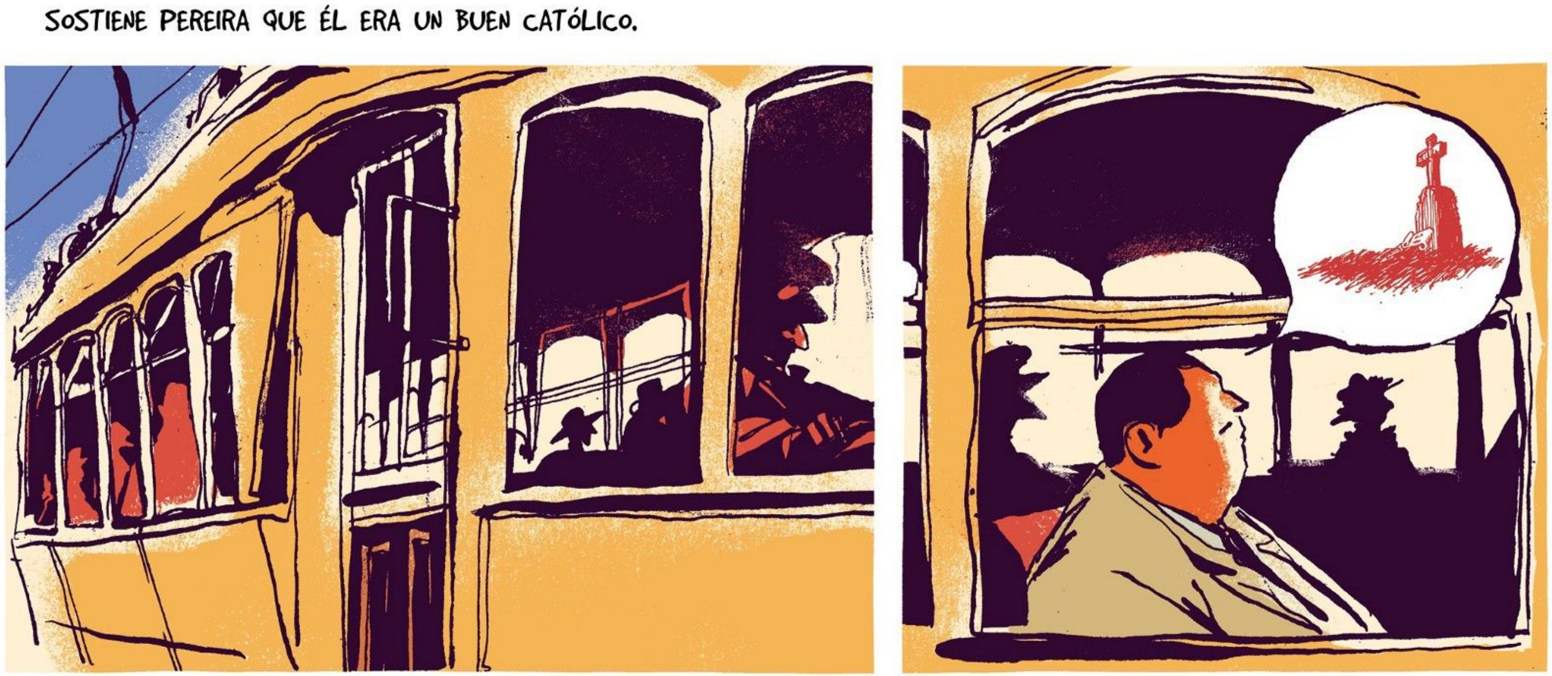
State channels with state assertions

Chris Buckland and Patrick McCorry



State channels

A **known set** of cooperating participants achieve local consensus, whilst relying on the blockchain to achieve **safety** and **liveness**

State channels

A **known set** of cooperating participants achieve local consensus, whilst relying on the blockchain to achieve **safety** and **liveness**

1. Participants commit funds to the channel under some initial conditions

State channels

A **known set** of cooperating participants achieve local consensus, whilst relying on the blockchain to achieve **safety** and **liveness**

1. Participants commit funds to the channel under some initial conditions
2. Parties sign new states off-chain

State channels

A **known set** of cooperating participants achieve local consensus, whilst relying on the blockchain to achieve **safety** and **liveness**

1. Participants commit funds to the channel under some initial conditions
2. Parties sign new states off-chain
3. If parties cannot cooperate off-chain, one party can force the continuation on chain

State channels

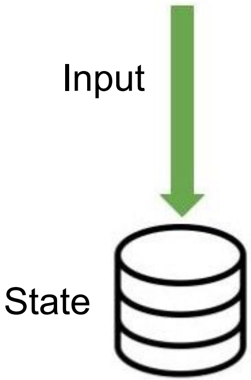
A **known set** of cooperating participants achieve local consensus, whilst relying on the blockchain to achieve **safety** and **liveness**

1. Participants commit funds to the channel under some initial conditions
2. Parties sign new states off-chain
3. If parties cannot cooperate off-chain, one party can force the continuation on chain
4. When parties move state back on-chain they are both given an opportunity to present their latest state - “Dispute resolution”

So what’s the problem?

