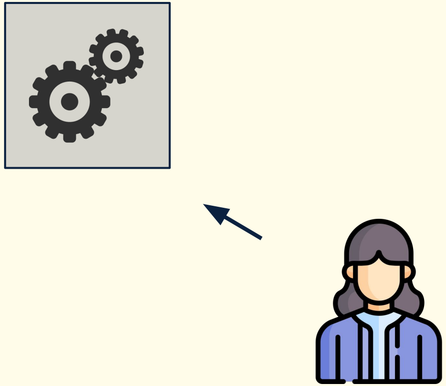
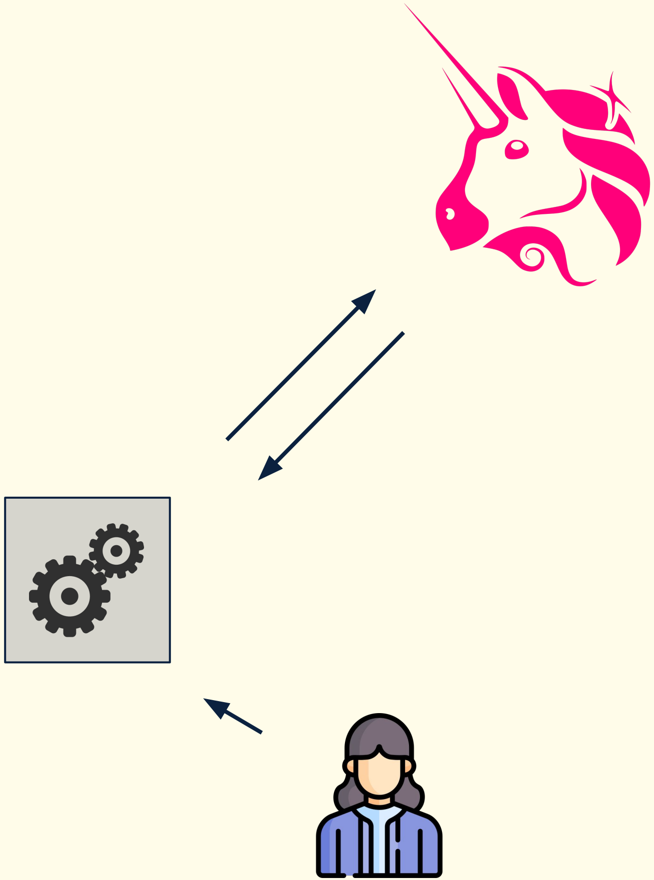
Mangrove

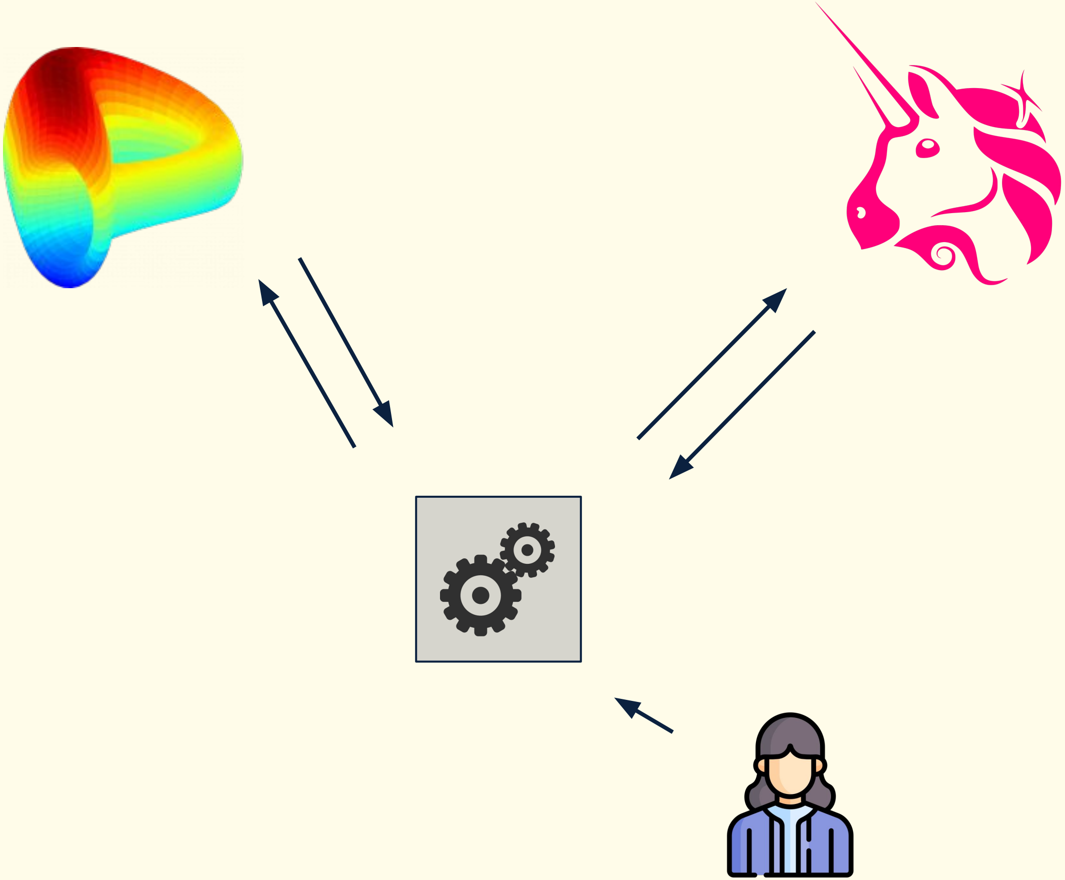
Fast and Parallelizable State Replication for Blockchains

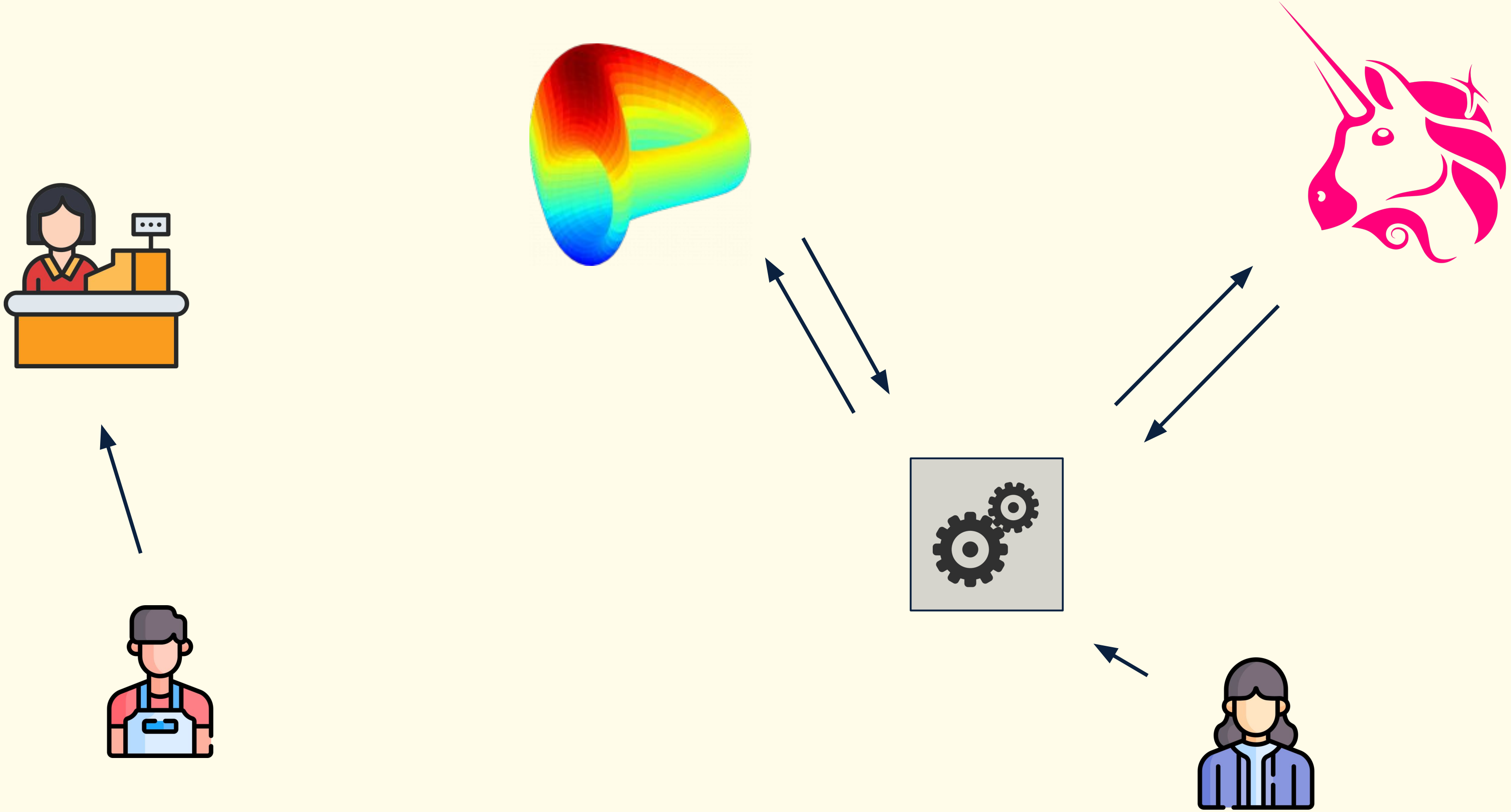
Anton Paramonov, Yann Vonlanthen, Quentin Kniep, Jakub Sliwinski, and Roger Wattenhofer

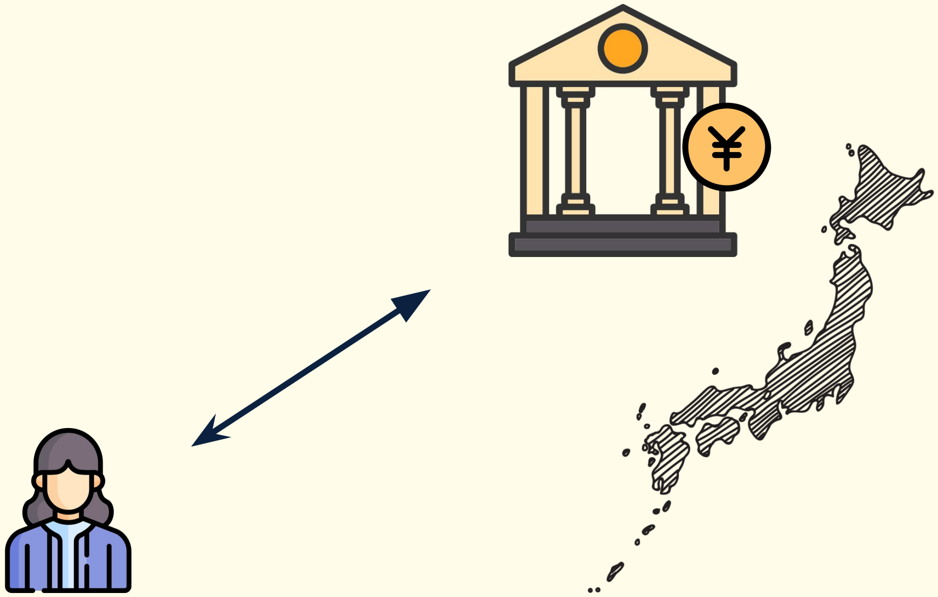
*ETH Zurich - **Dis**tributed **Co**mputing Group*

