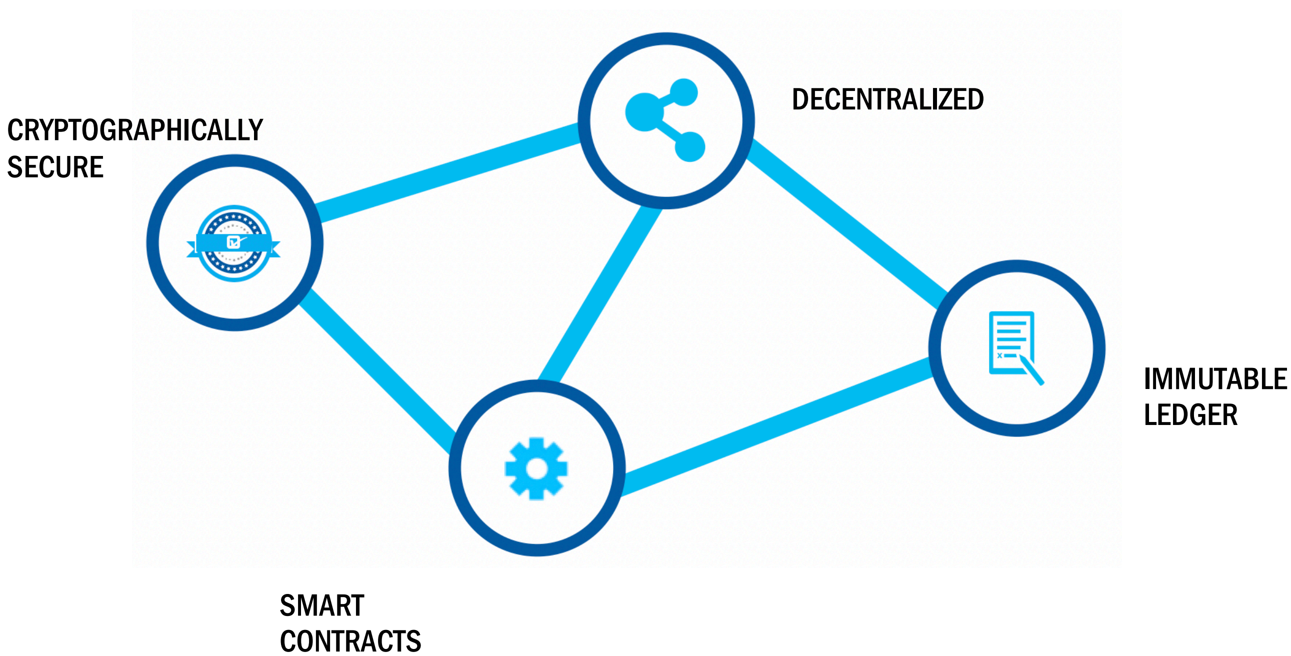
Enterprise Blockchain Platform Competitive Analysis

May 2017

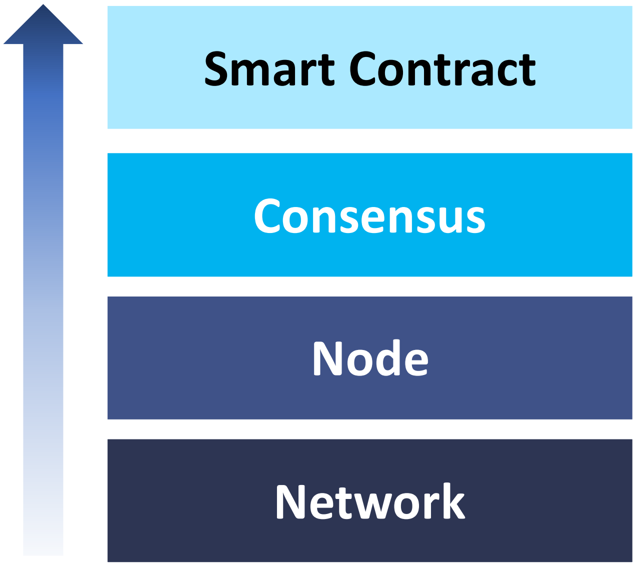
CONSENSYS

WHAT MAKES A BLOCKCHAIN A BLOCKCHAIN?

