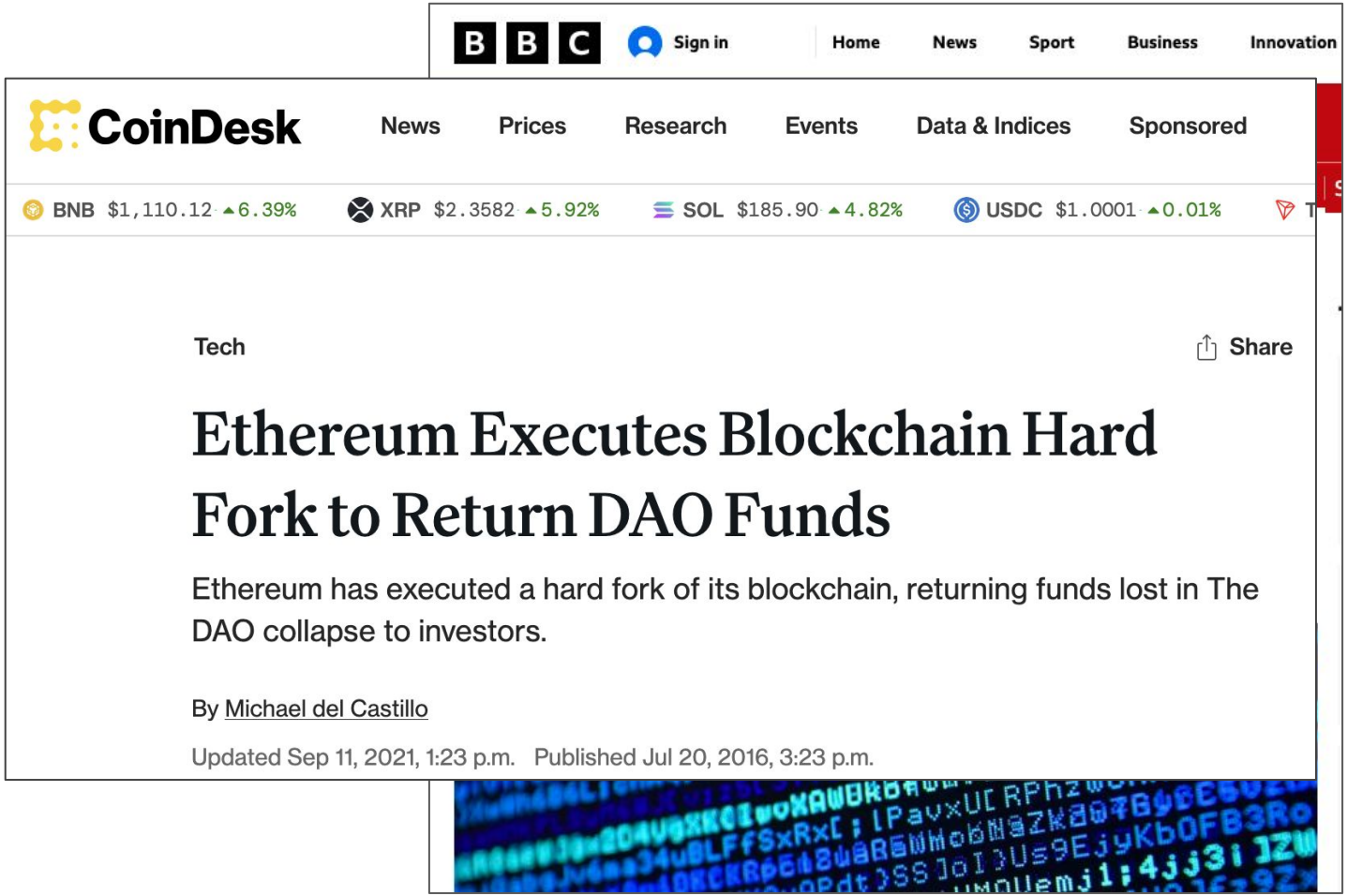
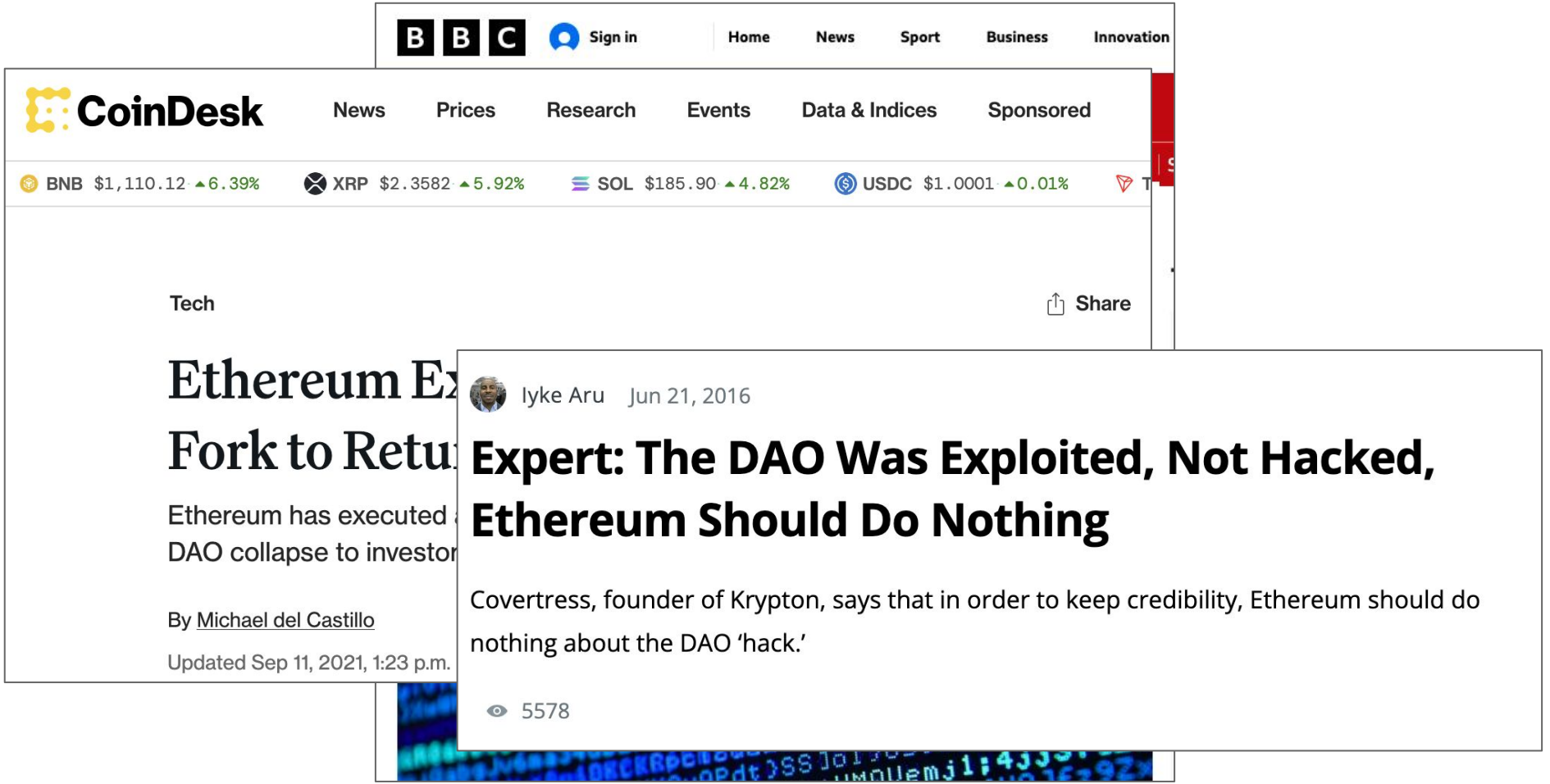
Bonsai: A Recovery Approach for Ethereum ERC-20 Transactions

Diogo Godinho Melita
David Rogério Póvoa de Matos
Miguel Filipe Leitão Pardal

November 7th 2025


BBC
Sign in
Home
News
Sport
Business
Innovation
NEWS
Home | Israel-Gaza war | War in Ukraine | Climate | Video | World | UK | Business | Tech
Tech
Hack attack drains start-up investment fund
21 June 2016


BBC
Sign in
Home
News
Sport
Business
Innovation
CoinDesk
News
Prices
Research
Events
Data & Indices
Sponsored
BNB $1,110.12 ▲6.39%
XRP $2.3582 ▲5.92%
SOL $185.90 ▲4.82%
USDC $1.0001 ▲0.01%
Tech
Share
Ethereum Executes Blockchain Hard Fork to Return DAO Funds
Ethereum has executed a hard fork of its blockchain, returning funds lost in The DAO collapse to investors.
By Michael del Castillo
Updated Sep 11, 2021, 1:23 p.m. Published Jul 20, 2016, 3:23 p.m.


BBC
Sign in
Home
News
Sport
Business
Innovation
CoinDesk
News
Prices
Research
Events
Data & Indices
Sponsored
BNB $1,110.12 ▲6.39%
XRP $2.3582 ▲5.92%
SOL $185.90 ▲4.82%
USDC $1.0001 ▲0.01%
Tech
Share
Ethereum Ex
Fork to Retu
Ethereum has executed
DAO collapse to investor
By Michael del Castillo
Updated Sep 11, 2021, 1:23 p.m.
Iyke Aru Jun 21, 2016
Expert: The DAO Was Exploited, Not Hacked, Ethereum Should Do Nothing
Covertress, founder of Krypton, says that in order to keep credibility, Ethereum should do nothing about the DAO 'hack.'
5578

Agenda

- ➔ Background
- ➔ Related Work
- ➔ Bonsai Solution
- ➔ Evaluation
- ➔ Conclusion

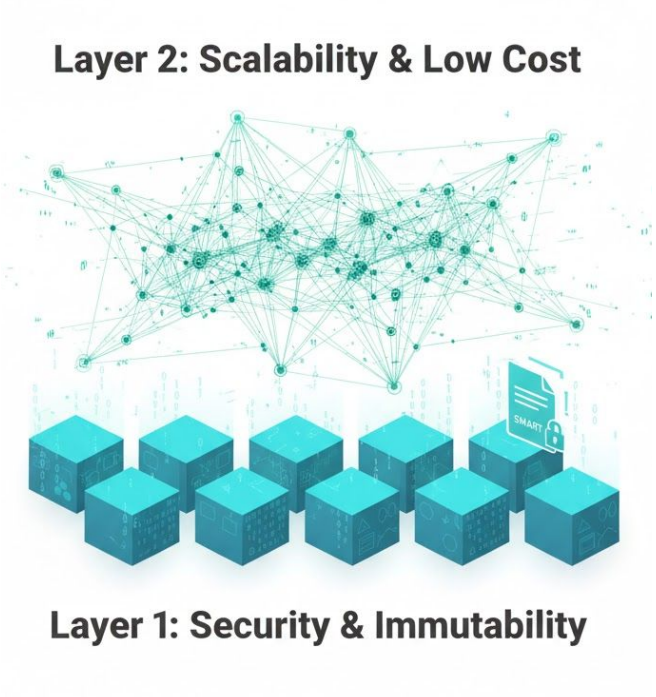
Background

Blockchain

- ➔ Blockchain overview
- ➔ Smart Contracts

Blockchain

- ➔ Blockchain overview
- ➔ Smart Contracts
- ➔ Layer 2 Blockchains



Blockchain Immutability

- ➔ Immutability - advantages and challenges
  - ◆ Removal Strategies
  - ◆ Bypass Approaches

Related Work

Reversible Tokens

- ➔ Recoverable Token proposal [1]
  - Users left at risk if tokens spent before reversal request
  - Arbitration trials with possible voting influence

[1] F. F. Martins, D. R. Matos, M. L. Pardal, and M. Correia, “Recoverable Token: Recovering from Intrusions against Digital Assets in Ethereum,” in 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). Cambridge, MA, USA: IEEE, Nov. 2020, pp. 1–9.

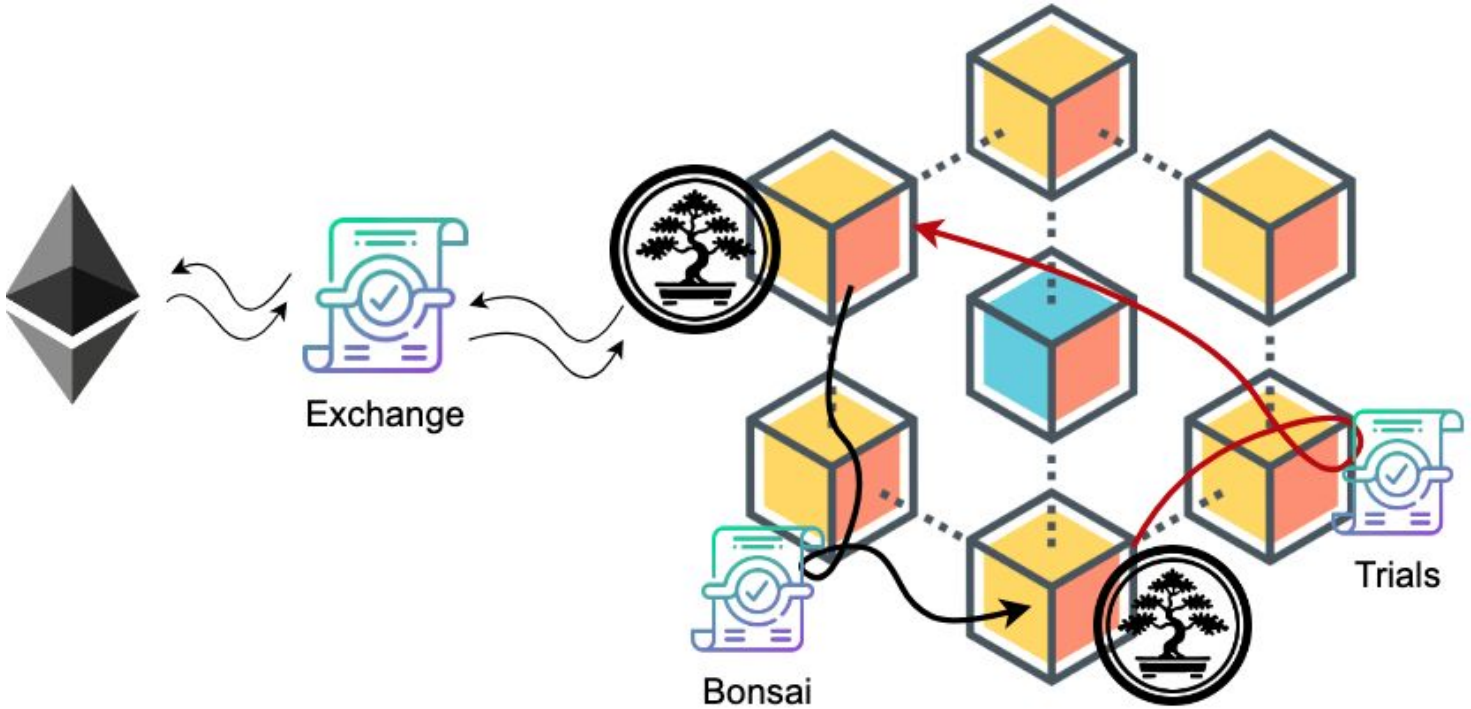
Reversible Tokens

- ➔ Recoverable Token proposal [1]
  - ◆ Users left at risk if tokens spent before reversal request
  - ◆ Arbitration trials with possible voting influence
- ➔ ERC-20R and ERC-721R proposals [2]
  - ◆ Tokens may not be located
  - ◆ Victims of recursive reversals not compensated
  - ◆ Possible voting influence and centralized pool of arbitrators

[1]F. F. Martins, D. R. Matos, M. L. Pardal, and M. Correia, “Recoverable Token: Recovering from Intrusions against Digital Assets in Ethereum,” in 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA). Cambridge, MA, USA: IEEE, Nov. 2020, pp. 1–9.
[2]K. Wang, Q. Wang, and D. Boneh, “ERC-20R and ERC-721R: Reversible Transactions on Ethereum,” Oct. 2022, arXiv:2208.00543 [cs]

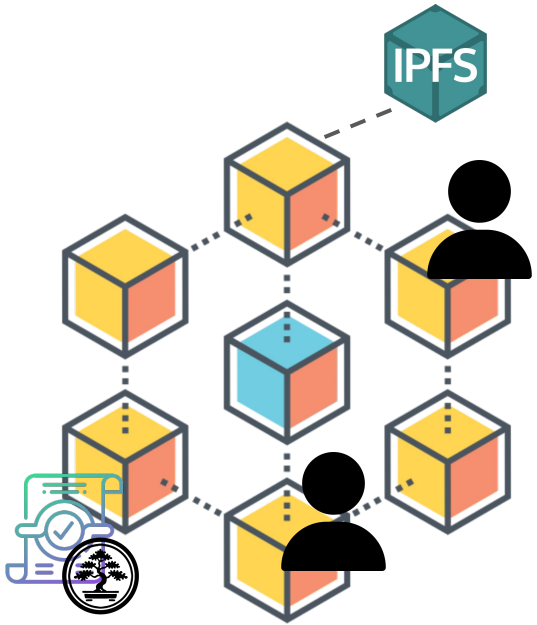
Bonsai Solution

Bonsai Overview

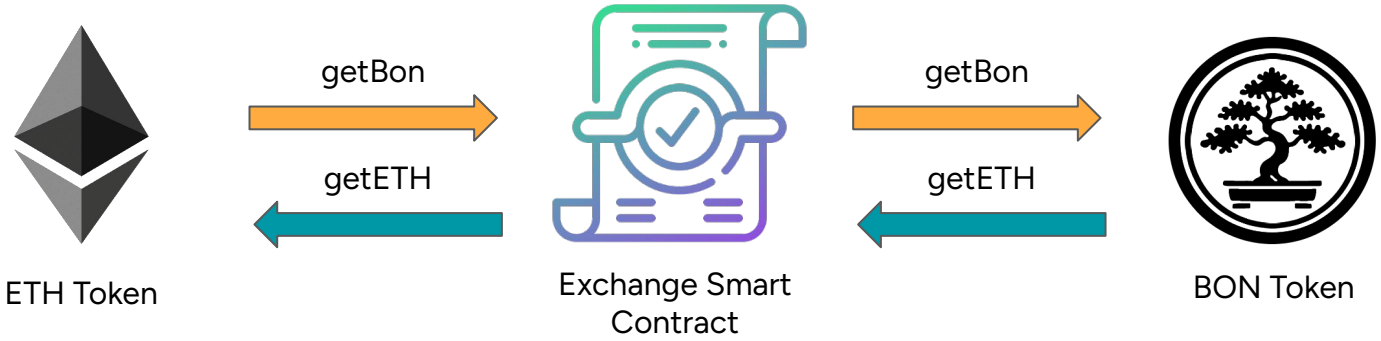


Architecture Components

- ➔ Users
  - ◆ Blockchain Users
  - ◆ Arbitrators
- ➔ Threat Model
  - ◆ Intrusions from ill-intentioned users
  - ◆ Human Error
- ➔ System Model
  - ◆ State



BON/ETH Exchanges

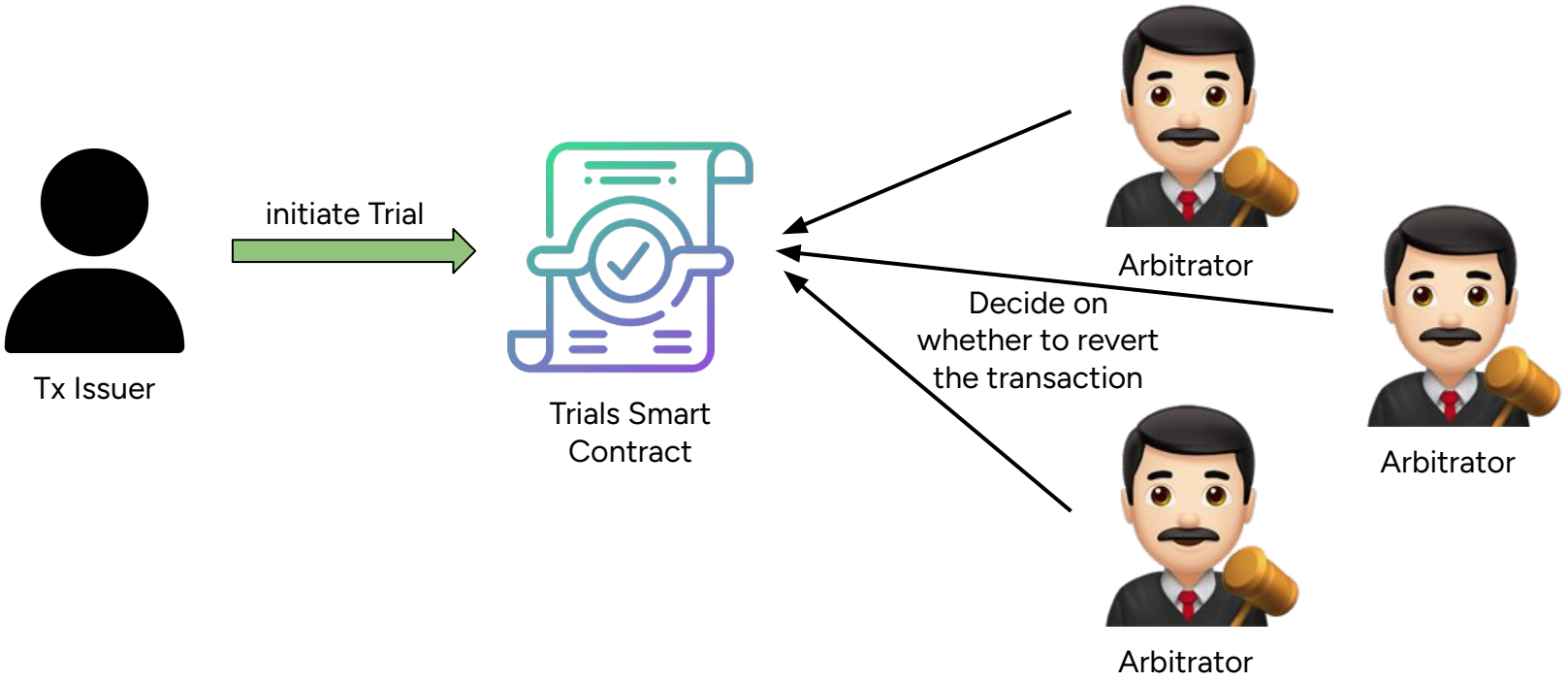


Bonsai’s balances

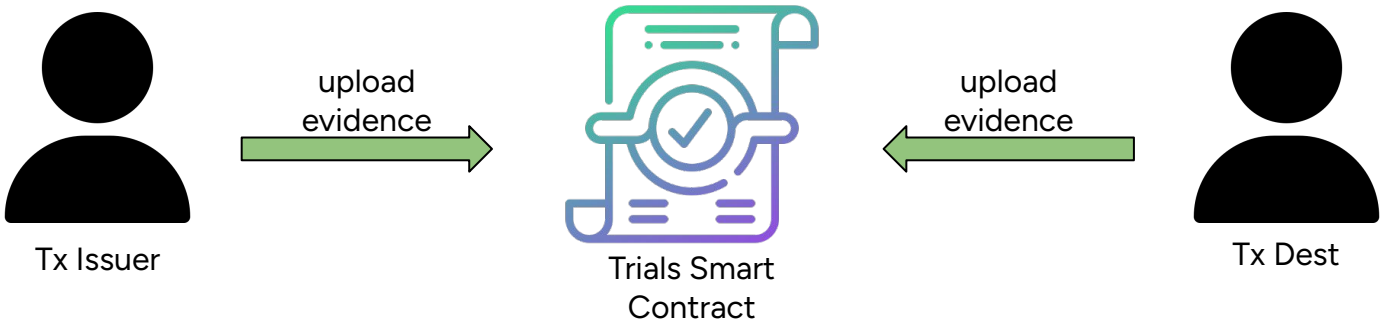
- ➔ Balance: freely spent network balance
- ➔ Unstable Balance: tokens associated with pending transactions.
- ➔ Stable Balance: Balance minus Unstable Balance; non-revertible tokens.
- ➔ Unstable tokens become stable after cool-down expires and user finalization.

