Kairos: Zero-knowledge Casper Transaction Scaling

Marijan Petricevic, Nick Van den Broeck

Monday November 27, 2023

Contents

1. Introduction

The Casper blockchain's ecosystem is in need of a scaling solution to achieve a higher transaction throughput and continue to stay competitive. As a first step towards providing a trustless scaling solution, the goal of the initial version 0.1 of the Kairos project is to build a zero-knowledge (ZK) *validium* [1] for payment transactions in a second layer (L2). This system will both enable a higher transaction throughput and lower gas fees. Here, *validium* refers to a rollup where the data, such as account balances, are stored on L2 rather than on the Casper blockchain directly (L1).

Additionally, Kairos V0.1 serves two other purposes:

- It is the first step towards a cheap and frictionless NFT (non-fungible token) minting and transfer system aiding Casper to become *the* blockchain to push the digital art industry forward.
- The conciseness and complexity of its scope allow us to explore the problem space of L2 solutions that leverage zero-knowledge technology and integrate with Casper's L1. Furthermore, it allows the team to collaborate and grow together by building a production-grade system.

Kairos V0.1 will support very few simple interactions and features. Users will be able to deposit and withdraw funds by interacting with an L1 smart contract controlled by Kairos. Transfers of funds to other participants will be serviced by the L2 and verified and stored by the L1. In the remainder of this document, we will detail the requirements of such a system.

In Section 2 (Product Overview) we describe the high-level features that Kairos V0.1 will support. Section 3 specifies the requirements based on the described interactions and features. Next, in Section 4 (Architecture), we propose an architecture of this initial version, together with the component interfaces and their interactions. We conclude the document with threat models and a glossary, which clarifies the terminology used throughout this document. Note that this document is accompanied by several blog posts detailing some of the design considerations in more detail, as listed in the bibliography [2] [3].

2. Product Overview

To have a common denominator on the scope of Kairos V0.1, this section describes the high-level features it has to support.

2.1. Product Application

2.1.1. Target Audience

The target audience comprises users familiar with blockchain technology and applications built on top of the Casper blockchain.

2.1.2. Operating Environment

The product's backend will be deployed on modern powerful machines equipped with a powerful graphics processing unit (GPU) and a large amount of working memory as well as persistent disk space. The machines will have continuous access to the Internet.

The CLI will be deployed on modern, potentially less powerful hardware.

2.1.3. Constraints

The product should be a centralized solution for this initial version 0.1.

The used proving system should be zero knowledge.

2.2. Features

2.2.1. Deposit Tokens Into L2 System

[tag:F00]: Users should be able to deposit tokens from their L1 account to their L2 account at any given time through a command line interface (CLI).

2.2.2. Withdraw Tokens From L2 System

[tag:F01]: Users should be able to withdraw tokens from their L2 account to their L1 account at any given time through a CLI. This interaction should not require the approval of the operator (see Ethereum's validium).

2.2.3. Transfer Tokens Within the L2 System

[tag:F02]: Users should be able to transfer tokens from their L2 account to another user's L2 account at any given time through a CLI.

2.2.4. Query Account Balances

[tag:F03]: Anyone should be able to query any L2 account balances at any given time through a CLI. In particular, users can also query their personal L2 account balance.

2.2.5. Query Transaction Data

[tag:F04]: Anyone should be able to query any L2 transactions at any given time through a CLI.

2.2.6. Verification

[tag:F05]: Anyone should be able to verify deposits, withdrawals, or transactions either through a CLI or application programming interface (API), i.e. a machine-readable way.

3. Requirements

Based on the product overview given in the previous section, this section aims to describe testable, functional requirements the system needs to meet.

3.1. Functional Requirements

3.1.1. Deposit Tokens Into L2 System

- **[tag:F00-00]** Depositing an amount of `tokens`, where `tokens >= MIN_AMOUNT` must be accounted correctly: `new_account_balance = old_account_balance + tokens`
- **[tag:F00-01]** Depositing an amount of `tokens`, where `tokens < MIN_AMOUNT` must not be executed at all
- **[tag:F00-02]** A user depositing any valid amount (condition stated in F00-00) to their `L2 account` must only succeed if the user has signed the deposit transaction
- **[tag:F00-03]** A user depositing any amount with a proper signature to another user's account must fail
- **[tag:F00-04]** A deposit request shall not be replayable.

3.1.2. Withdraw Tokens From L2 System

- **[tag:F01-00]** Withdrawing an amount of `tokens`, where `user's L2 account balance >= tokens > MIN_AMOUNT` must be accounted correctly: `new_account_balance = old_account_balance - tokens`
- **[tag:F01-01]** Withdrawing an amount of `tokens`, where `tokens < MIN_AMOUNT` must not be executed at all
- **[tag:F01-02]** Withdrawing an amount of `tokens`, where `tokens > user's L2 account balance` should not be possible
- **[tag:F01-03]** Withdrawing a valid amount (condition stated in F01-00, F01-02) from the user's L2 account must be possible without the intermediary operator of the system
- **[tag:F01-04]** Withdrawing a valid amount (condition stated in F01-00, F01-02) from the user's L2 account must succeed if the user has signed the withdrawal transaction
- **[tag:F01-05]** Withdrawing any amount from another user's L2 account must not be possible
- **[tag:F01-06]** A withdrawal request shall not be replayable.

3.1.3. Transfer Tokens Within the L2 System

- **[tag:F02-00]** Transfering an amount of `tokens` from `user1` to `user2`, where `user1's L2 account balance >= tokens > MIN_AMOUNT` must be accounted correctly: `new_account_balance_user1 = old_account_balance_user1 - tokens` and `new_account_balance_user2 = old_account_balance_user2 - tokens`
- **[tag:F02-01]** Transfering an amount of `tokens`, where `tokens < MIN_AMOUNT` must not be executed at all
- **[tag:F02-02]** Transfering an amount of `tokens`, where `tokens > user's L2 account balance` must not be possible
- **[tag:F02-03]** Transfering a valid amount (condition F02-00) to another user that does not have a registered L2 account yet must be possible.
- **[tag:F02-04]** Transfering a valid amount (condition F02-00) to another user should only succeed if the user owning the funds has signed the transfer transaction
- **[tag:F02-05]** A transfer request shall not be replayable.