Originally utilized and proven through use in Bitcoin technology, blockchain allows various use cases and implementations when applied to an enterprise setting. The key characteristics of this technology revolve around cryptography, immutability, security and decentralization. By distributing transactions through smart contracts and allowing validation through all participatory nodes in a shared system, blockchain is capable of creating new environments and paradigms on how business logic is processed through a platform and how untrusting stakeholders are able to interact with each other.



THE DIFFERENT LAYERS THAT MAKE UP A BLOCKCHAIN PLATFORM:



Smart contracts represent code or computer protocols that are able to facilitate business logic through enforcing the performance or adherence to guidelines of a contract

Consensus algorithms ensure that additional blocks added to the blockchain are validated as the truth while also ensuring that a history of the universe of transactions are maintained within the system

Messages are broadcasted throughout a blockchain network using nodes. Nodes pass transaction data and block information while validating transactions that are allocated through the blockchain.

Blockchain networks consist of the data and transactions that are passed among the various nodes and validators in the ecosystem. Blockchain networks are decentralized - there is no single stakeholder that controls the entire network. Trust Is distributed among the nodes in the network.

HOW DO WE EVALUATE BLOCKCHAINS FOR ENTERPRISE NEEDS?

We will evaluate blockchain platforms in two axes:

A) HOLISTIC EVALUATION

1. Enterprise Capabilities**: How the platform behaves in an enterprise setting and whether there are enterprises that currently have interest in using the platform. Describes whether the platform was designed for enterprise use or highly scalable levels of performance.**
2. Ecosystem: **The developer ecosystem around this product. The criteria describe the stakeholders that are in the environment as well who are the main advocates of the use of the platform.**
3. Market Proven**: This describes whether there are any existing use cases that involve established institutions. Successful implementations will determine whether something is market proven**
4. Smart Contracts**: Does this platform support smart contracts**
5. Open-Source**: Determines whether or not the code is open sourced**
6. Public Chain Compatibility**: Describes if this platform is compatible with the public chain**

B) TECHNICAL EVALUATION

1. Immutability/Data Integrity: In the context of ensuring data consistency, it is important to ensure the immutability of data. To ensure that something is unchanged over time and that you are able to audit any changes that occur to the underlying data, a blockchain uses a combination of cryptography along with asymmetric and symmetric encryption to facilitate this capability. Consensus mechanisms are used to ensure that data has been validated by nodes or node-like entities prior to processing and appending transactions to a shared database.

2. Scalability: For enterprise use cases, large institutions require scalability in their blockchain based system in order to produce the necessary throughput and execute large scale business

3. Privacy: As blockchain allows trust among ordinarily untrusting parties, privacy is important in keeping certain transactions private between certain counterparties, while still maintaining the main principles that govern a blockchain.

4. Permissioning: Public blockchains are designed to be accessible by the entire ecosystem of users. Permissioning creates an environment where only trusted counterparties are allowed to take part within the workings of a blockchain solution.

5. Security: A key feature of blockchain, security plays a significant role as transactions need to be built on a protocol capable of withstanding malicious actors. The robustness of a blockchain platform can be measured by how resilient it is against malicious actors.

6. Manageability: The details and configurations of the underlying technology protocol create different dynamics in terms of how manageable a platform is and how stakeholders are able to allocate resources towards utilization.

7. Governance: Governance is important to ensure that a codebase is moving into the direction of how stakeholders wish to utilize the system.

8. Maintainability: A system is only as robust as its capability of maintaining certain levels of performance and throughput. The entities that maintain a system factor into the overall utility and sustainability

9. Performance: Modifications and additional components are added to a platform to facilitate improved performance. Configurations to the architecture can create more efficient processing of transaction and code execution.

10. Extensibility: Whether platforms are designed to meet future growth is a primary factor in assessing the validity of the product. Blockchain systems require the capacity to iterate and improve upon existing technologies.

