WORLDQUANT UNIVERSITY

MASTERS OF SCIENCE IN FINANCIAL ENGINEERING

DATA FEEDS AND TECHNOLOGY (C18-S3)

THOMAS DARLINGTON ADISENU

CEPHAS AKORMEDIE-TAY

DAVID KOFI GOGOVIE

DAVID KWASI NYONYO MENSAH-GBEKOR

GROUP WORK PROJECT – SECOND SUBMISSION

KEY CONCEPTS AND DIFFERENCES IN BLOCKCHAIN TECHNOLOGIES

GROUP 2-A

2019

ABSTRACT

The introduction of Bitcoin in 2008 has unveiled the potential of Blockchain as a Decentralized Ledger Technology (DLT), and since then, several other Blockchain technology platforms have been developed, each with its own characteristics, pros and cons. This project seeks to explore and to compare key concepts and differences in some of the blockchain platforms available today such as Bitcoin, Ethereum, Hyperledger and Corda.

We begin by giving a brief overview of each of the blockchain technologies including aspects like foundation, use cases, currency and programming language before moving on to discuss the main key concepts and concerns of the technology such as scalability, consensus protocol, privacy, degree of decentralization and settlement finality.

Keywords: Blockchain (DLT), Bitcoin, Ethereum, Hyperledger, Corda, Scalability, Consensus protocol, Privacy, Degree of decentralization and Settlement finality

Blockchain Technologies:

A blockchain is a complete, permanent, public, and decentralized transaction ledger, which can be broken down into several components namely: Hashing (cryptography), Private/public key cryptography, Merkle trees and Consensus. Unlike traditional application blockchains runs on a peer-to-peer network of computers rather than a single centralized computer and hence not controlled by a single entity.

Developed by *Satoshi Nakamoto in 2008*, Bitcoin was the first blockchain technology that hit the market to be used as a cryptocurrency. Governance is distributed among all participants.
The Bitcoin network is unsuitable for building applications since it is not Turing complete and not a general-purpose environment for blockchain application development.

Developed by *Vitalik Buterin and founded by Block.one*, Ethereum is an open source software application based on blockchain technology which goes beyond being a currency and seeks to provide developers the framework to write their own decentralized blockchain applications (smart contracts). In other words, there is Ethereum Virtual Machine (EVM) which runs the programming code written on it. *Ether* is the name of the currency used in the Ethereum network and is used to power the network by providing people with the incentives to mine blocks and is also used to pay people under smart contract conditions. Ethereum uses *Solidity* as its programming language and governance is distributed among all participants on the network. In terms of use cases unlike some other blockchains, Ethereum is independent of any specific area of application. That is, it can be used in the finance industry, healthcare, logistic and supply chain etc.

Hyperledger is an open source hub for blockchain technology developments by collaborating with cross-industry professionals and integrating independent open protocols and standards for specific modules with the aim of improving the performance and reliability of the blockchain technology and distributed ledgers. *IBM contributed the code for Hyperledger which is hosted on the Linux Foundation* and governed by the organizations in the chain. Hyperledger does not have a native cryptocurrency but has the ability to create one. It supports smart contracts and uses Google's *Golang* language as its programming language. In terms of use cases, it aims to provide modular, extendable architecture in various industries. One of the most critical Hyperledger projects is the Hyperledger fabric which is the foundation and allows components such as consensus and membership to be pluggable. Other critical projects include *Sawtooth, Indy, Iroha and Burrow*. Hyperledger fabric allows data to be stored in multiple formats and allows participants to create separate ledger of transactions through channels. Sawtooth separates core system from application. Indy is purposely for identity management. Iroha is for blockchain integration in enterprise architecture or IoT projects while Burrow is a simple single-binary blockchain optimized for developers.

Corda is an open source blockchain platform with *R3* as its brainchild and thus serves as its governing body as well as organizations involved. It began with focus on the financial sector and now derives some of its use cases through easy management of legal contracts as well as other shared data between mutually trusting organizations. It allows interoperability among diverse applications. Corda was open sourced in 2016. Corda uses a programming language called *Kotlin* which targets JavaScript and Java Virtual Machine (JVM). Corda does not have a native currency. Recent news has it that Corda may possibly be integrated into and become part of the Hyperledger project serving as a complement to Fabric.