A cooperation break down results in the usual costly **transaction fees**, and high latency

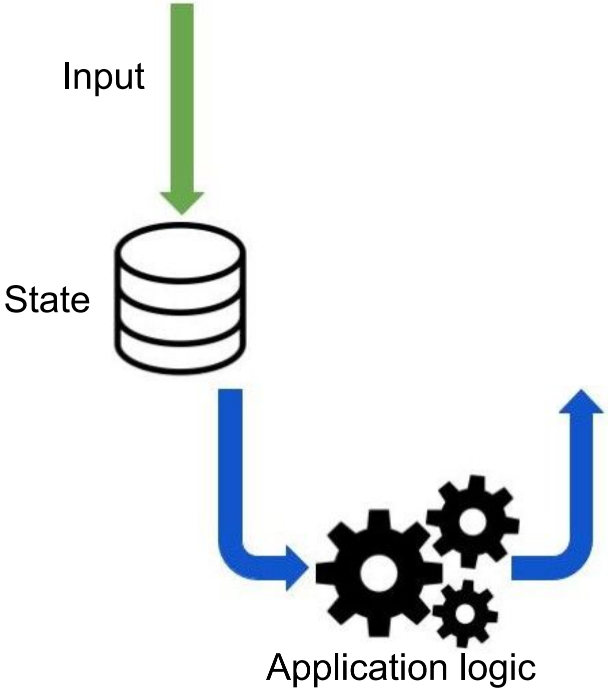
Smart contracts



Input

State

Smart contracts

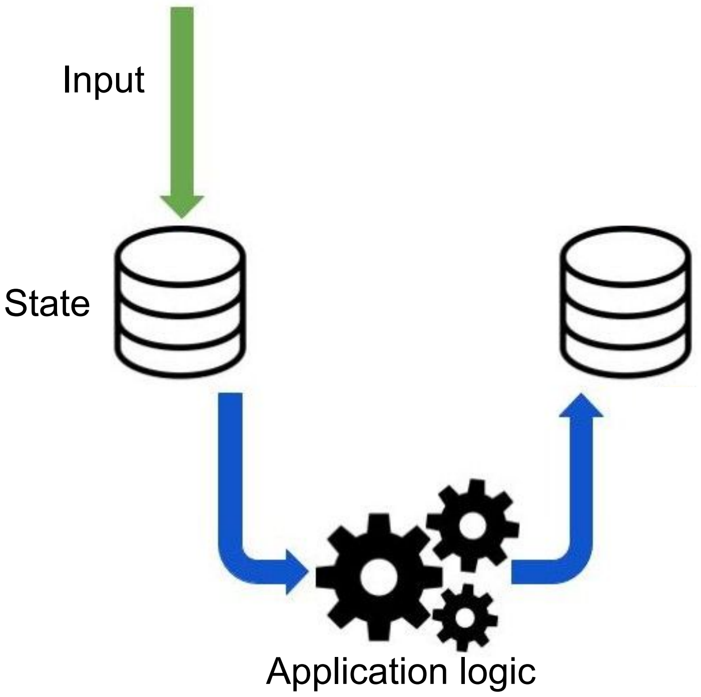


Input

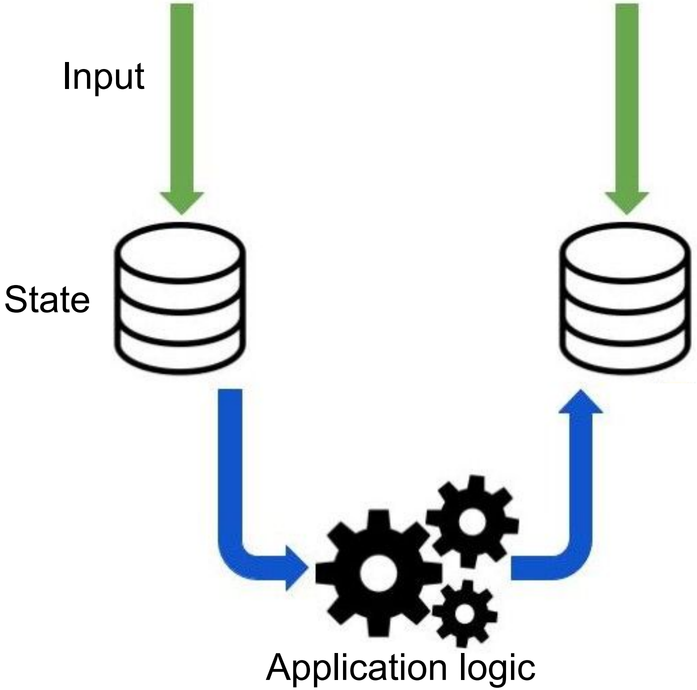
State

