Blockchain scaling with layer 2: theory and practice

The internet was born as an instrument for radical self-expression. When the web was young, it was all about creativity and experimentation in a truly decentralized peer-to-peer fashion. However, over time it grew from a network of hobbyists into a multi-billion industry and gradually its great power was usurped by corporations, governments and large ISPs. Over three billion people use the internet monthly, although it’s just a handful of ISPs that serve the majority of the traffic in each country. The internet has grown to billions of websites, but most user activity is happening on Facebook, Google, Twitter and other major platforms.

### Scalability

The goal of any real blockchain technology is to bring freedom and true decentralization back to the people. Bitcoin does it for money and digital payments, Ethereum and the Web 3.0 paradigm for the Internet of Value and decentralized applications and so on. However, once you start digging deeper into the technology you will soon learn that everything has a cost. In blockchain, you can get decentralization and censorship-resistance, but always at a cost of scalability and speed. In fact, this phenomenon has a formal proof and is called DSC trilema or DCS Theorem (<https://arxiv.org/pdf/1801.04335.pdf>), which is just a special case of the more widely known CAP Theorem.

DCS Theorem states that one can achieve only two of the following three properties in a distributed system:

1. Decentralization: to what extent the system is resistant to the failure of its singular element and how much power or influence that element has.
2. Consensus: if decisions are made by a consensus or single-handedly.
3. Scale: if the system is able to serve a global market (for practical purposes this should be north of several 100s of thousands of transactions per second for a global network such as Bitcoin or Ethereum).

To practically achieve its goal of being decentralized, peer-to-peer, consensus-driven and trustless, any blockchain must choose (1) and (2) in this ‘trilemma’. This is why scalability, speed and throughput is an inherent problem for any public blockchain. This might sound like a dealbreaker but thanks to the concept of Second Layer networks on top of public blockchains, we can now enjoy almost unlimited scalability and preserve those very important properties of the base layer network. In this article we will examine some of the existing solutions and how they will help in bringing the power of blockchain into the hands of billions of users.

### Other existing issues

Similar to scalability, there’s another problem that is not being solved by most blockchains: privacy. The nature of consensus-driven distributed databases like Bitcoin and Ethereum is that they save all data and all user transactions from the beginning of time in a tamper-proof and immutable fashion. This is important for achieving decentralization but not necessarily good for personal or commercial privacy. Second layer scaling solutions are addressing this issue in a very elegant and native way.

Before diving deep into the analysis of existing solutions, it is worth noting that off-chain scaling is not the only option. For example, per DCS Theorem described above, one can achieve pretty good scaling by sacrificing the decentralization properties of blockchain. Such an approach is pioneered by DPoS blockchains, for example the EOS network. In EOS, the network nominates multiple witness nodes as representatives that help process transactions and smart contracts faster without polling the entire network.

Public blockchains are pretty much ideal examples of the network effect – high usage of the network attracts more applications, businesses and users. That’s why there won’t be too many base level blockchain at any point in time; rather, all usage will converge on a few of the most advanced, highly secure and widely used networks. Bitcoin for payments and money, Ethereum for dApps and trustless code execution. If we want to keep those networks secure, they must have some limit on the throughput. This is another reason for second layer scaling solutions to become main, and maybe the only way most people will interact with blockchain applications in future. The base layer will be reserved for the most sensitive and security-demanding transactions and for anchoring data from sidechains, state channels, payment networks, etc. Now let’s dive deep into second layer technologies and solutions that are available on the market at the moment.

### Classification of Layer 2 Solutions

Sidechains historically were the first proposal for how we can achieve almost unlimited scaling and good privacy, preserving the security of the base layer protocol. Liquid and RSK sidechains for Bitcoin, or Plasma for Ethereum, are some of the most advanced and market-ready implementations, though there’s many more projects in the working process. Sidechains allow users to lock some coins up on the main chain and in return get coins on the parallel chain with its own rules, consensus and much more flexibility on how the protocol is governed. Sidechains add throughput, flexibility and allow one to experiment with consensus rules.

