MAP PROTOCOL – THE BLOCKCHAIN ASSETS FREEWAY

ABSTRACT

As more and more blockchains come to fruition, the barriers between chains are becoming more and more bothersome. Besides, the emerging of various layer 2 networks are adding more gravity to the problem. The diversity of the features of different blockchain networks makes connecting all chains extremely hard, if not impossible. Many solutions have been proposed, but very few are satisfying either due to the presence of the privileged admin role or due to the limit number of blockchains that can be connected. With these in mind, we are here to present the MAP protocol, a trustless cross-chain communication protocol to connecting all kinds of blockchains. MAP protocol team is tasked with the mission to build the digital assets freeway for the ever-growing blockchain world. The protocol itself aims be the secure end-to-end solution for any blockchain resident to move and exchange assets freely and quickly. To fulfill this role, MAP team is building on three layers simultaneously: a dedicated blockchain served as the infrastructure freeway connecting all kinds of blockchains to break the barriers; the MAP Assets layer where all kinds of assets are mapped to MAP chain in a non-custodial style via trustless smart contract; and the DeFi Application layer where all kinds of applications including but not limited to DEXes, games and NFTs can be built with the cross-chain capabilities enabled by the MAP chain and MAP assets.

INTRODUCTION

Since the birth of the Bitcoin in 2009, thousands of public chains have been produced by using blockchain technology and those are widely used in multiple application fields such as IoT, finance, governance, identity management, and traceability. In the early 2010s, there are only few blockchain. And the terminology blockchain interoperation mostly refer to the cross-chain technology of transferring coins between these blockchains. In 2016, Vitalik Buterin summarizes the ways of reaching interoperability into three primary categories of strategies [1]: 1) Hash-locking: setting up operations on two chains with the same trigger, e.g., the preimage of a particular hash. 2) Centralized or multisig notary schemes: where a party or a group of parties agree to carry out an action on one chain should some event on another takes place; 3) Sidechain/relays: where one blockchain can validate and read events and/or state in other blockchains.

Hash-locking technique, especially hashed time-locks contracts (HTLCs) [2] inspire trustless atomic cross-chain swap [3] where assets sitting on separate blockchains can be exchanged directly in a Peer-to-Peer way without involving any mediation or escrow service. The downside side is that such kind of atomic swap cannot be easily generalized and needs to be carefully constructed according to the features of target blockchains. Although, HTLCs are the foundation of famous lightning networks [4], we are not seeing large scale deployment of cross-chain interoperability following hash-locking technique. Centralized notary schemes are the easiest technique strategy and normally provide more fluent user experience by employing centralized servers. The downside is also obvious. All users must blindly trust whoever is providing the service and believe in good faith even when large scale of assets is under custody. Clearly, this is not the path we'd like to follow. Two-way pegged sidechain [5] and BTC-Relay [6] belonging to the third category as outlined by Buterin, where the former can transfer digital asset from parent chain to side chain and the latter opens a one-way bridge from Bitcoin to Ethereum. In both scenarios, the receiver side need to verify that something happened on the sender side. This is where the SPV (Simplified Payment Verification) technique [7] kicks in. To facilitate SPV technique, one needs to build a light client for the interesting blockchains. But before we dive into the jargons, let's take a step back and get a bird's-eye view of the cross-chain interoperability problem.

Blockchain technique is also called distributed ledger technique and is often regarded as a distributed database. Any user can read & write to this database. Read means users could retrieve the data from the blockchain (e.g., state of certain accounts or transaction in certain blocks). It can be achieved by query full node (i.e., a node downloading the entire blockchain and update internal state in real time). Besides, users could read from the blockchain using SPV technology. SPV is much cheaper in network cost than fully synchronization. And to write to the blockchain, users must broadcast their write requests (pending transactions) to the P2P network and wait for the consensus engine to commit them, e.g., packed into a block.

Analogously, chain interoperability means one blockchain (active chain) can read/write to another blockchain (passive chain). Most current chain interoperability solution suggest using SPV technology for cross-chain read. By reading with SPV technology, all information is accompanied with cryptographic proof and the receiver need a way to get “trusted” or “real” block header of the corresponding chain. In this way, the receiver can verify the cryptographic proof against the info contained in the “trusted” header. In the cross-chain write scenario, the receiver is the passive chain. If the passive chain can verify that certain things happened on the active chain, it can change its on-chain state to respond to such awareness. Of course, any state changes on the passive chain must be triggered by valid transaction. In this context, someone must construct a valid transaction containing the things happened on the active chain as well as the related cryptographic proof and submit the transaction to the passive chain. Once this transaction is committed to a confirmed block of passive chain, the cross-chain write is complete. Then another problem pops up, how can the passive chain get the aforementioned “trusted” block header of the active chain? Some solutions introduce “the trusted relayer” to guarantee the truthfulness. Once again, to maintain the trustless property of MAP protocol, we don’t take this road, but employ a dedicated blockchain – MAP chain – to maintain light clients of all interested blockchains.

