DELPHI DIGITAL

Layer 2 Scaling on Ethereum

Thematic Insights

June 2019

85 Broad Street
New York, NY, 10004
www.delphidigital.io

Table of Contents

Analysts

Tom Shaughnessy
tom@delphidigital.io

Medio Demarco
medio@delphidigital.io

Executive Summary

In a recent report, we discussed how Bitcoin is scaling on Layer 2 through the Lightning Network. As a quick reminder, Layer 2 scaling solutions move on-chain, "Layer 1", transactions off-chain with the goal of improving speed, throughput and cost in a trust-minimized way. Lightning Network is a type of Layer 2 solution known as a Payment Channel, but there are other approaches under development as well such as State Channels, Sidechains, and Plasma Sidechains. Each has their own strengths and weaknesses.

While Bitcoin has some development going into these different areas (e.g. Blockstream's Liquid Sidechain), the primary focus of the developer community is scaling payments through Lightning Network, without materially changing the Layer 1 base blockchain.

Ethereum is a different story. Developers are working on Layer 1 scaling (e.g. Sharding) and a large variety of Layer 2 solutions. How the combination of both will look in a few years time is still an unknown, but their development is crucial for helping Ethereum maintain it's dominance relative to other smart contract platforms, and to support mass adoption.

Throughout this report, we'll focus on explaining the different types of Layer 2 solutions and analyze the projects building them. To the right, we've highlighted a few of the key projects spearheading this development in their respective categories. It's important to note, however, that this list is not exhaustive. As with all of our Insights posts, our goal is to make this complex topic easy to understand.

Payment & State Channels:

Raiden Network

Connext

Sidechains:

POA Network

SKALE

Plasma Sidechains:

Loom Network

Matic Network

Payment & State Channel Overview

DELPHI DIGITAL

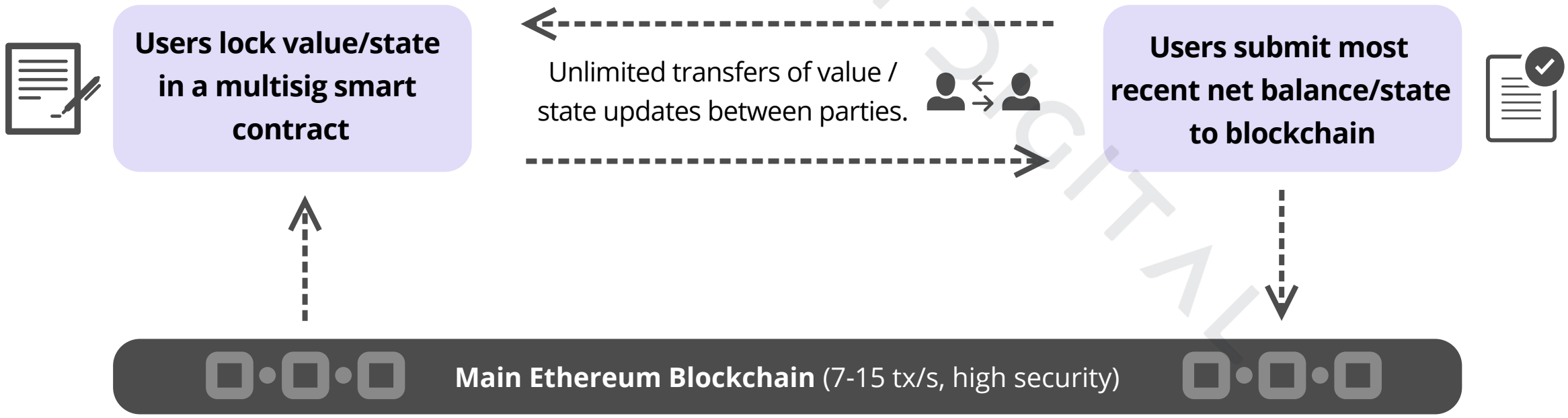
Payment Channels

- Two users, running node software, lock value (e.g. ETH) in a multisig smart contract on the blockchain. This opens a bi-directional payment channel between both of them.
- Transactions instantly update the balance of the payment channel without needing to involve the blockchain. The state of the channel balance is stored locally on the node.
- As more nodes come online, and more payment channels connect them, a peer-to-peer mesh network begins to form. This means that even if two nodes don't directly connect, they can still transact as payments are routed over the network of connected nodes.
- To settle, a user closes their payment channel, with the net balance finally being broadcast to the blockchain.

