Kingswap Technical White Paper

Introduction

By allowing the trading of digital assets, Decentralized Exchanges (DEXes) have enabled the growth of Decentralized Finance (DeFi) and become a core part of the Ethereum ecosystem. DEXes are interoperable with other protocols, secure, and permissionless – for example, there are few barriers for listing new tokens. Lately, DEXes have experienced a surge of trading volume[iiiiii]. According to industry analysts at defipulse.com, at the time of writing there is over $11 billion of "total value locked" in liquidity pools. This growth reflects a demand for a mechanism to perform trustless, flexible, and decentralized exchange of Ethereum-based digital assets.

The traditional means of value exchange is based upon a system of using bid and ask orders to allow buyers and sellers to specify the prices they wish to trade at. This approach, however, does not work well for DeFi. It is of limited efficiency with illiquid markets, it is vulnerable to front-running issues, and transaction fees make it cost-prohibitive for permissionless on-chain markets[iv]. Instead, DEXes are facilitated by Automatic Market Makers (AMM). AMMs work by pooling liquidity together and quoting prices to the end-user based upon a predefined formula and according to a deterministic algorithm. Each AMM has its own advantages and disadvantages – there is no universal approach and potential uses are based upon the mathematical algorithm of trade execution. The AMM model offers liquidity providers additional incentives as it allows them to continually generate income from trades.

The state of AMM models

The study of the design, challenges, and constraints of the automation of market-making, design, and liquidity provision predates the advent of blockchains[vvi]. However, with the rise of Ethereum and other smart-contract platforms, this pursuit has taken on a greater level of importance. These issues have now become vital to the growth and trajectory of the entire ecosystem.

Basic AMM models

Bancor Network

The Bancor Network represents an innovative attempt at utilizing a simple AMM model for trade execution, based on the following equation[vii]:

$$Price = \frac{\text{Reserve Balance}}{\text{Smart Token Supply} \times \text{Reserve Ratio}}$$

In Bancor Network, trades between one type of cryptocurrency and another, known as Bancor Pools, consisted of two parts: a Bancor token (BNT) and another ERC20 token. Originally there was no incentive for liquidity providers, and this proved to be a limitation. During the 2018-

2019 time period, the overwhelming majority of overall DEX liquidity moved to a different protocol, Uniswap. This led to a re-design of the Bancor Network AMM model[viii].

Alan Lu from Genesis proposed the constant invariant model[ix], it was further highlighted by Ethereum co-founder Vitalik Buterin[xxi]. The method was similar to the one used by competitor Uniswap, which became the first AMM to use the constant invariant function when it launched in 2018[xii]. That function works as follows:

$$x \times y = const,$$
$$where\ x - balance\ of\ ETH, y - balance\ of\ ERC\ token$$

In this approach, the compound value of the trading pair pool (ETH + another pool) remains constant, while the point at the AMM curve moves during the particular trade. (Figure 1)

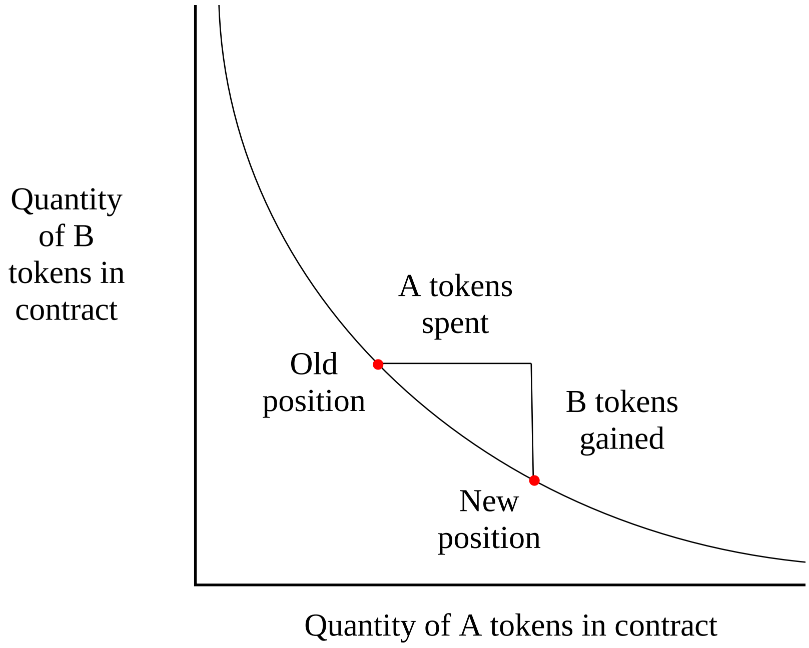
Quantity of B tokens in contract
A tokens spent
Old position
B tokens gained
New position
Quantity of A tokens in contract

Figure 1: The constant invariant AMM.
Source: Vitalik Buterin[xiii]

The constant invariant model showed to be gas efficient, simple to implement, and the resulting market feedback was positive.