Bonsai Smart Contract

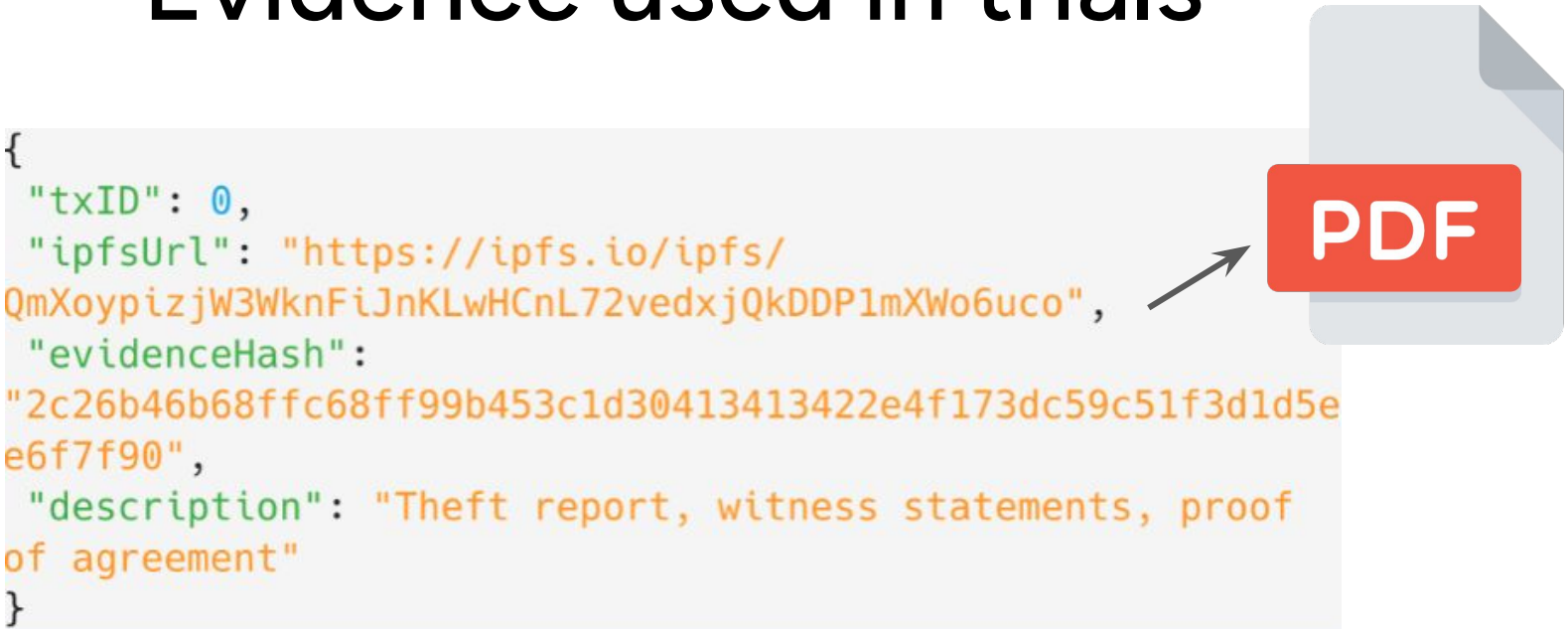
Trials


initiate Trial
Tx Issuer
Trials Smart Contract
Arbitrator
Decide on whether to revert the transaction
Arbitrator
Arbitrator

Trials

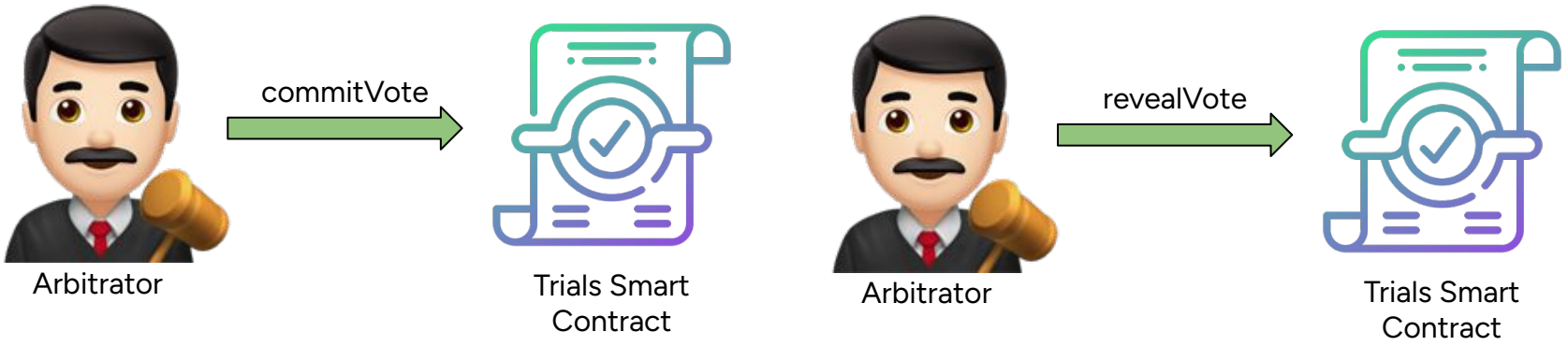

upload
evidence
upload
evidence
Tx Issuer
Trials Smart
Contract
Tx Dest

Evidence used in trials

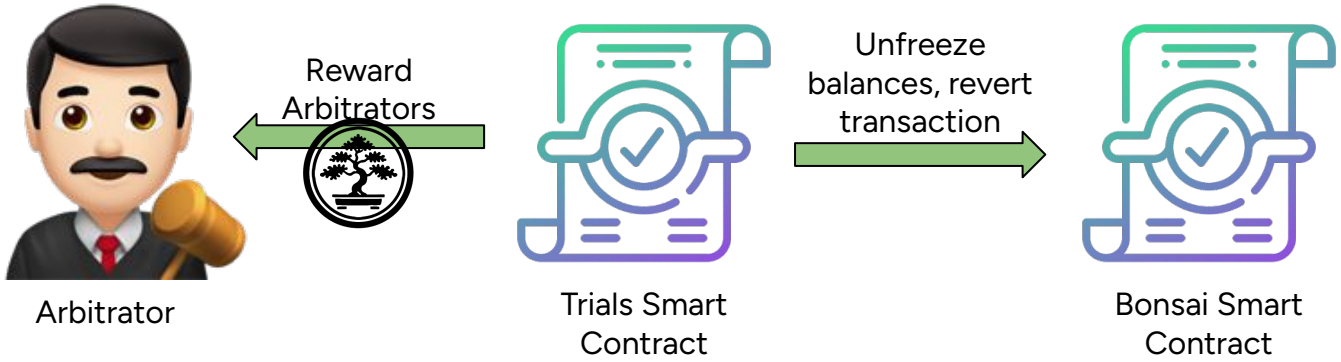


Evidence metadata example

Trials


commitVote
Arbitrator
Trials Smart Contract
revealVote
Arbitrator
Trials Smart Contract

Trials


Reward Arbitrators
Unfreeze balances, revert transaction
Arbitrator
Trials Smart Contract
Bonsai Smart Contract

Bonsai Insurance

- ➔ Protects user against reversals that impact them
  - ◆ but they were not a direct interested party
- ➔ Requires paying a % of the tx amount
- ➔ Plafond score
  - ◆ Metric used for compensation payouts

$$plafond = \frac{\min(membership,\ 10) \times \min(\sum payments\_made \times diff\_addresses,\ 100{,}000)}{\min(\#ReversalRequestsMadeLastYear,\ 0) + 1}$$

Insurance Compensation Example

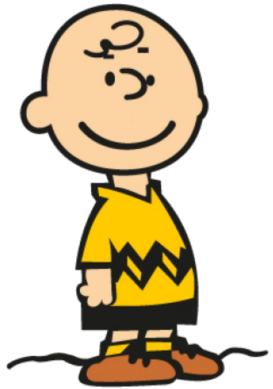
Alice

Balance: 5.25 BON

Bob

Balance: 0.25 BON

Charlie



Balance: 0 BON

Insurance Compensation Example

Alice

Balance: 0 BON

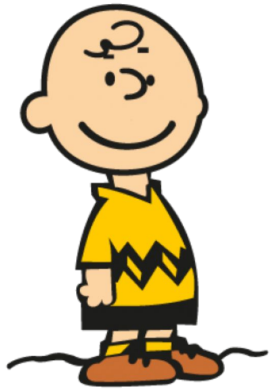
Transaction *t1*

5 BON tokens
(with 0.25 tokens paid
to the Insurance - 5%
of the tx amount)

Bob

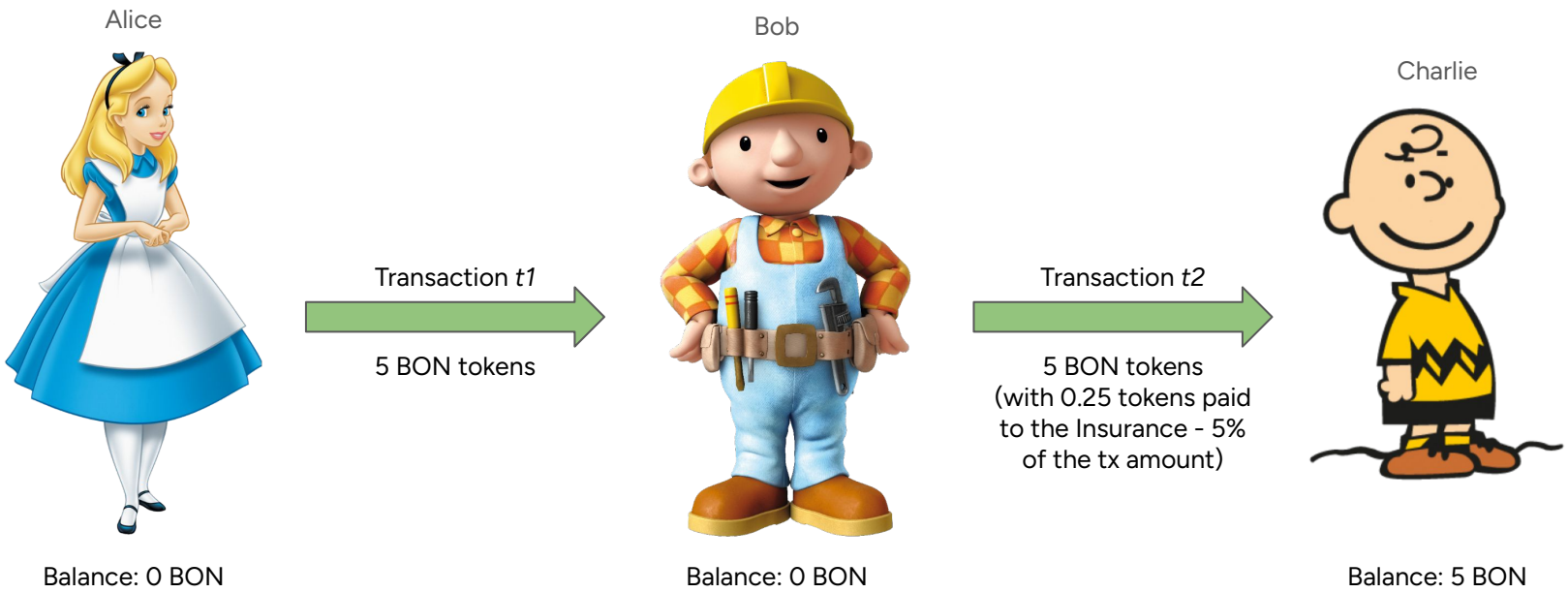
Balance: 5.25 BON

Charlie

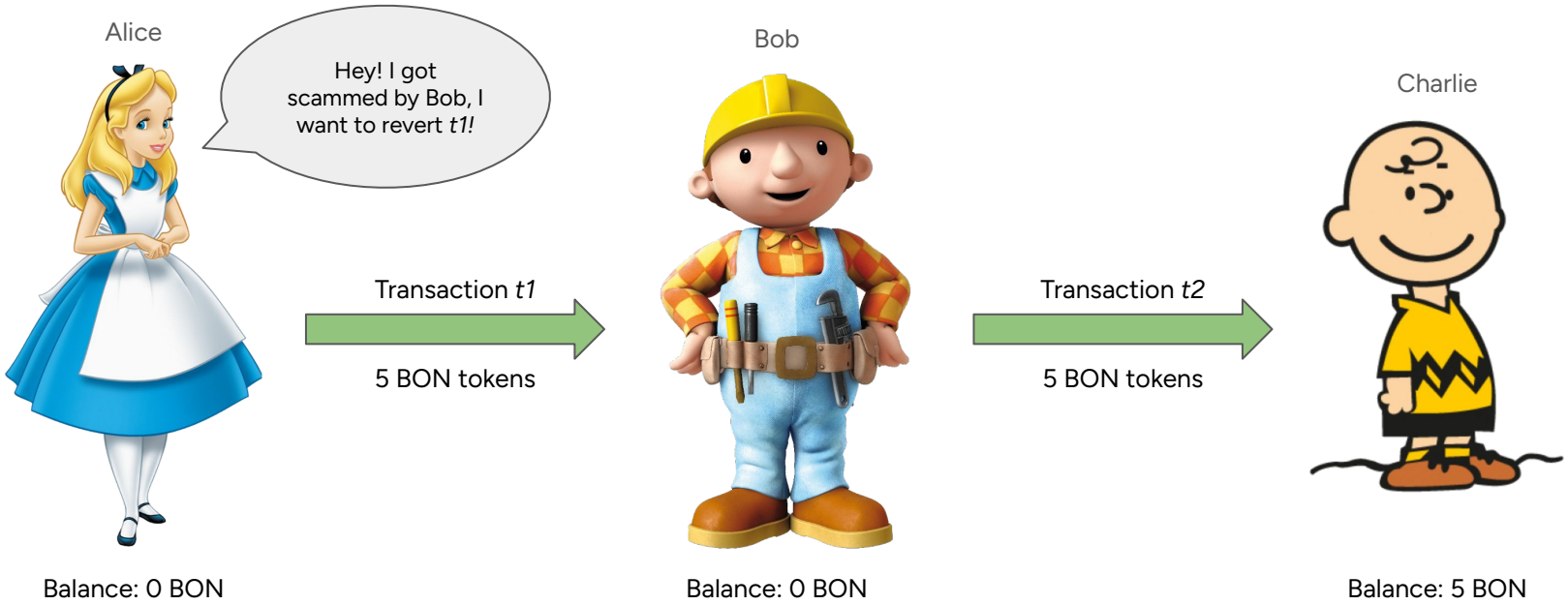


Balance: 0 BON

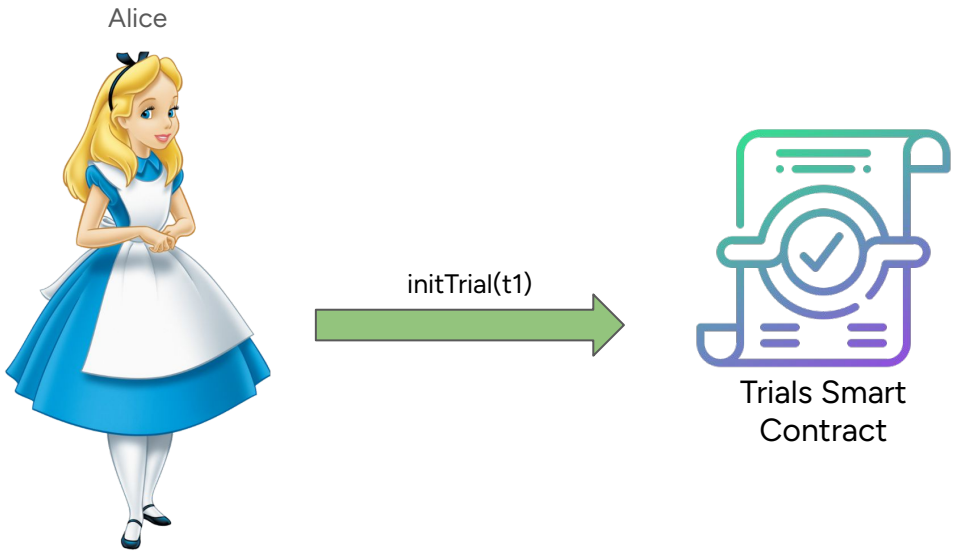
Insurance Compensation Example



Insurance Compensation Example

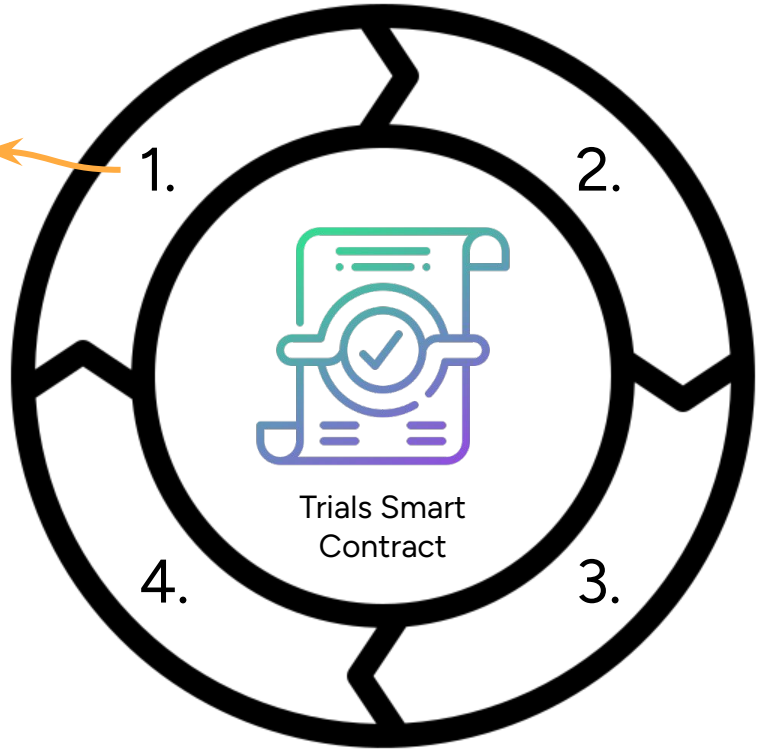


Insurance Compensation Example



Insurance Compensation Example

Trace transactions
- find tokens on users balances
- tranceTransactions algorithm

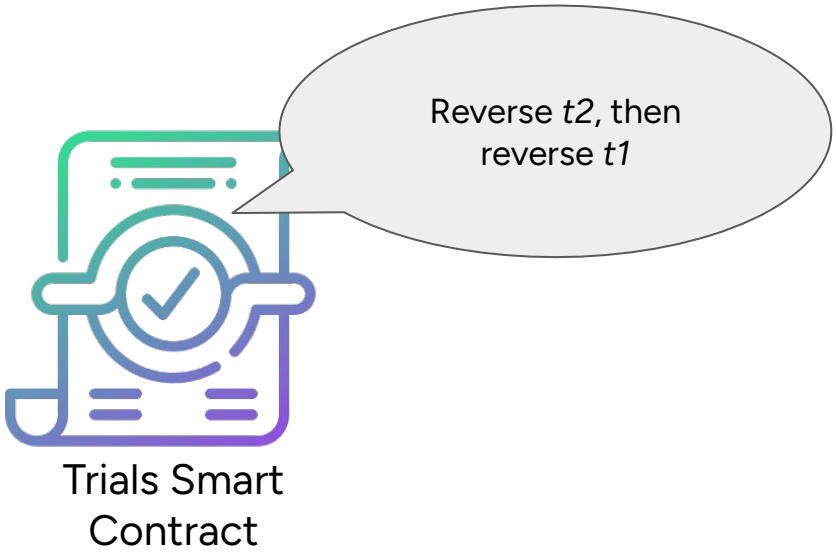


Trace Transactions

Algorithm 1 traceTransactions algorithm

```
1: function TRACETRANSACTIONS(txID, needed, txsToRevert, freezed)
2:     tx ← getTxByID(txID)
3:     if balanceOf(tx.dest) − frozenBalanceOf(tx.dest) ≥ needed then
4:         toFreeze ← needed
5:     else
6:         toFreeze ← balanceOf(tx.dest)
7:     end if
8:     txsToRevert.push(txID)
9:     freezed.push(toFreeze)
10:    if toFreeze == needed then
11:        return (txsToRevert, freezed)
12:    end if
13:    needed ← needed − toFreeze
14:    issuedTxs ← getIssuedTxs(tx.dest)
15:    for t ∈ issuedTxs in reverse order do
16:        tx′ ← getTxByID(t)
17:        if tx′.ID < txID then
18:            continue
19:        end if
20:        (txsToRevert, freezed) ← TRACETRANSACTIONS(tx′.ID, needed, txsToRevert, freezed)
21:        if tx′.amount ≥ needed then
22:            needed ← 0
23:        else
24:            needed ← needed − tx′.amount
25:        end if
26:        if needed == 0 then
27:            break
28:        end if
29:    end for
30:    return (txsToRevert, freezed)
31: end function
```

