October 2020

Decentral Park Capital

Layer 2 Networks

An exploration of the scaling solutions for Ethereum

L2 Research

Table of Contents

Executive Summary 3

Introduction 4

Part 1: Types of Layer 2 Solutions **6**
1.1. Payment & State Channels 6
1.2. Custodial Sidechain 6
1.3. Non-Custodial Sidechain 6
1.3.1. Plasma Sidechains 7
1.3.2. Rollups 7
1.3.2.1 Zk-Rollups 7
1.3.2.2 Optimistic Rollups 8
1.4. Table of tradeoffs 9
1.5. The current L2 landscape 10

Part 2: Payment & State Channels Projects **10**
2.1. Raiden Network 11
2.1.1. Value Accrual 11
2.1.2. Strengths 11
2.1.3. Weaknesses 11
2.2. Connext 12
2.3. Celer Network 12
2.3.1. Value Accrual 13
2.3.2. Constraints of the system 13
2.3.3. Strengths 13
2.3.4. Weaknesses 14

Part 3: Custodial Sidechain Projects **14**
3.1. SKALE 15
3.1.1. Approaching scalability with customizability 15
3.1.2. Close ties with Ethereum 15
3.1.3. Value Accrual 16
3.1.4. Dynamic economics 16
3.1.5. A locked up investor base 17
3.1.6. Strengths 18
3.1.7. Weaknesses 19
3.2. xDAI Chain 19
3.2.1 Targeting payments as a use case 20
3.2.2 Value Accrual 21
3.2.4. Strengths 21
3.2.5. Weaknesses 22
3.3. Loom Network 23
3.3.1. Value Accrual 23

3.3.2 An awkward birth 23
3.3.3. Strengths 23
3.3.4 Weaknesses 24

Part 4: Non-Custodial Sidechain Projects 24
4.1. Optimistic Rollups 24
4.1.1. Optimism 24
4.1.1.1. A single DeFi rollup 25
4.1.1.2. Is Optimism optimistic? 25
4.1.2. IDEX 26
4.1.2.1. Value Accrual 26
4.1.2.2. Who is using IDEX? 26
4.2. Validium (Starkware) 27
4.2.1 DeversiFi 27
4.2.1.1. Value Accrual 27
4.1.2. dYdX 27
4.3. zk-SNARKs 28
4.3.1. zkSync 28
4.3.1.2. An optimistic competitor? 28
4.3.2. Loopring 28
4.3.2.1. Siloed liquidity 29
4.3.2.2. Value Accrual 29
4.3.2.3. Strengths 30
4.3.2.4. Weaknesses 30

Part 5: Plasma Sidechain Projects 30
4.4.1. OMG Network 31
4.4.1.1. A fast, but centralized operation 31
4.4.1.2. Value Accrual 32
4.4.1.3. Strengths 32
4.4.1.4. Weaknesses 33
4.4.2. Matic Network 33
4.4.2.1. Value Accrual 34
4.4.2.2. Is a Matic gaming ecosystem developing? 34
4.4.2.3. Strengths 35
4.4.2.4. Weaknesses 36

Part 6: Relative Valuation Analysis 36

Part 7: The L2 Thesis 37

Executive Summary

The constraint of Ethereum's blockspace has meant that, as Ethereum network utilisation reaches its capacity, transaction fees have been pushed to intolerable heights for certain users. Layer 2

solutions aim to provide a more scalable environment for dApps and users by taking transactional activity off-chain. The Layer 2 landscape has been rapidly expanding recently as the demand for scalable platforms from dApps intensifies. While it is clear that all types of L2 solutions make certain tradeoffs between security, performance, and usability, those that take a more generalized approach are more likely to succeed in the long-term. Over the coming months, close monitoring of on- and off-chain developments will be necessary in order to adjust conviction in these early stage L2 networks.

Introduction

Over the course of 2020, Ethereum has seen its network usage skyrocket, largely driven by a surge in DeFi activity. When Ethereum's network utilisation was surging the most in August and September, this coincided with periods of intense liquidity mining and notable DeFi project launches, such as CRV, SushiSwap, and UNI. As transaction count grew significantly in the run up to August this year, Ethereum blockspace became more congested, throttling fee prices as users looked to outbid each other to get their transactions confirmed.

As the blockspace of Ethereum became fuller, fees continued to increase, effectively nudging out lower value transactors where the fee-to-transaction value ratio was becoming too large. The rise of DeFi protocols has also meant that Ethereum has a significant portion of its value settled on-chain (as opposed to transactional activity through centralized exchanges). Most of DeFi activity is therefore exposed to Ethereum's fee dynamics.

During these periods of fees spikes, transactions on Ethereum started to drop steadily. This initially suggests certain Ethereum users are priced out with higher fees whereby it is no longer economically viable for them to carry on transacting. This reduction of activity is then reflected in a lower overall transaction count where low value transactors wait for fees to reduce, driving transaction count up again.

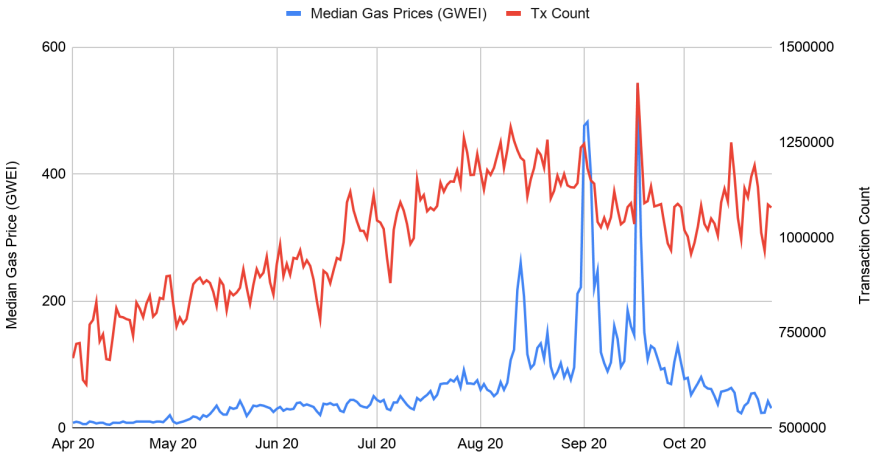

Figure 1: Median gas prices and transaction count on Ethereum (Blockchair).

We can also see a strong positive correlation between median transaction fees and transaction size, meaning as average fees increased the average transaction size also increased. This further supports the idea that certain users cease to make lower value transactions in high fee environments.

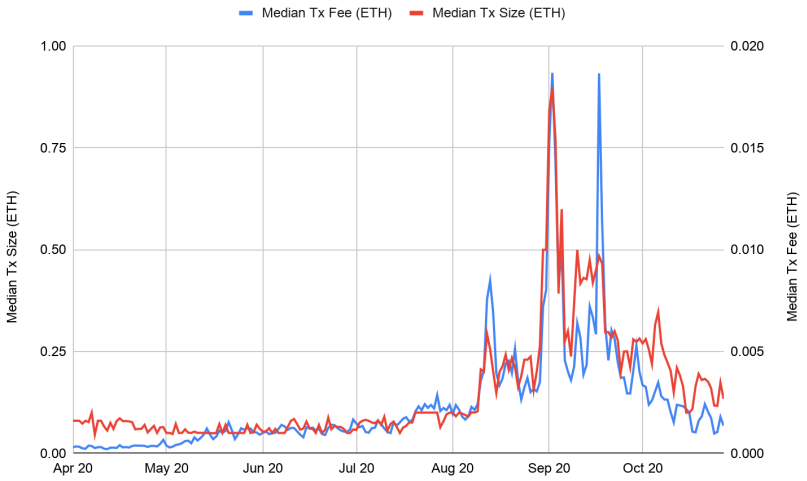

Figure 2: Median transaction fee and size on Ethereum (CoinMetrics).

So where does this leave us? First, Ethereum seems to be demonstrating what Nic Carter refers to as a fee-chain usage oscillation.[1] High network utilisation grows along with transaction count, driving fees upwards. Low value users cease to transact lowering transaction count and fees. As fees get cheaper, these lower value users start transacting once again - the cycle repeats. Since the start of October, we are even starting to see initial signs of rising transaction count as fees have dropped significantly from their peaks in August and September (Figure 1).

Scaling the Ethereum Network

Given the cyclicality, we should expect similar dynamics to play out again in the future, whereby fees continue to become prohibitively expensive for certain users during certain periods. Ethereum's fees dynamics may even be more salient and potentially disruptive as the ecosystem matures - a larger portion of Ethereum's value is to be settled on-chain as more projects and tokens come into the DeFi space. Therefore, Ethereum needs to scale to accommodate increased usage

Ethereum has the option of simply raising its gas limit as a way of stabilising fees. However, raising the gas limit comes at a cost of making the Ethereum network more vulnerable to DOS attacks as well as increasing validator requirements.[2]

Alternatively, Ethereum can scale by way of Layer 2 (L2) initiatives. Generally speaking, L2 is a collective term for solutions that take transactional activity off-chain in order to relieve the base layer chain of network congestion. By doing so, L2 solutions aim to lower transaction costs and increase throughput while providing most, or all of the security guarantees of the base layer chain.

[1] Public blockchain fee cyclicality and negative feedback loops (Nic Carter, 2020)
[2] What is Ethereum's Uncle Rate and Why Does It Matter?

In the following chapter, we will explore the different types of L2 solutions that exist today and dive deeper into specific projects that are implementing their respective solution, with a focus on potential value accrual. After, a L2 macro thesis will be laid out breaking down the types of solutions that will more likely succeed and where the best investment opportunities lie.

Part 1: Types of Layer 2 Solutions

1.1. Payment & State Channels

Payment Channels are a specialized L2 solution whereby parties lock up value in a multisig smart contract and create a bi-directional Payment Channel between them off-chain. This allows everyone within the payment channel to transact instantly because balance updates do not involve the layer 1 blockchain (e.g. Ethereum). Only when the users decide to close their Payment Channel does the net balance get published to the layer 1 blockchain.

State channels are a more generalized version of Payment Channels in that they can handle state transitions (like voting or messaging) beyond just payments between parties in a channel. Like Payment Channels, State channels require each participant to deposit value or state in a multisig smart contract but can perform unlimited transfers of value *or* state without interacting with the mainchain. Only when participants want to exit the channel do they perform an exit to the main chain.

While State Channels improve scalability, they often require 3rd parties to monitor the state updates to provide a layer of security as well as require deep pools of liquidity for payment dApps channels.

1.2. Custodial Sidechains

Sidechains are faster and cheaper blockchains that are tied to another blockchain. Sidechains are custodial if its creation relies on a brand new consensus mechanism and security guarantees. For example, value can be locked in a smart contract on Ethereum which can then be credited on the connected sidechain for users to interact with.

Custodial sidechains may not be considered to be an L2 solution by some given their stronger security independence to L1 chains (i.e. Ethereum) but are still included given that they have some meaningful connection to L1 chains in order to attract activity away from it.