3.1.4. Query Account Balances

- **[tag:F03-00]** A user must be able to see their L2 account balance when it's queried through the CLI
- **[tag:F03-01]** Anyone must be able to obtain any L2 account balances when querying the CLI or API
- **[tag:F03-02]** Account balances must be written by known, verified entities only
- **[tag:F03-03]** Account balances must be updated immediately after the successful verification of correct deposit/withdraw/transfer interactions
- **[tag:F03-04]** Account balances must not be updated if the verification of the proof of the interactions fails
- **[tag:F03-05]** Account balances must be stored redundantly [4]

3.1.5. Query Transaction Data

- **[tag:F04-00]** A user must be able to see its L2 transactions when they are queried through the CLI
- **[tag:F04-01]** Anyone must be able to obtain any L2 transactions when querying the CLI or API
- **[tag:F04-02]** Transaction data must be written by known, verified entities only
- **[tag:F04-03]** Transaction data must be written immediately after the successful verification of correct deposit/withdraw/transfer interactions
- **[tag:F04-04]** Transaction data must not be written if the verification of the proof of the interactions fails
- **[tag:F04-05]** Transaction data must be stored redundantly [4]

3.1.6. Verification

- **[tag:F05-00]** Anyone must be able to query and verify proofs of the system's state changes caused by deposit/withdraw/transfer interactions at any given time

3.2. Non-functional Requirements

These are qualitative requirements.

- **[tag:NF00]** The application must not leak any private or sensitive information like private keys
- **[tag:NF01]** The backend API must be designed in such a way that it's easy to swap out a client implementation
- **[tag:NF02]** The CLI should respond to user interactions immediately
- **[tag:NF03]** The CLI should be designed in a user-friendly way
- **[tag:NF04]** The L2 should support a high parallel transaction throughput[1]
- **[tag:NF05]** The whole system must be easy to extend with new features

4. A Suggested Architecture

To give the reader an idea of what a system defined in the previous sections might look like, this section proposes a possible architecture. The features and requirements described previously suggest two core components in the system. A CLI and an L2 node implementing the client-server pattern. The L2 node should not be monolithic but rather obey the principle of separation of concerns to allow for easier extensibility and replacement of components in the future. Therefore, the L2 node unifies various other components described in more detail in the following Section 4.1 and exposes them through a single API.

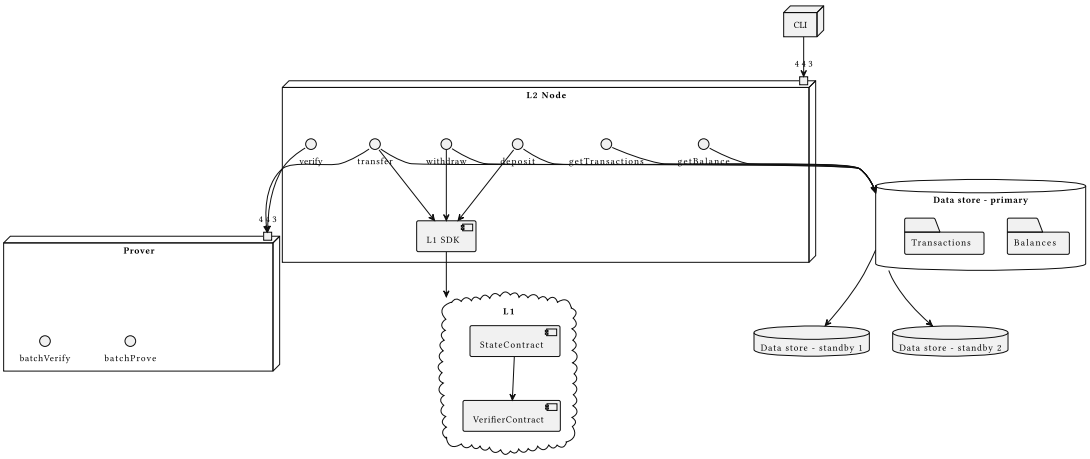

Figure 1: Components diagram

[1]Read [5] for more insight into parallel vs. sequential transaction throughput.

4.1. Architecture Components

4.1.1. Client CLI

The client CLI's user interface (UI) is comprised of commands allowing users to deposit, transfer, and withdraw funds allocated in their L2 account. Once a user executes any of the commands, the client delegates the bulk of the work to the L2 node (Section 4.1.2). Moreover, the client CLI can be used to verify past state changes and to query account balances and transfers.

4.1.2. L2 Node

As constrained in Section 2.1.3, the L2 node is centralized. The detailed reasoning behind this decision, potential dangers, and our methods for dealing with these dangers are explained in [6].

The L2 node is the interface through which external clients (Section 4.1.1) can submit deposits, transfers, or withdrawals of funds. Moreover, it is connected to a data store (Section 4.1.4) to persist the account balances, whose state representation[2] is maintained on-chain. State transitions of the account balances are verified and executed on-chain, requiring the node to create respective transactions on L1 using the L1′s software development kit (SDK). These transactions, in turn, call the respective endpoints of smart contracts described in Section 4.1.5 to do so. To execute batch transfers the node utilizes a proving system provided by the Prover service (Section 4.1.3). For deposits and withdrawals, the node creates according Merkle tree updates of the account balances [7].

4.1.3. Prover

The Prover is a separate service that exposes a *batchProve* and a *batchVerify* endpoint, mainly used by the L2 node (Section 4.1.2) to prove batches of transfers. Under the hood, the Prover uses a zero-knowledge proving system that computes the account balances resulting from the transfers within a batch and a proof of correct computation.