Balancer

The generalized version of the constant invariant used by Balancer is as follow:

$$\prod_{i=1}^{n} R_i^{W_i} = const$$
$$where\ R_i : reserve\ of\ i - th\ asset, w_i : weight\ of\ i - th\ asset$$

This approach enables market-making two or more assets. In the condition that fees are zero, mean markets make it so that the weighted geometric mean of the reserves remains at a constant. The following is an example of an equal-weighted portfolio of three assets, calculated by the formula $(x \times y \times z)^{1/3} = const$:

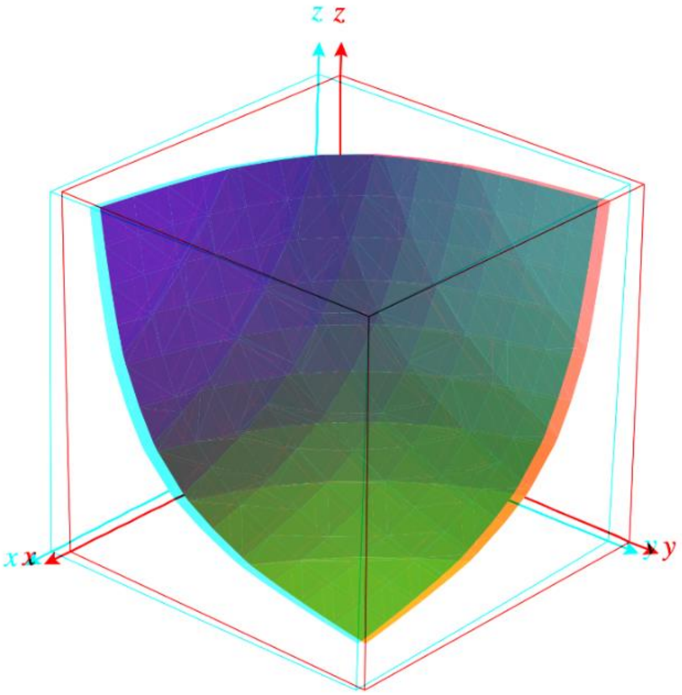

Figure 2: The constant invariant AMM.
Image Credit: Balancer Whitepaper[xiv]

Due to its simplicity, the potential to power low-liquidity markets, and a clear incentive structure that rewards liquidity providers, the constant invariant approach has so far emerged the winner of the competition between DEX approaches. In particular, Uniswap and Balancer have found success with the constant invariant model. This has allowed them to provide liquidity for the tokens that trade on them.

This approach does come with some major drawbacks though. For a trader, it is capital inefficient and can lead to outsized slippage costs. For liquidity providers, there is the financial risk of high volatility – profit can only be achieved within a certain price range, and money is lost when a large price movement occurs. This can be seen in the following chart:

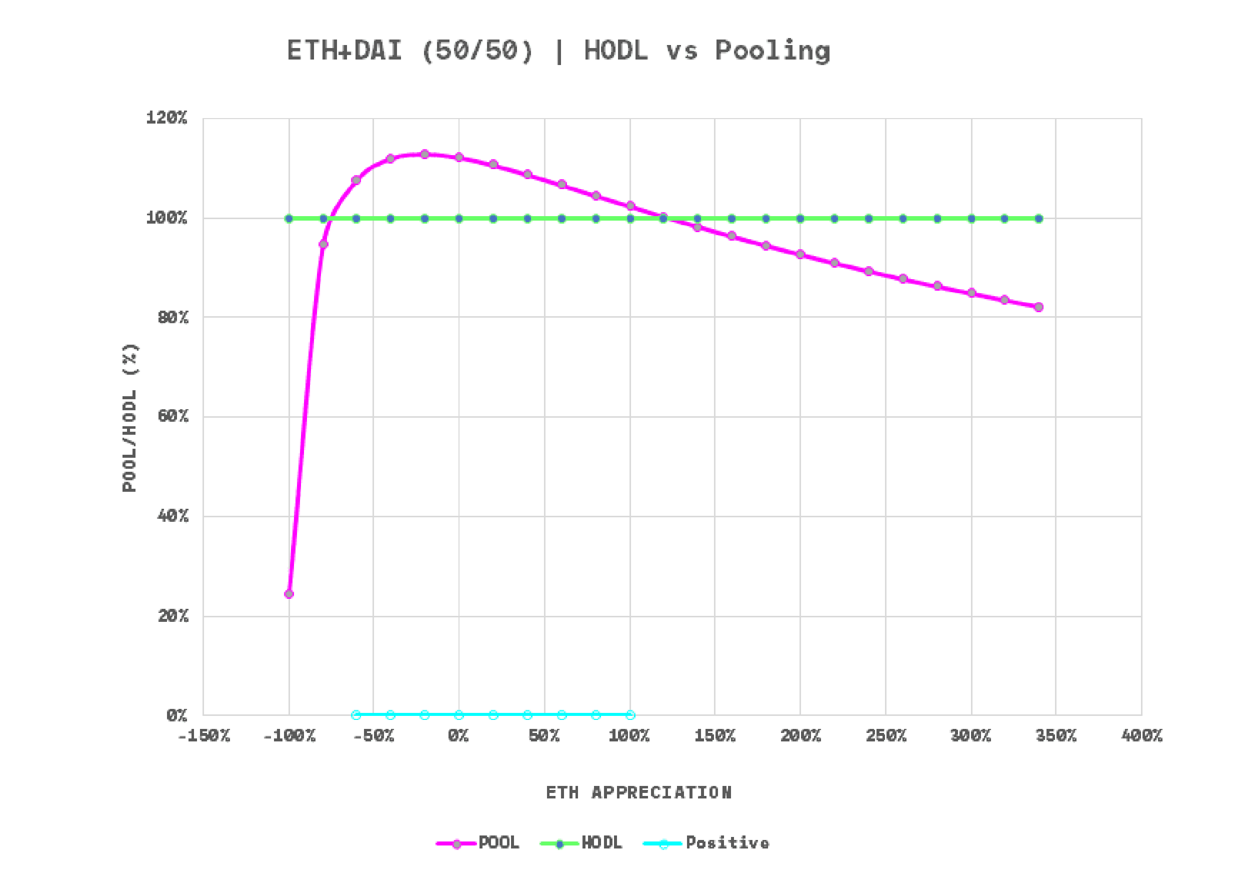

Figure 3: Uniswap ETH vs. DAI pool profit/loss curve. Image Credit: AlfaBlok[xv].

Curve

It should be noted that generalized constant invariant AMMs are not an ideal match for all classes of digital assets. In early 2020, Curve Protocol was launch, and it introduced another AMM, but this one developed specifically for low-volatility assets such as stable coins[xvi][xvii]. It combines a constant-sum invariant $x + y = const$ with a constant-product invariant $x \times y = const$:

$$x^{D^{n-1}} \sum x_i + \prod x_i = x^{D^n} + \left(\frac{D}{n}\right)^n$$

$$b_i - balance\ of\ i - th\ asset, d - sum\ of\ all\ balances\ of\ assets\ before\ swap,$$
$$x - imbalance\ coefficient$$

Curve Protocol's invariant AMM approach has shown to be quite a bit more capital efficient for trading stable coins, compared to the constant-product of Uniswap:

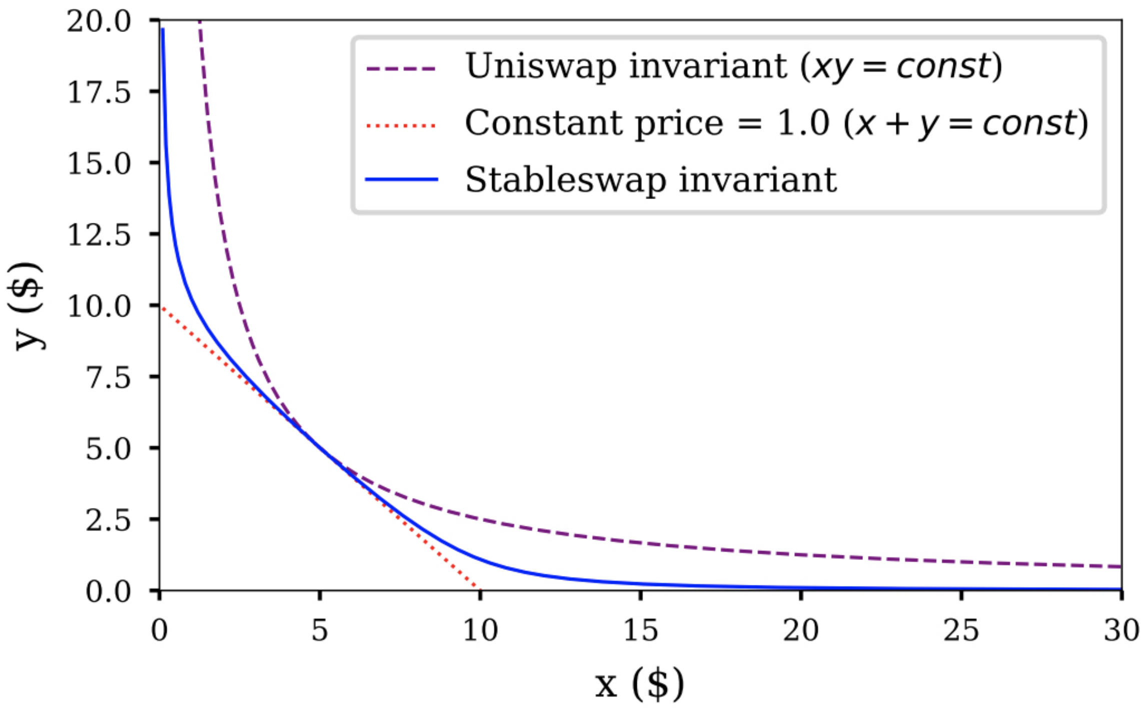

Figure 4: Comparison of Curve invariant with Uniswap (constant-product) and constant price invariants. The assets have an ideal price of 1.00. There is x = 5 and y = 5 coins initially. Image Credit: Dmitriy Berenzon[xviii].