Now, we further discuss some areas of key concern to the technology such as challenges in aspects like scalability, consensus protocol, privacy, degree of decentralization and settlement finality:

Scalability:

In recent times during the ICO (initial coin offering) bubble, several blockchain technologies have faced the issue of scalability. Scalability in blockchain refers to how the network system can handle increasing number of transactions and since blockchains originally, are decentralized systems, scalability is a real cause of concern as opposed to centralized systems where all the transaction processing is done at a single node.

Apart from *increasing the block size and reducing the complexity of mining blocks* as a way of addressing the scalability issues in blockchain technologies like Bitcoin, Ethereum on the other hand is looking to address its scalability issues by implementing what it calls *layer 1 and layer 2 solutions*. Layer 1 solutions looks at the core of the blockchain. In other words, layer 1 is the base consensus layer for the Ethereum protocol and the layer 1 solution increases Ethereum's transaction throughput by increasing the capacity of the base blockchains and these changes typically require a hard fork. S*harding* is an example of a layer 1 solution, an idea which came from databases where the state of the database is split into shards to increase scalability. In Ethereum, sharding is implemented by segmenting the blockchain state into different shards such that individual nodes process only transactions assigned to their shards. Layer 2 solutions seeks to build solutions on top of Ethereum's base layer protocol. In other words, building smart contract solutions to interact with software running off-chain and this typically does not require a hard fork. *State channels* is an example of a layer 2 solution which moves some of the state management off the blockchain. The state which is continuously signed by the parties involved can at any point in time be settled on the chain where the signatures of the participants is verified. A subset of state channels are *payment channels*. As another way of improving scalability, Ethereum seeks to upgrade to proof-of-stake consensus algorithm. Scalability however is not prevalent in Hyperledger and Corda since they operate as private networks and do not require all nodes in the network to process transactions.

Consensus Protocol:

Consensus protocol is the primary rules governing a system that shows how the system should work and therefore how all network nodes should interact, how data is transmitted between them and the requirements for a valid block. Consensus algorithms are mechanisms implemented to ensure these rules are adhered to. In other words, they are responsible for maintaining the integrity and security of a decentralized system. There are so many consensus algorithms available such as *POW (proof-of-work), POS (proof-of-stake), POA (proof-of-authority), POET (proof-of-elapsed-time), PBFT (practical byzantine fault tolerance)* just to mention a few. POW was the first consensus algorithm to be created mainly attributed to Satoshi Nakamoto which he used in Bitcoin. It involves solving a computationally intensive puzzle to be able to add a block to a blockchain, a process generally referred to as *mining*. This process may involve several attempts and so miners with high hash rate stand a better chance of finding a valid block. This leads to miners coming together to form groups known as mining pools in the hopes that through the shared efforts of each member in the group, they would be able to solve the computationally intensive puzzle. *This to some extent introduces centralization into the system contrary to the decentralization properties of blockchain technology*. Bitcoin and Ethereum are currently based on the POW consensus algorithm, though Ethereum has plans in the pipeline to upgrade to use POS consensus algorithm.

Since Bitcoin for example is a public permission-less blockchain, anyone can validate and add a transaction to the blockchain regardless of whether the participant is part of the transaction or not, and as only one user can do so at a time, participants compete among each other letting their computer solve for the cryptographically intensive puzzle and in return, participants are awarded Bitcoins. Likewise, participants receive Ether for mining blocks in the case of Ethereum through the

POW consensus algorithm. In order to avoid the need to use huge computer resources just to solve a puzzle, an alternate consensus algorithm was developed known as POS (proof-of-stake) where participants with higher stakes are chosen to validate a block in the view that the higher your stake, the higher the chance of finding a valid block since you lose your stake if your block is found to be invalid by other participants.

In Hyperledger, consensus is not required by all network participants and if consensus is however required, Hyperledger relies on pluggable consensus algorithm such as *PBFT (Practical Byzantine Fault Tolerance)*. Corda supports a wide variety of consensus mechanism and primarily achieves consensus at the *level of individuals transaction* rather than the entire network at large. In other words, consensus is mostly limited to participants involved in the transaction.