Application logic

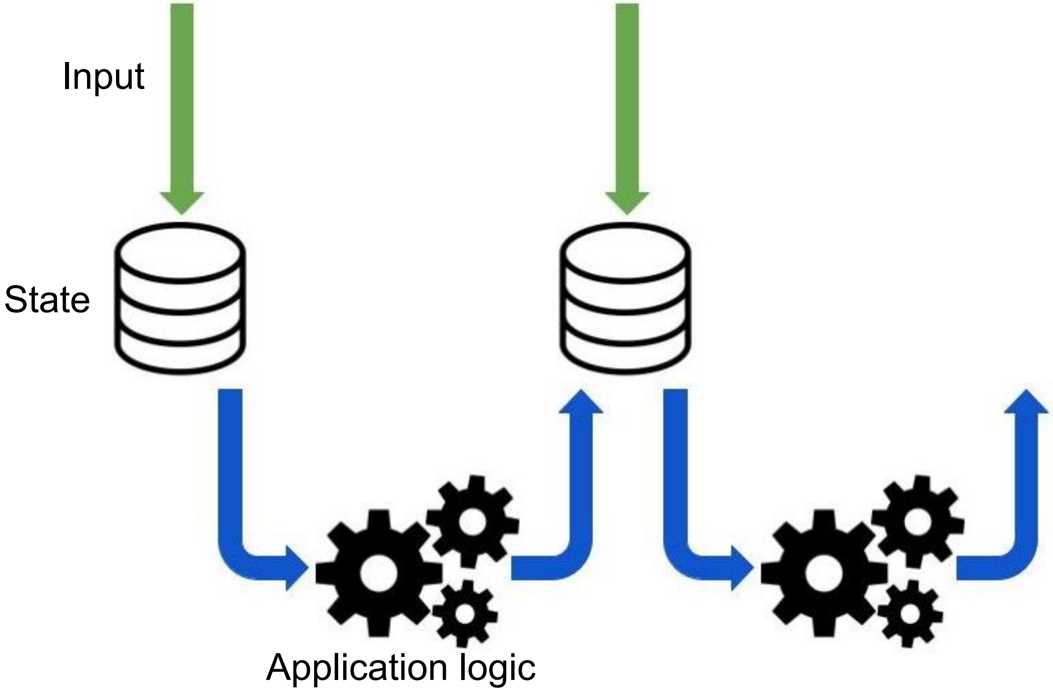
Smart contracts



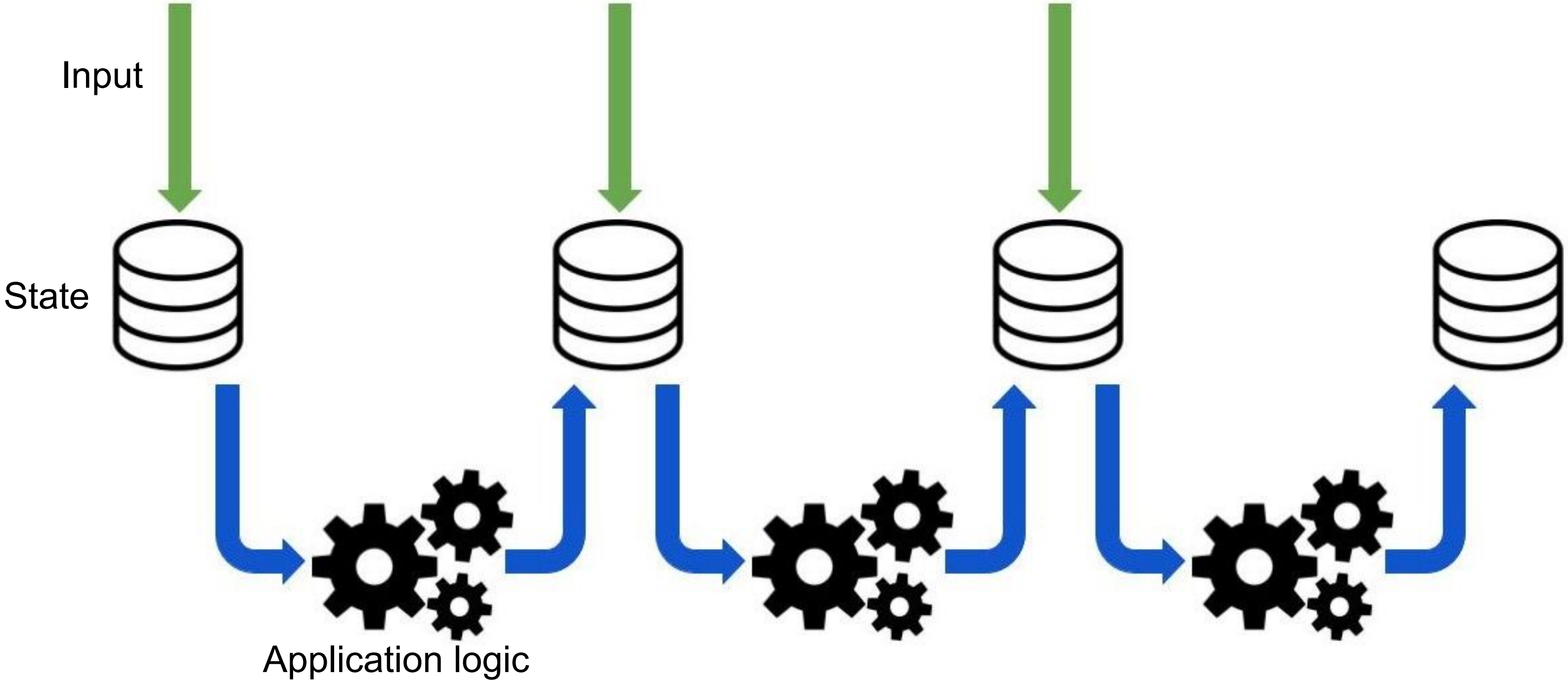
Smart contracts



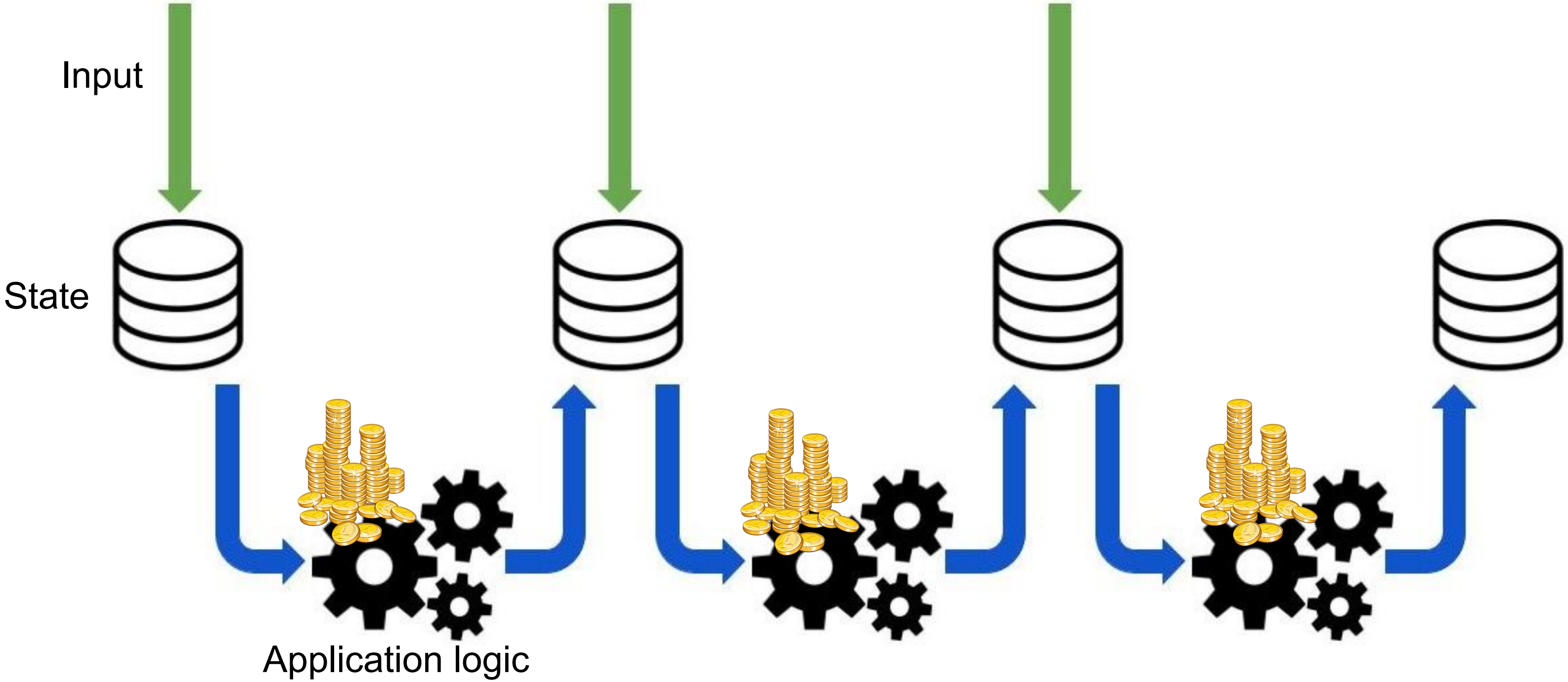
Smart contracts



Smart contracts



Smart contracts


Input

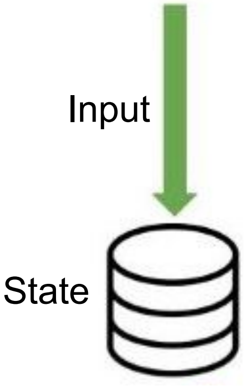