State Channels

- State channels are a more generalized version of payment channels in that they can handle any state transitions or interactions. They are not limited to value transfer like payment channels are.
- Users can lock up state in the channel, make near unlimited changes and eventually the users settle the channel and update their final state to the main chain.
- An example is playing chess through a state channel, making thousands of moves, and eventually closing to the main chain.

Simplified Two Party Payment/State Channel Diagram



Payment & State Channel Implementatons

DELPHI DIGITAL

Raiden Network

- Raiden Network was one of the first projects focused on scaling Ethereum and has been under development since 2015. Raiden is a payment channel implementation and currently has two phases of development: 1) µRaiden and 2) The Raiden Network.
- µRaiden ("Micro Raiden") is a simplified version currently live on the Mainnet. It facilitates trust-minimized instant transfers between two parties. µRaiden does not charge a transaction fee, and only opening/closing a payment channel incurs a GAS fee on Ethereum.
- µRaiden does not support multihop transfers, and therefore only allows users to transfer tokens in one direction to predetermined receivers.
- For development phase 2, the full realization of The Raiden Network, this limitation will be removed enabling multi-hop transfers through a network of bi-directional payment channels.
- Once Raiden Network is fully live it will charge two types of fees- 1) protocol level fees and 2) peripheral fees. Protocol fees will be paid to routing nodes and denominated in the token that is transferred in the channel. Peripheral fees will be payable to services that help the network operate and will be paid in RDN, Raiden's native token.
- The project is moving towards its next update, Ithaca, which aims to feature faster routing services, monitoring services to watch channels when users are offline, and the ability for users to earn fees by handling transfer through their own payment channels.
- Work on a light client has begun to allow users to interact with the network easily through consumer wallets (Metamask, status) and use the Raiden network to make token transfers using low end devices.

Connext

- Connext has a working implementation of its State Channels live on the Ethereum Mainnet.
- The current version (v1.0) has a single centralized hub, run by Connext, which allows transactions to be made in ETH or DAI. While Connext is the only entity routing transactions, the underlying protocol is non-custodial although there is trust required in its use. For example when using their Dai Card application, the hub can steal a user's payment value while a transaction is in-flight. In addition, if a user goes offline the hub is the only entity that persists their channel's state. This may help usability, because it allows for easy cross-device support, but it's bad in the event the hub goes down and a user needs to recover their funds. When taking both of these factors into account, using the current deployment of Connext in any meaningful way is a risk.
- In the future (v2.0), Connext will become decentralized allowing multihop payments to be routed across a network of nodes. It will also support generalized state changes and interoperate with Counterfactual's framework. v2.0 will allow transactions to be made in any Ethereum ERC-20 token.
- Connext does not have it's own token and the network does not collect any fees. Nodes that route transactions and provide storage services may collect fees in the future if they choose to.
- Connext, Spankchain and Kyokan together received a $420k from the Ethereum Foundation in October 2018 to build a non-custodial payment channel hub.
- There are a number of DApps/wallets already using their State Channels including Spankchain, Mosendo, Provide Payments, and Ujo.

Sources:

Sidechains & Plasma Overview

DELPHI DIGITAL

Sidechains

- A side chain is a distinct and separate blockchain that is attached to the main blockchain using a two-way peg.
- Value (ETH) is locked on the main Ethereum blockchain and credited on the sidechain. Users can than interact with this value off-chain and eventually move it back to the Mainchain.
- Starting a sidechain requires the creation of an entirely new blockchain, with its own consensus mechanisms and security guarantees. While transactions can be faster/cheaper due to trade-offs made with the consensus mechanism, the security will be weaker as well.