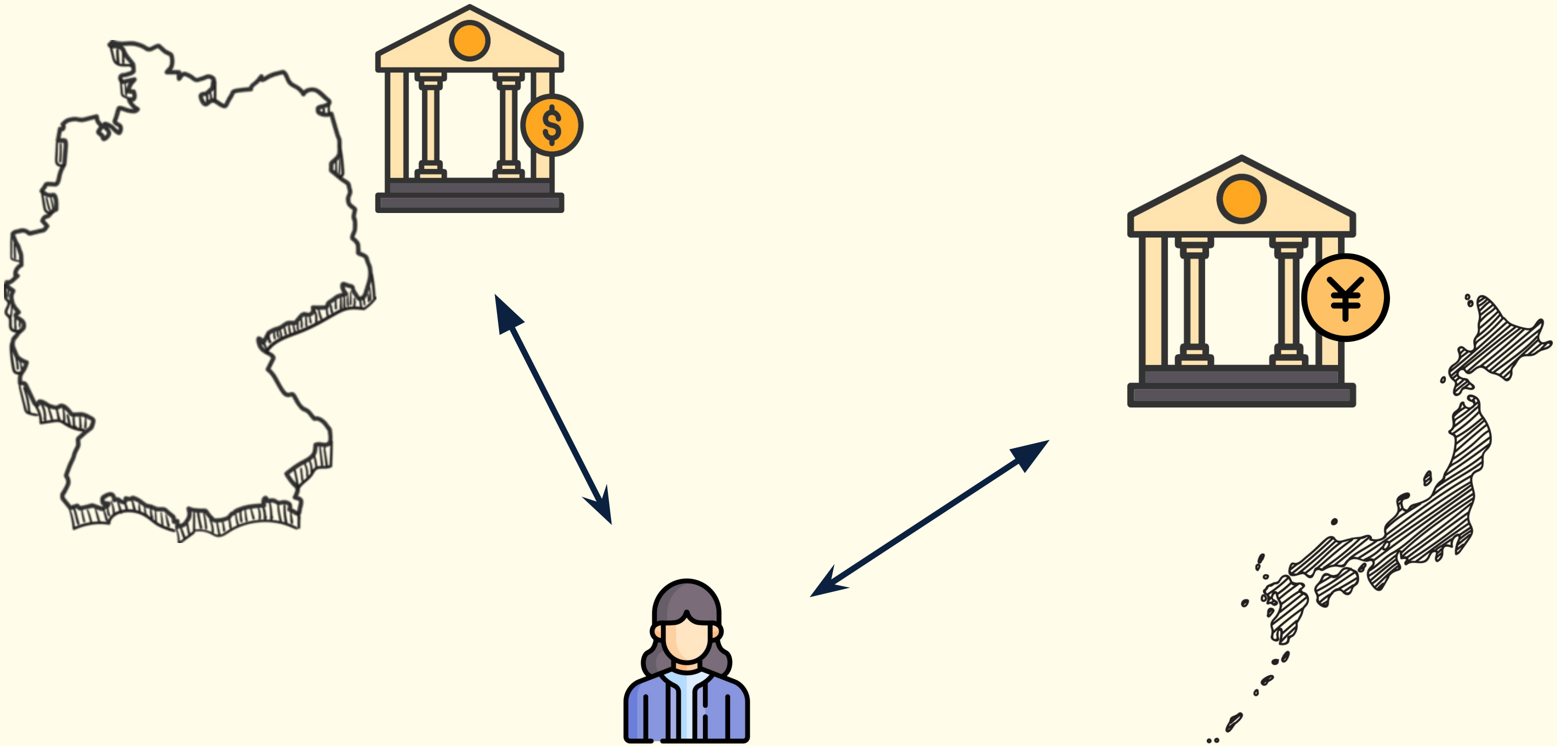


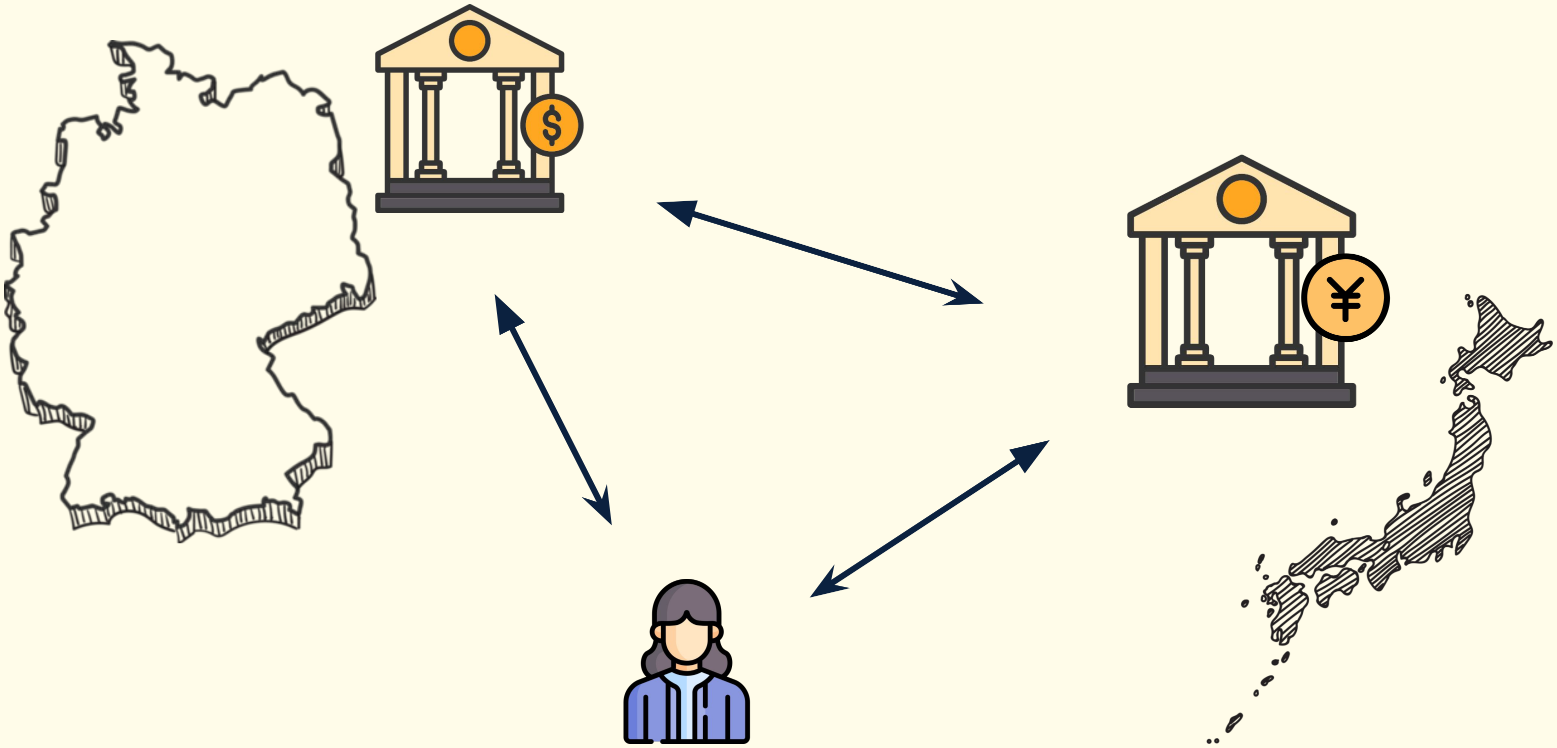




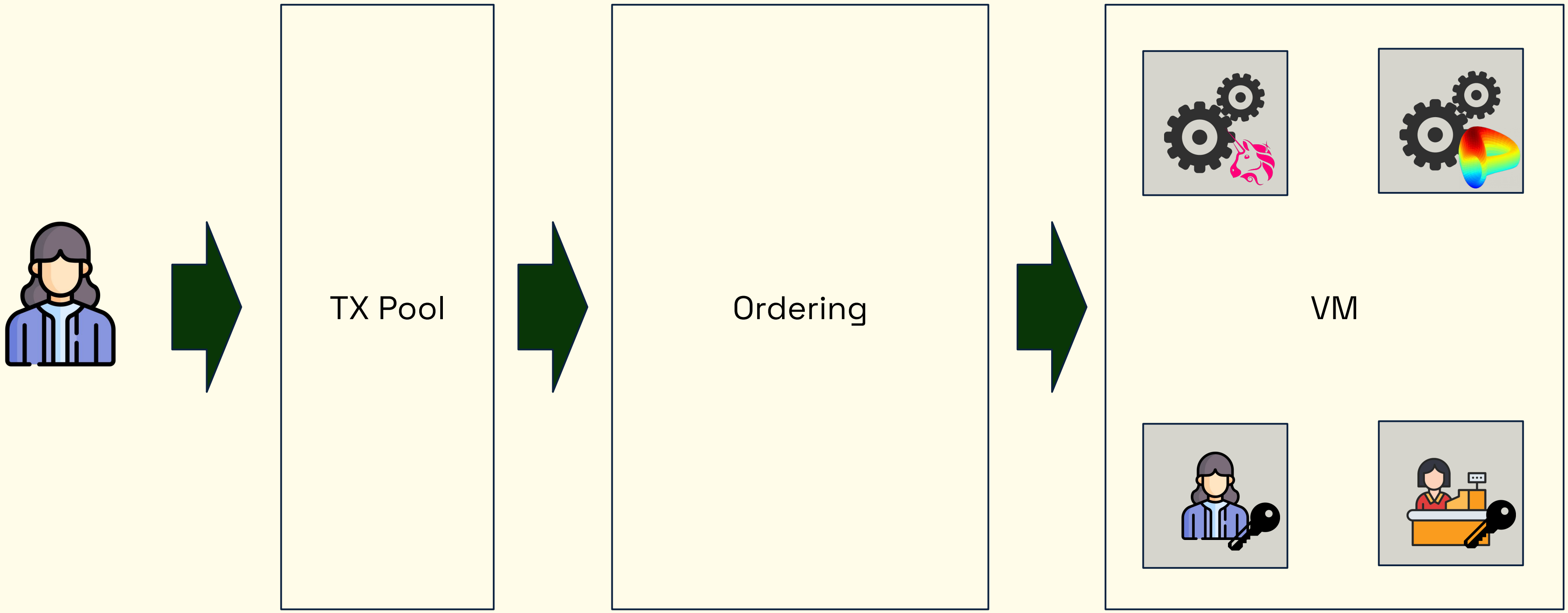




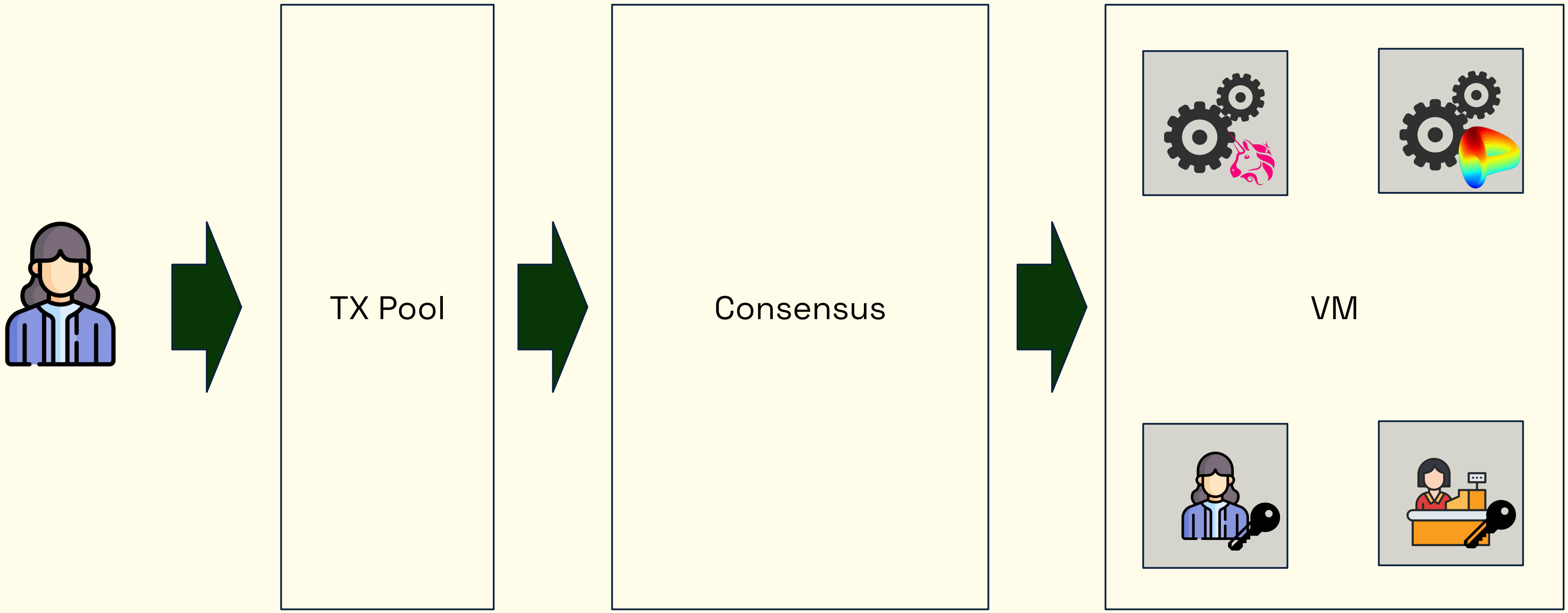




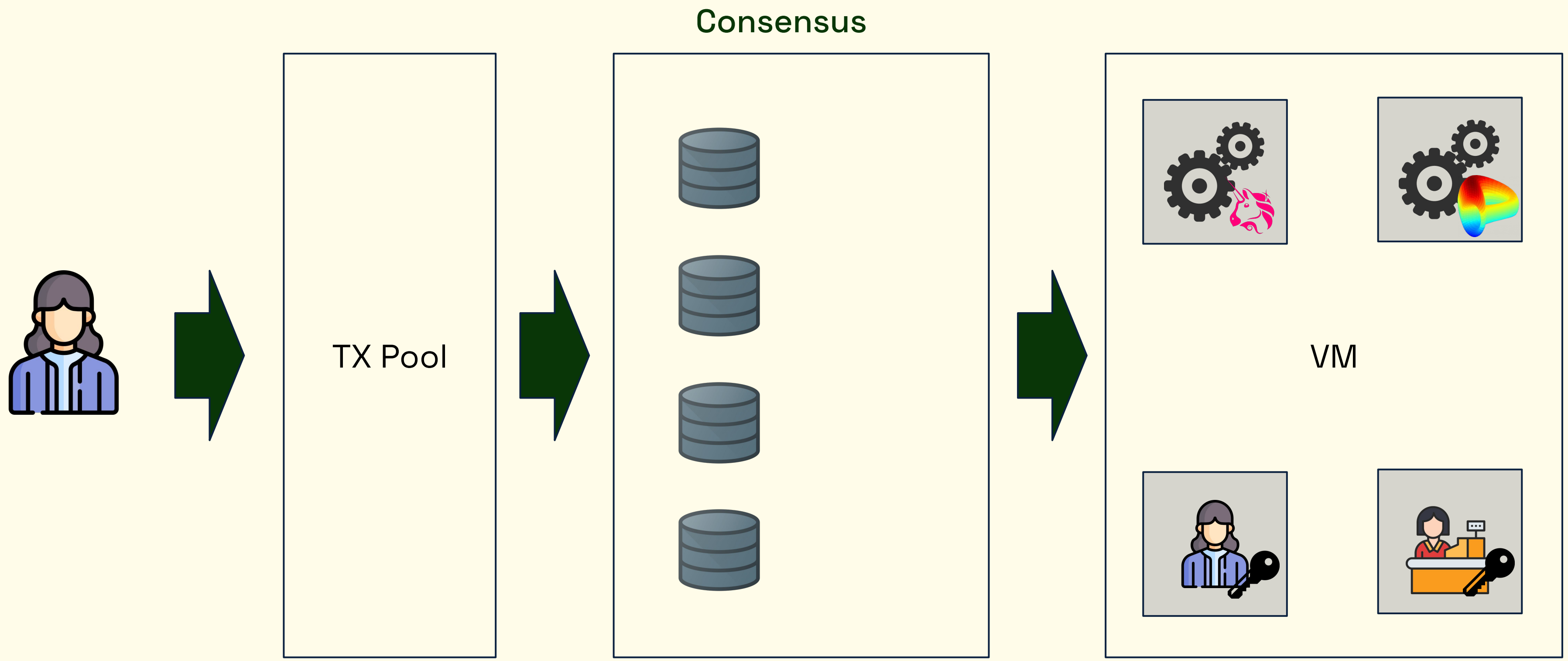
Current Model