State

Application logic

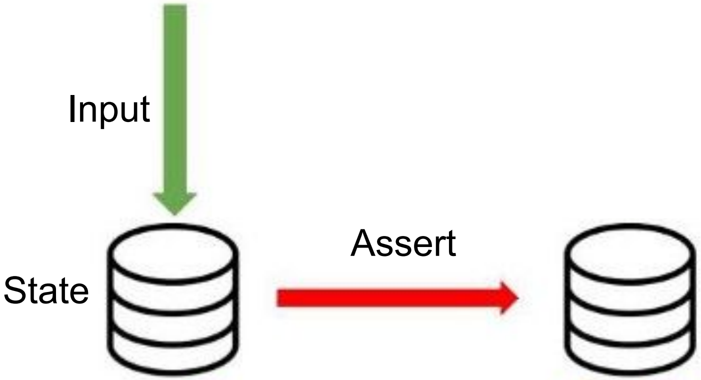
‘Optimistic’ smart contracts

Accept any state as input, then wait for a fraud proof

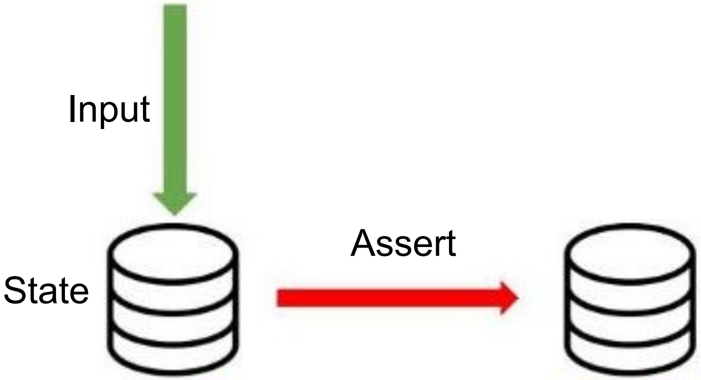
Optimistic smart contracts

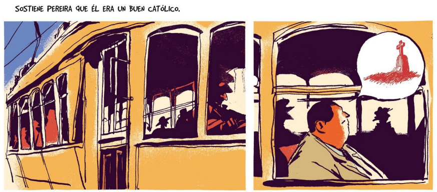


Optimistic smart contracts

