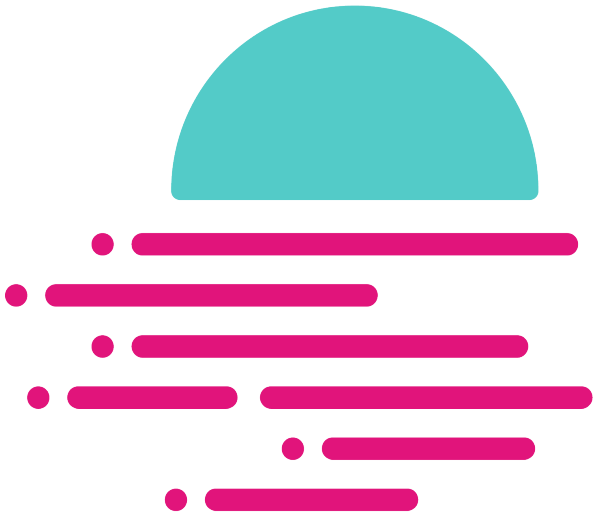
arrington CAPITAL

Moonbeam: EVM + XCM

A Meeting Ground For Multi-Chain Applications ("xApps")



June 8, 2022

Disclosure

Arrington Capital and/or its affiliates (collectively "Arrington Capital") has a financial interest in the success of the Moonbeam and Polkadot ecosystem, including affiliated ecosystems, initiatives and projects including (but not limited to) Acala, Karura, Moonbeam, Moonwell and Subquery (collectively "Polkadot Ecosystem"). Arrington Capital currently owns DOT and GLMR tokens. However, as a best practice, Arrington Capital will not trade DOT or GLMR tokens three days prior to or three days after the publication of this research.

As of the publication date of this report, Arrington Capital, and others that contributed to this report, are supporters of the Polkadot and Moonbeam Ecosystems and stand to realize gains through various manners of participation. All content in this report represents the opinions of Arrington Capital. Arrington Capital has obtained all information herein from third-party sources they believe to be accurate and reliable, including the Polkadot and Moonbeam ecosystem teams. Third-party sources may not have been independently verified and accuracy or completeness cannot be guaranteed and not be relied upon as such. Information is presented "as is", without warranty of any kind – whether express or implied.

This document is for informational purposes only and is not intended as an official recommendation or confirmation of any transaction. The information contained herein does not take into account the particular investment objectives, regulatory status or financial circumstances of any specific person who may receive it. All market prices, data and other information are not warranted as to completeness or accuracy, are based upon selected public market data, and reflect prevailing conditions and Arrington Capital's views as of this date, all of which are accordingly subject to change without notice. Arrington Capital has no obligation to continue offering reports regarding the project. Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances.

Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. This report's estimated fundamental value only represents a best efforts estimate of the potential fundamental valuation of a specific token, and is not expressed as, or implied as, assessments of the quality of a token, a summary of past performance, or an actionable investment strategy for an investor.

This document does not in any way constitute an offer or solicitation of an offer to buy or sell any investment or token discussed herein.

The information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond Arrington Capital's control. Investors should conduct independent due diligence, with assistance from professional financial, legal and tax experts, on all tokens discussed in this document and develop a stand-alone judgment of the relevant markets prior to making any investment decision.

By accepting this information the recipient agrees and acknowledges that no duty is owed to the recipient by Arrington Capital. The recipient expressly waives any claims arising out of the delivery of the information or the recipients use thereof or reliance thereon.

Executive Summary

Moonbeam is a Polkadot Parachain which combines the functionality of the EVM with Polkadot's multi-chain infrastructure. We believe it could evolve into the central hub for Polkadot assets and become a conduit to EVM-based projects.

Ethereum's scalability challenges have fuelled the rise of new blockchains which try to cater to different use cases. There is no general purpose blockchain that can meet the unique demands of all applications. This lies at the heart of Polkadot's approach: infrastructure to deploy application-specific blockchains, moving beyond homogenous and generalized computing.

Despite Ethereum congestion, the EVM dominates developer and user mindshare. EVM chains from Ethereum to alternative EVM-based L1s have captured the lion's share of blockchain activity across most sectors.

