GlobalLogic®

Blockchain Interoperability (Part 2)

January 2021

By
Harish Jaggi & Raj Jha

Contents

Our Research on Interoperability - Continued

In Blockchain Interoperability - Part 1, we examined the broader concept of interoperability and why businesses need it. In this second part of the whitepaper, we continue to share findings from our interoperability research.

Oracle

Oracles are used prominently to interoperate blockchain with other systems and tools. This can be depicted as an agent that transfers external data on the blockchain platform for on-chain purposes. This is accomplished via smart contracts that infuse information about real-world events in the blockchain platform in a structured way. Such data can be emulated to train and automate processes based on real-world events, based on artificial intelligence. For example, if a disease is detected, a third-party insurance contract can be invoked automatically, notification will be propagated to all stakeholders and approvals will be sought without human intervention. Oracles are analogous to smart contracts, but with less trust quotient. To get wider applicability, Oracles will need to be equipped with trust. Two widely used solutions are using a trusted third party or using cryptographic attestations.

API Gateway

An Application Program Interface (API) can be perceived as a code snippet that regulates the access point to the server. This is a hand-shaking mechanism architects and developers need to use to interact with an API, data repository, library or code.

This interface is a wrapper that organizes the requests processed by an encapsulated underneath architecture, enabling the users to focus on business logic rather than worrying about the rest of the intricacies. This acts as a translator that receives several requests and combines and converts them into a single request, thereby reducing back-and-forth.

Co-chains - A co-chain allows a business to run an independent private blockchain while leveraging public networks to create a hybrid blockchain ecosystem. This is the best-of-both-worlds proposition. Co-chains also provide interoperability between different co-chains.

Co-chains - A co-chain allows a business to run an independent private blockchain while leveraging public networks to create a hybrid blockchain ecosystem. This is the best-of-both-worlds proposition. Co-chains also provide interoperability between different co-chains.

Algorand and Kadena are offering co-chain architecture to build hybrid blockchain solutions. Based on Algorand's literature, the main characteristics of co-chain are:

1. It works independently from the public blockchain, keeps all transactions private, chooses its own validators, and runs its own consensus algorithm.

2. Interoperates with the public main-chain and other co-chains.

3. It can use all the offerings of Algorand custom protocols like atomic transactions, layer-1 contracts, primitives and tools by default.

4. Any improvements or upgrades of the Algorand protocol will automatically apply on co-chains.

Researchers are also developing engines to establish interoperability among many heterogeneous blockchains.