1.3. Non-Custodial Sidechains

Non-Custodial sidechains are separate blockchains designed to be faster and cheaper alternatives to layer 1 chains. The security of these chains ultimately rely on layer 1 consensus layer.

1.3.1. Plasma Sidechains

Plasma sidechains are new blockchains that are tied to a parent chain (i.e. Ethereum). Plasma sidechains are not dependent on their consensus mechanisms but instead rely on the parent chain's security guarantees which is stronger. This means that if there are any security threats to the plasma sidechain at any given point, uses assets can be exited back to the parent chain

The biggest advantage that Plasma Sidechains have is that if the child chain (and all of its assets) is corrupted, users (along with their assets) are able to fall back to the parent chain. Plasma sidechains directly benefit from using the parent's chain security guarantees while at the same time being able to increase transaction throughput. At the same time, one of the challenges that Plasma has had for a while is the required 'exit window' for users who want to withdraw their assets from the plasma sidechain.

1.3.2. Rollups

Rollups are scalability techniques that aggregate a number of off-chain transactions and publish a reduced amount of data on-chain. Rollups can be split into two broad categories: zk-Rollups and optimistic rollups (ORs).

1.3.2.1 Zk-Rollups

Zero-knowledge (ZK) rollups is a technology that allows one individual to prove to another that a statement is true, without disclosing any information beyond the statement's validity. ZK proofs are an attractive scalability solution because instead of needing to write many transactions on layer 1, multiple transactions can be represented in a single succinct proof that is submitted to the mainchain.

They are also a form of *validity* proofs meaning they are *pessimistic* in nature and *only* present evidence that a state transition is correct.

zk-SNARKs and zk-STARKs are the two main zk-Rollup variations which posses certain tradeoffs:

zk-SNARKs:

- More established as a technology
- Offers quick verification (if computation is small)
- Efficient because the proofs are small in size (if computation is small)
- Require trusted set up (when zk-SNARK protocol is launched)

zk-STARKs:

- More recent and experimental
- Faster prover time is 10x faster than zk-SNARKs as computation size increases
- Does not require trusted set-up
- Resistant to quantum computing
- Proof sizes are larger than zk-SNARKs

On the surface, L2 solutions that implement zk-STARKs may be a more desirable proof type but it may just take time for the technology to be commercialized given the large proof sizes.

zk-Rollups generally keep data on-chain while solutions like Validium keep data availability off-chain. Keeping data *off-chain* dramatically improves throughput compared to keeping on-chain but means the protocol displays more of a custodial system. This is because users are informed that the chain is valid but they are unaware of the state itself meaning changes in state are explicitly disclosed to users. Therefore, keeping data availability off-chain means there is no guarantee users are able to claim their funds directly from the zk-rollup contract on the mainnet without additional layers of security.

This difference will likely determine what kind of application uses each technology. Use cases that require high trust assurances, such as decentralized crypto payments, might be more well suited for zk-Rollups while HFTs might benefit from the more performant Validium.

1.3.2.2. Optimistic Rollups

Optimistic Rollups (OR) are similar to Plasma in that they snapshot a sidechain's state on-chain but, unlike Plasma, they tradeoff scalability to run an EVM compatible virtual machine (called Optimistic Virtual Machine).

ORs assume an *optimistic* view of the world assuming that blocks represent correct states until proven otherwise. Blocks are assumed to be correct unless a single honest verifier calls out incorrect state transitions. Optimistic-based L2 solutions have become more common recently due their ease of deployment and immediate scalability advantages. Multiple dApps can deploy their smart contracts onto the same rollup and become composable with each other.

However, validity proofs are arguably a more desirable L2 approach overall given they can only provide correct state transitions to the base layer. Below is a summary table highlighting the tradeoffs i've identified between fraud proofs and validity proofs:

Validity Proofs (Pessimistic)	**Fraud Proofs (Optimistic)**
Nothing is accepted unless correct	Require fewer computational resources - not needed for every transition
Not possible for validators to steal funds or corrupt rollup state	Only requires single honest verifier
Faster time-to-finality	Flexible for general-purpose computation
Needed for every state transition impacting scalability	Vulnerable to DDOS attacks - 'silence' is implicitly assumed to be good
Computationally expensive	Requires exit windows and higher time to finality which limits composability
May require trusted setup	Requires collateral

Figure 3: Tradeoffs between Validity Proofs and Fraud Proofs.

1.4 Table of Tradeoffs

It is clear that the wide range of L2 approaches each have their tradeoffs. Below is a table summary comparing each type of L2 solution from a design, performance, security, and usability perspective. The key takeaway here is that one size does not fit all and there exists nuance in how each solution can be performant, secure, and usable. For example, Validium-based solutions can offer very high throughput relative to most other L2 designs but can only achieve this by keeping data availability off-chain (therefore reducing security guarantees).

	State Channels	Plasma	Sidechains	OR	zk-Rollups	Validium
Design						
Data	Off-chain	Off-chain	On-chain	On-chain	On-chain	Off-chain
Cryptographic Research	Standard	Standard	Standard	Standard	Experimental	Experimental
Performance						
Throughput (ETH 1.0) TPS	Limitless	1-9k	10k+	2k	2k	20k+
Throughput (ETH 2.0) TPS	Limitless	1-9k	10k+	20k+	20k+	20k+
Tx Costs	Lowest	Lowest	Low	Low	Low	Low
Security						
User Liveness	Yes	Yes	No (Bonded)	No (Bonded)	No	No
Requires New Consensus Layer	No	No	Yes	No	No	No
Validators/Operators Freeze Funds With Quorum?	No	No	Yes	No	No	Yes
Validators/Operators Confiscate Funds Quorum?	No	No	Yes	No	No	Yes[1]
Usability						
Exit Strategies	No	Yes	No	No	No	No
Expected Withdrawal Time	1 Confirmation	1 week[2]	1 Confirmation	1 week[2]	1-10 minutes	1-10 minutes
Capital Efficient	No	Yes	Yes	Yes	Yes	Yes
Requires On-chain Tx	Yes (Channel)	No	No	No	Yes/No[3]	No
Time to Subjective Finality	Instant	1 Confirmation	N/A	1 Confirmation	1-10 minutes	1-10 minutes
EVM Portability	No	No	Yes	Yes	Scheduled	No
Native Privacy	Limited	No	No	No	Yes	Yes
Smart Contracts	Limited	Limited	Yes	Yes	Yes	Yes

[1] Through StarkEx contract upgradability.
[2] Can vary but 1 week is common.
[3] Depends on implementation. Loopring does, zkSync does not.

Figure 4: Performance, security and usability of different L2 solutions.

1.5 The Current L2 Landscape

Figure 3 below presents a high-level overview of the current L2 landscape with live projects placed in their respective category. In the next section, L2 projects within each category will be analysed according to their technology, development, and token value accrual (where applicable).

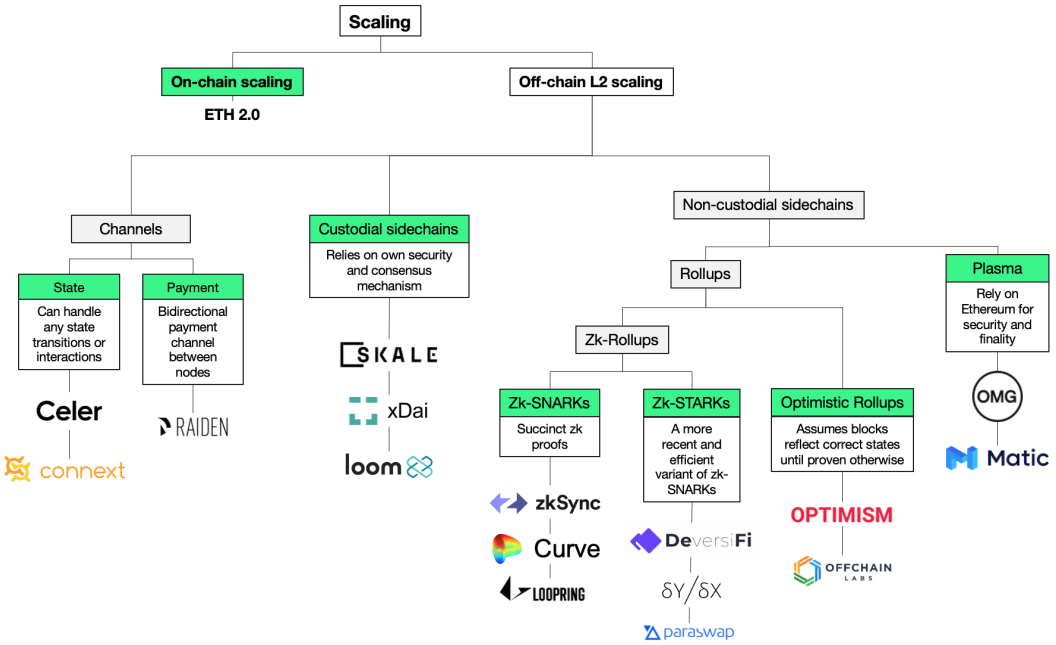

Figure 5: A high level overview of the current L2 landscape.

Part 2: Payment & State Channel Projects

Payment & State Channels			
Project name:	**Raiden Network**	**Connext**	**Celer**
Issuer:	Brainbot	Connext Labs Inc	ScaleSphere Foundation
Symbol:	RDN	N/A	CELR
Transaction Asset	Transaction asset	Any Asset	CELR
Transaction Costs	?	No fee	No fee (exc. Rollup chain txs)
Layer 1 Serviced	Ethereum	Ethereum	Agnostic
Initial Distribution	100M		600M
Circulating supply	67M	N/A	4B
Max supply	100M	N/A	10B

2.1. Raiden Network

Raiden Network was one of the first projects dedicated to scaling Ethereum and is a Payment Channel implementation for Ethereum.

Users can pay protocol fees to routing nodes which are denominated in the tokens that are transferred in the channel. Users also have to pay a second layer of fees denominated services that help operate the network. This second set of fees are denominated in its native cryptoasset, RDN.

Raiden Network claims to be cheaper because users only have to pay for nodes forwarding the transfers from the payer to the payee.

2.1.1 Value Accrual

Given that RDN acts as a fee token, value accrual will be limited given the limited use of the token beyond paying services who might eventually sell their RDN to cover their real-world costs. The number of open channels has been flat for over a year (~90 channels) as well as the number of unique accounts per day (~55).[3]

2.1.2. Strengths

- Transfer fees on the Raiden Network are much lower than on-chain transaction fees

2.1.3 Weaknesses

- Raiden is limited to only payment transactions which severely narrows its use cases as it cannot cater for general state transitions
- The RDN token value accrual is weak
- The value proposition of Raiden is highly dependent on the number of participants increasing, as routes between payer and payees can be more easily found without having to open further but direct channels
- Adoption of Raiden over the last 12 months has been unimpressive

Raiden Summary *- Payments channels like Raiden may have some meaningful adoption but the investment opportunity is unattractive from a value accrual perspective.*

2.2. Connext

Connext is a state channels network on Ethereum which allows transactions to be routed off-chain across a network of nodes. Connext does not have its own token and the network does not collect any fees meaning Connext does not present itself as an investable opportunity for DPC. Nodes routing transactions and providing storage may choose to collect fees in the future if they choose to.