Insurance Compensation Example



Insurance Compensation Example

Trials Smart Contract

Insurance Compensation Example

Alice

Balance: 0 BON

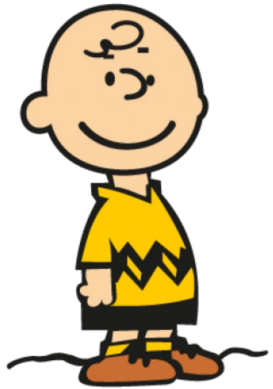
Bob

Balance: 5 BON

Transaction *t2*

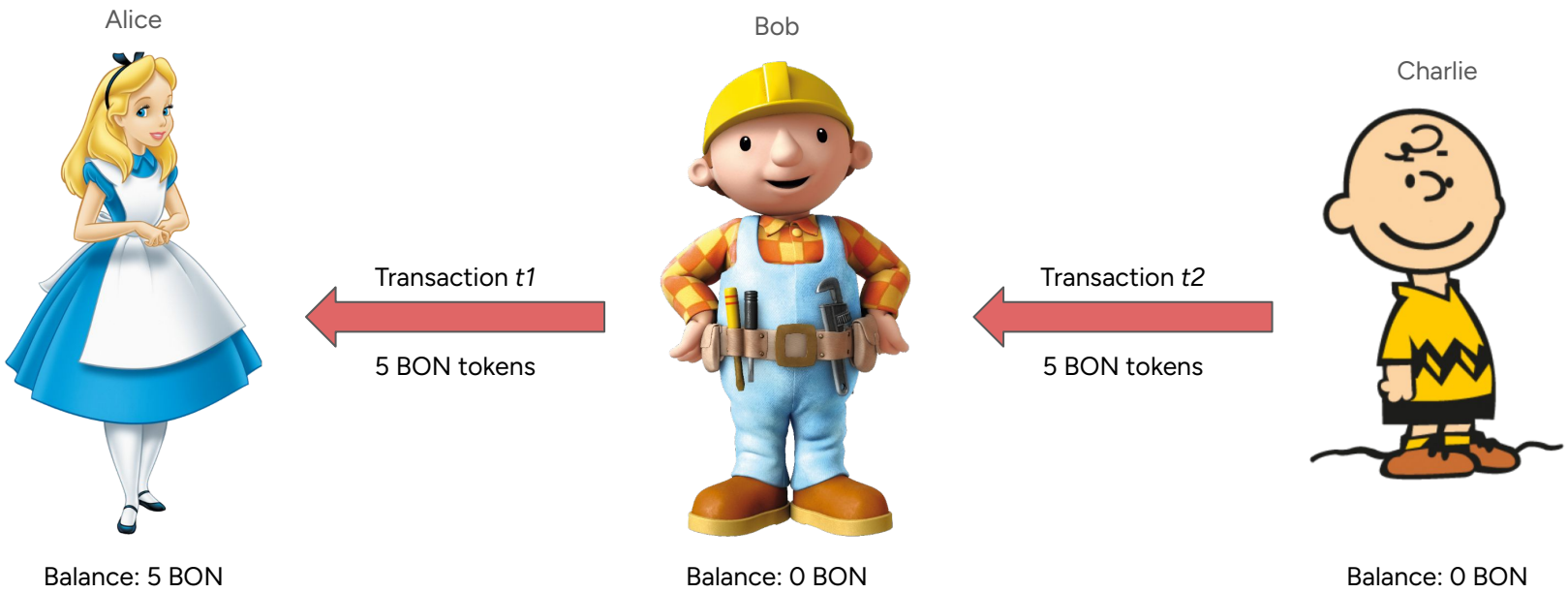
5 BON tokens

Charlie

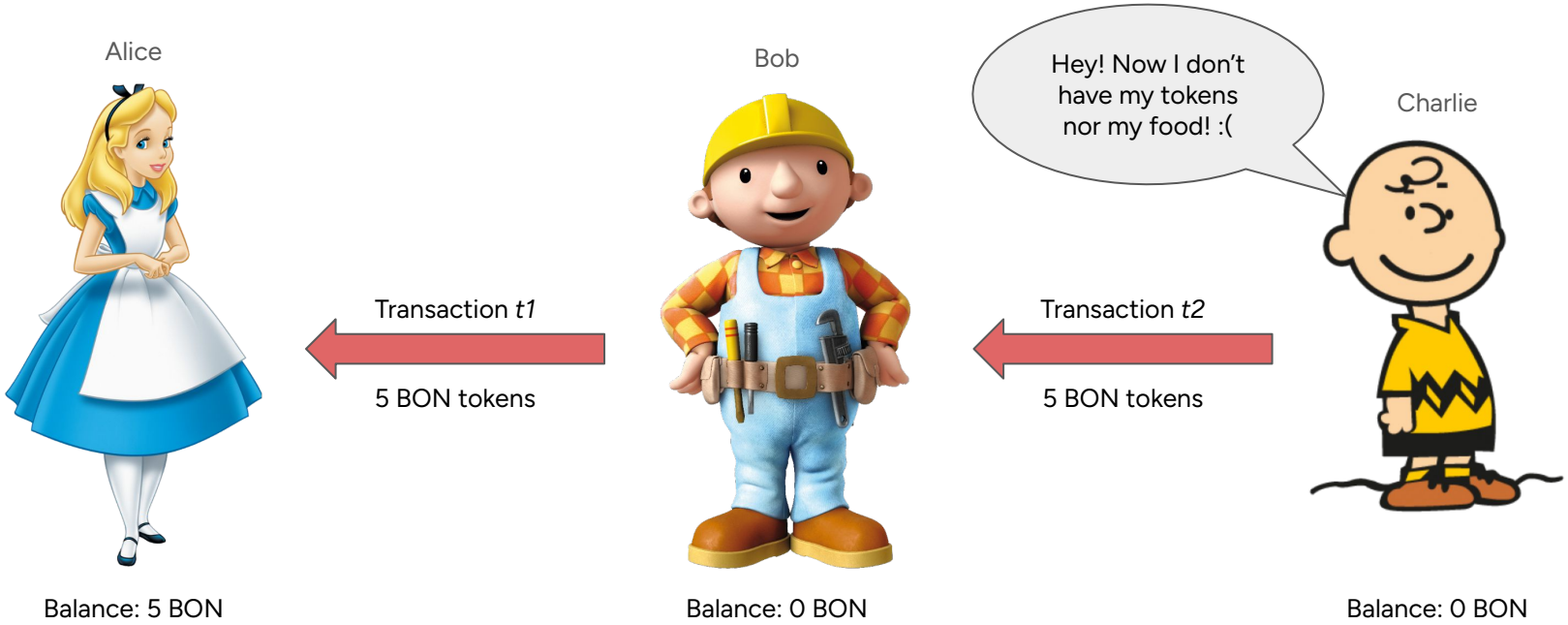


Balance: 0 BON

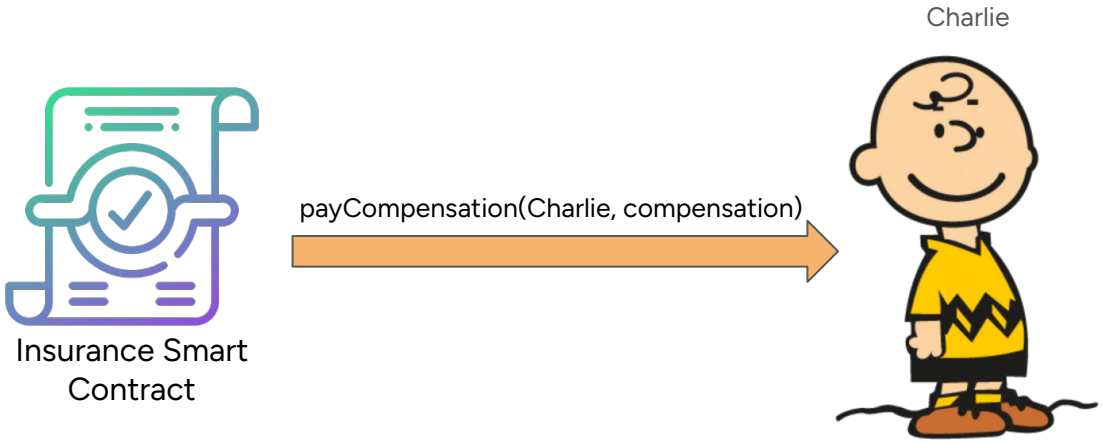
Insurance Compensation Example



Insurance Compensation Example



Insurance Compensation Example



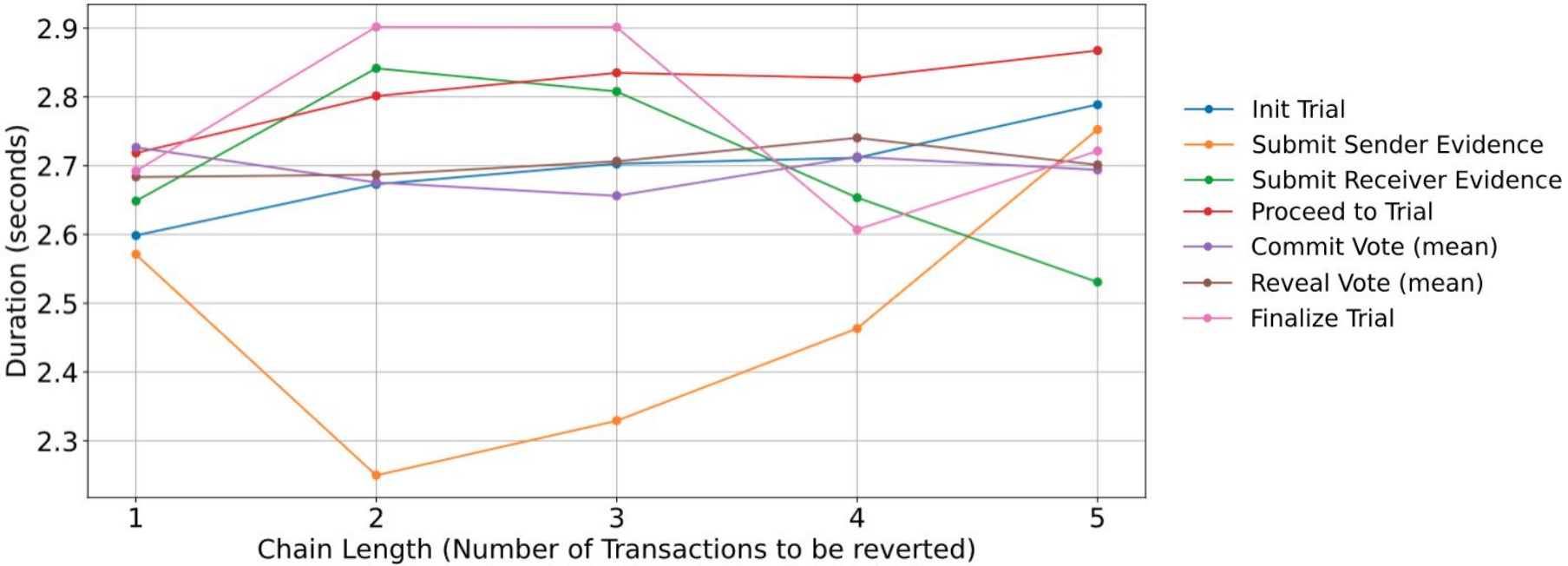
compensation = min(tx.amount, plafond, HC, balanceOf (Insurance) – ResReq)

Evaluation

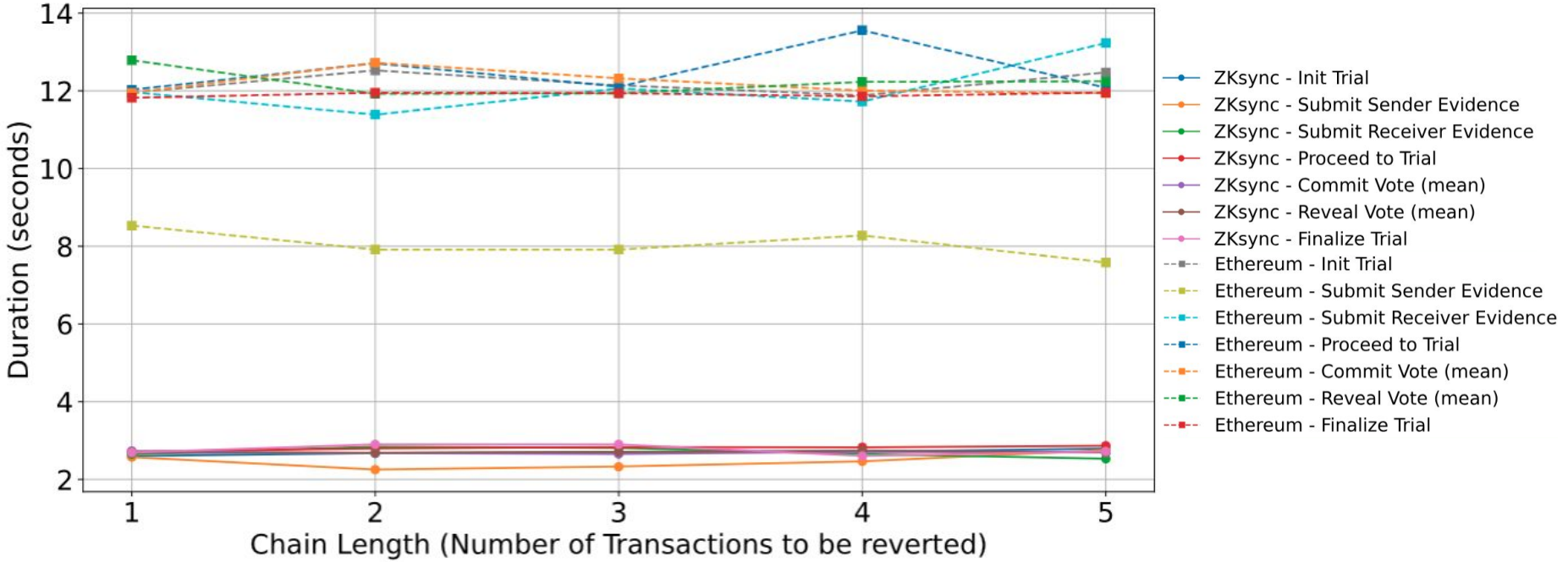
Evaluation Methodology and Setup

- ➔ Unit and integration testing
- ➔ Testing on a Layer 1 and a Layer 2 blockchain
  - ◆ L1 - Ethereum Sepolia
  - ◆ L2 - ZKsync Sepolia
- ➔ Metrics
  - ◆ Trial latency
  - ◆ Reversal cost