Privacy:

Data privacy of blockchain refers to the property of blockchain providing confidentiality to data and as privacy and security go hand in hand, it is critical to mention a few security requirements of blockchain transactions such as consistency, integrity, confidentiality, anonymity, preventing double spending attacks, tamper-resistance etc. The concept of consistency in blockchain is having the same copy of transaction data across the network nodes. Integrity refers to reliability of the data. Confidentiality is preventing unauthorized access to transaction data such as transaction amount and addresses. Anonymity refers to hiding user identity. Double spending attack prevention as the name implies refers to avoiding the possibility of double spending your money. Tamper-resistance means that once a transaction is settled and finalized in the blockchain it cannot be altered.

In general, most blockchain technologies utilizes encryption mechanism (cryptography) by generating a private/public key pairs with the private key used to digitally sign the transaction while the public key is used to verify the transaction. Bitcoin uses *ECDSA (elliptic curve digital signature algorithm)* as its digital signature scheme for signing transactions as opposed to the *standard elliptic curve "secp256k1"* used by some other blockchain technologies. Blockchain technologies also typically maintain a hash value of a block in addition to the hash value of previous blocks forming a concept known as the *Merkle tree* making the blockchain tamper resistant since a change in a single unit of the data would affect hashes of the linked blocks in the entire blockchain. Due to this hashing scheme for encrypting the data, it raises the level of security in the system and hence data privacy.

Bitcoin and Ethereum as stated previously are public permission-less blockchains since anyone can access the data introducing privacy issues and concerns. Bitcoin for one does not guarantee anonymity despite the cryptographic (pseudo-anonymity) nature of addresses and as data is public, anyone can infer addresses of transactions to its real user name posing privacy issues. On the other hand, privacy issue is not prevalent in Hyperledger and Corda. Hyperledger is more of a consortium blockchain as it keeps some of its transactions private (permissioned) depending on the use case. Corda also by design is a private (permissioned) blockchain as it makes data available to only participants involved in the transaction, hence has no privacy issues.

More so, other security and privacy techniques for blockchain have been designed such as *mixing services* which for example helps to prevent user addresses from being linked or inferred. Mixing refers to random exchange of coins between users to obfuscate the observer from knowing the actual ownership of coins. This technique has limitations though. (Other complete anonymity mechanisms also exist such as *zero knowledge proof* which are being used in some other blockchain technologies). *In summary, there is no single best technique to address these privacy problems and so multiple combination of techniques can be more effective.*

Degree of Decentralization:

Decentralization is to host a service at different locations or points in a network at the same time rather than to entrust a single node the responsibility of managing the entire network as seen in centralized systems. Though decentralization concept is generally the same, different blockchain technologies go about it in different ways. Some benefits of decentralization are reduced cost and monopoly as there is no central authority, more security as in when there is an attack on one node, it does not compromise the entire network. Decentralization induces resistance to distributed denial-of-service attacks (DDoS). DDoS refers to the availability of data even when one network node is shut down. The more nodes there are at different geographic locations, the stronger the decentralization and this falls in the category of physical decentralization. Political decentralization is when it is hard for one group to put their interest on top of others. There is also the issue of consensus protocol that determines the degree of decentralization in blockchain technology. Decentralization however comes with cost such as low transaction throughput as each node in the network would have to process the transaction.

As stated earlier, Bitcoin and Ethereum uses proof-of-work consensus algorithm while Hyperledger uses PBFT. Proof-of-stake which Ethereum is moving onto is most crucial to decentralization as it informs how the blockchain changes as it depends on the amount staked by participants in different locations. Bitcoin transaction processing is slow (7tps) and 10 minutes to validate a block. This has attracted transaction fees as miners are incentivized to process transactions with higher fees compromising on the general interest of all transactions. Ethereum transaction processing is 15tps though better than Bitcoin, is still not efficient when compared to the 2500tps for centralized system like VISA. Usually public blockchains like Bitcoin and Ethereum allow everyone access to the network making them more decentralized. On the other hand, private permissioned blockchains sacrifice some amount of decentralization to attain privacy and an example is Corda. In consortium blockchain, though privacy exists, the network is administered by several organizations collaboratively, and so has some degree of decentralization compared to pure private chains. Hyperledger falls within this category of consortium blockchain.