The Graph recently announced that it would be working with Connext in order to enable small micropayments between different participants in The Graph's network[4]. This may indicate that Connext might be the first State Channel network to deploy at scale while other projects have tried to commercialise similar architecture with new token mechanics (see Celer below).

Connext Summary *- Connext does not present itself as an investable opportunity in its current form.*

[3] Raiden Analytics
[4] The Graph is implementing state channels technology on its Ethereum-based network (The Block)

2.3. Celer Network

Celer Network is a blockchain-agnostic platform that can facilitate fast low-cost off-chain payments as well as *state* transitions. By allowing for state transitions, the Celer Network can be used for applications that involve more complex interactions, such as games. Users can open a channel with each other (either directly or through a common intermediary) in order to play while paying zero transaction fees to install, use, and uninstall applications.

State Channels seems to make the most sense when the applications:

- have to deal with a large number of transactions or interactions (which would incur high fees on-chain)
- only require a small number of participants in an environment (e.g. 1v1 arcade game)

While Celer seems to improve on scalability by moving activity off-chain, State Channel adoption requires overcoming the issue of needing users to be constantly available online in order to sign new states between each other.

The team announced earlier this year they would be launching a Delegated Proof-of Stake (DPoS) sidechain in order to offer dApps a wider range of infrastructure options that vary on security, cost, and throughput. For example, low-value but high frequency transactions can occur within Celer's State Channels while higher value transactions (where stronger security is more important) can capitalise on a separate sidechain.

The clear benefit here is that Celer is broadening its toolbox for dApps that may have differing requirements. The issue is that creating a sidechain means creating a new consensus mechanism from scratch. Celer is cleverly leveraging their existing State Channel validator set to provide block producing capabilities.

2.3.1. Value Accrual

Celer uses its own native cryptoasset, CELR, to incentivise users to make the network more secure, stable, and efficient. CELR is used in the following ways:

- As a fee token for providers who secure channel state for when users go offline in channels and validators that batch transactions on the Celer sidechain
- Staked by validators in order to perform state monitoring and earn service fees
- Rewarded to service providers who contribute liquidity in order to serve their clients (bootstrapping mechanism)
- Staked by service providers who borrow liquidity from capital contributors in order to maximise their chances of winning their auction

The CELR token should accrue value as more users and dApps join the Celer Network, and fees increase to validators. As more validators support the network, Celer becomes even more efficient at supporting its user base.

2.3.2. Constraints of the system

However, there are a few drawbacks regarding Celer's design that may hinder its adoption. Firstly, State Channels by their design tradeoff scalability with liquidity and security. Celer is forced to address these issues by introducing various incentive mechanisms which add further layers of complexities and economic considerations. Second, using OR as the proof method on the sidechain means there will be significant withdrawal friction for users who want to exit onto other chains and the latency. Questions also remain with how composable the sidechain can be with other layer 1 chains given the different settlement model to other base layers like Ethereum.

2.3.3. Strengths

- By creating a more holistic approach to scaling, Celer has the ability to cater for a wider range of dApps and use cases where each might require high transaction throughput or higher security guarantees of a layer 1 security
- State Guardian Network tackles the issue of nodes going offline and ensuring availability - one of the significant drawbacks of standard State Channels designs
- Cost for smart contract transactions are zero-fee as parties within a channel are only updating state between themselves
- Users do not have to pay the layer 1 gas fees for including their transactions in layer-2 rollup (more on OR later)
- A hybrid approach means if there is congestion on the layer 1, users can have strong assurance that their transaction is confirmed based on the security guarantees of the DPoS consensus

2.3.4 Weaknesses

- Liquidity has to be moved off-chain and locked in order for state channels to be created and used
- The number of parties within a state channel needs to be pre-defined which may not be optimised for large sets of highly active users within an dApp moving in and out
- The use of OR provides high throughput at the expense of breaking composability and adding UX friction

Celer Summary *- Celer strategy as an L2 is not clear and it will likely struggle to compete effectively against other projects that implement sidechains from genesis. The ability for the CELR token to attract significant value accrual is also questionable.*

Part3: Custodial Sidechain Projects

Custodial Sidechains			
Project name:	**SKALE**	**xDAI**	**Loom**
Issuer:	SKALE Labs	POA Network	Loom Network

Symbol:	SKL	xDAI	LOOM
Transaction Asset	N/A	xDAI (stable)	N/A
Interoperability	Ethereum Bridge	Bridges (2x Ethereum)	Ethereum, Binance, Tron Bridges
Staking	Live	Live	Live
Transaction Costs	?	$0.000021	$0
Production	Mainnet June 2020	xDAI Bridge Q4 2019	Mainnet September 2018
Market Cap	$125M (Public Sale Val.)	$32M	$15M
Initial distribution	4.55B	8.5M	600M
Current supply	4.55B	2.8M	970M
Max supply	7B	No Max	1B
TVL	$60m	$2m	?
dApps	?	31	4

3.1. SKALE

SKALE Network is an L2 scaling solution for Ethereum primarily aimed at scaling smart contracts as well as improving the affordability/usability for dApps developers.

3.1.1. Approaching scalability with customisability

SKALE operates *custodial* sidechains meaning each SKALE sidechain has its own Delegated Proof-of-Stake (DPoS) consensus mechanism (and therefore doesn't rely on Ethereum at the consensus layer). Unlike other sidechain networks, its clear SKALE is doubling down on modularity and customisability for dApp developers. dApps can create highly-customisable, modular sidechains where they can tailor their infrastructure based on their individual needs (i.e. consensus mechanics, virtual machine, frequency of shuffling). This is roughly analogous to what Parity Substrate aims to do for the Polkadot ecosystem and does not exist for other L2 solutions like Plasma or Optimistic networks. Overall, this level of customisability for dApp developers is attractive because resource costs are relative to network overall utilisation while also being able to cater for a wide range of use cases like DeFi, Games, and Commerce.

SKALE's architecture as a L2 solution is unique due to the fact that each elastic sidechain is operated by a group of subnodes. Depending on the size of the sidechain, a certain number of subnodes are selected from a subset of nodes in the whole network. A problem here is that individual dApps would be at risk of potential collusion if how the nodes are selected is not random or rotated. The SKALE team acknowledges this and has designed the network to rotate nodes frequently so that independent sidechains can benefit for the security of the *whole* SKALE network.

3.1.2. Close ties with Ethereum

SKALE will be closely tied to the Ethereum ecosystem. The network will be interoperable with ethereum allowing users to deposit assets in SKALE smart contracts that exist on Ethereum. SKALE will also innovatively use Ethereum's randomness to select to assign nodes for each of the network's sidechains. SKALE will also feature EVM compatibility and Ethereum developer tooling like Truffle allowing developers to leverage their existing tools to migrate to the network more easily.

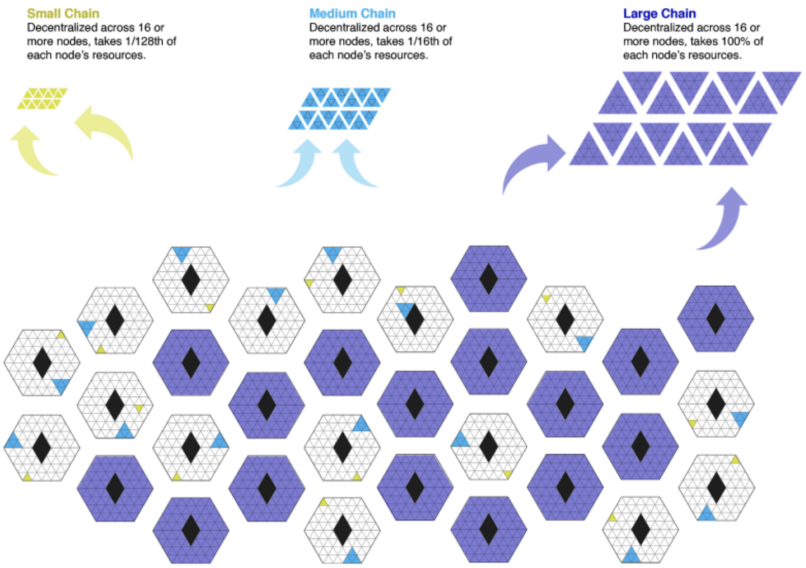

Figure 6: A high-level overview of SKALE subnode selection

3.1.3 Value Accrual

SKALE is directly investable through its native cryptoasset, SKL. The main function of SKL is to incentivise validators to support the network by contributing hardware resources and operational upkeep efforts. Rewards for validators will mainly come from two sources:

1) Network issuance (i.e. SKL Inflation from nodes that stake SLK tokens)
2) dApp fees

Token holders choose to stake for 3, 6, or 12 months. Staked SKL that is locked for longer periods will have a higher reward rate. This roughly works out 1.5x for 6 months and 2x for 12 months when compared to staking for 3 months. Incentivising longer term staking not only beneficial for network security but also likely drives SKL off the secondary market for longer periods.

3.1.4. Dynamic economics

Apart from network issuance, SKL's ability to accrue value is directly tied to the network's ability to attract dApp developers who are willing to pay in order to build on the SKALE network. For me, the main driver that will get dApp developers to do this are three fold: the customisability aspect, traffic dynamics being limited to each sidechain, and the Ethereum interoperability and tooling.

Years	SKL Minted	% of Total SKL Supply
1	385M	6%
2	346.5M	5%
3	308M	4%
4	26.59M	4%
5	231M	3%
6	192.5M	3%

Figure 7: SKL rewards 6 years after mainnet launch

For dApp fees, SKL that are deposited by dApp developers gets allocated to a bounty pool where it eventually gets distributed out to validators as rewards. It seems like the thinking here is that when the SKALE network matures, the rewards from dApp fees will form a larger portion of the validator rewards on a per node basis. As is typically the case for a larger number of networks, issuance will be more heavily weighted for the earlier years and decay each year in the first six years.