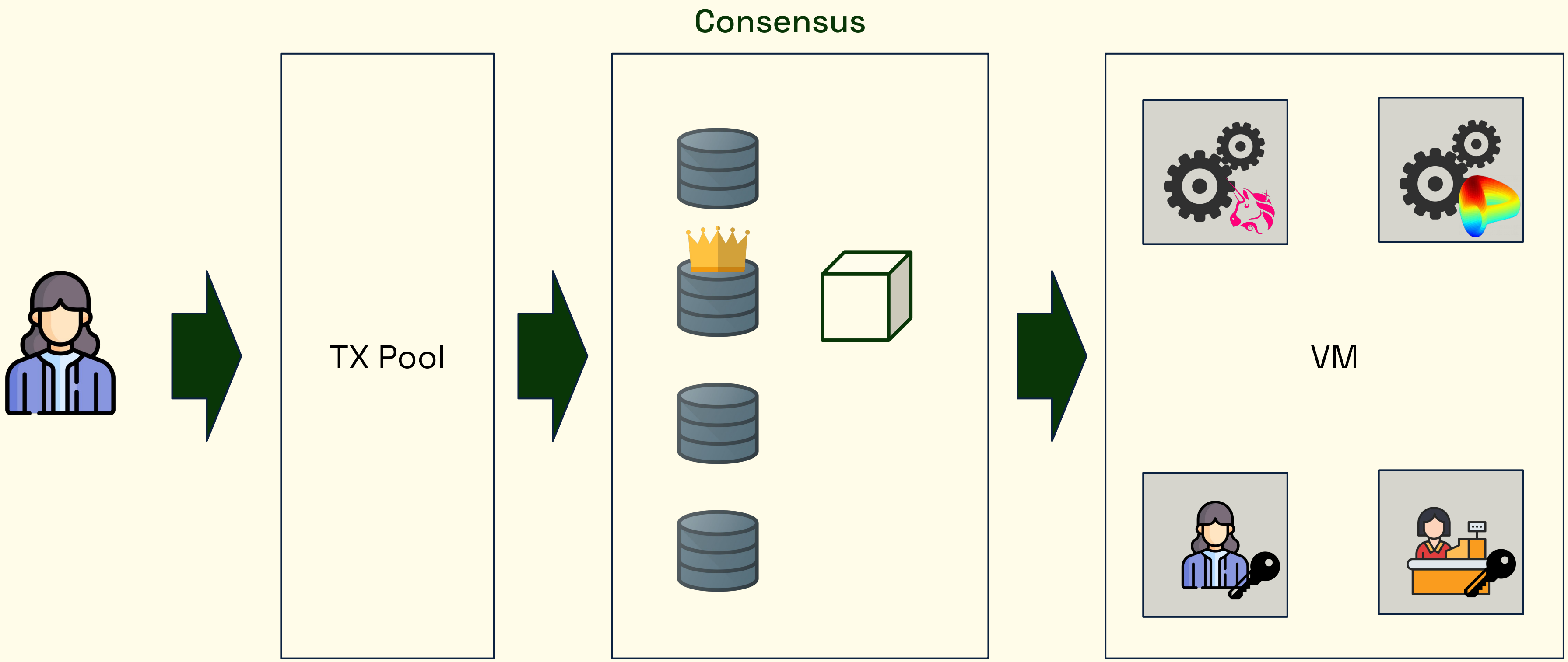
Current Model



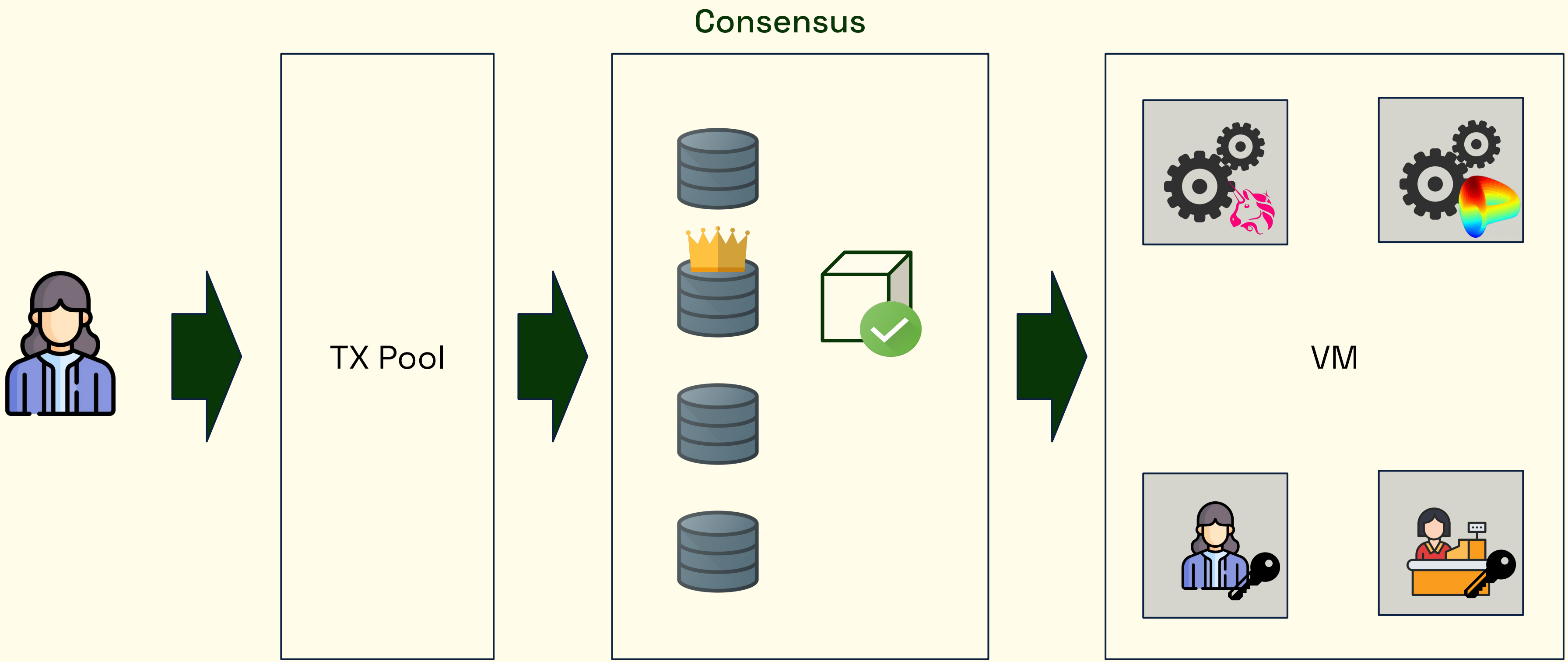
Current Model



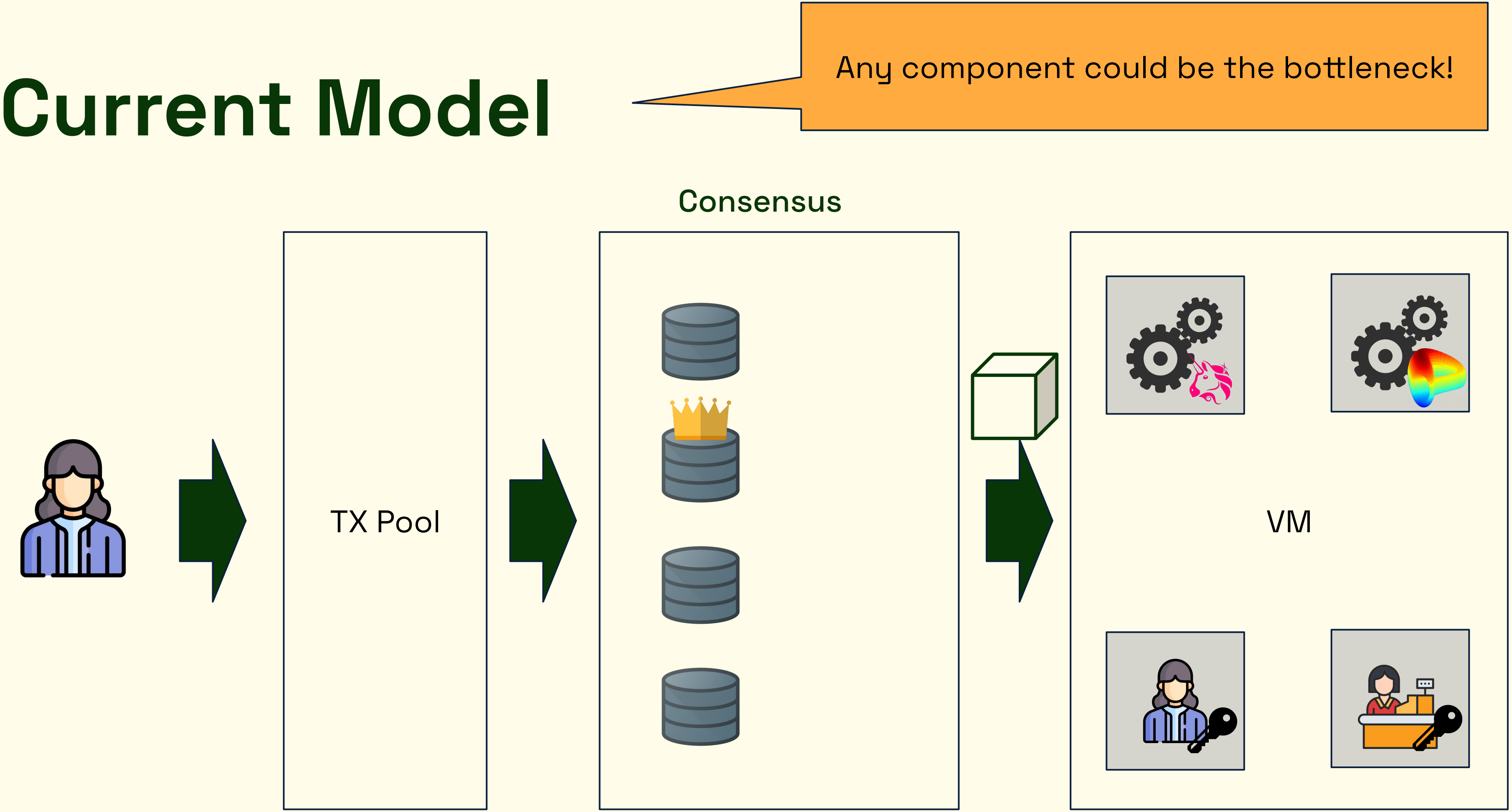
Current Model



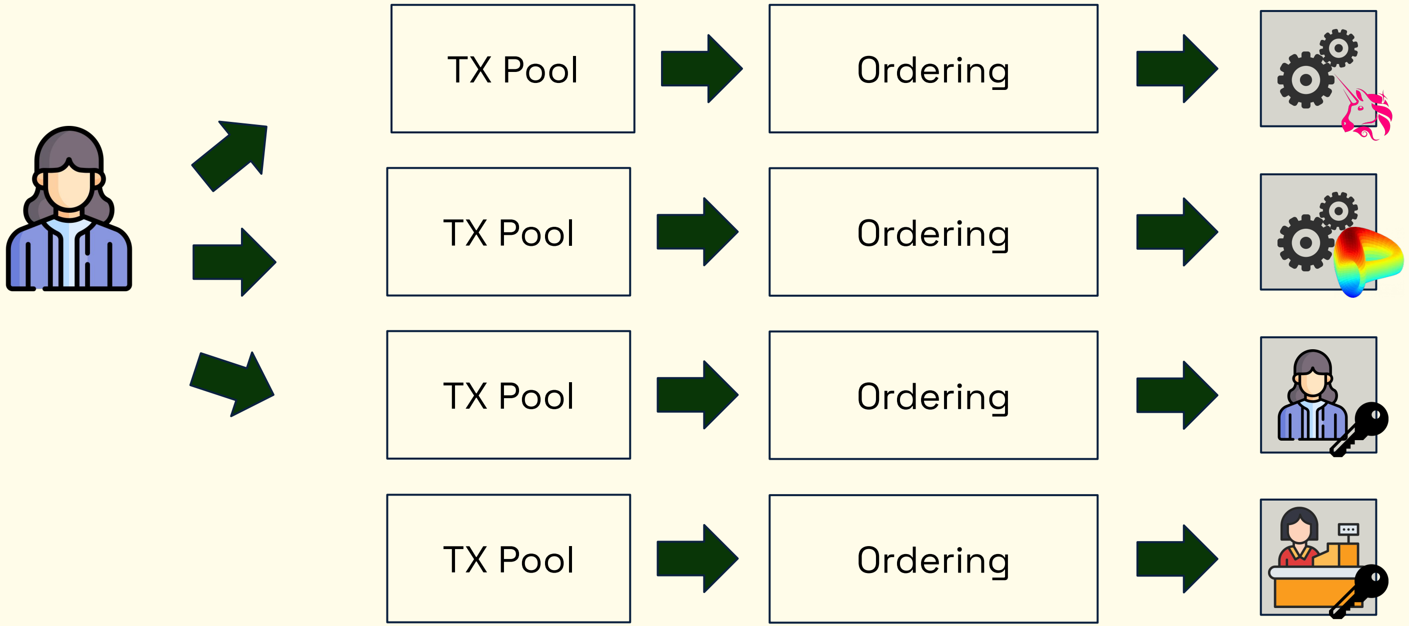
Current Model



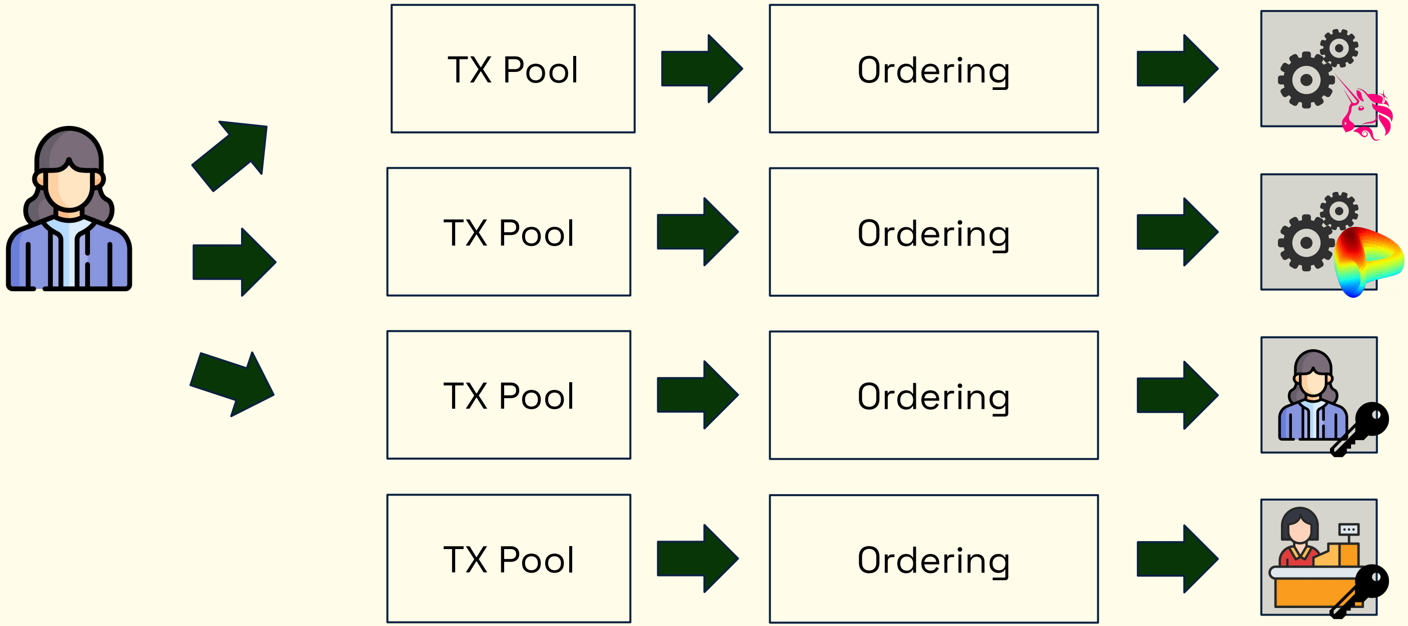
