Layer One dot Five Technology

Trustless Architecture for an Asset-Referencing Sidechain Coin, Backed by Bitcoin Collateral

Miro Sarbaev Lexis Tikhvinskiy

February 19, 2023
Commit e2a82d7

Abstract

Instead of the term "stablecoin", we use "DeARC", which stands for "decentralized Asset-Referencing Coin".

Layer One-dot-Five (L15) is a system that enables L15$ - a *DeARC*, algorithmically price-synchronized to the US dollar and backed by Bitcoin collateral. L15 combines the principles of the Lightning network and the sidechain: it encumbers Bitcoin collateral in a Lightning-style DLC while its commitment signatures are recorded on the sidechain. L15 is merge-mined with Bitcoin, which allows miners who win blocks on both chains simultaneously to trustlessly validate collateral release. The resulting system is interoperable with the Lightning Network.

Along with enabling the *DeARC*, L15 can potentially be a platform that developers can use to implement a subset of smart contracts, covering practical consumer finance use cases, like pull transactions and subscription payments.

For the latest version of this paper, please visit
https://l15.dev/L15-stable.pdf

Acknowledgments

The authors would like to extend their sincere thanks to:

Dr. A. Bekin, co-author of the *L15 Economics* paper for significant contributions to making the paper digestible.

Katherine N. Golubev, the communications artist, for making the English language flow.

K., for providing the Bitcoin industry guidance and bringing the spirit of the true cypherpunk into the mix.

Table of Contents

1 Introduction

Bitcoin's development as an asset discourages its use in day-to-day transactions. This elevates the need for an integrated transactional coin within the ecosystem. A *DeARC* issued to a user in exchange for collateral in Bitcoin can become that transactional coin. While a solution is available in the ERC20 ecosystem, most Bitcoin users find this path too tolling. This cost assessment is made not only in terms of the fees but also considering the time needed to traverse layers of intermediaries, the compounded risk of several innovative solutions chained together, and the added exposure to centralization risks introduced by some intermediaries.

L15 (Layer One-dot-Five) is a system that enables L15$ - a collateralized *DeARC*, near-native to the Bitcoin ecosystem. L15 is not strictly *native* since it has its own chain – a Bitcoin merge-mined sidechain that tracks two new digital assets: a *DeARC* and a stabilization coin.

At its core, L15 is a decentralized protocol that utilizes DLC (Dryja, 2017) and Layer 2 payment channel[1] principles while storing channels' states in the L15 blockchained ledger, which allows for implementing financial smart contracts.

While leaving other platform possibilities intact, we focus on building a single canned feature on top of L15 - the *DeARC* L15$, created in L15 as a product of overcollateralized loan facilitated by the L15 contract.

[1] As defined in https://en.bitcoin.it/wiki/Payment_channels

2 Product

L15 is a proof-of-work pegged sidechain variant which supports the use case of a collateralized loan contract. It locks users' Bitcoin and creates a *DeARC* L15$, referencing the US dollar price.

Users make deposits in Bitcoin and borrow against the deposited value. Repaying the loan is equivalent to providing proof of burn for borrowed L15$ and accrued interest, which automatically makes the Bitcoin deposit spendable by the borrower. If the value of the Bitcoin deposit falls below the minimum collateralization ratio, the loan can be liquidated by the contract. The US dollar value of L15$ is backed by the US dollar value of the underlying Bitcoin deposits held by L15 contracts. To maintain the price reference of L15$ to USD, L15 uses fees, loan interest rates, and, most importantly – Decentralized Stability Management (DSM), based on the native Stabilization Reserve coin - L15SR, along with Decentralized Stability Fund (DSF), as described in the Economics paper. L15SR is also used to reward miners and pay transaction fees.

Initially inspired by Maker DAO, L15 improves on the model in two significant ways: first, it is designed to be more decentralized, and second, it has a more resilient economic model.

3 A Pegged Sidechain Variant

Just like in any other sidechain, L15 users lock their Bitcoin and, in return, receive an asset they use on the sidechain. However, there are notable differences.

The original sidechain locks your Bitcoin and gives you $BTC_{\text{sidechain}}$. This new sidechain asset represents the locked amount and costs precisely 1 BTC per 1 $BTC_{\text{sidechain}}$, i.e., it is backed by the locked Bitcoin and references the Bitcoin price. The interchange rules between locked Bitcoin and $BTC_{\text{sidechain}}$ are very straightforward: $BTC_{\text{sidechain}}$ can be exchanged back to BTC at any time, at a 1:1 ratio. Locked Bitcoin is agnostic of its original owner: it will be released to anyone who supplies an equal amount of $BTC_{\text{sidechain}}$.