Settlement Finality:

Settlement finality is one of the major ongoing disputes between public and private blockchains. All things equal, centralized systems have finality since there are middle men with the central authority to handle the daily transactions and are paid for their job but however there can be problems for instance when the system is hacked. On the other hand, decentralized blockchain systems generally and probabilistically depending on the setup, do not have finality as there are no central authority responsible for that but rather uses consensus method discussed earlier to attain settlement finality, and this makes blockchain decentralized technology so revolutionary and there are growing indications that some of its challenges being discussed here will be a thing of the past as technology advances into the future though some claim it will be at the cost of decentralization.

The concept of finality really has to do with the notion that once an operation is completed, that operation is completed for good and the system cannot reverse it and it is particularly important in the financial industry where institutions need to quickly have certainty of the settlement of a transaction for example sending money into someone's account and knowing after some time that it has actually hit the person's account and ownership settled with the account holder. In general, however, there is no true 100% settlement finality as system design can be adapted to meet certain requirements when there is the need. Also, in proof-of-work, there is the chance of a *51% network control attack* to reverse a transaction while in proof-of-stake, there is the concept of *nothing-at-stake*, where validators do not really mind losing their stake just to hurt the network. Again, in proof-

of-work, you wait at least 3 block confirmations or more reasonably 6 block confirmations before considering a transaction reasonably finalized while in proof-of-stake, a transaction can be considered finalized if about 2/3 of the validators confirm so.

Bitcoin being public has *no finality certainty* as tampering is possible by gathering 51% of computing power of the network as it is based on the POW consensus algorithm. With transaction throughput of 7tps and block confirmation time of 10 minutes, a waiting time of at least 30 minutes (3 blocks) is required before considering a transaction as settled and the more blocks are added the more it can be considered finalized. Ethereum also being public with an average transaction throughput of 15tps and lesser block confirmation time is considered more efficient than Bitcoin and have *a better settlement finality* as block validation is done by few selected nodes. On the other hand, private blockchains usually do not have consensus algorithm making possible block generation time faster and safer but sacrifices a little bit of decentralization as explained earlier. In other words, settlement finality in private networks is *immediate* as transaction is between only the parties involved. Consortium blockchain when required uses consensus algorithm such as PBFT but however, block-generation time is shortened by voting only few trusted validators. Hyperledger being more of consortium and Corda due to their private nature have *better settlement finality* than Bitcoin and Ethereum as decision is made between only the parties involved in the transaction rather than the entire network.

Conclusion:

The blockchain technology can be broadly categorized into three main groups (public, private and consortium) with private blockchains having higher performance than public blockchains, consortium falling in between but more of private. Also, blockchain technologies differ greatly especially on vision and use cases and the choice of a blockchain depends on the nature of business. Blockchain has many envisioned use cases, but it will not be possible without addressing the issues of scalability and thus each blockchain technology is using different tradeoffs to address these issues. *Also, a table for quick comparison can be found in the appendix below.*

References

Goyal, S. and Goyal, S. (2020). *Hyperledger vs. Corda R3 vs. Ethereum: The Ultimate Guide*. [online] 101 Blockchains. Available at: https://101blockchains.com/hyperledger-vs-corda-r3-vs-ethereum/ [Accessed 29 Jan. 2020].

Merehead. (2020). *Comparison: Ethereum vs Hyperledger Fabric vs R3 Corda - Merehead 1838*. [online] Available at: https://merehead.com/blog/comparison-ethereum-hyperledger-fabric-r3-corda/ [Accessed 29 Jan. 2020].

Corda. (2020). *Corda v Hyperledger v Quorum v Ethereum v Bitcoin | Corda*. [online] Available at: https://www.corda.net/blog/corda-v-hyperledger-v-quorum-v-ethereum-v-bitcoin/ [Accessed 29 Jan. 2020].

Corda. (2020). *Corda | Open Source Blockchain Platform for Business*. [online] Available at: https://www.corda.net/ [Accessed 29 Jan. 2020].

Medium. (2020). *Introducing Corda 4*. [online] Available at: https://medium.com/corda/introducing-corda-4-18e3b588b71c [Accessed 29 Jan. 2020].

IBM Developer. (2020). *Top 6 technical advantages of Hyperledger Fabric for blockchain networks*. [online] Available at: https://developer.ibm.com/technologies/blockchain/articles/top-technical-advantages-of-hyperledger-fabric-for-blockchain-networks/ [Accessed 29 Jan. 2020].