Current Model



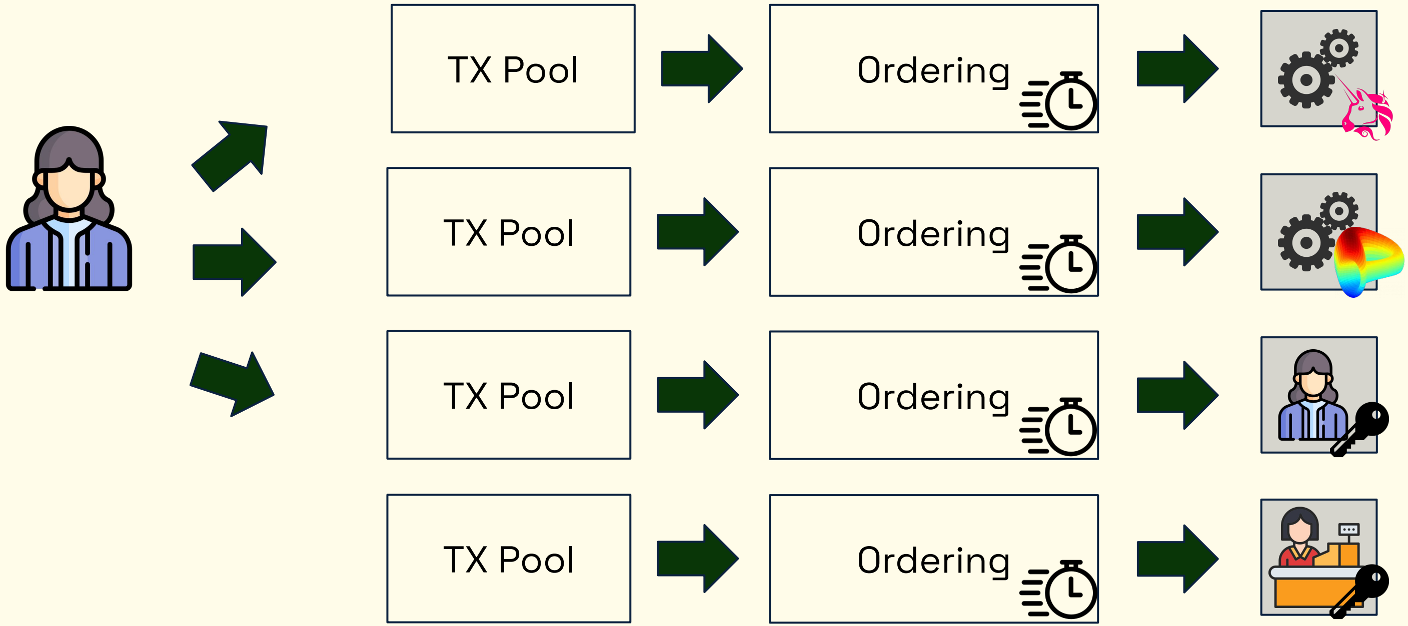
Horizontal Scaling



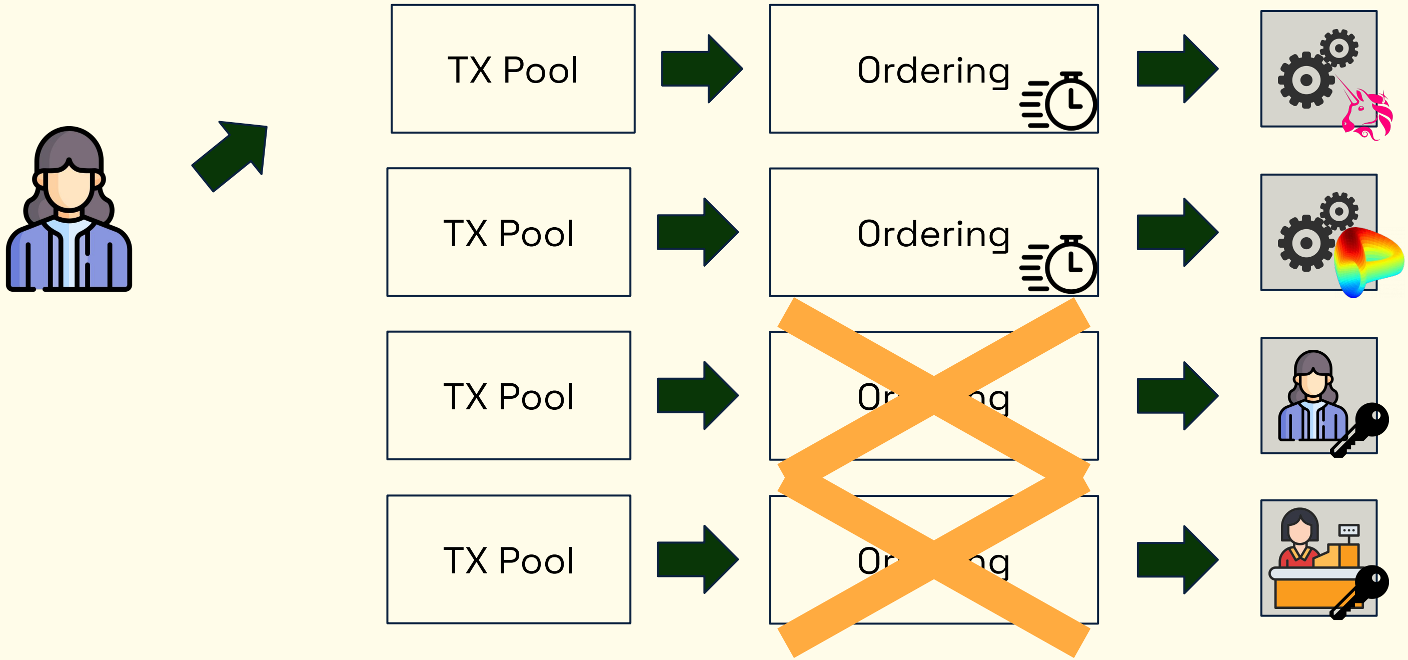
Horizontal Scaling + Low Latency



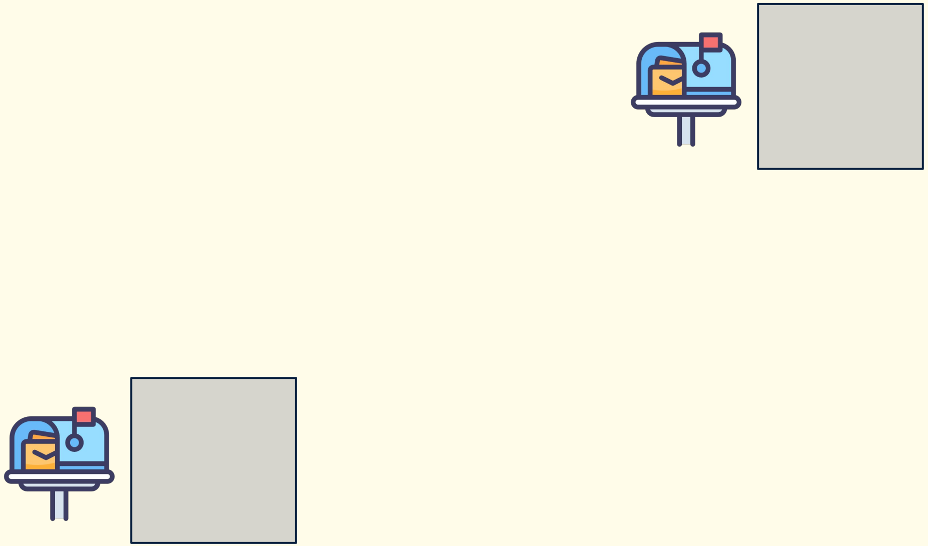
Horizontal Scaling + Low Latency