ENTERPRISE BLOCKCHAIN PLATFORMS: COMPARISON SUMMARY

Enterprise Ethereum:

Enterprise versions of Ethereum are capable of significant performance along with adherence to the core tenets of a blockchain platform. While transactions are not mined the same way that would occur on the public chain, different configurations of consensus ranging from Proof of Authority to Byzantine Fault Tolerance are used to ensure the validity of transactions when they are appended to the Ethereum Virtual Machine. Currently various enterprise implementations of

Ethereum are maintained by the Enterprise Ethereum Alliance which oversees a significant amount of the large-scale implementations of Ethereum technology.

Hyperledger Fabric:

Fabric is distributed database technology that is currently being created by the Hyperledger Foundation towards creating a system that can allow large institutions and corporations to process transactions in a shared database. The platform is capable of scalability and throughput in the context of various use cases, though adherence to certain blockchain tenets such as immutability and permissioning may be limited by certain technological restrictions that the architecture is built upon. In assessing core principles of blockchain and how the technology is assembled and configured, Fabric does not demonstrate direct implementation of various characteristics of a true blockchain platform.

R3 Corda:

Corda is a platform built with the core principles of blockchain in mind when designing the solution. With significant influence from Bitcoin core developers, Corda expands upon various concepts like immutability and data integrity while adding additional concepts formulated specific to the context of Corda. Corda is a self-proclaimed decentralized database that makes modifications to existing technology in order to ensure transaction throughput and scalability. As of now, a lot of the concepts behind Corda are still theoretical though show potential roadmaps of how functionality can be achieved.

A) HOLISTIC EVALUATION

	Enterprise Ethereum		Hyperledger Fabric		R3 Corda	
Enterprise Capabilities		Designed and built to bring Ethereum to the enterprise environment with enhanced scalability and privacy features		Designed and built for specific enterprise use cases		Designed and built for specific enterprise use cases. Not general purpose / less flexible architecture
Ecosystem		Largest community of developers with proven innovation power – network effect is key for new technology. Strong collaboration and sharing of best practices		Limited developer base mainly driven by enterprise background. Risk vendor lock-in		Relatively new and hence difficulty to access developers. Risk of vendor lock-in

Market Proven		Ethereum is live since July 2015 with many applications battle-tested		No large enterprise deployments - IBM bluemix with some potential		No large enterprise deployments
Smart Contracts		Yes – EVM		Yes – Chaincode		Yes - State Objects, Contract Code, JVM
Open Source		Yes		Yes		Yes
Public Chain		Yes – compatible		No		No

B) TECHNICAL EVALUATION

	Enterprise Ethereum		Hyperledger Fabric		R3 Corda	
Immutability / Data Integrity		Tested Immutability		Data Integrity not guaranteed		Theoretical Immutability
Scalability		Enterprise design		Existing technology		Scalable framework
Privacy		System designed around privacy		Enables privacy in certain contexts		Capable of private transactions
Permissioning		Permissioning at four layers of the stack		Infrastructure configuration only		Consortium framework
Security		Security at four layers of the stack		Centrally dependent		Decentralized trust
Manageability		Innovative technological approach		Legacy technology focused		Dependent upon further development
Performance		Market proven capabilities		Limited successful deployments		Not been enterprise tested
Governance		Emerging enterprise following - decentralized		Large governance structure		Bank consortium
Maintainability		Large scale enterprise community		IBM-focused development community		Financial institution stakeholders
Extensibility		Public chain interoperability		Centrally dependent		Decentralized trust

TECHNICAL FEATURE DEEP-DIVES

1. IMMUTABILITY / DATA INTEGRITY

	Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Smart Contracts	All transactions (whether between accounts or smart contract to smart contract) cryptographically secured for immutability	N/A	UTXO model - structurally similar to bitcoin
Consensus	Nodes agree on shared states due to modular consensus algorithms	Ordering service append blocks to Kafka topic partitions	Network map cached and distributed throughout network. Map publishes IP addresses to reach all nodes
Nodes	Replicated across all nodes; cryptographically secured for immutability; transactions are signed and not mutable	N/A	Notary service distributed over multiple nodes
Network	Replicated state distributed across network	N/A	Corda network contains multiple notaries

In assessing one of the key tenets of blockchain technology, it is apparent that private instantiations of Ethereum such as Quorum are capable of facilitating the same levels of immutability and data integrity that can exist in a public blockchain network. While comparing this characteristic to technologies used in IBM Fabric, such as the Kafka ordering service (which is perceived to be immutable), the distinction becomes obvious as transactions executed in Quorum are actually replicated across the Ethereum Virtual Machine and validated through the implemented consensus mechanism. While Corda also aims to achieve this level of immutability in their code base, the technology is still needs further development as low level technical implementations need to be instantiated in order to validate a lot of their high-level assumptions.