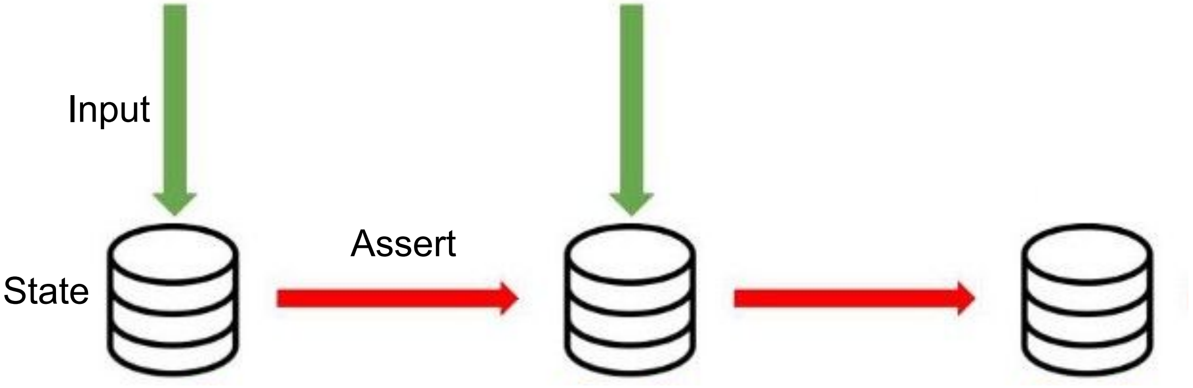


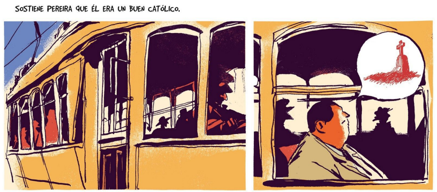
Optimistic smart contracts



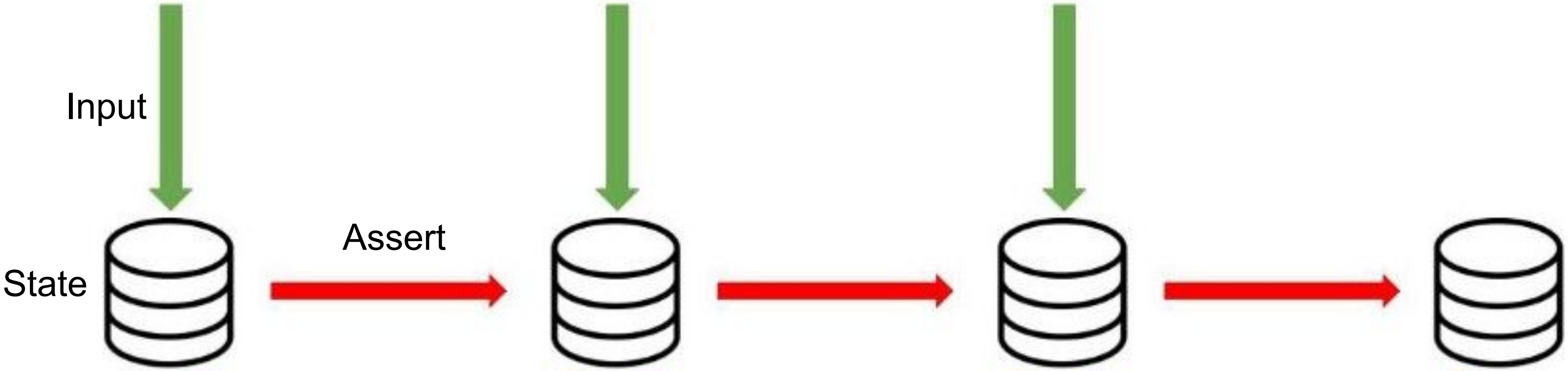


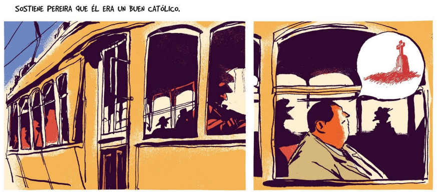
Optimistic smart contracts



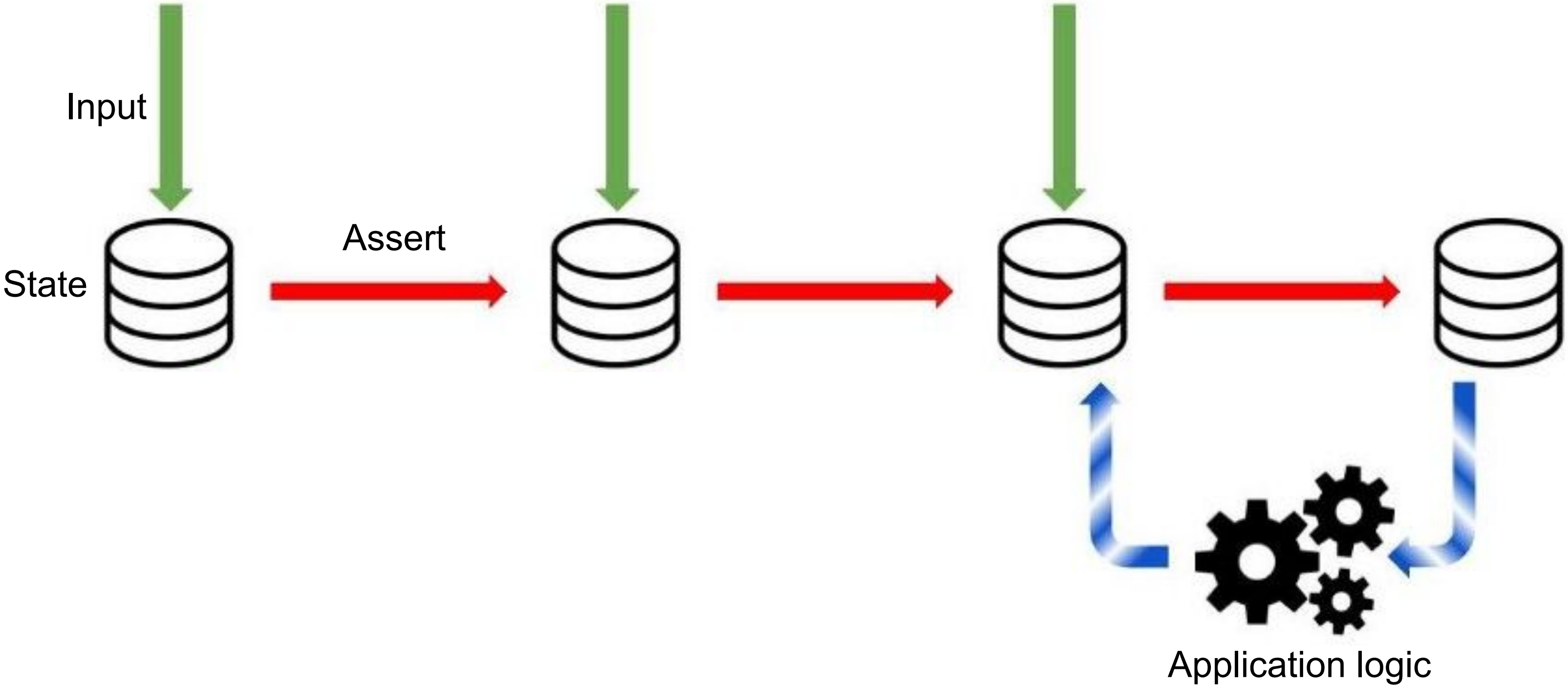