Atomic swap, two-way pegged sidechain, BTC-Relay are all early solutions of chain interoperability and are mostly designed for specific blockchain and thus not systematic. This means these solutions is hard to extend for constructing an interoperation network for multiple

chains. Then, two systematic interoperation protocol Polkadot [8, 9] and Cosmos [10] were proposed.

Polkadot defines a complete cross-chain interoperability underlying protocol. It has a complete cross-chain read and write specification, and through this protocol, it built a complete cross-chain interoperability ecosystem. The characteristic of Polkadot is to communicate and coordinate the cross-chain interoperability of all para chains through a relay chain. The validator on the relay chain will be allocated to each para chain to work with its collator, and the para chain block header provided by collator will be synced to the relay chain. After that, the XMCP protocol [11] is used to transfer cross-chain messages. Of course, the cross-chain status needs to be obtained through the SPV solution after obtaining the block header from the relay chain, and the cross-chain write operation needs to be customized through the para chain. The smart contract system parses the specification information defined by XMCP and executes it. We must note that the soul of Polkadot is the relay chain. The relay chain not only needs to coordinate cross-chain information interaction, but also take the responsibility of the shared security in the entire system.

Cosmos is also a complete cross-chain interoperability operating system. It defines a set of IBC [12] protocols for cross-chain communication, which can guarantee asset transfer or data transmission between different chains, and communication between different HUB chains requires cross-chain communication through the IBC protocol. Reading between different HUB chains requires a Relayed cluster to provide blockheads. The design of the IBC protocol is like the two-way pegging. It consists of four parts: first, Tracking, where the Relayed cluster collects block headers for each HUB chain; then Bonding, which locks a portion of an asset on a chain; and then Proof Relay, which gets the block head and corresponding SPV proof from the Relayed cluster; and finally, The Validation, the proof obtained in the next step is validated and can be followed if the validation passes. Cosmos's cross-chain read operations rely on SPV proof provided by the Relayed cluster, while cross-chain writes required subsequent operations through the proof of validation through smart contracts.

Do we still need MAP protocol after the emergence of Polkadot and Cosmos? The answer is YES. Indeed, MAP protocol shares many similar features of Polkadot and Cosmos, i.e. rely on

cryptographic proof rather than trusted relayers when verifying cross-chain message, facilitate cross-chain transfer as well cross-chain swap, the dedicated MAP chain also adopts Proof-of-Stake and Byzantine Fault Tolerance consensus just as Polkadot and Cosmos. Yet, the biggest difference is that Polkadot and Cosmos have been focusing on connecting isomorphic chains within its own ecosystem, e.g. blockchains built with Substrate or Tendermint Core and Cosmos-SDK. This explains the current isolation state of both realms from the flourishing EVM world. With MAP protocol, we started our journey with the mission to connect heterogeneous blockchains, with a dedicated blockchain we can easily add in necessary features to connect all existing blockchains as well as those yet to come. By supporting IBC protocol on MAP chain, MAP chain can easily talk to the Cosmos world. By integrating ICMP protocol, MAP chain can connect Polkadot world. By building cutting-edge protocol for Proof-of-Work chains, MAP can even connect Bitcoin as well as Ethereum. In this way, we are hoping to build the real asset freeway for the blockchain world to enable the circulation all kinds of assets on heterogeneous blockchains.

MAP Protocol Overview

Map protocol aims to be the secure end-to-end solution for any blockchain resident to move and exchange assets. The chain itself can achieve lightweight arbitrary interaction without the need to relay through a relay chain under the independent self-verified consensus mechanism. And for the non-independent self-verified consensus mechanism, the chain can achieve lightweight arbitrary interaction through the relay anchoring mechanism. The reason for the difference here is that blockchains of independently self-verified consensuses (e.g., POW, POS, etc.) can independently verify the legitimacy of individual blocks. However other consensus mechanisms such as DPOW, DPOS, which need to be anchored to other relay chains because additional electoral representation information is required to verify the legitimacy of blocks. Any blockchain system that supports MAP protocol can interoperate with other blockchain that also supports the MAP protocol. In this way, an open blockchain interoperability ecosystem is formed. There are no specified relay chains or other types of central chains in the MAP ecosystem and each blockchain system maintains sufficient independence to ensure the validity and consistency.