Plasma Sidechains

- Plasma implementations are similar to sidechains in that a child blockchain is created that is tied to the parent.
- The major difference is that the root of each plasma block is published to the main Ethereum blockchain. This essentially compresses the transactions that occur on the plasma sidechain and records them back on the mainchain. This offers much greater security guarantees over standard sidechains given that users can prove their ownership/transaction history.
- Sidechain users are entirely dependent on the security of the sidechain itself. Plasma sidechains can use weaker consensus mechanisms (POA) for higher throughput while still benefiting from better security guarantees.

Main Ethereum Blockchain (7-15 tx/s, high security)

Side Chains

Users lock assets in a smart contract on the Mainchain

Dependent on consensus mechanism

1-1 assets created on side chain. Users can transfer within side chain. Security dependent on side chain's consensus algorithm.

Plasma

Users lock assets in a smart contract on the Mainchain

Not dependent on consensus mechanism - can fall back to Mainchain

Assets are created on the plasma chain but security is not completely dependent on the plasma chain's consensus algorithm - can rely on the Mainchain

Sources: Vasa, Eric Olszewski, Plasma Group

Sidechain Implementations

POA Network

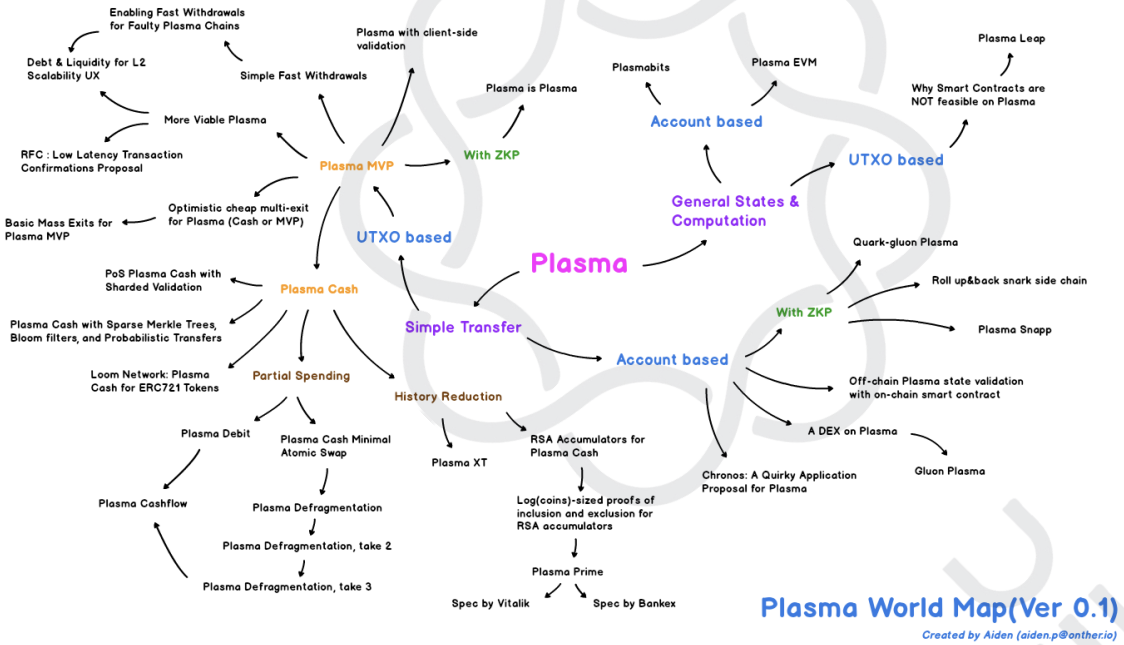
- POA Network is a suite of sidechain based solutions that are compatible with Ethereum.
- POA Network's Core Chain implements a Proof-of-Authority ("POA") consensus mechanism where only US public notaries can act as validators. Unlike Proof-of-Stake systems where validators are incentivized to act appropriately, or risk losing their locked up capital, with POA the validators have their identities at stake, creating personal accountability. Adding or removing validators is done through an on-chain vote. The Core Chain is live and has a number of DApps currently running on it, which can be seen here.
- POA's TokenBridge connects Ethereum to the Core Chain and was the first live cross-chain bridge. It launched in May 2018. It can facilitate token transfers between any two EVM (Ethereum Virtual Machine) based chains.
- POA20 is an ERC-20 token that represents POA Network tokens on Ethereum. POA native coins are transformed into POA20s through the TokenBridge.
- Despite it's name, POA Network is starting a transition away from Proof-of-Authority and towards a Delegated Proof-of-Stake consensus model. This started with the new xDai Stable Chain, which will be one of the first networks to implement their new staking consensus mechanism called xDai DPOS.
- An interesting aspect to point out is that this new chain will have two tokens. xDai, which is pegged to the Dai stablecoin, will act as the transactional currency, while the new DPOS token is dedicated solely for staking.
- Initially DPOS staking will take place on the xDai Stable Chain but will be used to stake others in the future once they are launched.
- Existing POA token holders will have the option to participate in DPOS reward distribution incentives, however, the details are still being determined.