Mooniswap

There are other proposals for alternate approaches towards improving AMM logic, pertaining to solving problems of slippages and impermanent losses of liquidity providers. Take Mooniswap for example[xix]; this protocol reduces arbitrage opportunities by introducing "virtual balances.[xx]" This is a concept where when a swap occurs, the pool does not immediately offer an arbitrage opportunity in the opposite direction. Rather, it slowly improves the price over a duration of time. It is significantly less risky and has greater upside for liquidity providers compared to Uniswap. The challenge of this approach is that of dependency on oracles. This moves the trust to a centralised entity, plus there is also the risk of front running, which has been noticed by certain protocols.

The challenges of impermanent loss still seems to be open one. Options available to reduce this would be explored by Kingswap in the roadmap. AMMs have proven so far, they are viable for pricing fungible tokens because it is possible to pool liquidity, but it is unclear yet how it might works with assets that are hard to price - like options or any time-based derivative. Kingswap intends to look at ways in which we could add more assets.

Layer 2 Optimizations

One of DeFi's key challenges is transaction cost, another is the time it takes for transactions to get committed. Kingswap team has been looking at various alternatives to provide improvement in both. Currently we have been looking at various layer two solutions namely state channels, side chains, plasma, optimistic rolls ups and Zero Knowledge based solutions.

Level	Function	Protocols
Network Management	Routing	Silent Whispers[xxi] SpeedyMurmur[xxii] Spider Routing[xxiii] Flare Routing[xxiv] Splitting Payments[xxv] Hoenisch and Weber Atomic Multi-Path[xxvi]
	Re-Balancing Channels	REVIVE[xxvii]
	Channel Stability	PISA[xxviii] Avarikioti et al.[xxix]
	Anonymity/Privacy	Fulgor & Rayo Tumblebit[xxx]
Network	Construction	HTLC Sprites[xxxi] State Assertion Virtual Channels Counterfactual[xxxii]
Off-chain Channels	State	Z-Channel Perun[xxxiii] NoCUST[xxxiv]
	Duplex Payment	Raiden[xxxv] Lightning[xxxvi] Decker et al. BOLT[xxxvii] Teechan[xxxviii] Burchert et al. TumbleBit[xxxix]
	Simplex Payment	Simplex Dimitrienko et al. Takahashi et al.
	Probabilistic Payment	Pass et al. Hu and Zhang

Figure 5: SoK: A Taxonomy for Layer-2 Scalability Related Protocols for Cryptocurrencies. Image Credit: Maxim Jourenko[xl].

State Channels

State Channels allow for two-way pathways to be opened up between a pair of users that want to transact with each other. It functions by having each participant in the channel sign transactions with private keys. This ensures that participants are in fact true and authorized. These channels are only known to participants – they are off-chain and private. That allows for anonymous and instant transactions within them. Channels also have a predetermined lifespan – either in terms of time or amount of transactions. Channels can be closed by participants if they provide the blockchain's last updated state of transaction. Upon a channel closing, its transaction history can be uploaded into the system in order for the outcome to be finalized.

Sidechains

A sidechain is a concept where a separate blockchain is attached to a parent blockchain using a two-way peg. That enables assets to be interchanged at a predetermined rate between the sidechain and the parent. The original blockchain is referred to as a "main chain" while all additional blockchains are referred to as "sidechains."

Plasma

Similar to state channels, Plasma shares the underlying goal of moving as many transactions off of the main chain as possible. These child chains can take on varying levels of complexity. They can have their own mechanisms of consensus, block sizes, or confirmation times. Design can be adjusted depending on application. In case there are disputes or the user wants to stop transacting on the child blockchain, it is possible to bring state updates to the main Ethereum network.

Zk Rollups

With Zk Rollups, an operator is required to generate a SNARK for every state transaction, which is then verified by the Rollup contract on the mainchain. This SNARK proves there is a series of transactions – and all are accurately signed by owners – which correctly updates account balances. This leads from the old Merkle root to the new one. There are several fundamental issues with Optimistic Rollup which ZK Rollups fix: eliminating a potentially major tail risk relating to funds being stolen and other attack vectors; reducing withdrawal time to a few minutes from 1-2 weeks; enables fast tx confirmations and exists in almost unlimited volumes; and introduces privacy by default. One of the first protocols to deploy Zk Rollups is Loopring (other protocols which use ZkSNARKs include zkSync[xli]). Loopring's approach is based upon using GPU-based proof generation and recursive SNARKs[xlii]. The key difference between the two has to do with the underlying mathematical proof systems. Loopring uses Groth16[xliii], which has an application-specific trusted setup, whereas zkSync uses PLONK[xliv], which uses a universal setup. One other consideration is that there is a choice between non-interactive zero knowledge proofs[xlv] that are being used in DEX's – SNARKs, STARKs[xlvi], and others, such as SNARGs[xlvii]. DeverseFi, for example, uses STARK[xlviii].