4.1.4. Data Store

The data store is a persistent storage that stores the performed transfers and the account balances whose state representation is stored on the blockchain. To achieve more failsafe and reliable availability of the data, it is replicated sufficiently often by so-called standbys (replicas). In the case of failure, standbys can be used as new primary stores ([4]).

[2] The state representation is the Merkle root, see Section 5.

4.1.5. L1 State/ Verifier Contract

The L1 State and Verifier Contracts are responsible for verifying and performing updates of the Merkle root of account balances. They can be two separate contracts or a single contract with several endpoints. A state update only happens if the updated state was verified successfully beforehand. The contracts are called by the L2 node by creating according transactions and submitting them to an L1 node.

For the Merkle tree root to have an initial value, the State Contract will be initialized with a deposit. This initial deposit then becomes the balance of the system.

4.2. APIs

The following section proposes a possible API of the previously described components.

4.2.1. Client CLI

Name	Arguments	Return Value	Description
get_balance	accountId: AccountID	balance: UnsignedINT	Returns a user's L2 account balance. The UnsignedINT type should be a type that allows for safe money computations (Read [8])
transfer	sender: AccountID, recipient: AccountID, amount: UnsignedINT, token_id: TokenID, nonce: Nonce, key_pair: KeyPair	transferId: TransferID	Creates, signs and submits an L2 transfer to the L2 node. A cryptographic nonce should be used in order to prevent replay attacks.
getTransfer	transferId: TransferID	transfer: TransferState	Returns the status of a given transfer: Cancelled, ZKP in progress, batch proof in progress, or "posted on L1 with blockhash X"

deposit	depositor: AccountID, amount: UnsignedINT, token_id: TokenID, key_pair: KeyPair	transaction: Transaction	Creates an L1 deposit transaction, by first asking the L2 node to create an according L1 transaction for us, afterward signing it on the client-side and then submitting it to L1 through the L2 node
withdraw	withdrawer: AccountID, amount: UnsignedINT, token_id: TokenID key_pair: KeyPair	transaction: Transaction	Creates an L1 withdraw transaction, by first asking the L2 node to create an according L1 transaction for us, afterward signing it on the client-side and then submitting it to L1 through the L2 node
verify	proof: Proof, public_inputs: PublicInputs	result: VerifyResult	Returns whether a proof is legitimate or not

4.2.2. L2 Node

Name	Arguments	Return Value	Description
get_balance	accountId: AccountID	balance: UnsignedINT	Returns a user's L2 account balance. The UnsignedINT type should be a type that allows for safe money computations (Read [8])

transfer	sender: AccountID, recipient: AccountID, amount: UnsignedINT, token_id: TokenID, nonce: Nonce, signature: Signature, sender_pub_key: PubKey	transferId: TransferID	Schedules an L2 transfer, and returns a transfer-ID
getTransfer	transferId: TransferID	transfer: TransferState	Returns the status of a given transfer: Cancelled, ZKP in progress, batch proof in progress, or “posted on L1 with blockhash X”
deposit	depositor: AccountID, amount: UnsignedINT, token_id: TokenID	transaction: Transaction	Creates an L1 deposit transaction containing an according Merkle tree root update and accompanying metadata needed to verify the update based on the depositor’s account ID and the amount. The returned transaction is an L1 transaction that has to be signed by the depositor on the client-side.
withdraw	withdrawer: AccountID,	transaction: Transaction	Creates an L1 withdraw

	amount: UnsignedINT, token_id: TokenID		transaction containing an according Merkle tree root update and accompanying metadata needed to verify the update based on the withdrawer's account ID and the amount. The returned transaction is an L1 transaction that has to be signed by the withdrawer on the client-side.
submitTransaction	signedTransaction: SignedTransaction	submitResult: SubmitResult	Forwards a signed L1 transaction and submits it to the L1 for execution.
verify	proof: Proof, public_inputs: PublicInputs	result: VerifyResult	Returns whether a proof is legitimate or not

4.2.3. L1 State/ Verifier Contract

Name	Arguments	Return Value	Description
verify_deposit	depositor: AccountID, amount: UnsignedINT, token_id: TokenID, updated_account_balances: MerkleRootHash, update_metadata: MerkleRootUpdateMetadata, signature: Signature		• Verifies that the transaction contains the same amount of tokens used to update the account balance • Moves the amount from the depositor's L1 account to the

			account owned by the system • Verifies the depositor's signature • Verifies the new Merkle root given the public inputs and metadata • Updates the system's on-chain state on successful verification
verify_withdraw	withdrawer: AccountID, amount: UnsignedINT, tokenId: TokenID, updated_account_balances: MerkleRootHash, update_metadata: MerkleRootUpdateMetadata, signature: Signature		• Verifies that the transaction moves the same amount of tokens used to update the account balance • Moves the amount from the account owned by the system to the withdrawer's L1 account • Verifies the withdrawer's signature • Verifies the new Merkle root given the public inputs and metadata • Updates the system's on-chain state on successful verification

verify_transfers	proof: Proof, publicInputs: PublicInputs		• Verifies that the proof computed from performing batch transfers on the L2 is valid • Updates the system's on-chain state on successful verification

4.3. Component Interaction

Figures 2 and 3 show sequence diagrams for processing a user's deposit and transfer requests, respectively.

4.3.1. Deposit Sequence Diagram

Depositing funds to user `Bob`'s account is divided into three phases, which are modelled in the following sequence diagrams.

In the first phase (Figure 2) users submit their deposit requests through the client CLI to the L2 node. The L2 node creates an L1 transaction (*Deploy*) containing the according Merkle root update and the update metadata, which can be used to verify that the update was done correctly. More precisely, the *Deploy* contains a *Session* that executes the validation of the Merkle tree update, performs the state transition and transfer the funds from the user's L1 account (purse) to the systems L1 account. This *Deploy* needs to be signed by the user before submitting, this is achieved by making use of the L1′s SDK on the client-side.