Skale

- SKALE, a highly modular and configurable execution layer, is a network of Elastic Sidechains run by independent validators. Each validator node contains a number of "Virtualized Subnodes", allowing them to validate multiple Elastic Sidechains at the same time. This differs from most other sidechain implementations, where a node typically only validates a single sidechain.
- A weakness for sidechains is that they're only as secure as their validators/consensus. To prevent collusion, validating nodes are randomly shuffled similar to how shard validators will work in ETH2.0. To further disincentivize bad actors, nodes stake collateral, in the form of SKALE utility tokens, on the Ethereum Mainnet and are rewarded/penalized based on their behavior.
- Communicating between various layer 2 solutions, and even layer 1 shards, is largely still an unsolved challenge. However, SKALE's communication layer connects each Elastic Sidechain, allowing users to transfer digital assets and call smart contracts across them.
- Data availability is a common problem for layer 2 solutions and SKALE has it's own proposed solution, which can be read about more here.
- The consensus mechanism is called SKALE Parallel Asynchronous Consensus (SPAC), and is based on a variant of Asynchronous Byzantine Binary Agreement. It's designed to guarantee finality and does not fork. Elastic Sidechains can tolerate < ⅓ nodes acting malevolently or going offline before halting.
- SKALE DevNet went live in February 2019, with the Mainnet launch expected in Q3 2019.
- SKALE raised $9.65 million in funding, comprised of a $8.86 million Simple Agreement For Future Tokens (SAFT) in October 2018 and a $785,000 seed SAFT raised earlier that year. Investors include Multicoin Capital, Boost.VC, Canaan Venture Partners, Galaxy Digital, among others.
- SKALE Storage is also an alternative to using IPFS. It's a trust-minimized, cost-effective storage layer capable of handling files up to 100MB.
- Deploying Solidity smart contracts to an Elastic Sidechain is a simple process for developers, requiring them to only change 2 lines of code.
- SKALE does not currently implement Plasma but may in the future when the technology matures.

Sources:

The Many Forms of Plasma



The term Plasma is often thrown around as if it were a single solution, but it's actually an umbrella term that describes a broad category of different solutions, each with their own use cases and trade-offs. To the right, we've highlighted a few of the more popular Plasma variants being used by different projects today.

Recently there has been development progress made such as LeapDAO implementing DAI transfers on their Plasma Leap chain, OmiseGO releasing the alpha of its Plasma MoreVP and Loom expanding the capabilities of its Plasma Chain. However, despite these advancements in research and development, Plasma is still an immature, albeit promising, technology. In the near-term, we believe it's likely that channels and sidechains gain more traction barring a new research breakthrough.

Plasma MVP

- Plasma MVP is a simple form of plasma that has a UTXO based model. It supports high throughput payments but not more complicated transactions
- Plasma MVP relies on an operator that is a single entity which runs the entire plasma chain, as such it relies on POA consensus or Proof-of-Authority. Blocks on the plasma chain are composted of sets of transactions which is turned into a Merkle Tree. The root of this tree is published as a commitment to the Ethereum blockchain for security.
- More Viable Plasma was created to remove confirmation signatures for a faster and less storage intensive process.