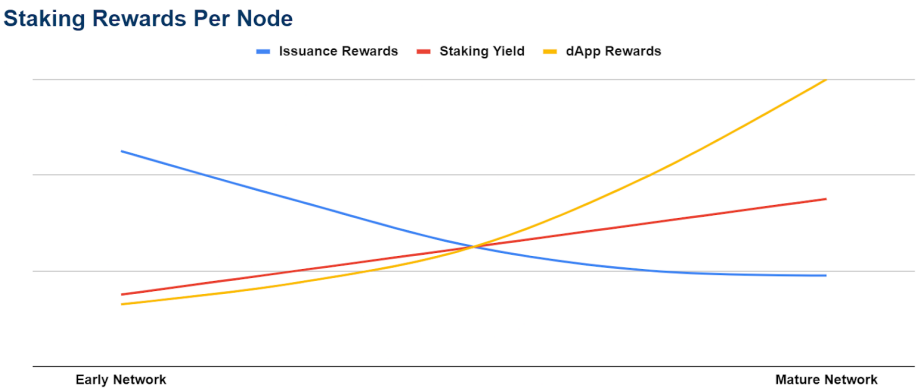

Figure 8: SKL rewards visualisation as a function of network maturity

An interesting economic mechanism for SKALE is that the network strikes a balance between supply and demand in order to create a more cost effective network. Given there will be finite resources available at any given time, if the network becomes over utilized, then the price of creating a sidechain has to climb as node resources become more scarce.

Having a network utilisation (defined as % of total network resources available) above 85% drives up the sidechain cost dramatically. Becoming over utilized as a network runs the risk of deter further usage of the network and so nodes are then incentivised to contribute further resources. By doing so, nodes will increase supply to meet demand and therefore reduce prices. In theory, this mechanism should also help provide price stability for dApp developers.

3.1.5. A locked up investor base

One of the more unique aspects to the SKALE token economics is all tokens are not liquid upon launch but are instead staked to secure the network with varying vesting periods. The total supply SKL distribution is as follows:

- 27% for delegator allocation - includes early supporters with lockup periods ranging from 6-36 months based on SAFT agreements and public allocation where participants were required to stake at least 50% of their tokens for 90 days before becoming liquid. Private allocation bought in between $7m and $149m fully diluted market value with the public sale buying at $210m fully diluted market cap.
- 10% to the N.O.D.E. Foundation vesting over a seven 7 year period since launch
- 20% for SKALE team and will be unlocked after 1 year and vest over 3 years
- 2% for the ecosystem fund unlocked at launch
- 8% for protocol development fund unlocked after 6 months and fully vested after 1 year
- 33% for validator rewards

Analysing the vesting schedule for the SKL, a potential supply glut could come in from 6-14 months when the free float SKL supply increases from 15% to 60% with the largest contributors stemming from early supporters, protocol development fund, and validator rewards.

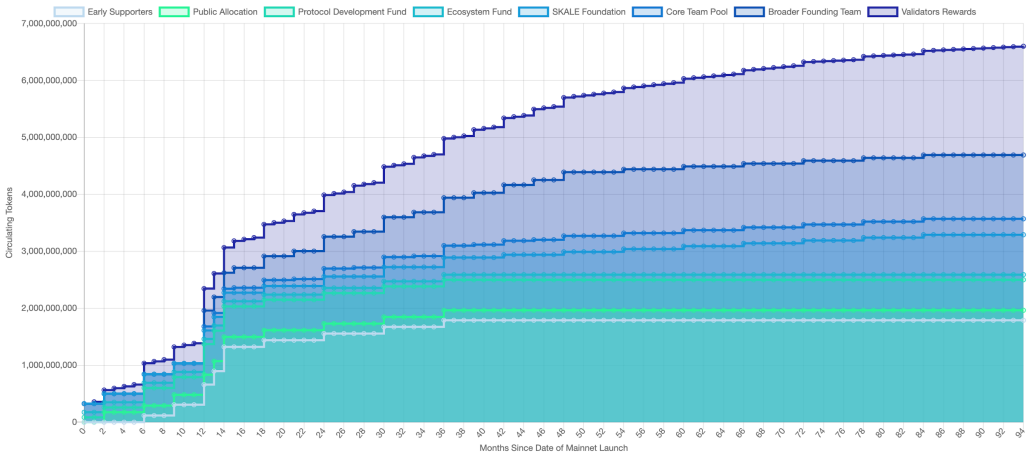

Figure 9: Vesting schedules for the SKL token over 94 months.

3.1.6 Strengths

- SKALE is taking a strong *generalized* approach providing infrastructure that will be more effective at catering for multiple use cases
- Sidechains are configurable to each dApp meaning that dApps will unlikely overpay on security
- It will be easier for Ethereum dApps to migrate over due to the EVM compatibility and Ethereum-based tooling. It is clear the SKALE team have recognised the importance of this by explicitly building out an Ethereum 'flavoured' ecosystem[5]
- dApps alleviate transaction fees for their users completely similar to plasma sidechains like Matic

[5] SKALE Blog - "SKALE Network Announces over 40 Partners in its Ethereum Scaling Ecosystem."

- Pooled security means each independent sidechain is secured by the entire network's resource
- SKALE has a strong set of validators including Staked, Chorus, Figment, and Ankr
- The network boasts as having $80m TVL by validators securing the network today[6]

3.1.7. Weaknesses

- SKALE only launched their network in October 2020 and has yet to prove out its model in the wild
- Other L2 solutions that are building momentum (like Optimism) may reduce the attractiveness of dApps wanting or needing to stake SKL to pay for SKALE Network utility. The rollout of ETH 2.0 may also dilute SKALE's value proposition as a platform for more performant dApps
- The USD price of chain purchasing/rental will fluctuate with the market price of SKL. Prospective dApp developers have to calculate their real-world costs driven by both the network utilisation ratio and SKL market price
- A key threat to SKALE's modularity USP is Parity's substrate - a modular blockchain framework that allows developers to build custom EVM compatible chains and Polkadot parachains. SKALE's edge might be it's stronger Ethereum ecosystem ties and developer tooling.
- SKALE was launched with a punchy fully diluted market valuation (~$125m) which potentially reduces the return multiple as an investment
- Rewards are currently set to be distributed once per month which might deter delegators who are looking for more frequent rewards for securing the network but equally ensure that participants are aligned with the network long-term

SKALE Summary *- SKALE's success will likely be driven by its ability to offer highly customisable sidechains for dApps to build on and its strong ties to the Ethereum ecosystem. The SKL token is an attractive investable opportunity where it has the ability to accrue and maintain value but launching with a high valuation weakens the prospects of significant returns.*

3.1. xDAI Chain

xDAI Chain is a sidechain to Ethereum designed to be a stable payments platform for users and dApps. xDAI Chain achieves this by using a Dai-pegged stablecoin, xDAI, as its native currency. Using xDAI on a sidechain allows users to have lower and more stable transaction costs (~$0.000021) than on the Ethereum mainnet. This is in contrast to most other L2 solutions which introduce new but volatile transactional currencies (e.g. Celer).

xDAI works by users locking any asset Ethereum and minting a 1:1 representation on the xDAI chain. The xDAI chain (including the bridges) is validated by a private PoS consensus (with MakerDAO, Giveth, POA, Protofire being the validators). In the coming months, xDAI will be moving to a fully permissionless network allowing any to become validators.

[6] Coindesk - "Ethereum Layer SKALE Launched Mainnet Phase 2 With $78M Already Staked."

One of xDAI Chains' issues today is its limited throughput capabilities. It currently has a transactions-per-second of ~70 (~4.6x Ethereum)[7]. While this may seem lower than other scaling solutions (e.g. Matic network), there are many reasons as to why xDAI Chain can become more performant:

- xDAI can be scaled horizontally - this could be done by adding more chains connected by bridges
- xDAI can be scaled vertically - essentially optimising nodes
- When xDAI implements HoneyBadger BFT consensus, it will likely improve this throughput by 5x

3.2.1 Targeting payments as a use case

Using a stable native currency means xDAI can cater for a wide range of use cases that benefit from low, predictable costs. This may be why have seen a multiple (often payment-related) use cases come to fruition in the last few months:

- **Peer-to-Peer Payments** (Burner wallet) - quick, inexpensive, easy solution to carry and exchange small amounts of crypto in web browser
- **Prediction Markets** (Gnosis Prediction Market is moving to xDAI) - providing a scalable platform for prediction market participants with lower stakes
- **NFTs** (Nifty.Ink) - allowing users to create and mint NFTs for free (use of meta transactions)
- **Blockchain Games** (DAOG) - providing low, predictable costs and high speeds for multi-player game environments
- **DAOs and governance layers** (Galt Project, Vocdoni) - providing a scaling solution that is capable of handling voting procedures effectively and efficiently with low costs.

For the staking returns, APR is calculated in 2 ways: time-based emissions and supply-based emissions. Each has a maximum of 7.5% APR.

For time-based calculations, emissions are earned on the amount stakers stake in the protocol meaning stakers are incentivised to stake longer to maximise their APR.[8] For supply-based emissions, APR is calculated based on a total supply factor parameter whereby the total supply is adjusted by multiplying it by the total supply factor. The ratio of total STAKE locked in the contract to the adjusted total supply then dictates the level of APR (up to a max of 7.5%). This design should encourage a larger portion of the circulating STAKE supply to be locked up for longer but it also theoretically allows for up to 15% inflation in perpetuity.

3.2.2. Value Accrual

By supporting the xDAI chain security via consensus, STAKE holders receive a number of incentives. At a high level, STAKE holders receive rewards in the following ways:

---

[7] TPS is an imperfect measure of scalability. A more useful measurement is the cost to run a node relative to throughput capabilities.
[8] Time-based emission formula.

- Staking rewards from emission
- Transaction fees paid to validator who seals block
- Bridge fees of 1% (ETH - xDAI AMB Bridge) from assets transferring from xDAI to Eth
- xDAI rewards - DAI Interest for STAKE stakers through MakerDAO's DSR
- EXIT rewards - there is little information about this right now but it seems to be a separate stable currency backed by soft ETH

STAKE's value accrual will be driven by the protocol's ability to attract asset migration through its bridges as well as transaction fees accrued from transfers and smart contract interactions. Given xDAI fees are low, very high volume is also necessary to drive sufficient value to token stakers. As of October 29th, xDAI's fair value using TVL to supply ratio indicates that STAKE is overvalued by 17x. On transaction data that is available, xDAI Chain's transaction count has been fluctuating between 25k and 75k on a daily basis showing the chain still has some way to go relative to Ethereum's activity.[9]

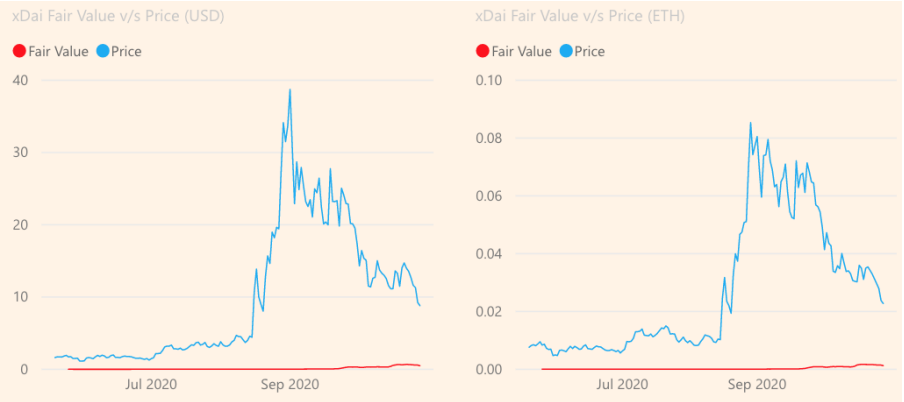

Figure 10: xDAI's APT vs price

3.2.4.Strengths

- Using a stable transactional currency presents a clear value proposition for dApps and users. Separating the role of STAKE and xDAI is a cleaner approach to achieving stability on one end and value capture on the other
- STAKE's ability to accrue value is directly tied to the xDAI chain adoption. The STAKE token has numerous revenue streams which makes it an attractive investment opportunity as more dApps and users become attracted to xDAI's stable system
- xDAI is a horizontal play meaning the STAKE token can capture further value as xDAI plugs into other chains beyond Ethereum
- xDAI has already attracted dApps to migrate some of their smart contracts over to the xDAI chain. These dApps have also varied in their sector demonstrating xDAI ability to attract a wide range of use cases and therefore activity
- xDAI has smart contracts and toolset compatibility for Ethereum lowering friction for dApp migration