Optimistic Rollup

Optimistic Rollup is an approach that offers an alternative to the standard Zk Rollup by removing the need for Zero Knowledge Proofs altogether. Instead of checking and verifying each transaction, the network instead assumes that they are all correct. User-intervention only arises when someone reports an incorrect transaction. This is done through the submission of a fraud proof. The initial overhead for optimistic rollup may be lesser than Zk Rollups, but it requires users to publish the complete transaction input set every single time. Zk Rollups have a great deal more flexibility.

	State channels	**Sidechains[0]**	**Plasma**	**Optimistic rollups**	**zkRollup**
Security					
Liveness assumption (e.g. watch-towers)	Yes	Bonded	Yes	Bonded	No
The mass exit assumption	No	No	Yes	No	No
Quorum of validators can freeze funds	No	Yes	No	No	No
Quorum of validators can confiscate funds	No	Yes	No	No	No
Vulnerability to hot-wallet key exploits	High	High	Moderate	Moderate	Immune
Vulnerability to crypto-economic attacks	Moderate	High	Moderate	Moderate	Immune
Cryptographic primitives	Standard	Standard	Standard	Standard	New
Performance / economics					
Max throughput on ETH 1.0	1..∞ TPS [2]	10k+ TPS	1k..9k TPS [2]	2k TPS [3]	2k TPS
Max throughput on ETH 2.0	1..∞ TPS [2]	10k+ TPS	1k..9k TPS [2]	20k+ TPS	20k+ TPS
Capital-efficient	No	Yes	Yes	Yes	Yes
Separate onchain tx to open new account	Yes	No	No	No	No [5]
Cost of tx	Very low	Low	Very low	Low	Low
Usability					
Withdrawal time	1 confirm.	1 confirm.	1 week [4] ([7])	1 week [4] ([7])	1..10 min [7]

Time to subjective finality	Instant	N/A (trusted)	1 confirm.	1 confirm.	1..10 min
Client-side verification of subjective finality	Yes	N/A (trusted)	No	No	Yes
Instant tx confirmations	Full	Bonded	Bonded	Bonded	Bonded
Other aspects					
Smart contracts	Limited	Flexible	Limited	Flexible	Flexible
EVM-bytecode portable	No	Yes	No	Yes	No
Native privacy options	Limited	No	No	No	Full

[0] Some researchers do not consider them to be part of L2 space at all, see https://twitter.com/gakonst/status/1146793685545304064

[1] Depends on the implementation of the upgrade mechanism, but usually applies.

[2] Complex limitations apply.

[3] To keep compatibility with EVM throughput must be capped at 300 TPS

[4] This parameter is configurable, but most researchers consider 1 or 2 weeks to be secure.

[5] Depends on the implementation. Not needed in zkSync but required in Loopring.

[7] Can theoretically be accelerated with liquidity providers but will make the solution capital-inefficient.

Figure 6: Evaluating Ethereum L2 Scaling Solutions: A Comparison Framework. Image Credit: Alex Gluchowski[xlix].

Layer 3 Bridges

Another of the challenges DEX's face is the size of the liquidity pool. In general, having just one blockchain and liquidity pool could increase the risk of the protocol to Layer 1 failures of various kinds. To reduce this risk, we have been exploring the possibility of various layer 3 bridges including Cosmos, Polkadot and Algorand.

	Protocol	Trust Model at each CCC Protocol Phase							
		Commit on chain X				Verify & Commit on chain Y		Abort on chain X (optimal)	
		TTP	Dynamic?	Collateral?	Type	TTP	Type	TTP	Type
Exchange Protocols (Atomic Swaps)	Traditional Custodial Exchanges	●	✗	✗	EC (single, restricted)	●	EV	●	EC (single, restricted)
	A2L	◑	✗	✓	EE (multisig +	○	DO	◑	EE + Timelock