After submitting, the L1 smart contracts take care of validating the new Merkle root, updating the system's state, and transferring the funds (Figure 3).

Lastly (Figure 4), the L2 node gets notified after the *Deploy* was processed successfully. The node then commits the updated state to the data store. After sufficient time has passed, the user can query its account balance using the client CLI.

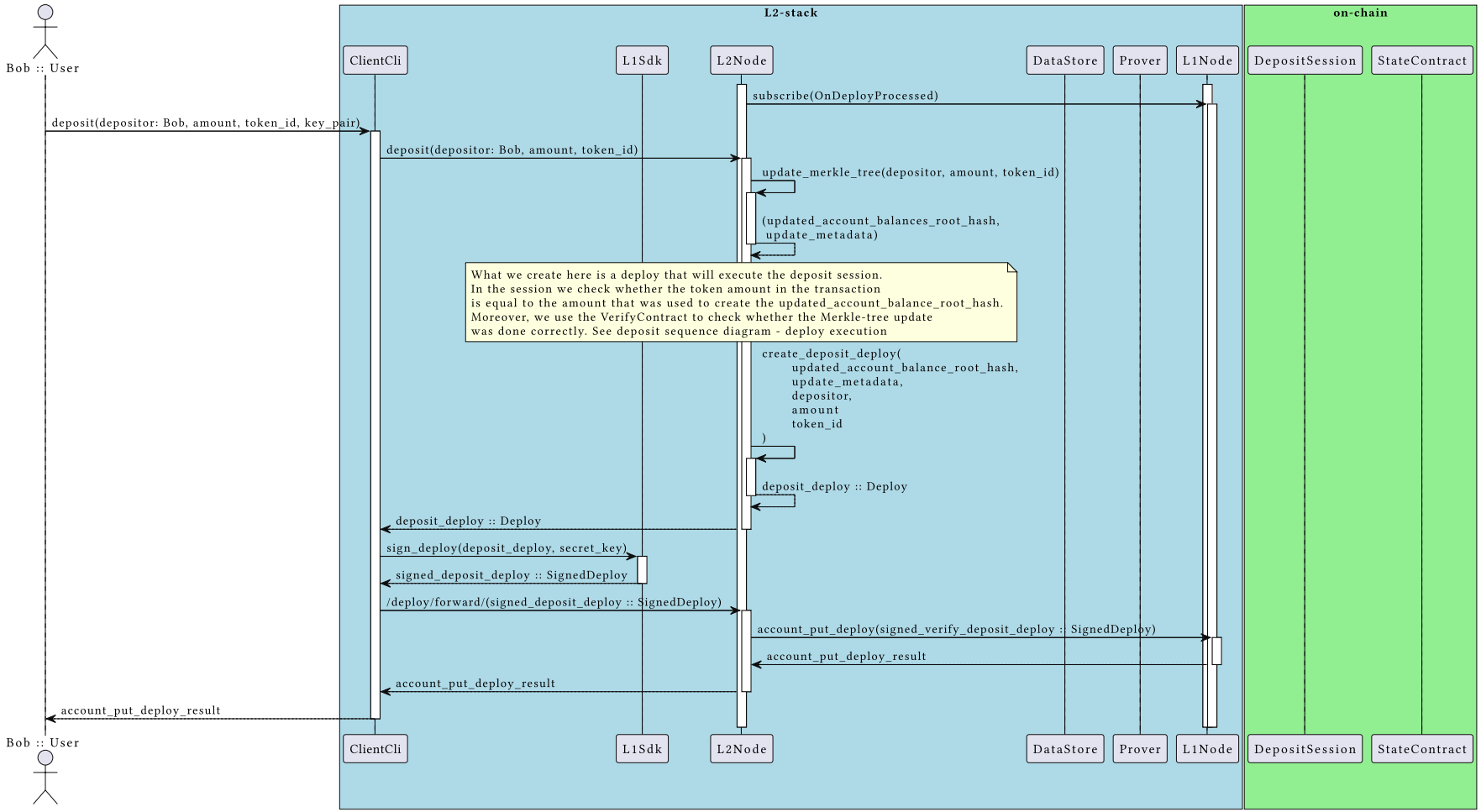

Figure 2: Deposit: User submits a deposit to L2 which gets forwarded to L1.