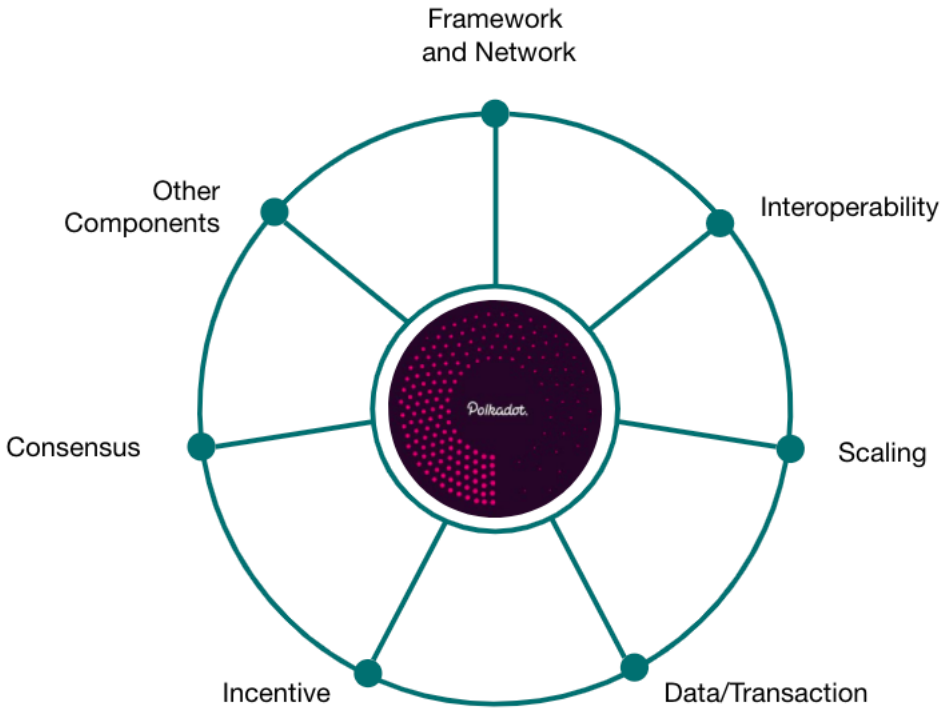
Engines

These are frameworks that construct customized blockchain and empower decentralized applications to interoperate between each other using reusable layers of consensus, contracts, network, data, scaling, incentives, application, tools and other protocols. Prominent examples are Polkadot, Cosmos, ARK and AION. We have analyzed each of these and done very deep research on Polkadot due to its wider acceptability. Thus, we will explain Polkadot to establish our thesis. The other engines behave in a similar way, with few variations.

The central chain for Polkadot is the relay chain (side-chain), which coordinates with the whole system, including parachains and parathreads. All the validators of the Polkadot ecosystem have stakes on relay chain and validate as proxy. The Polkadot ecosystem consists of parachain implementations that are actually "globally coherent dynamic data structures hosted parallel or side-by-side" to handle several use cases. Some of the parachains can be specific to particular applications, while a few of them are solely dedicated to smart contracts with utmost security or scalability. Every parachain should be able to generate proofs for state transitions. Proof generated by parachains will be validated by validators aligned to corresponding parachains.

Parachains remain connected with a relay chain by winning the secure slot in a "parachain slot auction." Parathreads do not remain connected to a relay chain but follow the same mechanism to win a time slot. The only difference between parachain and parathread is that parachain has to deposit up front to connect to a relay chain, and parathread operates on a pay-per-block basis on realization. In the Polkadot ecosystem, parachains can become parathreads and vice versa.

Parachains and parathreads are explained in the “Side-chains” section. Let’s dive deep into the Polkadot architecture to understand its core model and offering.



Levers	Polkadot Characteristics
Framework and Network	Polkadot is a heterogeneous, multi-chain network based on the Substrate framework. It guarantees cross-language support with WebAssembly, which is a light client, along with off-chain workers. This enables integration with other chains, APIs, Oracles and technologies.
Interoperability	Polkadot renders interoperability via state transition validation, consummated by the chain-relay validators. Parachains disseminate via cross-chain message percolation protocol. This protocol is a queue-based communication mechanism, essentially based on a Merkle tree.
Scaling	High scaling is possible with Polkadot. Transmission of state transition proofs from parachain to relay chain is accomplished using an erasure coding mechanism. The second tier consists of parachains. These are linked to a parachain, and that in turn is connected to the relay chain. The third level parachains are linked to second level parachains, and so on and so forth. This enables scaling of the parachains in a process known as sharding exponentially.
Data/Transaction	The Polkadot network consists of many entities that administer transactions, namely the collator, validator, nominator and fisherman. The collator constructs proofs for the validators. Transactions are subsequently executed and assembled in blocks. Collators can amalgamate to coordinate and share the rewards rendered from the block creation process. Validators construct and finalize blocks on the relay chain. The validators take them, depending on good behavior. If they misbehave, their block rewards can get denied or even confiscated for several such issues. Nominators provide their stake to validators in sharing the rewards or making them go away. Fishermen get prizes for reporting validators' misbehavior.
Incentive	Polkadot uses the DOT token as an incentive for nodes to produce results appropriately. Decentralized governance, operation and bonding are its prominent traits.
Consensus	Polkadot achieves consensus using BABE and GRANPA. BABE is the block production algorithm, while GRANPA is the finalizing algorithm. To ascertain a set of validators, it uses selection based on PoS named designated or nominated Proof-of-Stake. This is a unique type of PoS.
Other Components	Polkadot's state machine is compiled to WASM. This is a virtual environment that can trigger and run the state transition functions. Libp2p is a network library apt for peer-to-peer applications coded in the Rust programming language. These components need careful consideration in the overall architecture.

Results Based on our Four Months of Research

Disclaimer: The facts mentioned below are based on the current snapshot of work being done by blockchain interoperability projects around the globe. Research is going full throttle each day with optimized solutions just on the horizon.

We cannot compare diverse interoperability solutions because they follow different approaches, protocols and goals. Still, we took on this challenge and experimented with various options because interoperability is critical for enterprise and agnostic solutions. Being architects, we can't go wrong in today's age where the stakes are high.

