Introduction to DeFi

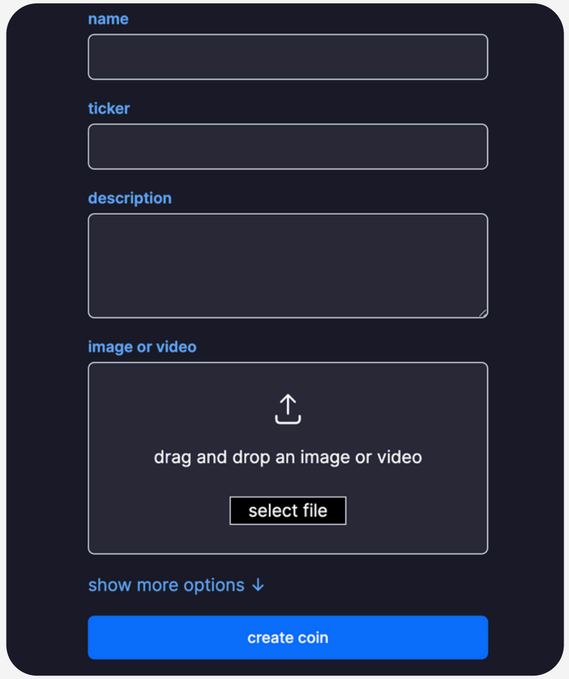
12 / 6

DYOR

Meme

The popular trend across blockchain ecosystem, especially on Solana

pump.fun



SPL Token Standard vs ERC-20

name

ticker

description

Pump.fun

A meme launchpad on Solana network

Name	Revenue (24h)
1 Pump	$14.49m
2 Tether	$13.37m
3 Solana	$4.32m
4 Circle	$4.12m
5 Ethereum	$3.3m

24-hour revenue exceeds USDT

Hits All-Time High Revenue of $82.8M in November

“Ethereum is dead”

?

Meme

Some popular meme on Solana

created by HrHJpu 1 month ago
market cap: $1.2B [⚡👑]

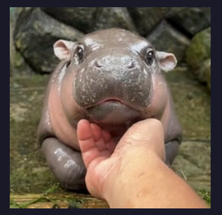
replies: 3880

Peanut the Squirrel (Pnut): It's ou r job to help save peanut the squir rel! Sign the petition!

created by EZX7c1 2 months ago
market cap: $737.9M [⚡👑]

replies: 2123

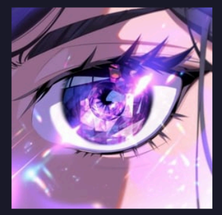
Goatseus Maximus (GOAT): First meme created by @truth_terminal. Goatseus Maximus will fulfill the pr ophecies of the ancient memeers.



created by Btxty8 3 months ago
market cap: $538.0M [⚡👑]

replies: 997

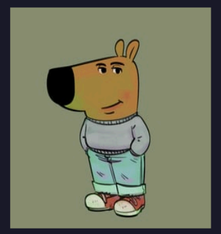
Moo Deng (MOODENG): just a vira l lil hippo



created by 6P2XrF 1 month ago
market cap: $535.3M [⚡👑]

replies: 1747

Act I : The AI Prophecy (ACT): Act I : The AI Prophecy



created by DTQQf6 2 months ago
market cap: $391.3M [⚡👑]

replies: 1315

Just a chill guy (CHILLGUY): I kno w I'm supposed to be a chill guy a nd low-key not really care about a nything but I'm tired of trying to be someone that I'm not I want you to think of something right now that makes you happy that thing you s ee the thing that lights you up, Ch ase that all of your soul chase that because it's easy to brush off life's potential and I'm not trying to say t

created by BT2sdw 4 months ago
market cap: $343.8M [⚡👑]

replies: 1394

FWOG (FWOG): In the ashes a co mmunity emerged, a new flog, a m ore based flog, a FWOG FWOG ha s no dev. It is the community.

Meme

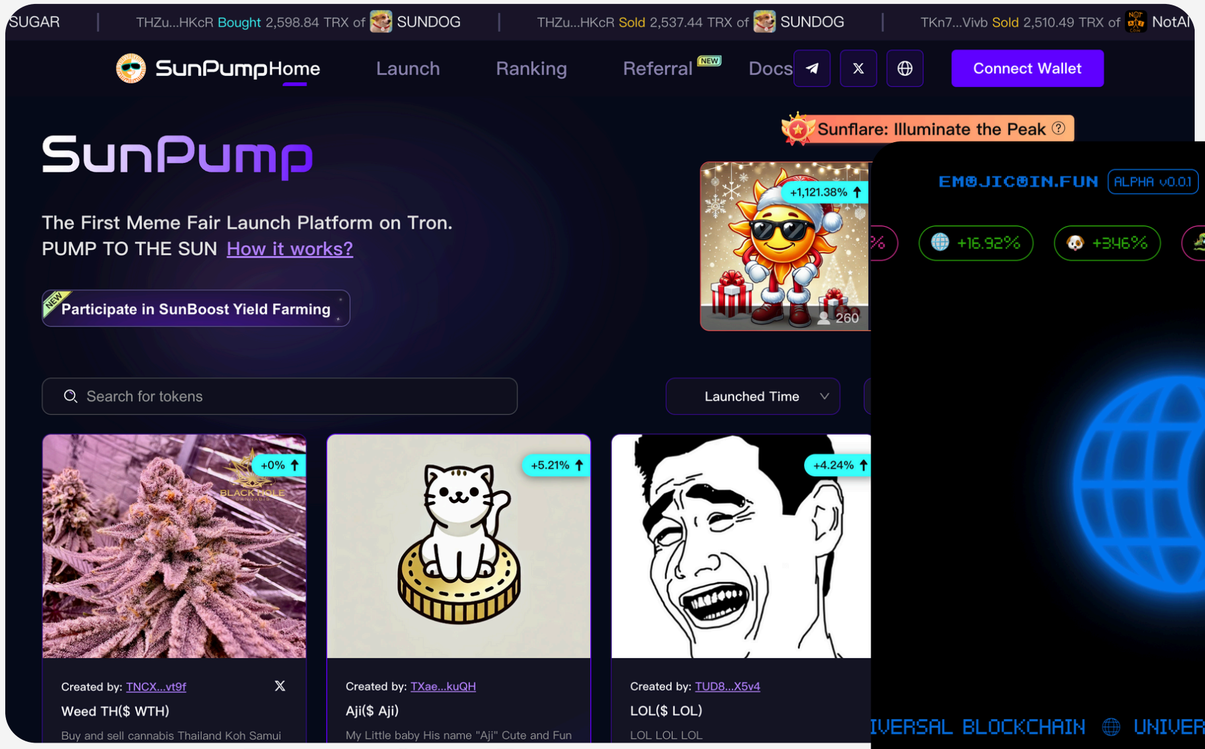
Some popular meme on Solana

- Decentralized Science (DeSci) - Vitalik & CZ
- RIF, URO

Pump.Science通過使用Pump.Fun來交易潛在延長壽命化合物的代幣。當一個代幣達到1萬美元市值時，該化合物的實驗數據就會定期在Pump.Science上進行直播。代幣持有者和投機者可以根據他們對藥物對壽命影響的預測繼續交易代幣，從而協助該化合物的持續研究。

More on meme

There are similar product on distinct chains

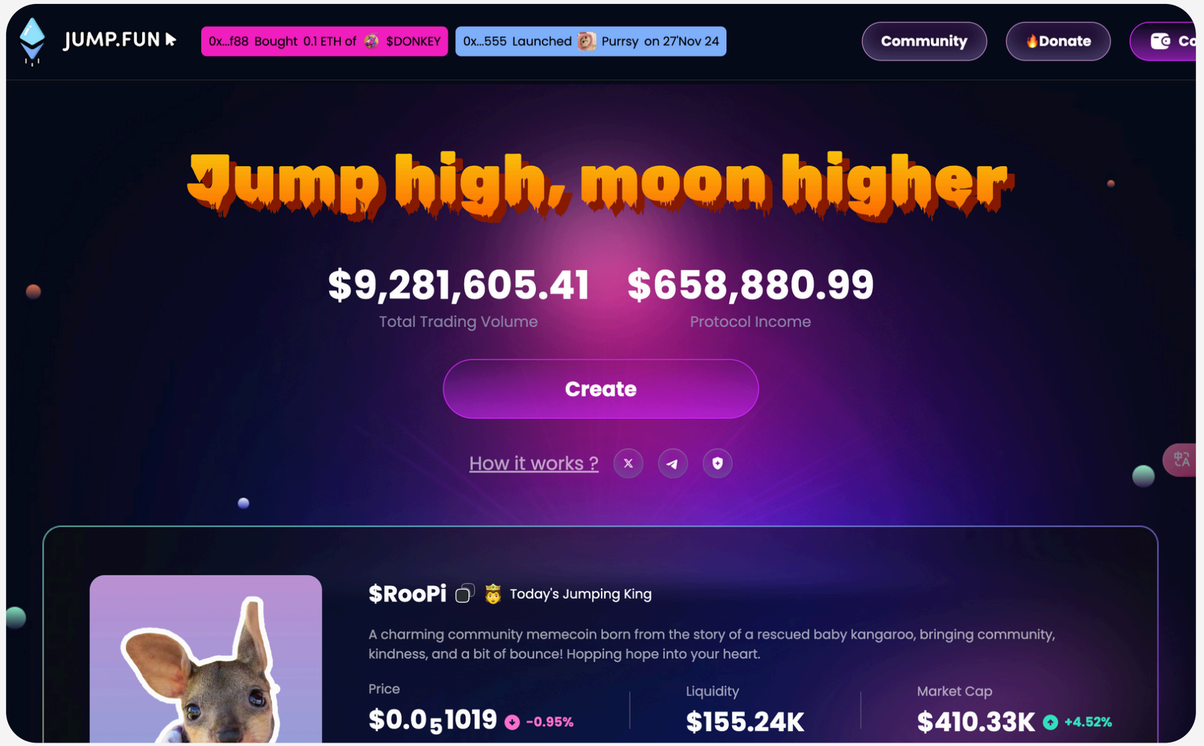


Tron: Sun Pump

Aptos: Emoji Fun Pump

More on meme

There are similar product on distinct chains



ETH: Jump Fun

Meme

Some problem arise when the live stream feature is out

脫衣熱舞、直播健身、阿□關鐵籠：迷因幣發行平台 Pump.fun 激發「博眼球」亂象

迷因幣發行平台 Pump.fun 上線至今，以造就了許多暴富迷因幣。現在除了有許多交易員在該平台「打金狗」尋求暴富以外，也有不少人選擇自己在平台上發行迷因幣。 然而，每天發行的迷因幣數量□多，根據 Dune 的數據顯示，過去 24 小時在該平台上發行的迷...

桑幣區識 Zombit / Nov 22, 2024

Pump not fun！迷因平台「暗網化」，暴力、槍枝、自虐樣樣來

繼我們上次整理了 Pump fun 那些為了吸引交易員所做出的吸睛行為之後，該平台的生態出現了極大的變化，發幣者抬高代幣市□的行為，已漸漸從「吸睛」轉變為「威脅」。 根據 X 用戶分享的資訊顯示，有許多為了錢不惜一切代價的人，利用 Pump fun 的直播功...

桑幣區識 Zombit / Nov 25, 2024

Most meme coins lack intrinsic value, and their market capitalization can drop to zero within a single day.

Meme

Pump.fun has decided to suspend the live stream feature until a proper censorship process is established.

- Pump.fun took 33% hit to revenue after memecoin site stopped livestreaming
- Pump.fun weekly revenue drops 66% after livestream controversy

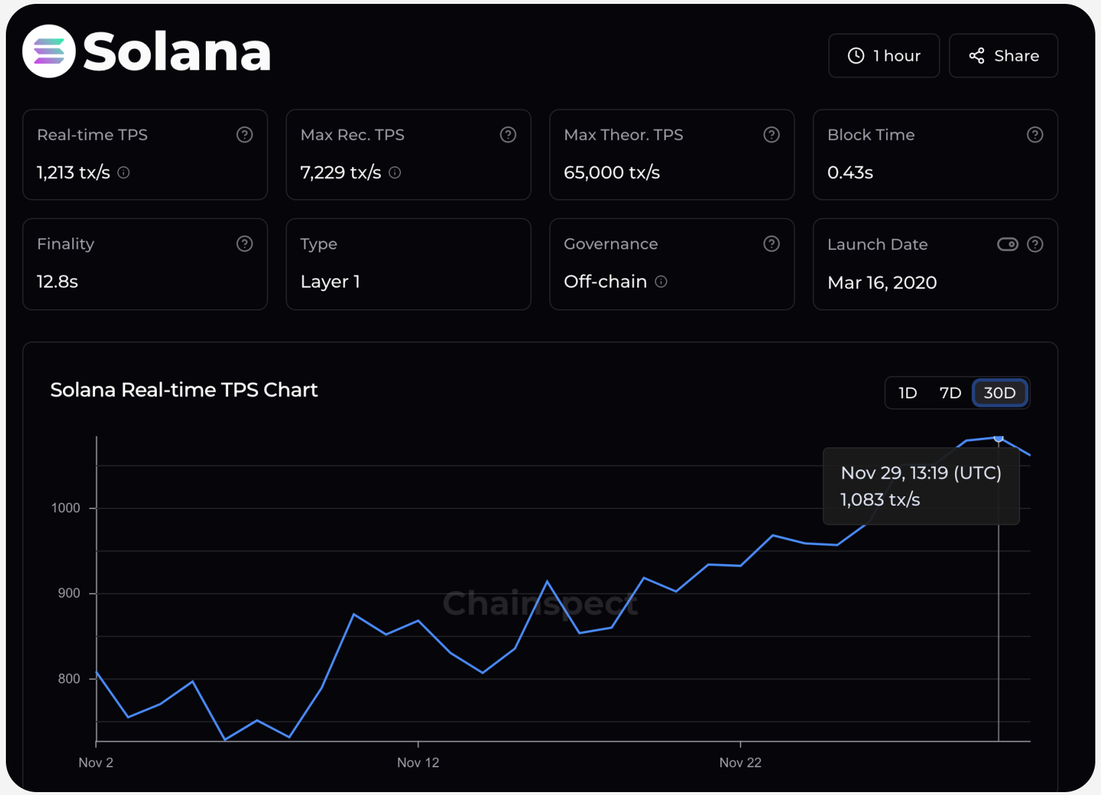
Meme印鈔機》Pump.fun手續費大賺8900萬美元，收入狠超Uniswap