L15$ coin, the L15 version of $BTC_{\text{sidechain}}$, is different. L15$ is backed by the locked BTC but is **not** referencing BTC in its price. Naturally, the interchange rules between locked Bitcoin and L15$ are defined by a more complex set of rules than the 1:1 fluidity of an original sidechain. As shown in fig. 1, for L15$, these rules are defined by the loan contract. Bitcoin in the L15 lockbox is not agnostic of its original owner: he is the only one who can unlock his Bitcoin deposit unless the contractural liquidation conditions are met or the contract term ends.

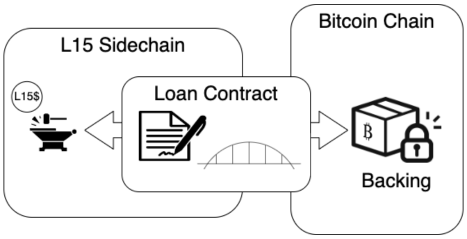

Figure 1: L15 as a Sidechain

3.1 Sidechain Challenges and Federated Solution

The original sidechain has two systemic challenges regarding decentralization and trustlessness — the *expressiveness challenge and* the *small-cap chain challenge*. These challenges are well-documented, mainly by their creators.

The *expressiveness challenge* refers to Bitcoins' inability to look outside its chain. It is described by the inventors of pegged sidechains as (Back et al., 2014, October 22): "One of the challenges in deploying pegged sidechains is that Bitcoin script is currently not expressive enough to encode the verification rules for an SPV proof." In practical terms, Bitcoin does not have any internal instruments to make it aware of transactions in a "chain B." As a result, if one wants to create a transaction in Bitcoin triggered by an event in "chain B," it must rely on an *outside entity*. A sidechain consensus would have been a natural choice for the role of an *outside entity*, but this choice leads to the emergence of the *small-cap chain challenge*: once the sidechain locks a value of Bitcoin that is greater than its own value, there is an incentive for the sidechain consensus members to steal that Bitcoin at the expense of destroying their sidechain.

The inventors of pegged sidechains had proposed and successfully implemented a fix by putting a "trusted *federation* of mutually distrusting *functionaries*" (Back et al., 2014, October 22) in charge of the locked Bitcoin. To form a federation, its members must be identified. To use *distributed consensus*, L15 had to devise an alternate approach, fixing the bridge between Bitcoin and the sidechain without a federation.

3.2 Alternate Approach for Fixing the Bridge

L15 is not a universal sidechain but a system that supports a single use case[2]. To a large extent, the *small-cap challenge* is solved by this limitation. Collateral is cryptographically locked to known outcomes via a DLC enforced by Bitcoin security.

[2] In fact, L15 can support a family of use cases similar to the *DeARC* case, potentially covering most of the needs of a financial ecosystem.

However, there are a few pivotal points within the collateralized loan use case when the outcomes are unknown and the contract is exposed to attestation by the L15 consensus. For example, it is not known which *DeARC* outputs will be used for the payoff. Additionally, in the case of a liquidation auction, it is impossible to know in advance who will end up owning the liquidated Bitcoin. There is less exposure than in the case of a general-purpose sidechain: the bounty is fragmented and available only for a limited time and in limited amounts. L15 consensus can only reverse or halt[3] a collateral payout, but it can not divert it to an address of its choice.

In part, L15 solves the *small-cap challenge* by "brute force." Merge-mining with Bitcoin creates a potential for L15 to pick up a significant hash rate quickly while staying centralized in the interim. However, the remaining exposure necessitates a solution for the *expressiveness* challenge, which manifests itself for L15 as the inability of cross-chain transactions to use the autocorrect feature of Nakamoto consensus. In Bitcoin, if an attacker creates a non-compliant block, the *next miner* will ignore the offending work, and the chain will self-regulate. A collateral release transaction, initiated in L15 by a *DeARC* burn, and completed across the bridge in Bitcoin, is different. It can be 100% legal in Bitcoin and simultaneously break the L15 consensus rules - Bitcoin miners will not be able to catch it. An attacker can inflict irreversible damage by discovering and disclosing the payout secret prematurely – miners in either chain cannot rectify this.