Let's see the results based on critical levers:

Functionality	Description	Notary Schemes	Side-chain (2-way)	Hashed-time-locks	Co-chain	Engine
Token Portability	A token can be sent from ledger A to ledger B. Token can be rebounded (by its new owner) from B to A.	Y	Y	N	Y	Y
Atomic Swap	A transfer between two parties is assured to be executed for both entities. If one of the parties does not conform, the transfer will not take place.	Y	Y	N	Y	Y
Cross-chain Oracle	A smart contract on ledger B reads from ledger A and performs an action when a particular event or state is read.	Y	Y	N	Y	Y
Cross-chain Asset Encumbrance	Tokens are locked on ledger A, and locking conditions are dependent on events on ledger B.	Y	Y	N	Y	Y

Deeper quantified results of these industry solutions are as follows:

Adoption Parameters	Notary Schemes	Side-chain	Hashed-Time-Locks	Co-chain	Engine
Interoperability Applicability	Permissionless chains but decentralized schemes can be used for interoperability among any kind of chains like Polkadot is doing	Permissionless chains	Permissionless chains	Hybrid chains (permissionless and permission)	Any chain under the sun
Data Exchange	Arbitrary data	Arbitrary data	Only digital assets, i.e., make bitcoin spendable on Ethereum dApp	Arbitrary data, i.e., based on tracking data from chain A trigger payment on chain B	Arbitrary data
Third-Party Need	Y	N	N	Y/N	N
Security	Single point failure	Secure	Secure	Secure	Secure
Latency	High	High	High	Very low	Very low
Vulnerability	Attacks possible, i.e., double spend	Attacks possible, i.e., double spend	Attacks possible, i.e., double spend	Less vulnerable	Much less vulnerable
Ease of Implementation	Medium	Hard	Easy	Easy	Hard
Transaction Finality	Decreases	Decreases	Decreases	Does not decrease	Does not decrease
Consensus Protocol Used by Solutions	Not applicable	Loom Network (delegated Proof of Stake) Liquid (Strong Federations)	Wanchain (Proof of Stake)	Algorand (pure Proof of Stake)	Polkadot (BABE and GRANPA) Cosmos (Tendermint)
Maintenance	Moderate	Moderate	High	Moderate	Low
Scalability	Moderate	Moderate	Moderate	High	High

Results Based on our Four Months of Research

Interoperability Mechanism	When to Use	Practical Applications
Notary Schemes	When interoperable blockchains BA and BB are both public and need to implement cross-chain transactions. When federation(s) or Notary(ies) are required to validate the transactions based on agreed consensus for interoperability. When use cases (such as custodial wallets) need to be implemented.	Crypto Central Exchanges. The famous Ripple technology also uses Notary mechanisms to exchange assets between global financial companies.
Hash-time-locks	When interoperable blockchains BA and BB are both public and need to implement Cross-chain atomic operations. When use cases like decentralized exchange, micro-payment (high volume/low latency), or cross-chain atomic swap are the core themes.	Wanchain, Komodo, LN, etc.
Side-Chain	When the mainchain needs scalability via the side-chain. When two-way-peg solutions need to be implemented.	Y BTC-Relay, Loom-Network, Liquid, etc.
Co-chains	When interoperable blockchain BA is permissionless but BB blockchain is permissioned or of consortium type. When businesses can perform private transactions on a permissioned blockchain and save transaction proof hash on a permissionless blockchain like Markel root or ZKP.	Algorand, Kadena
Engine	When interoperable systems are heterogeneous and there is a business need to establish a custom blockchain for interaction between the systems.	Polkadot, Cosmos, etc.
Oracle	When data needs to be shared from non-blockchain solutions to a blockchain solution via smart contracts.	Oracle Agent
API Gateway	When two non-compatible systems have to share data.	Custom code implementation

Conclusion

In this paper, we researched and took a systematic deep dive into industrial practices for blockchain interoperability. We elaborated on the importance of interoperability for enterprises as a core theme, with solid answers based on every single solution being contemplated under the sun, such as a crypto-based approach, Oracle, gateway, co-chain and some of the latest techniques, such as engines.