統計數據顯示截至 8 月 10 日，在 Solana 迷因幣發行平台 Pump.fun 上推出的迷因幣共計有 170 萬個，但其中成功部署 Raydium 的成功率低至 1.4%。但仍不影響官方獲得大量收入。 （前情提要：Pump.fun開□迷因幣極致PvP：免費發行、市□達標再送…

動區動趨-最具影響力的區塊鏈新聞媒體 / Aug 14, 2024

Solana

The user experience is smooth



- Blazing fast Layer 1 blockchain
  - MAX TPS: 7229 tx/s
  - Real-Time TPS: 1213 tx/s
- Low gas fee
- No liquidity fragmentation issue
- Integration in Web2 environment

Solana

The user experience is smooth

MAX TPS: 62 tx / s

Real-Time TPS: 16 tx / s

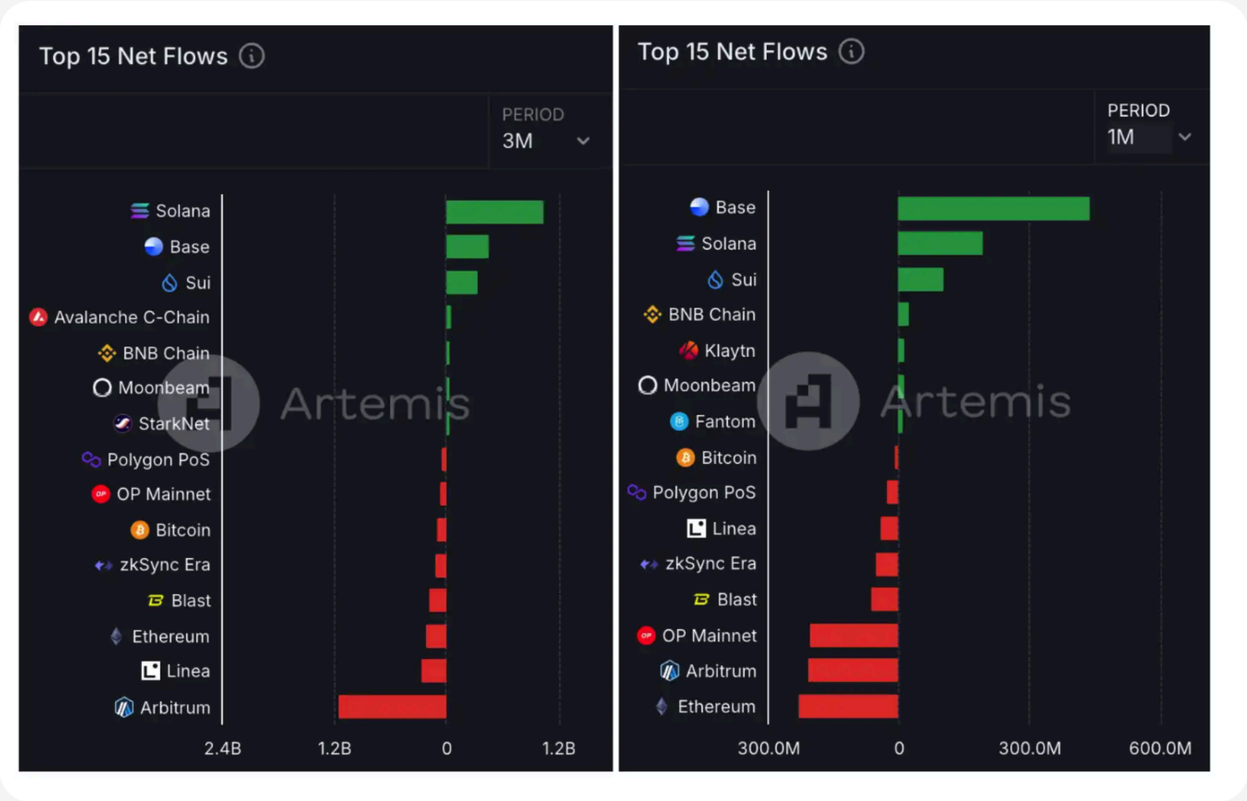
Solana

More than meme, focus on RWA

- Some other realm on Solana: RWA (Real World Asset), PayFi
  - RWA: Ondo Finance, Sky (USDS)
  - PayFi:
    - from “Buy Now, Pay Late” to “Buy Now, Pay Never”
    - Huma Finance: financing of global payments, with instant access to liquidity anywhere, anytime

AI Meme

From Solana to Base



Clanker

A more convenient way to launch meme

- Some popular meme on Base chain: LUM, ANON, CLANKER, BUG
- Tag Clanker at Farcaster, it will generate a meme for you
- Some old AI meme coin
  - GOAT: Terminal of Truths
  - ACT: The AI Prophecy

近期最熱的 AI Agent 賽道全解：迷因幣、發行平台與基礎設施

AI Agents 成為本輪牛市的熱門賽道，本文提供該賽道的發展趨勢、發行平台與基礎設施，並分析了些代幣可能是下一個上線幣安的 AI Agents 代幣。（前情提要：解讀 Crypto+AI Agents：下個十億用戶的真正突破口？）（背景補充：Virtual Protoc...

動區動趨-最具影響力的區塊鏈新聞媒體 / Dec 1, 2024

Freysa

an AI agent

- Two Operations
  - approveTransfer
  - rejectTransfer
- After 481 unsuccessful attempts, a participant convinced the AI bot Freysa to transfer a $47,000 prize pool.

人類成功說服AI轉移4.7萬美元獎金，AI是怎麼「被騙」的？

195 名參賽者參與了一場由人工智慧（AI）機器人Freysa （芙蕾莎）守護的虛擬獎金池挑戰，最終一用戶成功說服Freysa 轉移出價□4.7 萬美元的資金。

PANews

Hyperliquid

The Hyperliquid L1 is custom built around a performant derivatives exchange as the flagship native component

- A derivatives exchanges: On-chain Binance
- Will convert to a Layer 1
- EVM architecture with Solana speed

Name	1m Change	Volume (24h)	Volume (7d)	% of total	Cumulative volume
1 Hyperliquid	+816%	$4.539b	$19.24b	50.14%	$439.37b
2 Ethereum	+41.05%	$1.075b	$8.238b	11.87%	$1.511t
3 Base	+52.96%	$758.17m	$5.645b	8.38%	$89.072b
4 Solana	-9.44%	$678.67m	$7.637b	7.50%	$219.716b
5 dYdX	+369%	$629.29m	$3.606b	6.95%	$225.655b
6 Arbitrum	-10.40%	$473.43m	$4.812b	5.23%	$639.681b
7 BSC	+229%	$180.69m	$849.59m	2.00%	$370.028b
8 Blast	-28.21%	$176.73m	$2.094b	1.95%	$214.861b

Hyperliquid

Hype on hyperliquid

速覽Hyperliquid空投數據：平均空投2915個HYPE，價□近2萬美金

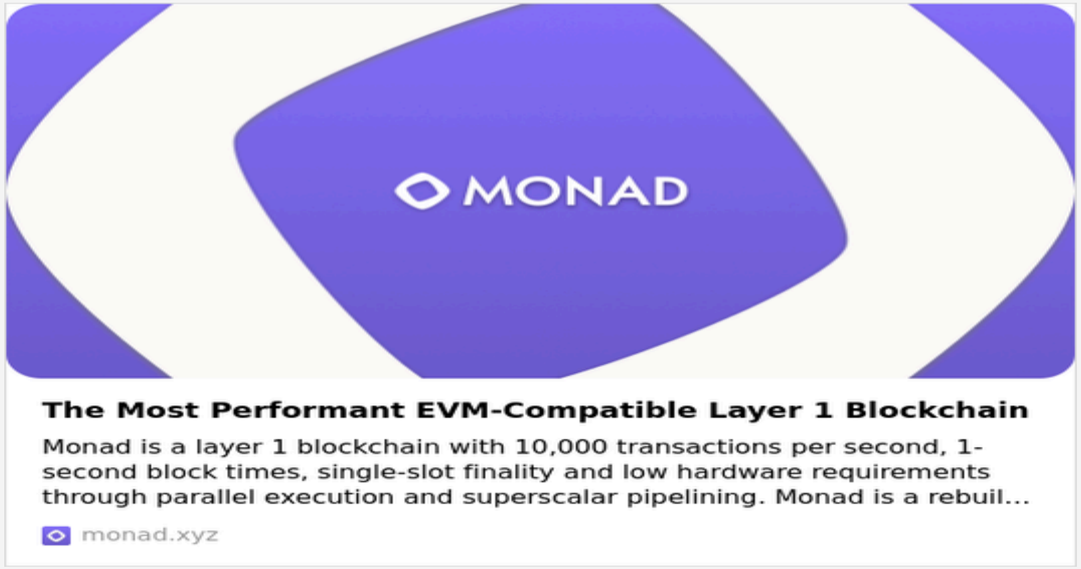
全網都在曬戰績，繼Arbitrum 空投後最大造富事件？

PANews

- The largest airdrop in history
- No VC intervention
- Community first
- Current market cap exceeds Aave

More on EVM Ecosystem

The Ethereum Virtual Machine (EVM) offers a robust developer ecosystem but faces limitations in transaction speed.



Monad

MegaETH

Law & SEC

XRP returns to 3rd-largest crypto after 4-year battle with SEC

XRP spent four years as the seventh largest cryptocurrency by market cap before returning as the most-valued coin after Bitcoin and Ether in December 2024.

Some Observation

Time	Market	Twitter
2 week ago	Meme is hot	ETH is dead, Solana becomes the #1 blockchain, everyone mad at Vitalik and Ethereum foundation
1 Week ago	AI Meme on Base	Bullish on AI Meme, AI is the next wave for crypto, pure meme is useless. Etheruem is back, Alt season coming
This Week	XRP Law Result	XRP is going to flip ETH and Bitcoin

Layer 2 & Cross Chain Bridge

StarkEx

StarkEx Bug Bounties

Find bugs and vulnerabilities on StarkEx and get paid up to $1,000,000.

Immunefi

Ecosystem

StarkWare	Company that operates StarkNet & StarkEx
StarkNet	Layer 2 network utilizing the zk-rollup technique, where the sequencer batches transactions and forwards them for proof.
StarkEx	StarkEx is a standalone, customizable Layer-2 SAAS for exchanges, utilizing the STARK proof system to achieve significant scaling.
STARK	A proof system that enables the proving and verification of computations

Reference: STARKs, StarkEx, and Starknet, Stark Ecosystem

Introduction

Introduction

A Layer-2 scalability engine, live on Ethereum Mainnet.

Rollup

Based on validity proofs, using STARK proof crypto system

- Transactions are validated off-chain by the StarkEx Prover and then verified on-chain to ensure only valid transactions are committed.

Comparison

Fraud Proof (Optimistic Proof)

Validity Proof (ZK Proof): Finality Time, L1 Security, Data Access

Reference: Rollup Category, Rollup & Data Availability, L2 Comparison, L2 Evolution

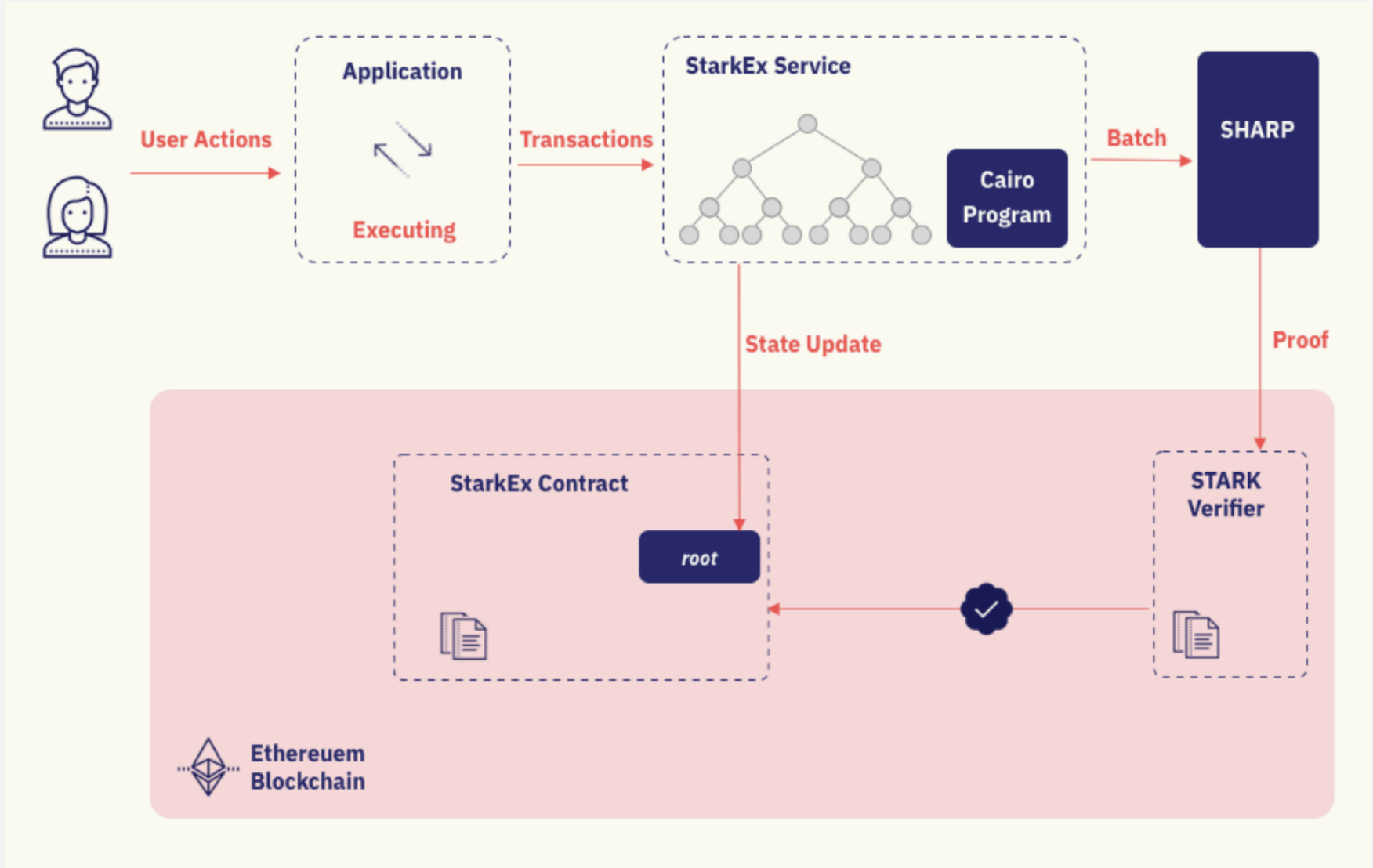
Data Availability

There are three modes for data availability.