Unlike other inter-blockchain communication projects, where mass assets are controlled by a handful of operators, we are building the whole solution in a more trustless and decentralized way. This means there is no trust third party. The security of MAP protocol should rely on the cryptographic evidence. To fulfill this role, MAP protocol is building on three layers simultaneously: 1) MAP chain, a dedicated blockchain that is fully EVM-compatible to maintain light clients of all interested blockchains to facilitate the trustless verification of cross-chain message; 2) MAP assets layer, transparent and bulletproof smart contracts to hold all wrapped cross-chain assets in a non-custodial style; 3) DeFi application layer, where all kinds of applications including but not limited to DEXs, Games and NFTs can be built with the cross-chain capabilities enabled by the MAP chain and MAP assets.

The underlying blockchain of MAP protocol serves as the light client to all interested blockchains. Using a dedicated blockchain to maintain all the light clients gives us the flexibility to integrate necessary features to connect to all kinds of blockchains that might come up. With the info preserved light clients, the MAP assets layer can easily validate the cross-chain message in a pure mathematical way. In this way, the assets guarded can only be moved around following fixed rules driven by cross-chain message with cryptographic proof. That is, no one in the system have the privileged power to touch users' fund and the trustless of MAP protocol is realized.

MAP CHAIN

MAP chain is fully EVM compatible build upon Proof-of-Stake mechanism and Byzantine Fault Tolerant consensus protocol. As aforementioned, the main purpose of MAP chain is to maintain light clients of all interested blockchains to facilitate the trustless verification of cross-chain message. Only in this way, can MAP protocol eliminate the unreliable human factor from the cross-chain communication, especially on the assets management process. That is, the correctness of the light client is the trust anchor of the whole MAP protocol. Thus, the main task of MAP chain is to maintain this anchor trust in pure mathematical way so that users of MAP protocol need to trust only the safety of the cryptographic primitives that already form the foundation of the whole blockchain universe.

IBFT AND POS

The technology strategy for MAP chain is easy to understand by considering the development of the blockchain world in the last few years. The explosive development of DeFi has made EVM the de facto industry standard platform to develop smart contracts. The criticism on the energy consumption of Proof-of-Work mechanism is pushing the whole blockchain world shifting to a more energy efficiency form. With the research advancement regarding to the safety of PoS, especially on the discovery of the infamous long-range and nothing-at-stake attacks as well as the proposition corresponding mitigation solutions [13], the once fragile PoS mechanism can now operate smoothly and safely. The actual operation experience of Cosmos, Polkadot and other PoS networks also prove the case. The possible forks intrinsic to the Nakamoto consensus is not user friendly, especially for those on-chain activities with strong financial attribute where one would like to know for sure if one transaction succeed or not instantly. This is where is Byzantine Fault Tolerance consensus protocol comes into play, especially with the inventory of PBFT (Practical BFT) protocol [14] and the improvement regarding to the blockchain scenario since then, such as IBFT (Istanbul BFT) [15-17], Tendermint [18, 19], HotStuff [20] etc. Nowadays, BFT consensus can easily scale to 100+ validators node while still guarantee network stability and quick confirmation within seconds to provide better user experience.

MAP chain adopts the leader based IBFT consensus featuring its simpleness, immediate finality, robustness in an eventually synchronous network as well as the support for dynamic validator set. With tons of research and engineering efforts into the IBFT consensus protocol, not only the safety and liveness can be guaranteed, but also a solid foundation is built so that we can quickly boost MAP Protocol. The validator set required by the IBFT protocol is selected and updated via the PoS mechanism mainly according to the staking weight measured in MAP token, the native token asset of MAP chain, among all candidate validators. To guarantee the diversity and robustness of the network, MAP chain supports at most 100 validators at the beginning and it will gradually extend to bigger size by continuously engineering optimization and by closely following the advancement from both academic and industry world.