						signature Lock)				
		Arwen	◑	✗	✗	EE (multisig + Hash Lock)	○	DO	◑	EE + Timelock
		Notarized HTLC Atomic Swaps	○	-	-	Hash Lock	●	EV	◑	EE + Timelock
		HTLC Atomic Swaps	○	-	-	Hash Lock	○	DO	○	Timelock
		ECDSA/DLSAG Atmoic Swaps	○	-	-	Signature Lock	○	DO	○	Timelock
		SPV Atomic Swaps	○	-	-	Standard payment	○	SC (chain relay)	-	-
Asset Migration Protocols	(Cryptocurrency-backed Assets)	Bidirectional Chain Relays	○	-	-	SC (chain relay)	○	SC (chain relay)	-	-
		XCLAIM, Dogethereum	●	✓	✓	EC (single, unrestricted)	○	SC (chain relay)	-	-
		tBTC	●	✗	✓	EC (committee, restricted)	○	SC (chain relay)	-	-
		RenVM	●	✗	✓	EC (committee, restricted)	●	CM	-	-
		Custodial Wrapped Assets	●	✗	✗	EC (single, restricted)	●	EV	-	-
	Sharding	ATOMIX	●	✗	✗	CC (shard X)	●	CM	●	CC (shard X)
		SBAC	●	✗	✗	CC (shard X)	●	CM	●	CC (shard X)
		Rapidchain	●	✗	✗	CC (shard X)	●	CM	-	-
		Fabric Channels	●	✗	✗	CC (shard X)	●	CM	●	CC (shard X)
	Side-chains	Federated Sidechains/Pegs	●	✗	✗	EC (consensus of Y)	●	CM	-	-
		RSK	●	✗	✗	CC (consensus of X)	●	CM	-	-
	Boot-strapping	Proof-of-Burn (Federated)	○	-	-	SC / Burn address	●	CM	-	-
		Proof-of-Burn (SPV)	○	-	-	SC / Burn address	○	SC (chain relay)	-	-
		Merged Mining/Staking	●	✗	✗	CC (consensus of X)	●	CM	-	-

Figure 7: Classification of existing Cross-Chain Communication protocols, in consideration of the selected TPP model at each protocol step. ○ – uses a TTP, ◑ - fully relies on synchrony and availability of participants, ◑ - hybrid. EC – External Custodian, CC –

Consensus Custodian, EE – External Escrow, SC – Smart Contract, EV – External Validator, CM – Consensus Committee, and DO – Direct Observation. (Source: Zamyatin, Al-Bassam, Zindros, Kokoris-Kogias, Moreno-Sanchez, Kiayias, Knottenbelt[l]).

Cosmos

Tendermint is a BFT (Byzantine Fault Tolerant) consensus layer, which was detailed in the Tendermint paper, as the Tendermint Core blockchain consensus engine. Cosmos is therefore an application layer built on top of the Tendermint protocol. This provides a framework for creating Cosmos zones in the Cosmos network. All zones use the same Tendermint Core blockchain consensus engine. Additionally, the original Tendermint whitepaper details Bitshares and the security of Delegated Proof of Stake – DpoS – as "dependent on the extrinsic ability of shareholders to accurately predict the future performance of delegates." The whitepaper goes on to describe an intrinsic scheme whereby bonded validators go on to become network operators.

The Stargate upgrade to Cosmos is worth noting as well. The Cosmos ecosystem will look to Cosmos Hub governance to vote on features which will comprise one of the largest updates to the protocol to date. Its primary features include:

1) Inter-Blockchain Communication (IBC) – the ability to exchange transactions of data and value across chains which are compatible.
2) Protobuf Migration – this accelerates front-development and increases by a magnitude of 10x to 100x the performance of blockchain; a new node can synchronize 200x faster, participating in consensus in minutes rather than days.
3) Chain Upgrade Module – enables validators to upgrade the chain software asynchronously in minutes rather than an hour or more.