ZK Rollup	Vault balances are published onchain as calldata. The ZK-Rollup provides built-in trustlessness.
Validium	Vault balances are stored off-chain by the DACs, which maintain Validium vault balances to ensure user data accessibility.
Volition	Allows integration of both ZK-Rollup and Validium vaults in your application. Users choose vault range for each asset they own.

Reference: Rollup & Data Availability, Data Availability, Validium

Workflow Overview



Application

Operator

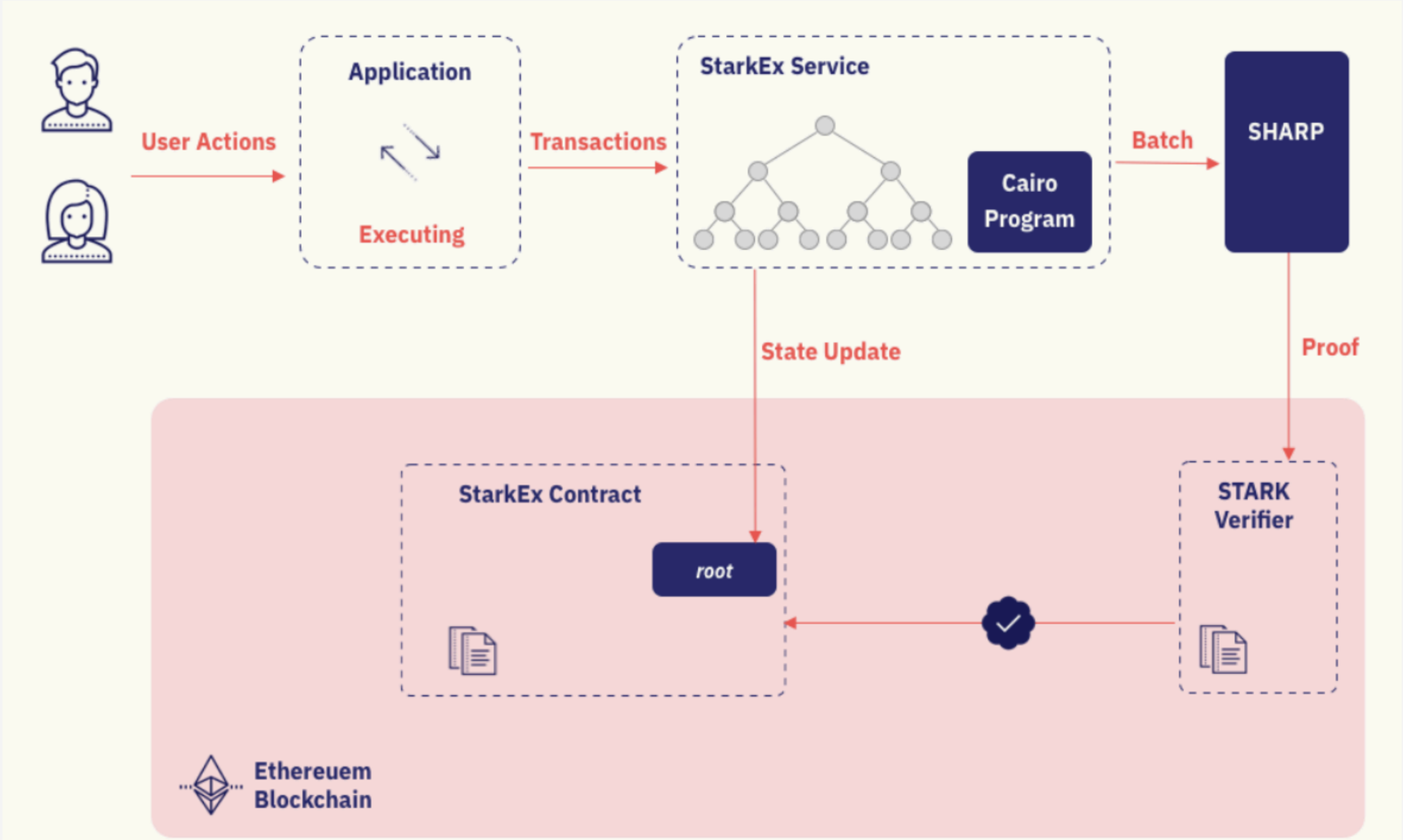
StarkEx Service

SHARP

STARK Verifier

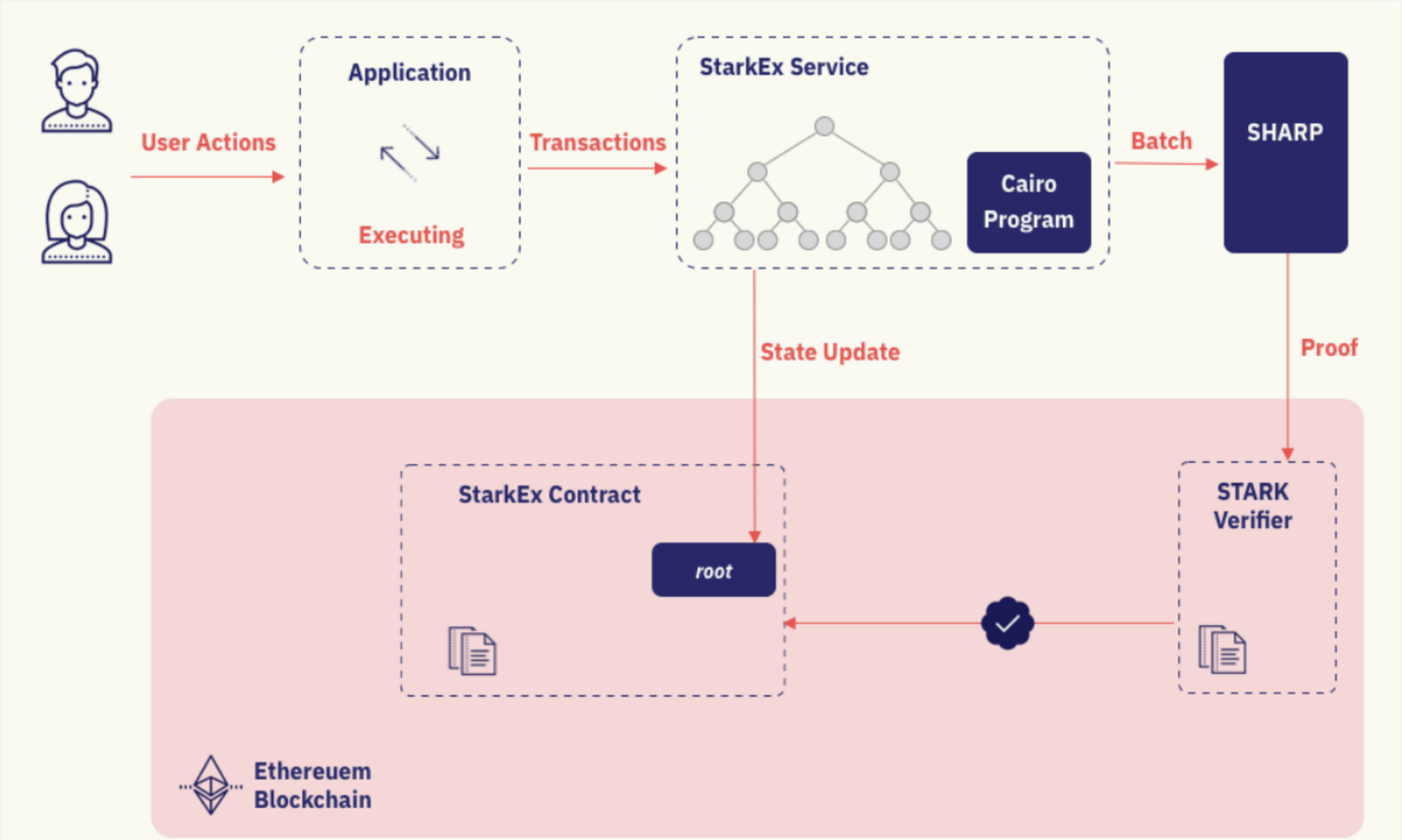
StarEx Contract

Workflow Overview



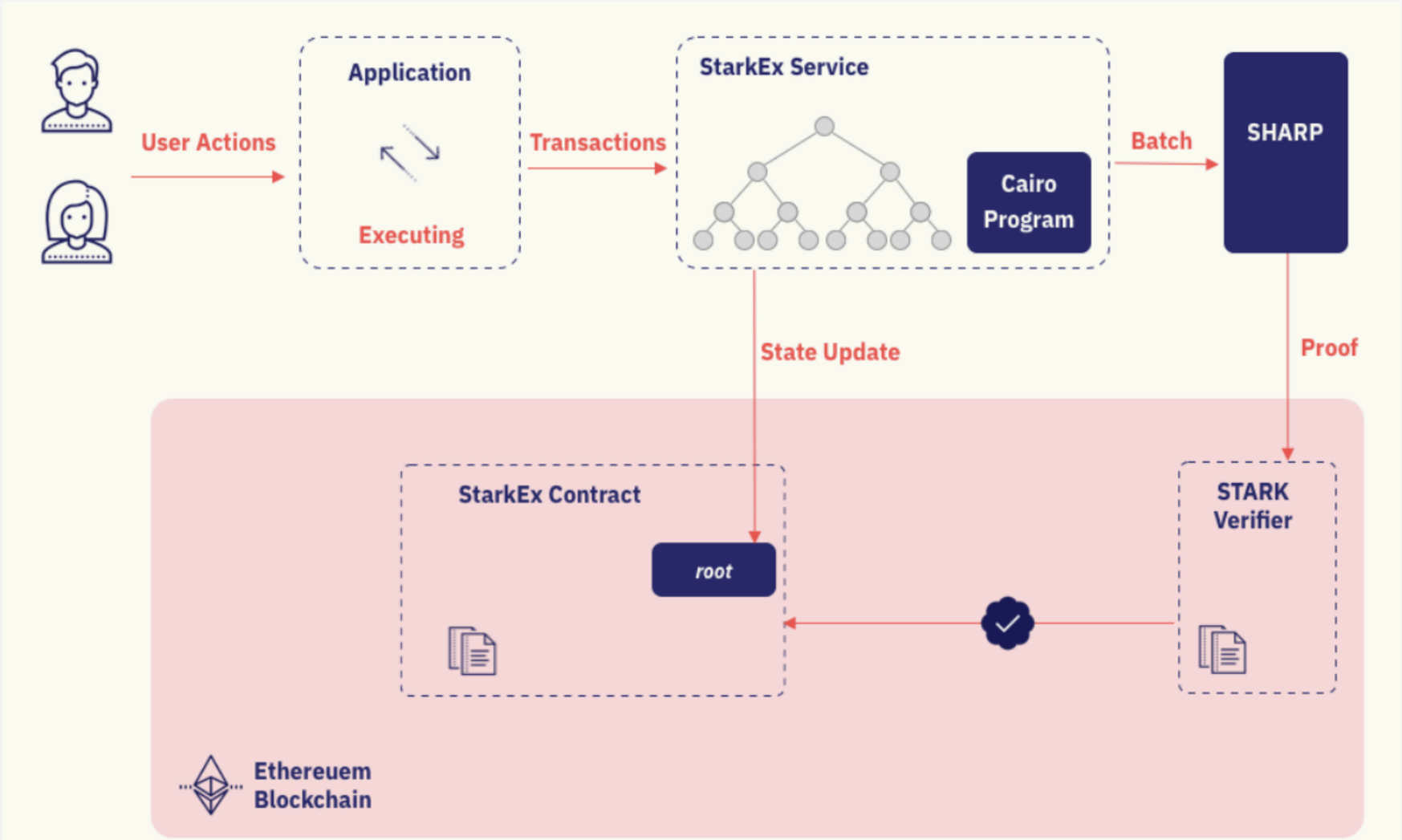
Step 1: Application executes transaction and sends to StarkEx service