Plasma Cash

- Plasma Cash is a design focused on storing and transferring non-fungible tokens (NFT). It was built to address the potential mass-exit issue of Plasma MVP. Each deposit to Plasma Cash is represented as a NFT. I.e. If a user deposits 100 ETH, they receive one token on the plasma chain worth 100 ETH.
- Plasma Cash is scalable as users only have to keep track of their own tokens, although each transaction requires a proof that goes all the way back to the block a token was created with, so these proofs can grow prohibitively large.
- It has difficulty dealing with divisible, fungible tokens, however.

Plasma Debit

- Plasma Debit is similar to Plasma Cash except each token is a payment channel between the user and the chain operator. This works best if the channel is linked with an operator vs. everyone opening channels between each other.
- For Plasma Debit to work, the user you wish to interact with must have a channel open with the hub and have enough funds within the channel to make sure the transfer can be completed.

Source: Ethresearch Plasma World Map, Learn Plasma

Plasma Sidechain Implementations

DELPHI DIGITAL

Loom Network

Full Report Available

- Loom Network allows developers to build DApp specific Plasma Sidechains on top of Ethereum. These sidechains can be optimized for a specific use case (e.g. gaming vs social media), with developers able to choose certain features, such as their consensus mechanism (the default is DPoS).
- LOOM is its token and, while it has various uses within their ecosystem, it's primarily for staking/delegating their sidechains.
- The development team has already deployed their own sidechains (PlasmaChain, GameChain & SocialChain) for third-parties to begin building on. PlasmaChain is their main sidechain, which they expect developers to build "Layer 3" sidechains on top of. Staking on PlasmaChain has been live since February 2019.
- Loom's PlasmaChain implements certain aspects of Plasma Cash, which Georgios Konstantopoulos developed to solve for the problems other Plasma variants had. However, it's important to point out that Plasma Cash is still lacking in certain regards.
- As a result, while PlasmaChain is using a version of Plasma Cash currently, it's not operating on a fully plasma based model. For example, Loom is currently using a "Transfer Gateway" to link the PlasmaChain to Ethereum due to the problems Plasma has with user exits. With this Transfer Gateway in use, it operates more like a standard sidechain rather than a full Plasma implementation.
- To solve for some of the problems Plasma Cash has with fungible tokens, Loom's team has developed a prototype implementation of Plasma Debit and has researched Plasma Flow.
- Loom's goal is to become a universal layer 2 hub and has announced plans to bridge Ethereum to Tron, EOS and Cosmos. As of June 2019, PlasmaChain is now interoperable with Tron.

Matic Network

- Matic Network uses sidechains for off-chain computation, the plasma framework for security and Proof-of-Stake consensus built on top of Tendermint. Ethereum is the first blockchain it will support but additional chains in the future to create an interoperable L2.
- Matic Plasma is similar to Plasma MoreVP, but it's an account-based variant compared to other UTXO-based implementations.
- Matic has deployed testnets on Ethereum's Ropsten and Kovan networks. Matic's alpha-Mainnet is expected to launch this month, with the beta-mainnet planned for Q3 2019. It's important to note, that staking MATIC tokens will not be available in the alpha-Mainnet, but will be in a future release.
- MATIC is their token which was sold through a Binance IEO in April 2019.
- Coinbase Ventures invested in the seed round. As a result, Coinbase Wallet will help users move their assets from Ethereum to Matic. Once the user's assets are on Matic, they will be able to transfer and trade them on Coinbase Wallet instantly. Users can use DApps built on Matic directly on Coinbase Wallet's browser or can use WalletConnect to access them through Matic Wallet.
- Prominent DApps such as Decentraland are working with Matic.
- Faster exits from the sidechain to the mainchain are an outstanding problem for existing plasma implementations. Matic is working with Nuo Network to solve this. At a high-level, when a user wants to exit from a Matic sidechain an NFT is minted representing their tokens which is then posted to Nuo as collateral. Nuo checks the validity of the NFT and releases the tokens represented by the NFT to the user on the mainchain. The token's come from Nuo's reserve pool and a small exit fee is charged to the user. After the challenge period, the NFT is redeemed and the tokens inside are credited to Nuo's reserves.