[9] xDAI Block Explorer

3.2.5. Weaknesses

- xDAI is competing in an increasingly competitive L2 space. xDAI marks an improvement in overall transaction costs and throughput compared to Ethereum mainnet but performance capabilities fall short compared to others like Plasma sidechains like Matic Network (7k TPS) or zk-rollups chains (Up to 20k TPS[10])
- Major DeFi dApps have taken an initial interest in deploying their smart contracts on alternative L2 solutions to xDAI (Synthetix with Optimism and Curve with zkSync). If network effects are the most important determinant of a L2 solution's success then xDAI might have an uphill battle for adoption
- Stake ratio naturally favours validators with larger stake proportional to total staked amount for all validator pools which may lead to centralisation of validators. There is an argument to be made that this reverses efforts to decentralise the chain over time and there may need to be a proposed solution whereby validators can be 'over-staked'
- xDAI relies heavily on MakerDAO's protocol. This presents single chain risk but can be mitigated once other stable assets are introduced and bridged. Dai is also one of the more illiquid stablecoins relative to Tether and USDC which makes bridging Dai onto the xDAI chain harder
- It is unclear whether xDAI's value proposition is diluted once Ethereum 2.0 gets underway and applications are eventually able to effectively communicate across shards asynchronously. xDAI might just be merely an intermediary solution.
- Infinite inflation mechanism - theoretically the network can have annual APR of 15% year-on-year giving exponential growth to total supply. While reaching 15% APR is unlikely to happen anytime soon, this remains a theoretical possibility
- Before consensus change are introduced with POSDAO later this year, xDAI remains much more centralized than Ethereum
- Dai is one of the more illiquid stablecoins out there compared to CEX USD variants (<1%)[11]

xDAI Summary *- xDAI has the ability to stand out from the crowd from other L2 solutions by giving dApp developers and users to transact with low but stable transaction costs. The STAKE token economics is attractive given the multiple reward streams for holders as well as xDAI Chain representing a horizontal play. However, the chain has yet to prove out that low, stable transaction costs is enough to migrate activity over from Ethereum and is arguably overvalued relative to its fair value.*

3.3. Loom Network

Loom Network allows developers to build dApp-specific sidechains on top of Ethereum. There are two main layers to the Loom stack:

- A BaseChain that acts a multi-chain platform
- Application-specific sidechains

BaseChain (originally called Plasmachain) is Loom's main sidechain which links to the Ethereum public blockchain at fixed intervals. It is managed by a DPoS consensus mechanism. It seems that

[10] Depends on the implementation but Validium chains can support 20k TPS.
[11] CoinMetrics Stablecoin Circulating Supply

the Loom architecture is focussing on NFTs given Plasma Cash does not support fungibility. The potential issue here is that without other implementations of other Plasma technologies (e.g. Plasma debit) payments are not natively supported, making Loom a more niche L2 solution despite claiming to be interoperable with other chains such as Ethereum, Binance Chain and Cosmos.

3.3.1. Value Accrual

The LOOM token is used to uphold the security of the Loom Network, namely the Basechain network. Validators and delegators can stake LOOM tokens to Loom sidechains and by doing so they receive block rewards, dApp hosting fees, and Transfer Gateway fees. Loom does not charge transaction fees in order to reduce users friction and instead relies on dApp hosting fees. There is currently a flat fee of 3000 Loom (~$59) per year but it is not clear how this can be adjusted based on market dynamics. Therefore, the demand for LOOM will theoretically be driven by dApps paying a monthly deployment fee of 3000 LOOM paid out to validators and their delegators.

3.3.2. An awkward birth

There are three main issues with Loom. First, the overall scope of the Loom seems limited by not easily allowing for fungibility on Loom sidechains. Second, according to dApp radar statistics, there is only one LOOM dApp that has *any* volume - Axe Infinity.[12] Transaction count on the Basechain is also consistently below 4k (and falling) in the last 14 days.[13] Third, the LOOM team has lacked a clear rollout strategy with the team now pivoting completely to healthcare records.

3.3.3. Strengths

- Having an application-specific approach allows sidechains to be optimised for a particular use case
- Users do not have to pay fees as these are completely abstracted away making a user experience more fluid and makes away for features like meta transactions for newly onboarded users

3.3.4. Weaknesses

- By using Plasma Cash, there is no possibility of fungibility for the assets supported on the sidechains. This means every asset is an ERC721 so payments are not natively supported.
- dApps are forced to spin up their own individual chains meaning each chain is application-specific. Not all dApps may want to do this and may just want to deploy on public sidechains like Matic. If dApp developers *want* high customizability, then SKALE might provide a richer foundation
- The Loom team has had a hard time remaining focussed lacked effective communication with the community, as well as pivoted their target market several times

[12] dApp Radar Loom Dashboard
[13] BaseChain explorer

- On-chain activity remains very low on the BaseChain - Loom publishes empty blocks frequently

Loom summary *- Loom has lacked a clear development strategy with activity being non-existent. Their NFT-only architecture already feels outdated compared to other solutions out there.*

Part 4: Non-Custodial Sidechain Projects

Non-Custodial Sidechains					
Project name:	**Optimism**	**IDEX**	**DeversiFi**	**zkSync**	**Loopring**
Issuer:		Aurora Labs S.A.		Matter Labs	Loopring
Symbol:	N/A	IDEX	NEC	N/A	LRC
Token Type	N/A	Staking	Governance	TBD	Staking
Initial Distribution	N/A	100M	600M	N/A	560M
Current Supply	N/A	538M	158M	N/A	1.2B
Total Supply	N/A	1B	618M	N/A	1.3B

4.1. Optimistic Rollups

4.1.1. Optimism

Optimism is a Public Benefit Corporation that provides optimistic rollup-based scaling solutions for Ethereum *without* the introduction of a new token. The first dApp to integrate with Optimism's testnet is Synehtix who have ported over their smart contracts to achieve:

1) Lower cost for users staking/unstaking SNX
2) Quicker confirmation times relative to Ethereum's (~0.3 seconds)

4.1.1.1. A single DeFi rollup

Optimism is being rolled out in phases (focussing on one network at a time) but there are potential collaborations for Chainlink and Uniswap that could be informative.[14] We could imagine a scenario where multiple prominent DeFi dApps congregate together to form a 'DeFi Rollup' where each dApp on the rollup could be composable with each other. As we have seen frequently in the past, network effects can be a powerful driver of activity rather than solutions that offer the best technology.

An alternative for a single DeFi rollup is for different dApps to run on different optimistic rollups that are able to communicate cross-rollup. A possible solution to this is to have individual rollups conforming to some sort of standard to share a common registry of accounts between them. For

[14] Ethereum scaling startup Optimism releases limited testnet of its Layer-2 solution

example, Alice on one optimistic rollup can send some value to Bob on a separate optimistic rollup without requiring Bob to have an account on Alice's rollup.

4.1.1.2. Is Optimism optimistic?

Optimistic rollups utilise fraud proofs in order to ensure correct state transitions occur. However, by using fraud proofs, the latency to finality (on-chain interactions) is a clear disadvantage compared to rollups using validity proofs given ORs can be reverted within a certain time frame. The UX of longer latency could be mitigated by the use of "exit LPs" who could facilitate instant withdrawals for users. Synthetix users wanting to exit funds from the Synthetix rollup could exit 'faster' by paying LPs to forward the assets before the exit window is complete.

There are also questions around what the formal process is to select transaction aggregators and what the specific bond requirements will be to deter malicious behaviour. Most systems will implement some kind of staking requirement to ensure the rollup is resistant to certain attacks. It is likely that the optimal bond amount will scale according to the total value locked (TVL) in the rollup chain. A balance is needed to be struck between having a low enough stake requirement to broaden out the aggregator set but high enough to reduce the number of malicious delays and invalid blocks.

In the short to mid-term, despite these issues, the protocols that have already stated their intention to migrate their smart contracts onto Optimism's OVM rollup (e.g. Synthetix) will seek to encourage other protocols to similarly migrate onto the same rollup.

Optimism summary *- Optimism will likely be a key stomping ground for existing DeFi applications to scale on a single DeFi rollup in the short- to mid-term given the power of network effects. Fundamental questions remain about OR composability.*

4.1.1. Arbitrum (Offchain Labs)

Arbitrum is an alternative optimistic-based L2 solution for Ethereum dApps. Arbitrum is similar in its design to optimistic rollups but their main difference lies in how dispute windows operate. Optimistic rollups have a longer potential window for dispute resolution while trading off on-chain costs. Arbitrum instead uses a 'multi-round' that shortens the window period but reduces costs to resolve disputes cheaply on-chain.

The Arbitrum team claim that Arbitrum can handle up to 390 swaps per second with a 55x gain in gas efficiency for the base layer[15]. Arbitrum launched their rollup testnet earlier in November 2020. To showcase the technology, the Arbitrum team ported over the Uniswap contracts allowing users to exchange their tokens through Arbitrum.

Arbitrum *summary - Arbitrum will quickly emerge as a competitor to Optimism's rollup solution but development is still in the very early stages. It is not clear if the solution will be favoured among dApps at present.*

[15] Arbiswap: our port of Uniswap V2 on Arbitrum Rollup

4.1.2. IDEX

IDEX is a non-custodial trading platform that uses a centralized OR that supports batch settlement of trades to reduce gas costs. Users are required to sign with their private keys in order to make any changes to this ledger but transactions are batched and settled on Ethereum every few minutes. This means that the core contract on Ethereum is solely responsible for escrowing user funds, eliminating the need for account balance information to be stored on-chain.

As IDEX uses ORs, nodes have to be incentivised to review all transactions published to the off-chain ledger, calling out fraudulent submissions as they occur. To compensate for their work, nodes earn a percentage (currently 50%) of the trade fees collected by the network.

4.1.2.1. Value Accrual

IDEX is a capital asset where staking nodes have a claim to a portion of the trading fees taken by the exchange. Therefore, IDEX's ability to accrue value relies on the exchange being able to facilitate consistent high volume - the higher the trading volume, the more revenue is generated and distributed out to staking nodes.