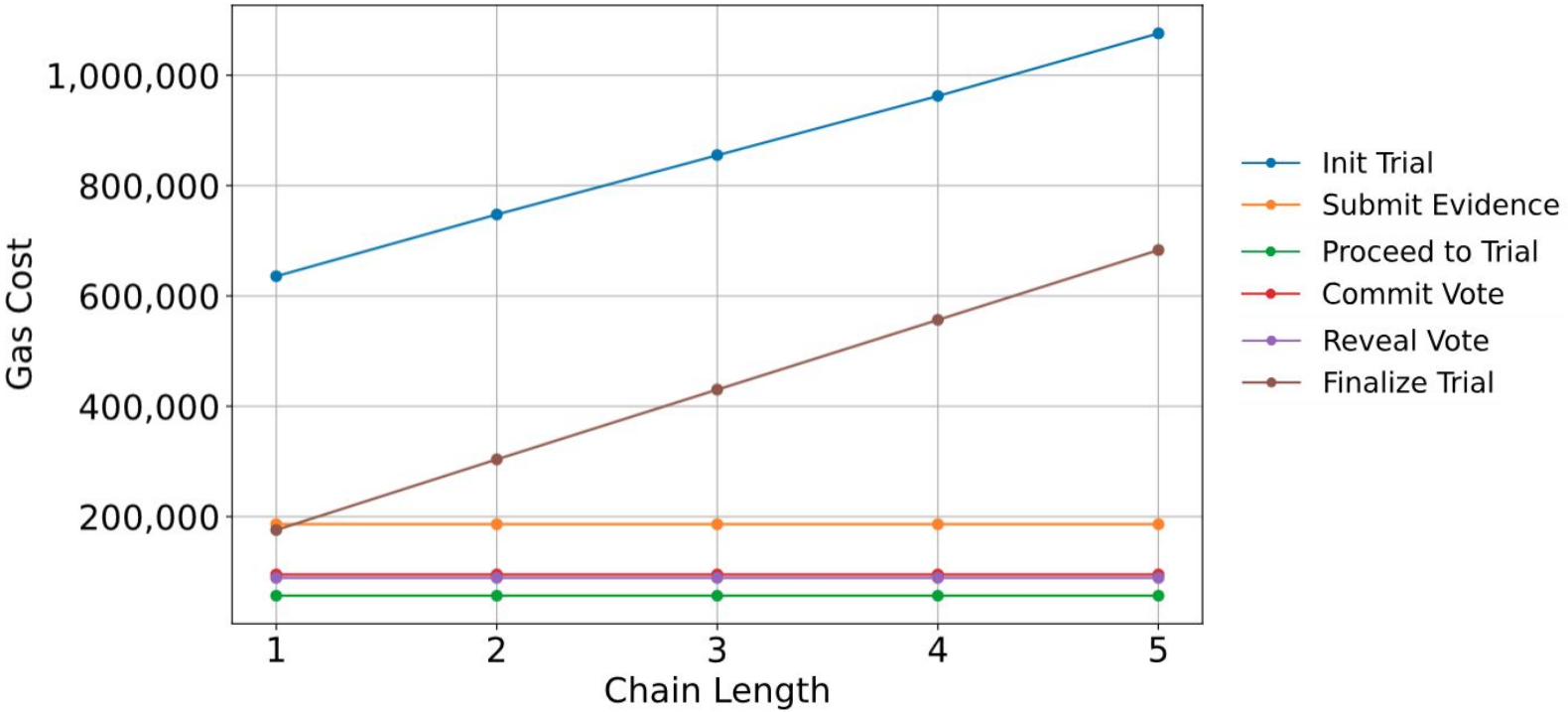
Time Consumption - ZKsync



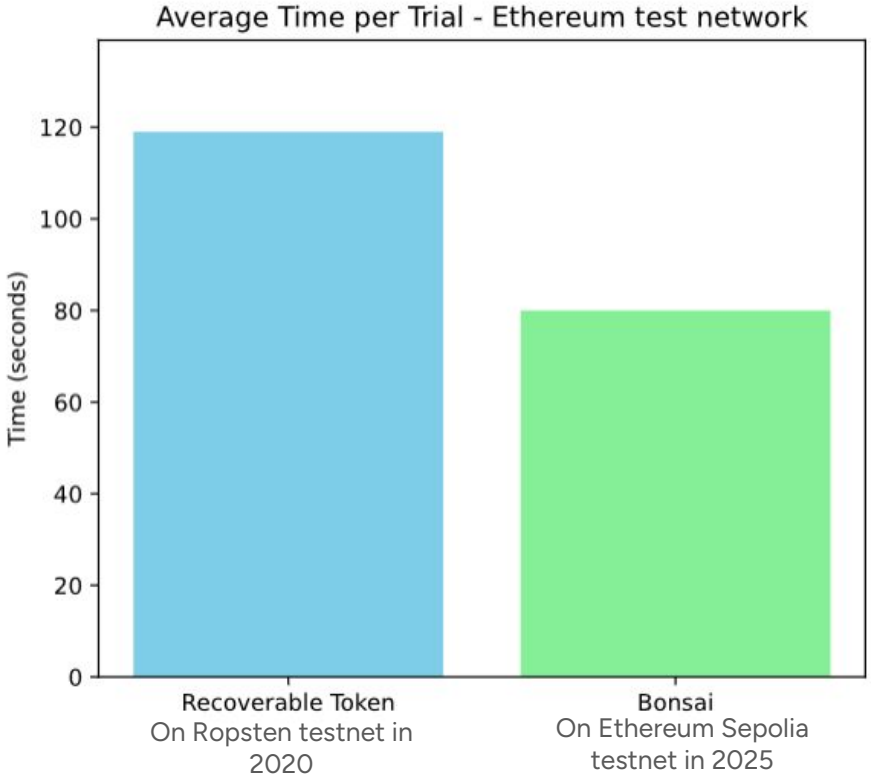
Time Consumption - L1 vs L2



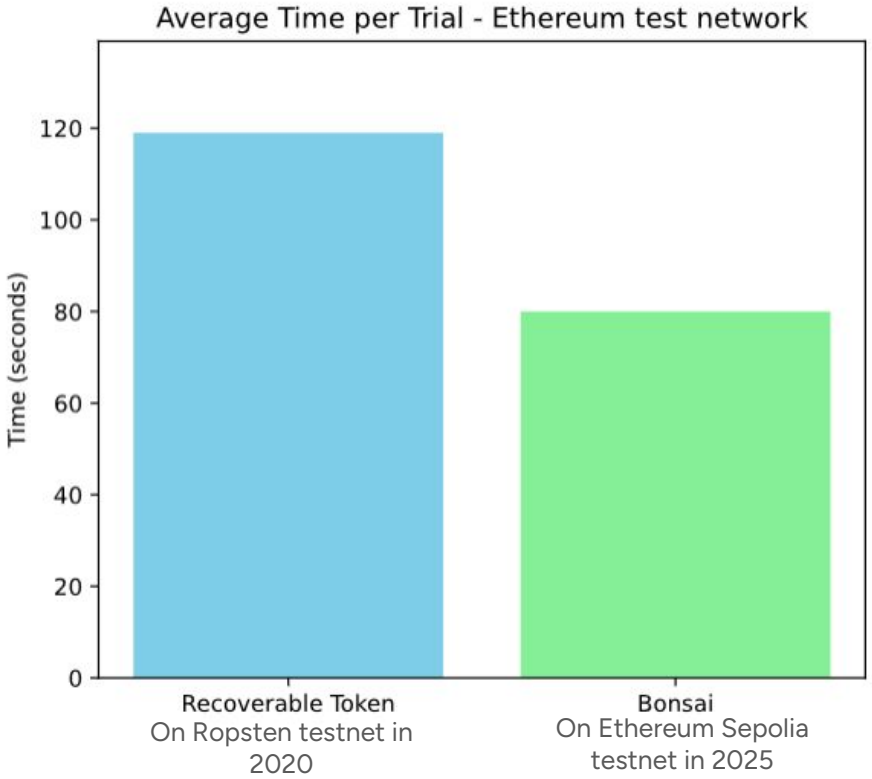
Gas Consumption

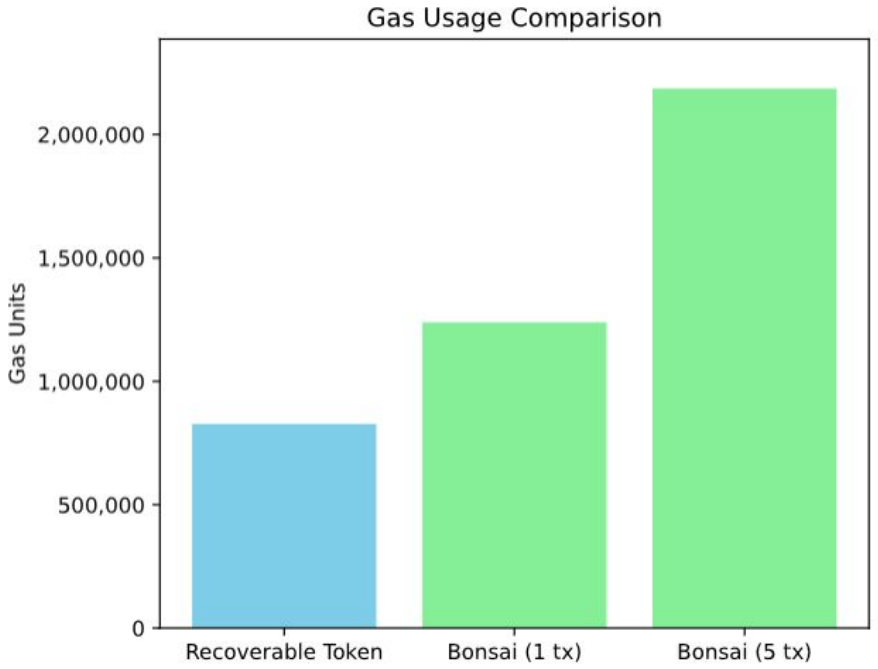


Comparison with Previous Work



Comparison with Previous Work





Conclusion

Achievements

- ➔ Bonsai - system allowing ERC-20 transaction reversals during a cool-down period, using trials and an insurance
- ➔ Layer 2 solutions provide time and cost advantages
- ➔ Bonsai promises an innovative approach for blockchain applications that require error redactability

Future Work

- ➔ Arbitrator Picking Procedure
- ➔ Notification System

Thank you!

Bonsai: A Recovery Approach for Ethereum ERC-20 Transactions

Work supported by national funds through Fundação para a Ciência e a Tecnologia, I.P. (FCT) under projects UID/50021/2025 and UID/PRR/50021/2025 (INESC-ID), 2024.07494.IACDC (WELL), and Project Blockchain.PT – Decentralize Portugal with Blockchain Agenda, (Project no 51), WP 1: Agriculture and Agri-food, Call no 02/C05-i01.01/2022, funded by the Portuguese Recovery and Resilience Program (PRR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.

Appendix Slides

How to prevent Recursive Reversals

How to prevent Recursive Reversals

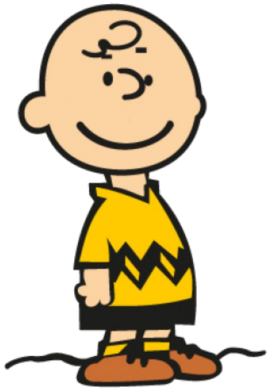
Alice

Balance: 0 BON

Bob

Balance: 5.5 BON

Charlie



Balance: 0 BON

How to prevent Recursive Reversals

Alice

Balance: 0 BON

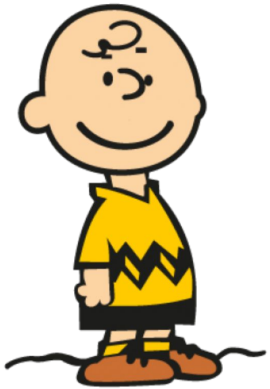
Transaction *t1*

5 BON tokens

Bob

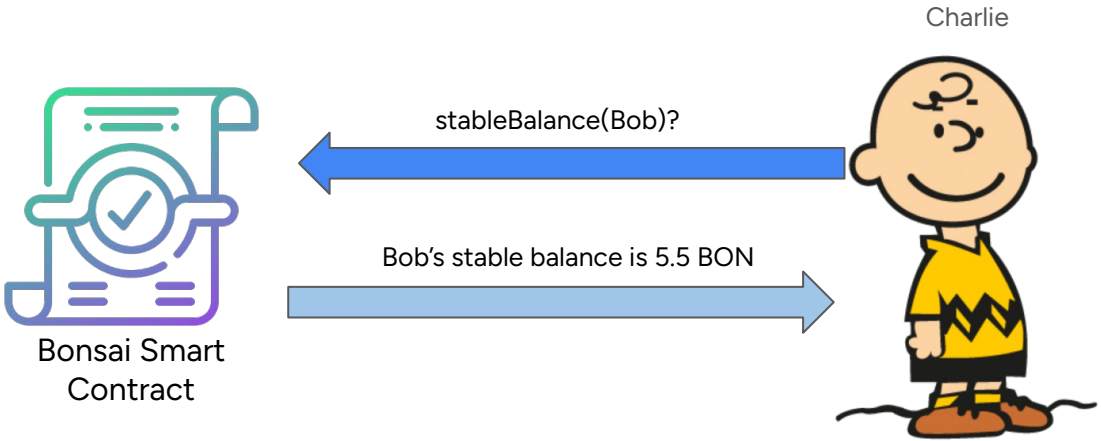
Balance: 10.5 BON
5 BON - unstable
5.5 BON stable