As an EVM-based Parachain, Moonbeam inherits both the rich infrastructure forged through years of EVM-based products and the multi-chain architecture that is uniquely enabled by Polkadot's XCM framework. It could thus become a prime destination for natively multi-chain applications. We believe that Moonbeam is positioned for a new generation of "xApps", applications which deploy across blockchains from day one.

This report attempts to unpack the technical foundations of Moonbeam and how it fits into the Polkadot ecosystem and the broader XCM framework. The first section focuses on Polkadot's multi-chain design and the rise of the EVM. The second section explores the consensus technology and token economics of Moonbeam and the unique use cases unlocked by XCM. In the third and final section, we briefly describe some of the major protocols building on Moonbeam.

Contents

1 Moonbeam: Polkadot Hub And EVM Conduit

1.1 The Multi-Chain Thesis

We previously published a report on Polkadot titled The League of Parachains. The report analogized Parachains to nation states mediated by the Relay Chain. The Relay Chain brings together a network of heterogeneous blockchains which represent unique use cases, cultures and monetary policies.

This is a natural representation of a multi-chain world. Polkadot applies this philosophy as a network of networks. Parachains are completely customizable, each dictating their own destiny – whether that is their technical architecture or consensus. On Ethereum, developers customize applications at the smart contract level. On Parachains, developers can tailor core blockchain logic for specific applications. Use cases vary widely, ranging from DeFi logic with native front-running resistance to gaming applications that allow users to pay blockchain fees using in-game currencies.

1.2 EVM Dominance

No other L1 comes close to Ethereum's success. Ethereum captures 65% of DeFi TVL[1] and likely more than 90% of NFT value. Ethereum has orders of magnitude more developers than any other chain[2].

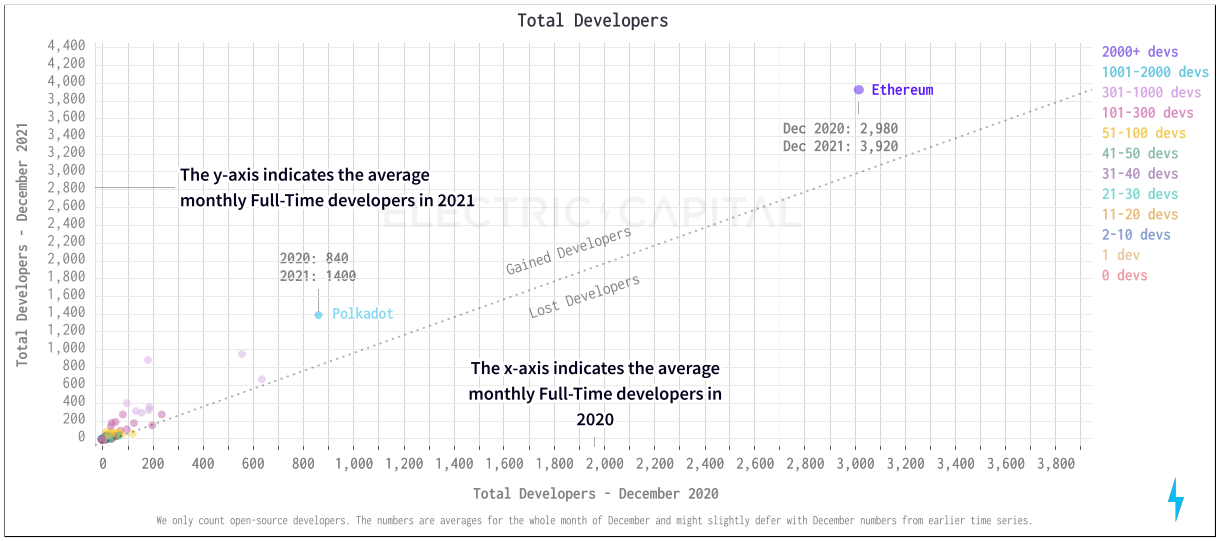


Figure 1: Total developer count in the Ethereum and Polkadot ecosystems in 2020 and 2021[3].

Ethereum can be described as a victim of its own success. The computational flexibility of the EVM comes at the cost of storing the state. The scaling problem is thus inherent to the base chain. As computational demand and gas fees climb, transactions below a certain value become entirely uneconomic – pricing out most users.