Staked validators are rewarded with MAP token according to the amount of token staked as well as the stability of their node, e.g., the efforts they devoted to maintain MAP chain. Holders of MAP token can either operate their own validator node or delegate their token to a well-established validator node to earn rewards. To attract more holders of MAP token to participate in the PoS mechanism, the incentive will be dynamic adjusted according to the ratio of staked token against the total tokens in circulation, e.g., the incentive will be automatically increased if the ratio goes down below a target value. Also, the incentive will be adjusted towards the other direction in case the staking ratio had reached certain level so that there are always enough assets in free circulation to keep the whole ecosystem healthy. There are other ways for MAP holders to earn more reward, such as being a “relayer” and feed the MAP chain with all kinds of message related to connected blockchains to keep the chain up to date or to earn rewards by contributing directly to the code base of MAP protocol, building inside the ecosystem and helping to boost the protocol etc.

Block of MAP chain is generated in epoch-based style. At end of each epoch a new validator set is selected according to the amount of staked MAP tokens. During one epoch, the set of validators remains intact, and the blocks are produced following leader-based style of IBFT consensus. Leader is chosen in a weighted round-robin way among all selected validators, where the chance of each validator get selected as leader is proportional to their staking weight. Note that there is also an on-chain random seed used as input parameter to add more entropy to the leader selection procedure. In this way, validator nodes can be protected from planned DDoS attack since no one can predict which one will be the next leader. Besides, public verifiable on-chain randomness is a crucial to on-chain fairness. On the blockchain level, MAP chain can utilize this to randomize the transaction sequence within the block to mitigate the infamous front-running attack [21], MEV (Miner Extractable Value) [22] etc. On the DeFi application level, a more transparent and fairness DeFi rules be easily drawn. On chain randomness is hard to build, especially to reach the unbiased property. MAP chain starts with an easy commit-and-reveal mechanism with the participation of staked validators. That is the proposer of each block will commit to a random value in that block, and the random value will only be revealed and added to on-chain entropy after some time. The introduced delay from commit and reveal is important to prevent the validator from trying to manipulate the on-chain randomness. Yet, we are seeing progress from academic world proposing better ways to solve the problem. Whenever a better solution is ready to massive deployment, MAP chain will absorb the cutting-edge solution.

On the design rational of MAP chain, we share the same view as Ethereum, especially on the sandwich complexity model. That is the bottom level architecture should be kept as simple as possible. Following this rational, the PoS mechanism, the on-chain randomness mechanism as well as the various light clients maintained by the chain are all implemented as smart contracts resident on MAP chain. Only in this way, we can quickly add in new features, e.g., a new type of light client of a new blockchain while keeping the consensus layer of the chain stable. Then a big question arises, is it possible to implement a light client for all blockchains? Luckily, the answer is YES.

LIGHT CLIENT

To validate the cryptographic proof for cross-chain message, a trusted root is required. Normally the cryptographic proof is the existence Merkle proof of a specific value in a (variant) Merkle tree, e.g., the Merkle Patricia Tree (MPT) in Ethereum or Immutable AVL (IAVL+) tree used in Cosmos and the trusted root is the Merkle root of the tree that is usually included in block header. Then by feeding all block headers of all interested blockchains to MAP chain, the availability problem of trusted root can be easily solved. Yet, with continuous efforts put into shortening the block generation internal, processing all uploaded block headers on MAP chain would consume considerable resources, especially when we are trying to connect more and more blockchains like Binance Smart Chain and Polygon networks are already producing blocks every 2 or 3 seconds. Another problem is that, how to validate the correctness of the uploaded block headers? The design of MAP protocol is to remove all trusted parties, thus relying on trusted parties to upload correct block headers is clearly not an acceptable solution. Following the advancement of SPV technology and light client construction technology, both problems can be solved in a trustless way. The core observation is that almost all blockchains can reach consensus with very limited information.

Nakamoto consensus-based chain, e.g., Bitcoin, new block header can be easily checked following the consensus rules, e.g., the hash link as well as the accumulated work etc. If Bitcoin network won't re-org more than n blocks, then a light client of Bitcoin only needs to preserve n+1 newest block headers to verify new block headers and update its internal state in an autonomous way. Considering the latency to relay the crossing-chain message, light clients built this way can store more block headers, e.g., block headers generated in the last 48 hours. With Bitcoin's 10-minute block interval, light client on MAP chain only needs to store 288 block headers. All block headers of Bitcoin need to be fed into MAP chain in this way, yet this is quite acceptable considering Bitcoin's block interval. On the other side, by adopting Flyclient technique, the number of blocks uploaded to MAP chain can be significantly reduced. Although the genesis state of a light client requires to be manually set up, the trustless feature is not compromised since anyone can check the correctness of the genesis state. We conject that this is basically the same as the "weak subjective" concept [23] populated in the Proof-of-Stake world.