Optimistic smart contracts

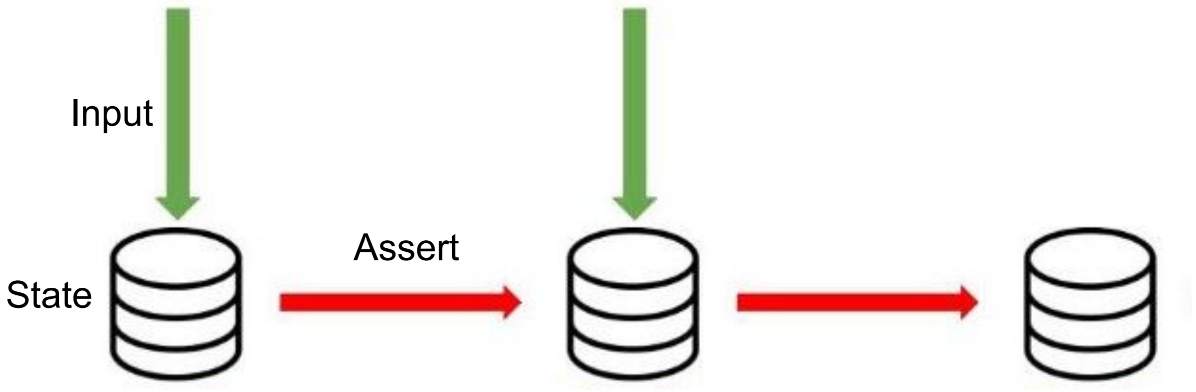




Optimistic smart contracts



Optimistic smart contracts

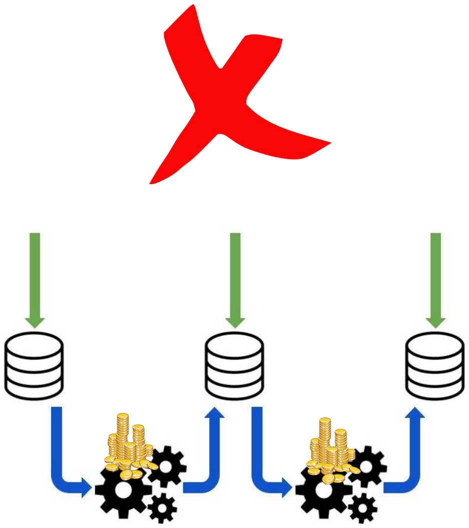


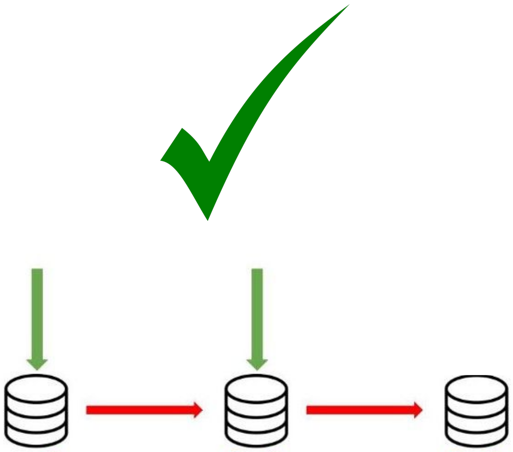
Optimistic contracts trade tx fees for latency