EVM chains (e.g. Polygon, Avalanche, etc.) are de facto extensions of Ethereum's EVM. Despite other implementations of state machines on blockchains, EVM chains have also captured the majority of the

[1] URL: https://defillama.com/.

[2] URL: https://github.com/electric-capital/developer-reports/blob/master/dev_report_2021_updated_012622.pdf.

[3] URL: https://github.com/electric-capital/developer-reports/blob/master/dev_report_2021_updated_012622.pdf.

alternative L1 market. More than 93% of DeFi TVL is associated with EVM-compatible L1 ecosystems[4]. These chains take advantage of the flexibility and infrastructure of the EVM without the constraints of the Ethereum network – without pricing out most ordinary users.

1.3 Polkadot's EVM Portal: Moonbeam

Much like Avalanche's C-Chain, Moonbeam has the potential to bootstrap the Polkadot ecosystem and become a central hub for developers. As the portal for EVM-based assets, Moonbeam could house most of Polkadot's initial DeFi and NFT activity. DeFi protocols like Uniswap, Curve and Sushi have already deployed instances on Moonbeam. New teams have been able to quickly iterate on mature and audited code; like Solarbase, an iteration of Uniswap. Once these assets and applications are inside of Polkadot, they inherit Polkadot's infrastructure and the XCM framework.

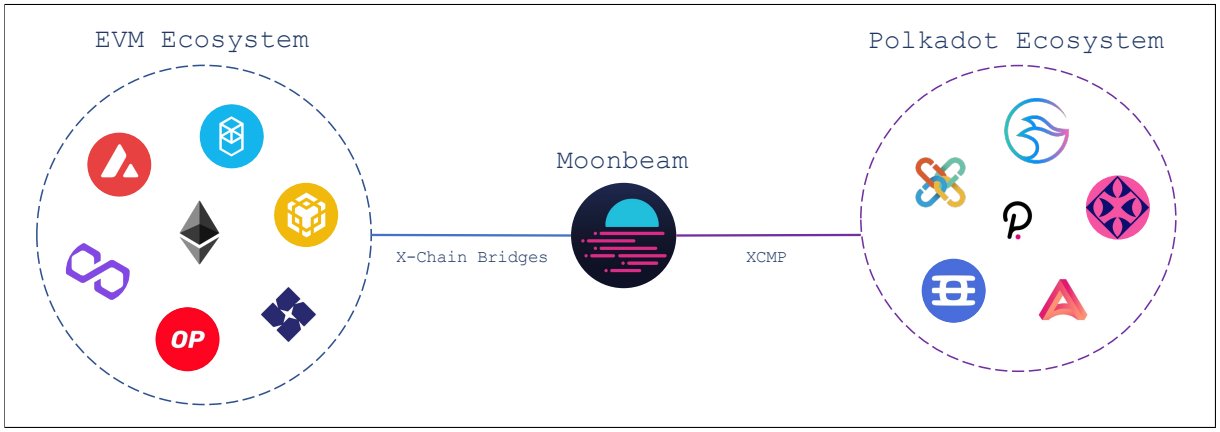


Figure 2: Moonbeam merges the Polkadot ecosystem of Parachains with the existing EVM ecosystem of blockchains.

[4].

2 Moonbeam Technology: EVM Plus XCM

In this section, we will attempt to describe the XCM framework and how Moonbeam could help unlock some of its unique capabilities. Before we do this, we briefly describe Moonbeam's technology stack.

Currently, Moonbeam has the following configuration[5]:

- It runs as a parachain connected to the Polkadot Relay Chain
- It has an active set of 64 collators
- It has infrastructure providers that provide API endpoints to connect to the network.