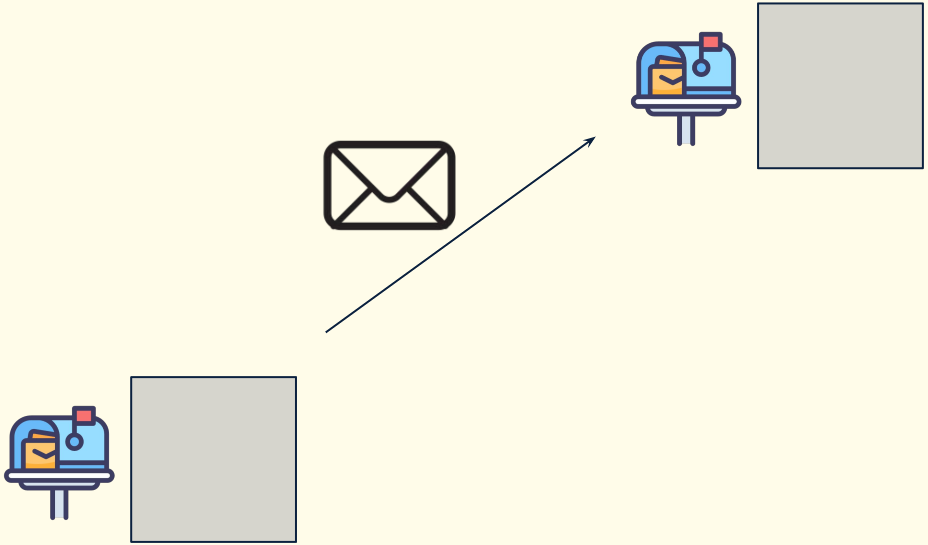
Replicated Actor Model



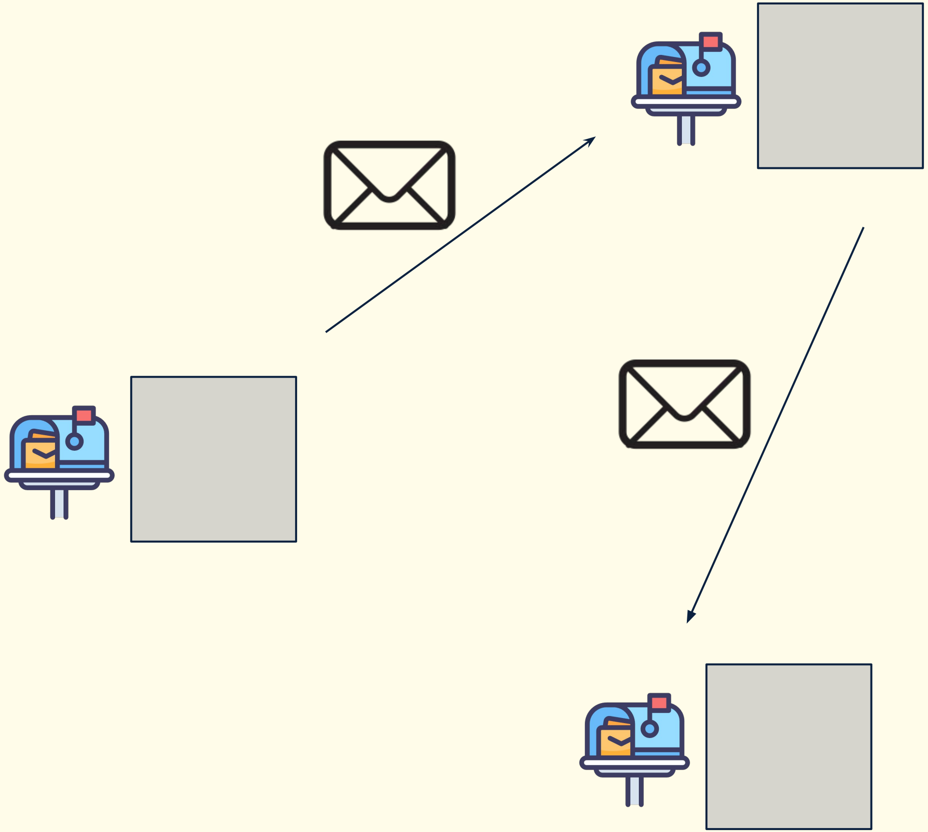
Actor Model



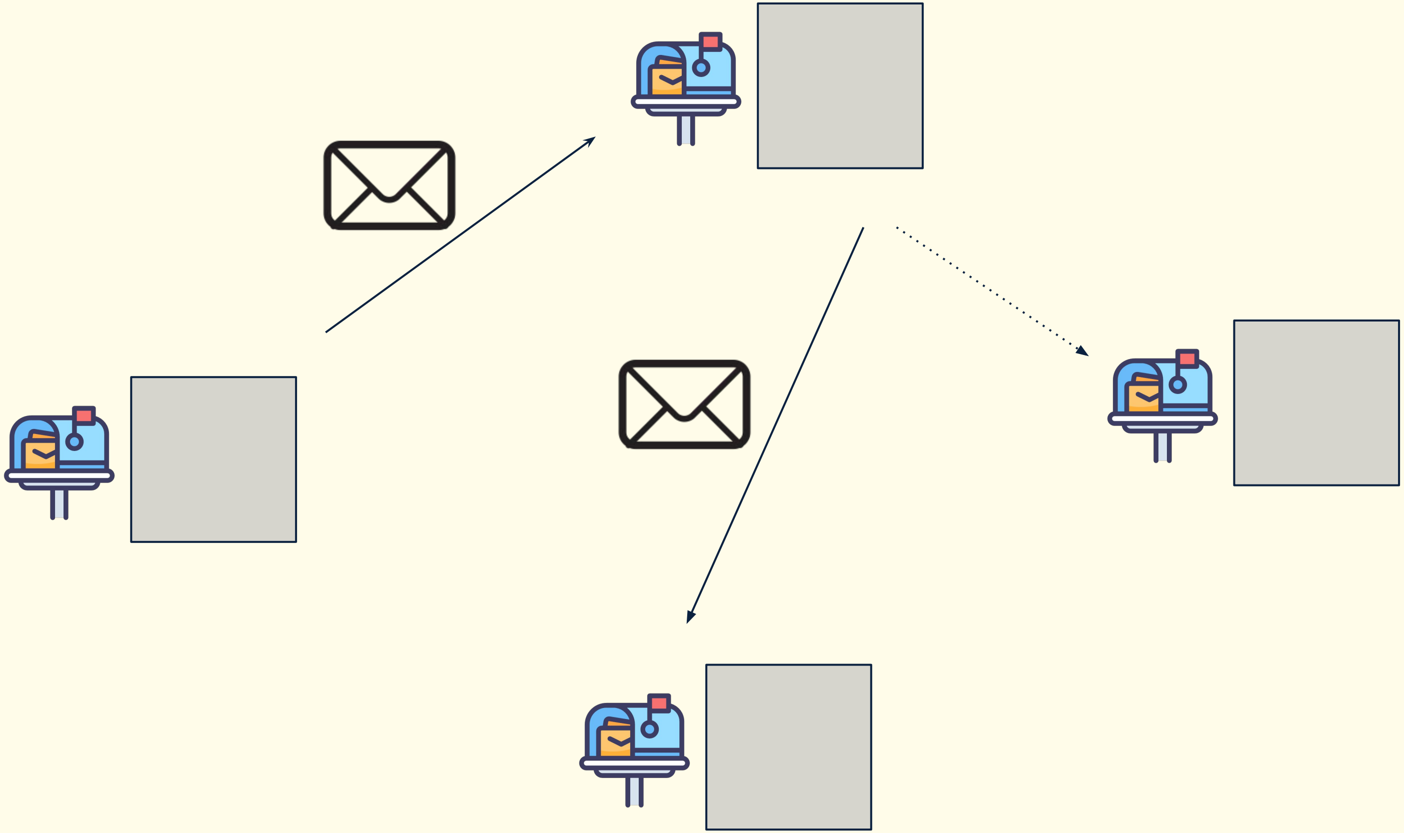
Actor Model



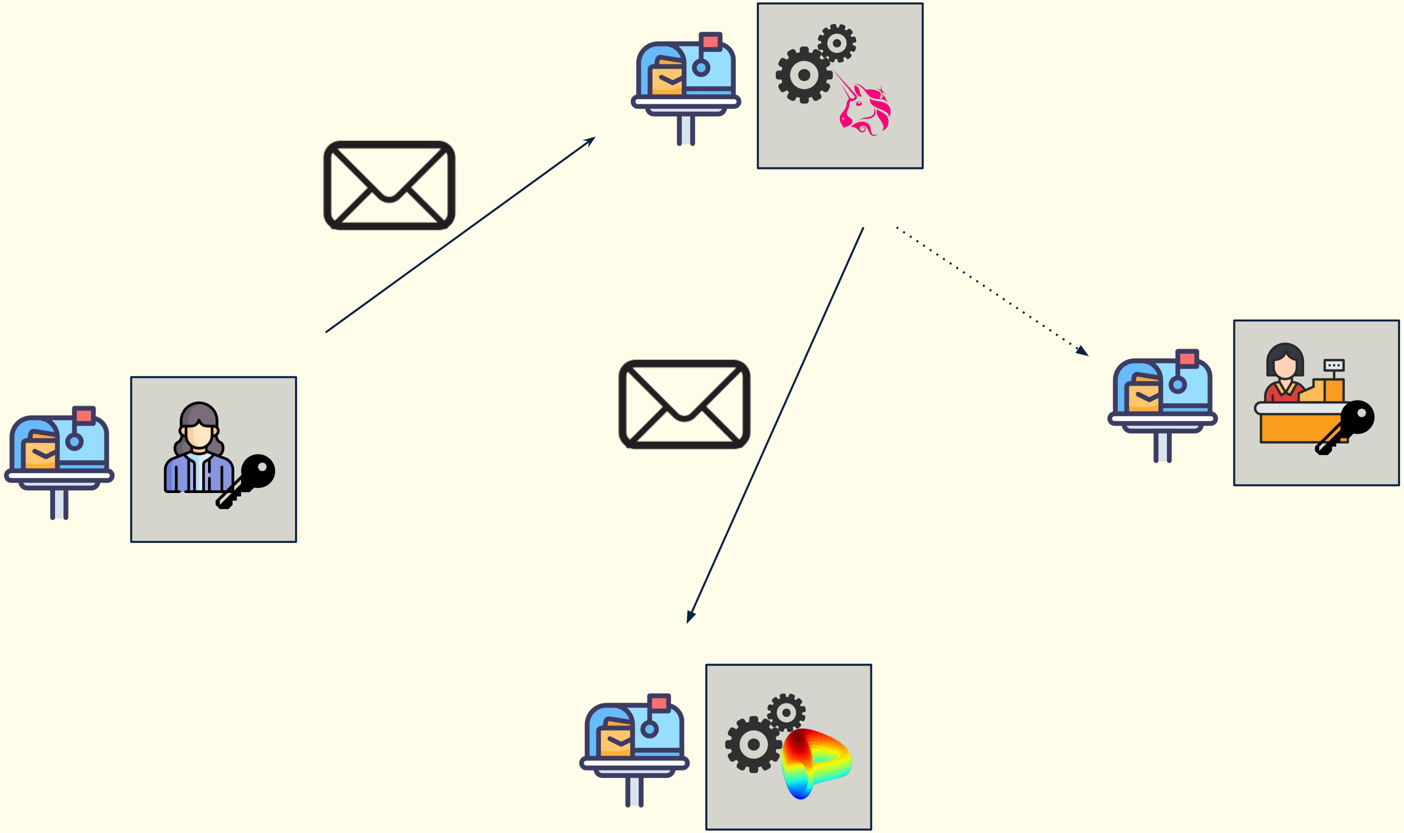
Actor Model