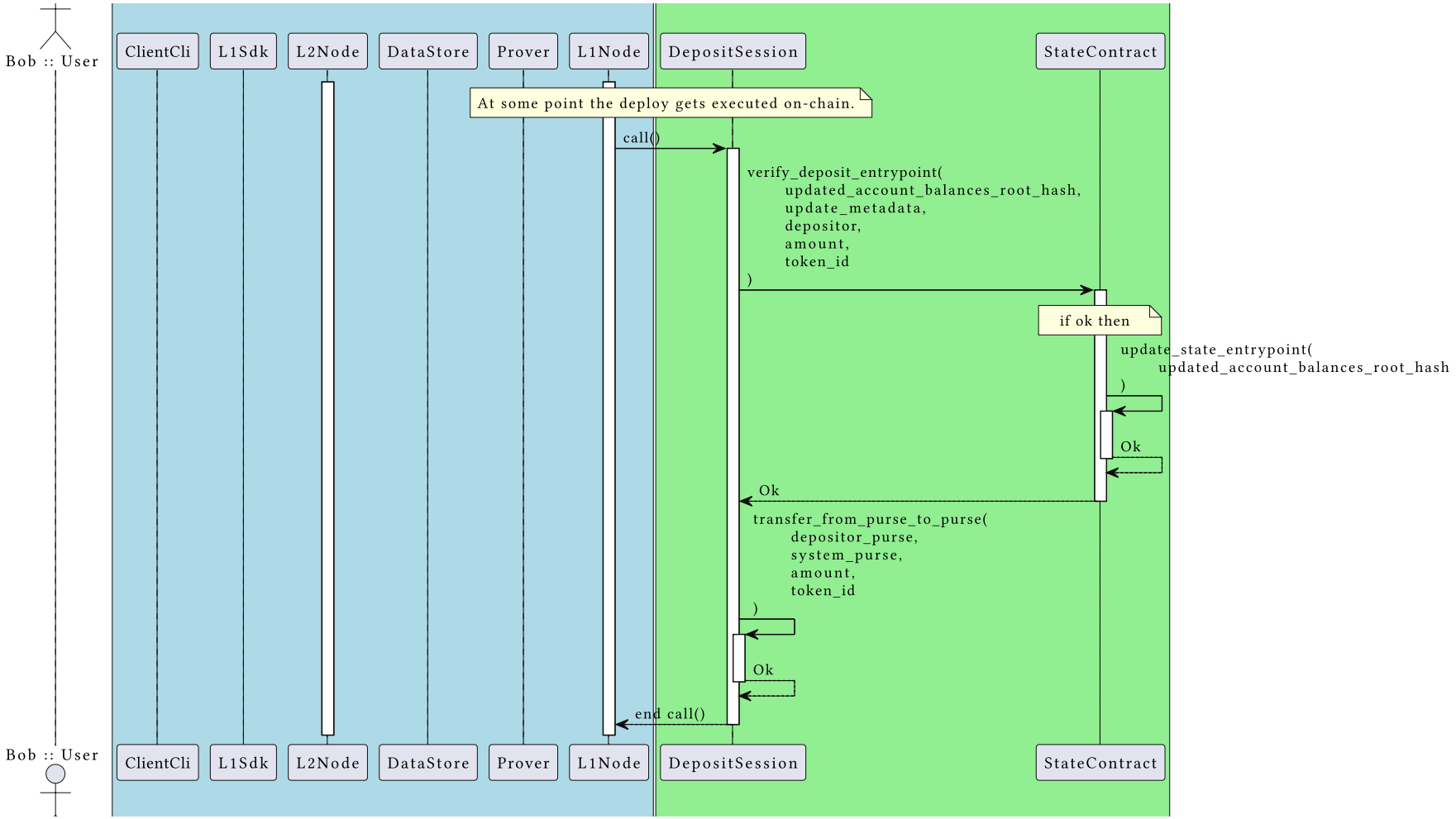

Figure 3: Deposit: Execution of the *Deploy* on L1.

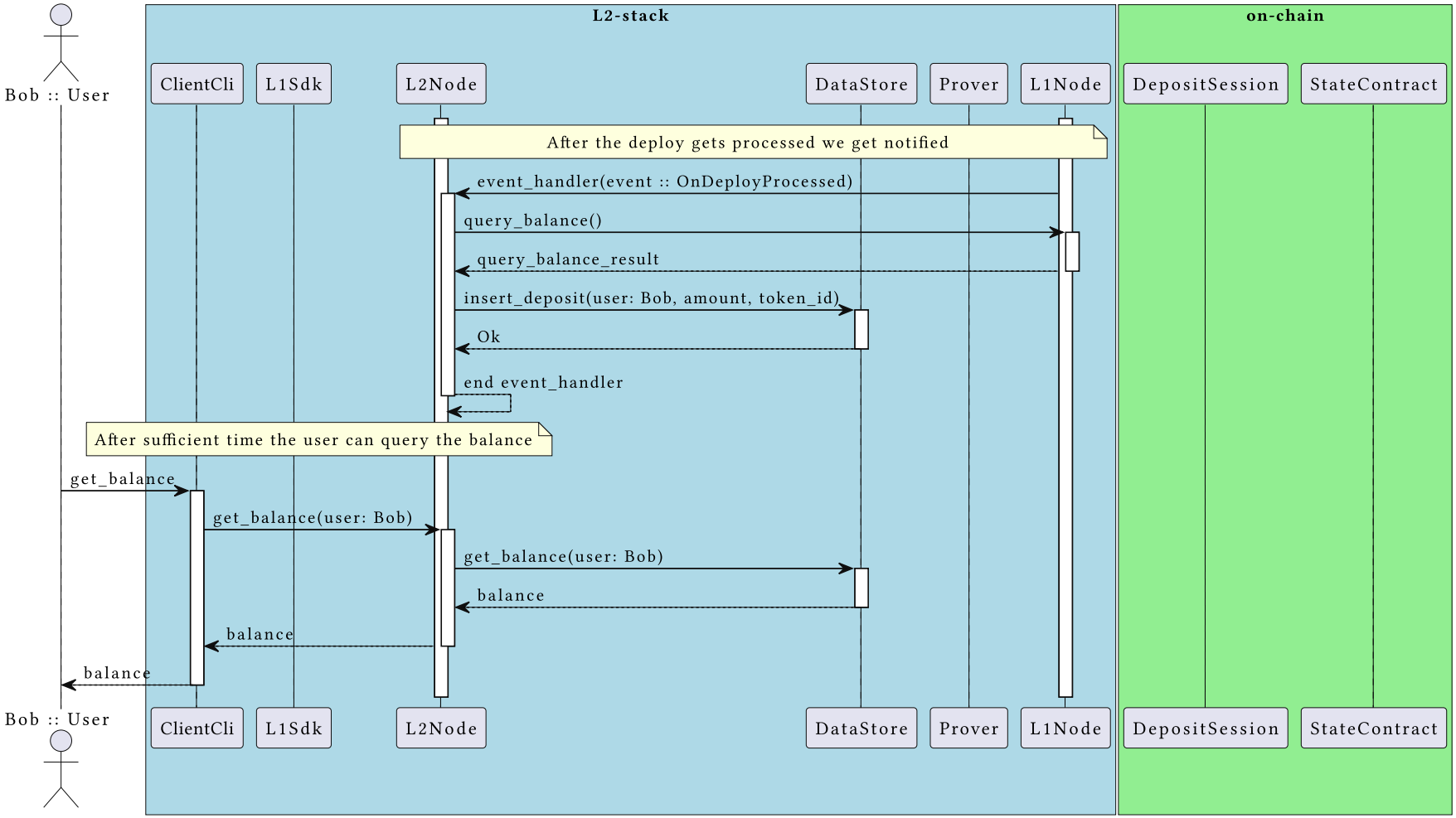

Figure 4: Deposit: Notifying the L2 after succcessfull on-chain execution.