2. SCALABILITY

	Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Smart Contracts	Increased smart contract performance – EWASM	Chain deployed in multiple docker containers	Smart contracts checked in parallel. Smart contracts isolated from underlying cryptography
Consensus	QuorumChain POA increase throughput	Multichannel consensus Kafka Ordering services	Nodes that are under heavy loads can access flow workers. Additional notary clusters
Nodes	Multiple voting-based consensus among Quorum Nodes	Additional endorsing peers and ordering service nodes	Partial visibility. Not all nodes need to see transaction graphs
Network	Multiprotocol network layer	Virtual private network (VPN)	Network map service publish node information.

Designing a system to be scalable is a major challenge among enterprise solutions. All three platforms have architectures designed to facilitate scalable systems that can be implemented in large scale enterprise solutions. While IBM Fabric utilizes several technological aspects of pre-existing systems, their scalability goals are achievable with the current push to production. As Ethereum is still an emerging technology that utilizes several novel concepts, the reconfigurations of various aspects allow for a highly scalable roadmap. Corda has architected out several aspects of their platform that can contribute to a scalability road map. Significant amount of emphasis is placed on ensuring that processes can be augmented to withstand heavier loads.

3. PRIVACY

	Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Smart Contracts	Transaction payload encrypted with symmetric and asymmetric encryption	Chain code services encrypted with TLS	Data distribution group (DDG). Transaction merkle trees
Consensus	Global state consensus with private state secured	BFT based algo (not ready for Fabric version 1.0 Alpha)	N/A

Nodes	Constellation Transaction Manager & Secure Enclave	Peers within channel broadcast transactions through Gossip Protocol	Key randomization
Network	Private state data stored only in local state database of parties	Channels; different levels of trust need to be in a private transaction	A permissioning service that automates the process of provisioning TLS certificates. Mix Network

Varying levels of privacy are implemented within these enterprise systems. While Fabric facilitates this type of service through its use of channels to isolate peers and chain code so that transactions are not visible to members outside of a particular channel. While this does induce privacy at certain levels, it should be discussed that the ordering service receives all transactions from all channels, so confidentiality is only pertaining to peers and not orderers. Quorum, as a private instantiation of Ethereum is able to facilitate more robust privacy through its constellation framework in which transaction managers determine different levels of access to payloads through use of symmetric and asymmetric encryption. While Corda is also finding ways to implement privacy, it must be accepted that the various methods are currently conceptual and require low level validation of the high-level assumptions.

4. PERMISSIONING

	Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Smart Contracts	Smart contract node designations	SDK peer and member configuration system	Contract constraints encoded in states
Consensus	Blockmaker and voter nodes validating transactions while only exposing private details to relevant parties	Varies by ordering service	Nodes check for connectivity in network map

Nodes	Observers, Blockmakers, and Voters nodes permissioned by roles	Endorser, committer peers, and ordering service nodes within a channel	Flow API's provide messaging, routing and delivery to nodes
Network	Network Manager controls access and permissioning	Virtual private network (VPN)	Semi-private network requires identity signing by root authorities

All three platforms are capable of implementing permissioning among the users and trusted nodes or node-type entities. R3 Corda has architectured out identity signing implementations that are capable of facilitating permissioned access for the various members of their consortium. IBM Fabric permissions users through how chain code dictates the level of access to certain channels enabling sufficient functionality. Enterprise instantiations of Ethereum rely on smart contracts to determine certain access among the recognized nodes within the network.