Usually, cross-chain transactions are associated with P2P atomic swaps; peers secure them by holding their own secrets. In our case, one of the peers to an "atomic swap" is L15 itself. But then, a public PoW blockchain is incapable of keeping secrets as a trustlessness and the stateless consensus, lacking persistent memory outside the ledger.

We solved two challenges in L15:

- How to statefully store the cross-bridge transaction secrets in the L15 chain while leaving its miners in control.
- How to enable *the next miner(s)* to contest, reverse and penalize cross-bridge transactions in Bitcoin that offend the L15 consensus rules.

Statefullness

In case of a payout, an actualized transaction that returns the collateral to the borrower (Alice) will spend a pre-defined Bitcoin output (collateral) to Alice's pre-defined address. One may notice a similarity to payment channel commitments, but there is a difference. In Lightning, commitments are stored off-chain by transaction participants. L15 stores unactualized payouts in Layer 1

[3] In some circumstances halting or reversal of the payout can initiate liquidation.

of its own chain, i.e., payment commitments are public. A miner who includes a payout into a block has to pick it from the L15 chain.

As with a payment channel commitment, until actualized, the payout transaction is “missing” a signature of, at minimum, one of the payment channel counterparties. Since the payout outputs are designated for Alice, the “missing signature” must be the signature of Alice’s counterparty. A signing actor must be present at two distinct moments: first, at the time of the loan set up to supply the public key, and second, at the time of the payout actualization to sign with the respective private key. The L15 Virtual Counter-Party is the entity and the technique responsible for providing the “missing signature” at the appropriate moment when a release condition on the L15 sidechain has been fulfilled.

Miners do not qualify for the Virtual Counter-Party role because they lack persistence by design and due to the fact that there is no cost function to the false attestation by a miner. To functionalize the *counter-party* requirements, L15 introduces an additional type of system participant: a bonded signer. Signers cannot be used individually[4]; they are assembled into collectives - the L15vroutnodes. When a user opens a new contract, a dedicated L15vroutnode is assembled out of the pool of all available signers.

Signers are required to supply bonds in Bitcoin, which is helpful in many ways, not least to help prevent Sybil attacks. Signers lock their bonds and get paid market rates based on availability to sign. The selection of a signer for an L15vroutenode is probabilistically random, with the random component provided by entropy from miners and the probability depending on the size of the signer’s bond.

An assembled L15vroutenode can produce a signature with a private key that individual participants do not know by using FROST(Komlo & Goldberg, 2020, December 22) K-of-N multisig to build collective counter-party signatures.

As Alice transacts with L15vroutenode using a payment channel, it is initiated as a 2-of-2 multisig on Bitcoin Layer 1. The first signature is Alice’s ($sig_{(\text{Alice})}$), and the second is the threshold multisig of L15vroutenode ($sig_{(\text{L15vroutnode(i)})}$), as shown in Equation 1, referred to as the (K-of-N)+1 signature scheme:

$A = sig_{(\text{Alice})} + sig_{(\text{L15vroutnode(i)})} =$

[4] ... if they were, the secrecy requirement would contradict the ground rule of participant’s anonymity as one cannot make assumptions about the abilities of an anonymous signer to keep secrets. Likewise, the availability of an individual signer for a one-year duration of a typical loan contract is also problematic. The solution is to assemble a collective signer - the L15vroutnode, a “Flying Macaroni Monster” consisting of individual “noodles” – signers.

$$= \underbrace{sig_{(\text{Alice})} + \overbrace{\left(sig_{(\text{signer 1})} + sig_{(\text{signer 2})} + \ldots + sig_{(\text{signer k})}\right)}^{\text{K-of-N}}}_{\text{2-of-2}} \tag{1}$$

This allows:

1. Alice to communicate with L15Vroutenode as a group,
2. Signers to interact with each other via the L15 chain and produce threshold signatures for the payment channel with Alice, and
3. Merged miners to “borrow” the ability to sign from the validators and enforce L15 consensus rules.

L15vroutenodes are not the *counterparties* per se: they are designed to be “service providers,” delivering services of stateful memory for contracts. The *counterparty* to all the L15 contracts is the whole L15 system, with miners having the final say on transactions.