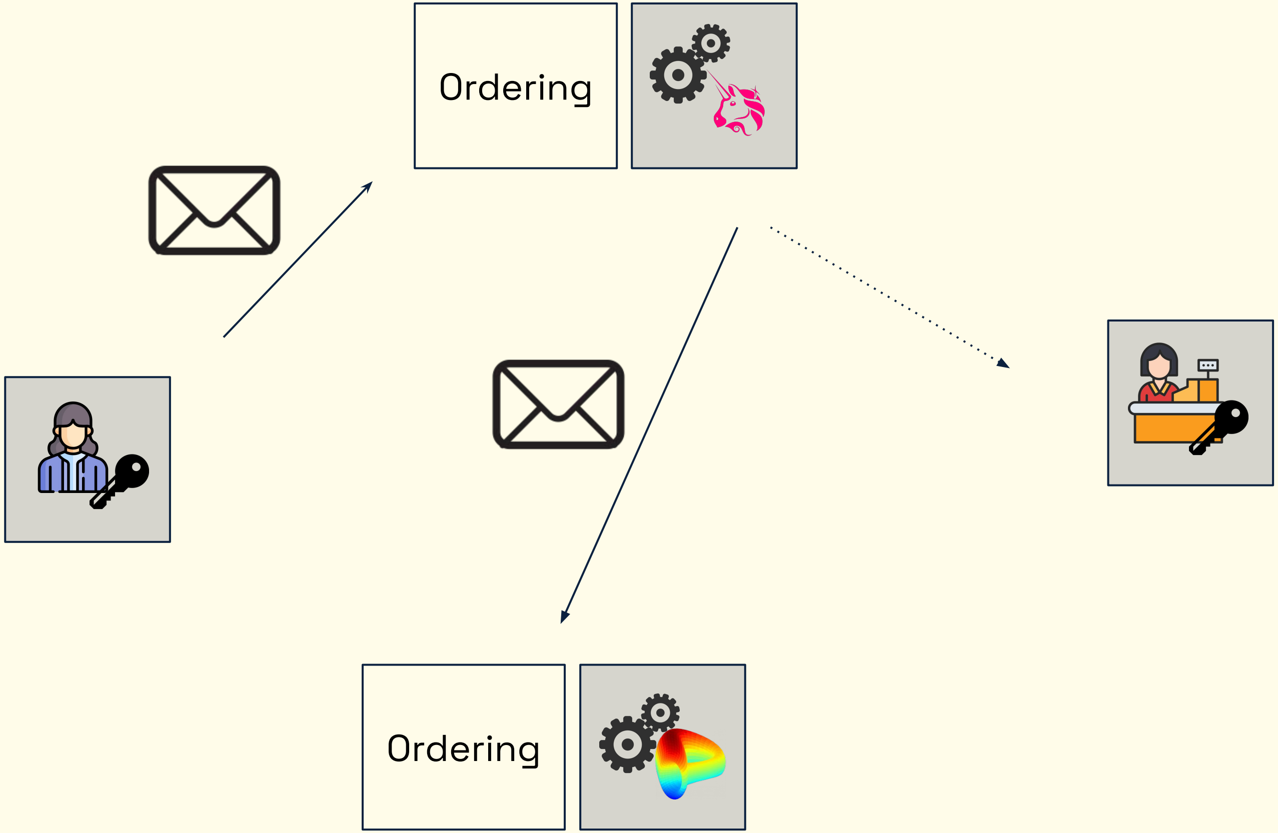
Actor Model



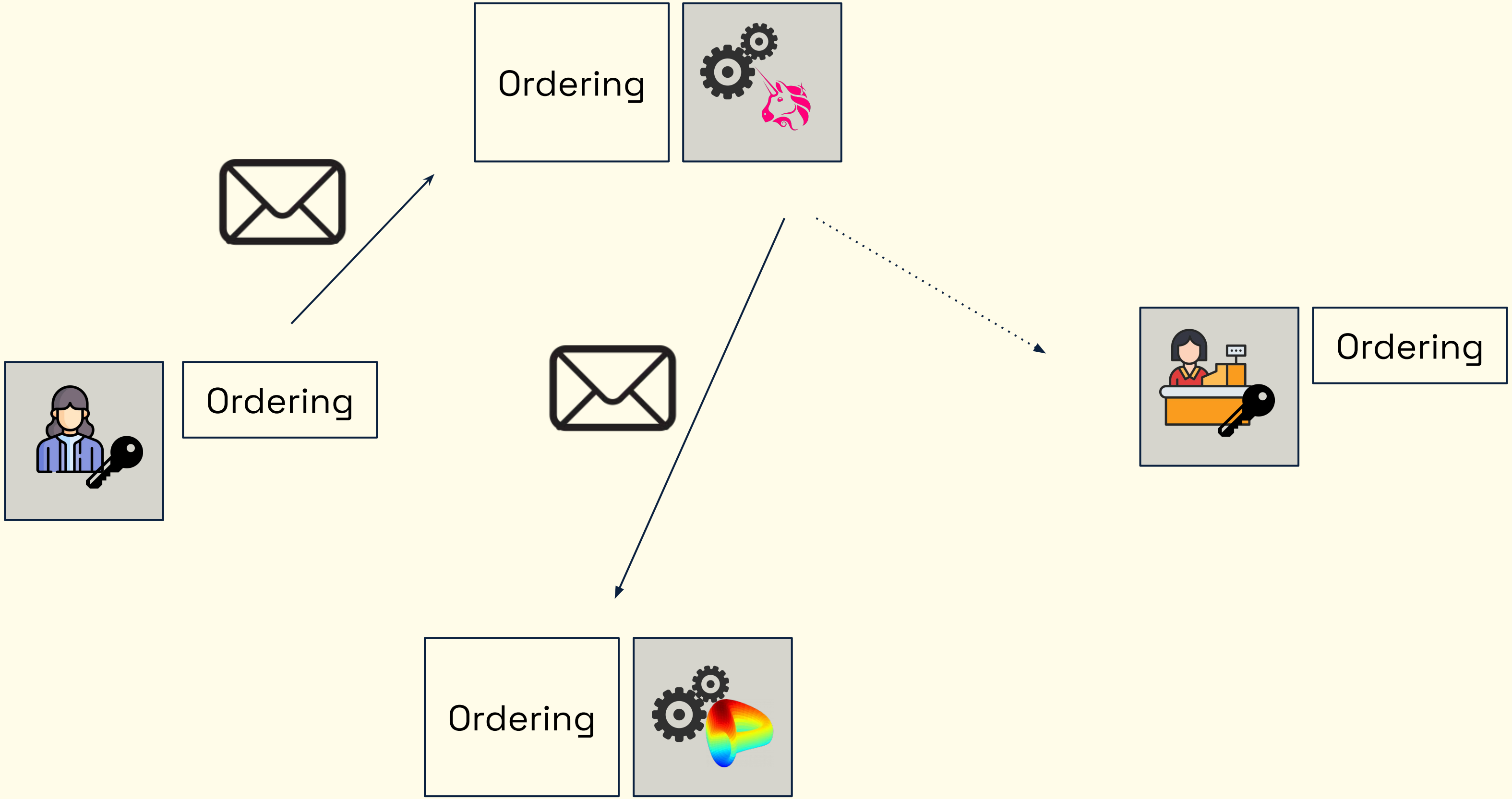
Replicated Actor Model



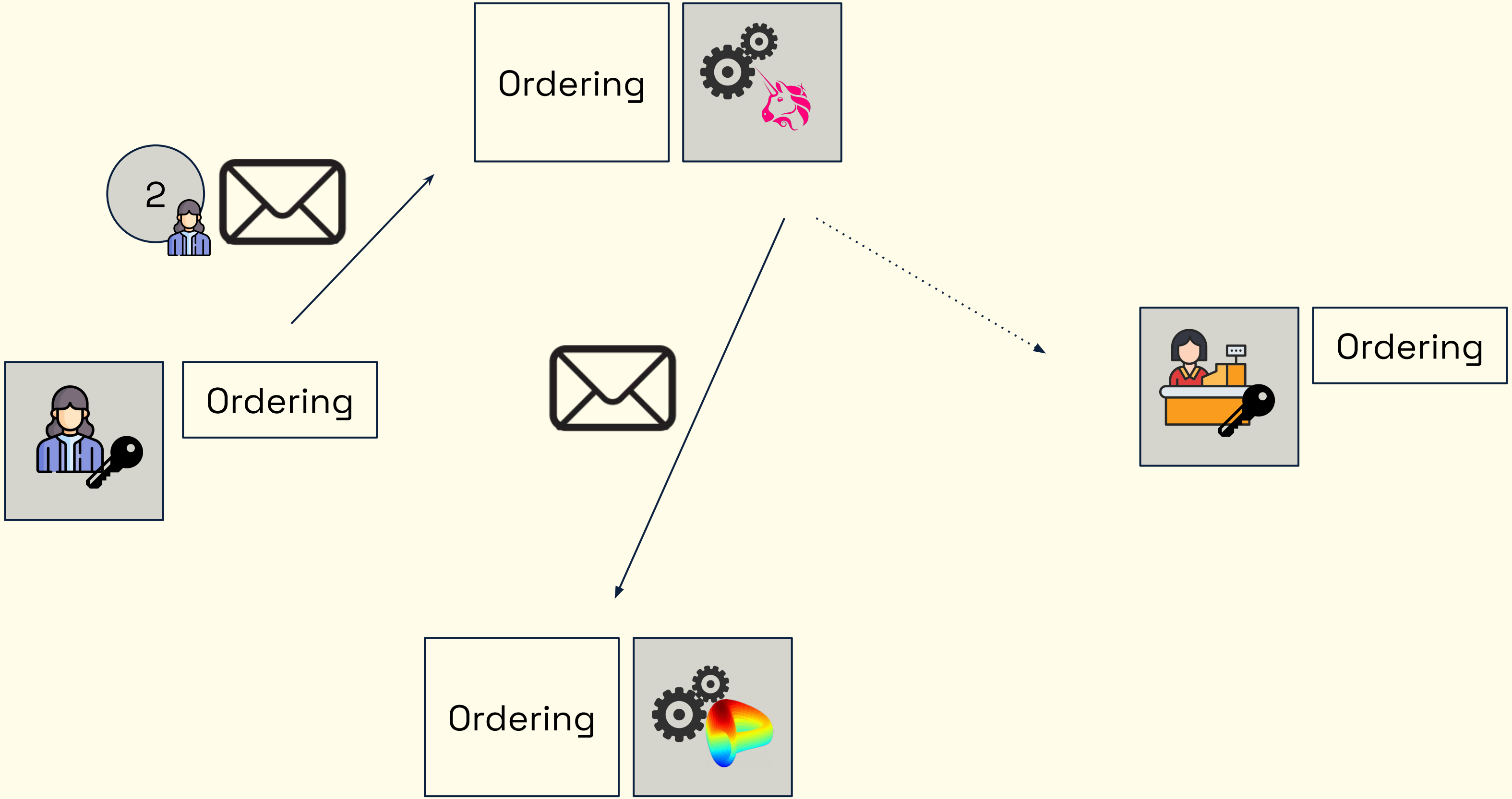
Replicated Actor Model



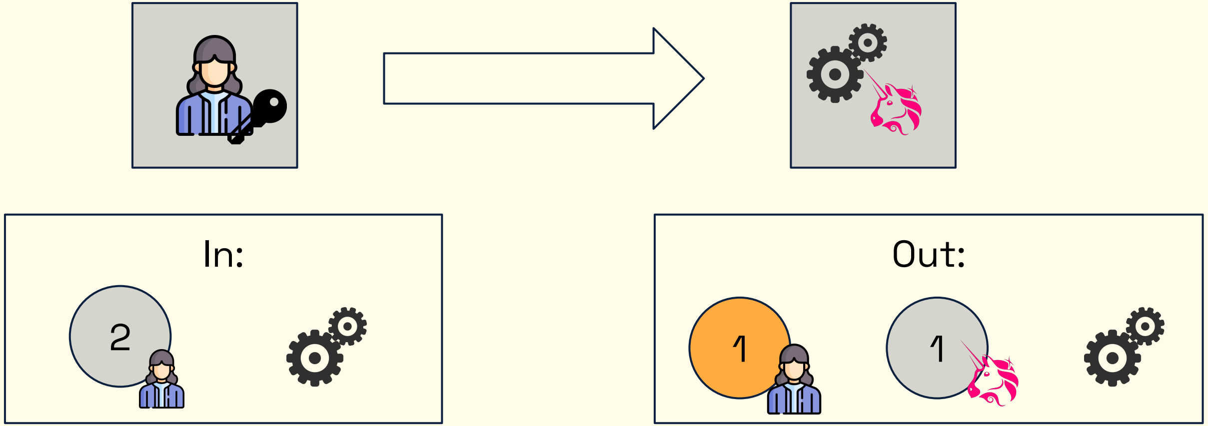
Replicated Actor Model