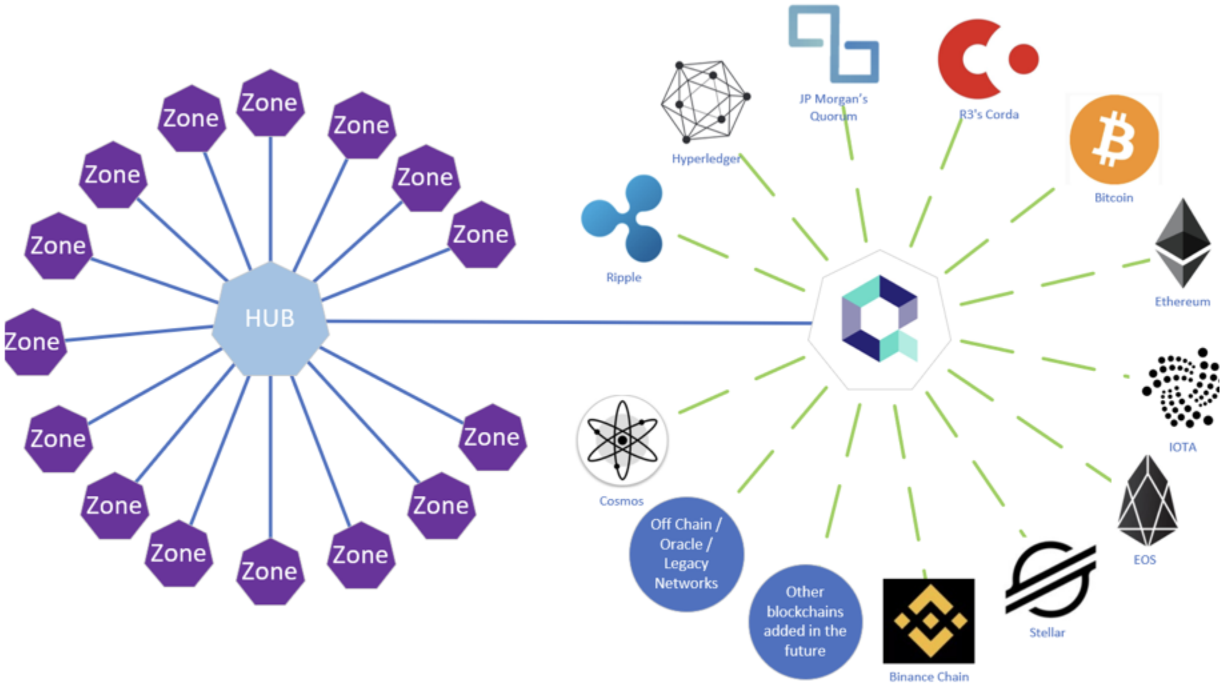

Figure 8: Hub in the Cosmos Ecosystem and connections via Cosmos IBC Protocol. Image Credit: Seq[li].

Polkadot

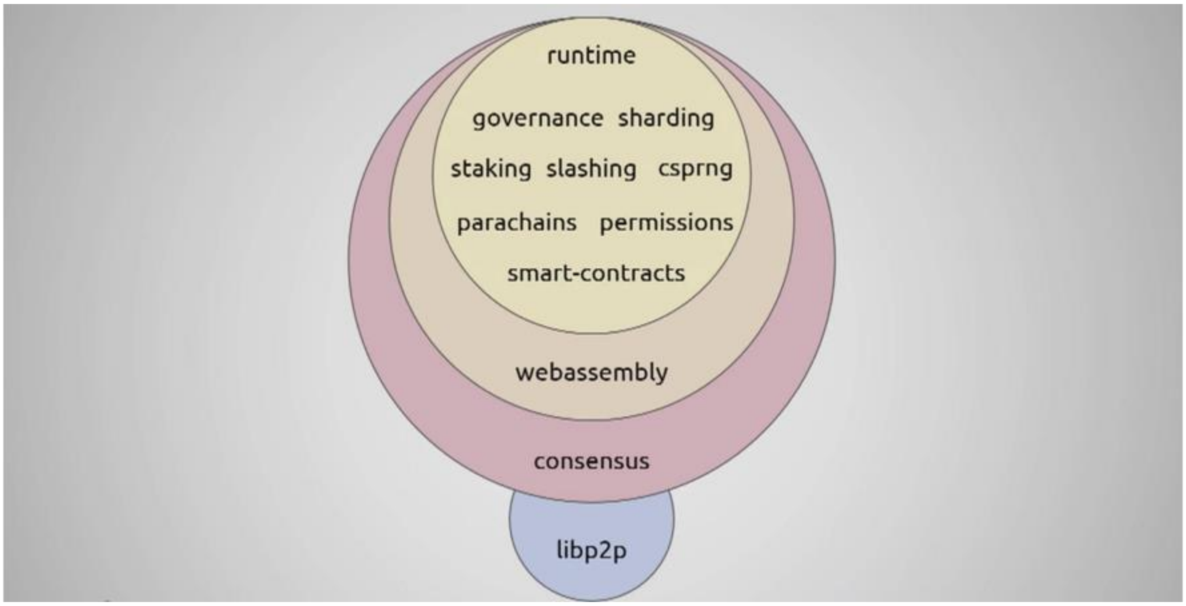

Figure 9: Parity Substrate Overview. Image Credit: Gavin Wood[lii].

Like Tendermint, the consensus mechanism of Polkadot also uses a Byzantine Fault Tolerant algorithm called HoneyBadger BFT. In the Polkadot whitepaper there is a mention of HoneyBadger BFT as an efficient fault-tolerant consensus that uses a scheme known as Nominated Proof-of-Stake (NPoS). In this approach, "parachains" have elected and bonded stake validators as network operators. The whitepaper further describes how parachain validators synchronize block data with other parachains. Polkadot, like Cosmos, has a homogenous IBC design, although it is more intertwined with overall methods of heterogenous IBC. In other words, blocks can be synchronized with a relay chain – possible Ethereum – and external block data is collate for inclusion by collators.

Algorand

The Algorand hybrid blockchain ecosystems allow participants to build and design their idealistic ledger to be integrated. This is done by allowing entities to define the attributes of the blockchain they prefer. Algorand's founder, Silvio Micali, these public and private ecosystems known as "Co-Chains" could offer a commercially viable method for enterprises and corporations to embrace distributed ledgers. With a Co-Chain such as Algorand, developers can build ecosystems that are completely independent of the public chain; there even may be the ability for Co-Chains deployed within this network to run on their own independent Algorand consensus mechanism and set of validators. These Co-Chains can also interact within the Algorand network based on their interoperability with the main chain. Finally, Co-Chains can acquire the underlying tools and features, as we see in the case of Algorand's permissionless layer. This allows Co-Chains to leverage existing resources such as smart contracts and Atomic transfers embedded in Algorand's Layer-1.