For Proof-of-Stake and BFT based blockchains, the construction of light client might seem quite difficult at the beginning. Thanks to the work of the Tendermint team, it turns that a more efficient light client can be built [24]. While the technique detail could be quite lengthy, the core idea is simple. In such networks, blocks are signed off by a group of selected staked validators, so by verifying a few digital signatures, the validity of a block can be easily checked. The set of validators could change over time, but in typical PoS networks, new set of validators also needed to be proved by the old set via signatures. In this way, with only a little information of current validator set, e.g., staked weight, public keys of each validator set, a light client can easily check new block headers as well as updating itself. There is even no need to upload all block headers, only a tiny few, e.g., those involved in a cross-chain operation, or validate set upgrade.

Light clients on MAP chain are initialized as smart contracts, so that the chain can quickly add new light client for new blockchains connected by MAP chain. Merkle proof verification and digital signature verification are crucial to the construction and operation of light client. But, implementing these cryptography primitives with Solidity is both tricky and inefficient, especially various cryptography primitives are used in different blockchains. To ease the development of light clients, all kinds of cryptography primitives are supported at the blockchain level and are exposed to EVM via pre-compiled contracts.

Solely maintaining light clients of connected blockchains on MAP chain is not enough for bidirectional cross-chain interoperation in a trustless style, MAP protocol requires the existence of MAP chain's light client on each connected blockchain. While on MAP chain, the gas price can be continuous optimized to stay as low as possible, on other chains, we must accept the reality. As MAP chain adopts PoS and IBFT, a light client can be easily built following above technique. To optimize the gas consumption of the light client on other chains, MAP chain adopts aggregate signature with BLS12-381 curve. In this way, the verification of the signatures of MAP chain's validators can be reduced to verify only one aggregated signature with one aggregated public key. As Ethereum is preparing to enable BLS12-381 related precompiled contracts, it can be expected that precompiled contracts of BLS12-381 will be widely supported in the near future.

RELAYERS

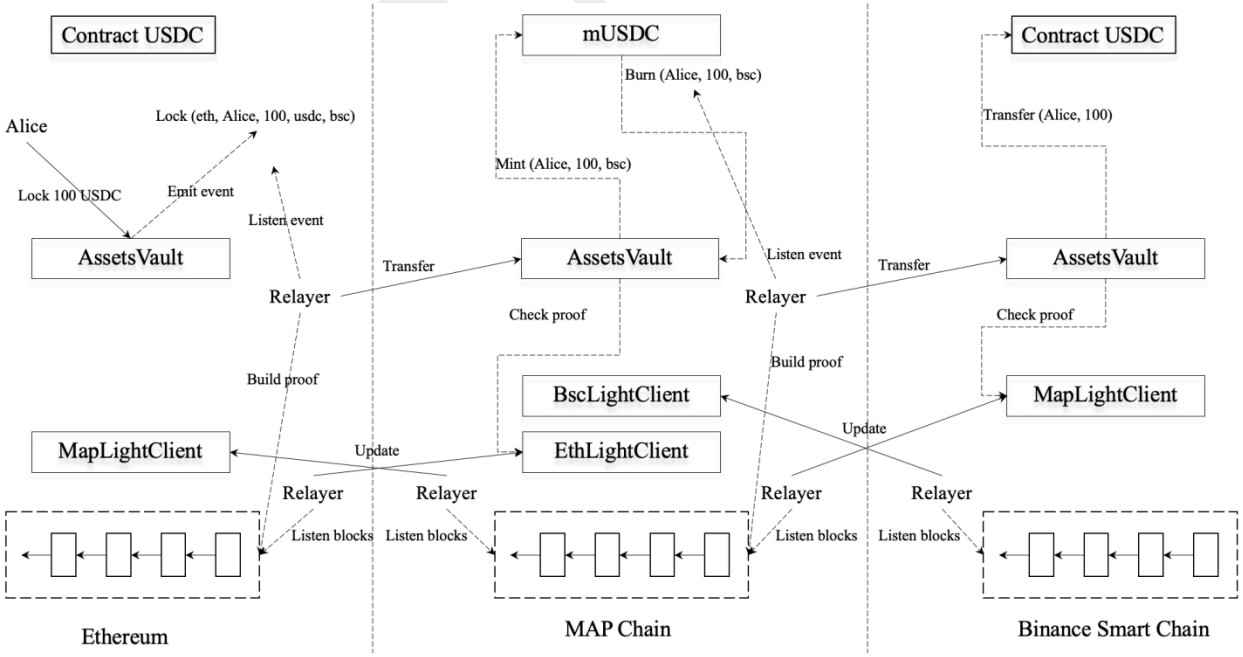
Light clients of connected blockchains on MAP chain and light clients of MAP chain on connected blockchains needs to keep up with the growth of the corresponding blockchains. This is where the relayer cuts in. Besides submitting block headers to various chains, relayers are also responsible for helping users to deliver cross-chain messages, such as cross-chain transfer. As submitting transactions to blockchains would consumes gas, all relayers are rewarded according to the useful work they have accomplished, e.g., the number of effective block headers submitted, the volume of cross-chain transfer.