A state channel is the approach where one completely reimagines the idea of trustless consensus between two parties. Instead of coming up with global consensus on a public network, we can use local consensus. In order to take advantage of state channels, one must create a payment channel with a node that’s connected to a larger network. Security in state channels is usually achieved by locking up some tokens on the main network and keeping them as collateral to ensure honest behavior.

Truebit is another approach that focuses on second layer scaling of blockchain computation (in contrast to blockchain payments). Truebit does not help to scale the number of transactions per second but allows the network to process more complex smart contracts and computations. This is achieved by basically “outsourcing” a computational task to an off-chain solver and then leveraging a game-theoretical algorithm in order to determine whether the result is correct.

### Plasma

Plasma is the sidechain implementation for Ethereum which is just a mainnet smart contract that takes care of all the rules and validation/governance on the Plasma chain.

Block validation on the sidechain is either done by a single operator or by a consensus of a much smaller set of validators than that of the base layer. This alone allows for the quickening of block frequency and number of maximum possible transactions in each block. Moreover, this will avoid the issue of block propagation and latency which is always the case for base layer blockchains, where the block must be accepted by tens of thousands of nodes around the world.

The main drawback and problem with this approach is that sidechains always introduce some degree of centralization. Developers of Plasma and RSK are very smart teams of experienced cryptographers and blockchain developers, so they try to make sure to preserve as much trustlessness as possible, but this is not always possible. The gateway that transfers Ether or Bitcoins is usually controlled by a single party and can be vulnerable to various attacks. Even though RSK’s federation of validators or a Plasma chain operator cannot necessarily steal user funds due to the protocol rules, they still can acquire transaction data, deanonymize users or withhold some information.

### Lightning Network

Lightning Network is probably the most well-known second layer payment network which is built for Bitcoin and Bitcoin-like blockchains (Decred, Litecoin). The idea of having a peer-to-peer network that consists of payment channels is almost as old as Bitcoin itself. Satoshi Nakamoto mentioned this approach in his comments on the BitcoinTalk forum when he was still active there in 2010. The Lightning Network utilizes the concept of payment channels to provide bi-directional monetary transfers, and envisions a network with near-instantaneous speed, zero counterparty risk, and low fees.

The main concept in LN is a payment channel that can be opened among any two users by including a special funding transaction in the underlying blockchain. Such a transaction is completed in a form of 2-of-2 multisig, meaning no party can single-handedly withdraw the money. To make sure that funds won’t be lost forever in the channel in the case of non-cooperation, or if the private key is lost, both sides sign each other’s transactions.

Once the channel is open and funded with some BTC, both parties can transact as fast as their peer-to-peer connection allows and pay no fees for doing so. Lightning transactions are completed in the form of cryptographic commitments. This allows for completely trustless payments: any party can close the channel and fix the outstanding trading balance on the Bitcoin blockchain at any time. In addition, LN ensures that it is impossible to cheat your trading partner by publishing an outdated commitment. This is done by having some lockup time on funds in the multisig. If Alice sees that Bob tries to cheat her by publishing some outdated state of their trading history (the one that is beneficial for him), she can simply provide proof in a form of a later commitment and free her funds from the multisig. Bob, in turn, will be punished for cheating by the protocol rules. It is the same general approach that Plasma uses to proof honesty on Plasma chain operators, though it is implemented in a different manner.

In most cases, both parties have an incentive to collaborate. In this case, the channel is closed with full cooperation by constructing a normal transaction from the original 2-of-2 escrow. This transaction would pay out the respective balance to each member, based off the most recent commitments. Neither individual has to go through the frictionary process of paying additional on-chain fees, nor lose out on the opportunity costs of time having their BTC locked up by the protocol.

The practical use-case of LN is not that every single user will publish an onchain transaction whenever they need to make a payment; rather it will work as an actual network. If Alice does not have a direct channel opened with Bob, she can always create a multihop transaction that will use several channels to reach its destination – pretty much the way internet or GSM routing works nowadays.