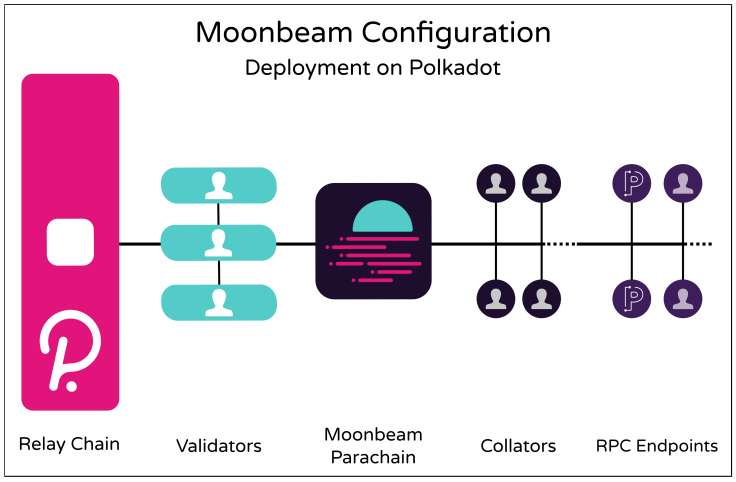


Figure 3: Moonbeam configuration on Polkadot.

Table 1: Important Moonbeam network variables and configurations.

Variable	Value
Minimum gas price	100 Gwei*
Target block time	12 seconds (expected to be 6 seconds)
Block gas limit	15M (expected to increase by at least 4×)
Transaction gas limit	12.995M (expected to increase by at least 4×)

2.1 Consensus And Token Economics

The Moonbeam network is a fully decentralized Delegated Proof of Stake (dPoS) network. Users can delegate collator candidates to produce blocks and earn rewards, relying on a customized consensus framework known as Nimbus.

GLMR is the governance token for the network, used for staking and securing the blockchain[6]. Additional uses for GLMR token include:

- Supporting the gas metering of smart contract execution

[5] URL: https://docs.moonbeam.network/learn/platform/networks/moonbeam/.
[6] URL: https://moonbeam.network/tokens/.

Table 2: Important Moonbeam staking parameters.

Variable	Value
Minimum delegation stake	50 GLMR
Maximum delegators per candidates	300
Maximum delegations per account	100
Round	1,800 blocks (6 hours)
Bond duration	Delegation takes effect in the next round (funds are withdrawn immediately)
Unbond duration	28 rounds (168 hours)

- Incentivizing collators and powering the mechanics around the creation of a decentralized node infrastructure for the platform
- Facilitating on-chain governance mechanism including proposing referenda, electing council members and voting
- Paying for transaction fees on the network.

Moonbeam targets a 5% annual inflation rate. Inflation is necessary to resource its security budget, fund ongoing Parachain slots and incentivize collators to produce blocks.

Of the 5% inflation:

- 1.0% incentivizes collators block production
- 1.5% reserved for the Parachain bond
- 2.5% allocated to staking rewards and the collator selection process.

Roughly 80% of transaction fees on the Moonbeam network are burned. The remaining 20% of transaction fees are sent to an on-chain treasury allocated via on-chain governance, used in future grants and initiatives to further network adoption.

2.2 Moonbeam's Development Stack

Substrate is the Polkadot blockchain SDK used to create and deploy Parachains. It provides a rich set of tools for creating specialized blockchains.

Several excerpts from Moonbeam documentation provide a detailed description of Moonbeam's development stack[7]:

> *Moonbeam leverages multiple existing Substrate frame pallets to provide key blockchain services and functionality, including core blockchain data structures, peer-to-peer networking, consensus mechanisms, accounts, assets, and balances. Custom pallets and logic in the runtime implement Moonbeam-specific behavior and functionality, such as cross-chain token integration. For leveraged pallets, Moonbeam will strive to stay as close as possible to the upstream Substrate codebase and incorporate Substrate bug fixes, enhancements, and new features on an ongoing basis.*

[7] URL: https://docs.moonbeam.network/learn/platform/technology/#substrate-framework.

Smart contracts on Moonbeam can be implemented using Solidity, Vyper, and any other language which can compile smart contracts to EVM-compatible bytecode. Moonbean aims to provide a low-friction and secure environment for the development, testing, and execution of smart contracts that is compatible with the existing Ethereum developer toolchain.

The execution behavior and semantics of Moonbeam-based smart contracts will strive to be as close to Ethereum Layer 1 as possible. Moonbeam is a single shard, so cross-contract calls have the same synchronous execution semantics as on Ethereum Layer 1.