Workflow Overview



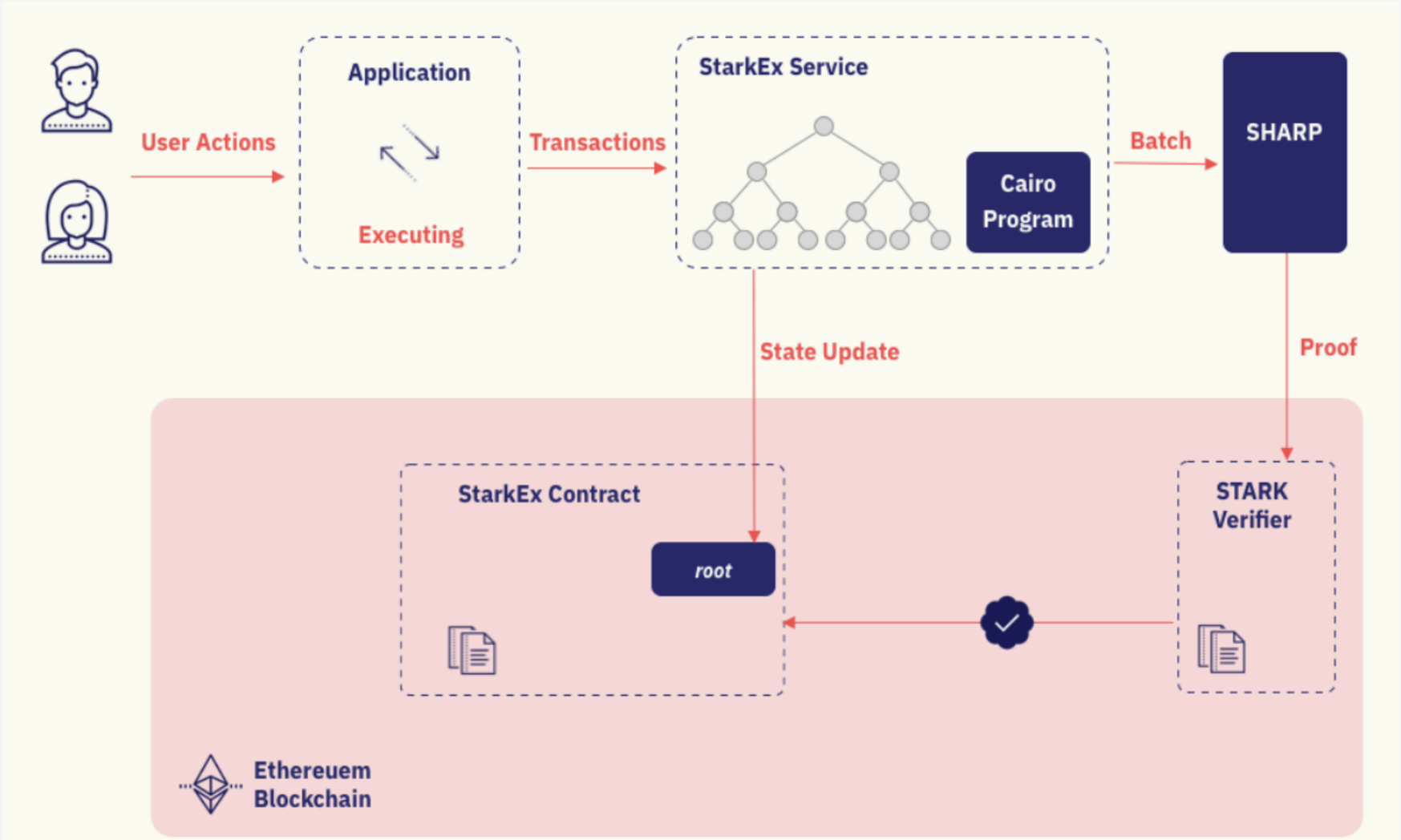
Step 2: StarkEx batches transaction and sends the batch to SHARP

Workflow Overview



Step 3: SHARP sends the STARK proof to onchain STARK Verifier

Workflow Overview

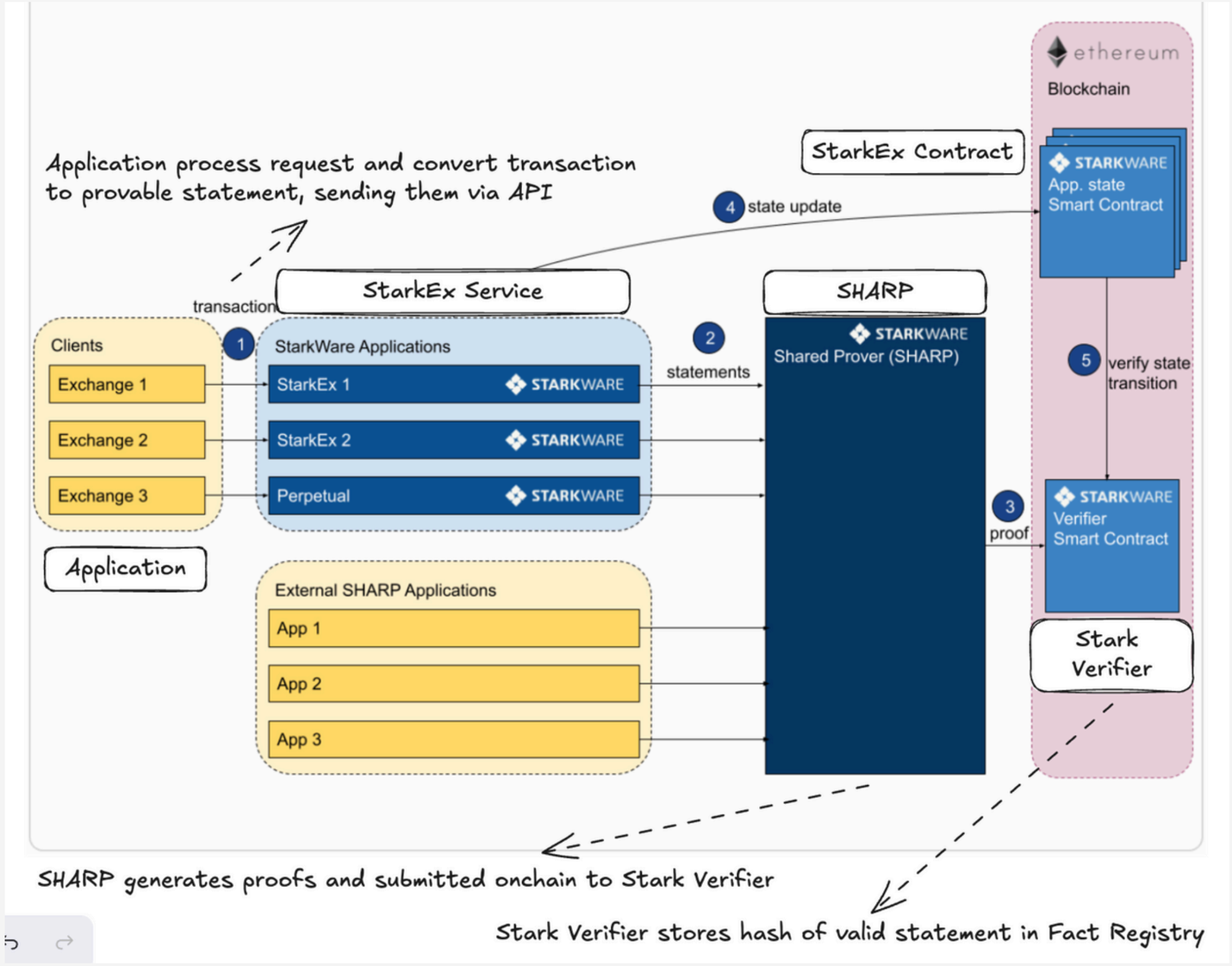


Step 4: StarkEx sends onchain update transaction to StarkEx contract if proof is valid

Component

Application	Processes user transactions and determines the business logic and execution order.
Operator	Entity that owns and responsible for Application
StarkEx Service	Batching operations and updating the system state. Each batch is sent as a Cairo execution trace to SHARP for verification.
SHARP	A shared proving service for Cairo programs processes and validates multiple proof requests, allowing proof sharing.
STARK Verifier	Receives and verifies a state-update validity proof.
StarEx Contract	1. Handle state updates 2. deposits and withdrawals

General Architecture



Step 1: Process requests, convert to provable statements, and send to SHARP.

Step 2: Transaction are batched together into a single statement.

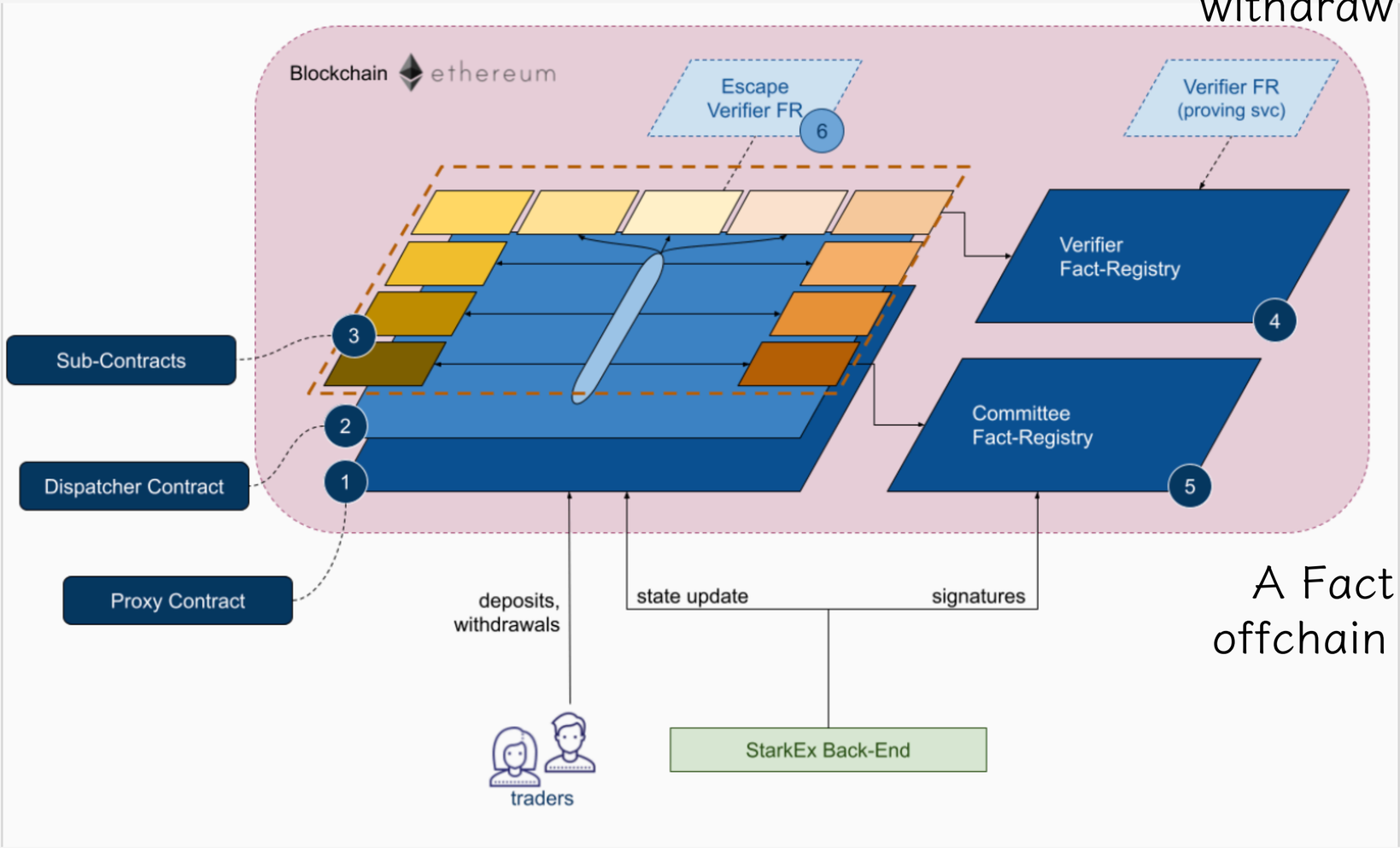
Step 3: SHARP transmits the proof to the onchain Verifier smart contract.

Step 4: Apply the state transition on the customer application's smart contract.

Step 5: Customer application's smart contract verifies that the transition statement is registered.

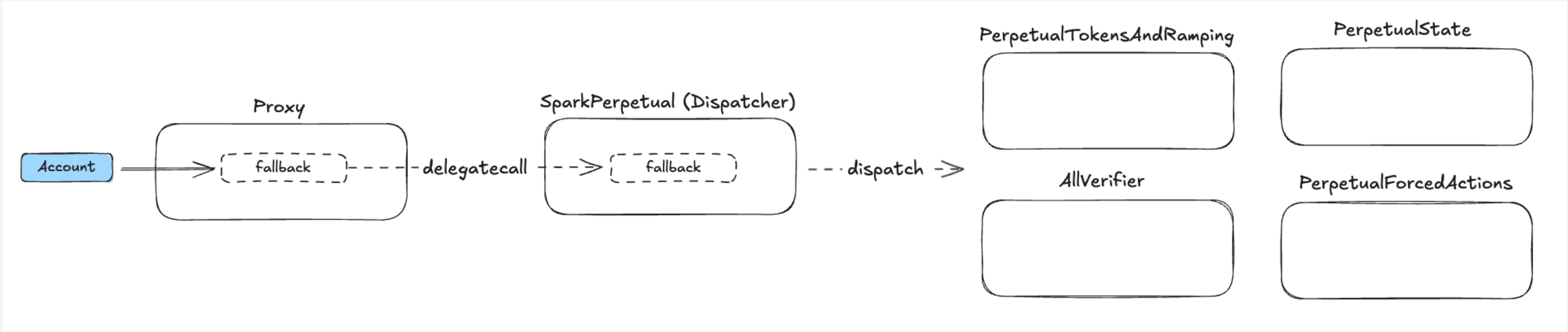
Contract Architecture

Allows traders to prove ownership and withdraw funds from a frozen contract



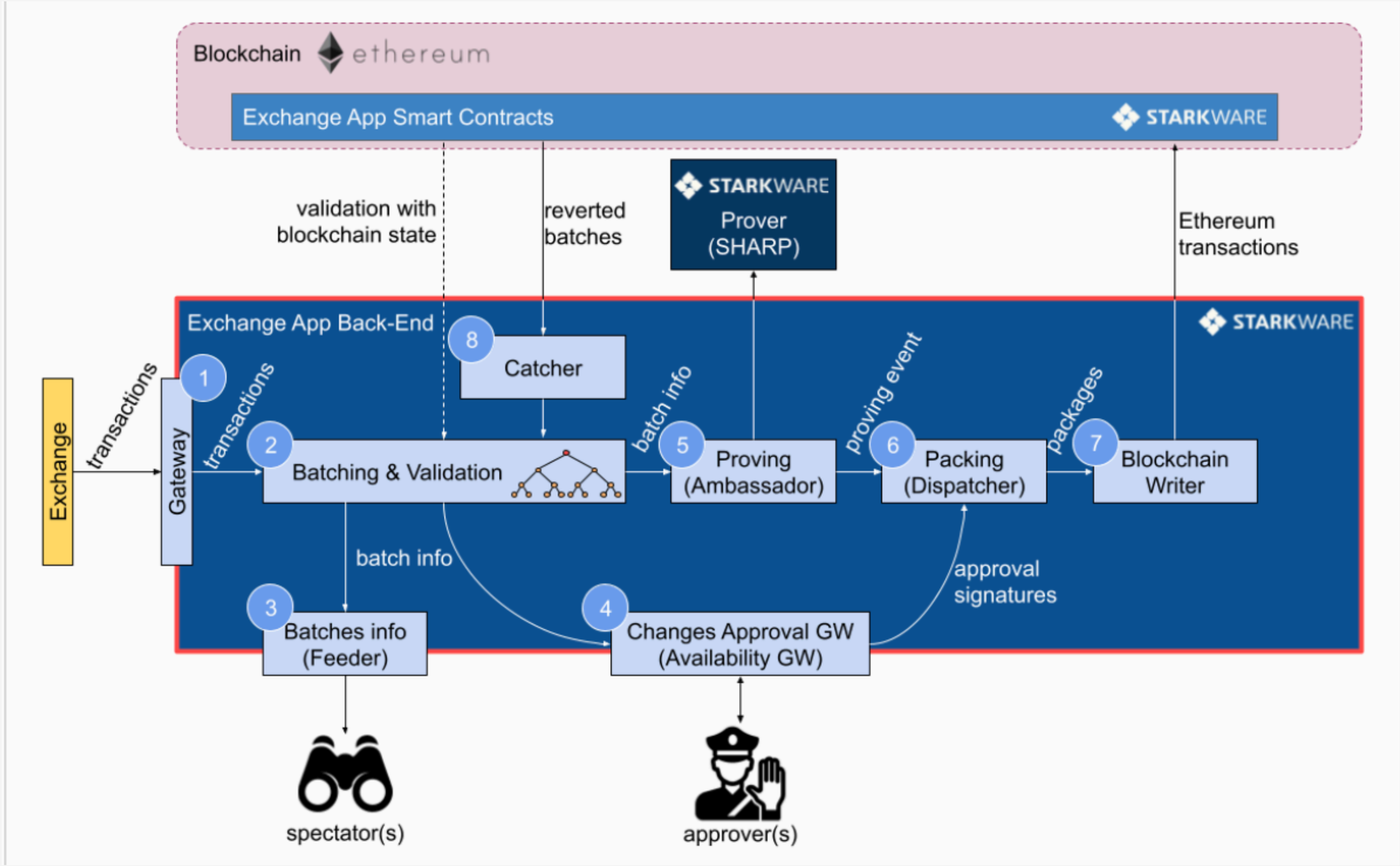
A Fact Registry enforcing custom offchain approval of state transitions

Contract Architecture



- PerpetualTokensAndRamping: deposit / withdraw
- PerpetualState: updateState / escape
- AllVerifier: registerVerifier / removeVerifier
- PerpetualForcedActions: forced withdraw / forced trade

StarkEx Service Architecture



Backend Architecture

Gateway: Receives transactions from the application and validates them based on stateless criteria.