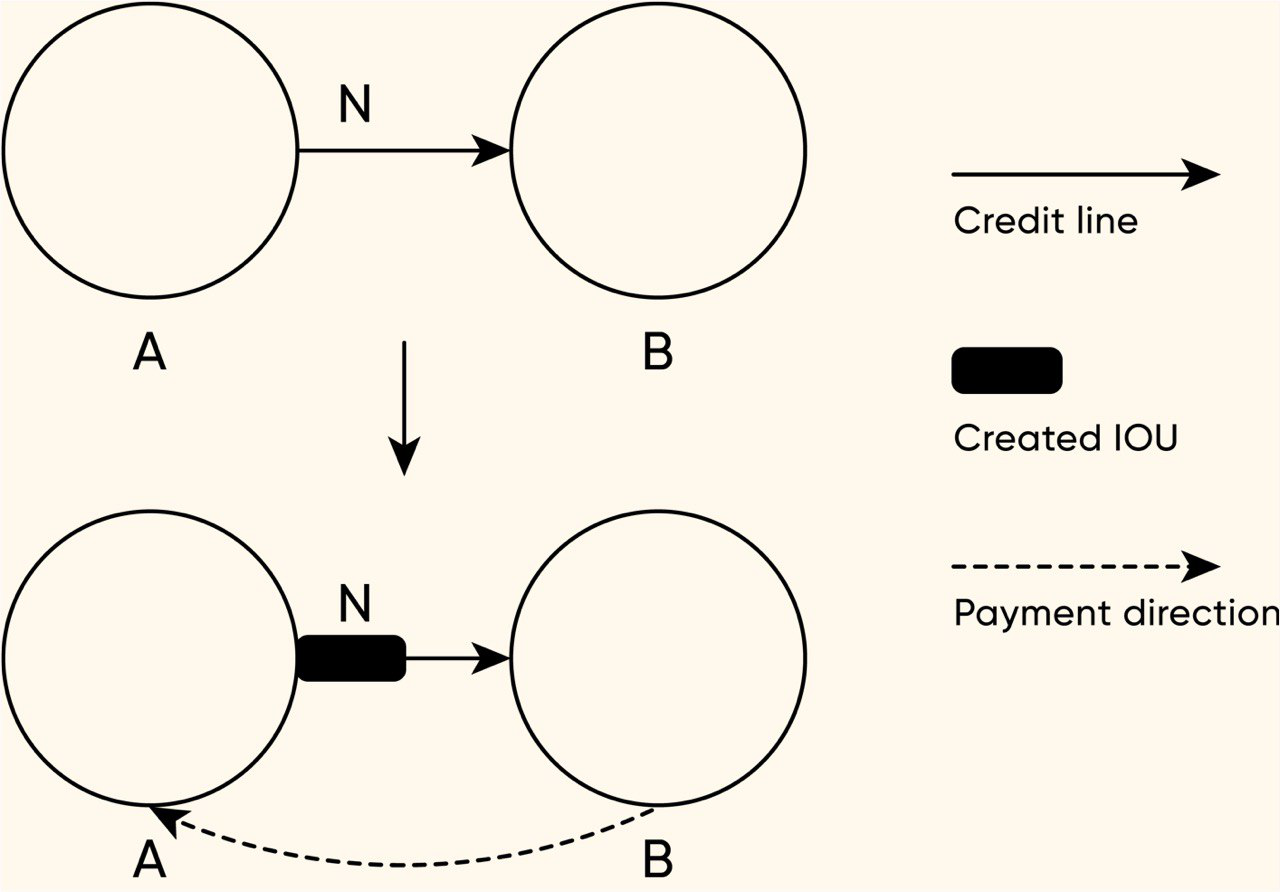
Another benefit of LN is that it’s not controlled by any particular corporation or even group of developers. The development started with writing a documentation called BOLT (Basis of the Lightning Technology). These BOLTs describe every aspect of the protocol in forensic detail using pseudocode and plain English. Then there are multiple teams around the world building actual implementation using different programming languages and platforms, but since they all collaborate on the same reference specification, the resulting software is interoperable.