4.3.2. Transaction Sequence Diagram

Transfering funds from user `Bob` to a user `Alice` can be divided into four phases, which are modelled in the following sequence diagrams.

In the first phase (Figure 5) users submit their transfer requests through the client CLI to the L2 node. The L2 node accumulates the transfer requests and checks for independence. In addition, the L2 node will check that the batch proof which is going to be computed next, a valid nonce.

After `t` seconds or `n` transactions (Figure 6), the L2 node batches the transfers, creates a proof of computation, and the according *Deploy* which will execute the validation and the state transition on-chain.

After submitting, the L1 smart contracts take care of first validating the proof and updating the state (Figure 7).

Lastly (Figure 8), the L2 node gets notified when the *Deploy* was executed successfully. The node then commits the updated state to the data store. After sufficient time has passed, the users can query their account balances using the client CLI

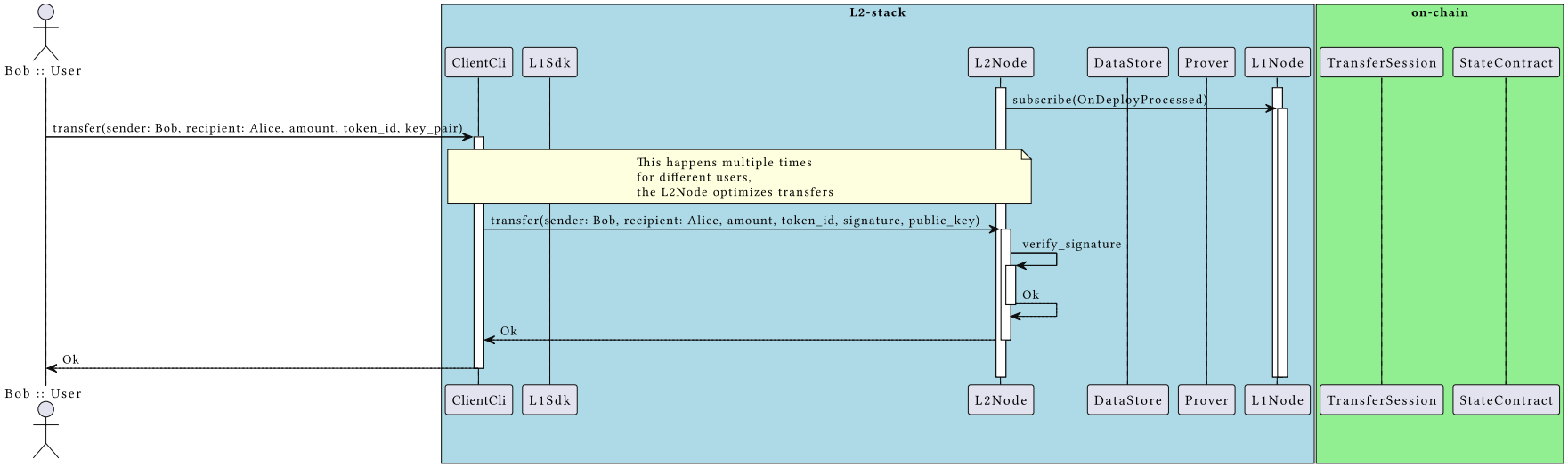

Figure 5: Transfer: User submits a transfer to L2.