Conclusion

The key driver for technical choices are to increase efficiency (decrease gas costs), increase throughput, potentially reduce impermanent loss, and increase the size of the liquidity pool by building bridges to other blockchains. The choice of optimistic rollups as immediate solution for L2 and looking at SNARK based Zero Knowledge rollups, as the optimization race is ongoing, Kingswap would decide based on the best possible choice in terms of speed, gas cost and size of proofs for the long term. As for layer three bridges, Kingswap would be building bridges first with Polkadot , then with Cosmos and finally with Algorand.

We believe Kingswap would give the users the optimal yield, while reducing the risks and increasing the size of pools within the limits of technological trade-offs.

[i] https://www.coindesk.com/august-uniswap-trading-record-volume-two-weeks-billion
[ii] https://www.trustnodes.com/2020/08/12/ethereum-defi-dexes-near-half-a-billion-in-daily-trading-volumes
[iii] https://www.theblockcrypto.com/linked/73675/dex-july-monthly-volume
[iv] https://thecontrol.co/a-comparison-of-decentralized-exchange-designs-1deef249f56a
[v] J. Abernethy, Y. Chen, and J. W. Vaughan. An optimization-based framework for automated market-making. In ACM Conference on Electronic Commerce (EC), 2011.
[vi] http://reports-archive.adm.cs.cmu.edu/anon/2012/CMU-CS-12-123.pdf
[vii] https://cryptorating.eu/whitepapers/Bancor/bancor_protocol_whitepaper_en.pdf
[viii] https://blog.bancor.network/announcing-bancor-v2-2f56b515e9d8
[ix] https://blog.gnosis.pm/building-a-decentralized-exchange-in-ethereum-eea4e7452d6e
[x] https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way/
[xi] https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281
[xii] https://hackmd.io/@HaydenAdams/HJ9jLsfTz?type=view
[xiii] https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281
[xiv] https://balancer.finance/whitepaper/
[xv] https://alfablok.substack.com/p/coming-soon
[xvi] https://www.curve.fi/stableswap-paper.pdf

[xviii] https://medium.com/bollinger-investment-group/constant-function-market-makers-defis-zero-to-one-innovation-968f77022159
[xix] https://mooniswap.exchange/docs/MooniswapWhitePaper-v1.0.pdf
[xx] https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281
[xxi] https://eprint.iacr.org/2016/1054.pdf
[xxii] https://arxiv.org/pdf/1709.05748.pdf
[xxiii] http://web.mit.edu/6.829/www/currentsemester/papers/spider.pdf
[xxiv] https://bitfury.com/content/downloads/whitepaper_flare_an_approach_to_routing_in_lightning_network_7_7_2016.pdf
[xxv] https://www.researchgate.net/publication/327470777_Split_Payments_in_Payment_Networks_ESORICS_2018_International_Workshops_DPM_2018_and_CBT_2018_Barcelona_Spain_September_6-7_2018_Proceedings
[xxvi] https://lists.linuxfoundation.org/pipermail/lightning-dev/2018-February/000993.html
[xxvii] https://eprint.iacr.org/2017/823.pdf
[xxviii] https://www.cs.cornell.edu/~iddo/pisa.pdf
[xxix] https://arxiv.org/pdf/1905.11360.pdf
[xxx] https://eprint.iacr.org/2016/575.pdf
[xxxi] https://arxiv.org/pdf/1702.05812.pdf

[xxxii] https://l4.ventures/papers/statechannels.pdf
[xxxiii] https://perun.network/pdf/Perun2.0.pdf
[xxxiv] https://eprint.iacr.org/2018/642.pdf
[xxxv] https://raiden.network/101.html
[xxxvi] https://lightning.network/lightning-network-paper.pdf
[xxxvii] https://medium.com/bolt-global/bolts-whitepaper-updated-2ad5bd8f0285
[xxxviii] https://www.cs.cornell.edu/people/egs/papers/teechan.pdf
[xxxix] https://eprint.iacr.org/2016/575.pdf
[xl] https://eprint.iacr.org/2019/352.pdf
[xli] https://zksync.io
[xlii] https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell/
[xliii] https://eprint.iacr.org/2016/260.pdf
[xliv] https://eprint.iacr.org/2019/953
[xlv] http://pages.cs.wisc.edu/~mkowalcz/628.pdf
[xlvi] https://eprint.iacr.org/2018/046.pdf
[xlvii] https://youtu.be/-EkUn4iD8Z8
[xlviii] https://www.deversifi.com/
[xlix] https://medium.com/matter-labs/evaluating-ethereum-l2-scaling-solutions-a-comparison-framework-b6b2f410f955
[l] https://eprint.iacr.org/2019/1128.pdf
[li] https://medium.com/@CryptoSeq/cosmos-an-early-in-depth-analysis-at-the-ecosystem-of-connected-blockchains-part-two-2d5a9886166
[lii] https://www.youtube.com/watch?v=iUMZyL5kTwc