Charlie

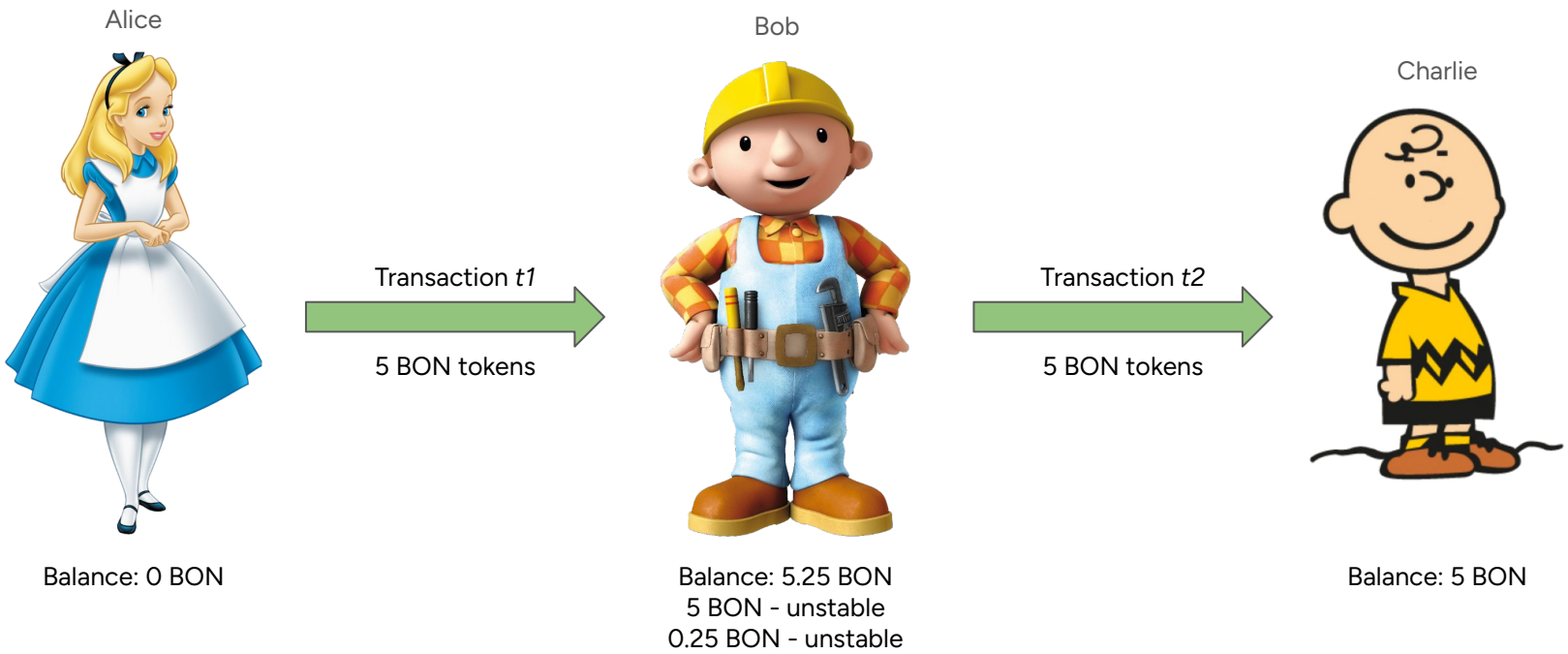


Balance: 0 BON

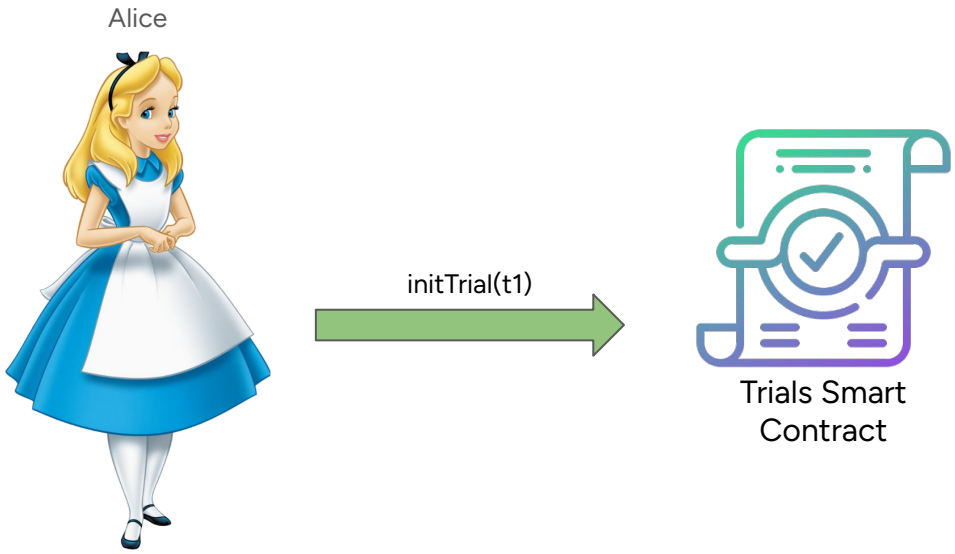
How to prevent Recursive Reversals



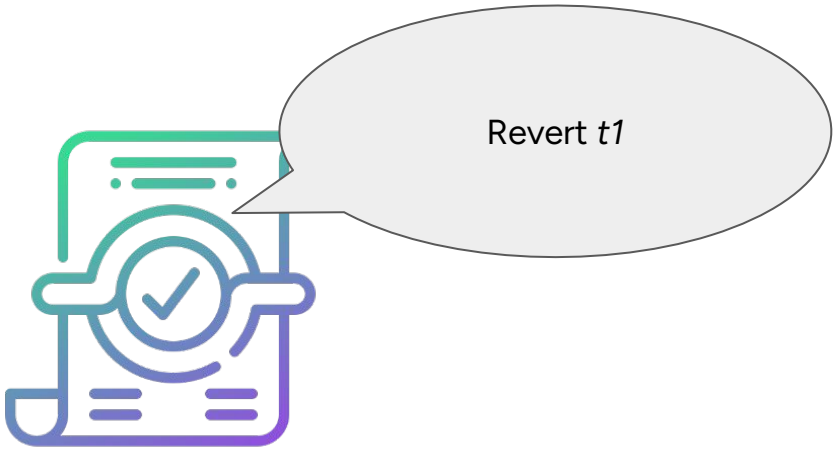
How to prevent Recursive Reversals



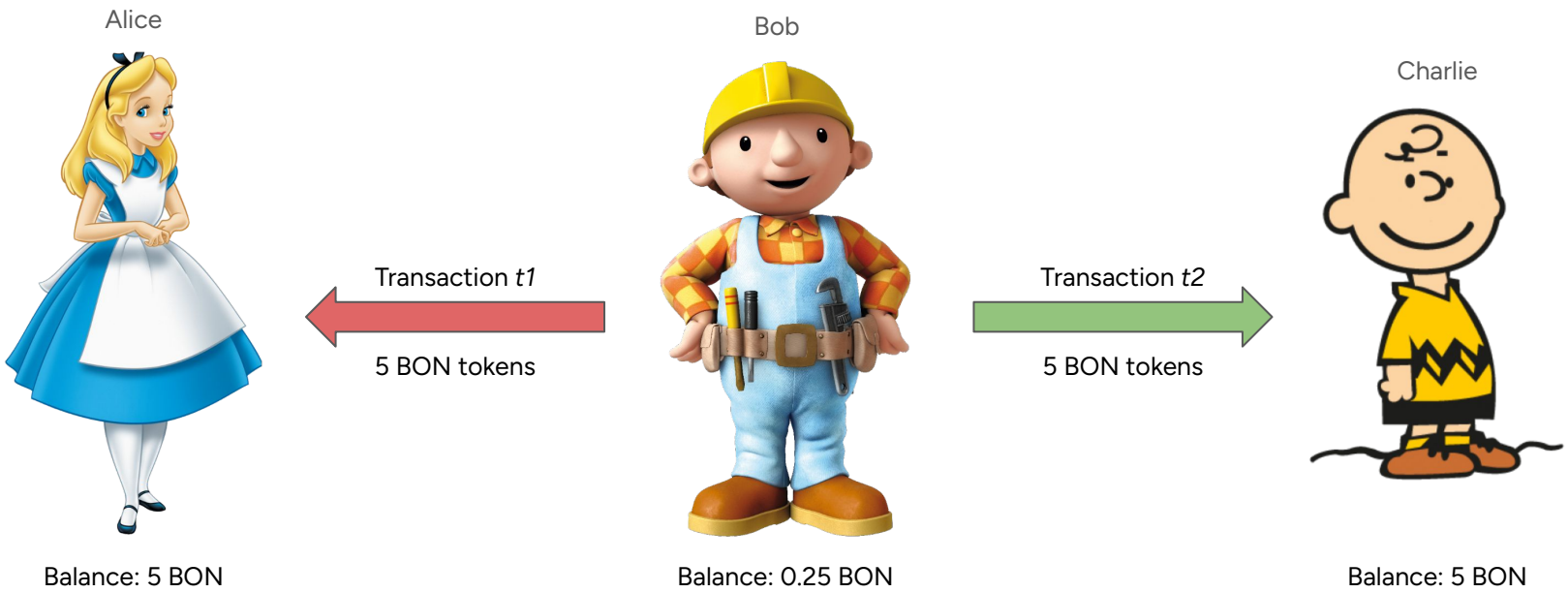
How to prevent Recursive Reversals



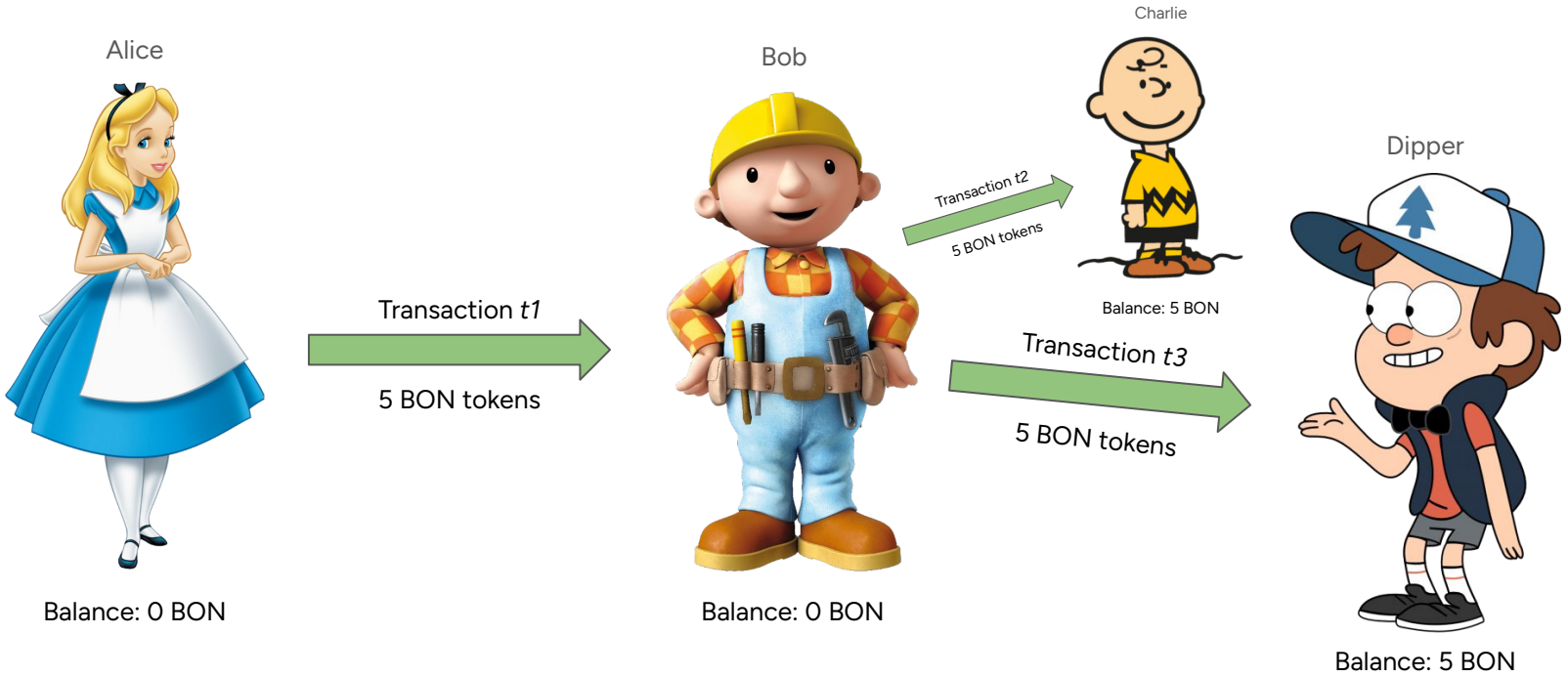
How to prevent Recursive Reversals



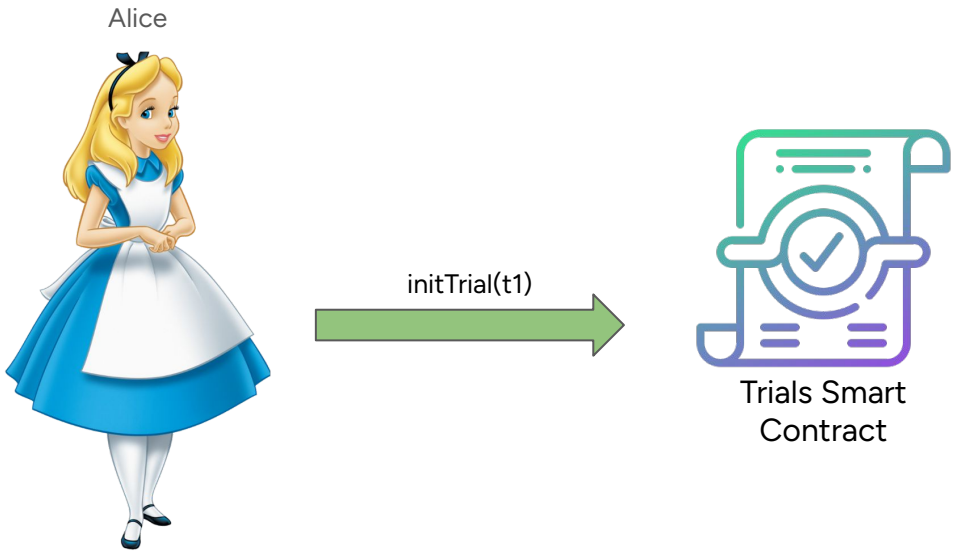
How to prevent Recursive Reversals



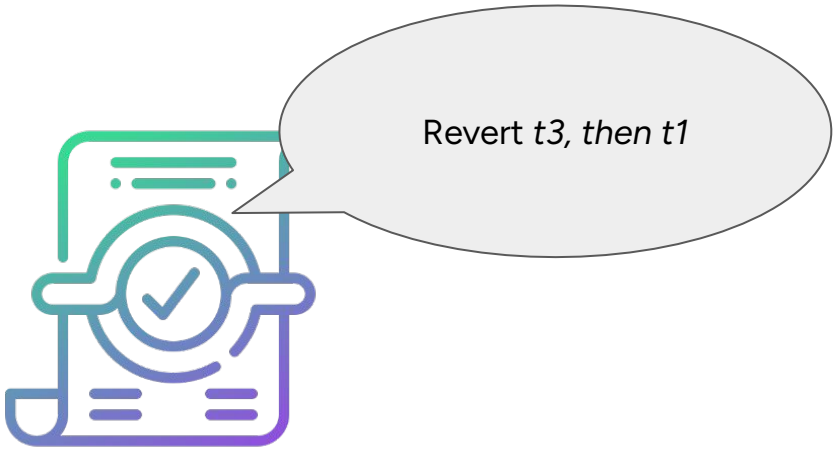
How to prevent Recursive Reversals



How to prevent Recursive Reversals



How to prevent Recursive Reversals



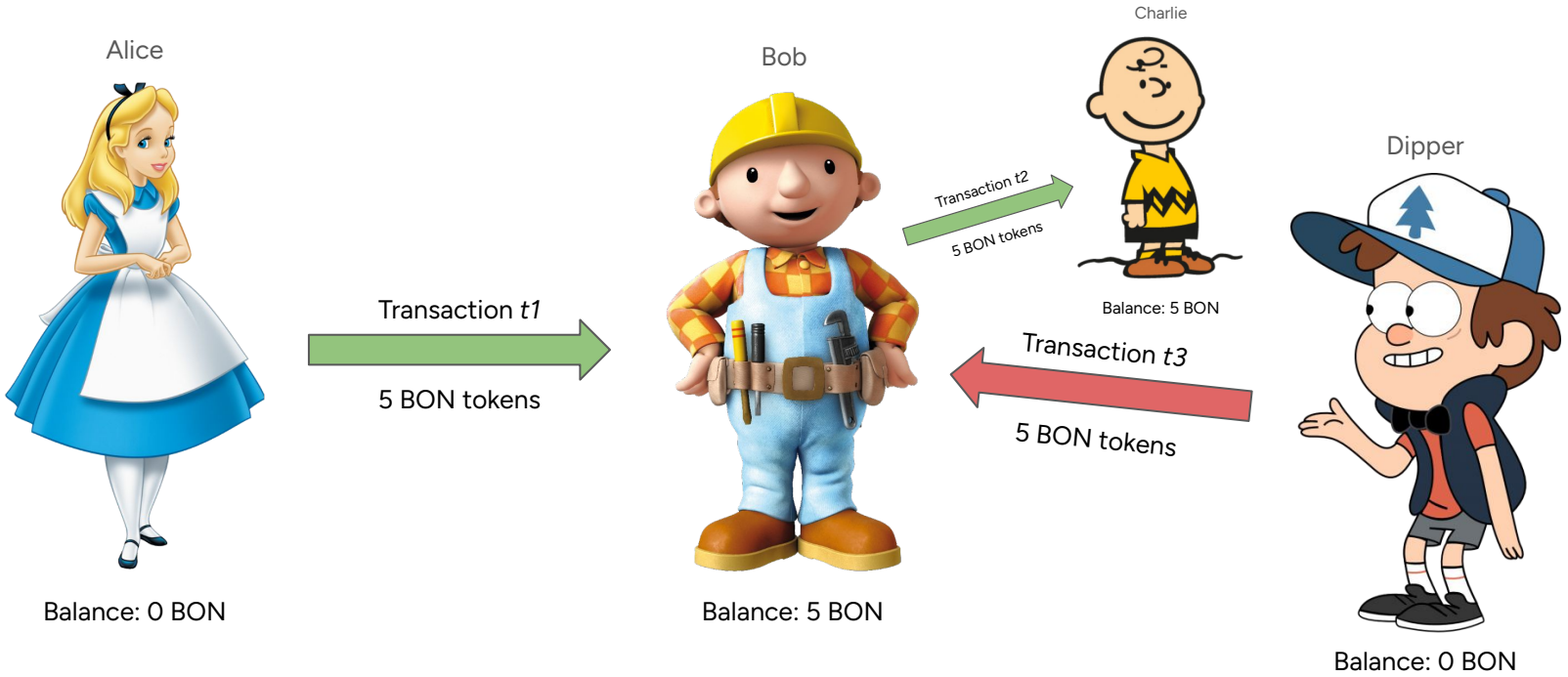
How to prevent Recursive Reversals

Algorithm 1 traceTransactions algorithm

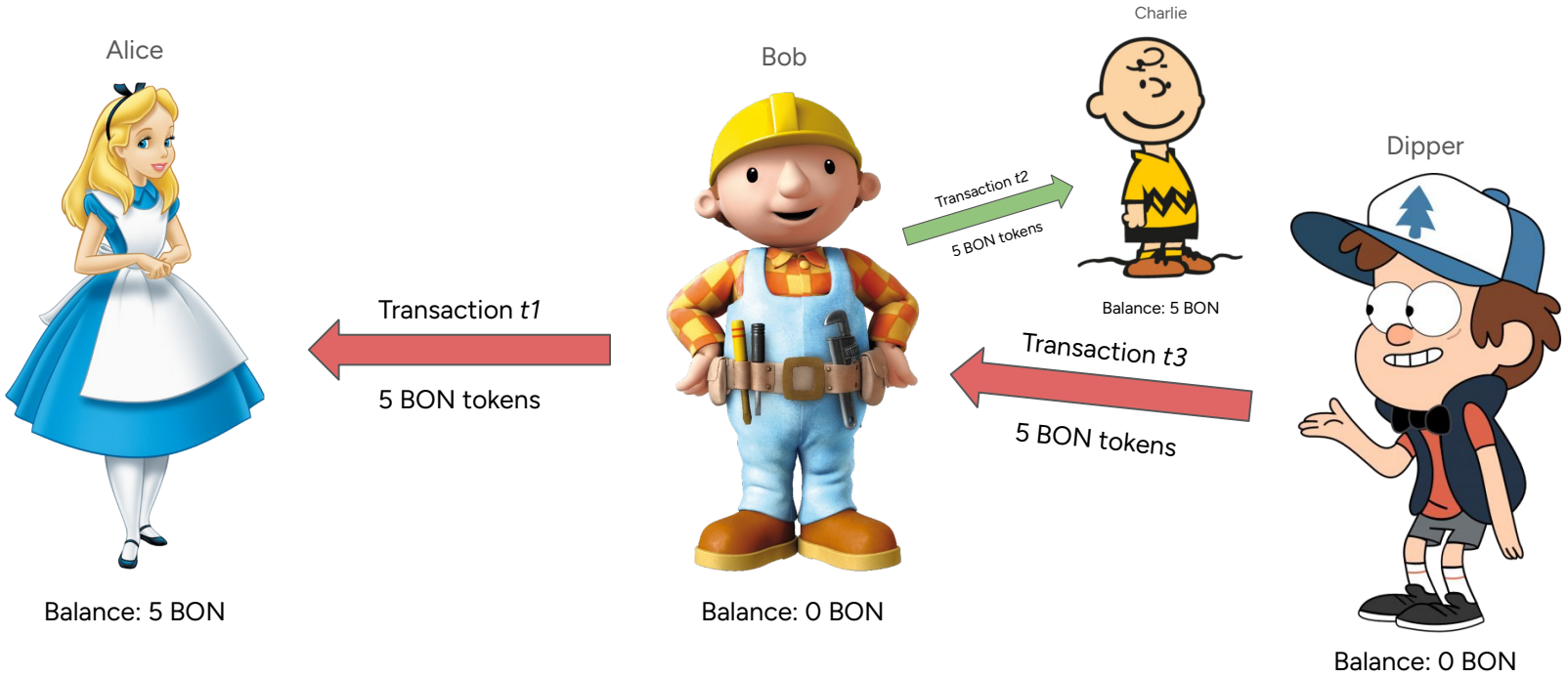
```
1: function TRACETRANSACTIONS(txID, needed, txsToRevert, freezed)
2:     tx ← getTxByID(txID)
3:     if balanceOf(tx.dest) − frozenBalanceOf(tx.dest) ≥ needed then
4:         toFreeze ← needed
5:     else
6:         toFreeze ← balanceOf(tx.dest)
7:     end if
8:     txsToRevert.push(txID)
9:     freezed.push(toFreeze)
10:    if toFreeze == needed then
11:        return (txsToRevert, freezed)
12:    end if
13:    needed ← needed − toFreeze
14:    issuedTxs ← getIssuedTxs(tx.dest)
15:    for t ∈ issuedTxs in reverse order do
16:        tx′ ← getTxByID(t)
17:        if tx′.ID < txID then
18:            continue
19:        end if
20:        (txsToRevert, freezed) ← TRACETRANSACTIONS(tx′.ID, needed, txsToRevert, freezed)
21:        if tx′.amount ≥ needed then
22:            needed ← 0
23:        else
24:            needed ← needed − tx′.amount
25:        end if
26:        if needed == 0 then
27:            break
28:        end if
29:    end for
30:    return (txsToRevert, freezed)
31: end function
```

$issuedTxs \leftarrow getIssuedTxs(tx.dest)$
for $t \in issuedTxs\ in\ reverse\ order$ **do**

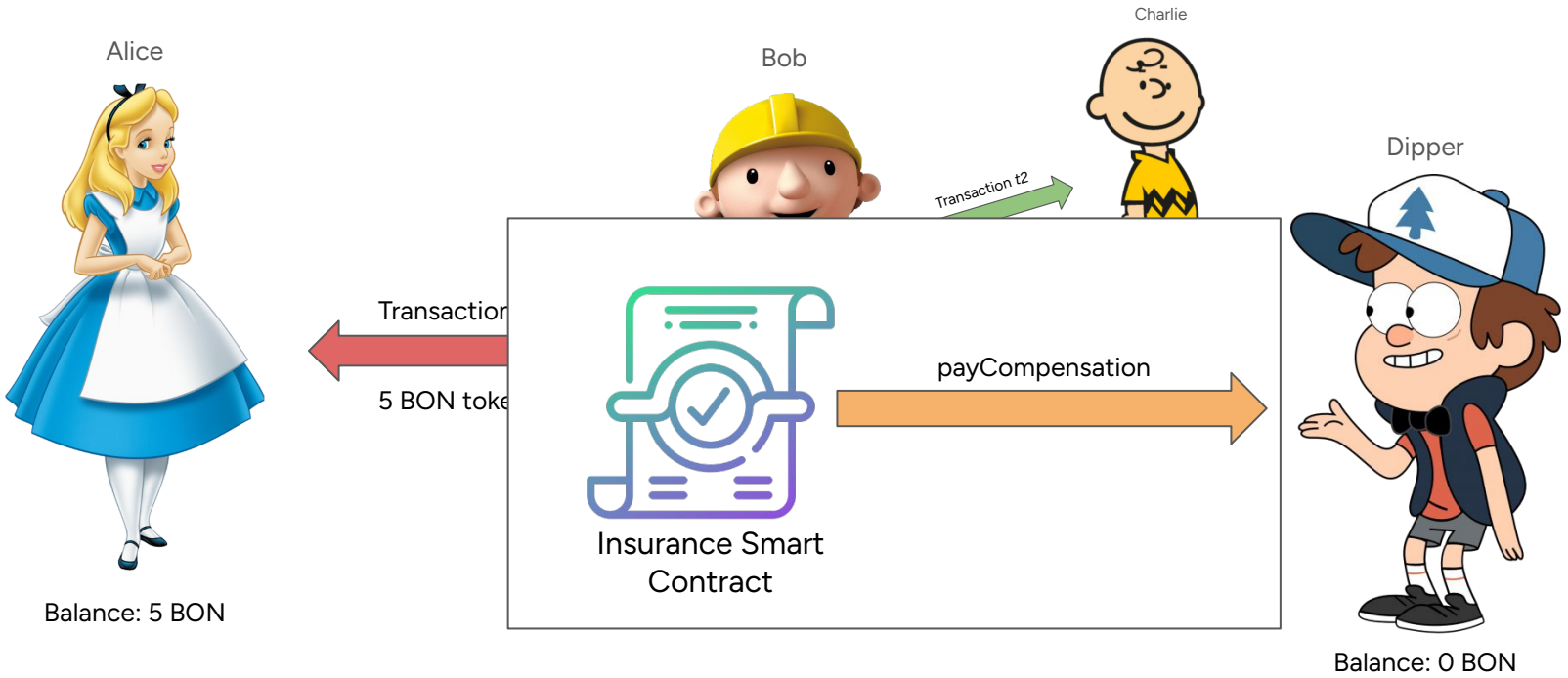
How to prevent Recursive Reversals



How to prevent Recursive Reversals



How to prevent Recursive Reversals



Insurance Problem Example

Insurance Problem Example

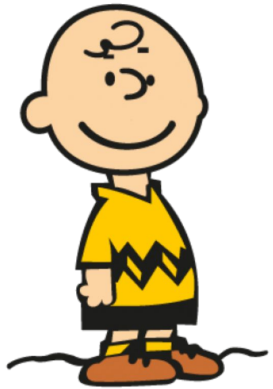
Alice

Balance: 0 BON

Bob

Balance: 0 BON

Charlie



Balance: 0 BON

Insurance Problem Example

Alice

Balance: 0 BON

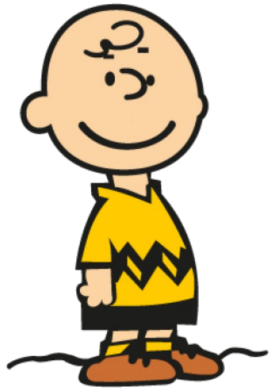
Transaction *t1*

5 BON tokens
(0.25 tokens paid to
the Insurance)

Bob

Balance: 5 BON

Charlie



Balance: 0 BON

Insurance Problem Example

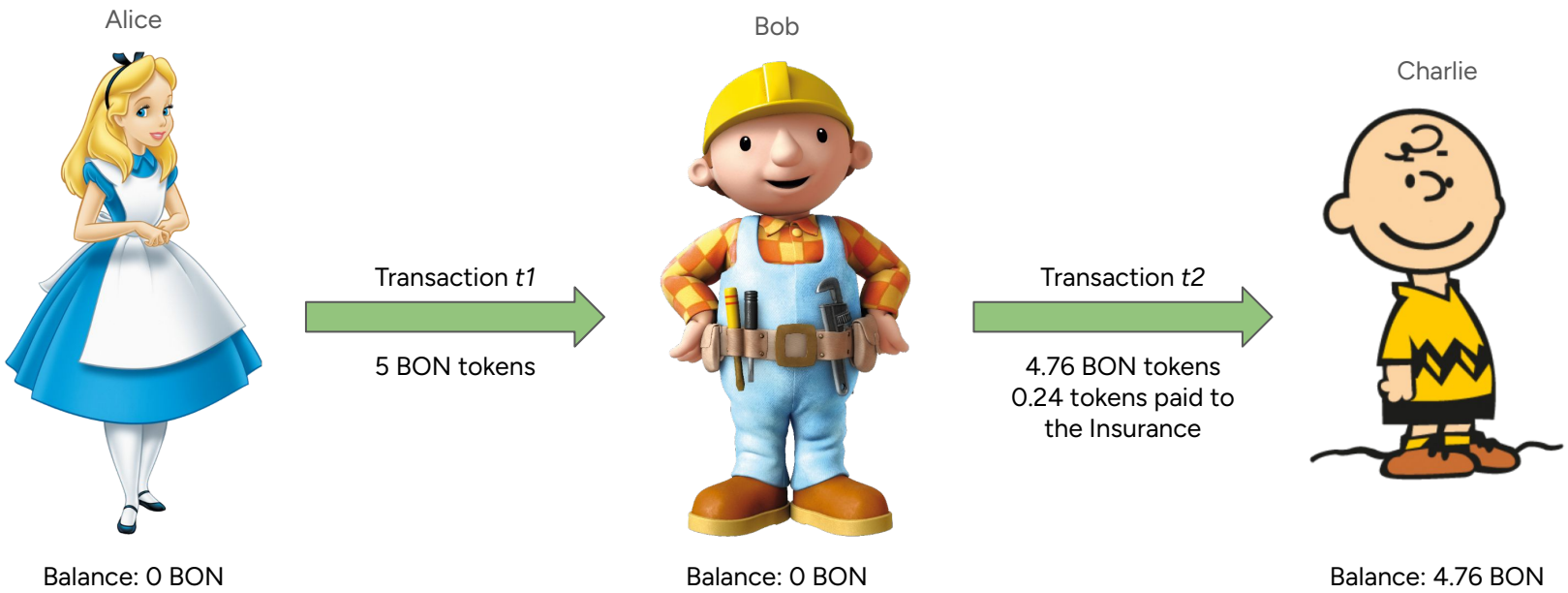
Bob

Balance: 5 BON

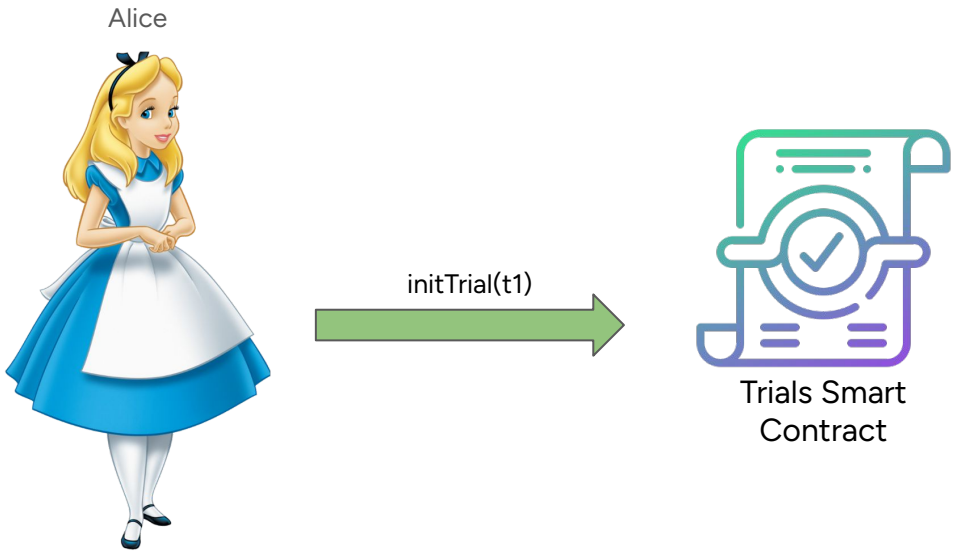
- ➔ Bob's balance is now 5 BON tokens, where all are unstable
- ➔ 5% fee required on every tx
- ➔ Maximum to be sent is:

5/(1.05) = 4.76 tokens,
0.24 tokens paid to the Insurance

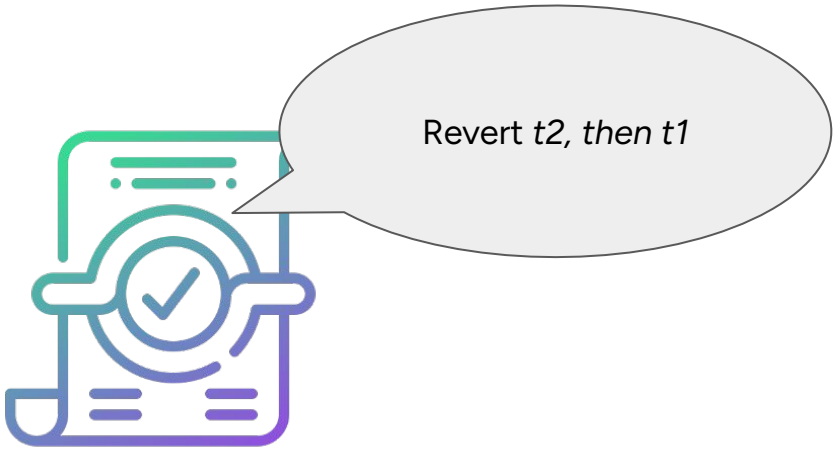
Insurance Problem Example



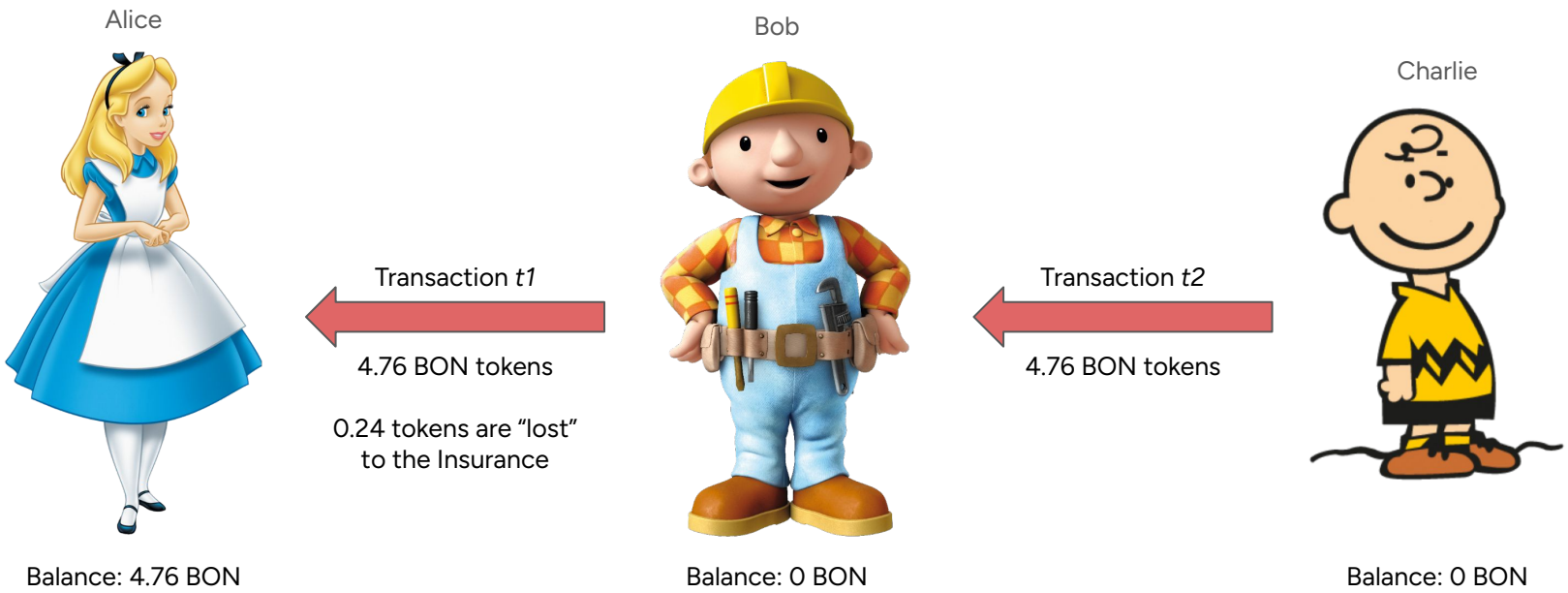
Insurance Problem Example



Insurance Problem Example



Insurance Problem Example



How to mitigate this

- ➔ Remove insurance
  - ◆ system would loose uniqueness
  - ◆ recursive reversals not solved - system similar to ERC-20R
- ➔ Reverse Insurance payments associated with transactions
  - ◆ would impact plafond
  - ◆ problem of who would pay the 1st reversal request fee
- ➔ Covering losses using Plafond
  - ◆ impact users with low plafond scores
- ➔ Temporarily freezing funds