After correctly set up, each light client can verify newer block headers according to the rules coded in the contract, so that dishonest relayer won't be able to trick the light clients to accept invalid block headers. Or in other worlds, the security of MAP protocol does not rely on trusted or honest relayers. With the existence of the reliable light clients, other applications on MAP chain can check the validation of cross-chain messages against the info provided by light clients. In this way, relayers cannot trick the on-chain application to accept forged cross-chain messages. This is vital for the security of MAP Assets layer, concerning the security of a mountain of assets. Besides,

we are also investing ways for relayers to participate in the on-chain random number generation process to help forge better on-chain randomness.

MAP Assets Layer

Assets management of cross-chain transfers is quite error-prone and usually comes with super admin who is capable of touch user funds. Nowadays, cross-chain transfer is the essential component for cross-chain interoperability, MAP protocol provides a trustless and solid solution to relief MAP ecosystem builders from the burden of technical challenge and security risks. The MAP assets layer is composed of bulletproof smart contracts dealing with cross-chain transfers and guarding users' funds. There is no privileged admin in the system and all asset-related operations such as minting, burning, and more can only be triggered with a cross-chain message backed by valid cryptographic proof, e.g., a Merkle proof. The cryptographic proof is checked against the information provided by the client clients.



Cross-chain assets are locked in the AssetsVault contract of that chain. For assets moving to MAP chain, MAP chain will wrap all assets from different chains, e.g., mUSDC is the wrapped USDC on MAP chain for USDC on Ethereum, BSC, etc. In the figure above, there is a MapLightClient contract deployed on Ethereum and Binance Smart Chain, respectively, and there are BscLightclient and EthLightClient contracts deployed on MAP chain. Relayers are monitoring each networks' status and update each light client by submitting new block headers to the corresponding contract. As we said before, light client here is to provide a trust root for the verification of cross-chain messages.

Let's illustrate what really happens behinds the scene if Alice is using MAP protocol to move 100 USDC from Ethereum to BSC via MAP chain.

1. Alice interacts with contract AssetsVault on Ethereum, to lock her 100 USDC to the vault.
    a. After the transaction is packed and successfully executed by Ethereum, Lock event is emitted indicating that Alice has indeed locked 100 USDC in contract AssetsVault to move the fund to BSC.
2. One relayer spots the Lock event emitted by contract AssetsVault on Ethereum and builds the corresponding Merkle proof to prove that this event is emitted by contract AssetsVault at certain block height. With all the information ready, this relayer submitted a proper transaction to contract AssetsVault on MAP chain.
    a. If the transaction is packed and during the execution of this transaction, contract AssetsVault on MAP chain queries contract EthLightClient to get the Merkle root at the corresponding block height and validate the cryptographic proof carried in the transaction.
    b. If the cryptographic proof passes the check and the corresponding event is not processed, contract AssetsVault will instruct contract mUSDC to mint 100 mUSDC for Alice.
    c. Then in the same transaction, the minted 100 mUSDC is burned and an event is emitted indicating that Alice is burning 100 mUSDC in order to have 100 USDC on BSC.
3. One relayer spots the Burn event emitted by contract mUSDC on MAP chain and builds the corresponding Merkle proof to prove that this event is emitted by contract mUSDC at

certain block height of MAP chain. With all the information ready, this relayer submitted a proper transaction to contract AssetsVault on BSC.

a. If the transaction is packed and during the execution of this transaction, contract AssetsVault on BSC queries contract MapLightClient to get the Merkle root at the corresponding block height and validate the cryptographic proof carried in the transaction.
b. If the cryptographic proof passes the check and the corresponding event is not processed, contract AssetsVault will transfer 100 USDC to Alice's address. Now Alice's 100USDC has been successfully transferred from Ethereum to BSC.