4.1.2.2. Who is using IDEX?

Over the last year, trading volume on the exchange has been less than impressive. Despite showing signs of positive growth in the run up of summer 2020, volume has steeply declined in the last 2 months after failing to surpass $4m over a 24hr period.

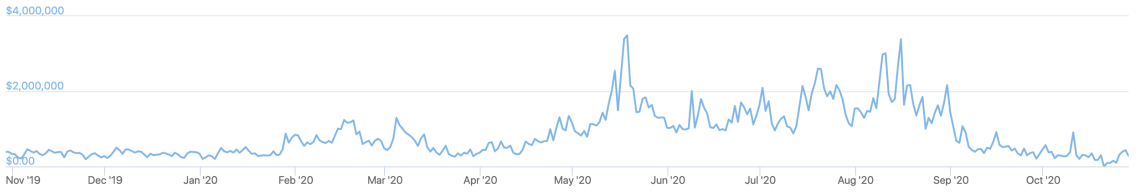

Figure 11: IDEX Exchange volume ($) for the past year.

IDEX's clunky UI, lack of clear strategy, and limited trading pairs are likely two main reasons for the lack of IDEX adoption. Until these issues are addressed, IDEX will unlikely ever gain meaningful traction.

IDEX summary *- The L2 exchange has failed to attract any meaningful liquidity or volume, facing stiff competition from other DEXs scaling. The overall likelihood that IDEX manages to take significant DEX market share is low.*

4.2. Validium (Starkware)

4.2.1. DeversiFi

The only investable contender within this bucket is necDAO which governs the zk-STARK based DeversiFi exchange underneath it. DeversiFi uses Starkware's DEX engine product to provide a self-custodial and high throughput venue for serious traders. While DeverisFi can facilitate ~9k+ TPS, it keeps making extra data availability assumptions due to data availability being off-chain.

4.2.1.1. Value Accrual

The token, NEC, is an interesting deflationary governance and utility token that give users:

1) Voting rights
2) Trading fee discounts
3) Ability to auction NEC for partial trading fees accrued on the exchange

The third creates a link between NEC price and DeversiFi trading volume and provides buy-side pressure for NEC on the markets. However, DeversiFi's exchange volume has dwindled since launching averaging around $200k per day and the lack of composability to DeFi has been a driver in the lack of adoption. The other issue here is that, because user balances are kept off-chain, a Data Availability Committee is necessary in order to ensure that users can withdraw funds in the case DeversiFi or StarkWare go offline. It therefore requires traders to trust a collection of trusted entities in order to keep data available.

Overall, DeversiFi could be a promising solution but it currently fails to show any meaningful traction so far meaning value accrual to the NEC token has been limited.

DeversiFi summary *- DeversiFi will struggle to attract liquidity from traders given the low composability with the rest of DeFi. Volume will likely stay low for the foreseeable future meaning its NEC token will unlikely accrue any meaningful value.*

4.1.2. dYdX

The derivative exchange, dYdX, partnered with StarkWare in August 2020, in order to collaborate on a L2 scaling solution for perpetual contracts. Like with DeversiFi, dYdX will operate in a centralized manner by moving computation off-chain and using Ethereum as the commitment layer.

Incorporating with StarkWare means users will be able to have instant trade settlement, lower gas & trading fees, as well as more performant price oracles. dYdX's usage of StarkWare as a L2 solution means there is no investable opportunity via a token, but it is worth highlighting that, together with DeversiFi, StarkWare is fast emerging as a trusted solution for exchanges looking to build out their scalability capabilities.

The key point here is that adding a token here may not be necessary to align incentives, given the validity proofs are *the* security assurance that users of StarkWare-based exchanges have. This may have certain implications for other zk-rollup centralized exchanges that implement a token within their design, as it may highlight that a token may not be necessary to ensure security, particularly when data availability is on-chain, such as Loopring (more on this below).

4.3. zk-SNARKs

4.3.1. zkSync

zkSync's is a zk-SNARK based L2 payment protocol on Ethereum. dApps that integrate with zkSync can offer their users transfers with instant confirmations, ultra-low fees ($0.001/tx) while still having full mainnet-level security.

4.3.1.2. An optimistic competitor?

Recently, Curve announced it would explore zkSync as an L2 solution due to zk-Sync offering a better all-round solution compared to OR if zkSync can offer smart contracts in their protocol[16]. This seems likely with technological breakthroughs throughout 2020 that have enabled zk-rollup based smart contracts[17]. Over time, the Matter Labs team have worked to include smart contract integration on the zkSync protocol allowing for a wider spectrum of use cases such as AMMs. A potential issue here is that it will require developers to become familiar with a new language (Zinc) but the team has confirmed there will be crossover with programming with Solidity.

Like all current zk-rollup solutions, zkSync also operates with a single centralized provider who generates the zero-knowledge proofs for blocks. Matter Labs is looking to decentralise the protocol by introducing a new consensus mechanism for block construction.[18] This can help eliminate some of the drawbacks with having a single, centralized operator while also maintaining its advantages at providing on-chain data availability and fast withdrawal times to L1.

zkSync summary - zkSync could be an attractive investable opportunity at some point in the future when the network's operation is decentralized and put to test in the wild.

4.3.2. Loopring

Loopring is also a zk-sidechain to Ethereum that uses zk-SNARKs that focuses solely on exchanges and payments. The Loopring protocol essentially provides a platform for developers to build zk-SNARK DEXs.

The Loopring protocol ensures that a DEX owner can provide a single proof that their users' trades are settled, their balances are correct, and deposit/withdrawals have been processed. DEX owners do not have to execute these through smart contracts but rather provide a small proof that ensures users the DEX is telling the truth. Loopring DEX operators have real world prover costs. DEX owners have an incentive to batch as many transactions in a block as possible (the upper limit currently being 1024). This is due to gas costs per transaction being lower when blocks are filled to their capacity. Therefore, Loopring's needs to be efficient but can only do this with increased adoption.

---

[16] Curve + zkSync L2: Ethereum's first user-defined ZK rollup smart contract!
[17] Zinc Programming Language Used For Smart Contract for zkSync
[18] Introducing zkSync: the missing link to mass adoption of Ethereum

4.3.2.1. Siloed liquidity

The hurdle rate to onboard assets onto Loopring's chain can be much lower than the total fees incurred by users frequently swapping assets on-chain. Once users move over to the Loopring protocol, they then face no transaction costs. The problem here is that liquidity is effectively siloed meaning capital cannot be put to work in DeFi without moving assets back onto layer 1.

4.3.2.2. Value Accrual

Loopring's native cryptoasset, LRC, is a staking token which:

- Gives users access to 70% of the Loopring protocol fees (~0.06% of every trade)
- Allows DEXs to operate (250k LRC w/ on-chain data availability, 1M LRC w/o on-chain data availability)

LRC is a capital asset where its value accrual is driven by the Loopring's ability to attract liquidity and trading volume that occur on the protocol. Since launching, the Loopring exchange has only had ~$400k in daily volume and $20m in deposits. This gives Loopring a fair value of $0.011 which suggests an 14x overvaluation at current market value.

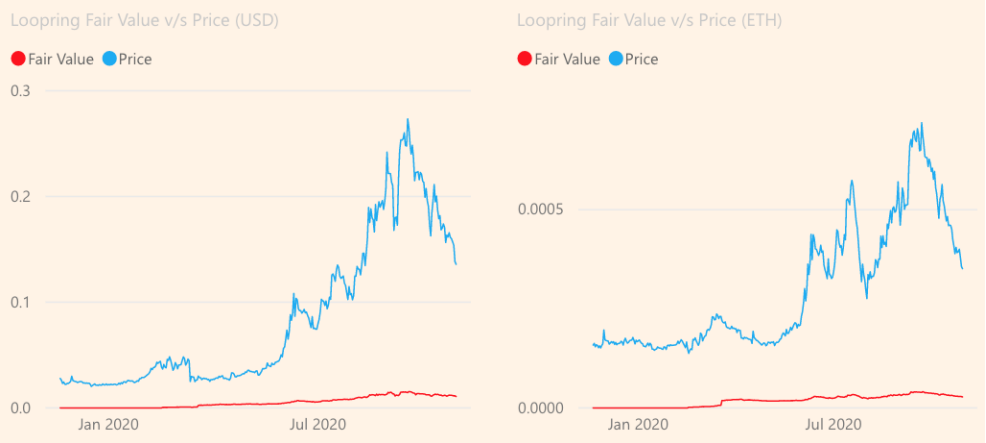

Figure 12: Loopring's APT vs price

4.3.2.3. Strengths

- High frequency traders can dramatically reduce their overall gas costs despite incurring costs from L2 account and deposit setups

4.3.2.4 Weaknesses

- Loopring's LRC token is hard to justify when other L2 exchanges are able to utilise other scaling solutions without the introduction of a token for security
- An awkward dynamic is introduced whereby DEXs built on Loopring have real world prover/operational overhead. They strongly rely on the protocol adoption in order to keep afloat which has been limited to date

- Loopring composability with Ethereum (and thus DeFi) is still a large problem. Loopring has introduced an operator solution which can mediate on-chain/off-chain interactions but requires an operator to store enough funds in his on-chain wallet in order to front assets on-chain. Furthermore, moving funds between both wallets is still slow (5-10 minutes)
- Loopring only has one exchange on the protocol (i.e. Loopring exchange)
- Other DEXs are looking to implement their own scaling solutions such as Uniswap for v3 which may dilute Loopring's value proposition
- The number of new users for the Loopring Exchange has kept flat (~30 new user/day)
- Loopring's LRC market price is above its fair value calculation

Loopring summary *- Loopring has failed to attract meaningful liquidity since Loopring's exchange launch at the start of 2020 with composability issues being a core reason for this. Lack of fundamentals and higher market prices means* LRC is also overvalued relative to its fair value.

Part 5: Plasma Sidechain Projects

Plasma Sidechains		
Project name:	**OMG Network**	**Matic Network**
Issuer:	OMG	MATIC
Symbol:	OMG	MATIC
Type	Staking	Staking
Transaction Asset	OMG (volatile)	MATIC (volatile)
Utility	ERC-20 & ETH. No smart contracts or NFTs	ERC-20, ETH, ERC721, ERC1155, Smart Contracts
Cost/Speed	3X cheaper / 100x faster than Ethereum	$0.000011 / 7000 TPS reported
Interoperability	Plasma Bridge	Plasma Bridge & PoS Bridge
Staking	2 weeks Exit Games	21 day waiting period, no minimums
Production	Mainnet Beta June 2020	Mainnet Beta September 2020
Initial distribution	98M	3.2B
Current supply	140M	3.8B
Max supply	140M	N/A
Market Cap	$510M	$66M

4.4.1. OMG Network

OMG goal is to support exchanges and wallet providers for cheaper, faster, value transfers. As a plasma sidechain, the OMG network batches transactions before committing them to the root chain

(i.e. Ethereum). OMG utilises a proof-of-authority (POA) consensus mechanism to bundle transactions together and submit the root hash to the parent chain. In contrast to ZK implementations such as Loopring, OMG relies on fraud proofs meaning the state transitions are assumed to be correct until otherwise.