Temporarily freezing funds

- ➔ Lock tokens on destination address for a short period of time (e.g. 1 hour)
- ➔ Would limit immediate movement of funds
- ➔ Under this model the system could ensure recovery of at least

$$\frac{txAmount}{1.05^{h-1}}$$

h is the number of hours since the original transaction was confirmed on the network

- ➔ Would introduce additional complexity to the system and need for automated token (un)freezing to improve UX

Limitations and Proposed Future Work

Evidence types and security

- ➔ There is no mechanism to ensure authenticity of evidence submitted
- ➔ Current evidence submitted as plain text visible on block explorers
- ➔ In chain encryption could be used but would introduce overhead on key sharing operations

Trial Disruption

- ➔ Many mechanisms are in place to prevent unintended behavior but others could arise
  - illegal evidence submission
  - use of mixers
  - passive participation to stall trial process
- ➔ Extensions require to properly address all problems
  - social studies
  - identity verification - which would be difficult in public networks
  - advanced fraud detection

Arbitrator penalties

- ➔ Faulty arbitrators are not penalized in current version
- ➔ Voting ends after 2f+1 votes but does not necessarily mean arbitrators who have not voted are faulty
  - ◆ could just need more time to decide
- ➔ Each vote is personal and driven by each arbitrator's experience
  - ◆ thus they cannot be penalized for voting differently from the majority
- ➔ Future Work could include a penalty system

Block and watch lists

- ➔ Watch lists for users involved in reversals
  - ◆ additional information in future trials
- ➔ Block lists for correctly identified faulty arbitrators and users involved in lots of reversals (dest. source)
  - ◆ users would have the ability to appeal and be removed

Arbitrator picking with VRF

- ➔ Current picking method inspired by VRF but not truly random
- ➔ Used of Chainlink VRF directly would allow achieving the desired randomness and have a more robust system
- ➔ Funding using tokens from Insurance

Arbitrator pools

- ➔ Require arbitrators to hold at least *t* tokens the amount under trial
- ➔ Trials where possible arbitrator pool is too small and predictable
- ➔ Pool of arbitrators with token staking

Notification system

- ➔ On-chain event listeners linked with wallets sending notifications to interested addresses
- ➔ Improves user experience

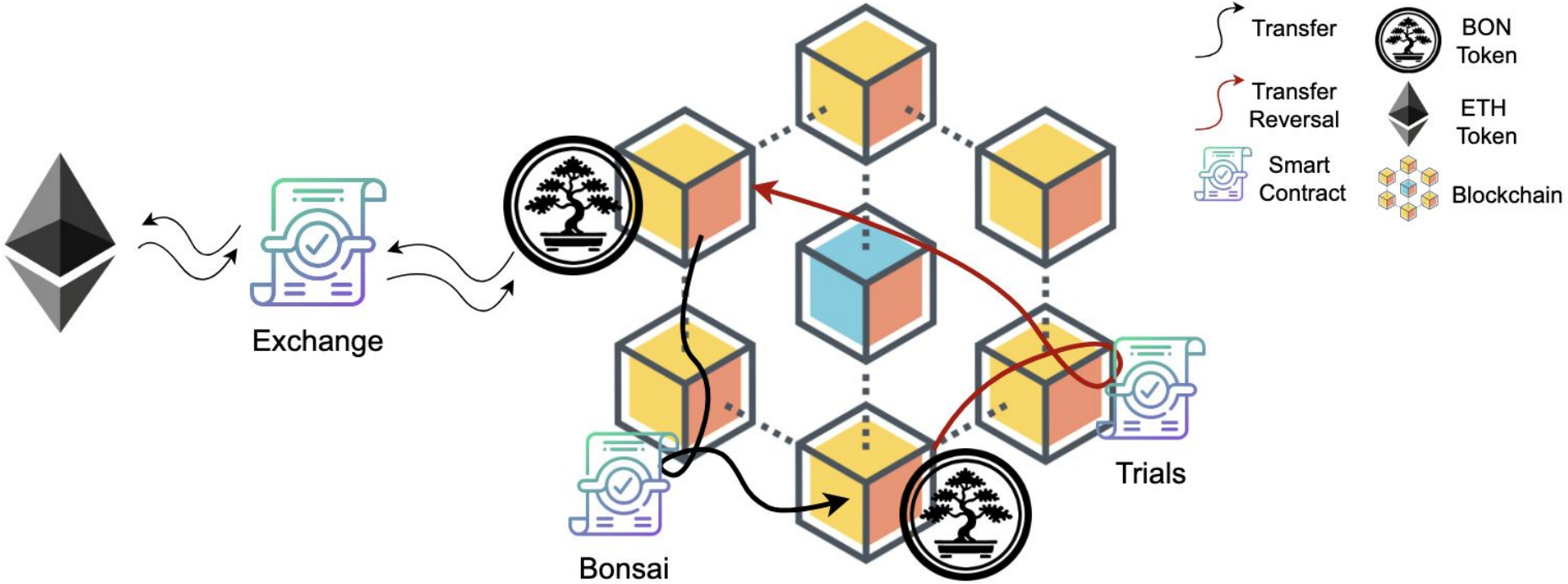
Automated transaction finalization

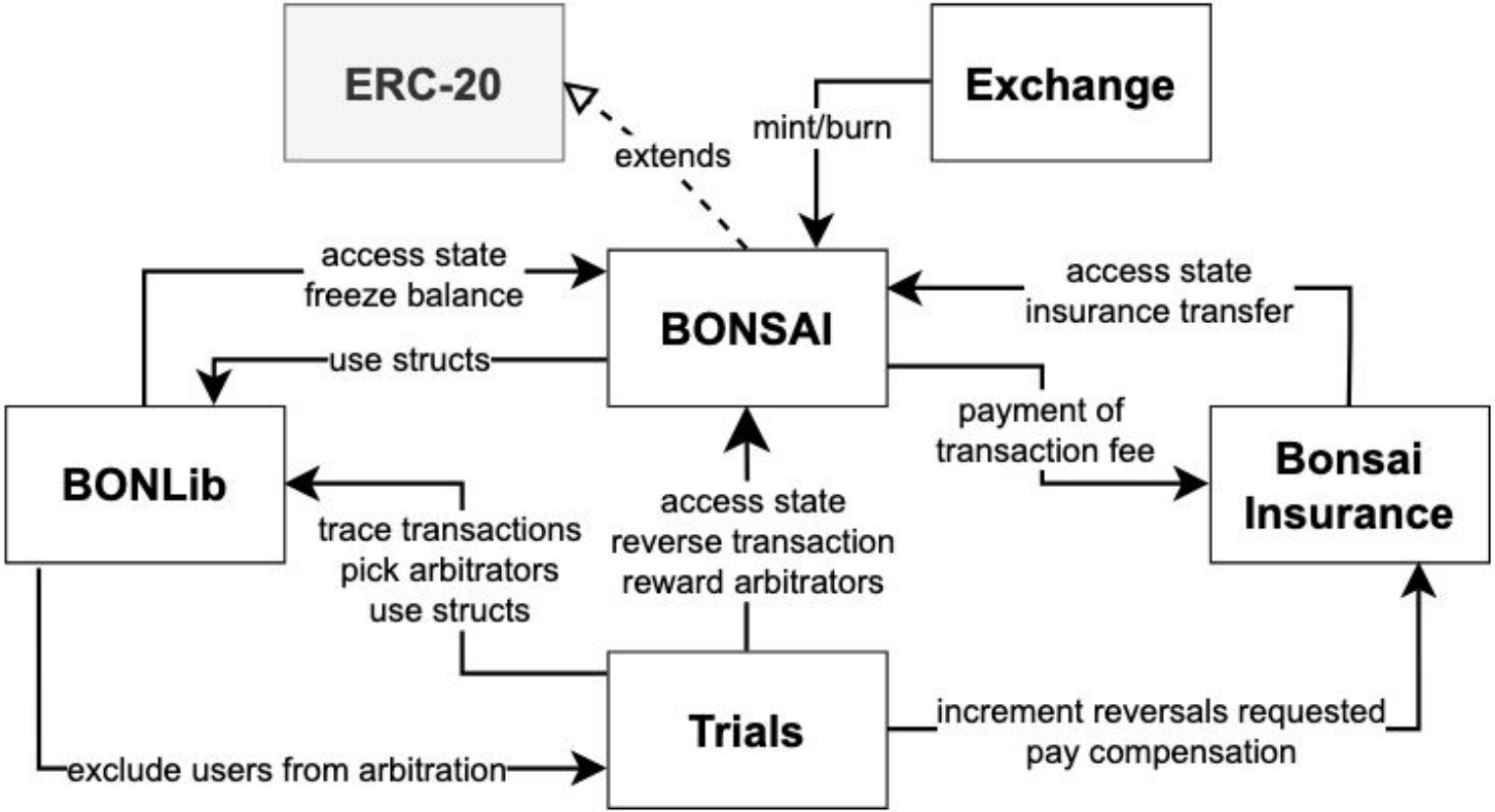
- ➔ Users required to finalize the transactions where they are the receiver to update stable balance
  - ◆ requires manual input and payment of gas fees
- ➔ Chainlink Automation Job Scheduler could be set to finalize all pending transactions, e.g., once per day
  - ◆ funding using Insurance tokens

New layer 2

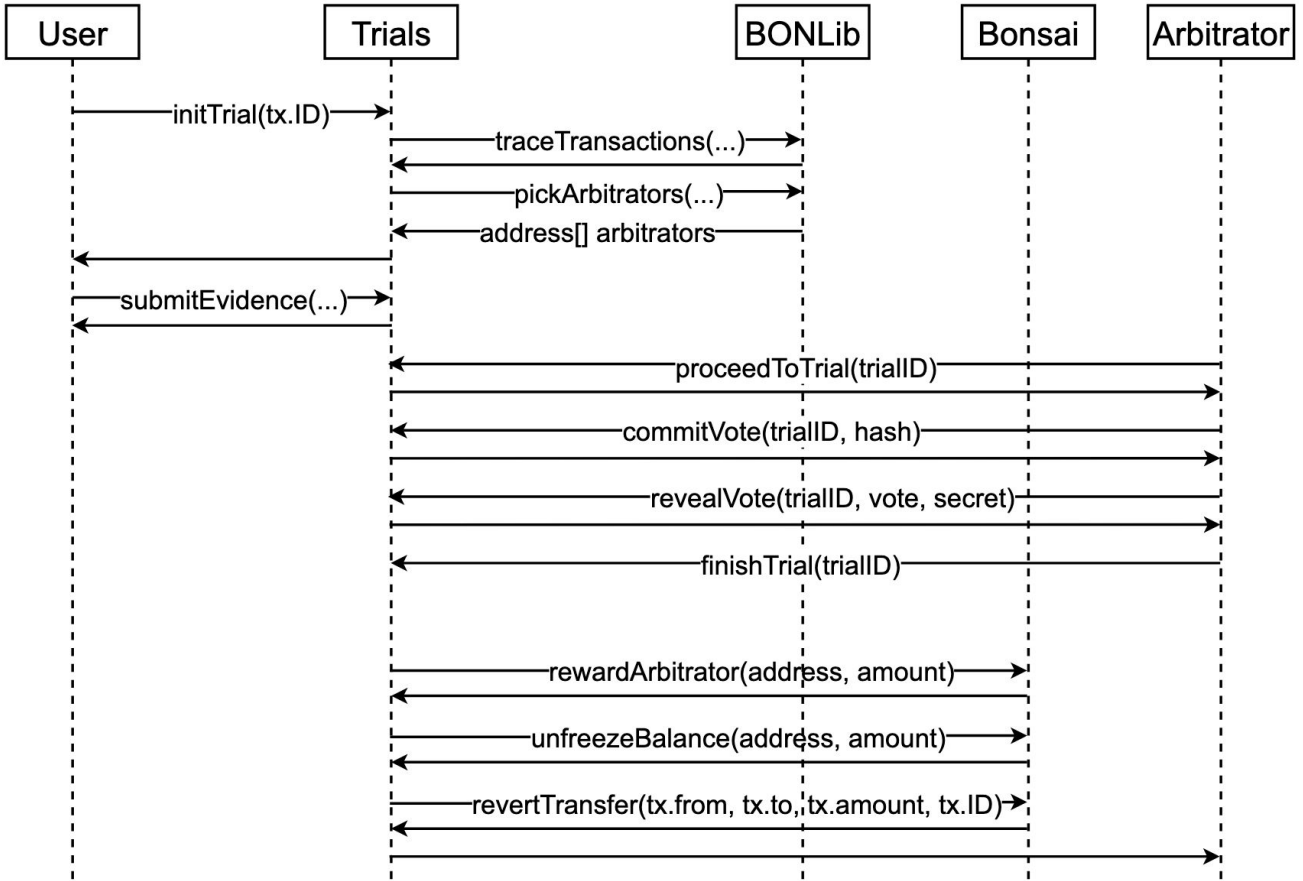
- ➔ Rollups with only finalized transactions
  - ◆ cool-down period expired
- ➔ Layer 2 consisting of mutable transactions
- ➔ Layer 1 immutable data

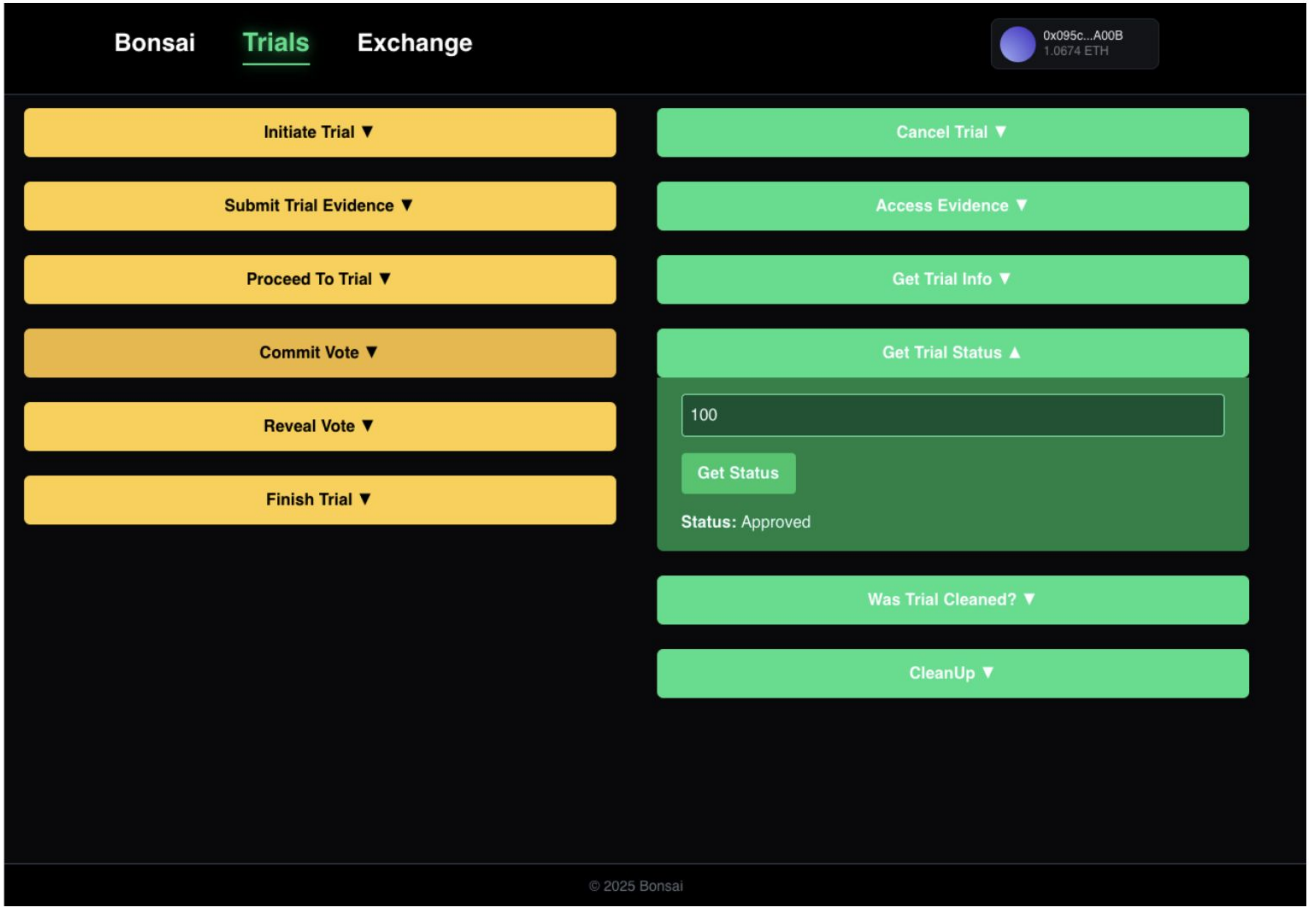
Thesis Images

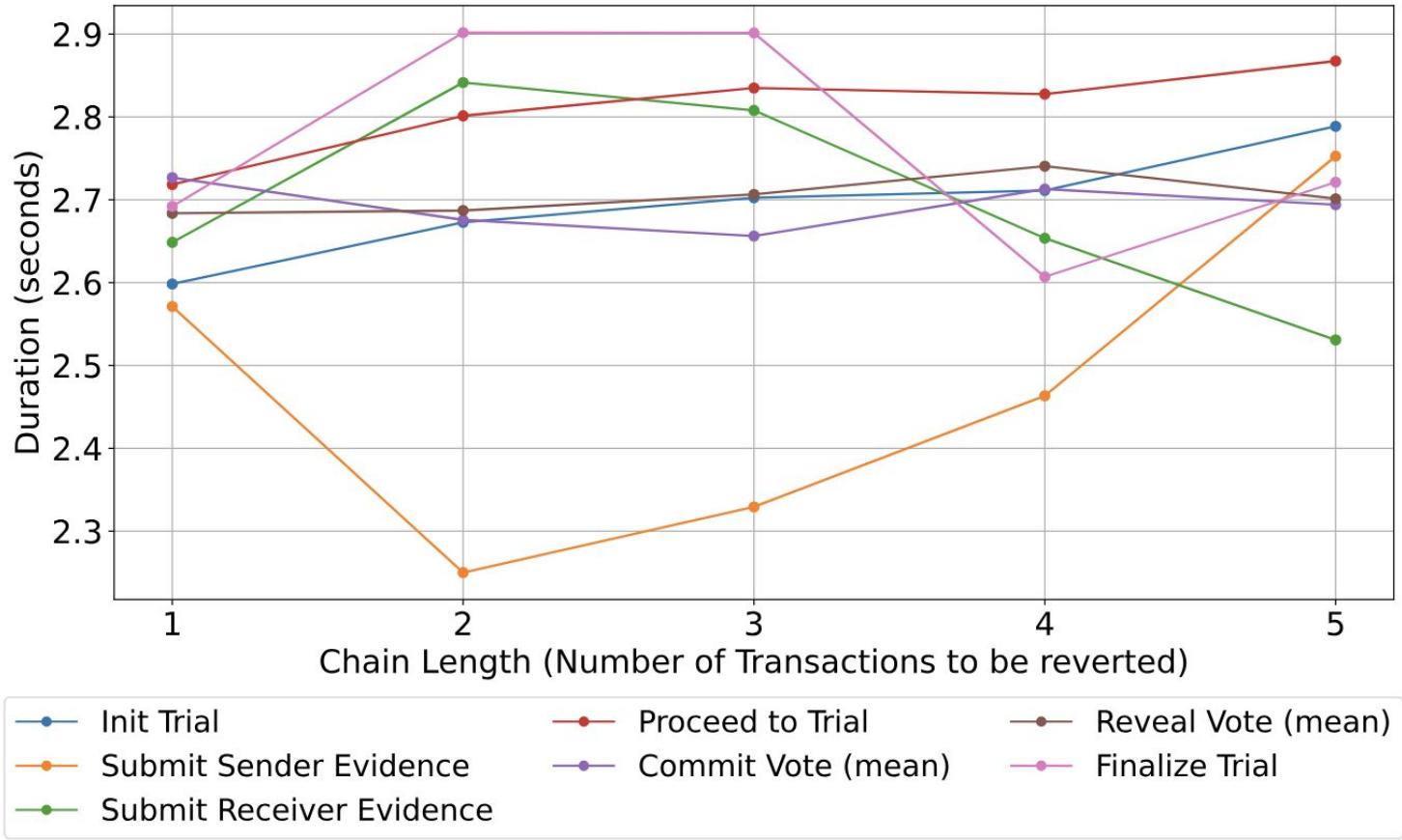

Transfer
Transfer Reversal
Smart Contract
BON Token
ETH Token
Blockchain
Exchange
Trials
Bonsai