5. SECURITY

Enterprise Ethereum	Hyperledger Fabric	R3 Corda
All blockchain transactions secured through asymmetric and symmetric key cryptography and block validation	Security of transactions dependent upon ordering service and interaction with client and endorsing peers	Features like Intel SGX convert non-BFT algorithms into trusted form using remote attestation and hardware protection

Fabric has various points of failure in the design which may prevent the same levels of security that can be found in any of the Ethereum platforms. While the ordering service layer is highly involved in processes affiliated with the data allocation, much needs to be improved to ensure complete secure transactions. Through use of a secure enclave and manager components of Quorum architecture, the Ethereum instantiation displays superior security. Corda also secures various features of its infrastructure using existing tools, though additional levels of implementation may be needed for ideal functionality.

6. MANAGEABILITY

Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Smart contracts determine block maker and voter nodes roles along with managing control within the network Network Manager - Manages permissions	Managed through different configurations of Docker containers to which chain code is deployed to. Configuration transactions create channels.	Transactions defined by JVM bytecode. Multiple notaries manage transactions. Bytecode-to-bytecode transpilation create flows to execute transactions.

As manageability is a key concern of how usable these platforms are, it is important to note that several technological layers are in place among the platforms to ensure functionality. While various aspects of the platform are managed by the deterministic smart contract code in Ethereum, use of Docker containers in deploying chain code in IBM Fabric also allows various configurations. The deployment of smart contracts into the JVM will also contribute to the management of different implementations of Corda.

7. GOVERNANCE

Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Governed through the Enterprise Ethereum Alliance	Governed through the Hyperledger foundation as well as IBM	Managed by R3 Start-up with many industry investors

While IBM Fabric has the strongest governance approach to moving their codebase forward, R3 Corda and Enterprise Ethereum Alliance are also approaching this topic with viable strategies

8. MAINTAINABILITY

Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Platform maintained by community of decentralized developers on open source technology	Though open source, platform development is primarily created by IBM team	Maintained by R3 banking consortium

One of the biggest strengths of the Ethereum platform is that the open source code is maintained by a large community of developers that exist throughout the entire ecosystem. IBM Fabric is open source though is heavily dependent upon IBM towards ensuring functionality. R3 as a banking consortium has prominent members that will contribute to this process.

9. PERFORMANCE

Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Segmented state DB allows perfect public state consensus without relying on multi-party computation or ledger segmentation	Version 1.0 Alpha allows performance where only signatures and read/write sets transferred around network	Performance varies by which consensus algorithm is implemented. RAFT, BFT etc. Currently theoretical

Performance in live environments is constantly a challenge amount enterprise use cases. The segmentation of private state and public state databases of a platform like Quorum allow improved throughput in enterprise use cases. As of today, IBM Fabric version 1.0 Alpha has seen limited success though road map is aggressive. There have not been any successful implementations of Corda even with reconfigurations of the platform consensus mechanisms.

10. EXTENSBILITY

Enterprise Ethereum	Hyperledger Fabric	R3 Corda
Platform can be interoperable with the public chain	Fabric allows developers to use variety of libraries and requires extensive monitoring	Not interoperable with other blockchains

Within the Enterprise Ethereum Alliance, private instantiations of Ethereum are interoperable with the public chain, opening up opportunities to dramatically extend the functionality of this system. With the backing of IBM, fabric has capabilities of extending their platform to other players though would require interoperability extensions by complementary platforms. Corda was designed to be primarily used within the banking

consortium where the platform can be extended among the various members of its consortium.

CONCLUSION

Through a thorough comparison of these three platforms, it is apparent that there are various discrepancies of value pertaining to how the systems can be used and implemented within enterprise settings. While each use case has its unique set of advantages and qualifications, much should be taken into consideration regarding how relevant each system coalesces to a blockchain environment.

The use of a true blockchain compared to a distributed database or decentralized database can elucidate much in terms of how robust a platform can be in the long term. In ensuring the maximum level of immutability, security, and non-repudiation of certain systems, much should be further explored in subsequent sections of analysis. While a significant portion of this comparison is based on provided documentation and expert analysis, further details pertaining to the usability of these platforms can only be elucidated through side-by-side comparisons and parallel production of systems using all the platforms. This process will determine performance indicators and other various metrics to prove usability and robustness in an enterprise environment.