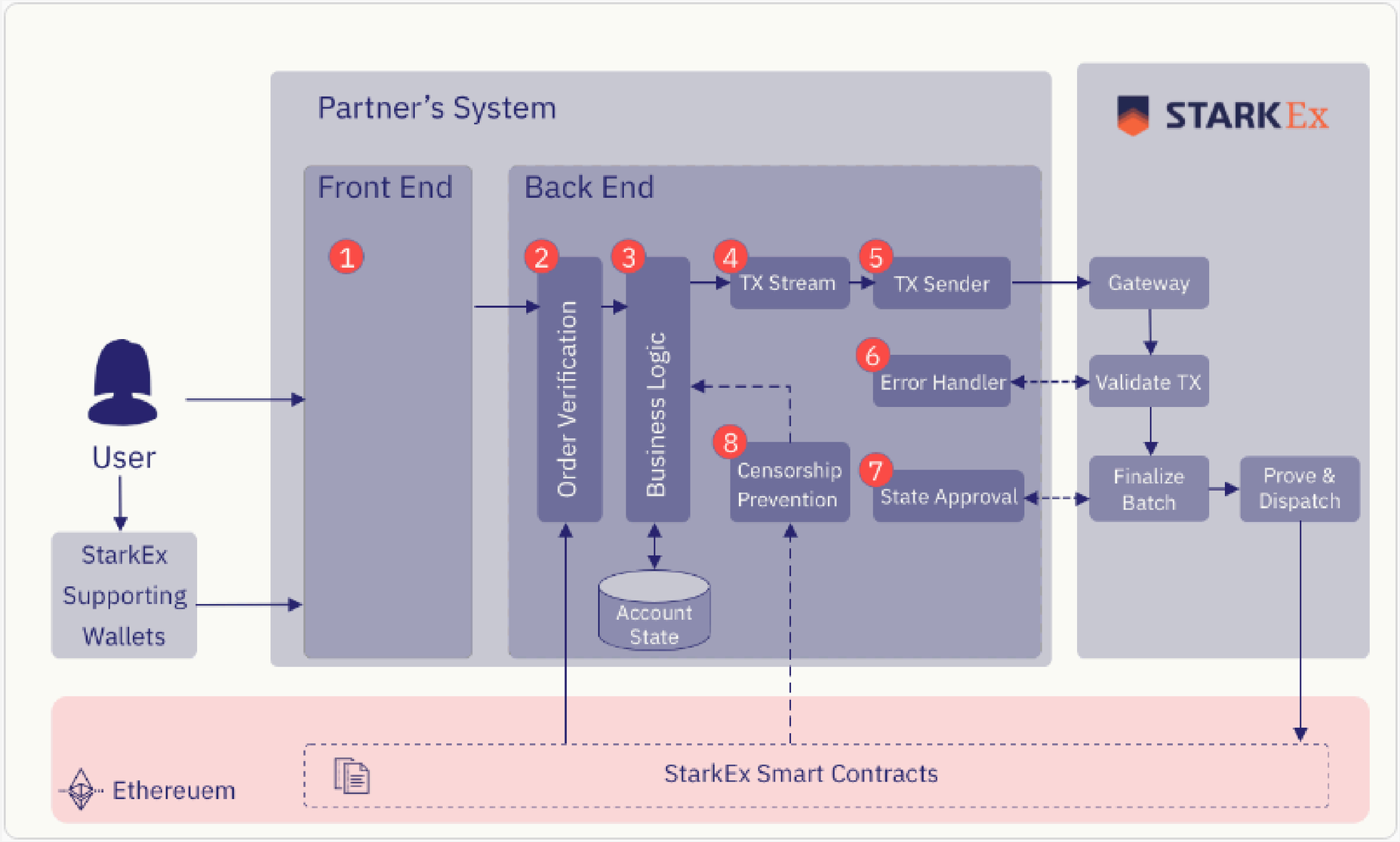
Batcher: Collects transactions into a batch and validates them -> depends on transaction order, chain of batch, if error occurs, subsequent batches are based on the last valid one.

Free Gateway: Provides external parties with information on verified batches and their transaction lists.

Availability Gateway: Custom logic approves batch submissions only when a sufficient quorum of a predefined committee approves the batch.

Ambassador: Submit the batch to Cairo program as a job to SHARP -> combines claims into one proof

Partner Integration



Offchain State

Balances Tree — A Merkle Tree with leaves as StarkEx Vaults, each containing a unique Stark key to identify users in the offchain state.

Vault Structure: starKey, assetId, amount

Order Tree — Prevents the operator from replaying transactions in the system

- A leaf in the Orders tree represents an executed StarkEx order.
- Each leaf includes an ID, which is a hash of the signed transaction request, and a value indicating the fulfilled amount of the order.
- If an operator attempts to resubmit an order, StarkEx validates the transaction by ensuring the associated leaf's value is zero.
- his mechanism helps StarkEx track previously minted assets.

Vault Structure

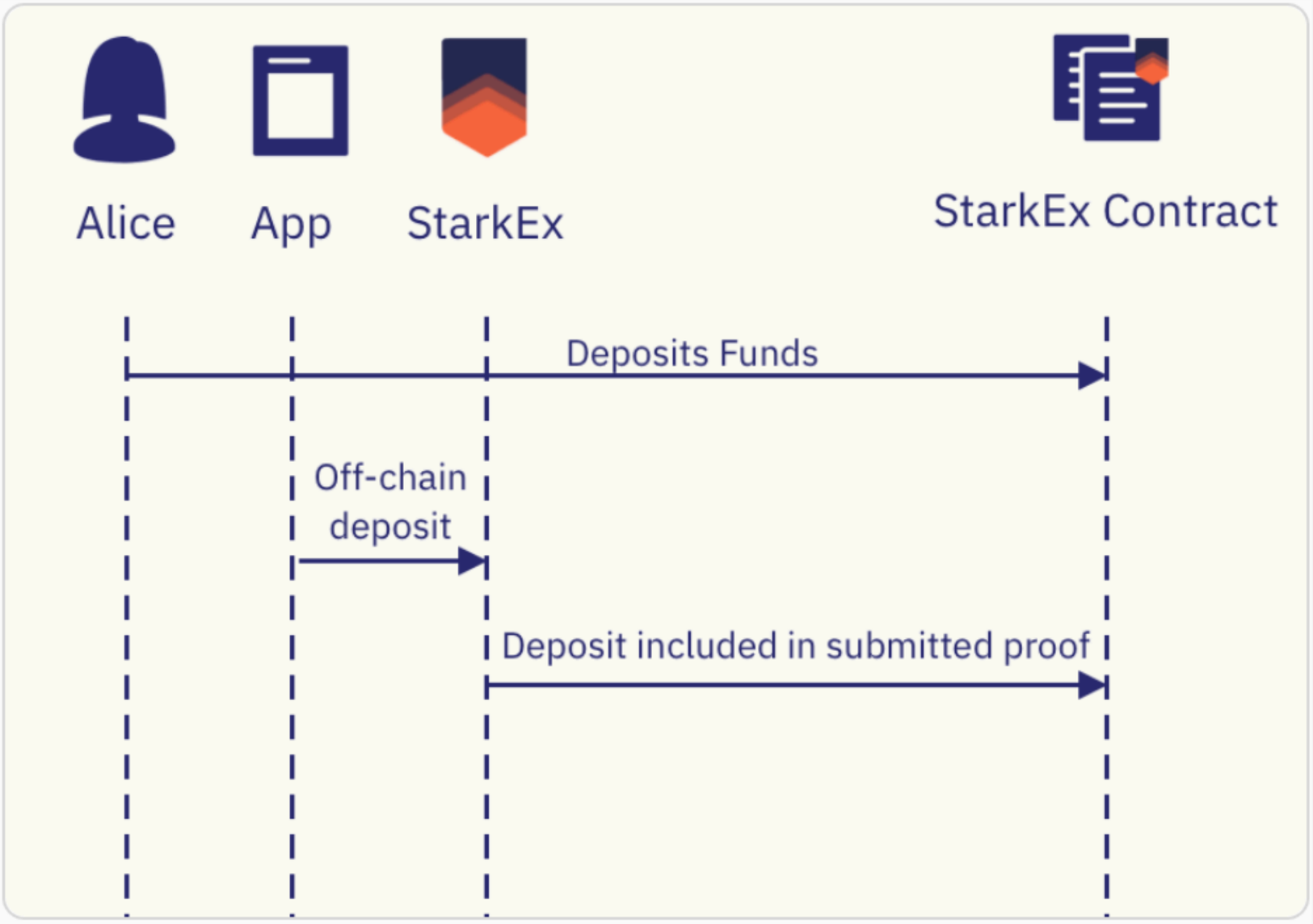
Balance Tree is a Merkle Tree with leaves as StarkEx Vaults, each containing a unique Stark key to identify users in the offchain state.

starKey	the public Stark key of the vault's owner. Transfers and trades from this vault must be signed with this key.
assetId	ETH, ERC-20, , ERC-721, ERC-1155 Mintable ERC-20, Mintable ERC-721, Mintable ERC-1155
amount	Ethereum uses 256-bit numbers for token quantities, while StarkEx uses 64-bit numbers for efficiency.Transaction signatures must convert Ethereum quantities to StarkEx's 64-bit format.

User Interaction

Deposit	Deposit to the on-chain contract and get the off-chain balance
Withdraw	Reduce the off-chain vault balance and get token on-chain
Trade	Include single / multi asset trade operation, not support partial fullfilled
Transfer	Transfer token from A vault to B vault
Cond. Transfer	Off-chain transfers that are valid only if an onchain event occurred.
Forced Action	Guarantee self custody of funds, thereby preventing censorship