OMG network's architecture has been optimised for payments. Specifically, Plasma uses MoreViable Plasma which allows for Fungibility of assets (necessary for payments use case) and eliminates the need for confirmation signatures (all transactions are considered valid by default). Bringing this full circle, OMG Network is hoping that centralized exchanges move their settlement layer onto the network while keeping their order matching centralized (as it scales much more easily). In other words, settlements can be made on L2 and then pushed to L1 for finality giving users the benefits of a DEX without time delays

4.4.1.1. A fast, but centralized operation

The current version of the network implements a Proof-of-Authority (PoA) as the consensus mechanism using a single operator within its consensus mechanism (the OMG team's node). Soon, OMG Network will transition to a Proof-of-Guarantee design whereby 'watchers' will be economically incentivised to oversee the transactions processed by the single node operator This design allows for faster value transfers by concentrating the number of block producers needed while also maintaining a level of decentralisation. It also means that the gas costs for nodes submitting blocks to the root chain is only limited to the single OMG node.

4.4.1.2. Value Accrual

The OMG token serves two main purposes with the OMG network:

1) Staking - Holding OMG gives users the right to run validator nodes on OMG's PoS network, using their tokens as a security deposit. By staking, OMG holders have the right to a claim on transaction fees that are distributed proportionally to the number of tokens staked.
2) Payments - It is the cryptoasset that is used to pay transaction fees. OMG will move from a fixed fee (currently set at 0.1806 OMG) to a dynamically adjusted fee based on one-third of the ETH gas fee.

Eventually there will be support for multiple fee tokens but it is unclear at this point when this will be (e.g. ETH, DAI). Therefore, OMG is predominantly a capital asset where its value is backed by the value of the transactions flowing through the network. It is clear that the OMG network still has a long way to go in terms of adoption. As of the 30th September, there has only been a total of 8,818 transactions[19]. While the OMG network has only been live since June 2020, it is incredibly important for OMG holders (and its underlying value) that it can attract real-world businesses onto the network in order to throttle throughput.

An OMG rewards calculator can be constructed based on certain parameter assumptions. The two main drivers in determining fees are the volume of transactions as well as the percentage fee. For OMG to have any value, the OMG network needs a sufficiently high transaction throughput which

[19] OMG Network explorer

can help boost transaction fees funnelled to watchers (OMG stakers) via the central operator. However, current usage seems low overall that makes it hard to justify its high market cap of $500m.

OMG network made headlines in August when it was announced that Tether would migrate USDT to the plasma chain.[20] It seems the total USDT moved was 3m but little is known about how that is being used.[21] It is also unclear as to how much value is currently locked on the OMG Network from Ethereum so a fair price of OMG based on total value locked (TVL) is challenging.

4.4.1.3. Strengths

- Fraud proofs are not needed for every state transition (only when they are challenged) which means they require fewer computational resources
- OMG finality runs in parallel to the layer 1 chain (Ethereum) meaning improvements in Ethereum's block times for 2.0 are also carried over to OMG
- There has been some interest from exchanges including Bitfinex (USDT) which has transferred over 3M USDT to the OMG chain and with continued testing we might start seeing this increase

4.4.1.4. Weaknesses

- OMG only supports the transfer of ETH and ERC-20 tokens so it only really caters for payment use cases but struggles beyond that
- Fraud proofs by definition view state transitions as correct until a party claims fraud. This brings in a necessary interaction between parties but also the party claiming fraud to be online (liveness). The interpretation of silence to implicitly mean consent is risky as an attacker can create the perception of silence with DDoS attacks.
- Users face potentially poor UX due to the standard exit games required when withdrawing assets back to the parent chain
- Smart contract services would have to continue to run on Layer 1 as there is not native smart contract support on the OMG chain

OMG summary *- OMG Network will only be able to compete in the payments sector. However, it does not have the best cost optimisation for users and it may not have a strong enough USP for the token to accrue significant value.*

4.4.2. Matic Network

Matic Network is an off-chain EVM-compatible set of sidechains with PoS consensus. Matic network is currently only deployed to Ethereum but, over time, is looking to be deployed to multiple chains (effectively representing a horizontal play).

Matic aims to build a dApp developer ecosystem with a focus on financial and gaming applications . By being EVM compatible means that Ethereum DeFi dApps that already exist on the main chain can

[20] Tether Integration Now Live on OMG Network
[21] Tether migration on OMG Network explorer

easily migrate over to the Matic plasma sidechain, potentially throttling the network's adoption. Matic has two main layers in its design:

- **Block Production (BP) layer** - Block producers follow a PoS consensus with a block producer being selected via Tendermint weighted round-robin algorithm
- **Checkpointing layer** - placed on top of the BP layer in order to detect fraudulent activity similar to fisherman in Polkadot

Matic Network uses fraud proofs (called checkpointing) to batch multiple sidechain blocks. These are then published to the Ethereum mainchain using the PoS layer. In the event of both the block producer and checkpointers both colluding, the submitted fraudulent proofs on the main chain can be challenged. If the challenge is successful, colluding parties are heavily penalized (stakes are slashed) while the challenger is rewarded (with the slashed staked of the validators). This increases security but the clear tradeoff here is that exit windows become necessary (up to 1 week). The Matic team seems to be addressing this issue by leveraging Nuo's reserve to act as a credit line but this has yet to be tested in the wild.[22]

In order to minimise any friction for users, the underlying MATIC token that is used to pay for network fees (consensus) should be abstracted away. It seems like MATIC is doing just this by forcing dApps to maintain a reserve of MATIC tokens with liquidity providers. However, this puts the burden on dApps to ensure they provide sufficient levels of liquidity and it is not clear how this is done from an operational perspective.

In July, Matic Network announced their Build-n-Earn Developer Programme designed to encourage developers to create the best possible version of their dApps on Matic Network. As of October 28th, the network has a mixture of ~25 dApps deployed but analysis on Dapp Radar shows that DAUs and volume traded is small. It is clear that the network is still in its infancy.

4.4.2.1. Value Accrual

The MATIC token has 2 main purposes within the Matic Network:

1) Staking token - Validators stake MATIC to participate in the PoS consensus
2) Transaction Fee - Transactions fees on Matic sidechains are paid in MATIC tokens

The Matic token will accrue value as more users are onboarded to use the dApps deployed on Matic Network. As more users transact, the more transaction volume and hence transaction fees that are distributed to validators. Cumulative transaction count has surpassed 632k which is promising but little data is public regarding transaction volume meaning insight into fee dynamics is challenging. An alternative valuation metric could measure the TVL in Matic Network as a proxy for chain utilisation.

4.4.2.2. Is a Matic gaming ecosystem developing?

Two main asset buckets that we can analyse are stablecoins (as a proxy measure for payments use case growth) and gaming-based tokens (as a proxy measure for gaming use case growth). The number of dollar-pegged stablecoins (DAI and USDT) that were locked in the bridge contract spiked

[22] Matic and Nuo partnership

at the start of October (3.3m and 2.6m respectively) but has sharply declined since. This temporary surge is likely a result of developers building/testing their dApps during one of Matic's incentivised developer programs.

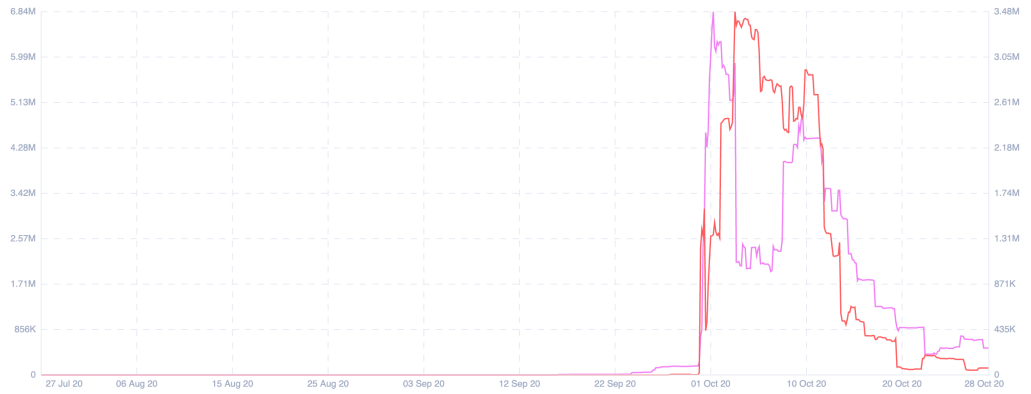

Figure 13: Stablecoins DAI (LHS) and USDT (RHS) locked in Matic Network's bridge contract address.

Taking the two most popular gaming tokens locked in the bridge contract shows a very different pattern. Decentraland's MANA token and Chain Games' CHAIN token have equally spiked but, unlike the stablecoins, there has been little withdrawal activity back onto Ethereum.

Figure 14: Gaming tokens CHAIN (LHS) and MANA (RHS) locked in Matic Network's bridge contract address.

An interesting analysis would be to determine the stickiness of certain assets as well as dApp activity in Matic as an indicator as to what type of use cases Matic is catering for most. Clearly, further data points are needed to make any strong conclusions but MATIC is starting to gravitate more towards the gaming sector. Solutions like Matic can offer a generalized platform for gaming developers who are seeking near-instant transactions, low fees, above strong trust assurances.

4.4.2.3. Strengths

- Matic uses EVM-compatible runtime known as Matic VM meaning it will be relatively easy for Ethereum dApps to migrate over
- Supports both fungible and non-fungible tokens allowing for MATIC to go after gaming and finance markets

- Can be used in conjunction with Celer to provide a holistic solution for scaling dApps – Celer's C channels integrating Matic sidechains
- Users do not have to open channels in order to use the network – just an Ethereum address
- POS bridge will be be effective at reducing the withdrawal time for users but may tradeoff security to accomplish this

4.4.2.4. Weaknesses

- There is only one public chain but it is unclear how quickly dApp demand will warrant further public MATIC chains to run in parallel. Interchain communication is then required for dApps selected by different MATIC chains to deploy their smart contracts
- Exit times from the sidechain to the mainchain continue to be a key problem for existing plasma implementations - using Nuo may be necessary but it arguably adds reliance risk and it's not clear how whether Nuo's reserve pool will be able to keep up with intense exit demand down the line
- Cost for checkpoint submissions goes up with ETH price unless checkpoint costs are changed regularly

MATIC summary *- Matic could quickly emerge as the de facto gaming-centric L2 platform, rather than DeFi. From an investment point of view, MATIC will accrue value as more dApps facilitate more network fees. MATIC is likely overvalued at current market prices but continued interest from gaming developers may signal a buy opportunity at lower levels.*

Part 6: Relative Valuations Analysis

The DPC fundamental relative valuation tool was used to compare tokenised L2 solutions across 5 distinct categories (market,tech, people, community, strategy). A score is calculated within each category and aggregated into a final score (equally weighted). Note that SKALE is excluded due to the SKL token not circulating yet. The analysis shows that xDAI leads the pack (57.7%) with Matic Network in at second (55.8%). The first takeaway here is that some of the highest scoring projects have some of the lowest market cap in this list, while some of the lowest scoring projects like OMG and Loopring have the highest valuations.