Sources:

Scaling Strengths & Weaknesses

DELPHI DIGITAL

Payment & State Channels

Strengths / Takeaways

- Tokens are locked in a multisig smart contract on the Mainchain. This creates a payment channel between two parties and provides it with liquidity.
- Very high throughput relative to the Mainchain. Channels can facilitate unlimited instant payments/state updates.
- Good privacy given that the transaction history is not publicly recorded on the Mainchain, only the net result is when the channel is closed.
- Very low to no fee transactions in channel.

Weaknesses

- Users need to stay online in order to maintain a record of their channels most recent state. Otherwise, a channel counterparty could potentially cheat them out of funds by submitting an older record of the state back to the blockchain, which is more beneficial to them. Watchtower services can help mitigate this by backing up a copy of a user's state to contest disputes on their behalf if they fall offline for a small fee (e.g. PISA).
- Routing multihop payments can still be a challenge.

Sidechains

Strengths / Takeaways

- Sidechains are independent blockchains bridged to the Mainchain through a two-way asset peg. Tokens are locked up on the Mainchain and then credited on the Sidechain.
- PoA, DPoS and PoS are common consensus mechanisms.
- Users don't always have to be online.
- Unlike payment/state channels, each new participant can use the existing sidechain rather than have to create a new channel.
- While it varies by the consensus mechanism, they offer high throughput and lower fees.

Weaknesses

- Validators of the sidechain can collude to censor or steal user funds from the sidechain. While the Mainchain may remain secure, a user's funds on a Sidechain are only as safe as the validators/consensus mechanism.
- Unlike the privacy a payment/state channel offers, every transaction is published on the sidechain.

Plasma Sidechains

Strengths / Takeaways

- Transactions that occur on a Plasma Sidechain are compressed into a hash which, is periodically submitted to the Mainchain. This provides better security for the user relative to a standard Sidechain. Plasma sidechains can use weaker consensus mechanisms (POA) for higher throughput while still benefiting from better security guarantees.
- In the future, it could allow for nested sidechains further improving scalability.

Weaknesses

- While weaknesses vary depending on the exact Plasma variant, exits from the Plasma Sidechain to the Mainchain are a common problem. They typically require a challenge period which currently can take 7-14 days.
- Plasma also requires that users maintain a record of the entire transaction history, including blocks where their funds weren't transferred, to prevent cheating. However, this record can be reset once the hashed state of the Sidechain is submitted to the Mainchain.

Leader Commentary

Below, we've included exclusive commentary regarding Layer-2 from leaders in the space, on where they see the true value from Layer-2 scaling and the major issues with the tech.

Georgios Konstantopoulos
Plasma Researcher

"Plasma offers massive throughput increases and latency decreases while having equal security to Layer 1 vs sidechains which rely on an independent network of validators for the security of funds. Major issues (large collateral requirements for state channels unlike plasma, assets used on layer-2 are illiquid, users must monitor the chain for safety) persist, but are being actively researched and worked on”

Michael Cullinan
Head of Business Dev. at Loom

"No blockchain, no matter how scalable, will be able to handle all of the world’s dapps on a single chain. Since Layer 2 extends horizontally across many chains / channels, it allows for infinite scaling — and therefore becomes a necessity. That said, it’s more than just a technique for improving the TX throughput of a given base chain. Layer 2 also gives developers the space to experiment with things like governance and new consensus mechanisms without risking or compromising the base layer. Additionally, interoperability enables users to transact across multiple chains and then securely store their assets on their Layer 1 of choice. As Layer 2 opens up such new possibilities, we can move beyond current infrastructure limitations and start to optimize for very particular application use cases — all the while inheriting a strong degree of base layer security.”