Self-regulation via the “Next Miner”

On the Bitcoin side, a cross-bridge release transaction is designed as a two-step process with the possibility for an *Enforcement Transaction* (EFT) to intervene in between.

Step 1, the *Payout Initiation* (POI), starts with Alice and her L15Vroutenode signing the outputs and posting POI into Bitcoin Layer 1. That makes the collateral UTXO spendable by Step 2 – *Closing Transaction* (CT). Two relative delays separate POI and CT – $T1$ and $T2$, as shown in fig. 2. $T1$ is designed to clear any potential reorgs in L15. $T2$ is designed to create $T_{(\text{delta})}$ - a time window for an *Enforcement Transaction* (EFT) if enforcement is necessary.

As shown in fig. 3, an external Arbiter initiates an EFT.

This transaction is fulfilled by a set of commitments, pre-signed by Alice with an `ANYONECANPAY` flag. An additional input with an Arbitrage Bond in BTC needs to be posted to actualize them. After that, collateral outputs and the Arbitrage Bond are auctioned for L15 native coins, and the proceeds are burned. Arbiter and Alice still get their money back - either entirely or partially. They create repayment transactions in the L15 chain, minting their Bond and Collateral and getting paid in L15 native asset(s): L15$ or L15SR.

Attestation of either the Arbiters’ or Alices’ honesty is performed by the L15 miners. The miner’s verdict is expressed by allowing Alice and Arbiter to mint different repayment amounts: transaction costs, rewards, and penalties are added or deducted from the parties’ dues following the consensus rules for payout

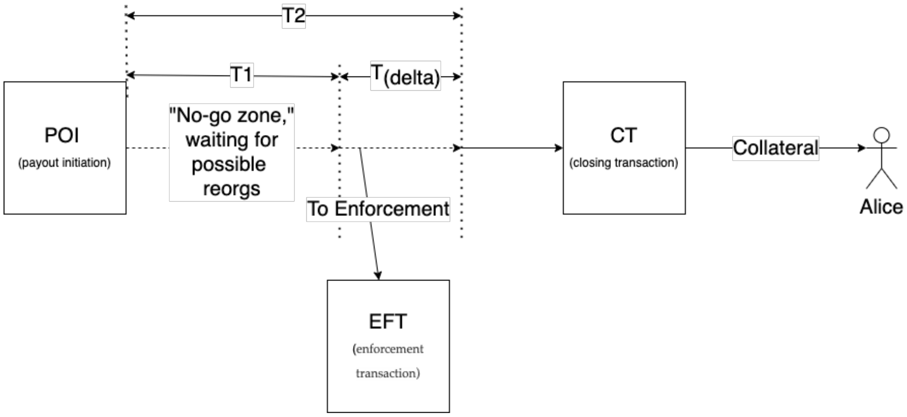

Figure 2: Payout Initiation, Closing and Enforcement

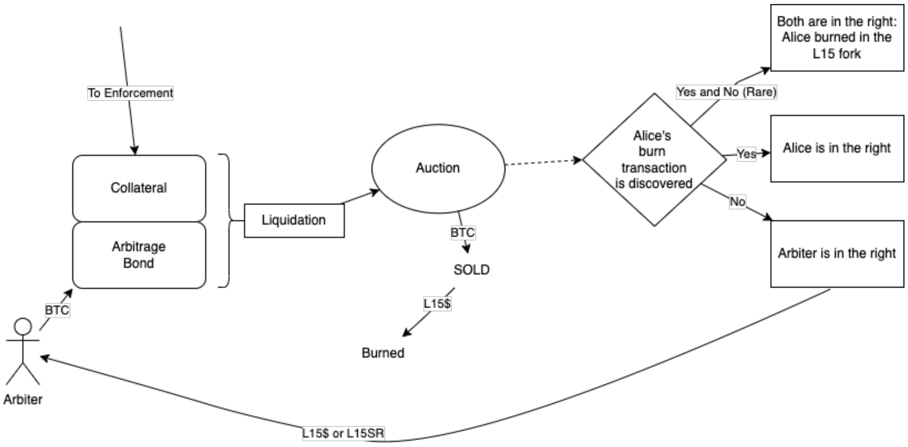

Figure 3: Enforcement Transaction

attestation, detailed in Attachment A.