	100%		20%	20%	20%	20%	20%
Project	Total Score	Marketcap	Market Score	Tech Score	People Score	Community Score	Strategy Score
xDai	57.69%	$28,970,863	62%	15%	64%	54%	93%
Matic Network	55.78%	$61,783,046	57%	41%	67%	51%	63%
Celer	45.35%	$14,603,967	23%	38%	64%	39%	63%
OMG	44.34%	$415,785,049	60%	28%	68%	40%	27%
Raiden Network	42.38%	$7,918,494	26%	36%	68%	26%	57%
Loopring	39.17%	$147,524,948	52%	22%	38%	34%	50%
IDEX	36.48%	$27,380,871	42%	22%	44%	22%	53%
Loom Network	34.49%	$17,701,660	41%	10%	40%	33%	50%

Figure 15: Relative valuations of tokenised L2 solutions as of October 29th.

xDAI's greatest area of weakness was its developer activity (a score indexed by Santiment). While xDAI's tech score is low relative to other networks like Matic, it is reassuring to see developer activity generally trending up overall throughout 2020. Matic Network scored fairly consistently across the

categories. Lower ranked projects fell noticeably lower in the tech and people with these projects unable to demonstrate clear developer activity growth or favourable team experience.

Part 7: The L2 Thesis

A game of tradeoffs

Diving deep into the types of L2 solutions shows that all possess some sort of tradeoff, whether this is scalability, security, or tooling. Second, L2 solutions are arguably still in their infancy with no single network showing very strong adoption today. However, an assessment of the *types* of L2 projects that will likely succeed can be made which could then be used to explain, at least in part, the lack of adoption for certain L2 projects as well as the relative valuations scores above.

The merit in generalized approaches

Generalized solutions that are able to provide flexible frameworks for a wide range of use cases will have a greater chance of success. Examples of generalized solutions would include SKALE, xDAI, Matic, and Optimism. This is because they often provide a general framework for developers to work with while also allowing for a certain level of composability within their own respective environments. For example, a dApp deployed on a generalized L2 chain can add value to other dApps deployed on the same chain.

More specialized L2 solutions, such as DeversiFi, will have a harder time achieving adoption because they remain isolated within the ecosystem and cannot offer functionality beyond their own single use case. The original value proposition of these specialized solutions may also be weakened if dApps start deploying their smart contracts on rollup chains to improve on scalability (e.g. DiversiFi vs Uniswap on a rollup).

State channels will likely play an important role in enabling instant micropayments between dApp users but TheGraph's integration into non-commercialized state channel networks is a meaningful signal. Increased adoption of these non-commercialized state channel networks by large players would arguably make their commercialized counterparts less attractive. We are also starting to see other L2 solutions that can facilitate micropayments while also natively supporting smart contract functionality. Networks like Celer, launched as a specialized platform but is now realising it has to broaden its horizons to offer a more generalized solution.

Blockchain agnostic or specific?

The question then becomes whether value will accrue to generalized solutions that are Ethereum-centric or blockchain agnostic. The answer is likely both but for different reasons.

Let's start with Ethereum-centric solutions. Right now, we are seeing growing momentum of dApps wanting to integrate with Optimism's or Arbirtrum's generalized rollup solution for Ethereum. If we start seeing key DeFi players like Synthetix and Uniswap porting over their smart contract then a single optimistic rollup chain might emerge, encouraging other dApps to follow suit. This would effectively form a single DeFi rollup that could end up dominating. In this scenario, there would not

be an L2 investable opportunity *per se* as the exposure would still be through the cryptoassets of the networks deployed on the rollup itself (i.e. SNX, UNI).

This is not to say there would only be one 'dominating DeFi rollup'. It is also reasonable to expect multiple rollups that will be underpinned by different technologies. For example, zkSync will likely be the zk-Rollup alternative to an optimistic-based solution where both exist in parallel to each other. Right now, it is unclear as to which rollup will be most preferred by dApps. Synthetix is the main ambassador for Optimism's rollup technology while Curve will likely be pushing the zkSync agenda forward.

Other 'bluechip' DeFi protocols are likely to provide more details as to how they intend to scale their system as part of major protocol upgrades (e.g. Uniswap V2 or Aave V2). Most DeFi protocols will be taking time to evaluate and test the generalized L2 solutions available before making any firm commitments. Broadly speaking, applications deployed on zkSync will do so because they view zk-Rollups as a superior technology to ORs from a UX perspective while applications choosing to deploy on Optimisms strive for easier EVM compatibility.

There are certain layer 2 networks that may launch their own native cryptoasset in the future. For example, zkSync could become an investable opportunity at some point in the future that we should consider if and when it decides to add a consensus layer (and therefore staking token) in order to remove its centralized operation.

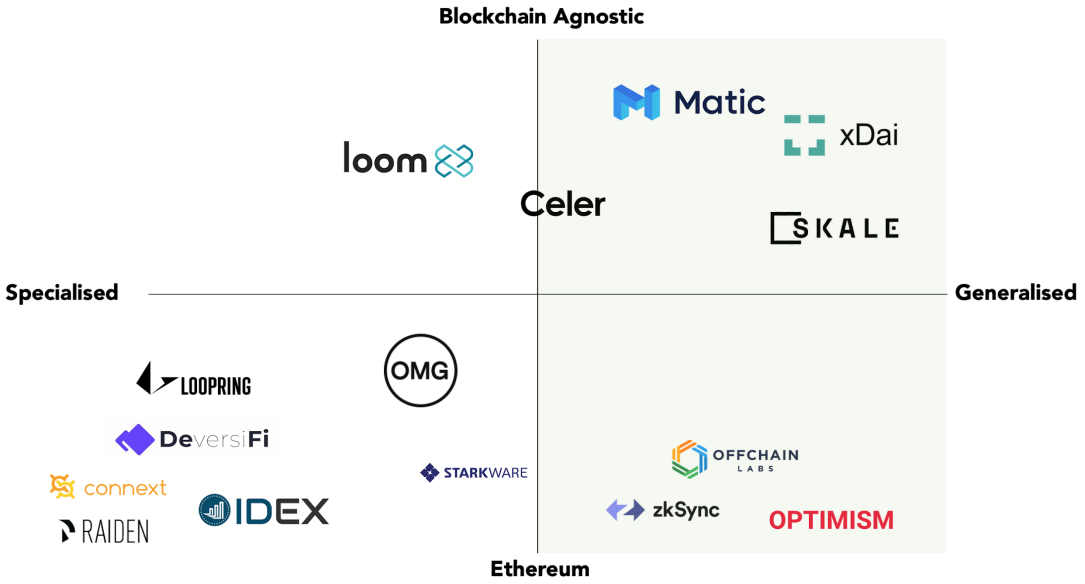

Figure 16: L2 projects on a generalized/specialized and Ethereum/Agnostic 2D plane. Green area represents areas most likely to see adoption.

In the short to mid term, it is likely that more dApps will deploy on Optimism despite the non-trivial drawbacks of fraud proof-based designs. For example, if Uniswap and Synthetix deploy their contracts on Optimism, there is a greater likelihood that other dApps do the same - they want to maintain composability with one another while also being able to achieve moderate scalability. As we've seen in the past, the driver of activity has rarely been the best technology but rather the network effects.

Over the long term, rollups will continue to play a significant (and non competitive) role in an ETH 2.0 world. If the Ethereum ecosystem is on the path to developing rollup technologies, Ethereum can offer its base layer for consensus and data availability and no more. The vast majority of EVM computation will be taken off the base layer and onto rollups operating within different shards. However, it is not clear as to whether these rollups will be zk-based or optimistic-based (or both!). Regardless of which technologies is chosen, the conviction lies in the idea that ETH will eventually become a rollup-centric network in time. Through this lens, bullish rollup adoption is bullish ETH 2.0.

More agnostic generalized solutions compete more directly with ETH 2.0 if they do not rely on Ethereum for finality. Matic, SKALE, and xDAI are the stand out solutions that have a chance of survival in this rollup-centric world for Ethereum. Each project has the ability to dominate different areas of the market by optimising *for* those markets. By definition, they all represent horizontal plays:

- **MATIC Network (medium conviction)** - provides a generalized platform for gamers that can optimise for seamless UX by trading off security assurances

- **SKALE (stronger conviction)** - provides a generalized platform for developers seeking to build highly configurable individual dApp chains

- **xDAI (medium conviction)** - provides a generalized platform primarily used for payments and NFTs by being the only stable payments chain.

Looking ahead

Matic Network's best chance of success will be to continue targeting gaming use cases. Matic Network can allow for the integration of optimistic rollups within their architecture for applications to use. Right now, Matic is overvalued to current activity and the market price will likely fall to meet its fair value. An ongoing analysis of valuation related on-chain activity such as TVL, staking, fees paid, as well as dApps deployed will be performed. Positive signals here would strengthen conviction around the Matic thesis at a time when market value might also be much lower.

For SKALE, it is unlikely that dApps Uniswap or Synthetix will migrate over to SKALE so the network's growth but that may not be detrimental - its stronger independence to Ethereum means attracting existing dominant dApps is not required for SKALE to fulfil its vision. SKALE's growth will instead stem from a wide range of scalable dApps built from the ground up that want to be easily composable with Ethereum. SKALE is in a good position for on-boarding these dApps by strategically provisioning Ethereum developer tooling and customisability. In the coming months, DPC can monitor key metrics (e.g. number of sidechains, node count, dApp fees) on an ongoing basis to evaluate the overall direction of the project.

For xDAI Chain, a lot of experimentation is likely yet to come both externally and internally - by dApps onboarding as well as xDAI transitioning into a fully permissionless network at the start of 2021. The most credible threat to xDAI Chain is its reliance on a peg-breaking stablecoin and its USP becoming obsolete in a rollup-centric ETH 2.0 world. For these reasons, the conviction of xDAI success is lower than SKALE.

Conclusion

The L2 landscape is still incredibly nascent with most L2 projects showing little tangible adoption. In the short-term, the battle between zk-Rollups and optimistic rollups will intensify as existing Ethereum dApps place different values on each of solutions' tradeoffs. During this time, market values for existing L2 networks will likely fall to meet their current fair values. However, in the mid-term, certain generalized L2 solutions like Matic Network, SKALE, and xDAI Chain will be able to uniquely position themselves as attractive platforms for users and dApps by optimising in different ways. Based on their token design, their ability to attract activity onto their respective chain will then directly drive value to each network's respective token.