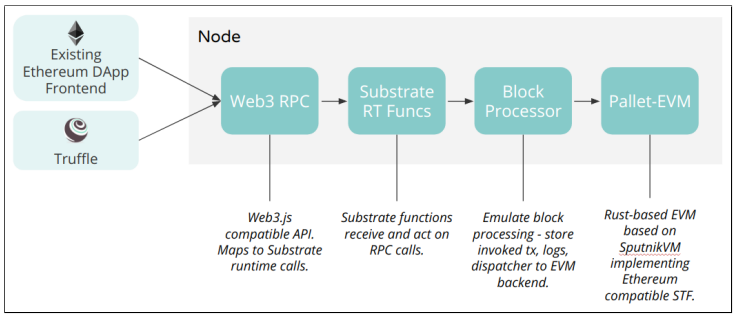


Figure 4: Moonbeam's EVM implementation.

A high-level interaction flow is shown above. A Web3 RPC call from a DApp or existing Ethereum developer tool, such as Truffle, is received by a Moonbeam node. The node will have both Web3 RPCs and Substrate RPCs available, which means that you can use Ethereum or Substrate tools when interacting with a Moonbeam node. These RPC calls are handled by associated Substrate runtime functions. The Substrate runtime checks signatures and handles any extrinsics. Smart contract calls are ultimately passed to the EVM to execute the state transitions.

Since the Moonbeam EVM is based on the Substrate Pallet-EVM, the platform has a full Rust-based EVM implementation.

2.3 Cross-Consensus Messaging

One of the main reasons why we are excited about Moonbeam's positioning in the multi-chain landscape relates to Polkadot's Cross-Consensus Messaging format. XCM and the Cross-Chain Message Passing Protocol (XCMP) are the foundation of Polkadot's multi-chain functionality[8].

XCM is classified as a "cross-consensus" messaging format rather than a messaging protocol. It cannot be used to "send" messages but rather expresses what should be done by the sender and receiver.

2.3.1 XCMP

There are three distinct systems for communicating XCM messages between its constituent chains:

1. UMP (Upwards Message Passing) – this allows Parachains to send messages to the Relay Chain
2. DMP (Downwards Message Passing) – this allows the Relay Chain to pass messages down to one of the Parachains

[8] URL: https://medium.com/polkadot-network/xcm-the-cross-consensus-message-format-3b77b1373392.

3. XCMP – this allows Parachains to send messages to other Parachains.

XCM helps express the meaning of the messages over each of these channels. It is a language for communicating information between unique consensus systems, enabling messaging between chains.

We believe that a general messaging format is inherently superior to a native message and transaction format:

1. Lack of compatibility between chains – Each unique destination would require a distinct messaging format and even a single destination may alter its native transaction / messaging format over time while smart contracts may get upgrades and blockchains introduce new features
2. Common use-cases do not easily fit into a single transaction – Unique methods may be required to withdraw funds, exchange them and then deposit the proceeds into a single transaction
3. Some operations such as payment of fees do not easily fit into a model which assumes fee-payment has already been negotiated like smart contract messages – Transaction envelopes provide some system of payment for processing.