Tkatchuk, R., Clifford, J., Simeone, M., Kirstein, M., Clifford, J., Simeone, M., Kirstein, M., Clifford, J., Simeone, M. and Kirstein, M. (2020). *When Comparing Blockchains, Decentralization Comes in Degrees - Dataconomy*. [online] Dataconomy. Available at: https://dataconomy.com/2018/05/when-comparing-blockchains-decentralization-comes-in-degrees/ [Accessed 31 Jan. 2020].

Harvard Business Review. (2020). *Will We Realize Blockchain's Promise of Decentralization?*. [online] Available at: https://hbr.org/2019/09/will-we-realize-blockchains-promise-of-decentralization [Accessed 31 Jan. 2020].

Arxiv.org. (2020). [online] Available at: https://arxiv.org/pdf/1903.07602.pdf [Accessed 31 Jan. 2020].

Hackernoon.com. (2020). *The Blockchain Scalability Problem & the Race for Visa-Like Transaction Speed*. [online] Available at: https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44 [Accessed 31 Jan. 2020].

Medium. (2020). *The Case for Ethereum Scalability*. [online] Available at: https://medium.com/blockchannel/the-case-for-ethereum-scalability-a66ed08d0bed [Accessed 31 Jan. 2020].

Chandler, S. (2020). *Blockchains Are Learning How to Scale, But At What Price?*. [online] Cryptonews.com. Available at: https://cryptonews.com/exclusives/blockchains-are-learning-how-to-scale-but-at-what-price-1492.htm [Accessed 31 Jan. 2020].

Projects, D., Michie, I. and Jannu, G. (2020). *Difference between Hyperledger Projects*. [online] Stack Overflow. Available at: https://stackoverflow.com/questions/49318332/difference-between-hyperledger-projects [Accessed 31 Jan. 2020].

Mango Research. (2020). *Settlement Finality in Blockchains: PoW vs PoS - Mango Research*. [online] Available at: https://www.mangoresearch.co/settlement-finality-pow-pos-blockchain/ [Accessed 31 Jan. 2020].

Appendix:

Blockchain technologies comparison.

Technology	Bitcoin	Ethereum	Hyperledger	Corda
Feature	---	General purpose	Modular	Specialized
Application	Just like the regular currency used for any business transaction between individuals and institutions.	Standard applications primarily used by P2P and B2B operations	Preferred platform for B2B operations and mainly used by companies.	Mainly used in the financial industry.
Utility (use-cases)	As a currency used to buy products and services and store of value.	As a currency as well as helps in developing decentralized applications (DApps).	An ecosystem that brings together many technologies in diverse industries such as finance, healthcare, internet of things, supply chain. Etc.	Synchronizing financial agreements between regulated financial institutions.
Founder	Satoshi Makamoto	Vitalik Buterin	Linux Foundation/IBM	R3 Group
Currency	Bitcoin	Ether	None	None
Tokens	None	Yes. Eg. ERC20 and ERC721. Used in for smart contracts	Yes. Used for chaincode	None
Scalable	No. (light)	No. (plasma)	Yes.	Yes.
Decentralization	Yes.	Yes.	Yes.	No.
Consensus protocol	Proof-of-work (POW)	Proof-of-work (POW) but upgrading to Proof-of-stake (POS)	Pluggable. E.g. Practical Byzantine Fault Tolerance (PBFT)	No. only parties involved at the transaction level.
Privacy	Public (permission-less)	Public (permission-less)	Consortium (in between private and public) permissioned	Private (permissioned)
Settlement finality	Probabilistic and slow. Must wait at least 3 blocks (30mins) or reasonably 6 blocks (60mins) confirmation.	Probabilistic and slow but can be fast depending on selected validators. Requires 2/3 of selected	Depends on PBFT	Fast

		validator's confirmation.		
Programming language	**C++ and Go (no support for smart contracts)**	**Solidity (support for smart contracts)**	**Go and Java (support for smart contracts)**	**Kotlin and Java (support for smart contracts)**
Supply type	**Deflationary (a finite amount of bitcoin will be made)**	**Inflationary (more tokens can be made over time)**	**Non-currency based**	**Non-currency based**