State channels + optimistic contracts = cheaper disputes

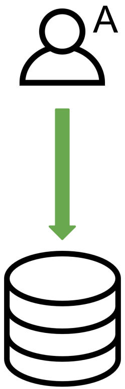
How does it work?

Dispute resolution takes place via assertions instead of being fully computed

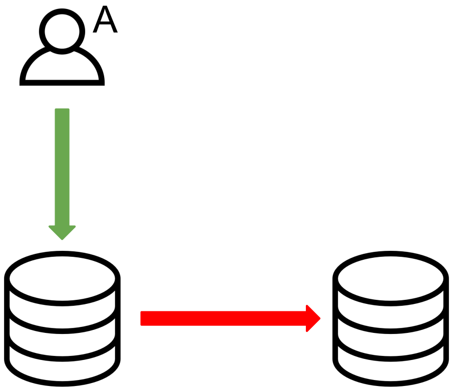




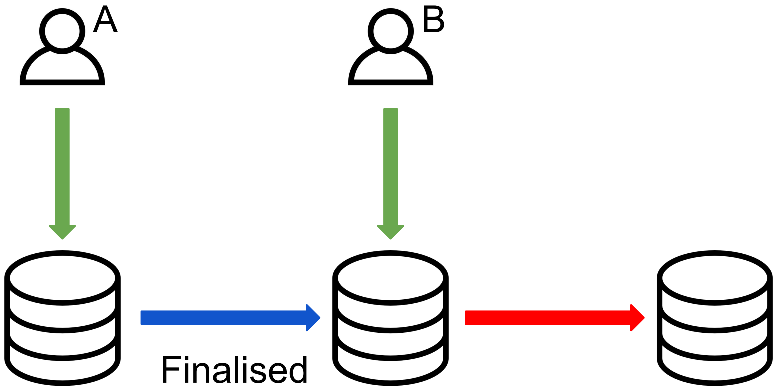
Why is this a good match?