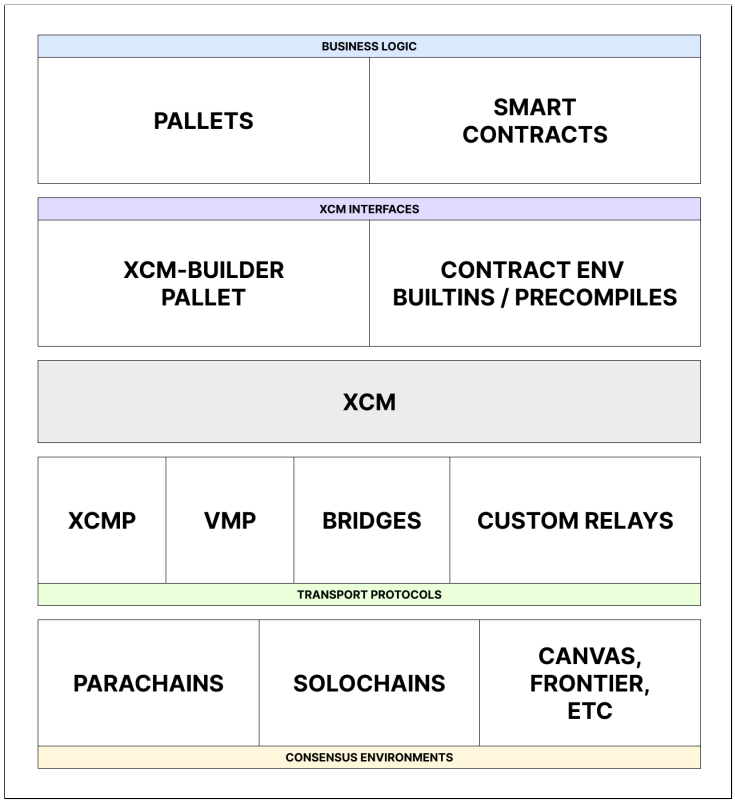


Figure 5: Polkadot's communication protocol stack.

2.3.2 XCMP Use-Cases

It is hard to predict exactly what types of use cases will emerge out of the XCMP framework. Some are easy to conceptualize, but it could still take several years before the composability benefits of generalized messaging are fully understood.

Below we describe some use cases which are relatively straightforward. One important caveat: there is a

chance that the "killer xApps" which take advantage of each of these features could only become possible once each of these use cases have had time to mature individually.

2.3.2.1 Token Transfer

Token transfers between chains are traditionally executed through exogenous bridges. These bridges come with various consensus mechanisms and security tradeoffs. Moving a token across two consensus systems traditionally required the token to be either locked in a smart contract or burned on one chain, with a corresponding token minted on the other chain. This allows for fungibility across multiple consensus systems but comes with a certain degree of vulnerability.

This mechanism is natively supported by XCMP, known as *teleporting* in XCM parlance.

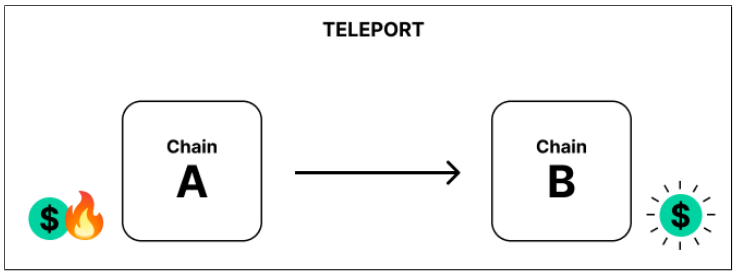


Figure 6: "Teleport" cross-chain transaction type.

Through XCMP, token transfers can become more complex without necessarily taking on additional security assumptions. One such example is the existence of "Statemint chains" – in this instance, a native hub for the DOT token. This could be useful when two chains that don't trust each other want to nominate a third chain and use its native assets as reserves. This means the derivative form of an asset is always fully backed, eliminating the "de-pegging" of the wrapped or synthetic assets.

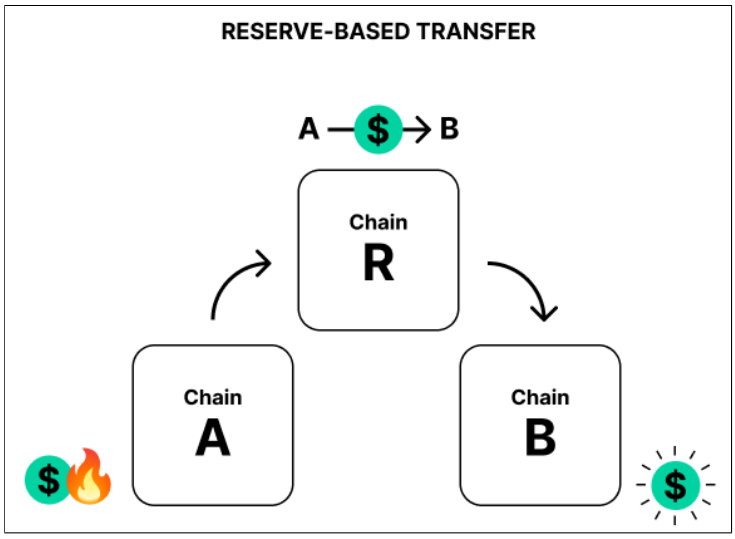


Figure 7: "Reserve-based" cross-chain transaction type.