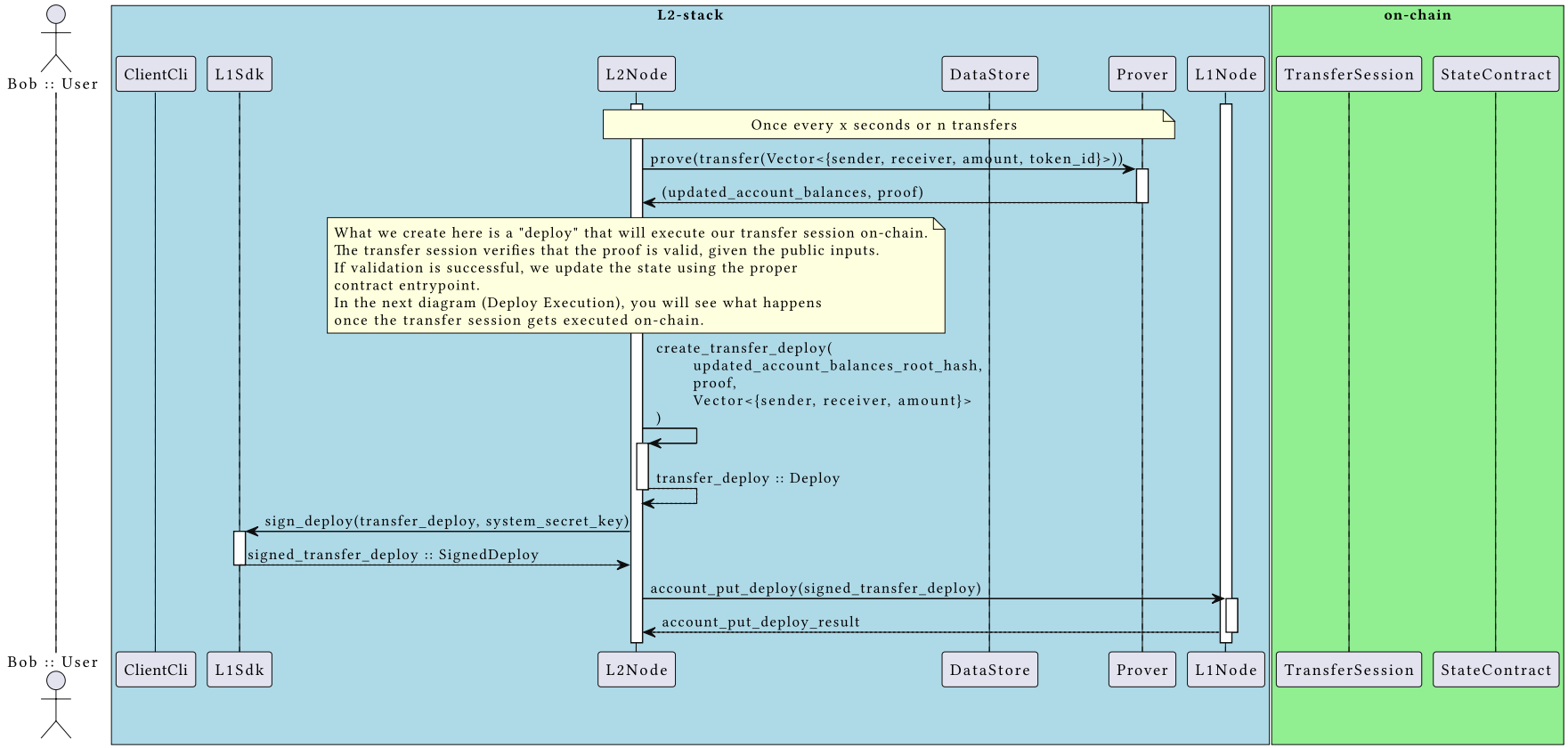

Figure 6: Transfer: Proving and submitting the proof.

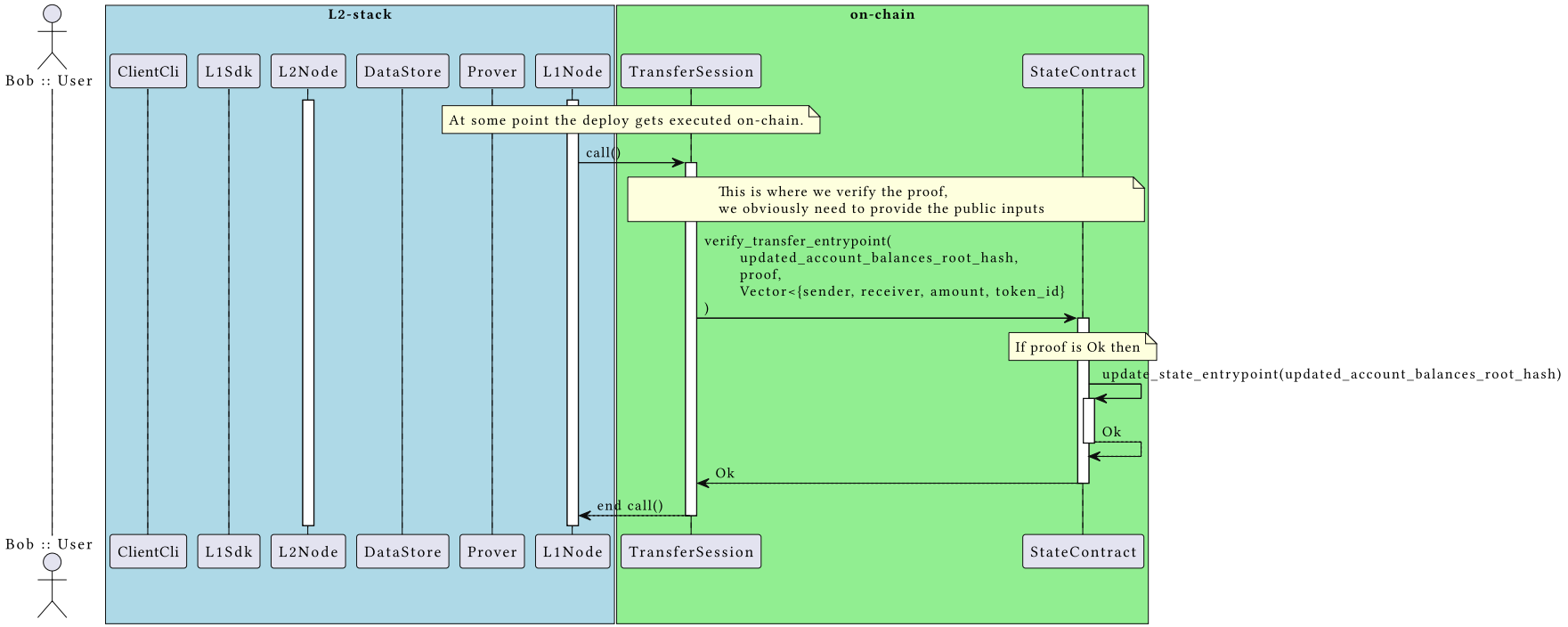

Figure 7: Transfer: Execution of the *Deploy* on L1.