Note that if Alice is transfer 100 USDC from Ethereum to MAP chain, then she will end up with 100 mUSDC sitting in her address on MAP chain. No trusted parties are involved in the above processing. All state changes related the assets moving are driven by the proper cross-chain messages with cryptographic proof submitted by relayers. In the above procedure, Alice only needs to send on transaction and all the rest are taken care by relayers in a pure trustless way.

APPLICATION LAYER

With the fundamental cross-chain transfers provided by the combination of MAP chain, light clients and MAP assets layer, cross-chain DeFi application can be easily built. The same asset scattering over multiple chains is reunited on MAP chain. With more and more assets converging on MAP chain, we are expecting MAP chain to be a central hub for assets circulating across whole blockchain world. Under this construction, all users safely migrate all their digital assets from one chain to another without chain barriers. Of course, we would need liquidity providers on each chain to lock some assets into the assets vault to kick start the whole system. Aside from the cross-chain fee that collected, liquidity providers will also be rewarded with MAP tokens.

With the burden of dealing with cross-chain messages and heterogenous blockchains, blockchain developers can focus on what they can build in a world without barriers, might be a cross-chain

DEX which finds the best exchange ratio across whole blockchain world for its users, might be NFT trading market where one can bid on any NFT even without the demand token in your wallet (that is bid with what you have and let the network swap for you automatically with the demand assets), or maybe a cross-chain data markets, where all kinds of information, e.g. prices from different chains are available in one place. Just migrate your DeFi application to MAP chain to enjoy the aggregation of diverse assets.

MAP Economic Model

MAP is the native token issued by the Map Standard Chain. The initial total amount is 10 billion. With the following application scenarios to help to improve the intrinsic value of MAP protocol as well as promote the development of the MAP protocol.

1. MAP chain uses PoS mechanism and nodes need to stake enough MAP tokens to become a validator candidate. Validators would receive rewards in MAP tokens if they are selected to participate in the consensus procedure.
2. Normal users can delegate their MAP tokens to preferred validator nodes to help the validator gain more staking weight and receive MAP token rewards by doing so.
3. Users with enough skills can also running a relayer node to help processing all kinds of cross-chain messages and receive MAP token to compensate gas consumption and earn more.
4. Holder of MAP token can participate in the on-chain governance once the module is finished and vote for the feature that you wanted, e.g. which blockchain should MAP chain connect first.
5. MAP tokens would be rewarded as incentives for Ecosystem contributor who improve MAP protocol, build Dapps and expanding technical or user communities

MAP New Tokenomics

To fully embrace Web3, MAP Protocol will incorporate DAO as a new important legal structure to promote various ecological participants to participate in MAP mainnet and its cross-chain

operation in the future. The DAO will serve as new primitive to realize the rights and interests for its users. Tokens and assets belonging to the ecological part will be voted by users in the form of proposals and users are able to participate, earn part of the tokens and share the benefits together. The new token distribution will be as follows:

Total Supply: 10,000,000,000 MAP

1,500,000,000 MAP (15%): Team

1,200,000,000 MAP (12%): Foundation

2,100,000,000 MAP (21%): Ecosystem (This Ecosystem removes the previous released 3.11% of 21%. The remaining 17.89% will form a DAO Treasure, used for developer incentives, cross-chain vault incentives, marketing and community incentives, etc. It will be released through DAO governance, and community members can participate in voting through community proposals. Participate and earn part of the tokens, and also share the benefits.)

2,200,000,000 MAP (22%): Institutions and Partners

3,000,000,000 MAP (30%): Mining (Increase mainnet mining rewards proportion to 30%. PoS mining will be released through 10 years. 3% (300,000,000 MAP) per year for PoS validator node incentives.)

Part	Previous	New	Details
Team	20%		**15%**
Foundation	15%		**12%**
Technical	9%	Ecosystem DAO	**21%**
Ecosystem	9%		
Institutions and Partners	32%		**22%**
Marketing	15%	Mining	**30%**

CONCLUSION

Centralized cross-chain interoperability can be quickly built, but all users' funds are at risk due to the blind trust on a few selected parties, as well as the extended attack possibilities introduced as demonstrated by the Poly network hack. Yet, the construction of decentralized cross-chain interoperate protocols can be challenging on the engineering side, but users are released from the aforementioned FUD. That is the reason behind the technical strategy of MAP protocol. Let the team take the engineering challenges as well as the burden, but let our users feel sense of relief and enjoy a safe and borderless cryptocurrency realm.