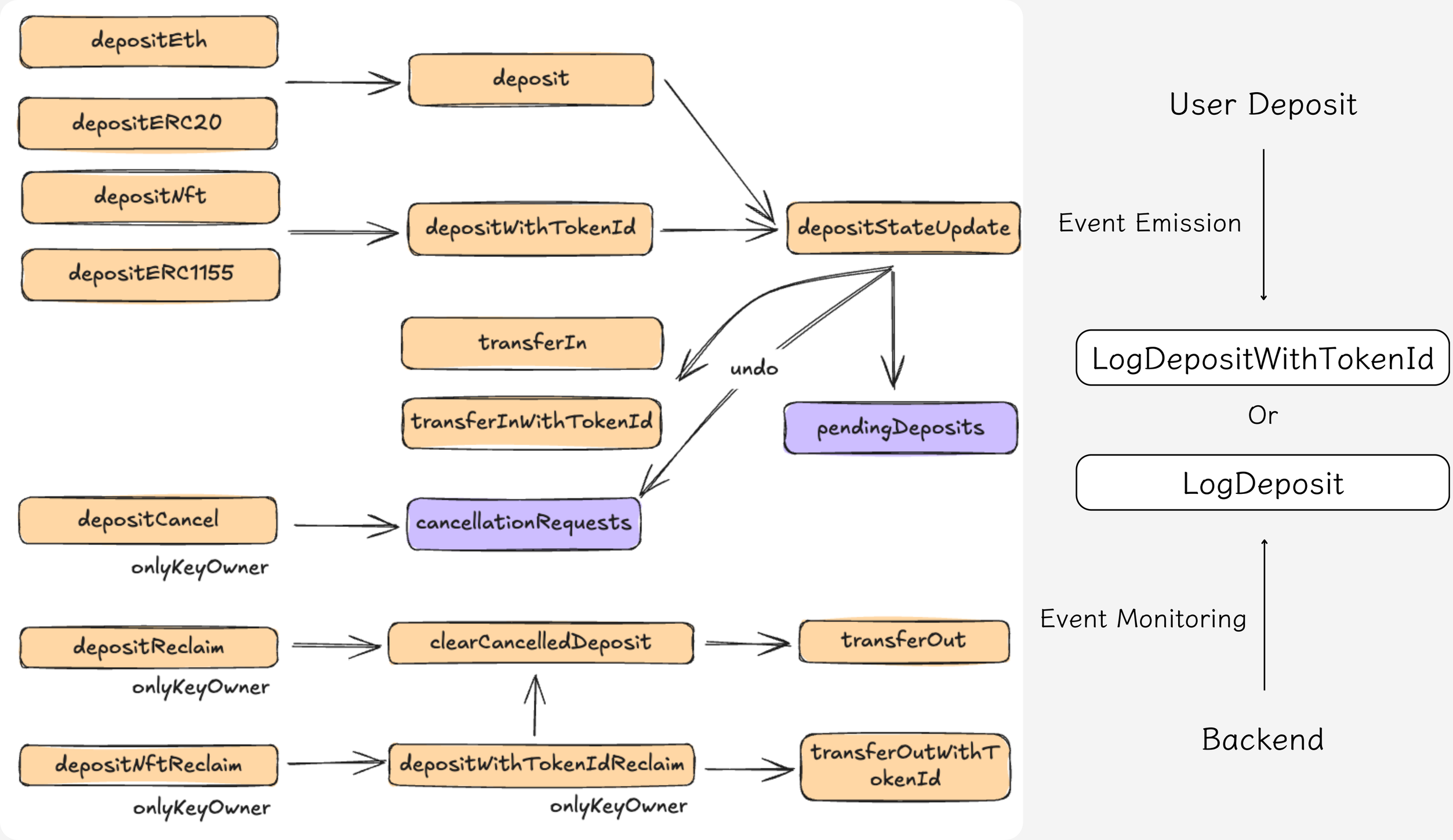
User Interaction - Deposit



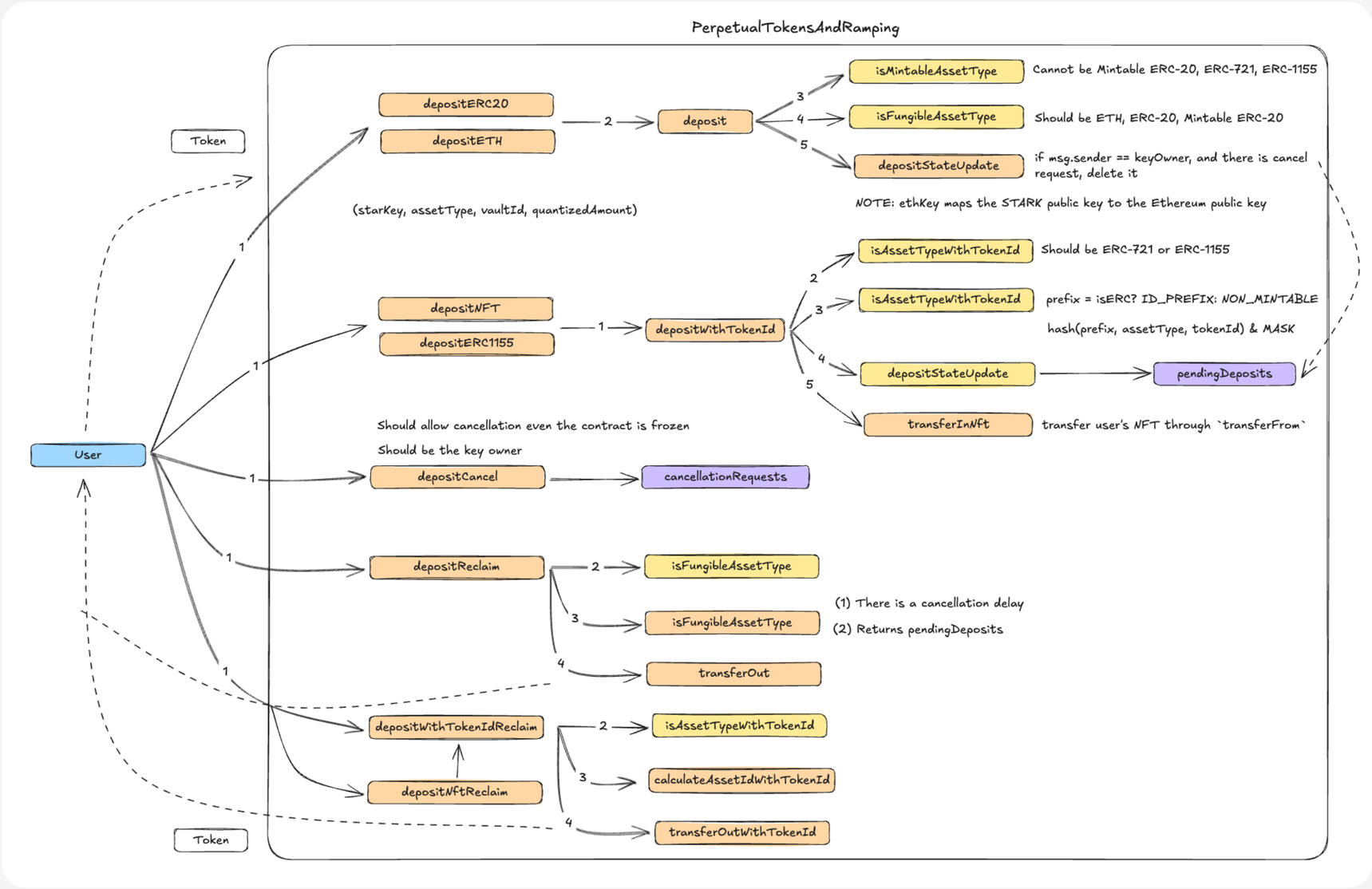
- Users first deposit funds into the StarkEx Contract.
- The backend service monitors the event and issues a request.
- The deposit is then included in the submitted proof and sent for verification.

User Interaction - Deposit

- Supported asset type: ETH, ERC-20, ERC-721, ERC-1155
- Deposit without token ID: depositEth, depositERC20 -> deposit
- Deposit with token ID: depositNft, depositERC1155 -> depositWithTokenId
- Users should first call `depositCancel` and then `depositReclaim` to withdraw tokens.
  - depositReclaim
  - depositWithTokenIdReclaim
  - depositNftReclaim
- Certain operations can only be done using an ethKey associated with that vault's starkKey.

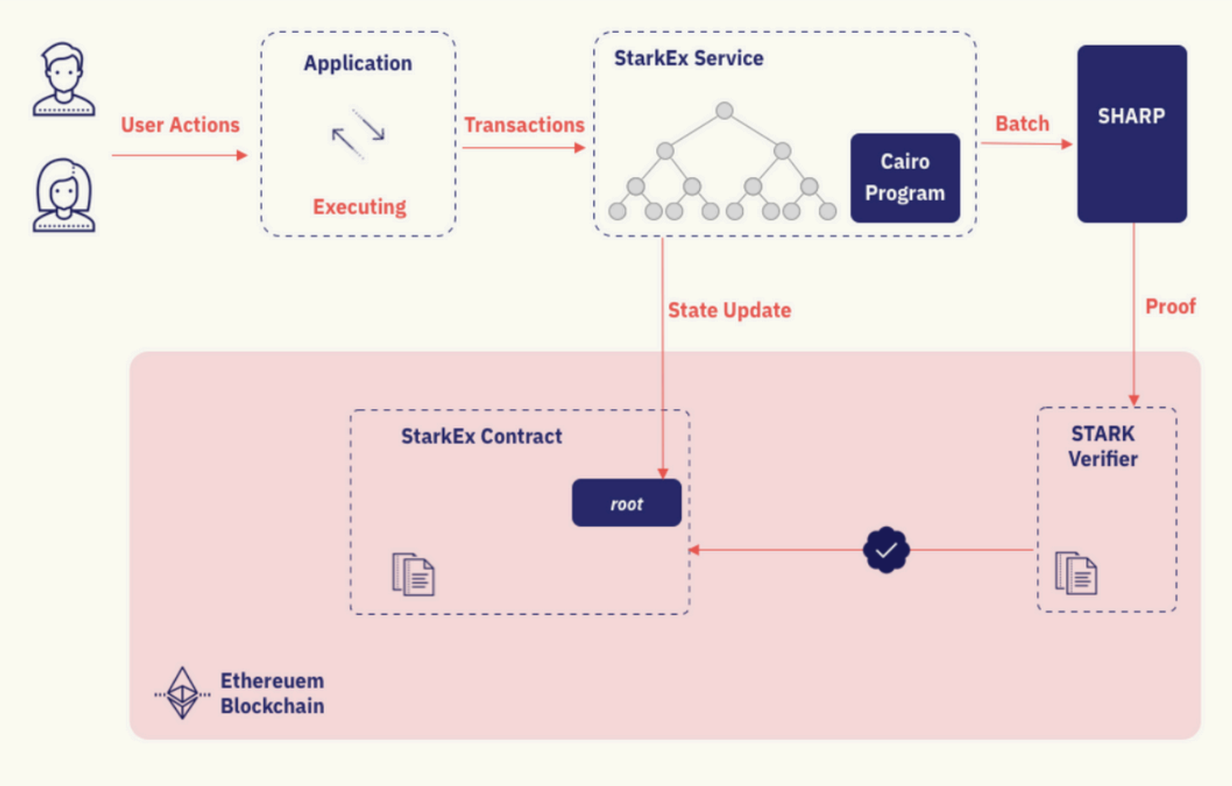

depositEth
depositERC20
depositNft
depositERC1155
deposit
depositWithTokenId
depositStateUpdate
transferIn
transferInWithTokenId
undo
pendingDeposits
depositCancel
onlyKeyOwner
cancellationRequests
depositReclaim
onlyKeyOwner
clearCancelledDeposit
transferOut
depositNftReclaim
onlyKeyOwner
depositWithTokenIdReclaim
onlyKeyOwner
transferOutWithTokenId
User Deposit
Event Emission
LogDepositWithTokenId
Or
LogDeposit
Event Monitoring
Backend