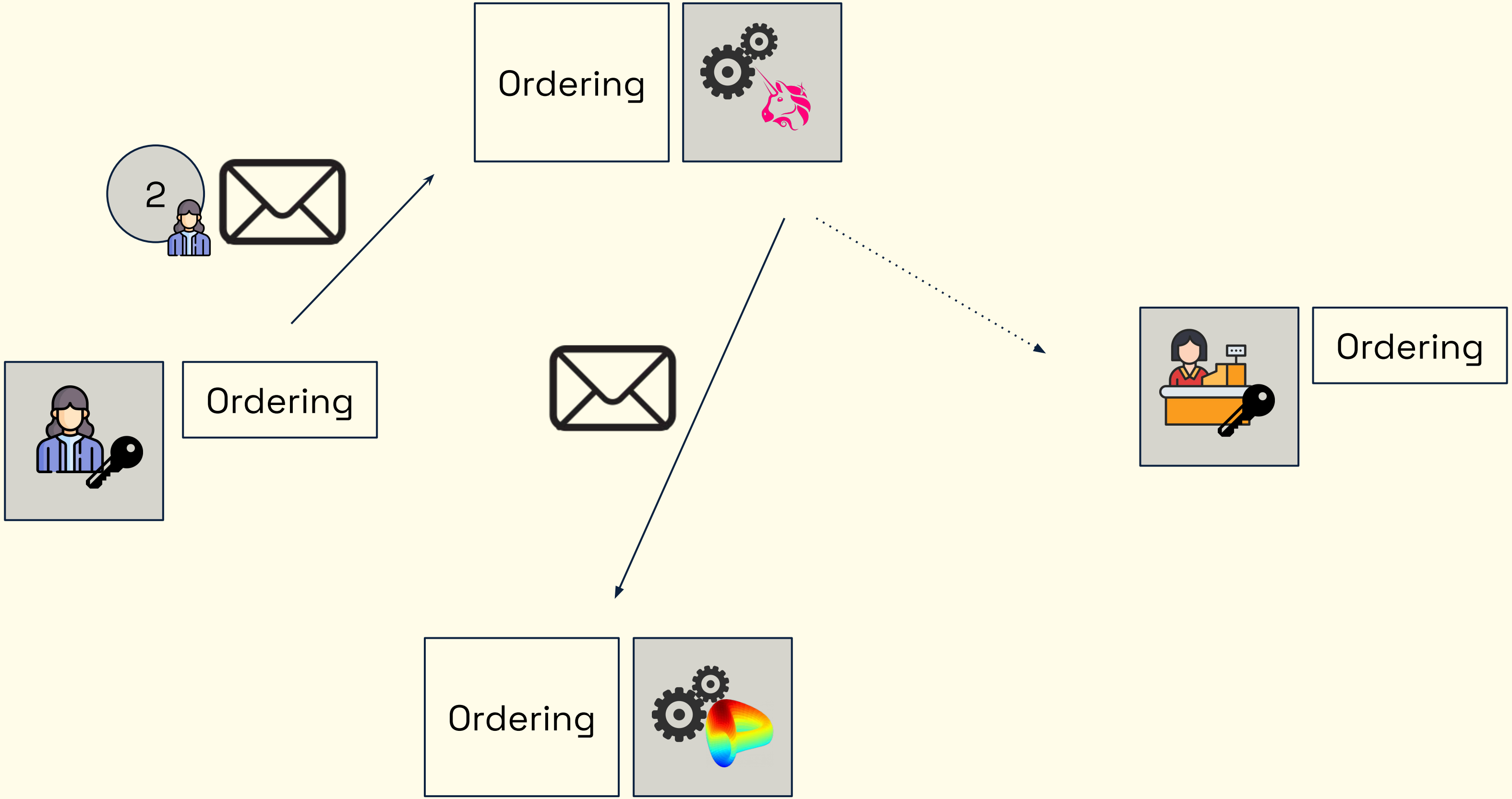
Replicated Actor Model



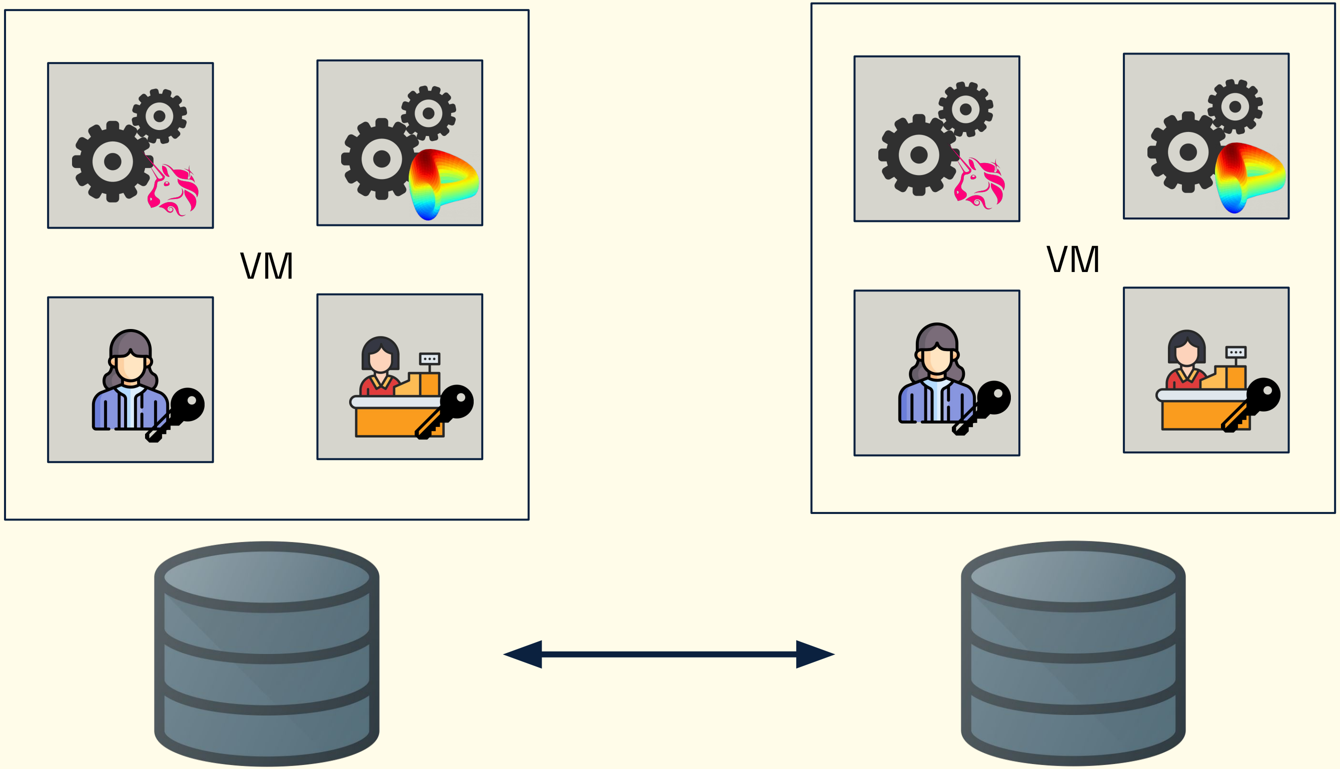
Transaction



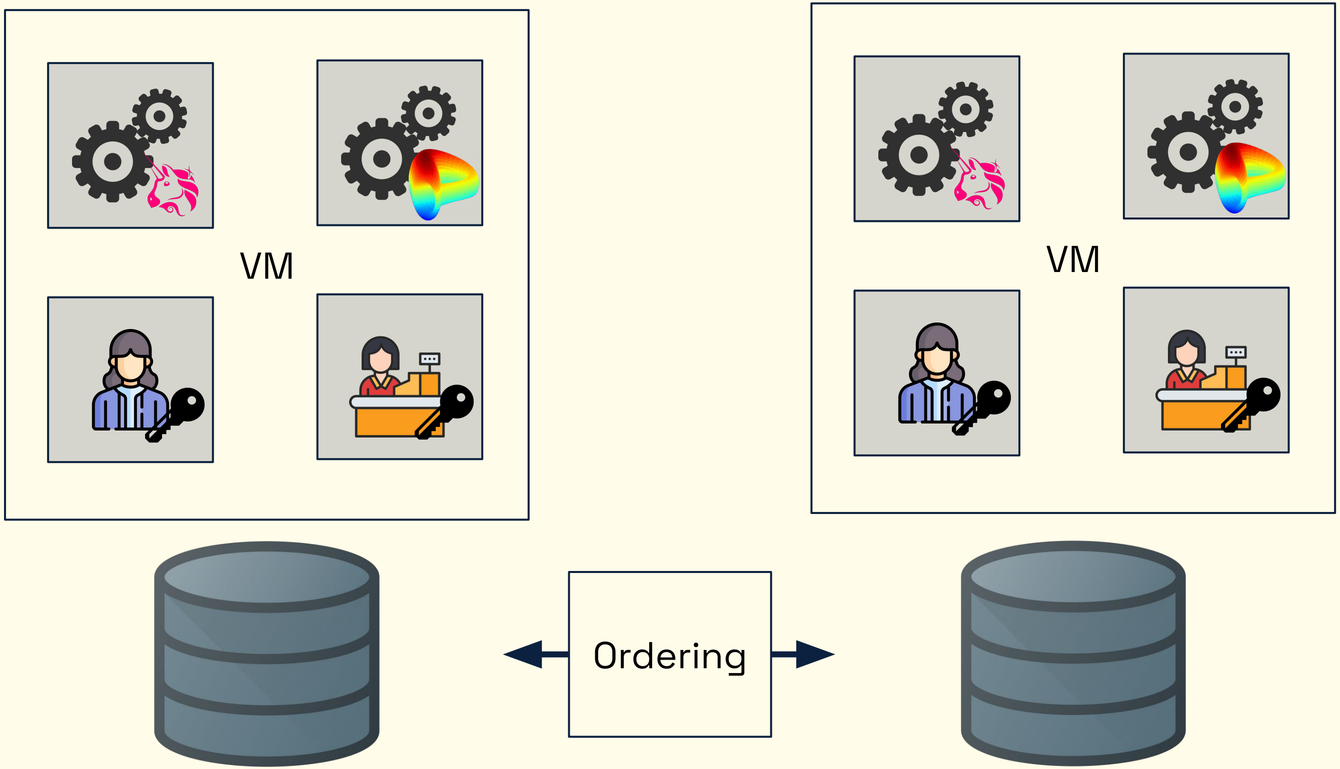
Replicated Actor Model



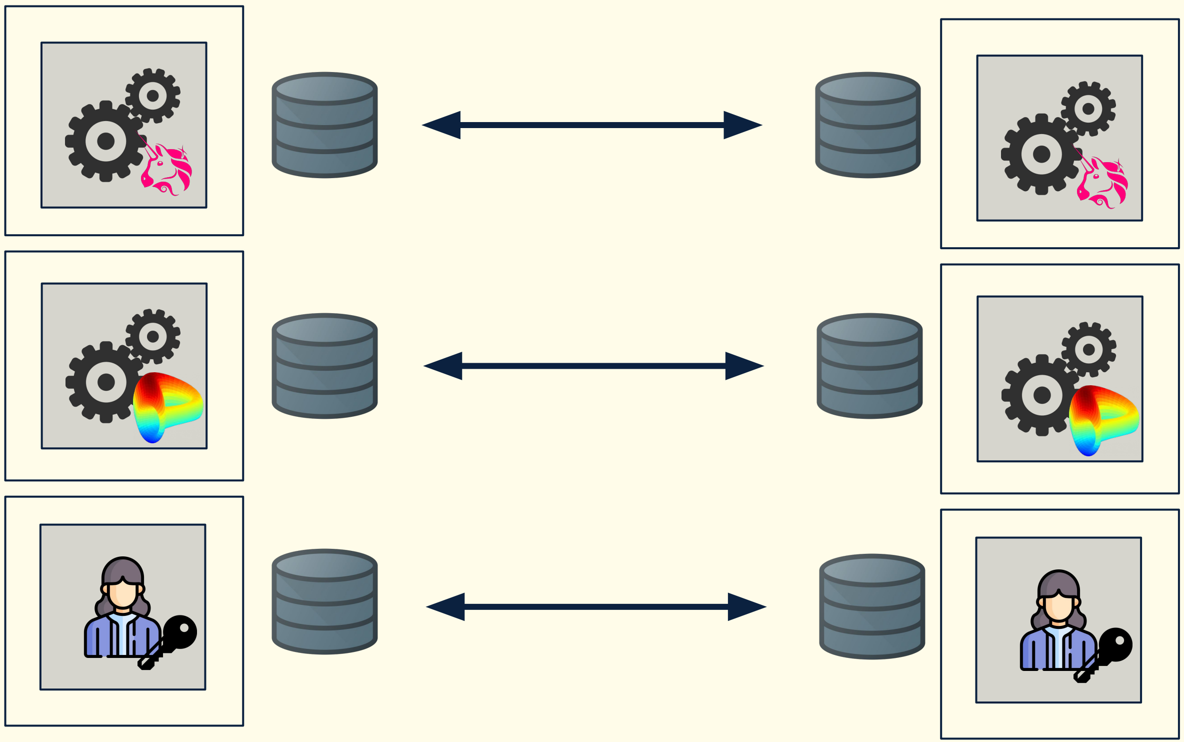