Burn Request

The safeguards described above secure the system against attacks where the collateral is released without a burn of the loan payoff. To protect from attacks in the opposite direction, when the payoff is burned, but collateral is not released, L15 has a specific script opcode `OP_BURN_REQUEST`. The new opcode signals miners to follow an L15 consensus rule that enforces the atomicity of the process in the direction from Bitcoin to L15. Burn is not considered valid unless there is a corresponding release transaction in Bitcoin, whether finalized or in progress. Otherwise, L15 miners will allow Alice to spend the L15$ that she had previously submitted for the burn.

Small-cap Miners in Charge

The described arrangement puts L15 miners in charge of the locked Bitcoin, which protects it with the most secure consensus mechanism, but does not necessarily resolve the *small-cap chain challenge*. Let's review how the latter is mitigated by the contract design and bounty fragmentation. Due to the presence of the arbiters, stealing the collateral would require an attack on the L15 auction, which exposes only a fragment of the bounty. The auction process is built similarly to the cross-bridge payout; an attack on it will inevitably face its own arbiter and attestation by the miners, resulting in recurrence that converges to a necessity for the attack to be an actual 51% attack. At the same time, L15 negates this possibility, as recurrence cannot be infinite by design. Loan contracts are immune from cascade failure: end-of-contract outputs are locked by pure Bitcoin DLC, independent of any decisions by consensus. In most cases, the extreme cost/reward ratio of breaking a single contract makes an attack like that prohibitive. But even if it succeeds, game theory predicts that sidechain consensus failure will bring the system to a halt, with the remaining collateral inaccessible to the attackers. DLCs will carry out a gradual auto–release of collateral to its owners as the contracts expire.

4 Conclusion

A sidechain that extends the Bitcoin functionality should strive to be on-par with Bitcoin in trustlessness and security. L15 aspires to fulfill this goal. L15 is a PoW chain designed to allow for the use of identity-lacking *distributed consensus*, *"a consensus (i.e., global agreement) between many mutually-distrusting parties who lack identities and were not necessarily present at the time of system set up."*(Poelstra, 2015, March 22)

The complexity of collateralized loan contracts requires stateful memory. In L15, it is provided by bonded signers, which is reminiscent of a Proof of Stake algorithm. The difference, however, which precludes L15 from being impacted by the PoS trust model deficiencies described in (Poelstra, 2015, March 22) is that signers do not participate in recording or maintaining the history of the L15 blockchain. This separates them from the power that would allow them to create a vulnerability.

The bridge between a sidechain and Bitcoin is the most challenging area for a trustless design. In L15, the attestation decision for transactions that cross the bridge is made exclusively by miners, which enables "self-regulation by the next miner" for collateral payouts, just like in Bitcoin. By design, L15 relies only on PoW to secure its chain and functionality. Considering the merged mining with Bitcoin, for L15, approaching the Bitcoin standard in trustlessness and security is primarily a question of increasing adoption by Bitcoin miners.

Attachment A

Consensus Rules for Payout Attestation

If Alice is in the right

Party	Penalty	Expenses	Loan payoff	Reward
Alice			Paid earlier	n/a
Arbiter	Deducted from bond	Deducted from Bond		

If Arbiter is in the right

Party	Penalty	Expenses	Loan payoff	Reward
Alice	Deducted from collateral	Deducted from collateral	Deducted from collateral	Deducted from collateral
Arbiter				Paid from Alice's Penalty

If everyone is in the right (Alice provided the proof-of-burn, but it was reorged)

Party	Penalty	Expenses	Loan payoff	Reward
Alice	n/a		Deducted from collateral	
Arbiter	n/a			Paid by L15 by inflating L15SR
L15		Paid by L15 by inflating L15SR		

References

Back, A., Corallo, M., Dashjr, L., Friedenbach, M., Maxwell, G., Miller, A., Poelstra, A., Timón, J., & Wuille, P. (2014, October 22). *Enabling blockchain innovations with pegged sidechains* [White Paper]. https://blockstream.com/sidechains.pdf

Dryja, T. (2017). *Discreet log contracts* [White Paper]. https://adiabat.github.io/dlc.pdf

Komlo, C., & Goldberg, I. (2020, December 22). *FROST: Flexible round-optimized schnorr threshold signatures* [Report]. https://eprint.iacr.org/2020/852.pdf

Poelstra, A. (2015, March 22). *On stake and consensus* [White Paper]. https://nakamotoinstitute.org/static/docs/on-stake-and-consensus.pdf