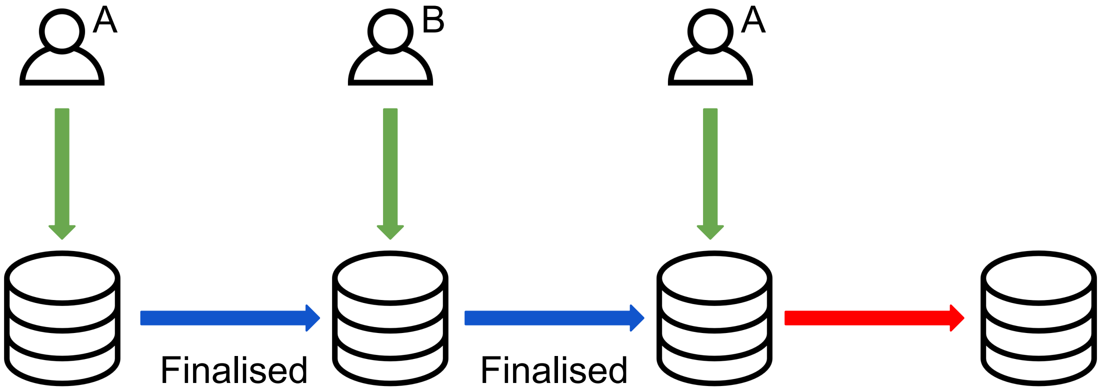
Why is this a good match?



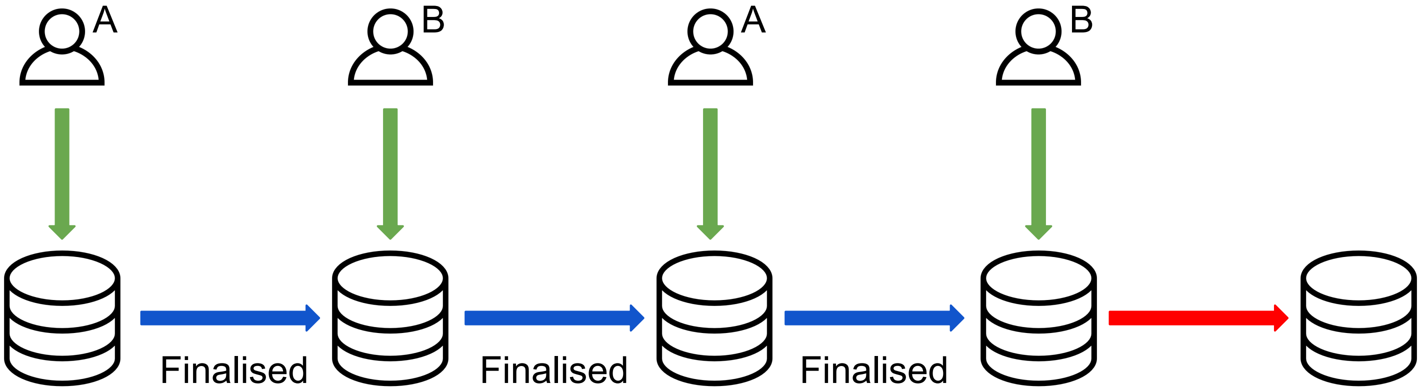
Why is this a good match?



Why is this a good match?



Why is this a good match?



The result

Taking turns as part of the worst case dispute in a state channel is **independent of the computational complexity** of the application

Experiment built on Ethereum:

60,000 + 40n gas per state assertion

*(where **n** is the number of input bytes)*

A cautionary note..

- Malicious counterparty can now transition to any arbitrary state if a party is offline

- Fraud proofs are restricted the block gas limit

A cautionary note..

- Malicious counterparty can now transition to any arbitrary state if a party is offline

- Fraud proofs are restricted the block gas limit

truebit

A cautionary note..

- Malicious counterparty can now transition to any arbitrary state if a party is offline

- Fraud proofs are restricted the block gas limit

truebit

OFFCHAINLABS

Related work

- Optimistic contracts - https://medium.com/@decanus/optimistic-contracts-fb75efa7ca84
- TrueBit - https://people.cs.uchicago.edu/~teutsch/papers/truebit.pdf
- Arbitrum - http://stevengoldfeder.com/papers/Arbitrum-USENIX.pdf
- Battleships - https://nms.kcl.ac.uk/patrick.mccorry/battleship.pdf

Thanks to

ethereum foundation grants

Ethereum Community Fund

RESEARCH INSTITUTE.