For example, several Parachains want to send DOT between each other. They have a local form of DOT fully backed by DOT controlled by the Parachain on the Statemint chain. When the local form of DOT

is sent between chains, the "real" DOT is moving between Parachain accounts on Statemint – all in the background and oblivious to the user. This mechanism eliminates reliance on exogenous "layer zero" bridges and federated sidechains.

2.3.2.2 Remote Access

Another use case is the control of an account / address from a remote chain. A local chain can have an address on the remote chain. The remote address could be used for receiving funds or transferring funds into accounts on the remote chain. This means a single contract could manage addresses on multiple chains. This again eliminates the need for "wrapped" or "pegged" synthetic assets.

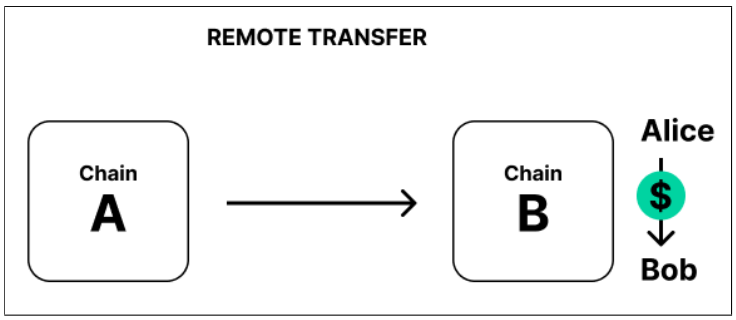


Figure 8: "Remote" cross-chain transaction type.

2.3.2.3 Cross-Chain Contract Calls

The cross-chain and remote contract calling features of XCMP are an order of magnitude improvement in user experience. In a traditional cross-chain bridge, a user would need to interact with a contract on the local chain and transfer an asset to the remote chain using a bridge. They would then interface on the remote chain and complete the remaining product flow. Users ultimately interact with multiple interfaces, wallets, fees and transactions.

With multi-chain contracts, a user can complete the entire flow within a streamlined experience. They don't have to leave the initial interface while XCMP passes all instructions and executes transactions across chains.

Cross-chain DeFi protocols could more efficiently and securely manage:

- Global liquidity aggregated on a single reserve chain – For example, all of aUSD's liquidity exists on the Acala Parachain. *Anybody could swap aUSD on the Moonbeam parachain even though no liquidity exists on that chain.* This means liquidity can be managed more efficiently, partially reducing liquidity fragmentation across chains
- Cross-chain prime brokerage – A single DeFi dApp could manage collateral across multiple chains and efficiently call liquidations. This becomes even more efficient if all the collateral existed on a minimum number of reserve chains
- Global DAO governance – Multi-chain DAOs could manage voting from a single chain akin to a system like Convex across dozens of blockchains.

This functionality could extend into NFT applications. In-game NFTs could have utility in a contract even if this contract lives on another chain. Again – users don't need to deal with the clunkiness of

moving assets across different blockchains with varied consensus protocols. A user could own an NFT in one game – on one chain – nonetheless giving it utility on another game and chain.

2.3.3 XC-20: Polkadot's ERC-20

The ERC-20 standard is the technical standard for all fungible tokens on EVM-compatible blockchains[9]. Moonbeam can interact with these assets as a fully functioning EVM chain. However, for ERC-20s to then interact with the rest of the Polkadot ecosystem, the Moonbeam team created a standard known as the XC-20[10].

The XC-20 standard creates compatibility between the EVM and the Substrate framework. XC-20s simplify the way Moonbeam brings together the ERC-20 standards and the Polkadot technology stack. Instead of token wrapping and bridging, Moonbeam uses the XC-20 standard to enable fully-functioned transfers and interoperability. Calling functions on XC-20 tokens invoke Substrate functionality, allowing EVM tools and smart contracts to interoperate with the Substrate layer.

[9] URL: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/.

[10] URL: https://moonbeam.network/blog/introducing-xc-20s-the-new-standard-for-cross-chain-tokens-on-dotsama/.

3 The Moonbeam Ecosystem

In the past, we have written about the Moonbeam team and their ability to attract blue chip deployments to a very new ecosystem. Major protocols like Uniswap, Curve and Sushi have committed to or deployed on Moonbeam.

In addition to these EVM deployments, we are encouraged to see a number of high-quality native teams building on Moonbeam. Below we describe some of the major projects in the ecosystem.