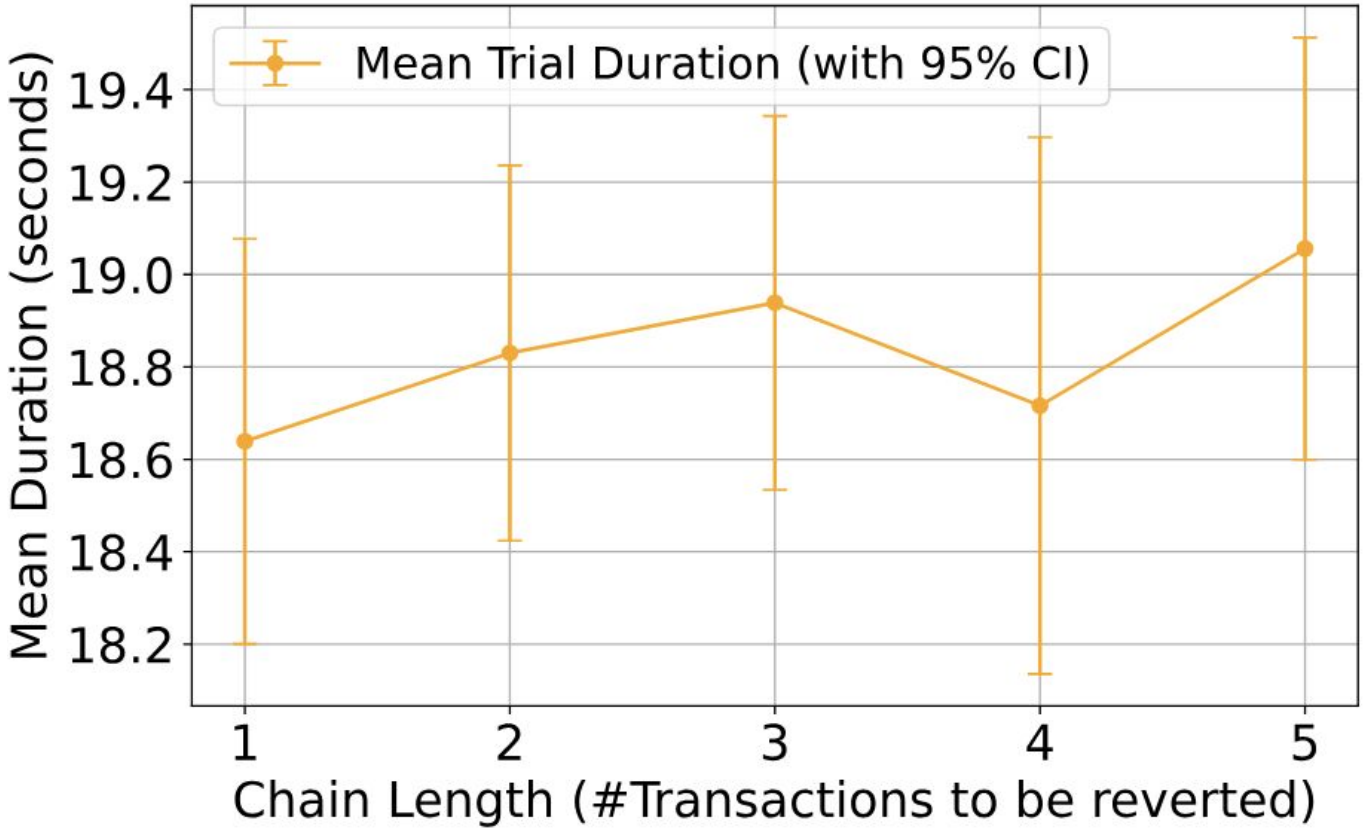

ERC-20
extends
Exchange
mint/burn
access state
freeze balance
BONSAI
access state
insurance transfer
use structs
payment of
transaction fee
BONLib
Bonsai
Insurance
trace transactions
pick arbitrators
use structs
access state
reverse transaction
reward arbitrators
Trials
increment reversals requested
pay compensation
exclude users from arbitration

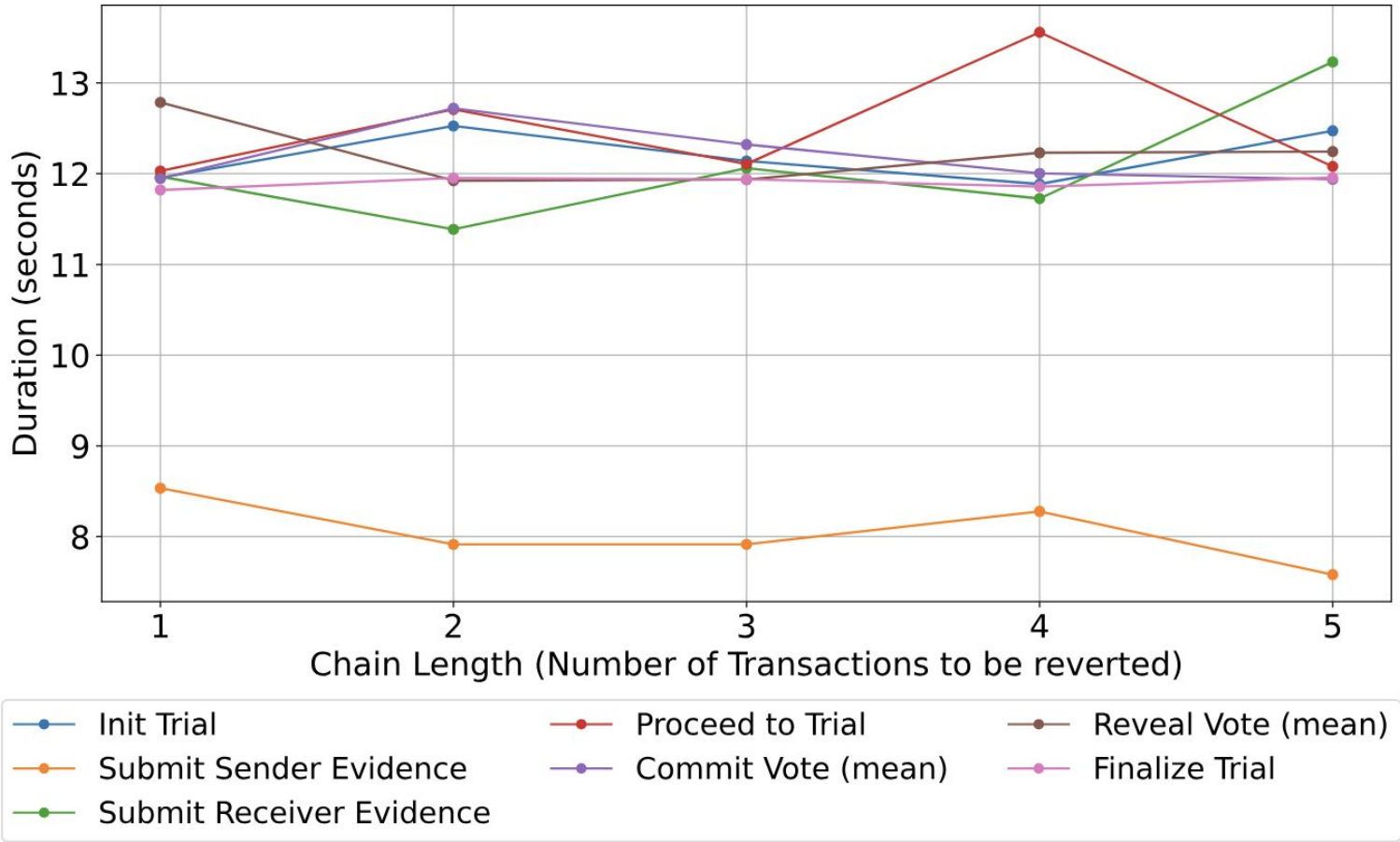
```
{
 "txID": 0,
 "ipfsUrl": "https://ipfs.io/ipfs/
QmXoypizjW3WknFiJnKLwHCnL72vedxjQkDDP1mXWo6uco",
 "evidenceHash":
"2c26b46b68ffc68ff99b453c1d30413413422e4f173dc59c51f3d1d5e
e6f7f90",
 "description": "Theft report, witness statements, proof
of agreement"
}
```

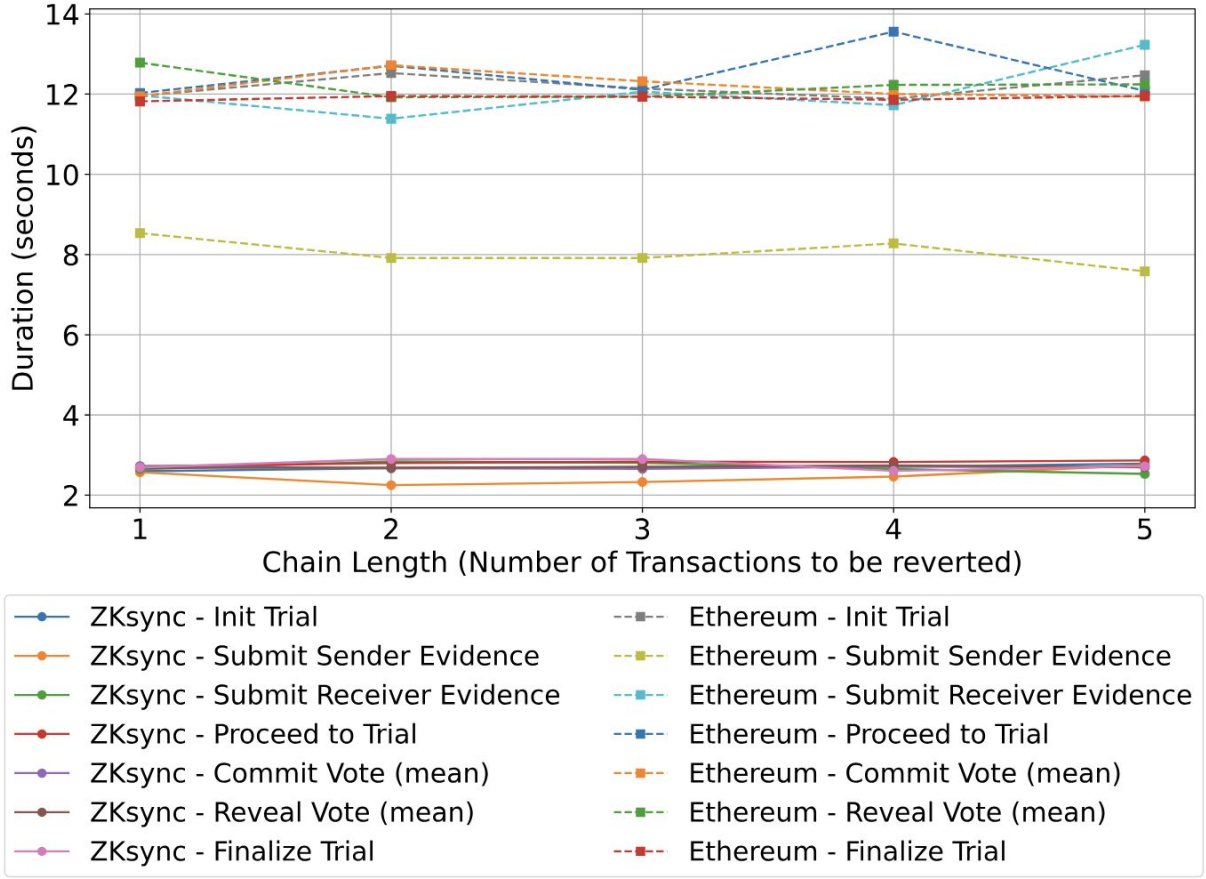

User
Trials
BONLib
Bonsai
Arbitrator
initTrial(tx.ID)
traceTransactions(...)
pickArbitrators(...)
address[] arbitrators
submitEvidence(...)
proceedToTrial(trialID)
commitVote(trialID, hash)
revealVote(trialID, vote, secret)
finishTrial(trialID)
rewardArbitrator(address, amount)
unfreezeBalance(address, amount)
revertTransfer(tx.from, tx.to, tx.amount, tx.ID)

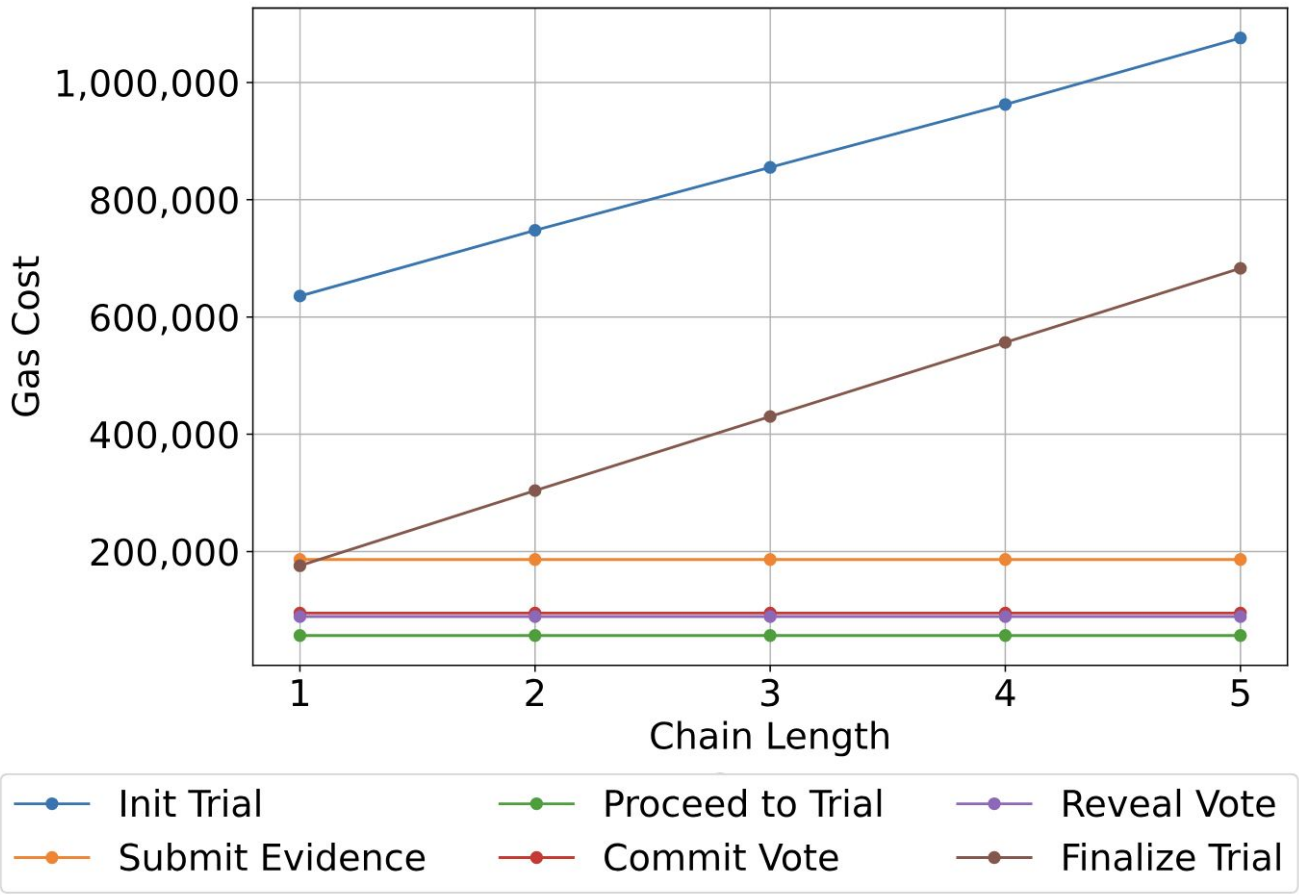

Bonsai
Trials
Exchange
0x095c...A00B
1.0674 ETH
Initiate Trial ▼
Submit Trial Evidence ▼
Proceed To Trial ▼
Commit Vote ▼
Reveal Vote ▼
Finish Trial ▼
Cancel Trial ▼
Access Evidence ▼
Get Trial Info ▼
Get Trial Status ▲
100
Get Status
Status: Approved
Was Trial Cleaned? ▼
CleanUp ▼
© 2025 Bonsai


Duration (seconds)
2.9
2.8
2.7
2.6
2.5
2.4
2.3
1
2
3
4
5
Chain Length (Number of Transactions to be reverted)
Init Trial
Submit Sender Evidence
Submit Receiver Evidence
Proceed to Trial
Commit Vote (mean)
Reveal Vote (mean)
Finalize Trial


Mean Trial Duration (with 95% CI)
Mean Duration (seconds)
19.4
19.2
19.0
18.8
18.6
18.4
18.2
1
2
3
4
5
Chain Length (#Transactions to be reverted)


Duration (seconds)
13
12
11
10
9
8
1
2
3
4
5
Chain Length (Number of Transactions to be reverted)
Init Trial
Submit Sender Evidence
Submit Receiver Evidence
Proceed to Trial
Commit Vote (mean)
Reveal Vote (mean)
Finalize Trial


Duration (seconds)
14
12
10
8
6
4
2
1
2
3
4
5
Chain Length (Number of Transactions to be reverted)
ZKsync - Init Trial
ZKsync - Submit Sender Evidence
ZKsync - Submit Receiver Evidence
ZKsync - Proceed to Trial
ZKsync - Commit Vote (mean)
ZKsync - Reveal Vote (mean)
ZKsync - Finalize Trial
Ethereum - Init Trial
Ethereum - Submit Sender Evidence
Ethereum - Submit Receiver Evidence
Ethereum - Proceed to Trial
Ethereum - Commit Vote (mean)
Ethereum - Reveal Vote (mean)
Ethereum - Finalize Trial


1,000,000
800,000
600,000
400,000
200,000
Gas Cost
1
2
3
4
5
Chain Length
Init Trial
Submit Evidence
Proceed to Trial
Commit Vote
Reveal Vote
Finalize Trial

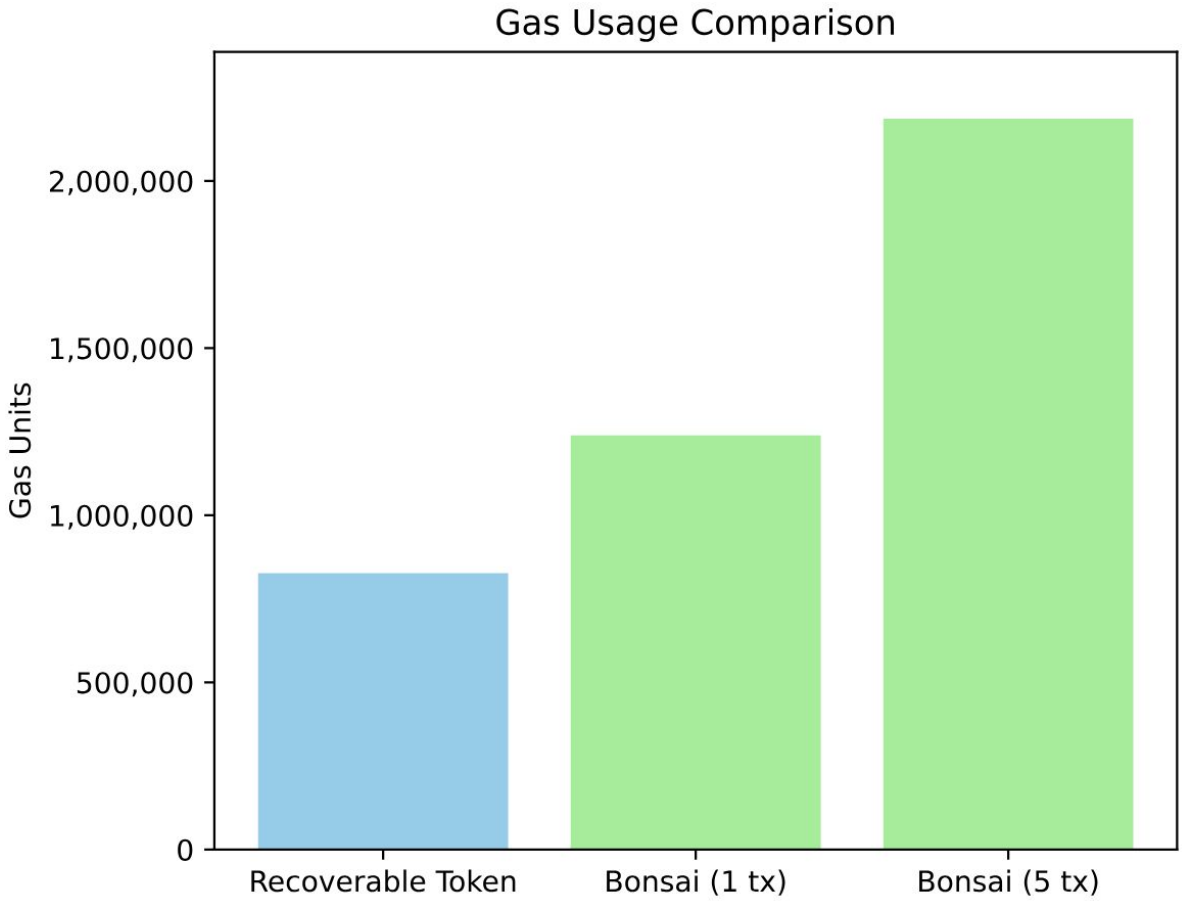
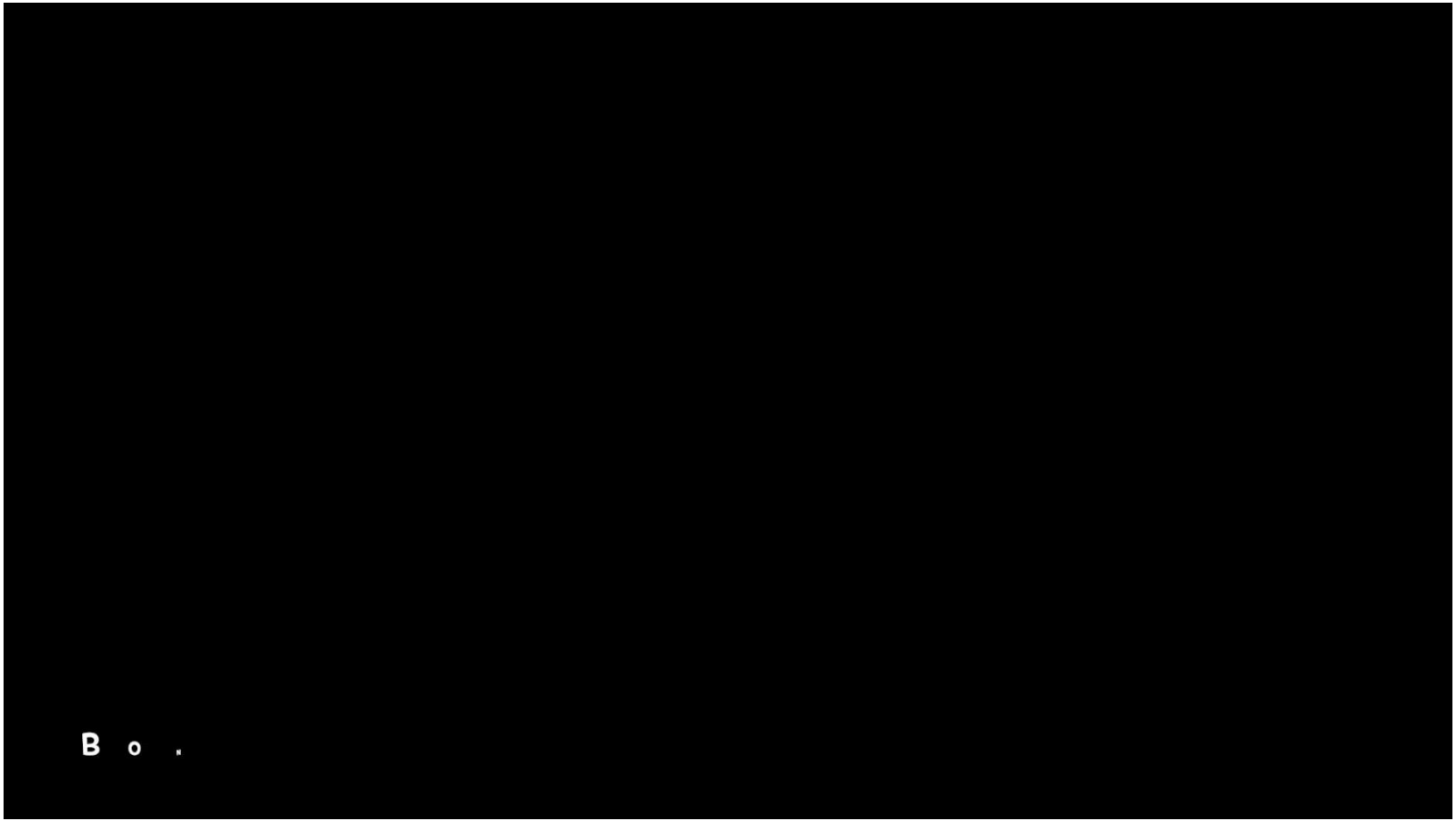