User Interaction - Deposit

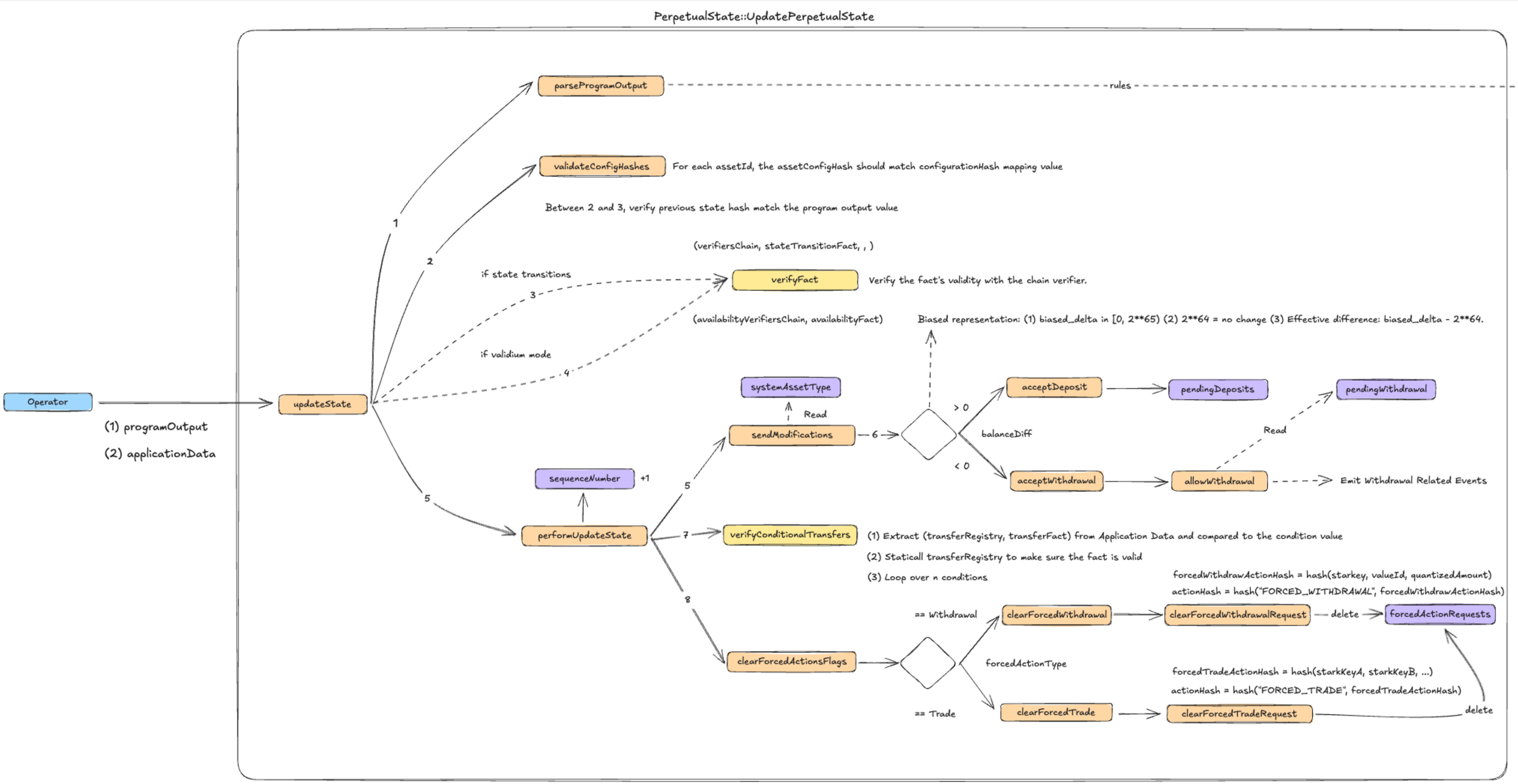


User Interaction - Deposit

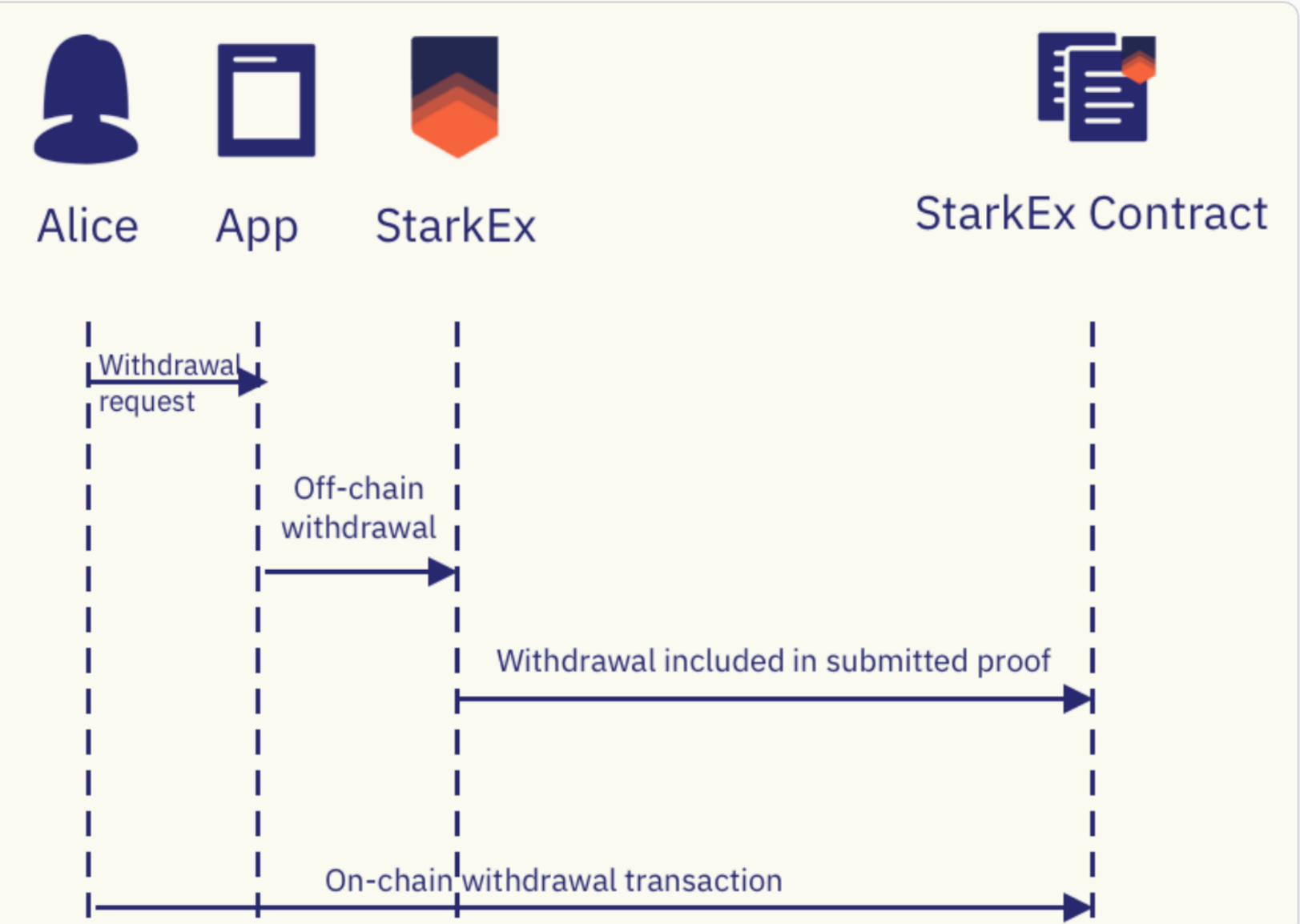
- The backend initiate an `add_transaction` API request with `DepositRequest` transaction type



- The state will be updated after the stark proof is verified on-chain.
- This update the `pendingDeposits` amount in the StarkEx Contract


PerpetualState::UpdatePerpetualState
Operator
(1) programOutput
(2) applicationData
updateState
parseProgramOutput
rules
validateConfigHashes
For each assetId, the assetConfigHash should match configurationHash mapping value
Between 2 and 3, verify previous state hash match the program output value
(verifiersChain, stateTransitionFact, ,)
verifyFact
Verify the fact's validity with the chain verifier.
if state transitions
if validium mode
(availabilityVerifiersChain, availabilityFact)
Biased representation: (1) biased_delta in [0, 2**65) (2) 2**64 = no change (3) Effective difference: biased_delta - 2**64.
1
2
3
4
5
systemAssetType
Read
sendModifications
6
> 0
< 0
balanceDiff
acceptDeposit
pendingDeposits
acceptWithdrawal
allowWithdrawal
Read
pendingWithdrawal
Emit Withdrawal Related Events
sequenceNumber
+1
performUpdateState
5
7
8
verifyConditionalTransfers
(1) Extract (transferRegistry, transferFact) from Application Data and compared to the condition value
(2) Staticall transferRegistry to make sure the fact is valid
(3) Loop over n conditions
clearForcedActionsFlags
== Withdrawal
== Trade
forcedActionType
clearForcedWithdrawal
clearForcedWithdrawalRequest
delete
forcedActionRequests
forcedWithdrawActionHash = hash(starkey, valueId, quantizedAmount)
actionHash = hash("FORCED_WITHDRAWAL", forcedWithdrawActionHash)
clearForcedTrade
clearForcedTradeRequest
delete
forcedTradeActionHash = hash(starkKeyA, starkKeyB, ...)
actionHash = hash("FORCED_TRADE", forcedTradeActionHash)

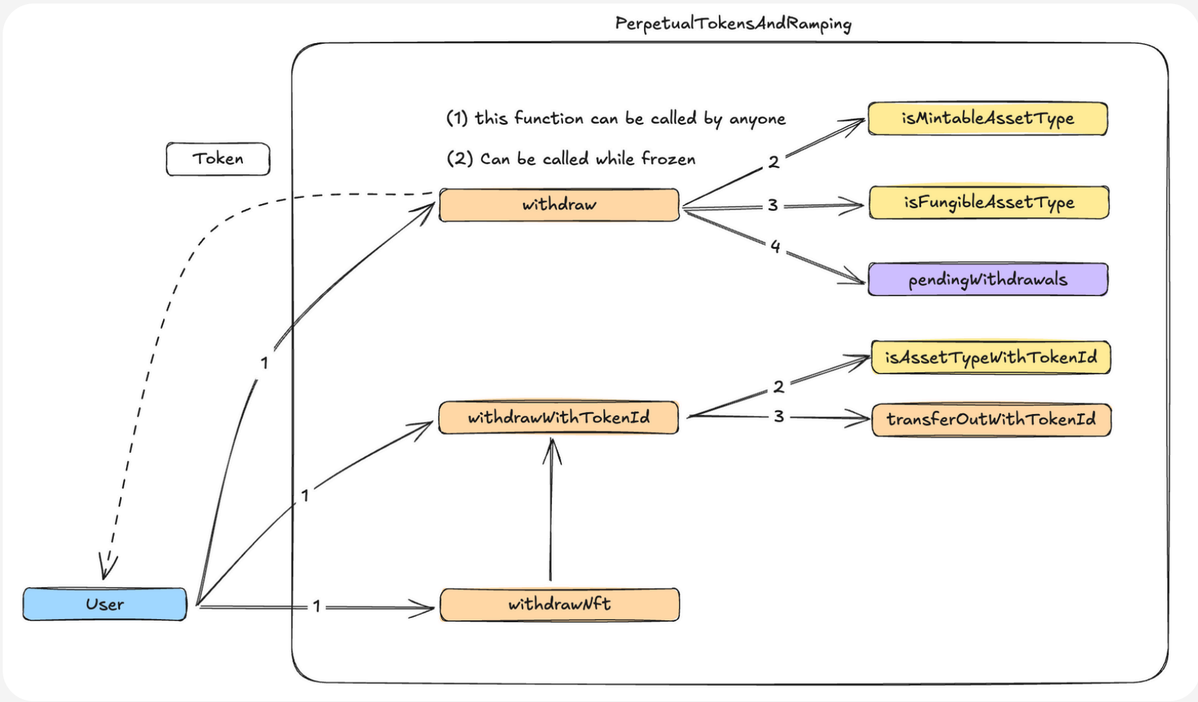
User Interaction - Withdraw



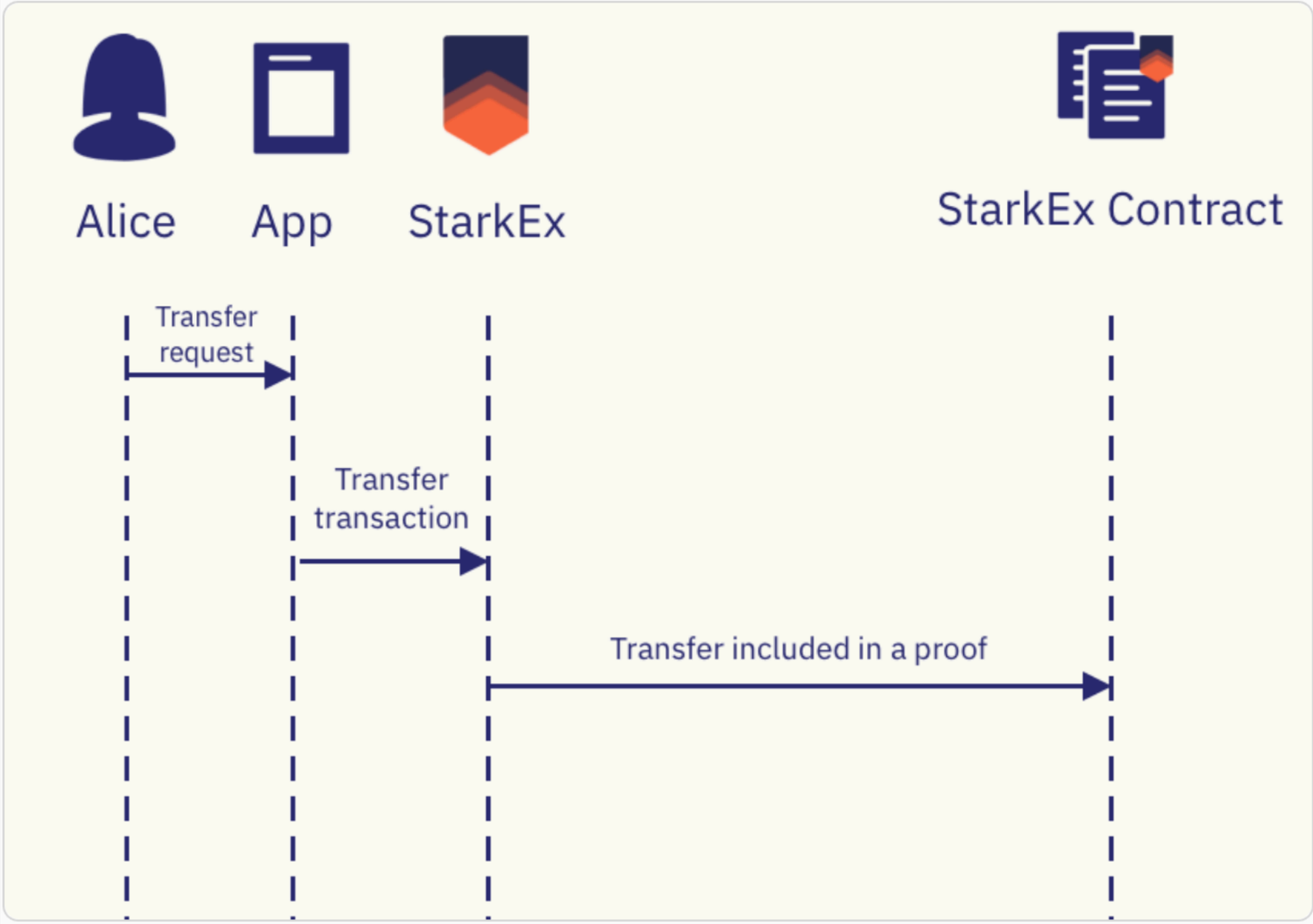
- User initiates a withdrawal request and updates the on-chain state,
- Later completes the withdrawal via an on-chain transaction.

User Interaction - Withdraw

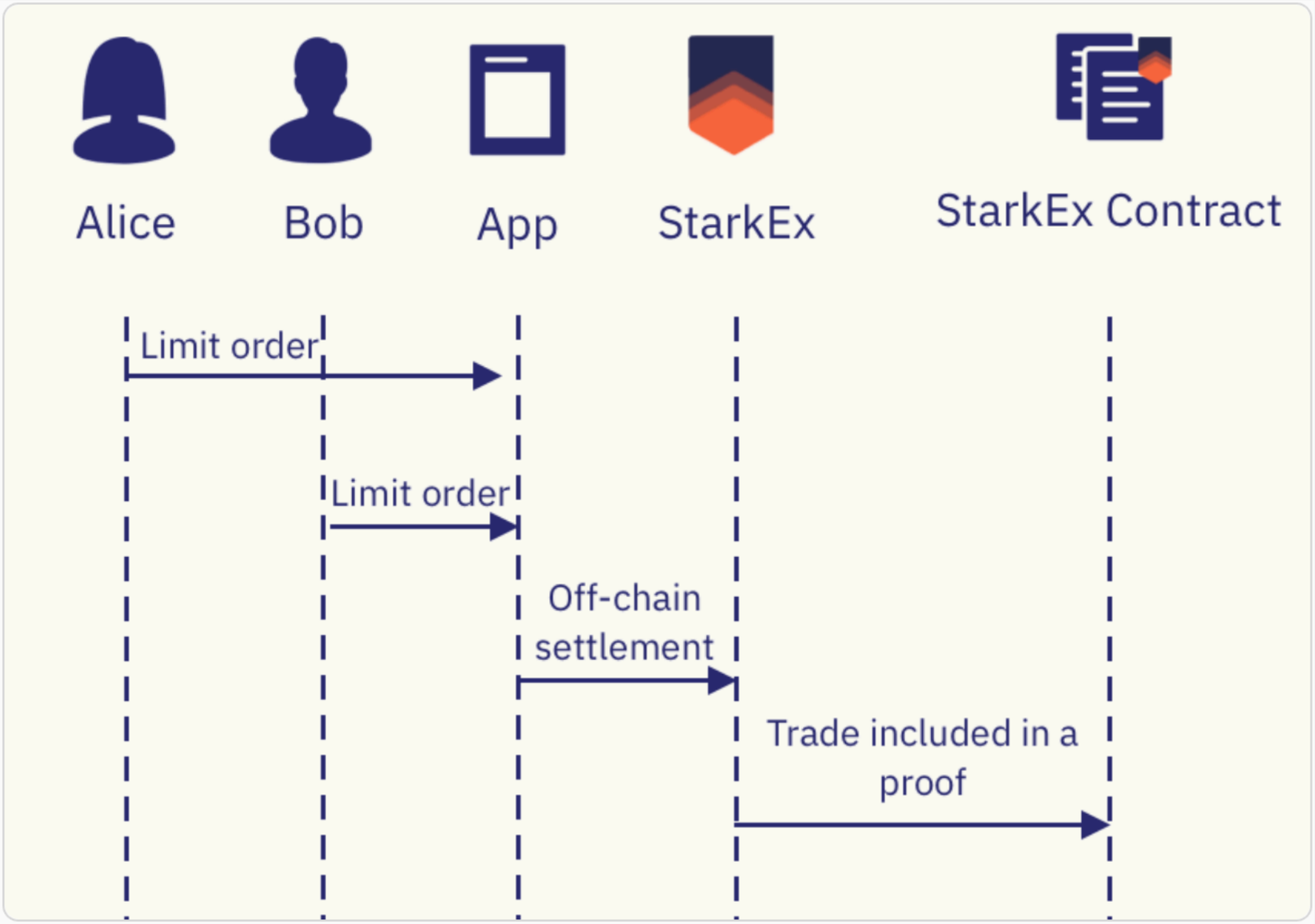
- Invoke `add_transaction` API request with the `TransferRequest` transaction type
- The transaction being validated and include in a batch
- The StarkEx contract updates the state -> pendingWithdrawal
- User withdraw the funds on-chain