REFERENCES

1. Vitalik Buterin. "Chain Interoperability". September 9, 2016. https://allquantor.at/blockchainbib/pdf/buterin2016chain.pdf
2. Bitcoin Wiki. 2016. Hash Time Locked Contracts. https://en.bitcoin.it/wiki/Hash_Time_Locked_Contracts
3. Maurice Herlihy. 2018. Atomic cross-chain swaps. In Proceedings of the Annual ACM Symposium on Principles of Distributed Computing. Association for Computing Machinery, New York, New York, USA, 245–254. https://dl.acm.org/doi/10.1145/3212734.3212736
4. Joseph Poon and Thaddeus Dryja. 2016. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. Technical Report. Lightning Network. https://lightning.network/lightning-network-paper.pdf
5. Adam Back, Mark Friedenbach, Andrew Miller and Jorge Timón. 2014. Enabling Blockchain Innovations with Pegged Sidechains. https://blockstream.com/sidechains.pdf
6. BTC Relay Github repo. https://github.com/ethereum/btcrelay
7. Satoshi Nakamoto. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf
8. Gavin Wood. 2016. POLKADOT: VISION FOR A HETEROGENEOUS MULTI-CHAIN FRAMEWORK. https://polkadot.network/PolkaDotPaper.pdf
9. Jeff Burdges, Alfonso Cevallos, Peter Czaban, Rob Habermeier, Syed Hosseini, Fabio Lama, Handan Kilinc Alper, Ximin Luo, Fatemeh Shirazi, Alistair Stewart and Gavin Wood.

2020. Overview of Polkadot and its Design Considerations. https://arxiv.org/pdf/2005.13456.pdf

10. Jae Kwon, Ethan Buchman. 2016. Cosmos Whitepaper. https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md
11. XCMP overview. https://research.web3.foundation/en/latest/polkadot/XCMP/index.html
12. IBC Github repo. https://github.com/cosmos/ibc
13. Wenting Li, Sébastien Andreina, Jens-Matthias Bohli and Ghassan Karame. 2017. Securing Proof-of-Stake Blockchain Protocols. http://www.ghassankarame.com/CBT_Blockchain17.pdf
14. Miguel Castro and Barbara Liskov. 1999. Practical Byzantine Fault Tolerance. https://pmg.csail.mit.edu/papers/osdi99.pdf
15. Yu-Te Lin. 2017. Istanbul Byzantine Fault Tolerance #650. https://github.com/ethereum/EIPs/issues/650
16. Roberto Saltini and David Hyland-Wood. 2019. Correctness Analysis of Istanbul Byzantine Fault Tolerance. https://arxiv.org/pdf/1901.07160.pdf
17. Roberto Saltini and David Hyland-Wood. 2019. IBFT 2.0: A Safe and Live Variation of the IBFT Blockchain Consensus Protocol for Eventually Synchronous Networks. https://arxiv.org/pdf/1909.10194.pdf
18. Ethan Buchman, Jae Kwon and Zarko Milosevic. 2018. The latest gossip on BFT consensus. https://arxiv.org/pdf/1807.04938.pdf
19. Yackolley Amoussou-Guenou, Antonella del Pozzo, Maria Potop-Butucaru, Sara Tucci-Piergiovanni. 2019. Dissecting Tendermint. https://arxiv.org/pdf/1809.09858.pdf
20. Maofan Yin, Dahlia Malkhi, Michael K. Reiter, Guy Golan Gueta, Ittai Abraham. 2019. HotStuff: BFT Consensus in the Lens of Blockchain. https://arxiv.org/pdf/1803.05069.pdf
21. Philip Daian, Steven Goldfeder, Tyler Kell, Yunqi Li, Xueyuan Zhao, Iddo Bentov, Lorenz Breidenbach, Ari Juels. 2019. Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges. https://arxiv.org/pdf/1904.05234.pdf
22. Kaihua Qin, Liyi Zhou, Arthur Gervais. 2021. Quantifying Blockchain Extractable Value: How dark is the forest? https://arxiv.org/pdf/2101.05511.pdf
23. Vitalik Buterin. 2014. Proof of Stake: How I Learned to Love Weak Subjectivity. https://blog.ethereum.org/2014/11/25/proof-stake-learned-love-weak-subjectivity/
24. Sean Braithwaite, Ethan Buchman, Ismail Khoffi, Igor Konnov, Zarko Milosevic, Romain Ruetschi, Josef Widder. 2020. A Tendermint Light Client. https://arxiv.org/pdf/2010.07031.pdf