Gas Usage Comparison
Gas Units
2,000,000
1,500,000
1,000,000
500,000
0
Recoverable Token
Bonsai (1 tx)
Bonsai (5 tx)

Table 2.1: Comparison between Optimistic Rollups and Zero Knowledge Rollups.

Feature	**Optimistic Rollups**	**Zero Knowledge Rollups**
Proof Mechanism	Fraud Proofs	Zero-Knowledge Proofs
Finality Speed	Slow (challenge period)	Fast (instant verification)
Gas Costs	Lower computation, higher withdrawal costs	Higher computation, lower withdrawal costs
Security	Correctness assumed unless challenged	Immediate cryptographic verification
Compatibility	Fully supports EVM	Limited EVM compatibility
Withdrawal Time	$\sim$1 week (due to challenge period)	Almost instant

Table 3.1: Comparison between Bonsai and other approaches

Characteristic	Bonsai	Recoverable Token	ERC-20R
Prevents burning of unstable tokens	Yes	No	Maybe
Keeps arbitrators' votes private	Yes	No	Maybe
Allows to compensate victims of recursive reversals	Yes	No	No
Has two different balances inside the network	No	No	Yes
Protects against liquidity pools	Yes	No	No
Keeps arbitrators' committees decentralized	Yes	No	No


B o .

Objectives

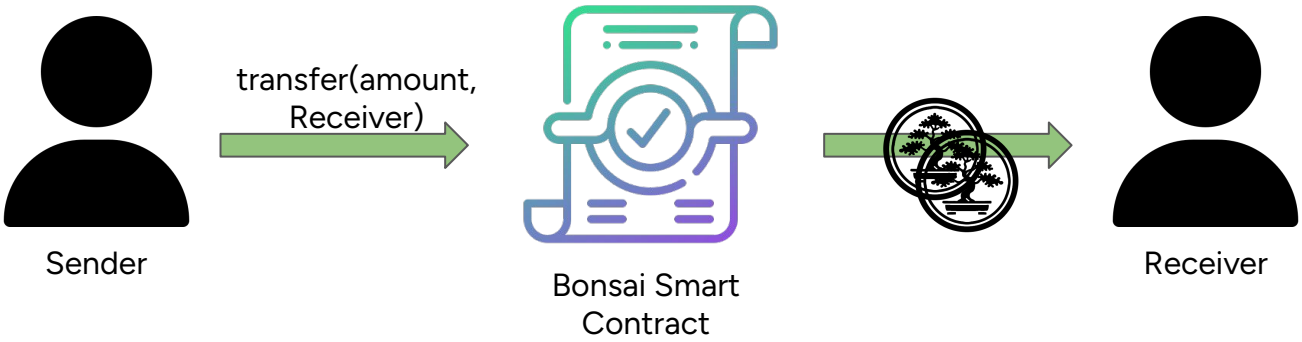
Objectives

- Recover from errors and intrusions
- Address immutability of Blockchain
- Achieve low latency and lower costs compared with previous work

Intrusion Recovery Systems

- ➔ Selective Re-execution
- ➔ Compensating Transactions
- ➔ Multi-versioned systems

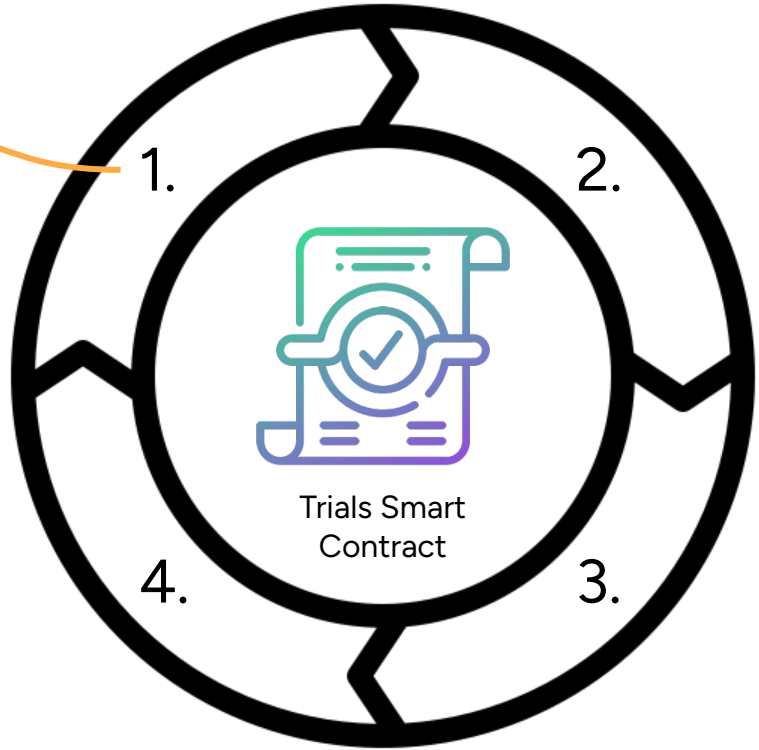
Token Operations - Transfer of BON



Token Operations - getting ETH

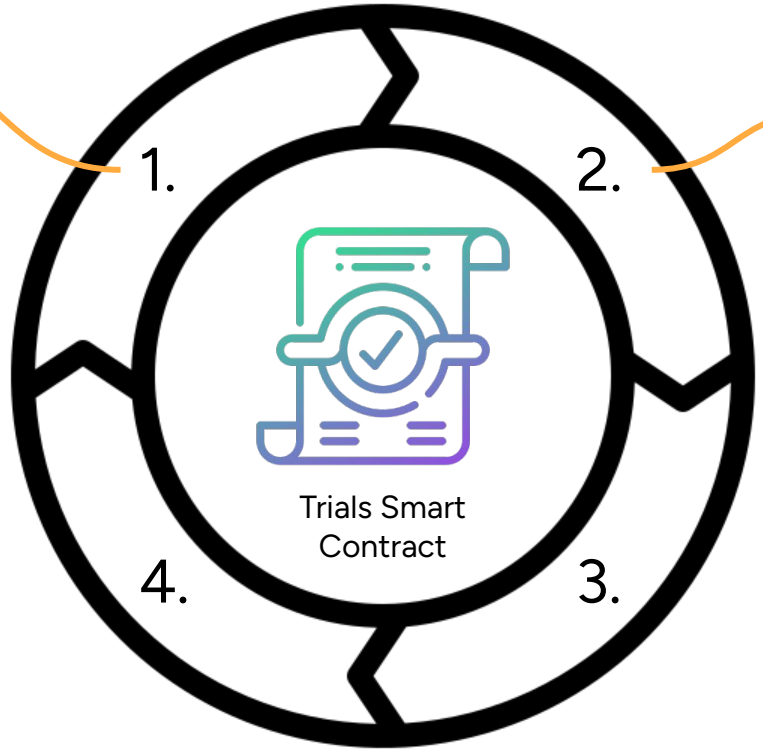
Trial Initiation - step 1

Trace transactions
- find tokens on users balances



Trial Initiation - step 2

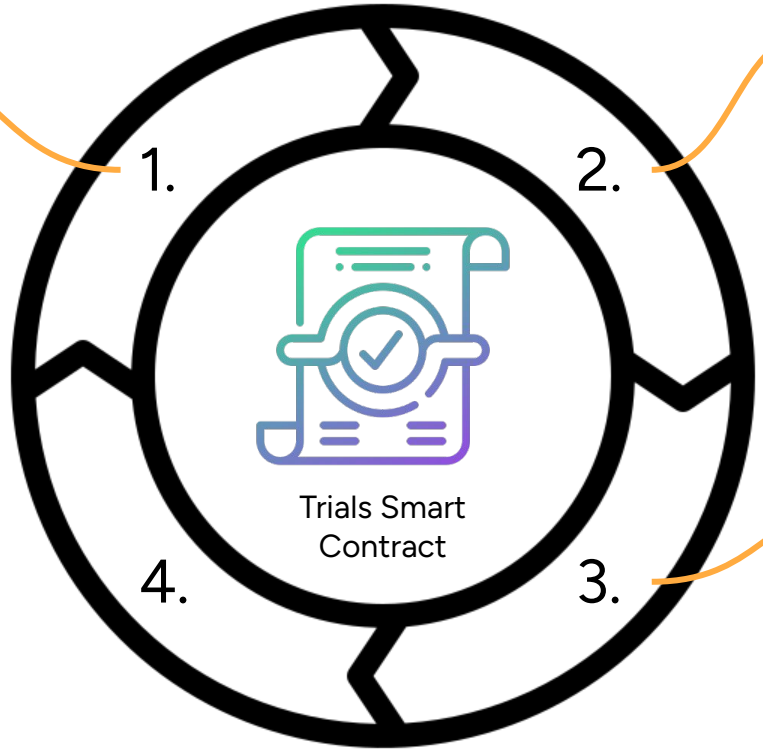
Trace transactions



Freeze Balances
- avoid users from spending funds signaled for reversal

Trial Initiation - step 3

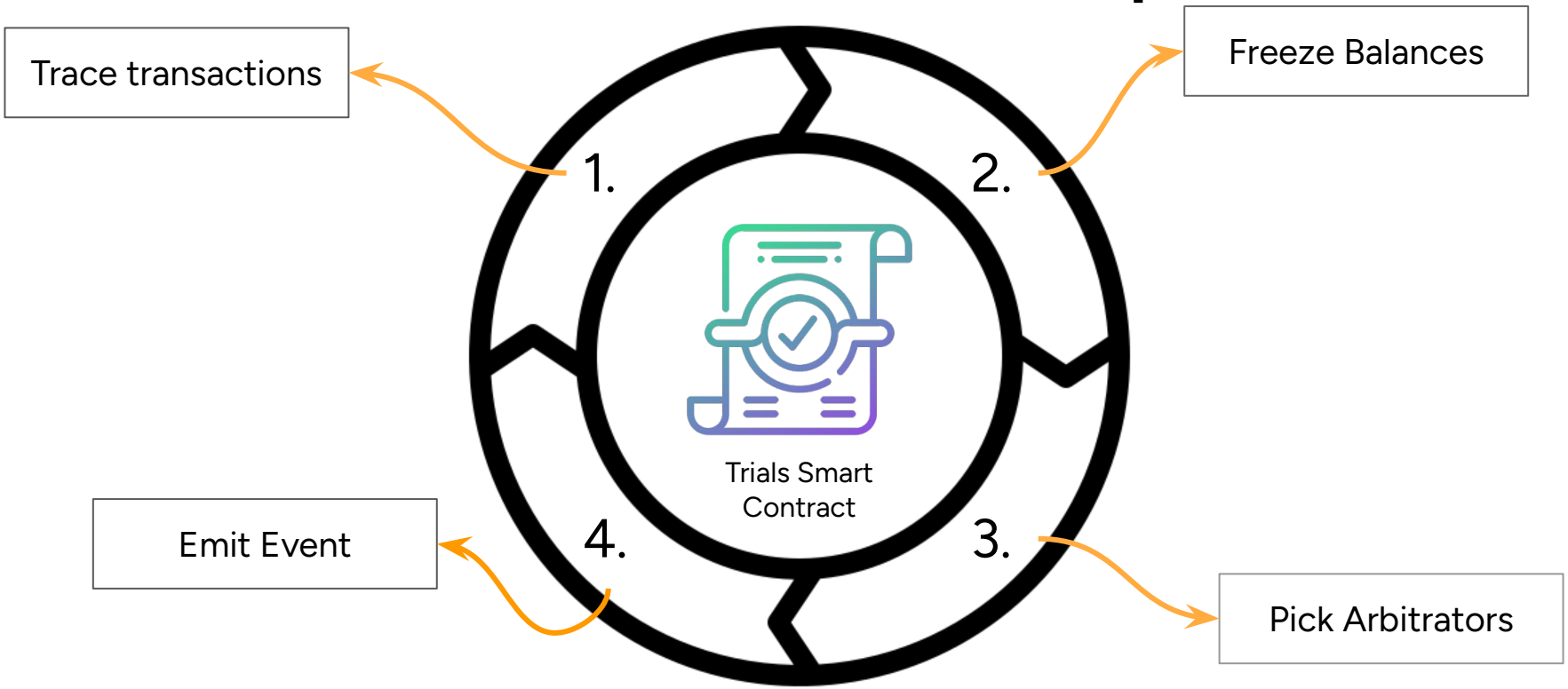
Trace transactions



Freeze Balances

Pick Arbitrators
- “randomly” from all users holding BON

Trial Initiation - step 4



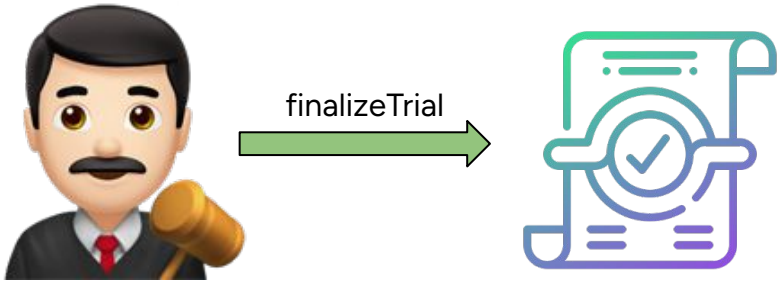
Trials

Arbitrator

commitVote

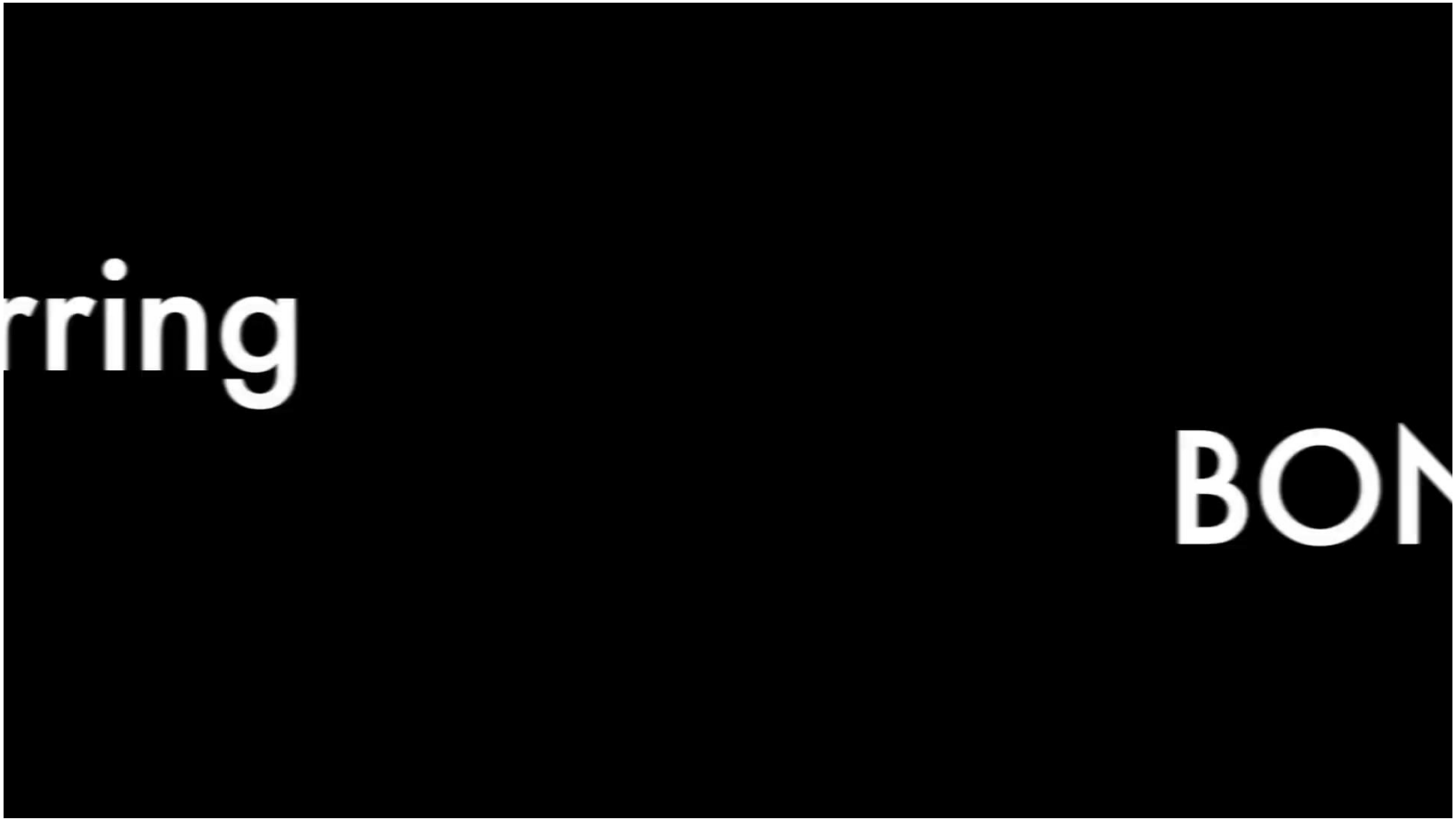
Trials Smart Contract

Trials



Trials

Demo


rring
BON

Source Code

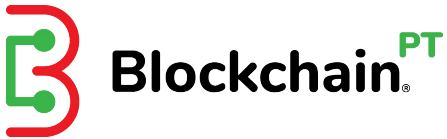
- ➔ Metrics: Size, Gas, Deployment costs
- ➔ Contracts Analysis: Slither[3]

Contract	Deployed Size (Byte)	Gas	LoC	Ethereum (USD)	ZKsync (USD)
Bonsai	20870	4386889	355	$30.88	$0.87
Trials	21917	4700802	377	$33.06	$0.94
BONLib	8861	1848415	205	$13.00	$0.37
BonsaiInsurance	5260	1098205	123	$7.74	$0.22
Exchange	2423	517301	40	$3.64	$0.10
Total	**59331**	**12551612**	**1100**	**$88.32**	**$2.50**

[3] https://github.com/crytic/slither

Acknowledgments

Work supported by national funds through Fundação para a Ciência e a Tecnologia, I.P. (FCT) under projects UID/50021/2025 and UID/PRR/50021/2025 (INESC-ID), 2024.07494.IACDC (WELL), and Project Blockchain.PT – Decentralize Portugal with Blockchain Agenda, (Project no 51), WP 1: Agriculture and Agri-food, Call no 02/C05-i01.01/2022, funded by the Portuguese Recovery and Resilience Program (PRR), The Portuguese Republic and The European Union (EU) under the framework of Next Generation EU Program.



Article Publication - NCA 2025

The 23rd IEEE International Symposium on Network Computing and Applications - November 5-7th, 2025

Bonsai: A Recovery Approach for Ethereum ERC-20 Transactions

Diogo Melita, David R. Matos, and Miguel L. Pardal
INESC-ID, Instituto Superior Técnico, University of Lisbon, Portugal
{diogo.melita, david.r.matos, miguel.pardal}@tecnico.ulisboa.pt