions are irrevocable. Finality may be a property of the platform by design, or it may not be. Even so, there is no system that provides 100 percent settlement finality as there are many things that can go wrong. Settlement is probabilistic in nature. Indeed, there are notable cases where things have gone badly wrong in BTC transactions.[13] Bugs in the underlying hardware or software have caused illegal forks or forks that reject valid blocks.[14] With Bitcoin and Ethereum transactions, it is better to wait for a high number of confirmations - at least 6 on BTC and 25 on ETH, for a more probabilistic “guarantee” that the transaction is indeed final. The importance of speed in reaching some degree of finality will become clear when more businesses use blockchain technology for typical business operations. If there are fast guarantees of finality, it will work well for business. If not, it won’t.[15] Corda has a roll-back capability - non-validating notaries can roll

---

[12] "What are the Biggest Threats to Bitcoin? - Krown." Accessed March 22, 2019. https://krown.io/1046/what-are-the-biggest-threats-to-bitcoin.
[13] "PSA: F2Pool is mining INVALID blocks : Bitcoin - Reddit." Accessed March 22, 2019. https://www.reddit.com/r/Bitcoin/comments/3c2cfd/psa_f2pool_is_mining_invalid_blocks/.
[14] "Bitcoin Network Shaken by Blockchain Fork | Bitcoin Magazine." Accessed March 22, 2019. https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/.
[15] "Blockchain Finality- Proof of Work and Proof of Stake - Medium." Accessed March 22, 2019. https://medium.com/coinmonks/blockchain-finality-pow-and-pos-35915a37c682.

back incorrect transactions. Hyperledger appears to have no obvious or documented method of resolving conflicts with invalid transactions. However, finality appears to be strictly maintained: "*in Hyperledger Fabric, this cannot happen — the blocks generated by a collection of orderers are said to be final because once a transaction has been written to a block, its position in the ledger is immutably assured. Hyperledger Fabric's finality means that a disastrous occurrence known as a ledger fork cannot occur. Once transactions are captured in a block, history cannot be rewritten for that transaction at a future point in time."* [16]

Conclusion

We have looked various features that Bitcoin, Ethereum, Hyperledger and Corda exhibit as blockchain technologies: scalability, consensus, privacy, decentralization and settlement finality. There is no clear winner; each of them caters well to a specific group. Bitcoin, being particularly inflexible in its development and, being a cryptocurrency rather than a platform, may encounter decreased decentralization due to the increasing difficulty and cost of mining. Ethereum, Hyperledger and Corda have room to develop and adapt to changes and developments in consensus algorithms, privacy, and settlement finality. Corda seems well-placed to cater for the financial industry having been designed for that purpose explicitly.

[16] "hyperledger-fabricdocs Documentation - Read the Docs." Accessed March 22, 2019. https://media.readthedocs.org/pdf/hlf/release-1.4/hlf.pdf.

References

1. "What is Blockchain Technology? A Step-by ...." Accessed March 22, 2019. https://blockgeeks.com/guides/what-is-blockchain-technology/.
2. "Bitcoin: A Peer-to-Peer Electronic Cash System - Bitcoin.org." Accessed March 22, 2019. https://bitcoin.org/bitcoin.pdf.
3. "On Scaling Decentralized Blockchains - The Initiative For ...." Accessed March 22, 2019. https://www.initc3.org/files/Scaling2016.pdf.
4. "How Will Ethereum Scale? - CoinDesk." Accessed March 22, 2019. https://www.coindesk.com/information/will-ethereum-scale.
5. "What Is Hyperledger? The Most Comprehensive Guide ... - Blockgeeks." Accessed March 22, 2019. https://blockgeeks.com/guides/hyperledger/.
6. "Transactions Per Second (TPS) – Corda – Medium." Accessed March 22, 2019. https://medium.com/corda/transactions-per-second-tps-de3fb55d60e3.
7. "The Ultimate Guide to Consensus in Hyperledger Fabric - Skcript." Accessed March 22, 2019. https://www.skcript.com/svr/consensus-hyperledger-fabric/.
8. "Corda Top Ten Facts #8: Pluggable Consensus – Corda – Medium." Accessed March 22, 2019. https://medium.com/corda/corda-top-ten-facts-8-pluggable-consensus-447545e6cb0d.
9. "Protect your privacy - Bitcoin.org." Accessed March 22, 2019. https://bitcoin.org/en/protect-your-privacy.
10. "4 Projects Seeking to Solve Ethereum's Privacy Paradox - CoinDesk." Accessed March 22, 2019. https://www.coindesk.com/four-projects-seek-solve-ethereums-privacy-paradox.
11. "Blockchain-for-Banks Startup Switches From Hyperledger ... - CoinDesk." Accessed March 22, 2019. https://www.coindesk.com/blockchain-for-banks-startup-switches-from-hyperledger-to-r3s-corda.
12. "What are the Biggest Threats to Bitcoin? - Krown." Accessed March 22, 2019. https://krown.io/1046/what-are-the-biggest-threats-to-bitcoin.
13. "PSA: F2Pool is mining INVALID blocks : Bitcoin - Reddit." Accessed March 22, 2019. https://www.reddit.com/r/Bitcoin/comments/3c2cfd/psa_f2pool_is_mining_invalid_blocks/.
14. "Bitcoin Network Shaken by Blockchain Fork | Bitcoin Magazine." Accessed March 22, 2019. https://bitcoinmagazine.com/articles/bitcoin-network-shaken-by-blockchain-fork-1363144448/.
15. "Blockchain Finality- Proof of Work and Proof of Stake - Medium." Accessed March 22, 2019. https://medium.com/coinmonks/blockchain-finality-pow-and-pos-35915a37c682.
16. "hyperledger-fabricdocs Documentation - Read the Docs." Accessed March 22, 2019. https://media.readthedocs.org/pdf/hlf/release-1.4/hlf.pdf.