3.1 Moonwell: Moonbeam's First Major Step For DeFi

Moonwell is a new decentralized capital markets protocol, unlocking liquidity on the Moonbeam Parachain. It will allow users to collateralize their assets for borrow/lend activity. The protocol is already live on Moonriver – Moonbeam's canary network. It has the highest TVL in the ecosystem at over $100M. We are excited to see how robust capital markets on Moonbeam will unlock broader multi-chain activity in Polkadot.

Moonwell is headed by Luke Youngblood, who helped build Coinbase's staking infrastructure. We published a blogpost on the Moonwell project earlier this year.

3.2 Zircon: Optimized Liquidity

Zircon is a decentralized exchange with an integrated risk system where liquidity providers (LPs) can provide single-sided liquidity which reduces capital inefficiency. This is achieved by tranching the classic 50/50 Uniswap AMM pool into float and anchor components. The system tracks the assets to continuously rebalance the underlying pool according to primary criteria:

- Any excess anchor tokens (caused by float growth and subsequent impermanent loss) is claimed by float holders
- Any excess float tokens in the underlying pool (caused by float depreciation and impermanent loss) is claimed by anchor holders.

This design shifts the impermanent loss curve to the right, reducing it on the upside while increasing it on the downside. Zircon's approach offers unique and potentially more profitable opportunities for LPs whilst reducing fees for traders.

3.3 Prime Protocol: DeFi's Prime Broker

Prime brokers in traditional finance allow users to borrow against the value of all investments in their portfolio. Lenders can offer lower rates because the pool of collateral is diversified, reducing the risk of liquidation. This is because the variance of the entire portfolio is lower than the variance of individual positions. Large banks currently serve as prime brokers because of their access to capital at low cost.

Providing a single, multi-chain and cross-margined platform that bridges liquidity between blockchains helps to universalize crypto money markets. This is what Prime Protocol aims to become. Prime issues stablecoin loans backed by any kind of digital collateral, including but not limited to positions in yield farms, liquidity pools, staked tokens, and money market deposits. We wrote about our original investment into Prime Protocol earlier this year.

Prime is launching across several blockchains with Moonbeam as its "brain-chain". Users will be able to deposit collateral from any supported chain and credit this to one global margin account. Stablecoin loans will be made available on any chain regardless of collateral location. Moonbeam is a particularly attractive place to deploy a protocol like Prime. The "EVM + XCM" framework creates a multi-chain architecture that is particularly useful for DeFi protocols that need to globalize collateral across blockchains.

3.4 Firefly: Sophisticated Trading With Moonbeam

The Firefly protocol is a decentralized exchange for perpetual futures and options products. It aims to provide users with the experience of a centralized exchange within the wider Polkadot ecosystem. The protocol will utilize rollups for near-instant settlement of trades that enables instant balance updates, efficient liquidations, lower liquidation penalties and higher leverage.

Firefly supports various collateral assets including DOT staking derivatives which helps unlock liquidity from staked DOT. This opens opportunities for DOT stakers to hedge or speculate on assets while capturing the staking rewards on Polkadot or the crowd loan participation rewards.

4 Conclusion

While it is still early in both the life of the blockchain and the ecosystem, we are excited about Moonbeam as a dual bet on Polkadot's unique interoperability framework and the EVM. Moonbeam is primed for the next generation of dApps – what some teams have begun calling "xApps". These are applications positioning themselves as multi-chain deployments from day one.

Moonbeam is an exciting place for these deployments. Developers and users inherit the rich tapestry of the EVM while accessing the generalized cross-chain communication functionalities of XCM.

The success of Ethereum is one of the most remarkable feats in crypto. There is no L1 technology as widespread as the EVM. Yet at the same time, it is important to differentiate Ethereum the network – which cannot yet support all of this demand – and the EVM, arguably the most exported technology stack across all blockchains.

Moonbeam is an attempt to embrace the success of the EVM while also looking toward Polkadot's vision for application-specific blockchains. This is a path forward for both scalability and multi-chain functionality. We are excited to continue our longstanding support of the Moonbeam project and look forward to seeing what types of applications emerge in this "EVM + XCM" environment.

***Authors**: Sam Kim, Ninos Mansor, Ninor Mansor*