The beautiful thing is that actions required to make or receive payment in Bitcoin via Lightning Network rarely take place on-chain. This saves very expensive blockchain real estate and speeds up trading significantly.

### GEO Protocol

GEO protocol is an off-chain scaling solution that can be built on top of any existing public blockchain and connect them in a single cross-chain network. There is no common ledger that requires computationally-expensive nodes and power to secure. Instead, it is an off-chain protocol that leverages a distributed network of state channels and trustlines connecting them. The advantage is that unlike Bitcoin, Ethereum or Plasma, a GEO node can be spun up on a comparably slow and cheap device – like a smartphone or Raspberry Pi computer.

GEO is leveraging the concept of trustlines which was pioneered by Ryan Fugger from Ripple. The idea is quite similar to bidirectional channels in LN or Raiden, although it is not based on the locked up multisig liquidity, but rather on a bilateral agreement between exactly two users. This agreement consists of two credit lines, as well as a balance indicating if, and how much, one party owes the other. Payments between non-trusting strangers are implemented by propagating balance updates through a network of trustlines until the payment reaches the receiver.

**

*Trustlines mechanics*

Trustlines consist of IOU (I Owe You) channels where users can issue their own currency or asset and the network facilitates free and unrestricted exchange of that asset. This also allows cross-blockchain exchange of value directly between holders without engaging with centralized exchanges. In order to preserve the decentralized and trustless nature of blockchain technology, the protocol does not allow freezing of either account or trustline.

Another concept developed by GEO protocol is composite channels, which are a combination of trustlines with user-issued assets and classic state channels with cryptocurrency locked up in an on-chain multisig wallet. This combines almost infinite scalability with a trustlessness of the base layer blockchain or multiple blockchains. At the end of the day, the user is allowed to not only make cryptocurrency transactions, but also tokenized fiat money, real world property and other assets. One tangible example of this technology would be a cross-chain DEX (decentralized exchange) enabled by the protocol from scratch.

### Celer Network

Celer Network is a blockchain agnostic and horizontally scalable protocol that increases the scalability of blockchains through off-chain scaling. It utilizes a layered technology architecture, with several core technical innovations including:

* Channel construct suite with sidechain channels and flexible support for generalized off-chain dApp state transitions
* Optimal state routing algorithm with 15x higher transaction throughput than existing state-of-the-art solutions
* Off-chain operating system that simplifies development and usage of off-chain applications on various platforms

It should be noted that there are other solutions that have taken a similar approach such as the Lightning Network, Raiden, Trinity and Plasma. Celer Network differentiates itself because it will be compatible with all the other projects fighting to scale on-chain. This is important to consider because other projects in this space such as the Lightning Network (LN) cannot work with ETH or EOS.

### Raiden Network

Just like Lightning Network for Bitcoin, Raiden creates a sequence of payment channels outside of the blockchain itself to resolve transactions quickly. Raiden, however, has its own ERC20-based token called RDN which is not required to make payments but will be used to get additional services. At some point the team has raised $33 million to fund the development of the project via an ICO – initial coin offering.

One of the first implementations of Raiden Network is called µRaiden, which is specifically designed for micro payments in ERC20-based tokens. The difference is that µRaiden only uses unidirectional payment channels, whereas Lightning Network is leveraging bidirectional payment channels.

### What Does the Future Hold?

The dynamics and development of public blockchains pretty much indicates the inevitability of further expansion and growth of second layer networks. The Bitcoin Cash experiment has proven that on-chain scaling is a dead end and even if it can technically solve the scaling issue, it will always do so at the expense of decentralization which in turn will completely destroy the purpose of why blockchains were created in the first place. In addition to scaling and privacy, second layer networks will extend the capacity of blockchain technology and open new use-cases that in turn will bring Ethereum, Bitcoin and other technologies into the hands of the next billion people.