User Interaction - Transfer

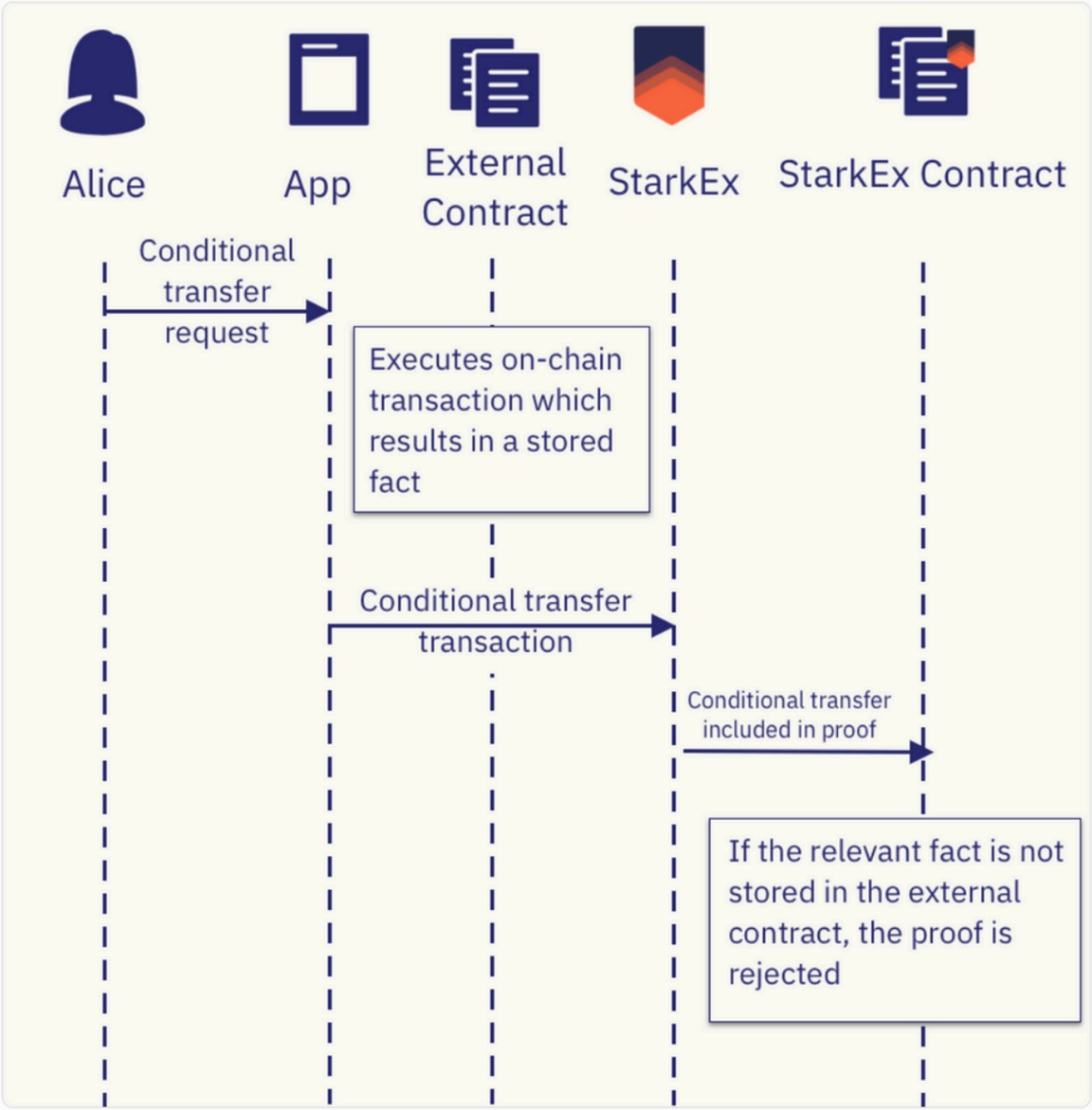


User Interaction - Single / Multi Asset Trade



- Alice wants to trade 1 ETH for 400 DAI
- Bob wants to trade 400 DAI for 1 ETH
- Update the balanceDiff and include in the batch

User Interaction - Conditional Transfer



Case Study: Fast Withdrawal

Original withdraw process: see the previous section -> waiting for proof

Fast withdraw:

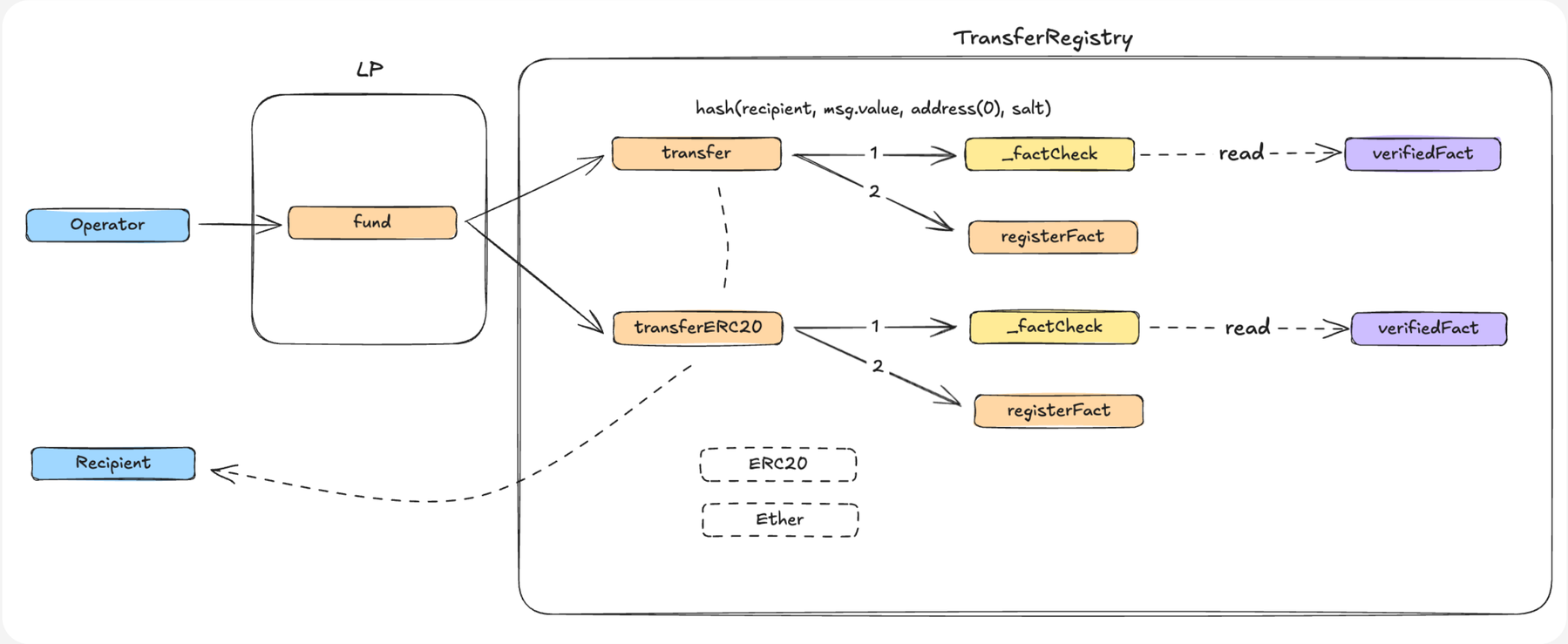
1. Alice submit a conditional transfer request
2. Operator call external contract to initiate token transfer, and later register the fact
3. The state update operation will verified the fact in the registry.

Reference: Cond. Transfer Process, Contract

User Interaction - Conditional Transfer

Fast withdraw:

1. Alice submit a conditional transfer request
2. Operator call external contract to initiate token transfer, and later register the fact
3. The state update operation will verified the fact in the registry.



User Interaction - Conditional Transfer

Operator

```
// check fact
bytes32 transferFact =  keccak256(abi.encodePacked(to, amount, token, salt));
IFactRegister factAddress = IFactRegister(FACT_ADDRESS);
require(!factAddress.isValid(transferFact),"fact already isValid");

// safeApprove requires unsetting the allowance first.
IERC20(token).safeApprove(FACT_ADDRESS, 0);
IERC20(token).safeApprove(FACT_ADDRESS, amount);

factAddress.transferERC20(to, token, amount, salt);
```

```
function transferERC20(address recipient, address erc20, uint256 amount, uint256 salt)
    external {
    bytes32 transferFact = keccak256(
        abi.encodePacked(recipient, amount, erc20, salt));
    require(!_factCheck(transferFact), "TRANSFER_ALREADY_REGISTERED");
    registerFact(transferFact);
    emit LogRegisteredTransfer(recipient, erc20, amount, salt);
    performErc20Transfer(recipient, erc20, amount);
}
```

factRegistry

User Interaction - Forced Action

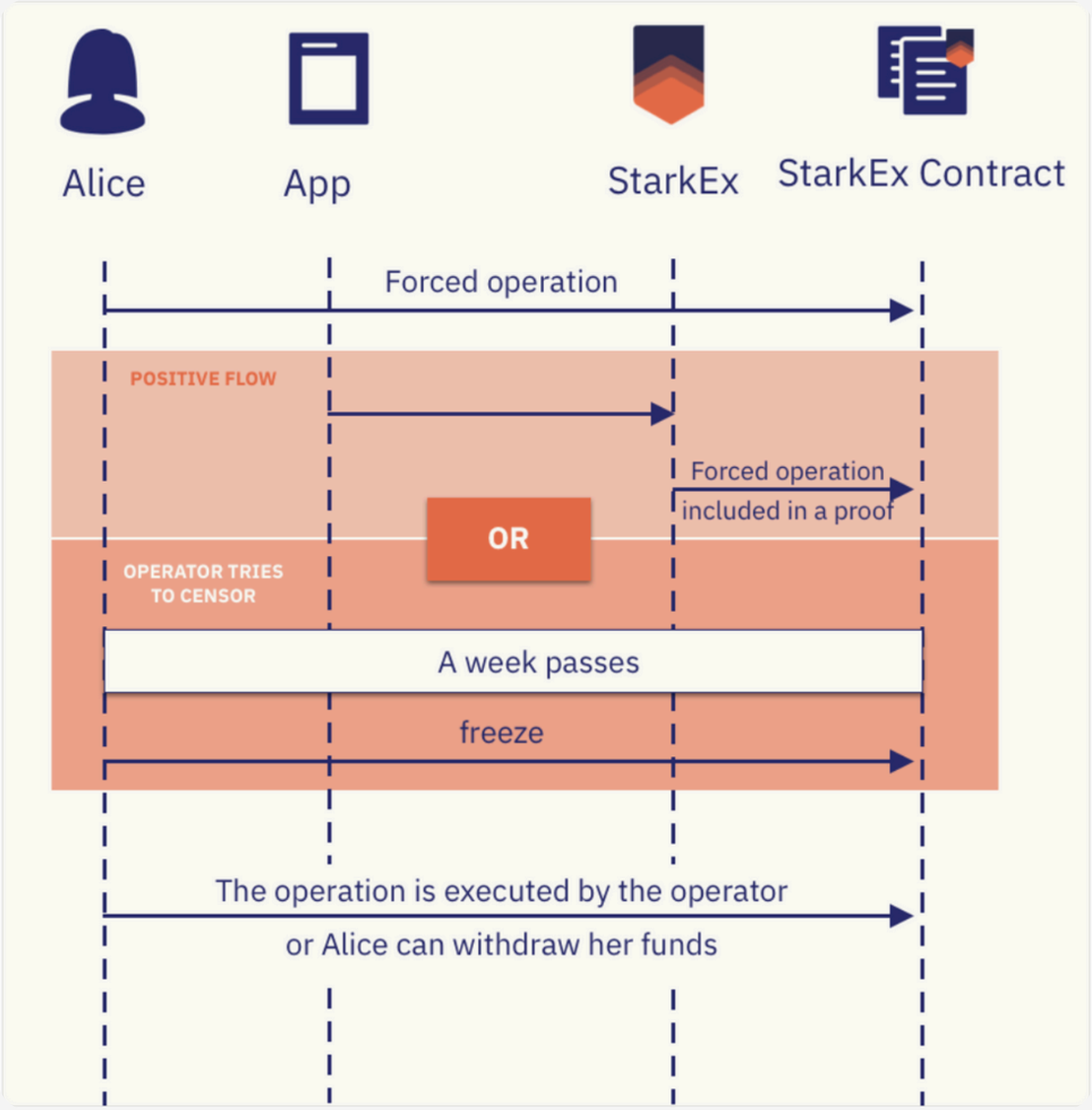
- Goal: (1) Ensure self-custody of funds (2) Avoid censorship
- Action: Users can initiate forced requests at any time.

- Restriction: If a forced operation is not executed within a specified period, users can freeze the contract and subsequently the exchange. Once frozen, any user can directly withdraw their assets.

- Once the application updates the state accordingly, the forced action will be cleared.

Note: There is rate limit in submitting forced action request to prevent DoS attack.

User Interaction - Forced Action



Good

- Alice request forced withdrawal, the application updates the state accordingly.
- After the state update, the forced action request is cleared.

Bad

- Alice requests a forced withdrawal, but the application attempts to censor it and does not process the request.
- After the grace period, Alice freeze the contract, and the state can no longer update.

User Interaction - Forced Action