Eric Olszewski
Author of Layer 2 Series

"What this community has failed to recognize time and time again is that users value convenience and low cost over security. Instead of finding a middle ground, we've opted for high security solutions that require so much effort on the part of the user that they hinder adoption. Plasma is a great example of this - a solution with no added trust assumptions but puts the onus of validating every transaction of the respective plasma chain on its users. Solutions to mitigate this are fraught with their own issues which makes me believe that using these for anything other than a payment bridge to a sidechain is a boondoggle. State channels offer greater promise but still fall victim to the same issues of plasma relating to "griefing". Sidechains are the logical conclusion of these layer two solutions, offering high configurability insofar as security and usability to meet the needs of each respective use case."

Disclosures

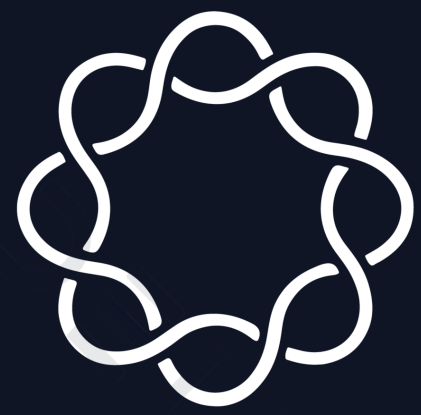
The Research Team may own the tokens represented in this report, and as such this should be seen as a disclosure of any potential conflict of interest. Anyone can contact Delphi Digital for full token disclosures by team member at Team@DelphiDigital.io. This report belongs to Delphi Digital, and represents the opinions of the Research Team.

Delphi Digital is not a FINRA registered broker-dealer or investment adviser and does not provide investment banking services. This report is not investment advice, it is strictly informational. Do not trade or invest in any tokens, companies or entities based solely upon this information. Any investment involves substantial risks, including, but not limited to, pricing volatility, inadequate liquidity, and the potential complete loss of principal. Investors should conduct independent due diligence, with assistance from professional financial, legal and tax experts, on topics discussed in this document and develop a stand-alone judgment of the relevant markets prior to making any investment decision.

Delphi Digital does not receive compensation from the companies, entities, or protocols they write about. The only fees Delphi Digital earns is through paying subscribers. Compensation is not received on any basis contingent upon communicating a positive opinion in this report. The authors were not hired by the covered entity to prepare this report. Delphi Digital did not receive compensation from the entities covered in this report for non-report services, such as presenting at author sponsored investor conferences, distributing press releases or other ancillary services. The entities covered in this report have not previously paid the author in cash or in stock for any research reports or other services. The covered entities in this report are not required to engage with Delphi Digital.

The Research Team has obtained all information herein from sources they believe to be accurate and reliable. However, such information is presented “as is,” without warranty of any kind – whether expressed or implied. All market prices, data and other information are not warranted as to completeness or accuracy, are based upon selected public market data, reflect prevailing conditions, and the Research Team’s views as of this date, all of which are accordingly subject to change without notice. Delphi Digital has no obligation to continue offering reports regarding this topic. Reports are prepared as of the date(s) indicated and may become unreliable because of subsequent market or economic circumstances. The graphs, charts and other visual aids are provided for informational purposes only. None of these graphs, charts or visual aids can and of themselves be used to make investment decisions. No representation is made that these will assist any person in making investment decisions and no graph, chart or other visual aid can capture all factors and variables required in making such decisions.

The information contained in this document may include, or incorporate by reference, forward-looking statements, which would include any statements that are not statements of historical fact. No representations or warranties are made as to the accuracy of such forward-looking statements. Any projections, forecasts and estimates contained in this document are necessarily speculative in nature and are based upon certain assumptions. These forward-looking statements may turn out to be wrong and can be affected by inaccurate assumptions or by known or unknown risks, uncertainties and other factors, most of which are beyond control. It can be expected that some or all of such forward-looking assumptions will not materialize or will vary significantly from actual results.



DELPHI DIGITAL

85 Broad Street
New York, NY, 10004
www.delphidigital.io