Since blockchain is a next-generation technology that is evolving with each passing day, several bottlenecks arise when attempting to make it work in large-scale enterprise solutions. There is hardly any implementation seen in the blockchain world where interoperability was successfully implemented on a large scale. This challenged us to research various solution offerings being developed around the globe.

Being architects, it was very important for us to educate clients about the right solution because this is a fundamental problem statement. Over the last six months, however, we have seen many solutions reach an inflexion point. This research gave us clear answers to pick the right solutions for a variety of use cases, coupled with realizing affordability, scalability and maintainability aspects of each one of them. Clear recommendations and applicability of various solutions in each category will help architects immensely.

Similarly, institutions such as the Chamber of Digital Commerce have formed crucial alliances with government bodies to attain the right regulatory balance. Evolving consensus mechanisms are now able to achieve the high scaling needed in enterprise solutions. This is indeed a eureka moment, as the three biggest problem statements in adoption of blockchain (scaling, regulatory frameworks and interoperability) are seeing credible solutions emerge.

This paper is forward-looking and helps make the blockchain ecosystem more practical and useful for enterprises and the architectural community. Knowledge and support for blockchain applicability will increase significantly based on these interoperability recommendations.

Version 2.0

We identified multiple new subjects and solutions around DL interoperability, such as the introduction of a third party (in Notary schemes), state finality between probabilistic and deterministic ledgers, state distribution between permissioned and permissionless ledgers and the double spend attack. Probing deeper into the details of these topics will be part of future work on interoperability.

Researchers and industries are also going ahead with principles of using a “blockchain of blockchains,” “cross blockchain dApps solutions” and undertaking other next-generation experiments to deal with complex use cases for permissioned blockchain interoperability. These are currently at a rudimentary level and are therefore beyond the scope of this paper, for now. We will research them once they attain maturity and surpass beta version stipulation, enabling us to pen down V2.0 in the near future. Stay tuned!

About the Authors

Harish Jaggi is a hard-core techie, a researcher, blockchain incubation expert, and a huge proponent of blockchain technology. He is spearheading the India charter of blockchain practice at Globallogic. He has over 20 years of extensive experience in the Information Technology industry and has 12 diverse certifications, including 3 on blockchain technology. He has extensively worked on Ethereum, Hyperledger, Solidity and Interoperability research in diverse domains. He has spearheaded blockchain projects, advisories, and initiatives since 2015. He is a regular speaker in prominent forums and meetups on blockchain technology. Many of his articles have been published by leading media houses.

Raj Jha is a researcher, open-source contributor and blockchain architect with several successful blockchain implementations to his credit. He is a senior blockchain architect at Globallogic. He carries 15 years of diverse experience in the Information Technology industry. He carries many certifications, including blockchain solution architect certification. He has extensively worked on Ethereum, Hyperledger, Solidity and Interoperability research in niche areas of application. He has played a coveted role in blockchain projects, advisories, and initiatives for years. His expertise lies in the integration of blockchain with third parties and prominent tools. Many of his articles have been published by leading media houses.

References

Our sincere thanks to the researchers and authors whose work inspired us. We admire your work in taking the blockchain bandwagon forward. Our sincere apologies if we have inadvertently missed any reference.

- R3 Reports
- Inclusive Deployment of Blockchain for Supply Chains: Part 3 – Public or Private Blockchains – Which One Is Right for You?
- Algorand Co-Chains
- How Co-chain Opens Many Possibilities On Blockchain?
- Blockchain in Global Supply Chains and Cross Border Trade: A Critical Synthesis of the State-of-the-Art, Challenges and Opportunities
- A Protocol for Interledger Payments
- A Primer on Blockchain Interoperability
- Algorand: Scaling Byzantine Agreements for Cryptocurrencies
- https://www.r3cev.com/s/ Chain-Interoperability-R3-Viewpoint-2.pdf

GlobalLogic®

GlobalLogic is a leader in digital product engineering. We help our clients design and build innovative products, platforms, and digital experiences for the modern world. By integrating strategic design, complex engineering, and vertical industry expertise, we help our clients imagine what's possible and accelerate their transition into tomorrow's digital businesses. Headquartered in Silicon Valley, GlobalLogic operates design studios and engineering centers around the world, extending our deep expertise to customers in the communications, automotive, healthcare, technology, media and entertainment, manufacturing, and semiconductor industries.



www.globallogic.com