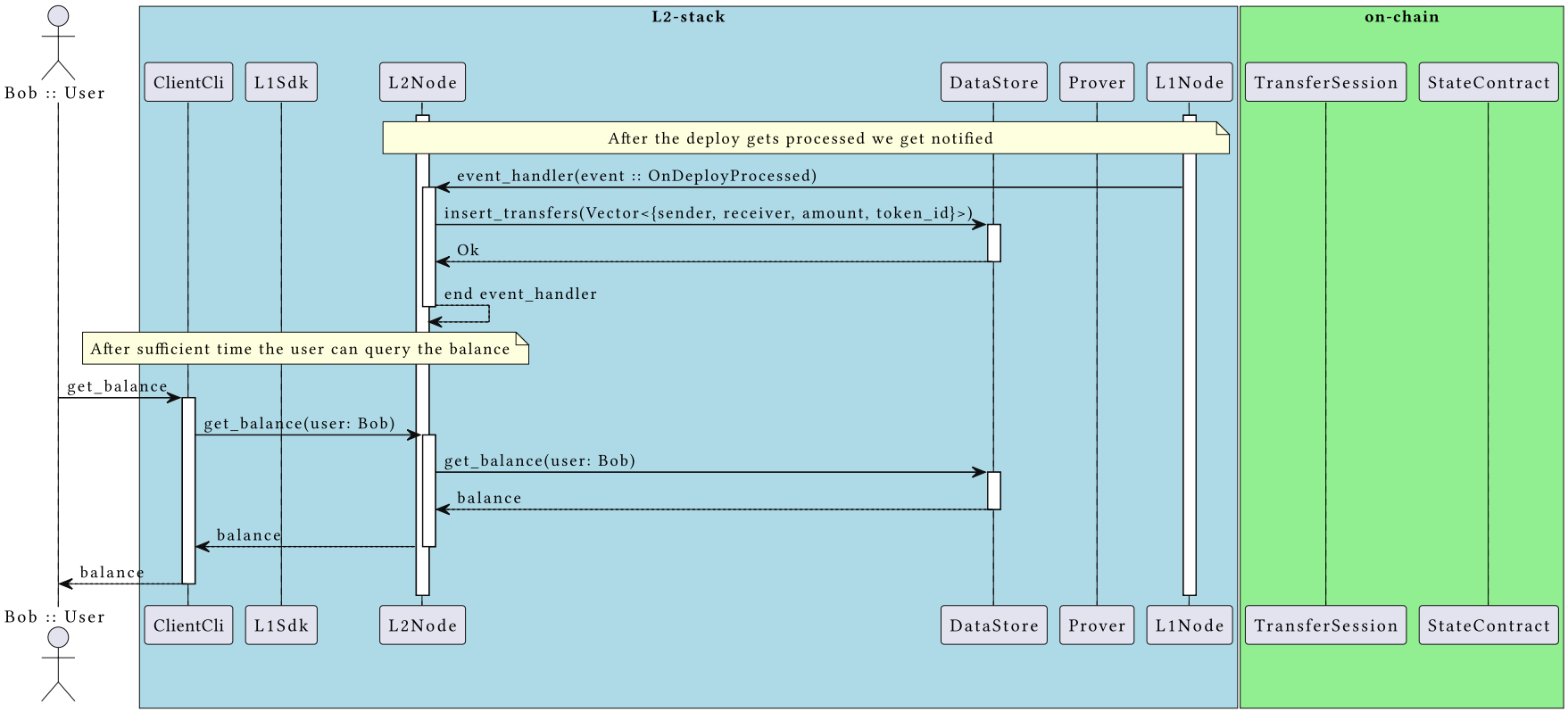

Figure 8: Transfer: Notifying the L2 after succcessfull on-chain execution.

5. Glossary

- L1: The Casper blockchain as it currently runs.
- L2: A layer built on top of the Casper blockchain, which leverages Casper's consensus algorithm and existing infrastructure for security purposes while adding scaling and/or privacy benefits
- Nonce/ Kairos counter: A mechanism that prevents the usage of L2 transactions more than once without the user's permission. It is added to each L2 transaction, which is verified by the batch proof and L1 smart contract. For an in-depth explanation, see [9].
- A zero knowledge proof (ZKP) is a proof generated by person A which proves to person B that A is in possession of certain information X without revealing X itself to B. These ZKPs provide some of the most exciting ways to build L2s with privacy controls and scalability. [10]
- Merkle trees are a cryptographic concept to generate a hash given a dataset. It allows for efficient and secure verification of the contents of large data strutures. [11]

Bibliography

[1] Nick Van den Broeck, "ZK validium vs. Rollup." [Online]. Available: https://github.com/cspr-rad/kairos-spec/blob/main/blogposts/validium-vs-rollup.md

[2] Nick Van den Broeck, "ZK provers: A comparison." [Online]. Available: https://github.com/cspr-rad/kairos-spec/blob/main/blogposts/compare-zk-provers.md

[3] Nick Van den Broeck, "CLI: Adding a trustless mode." [Online]. Available: https://github.com/cspr-rad/kairos-spec/blob/main/blogposts/trustless-cli.md

[4] Nick Van den Broeck, "Data redundancy." [Online]. Available: https://github.com/cspr-rad/kairos-spec/blob/main/blogposts/data-redundancy.md

[5] Nick Van den Broeck, "Sequential through of l2 ZK validia." [Online]. Available: https://github.com/cspr-rad/kairos-spec/blob/main/blogposts/sequential-throughput.md

[6] Nick Van den Broeck, "Why build a centralized l2?." [Online]. Available: https://github.com/cspr-rad/kairos-spec/blob/main/blogposts/centralized-l2.md

[7] Nick Van den Broeck, "Merkle trees: How to update without a zero-knowledge proof?." [Online]. Available: https://github.com/cspr-rad/kairos-spec/blob/main/blogposts/merkle-tree-updates.md

[8] Tom Sydney Kerckhove, “How to deal with money in software.” [Online]. Available: https://cs-syd.eu/posts/2022-08-22-how-to-deal-with-money-in-software

[9] Nick Van den Broeck, “L2 transaction uniqueness.” [Online]. Available: https://github.com/cspr-rad/kairos-spec/blob/main/blogposts/L2-Tx-uniqueness.md

[10] “Zero knowledge proof.” [Online]. Available: https://en.wikipedia.org/wiki/Zero-knowledge_proof

[11] “Merkle tree.” [Online]. Available: https://en.wikipedia.org/wiki/Merkle_tree