Validators



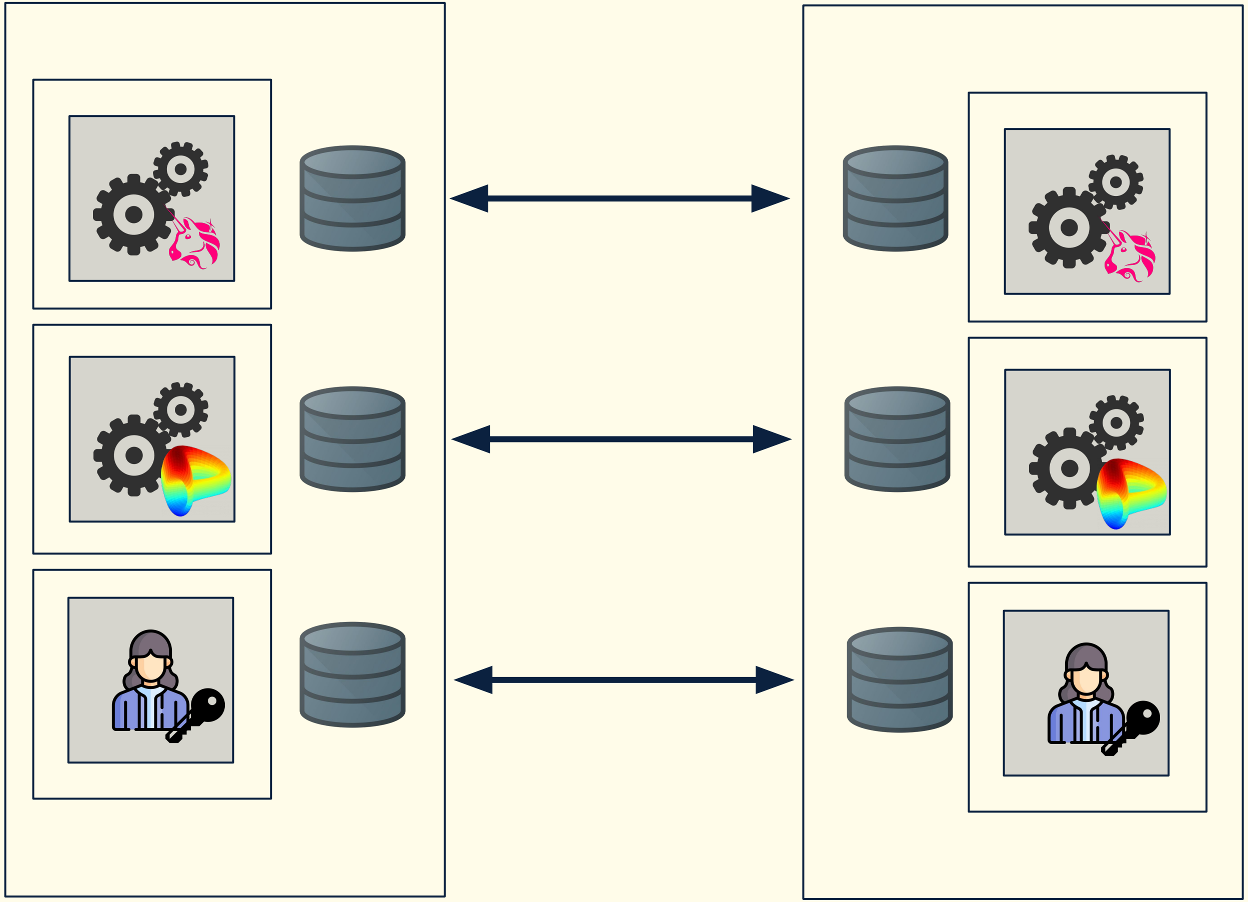
Validators



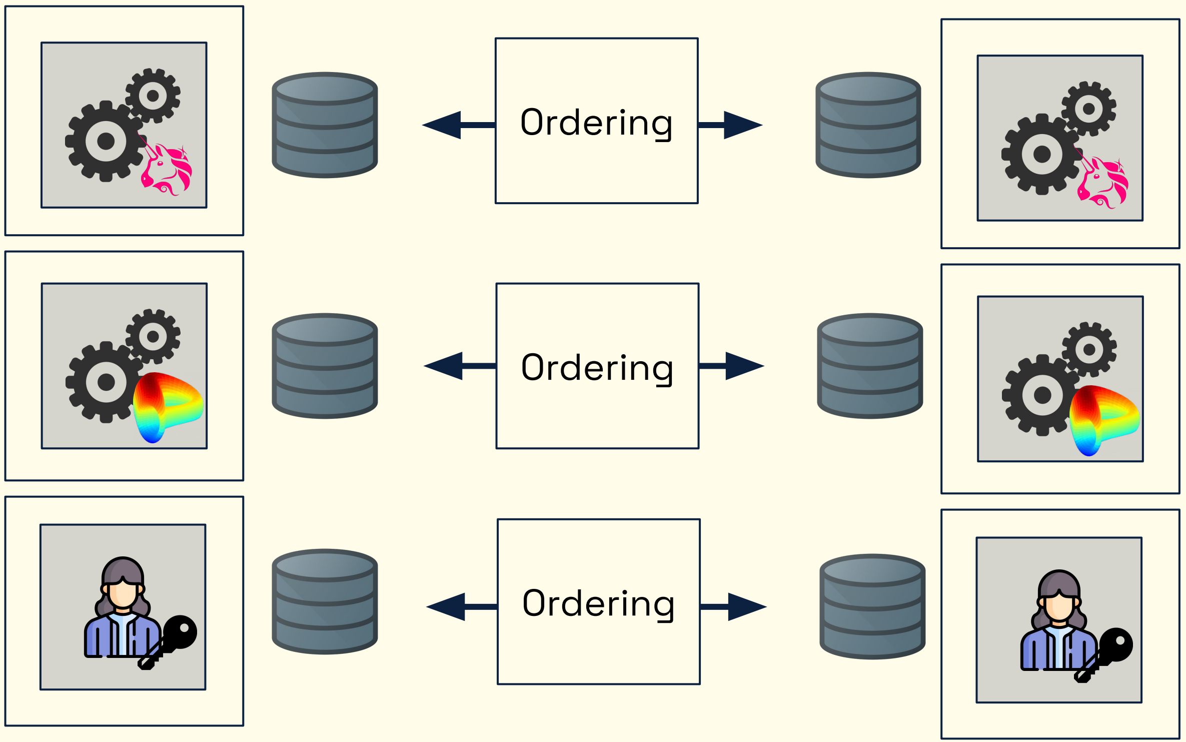
Validators



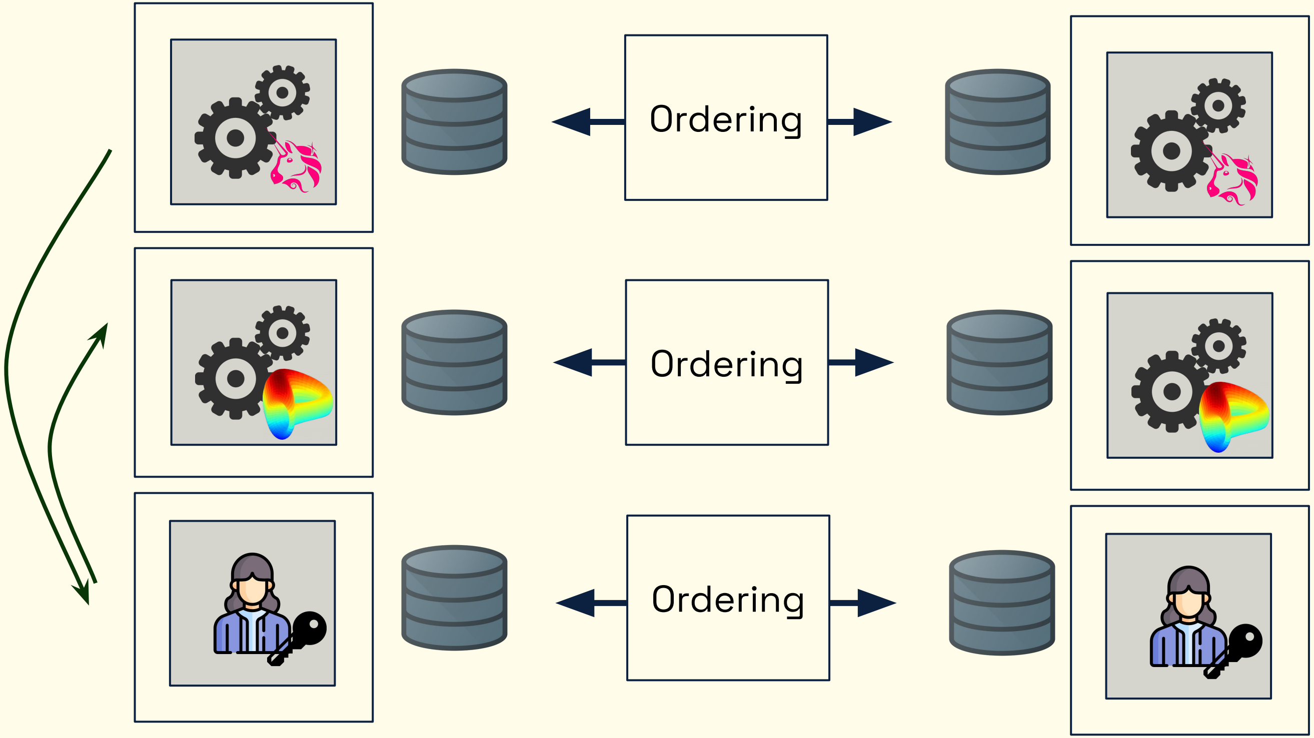
Validators



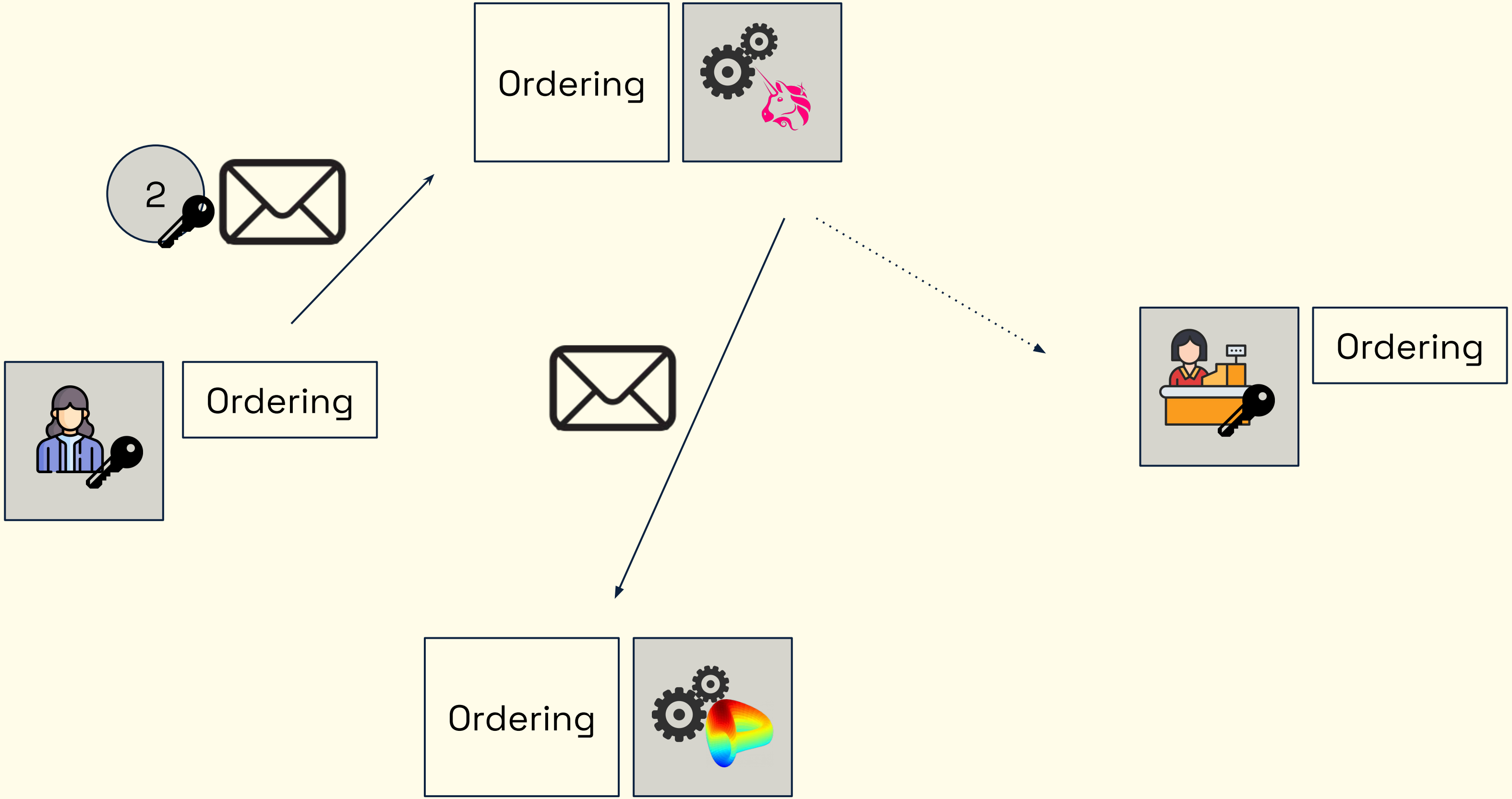
Validators



Validators

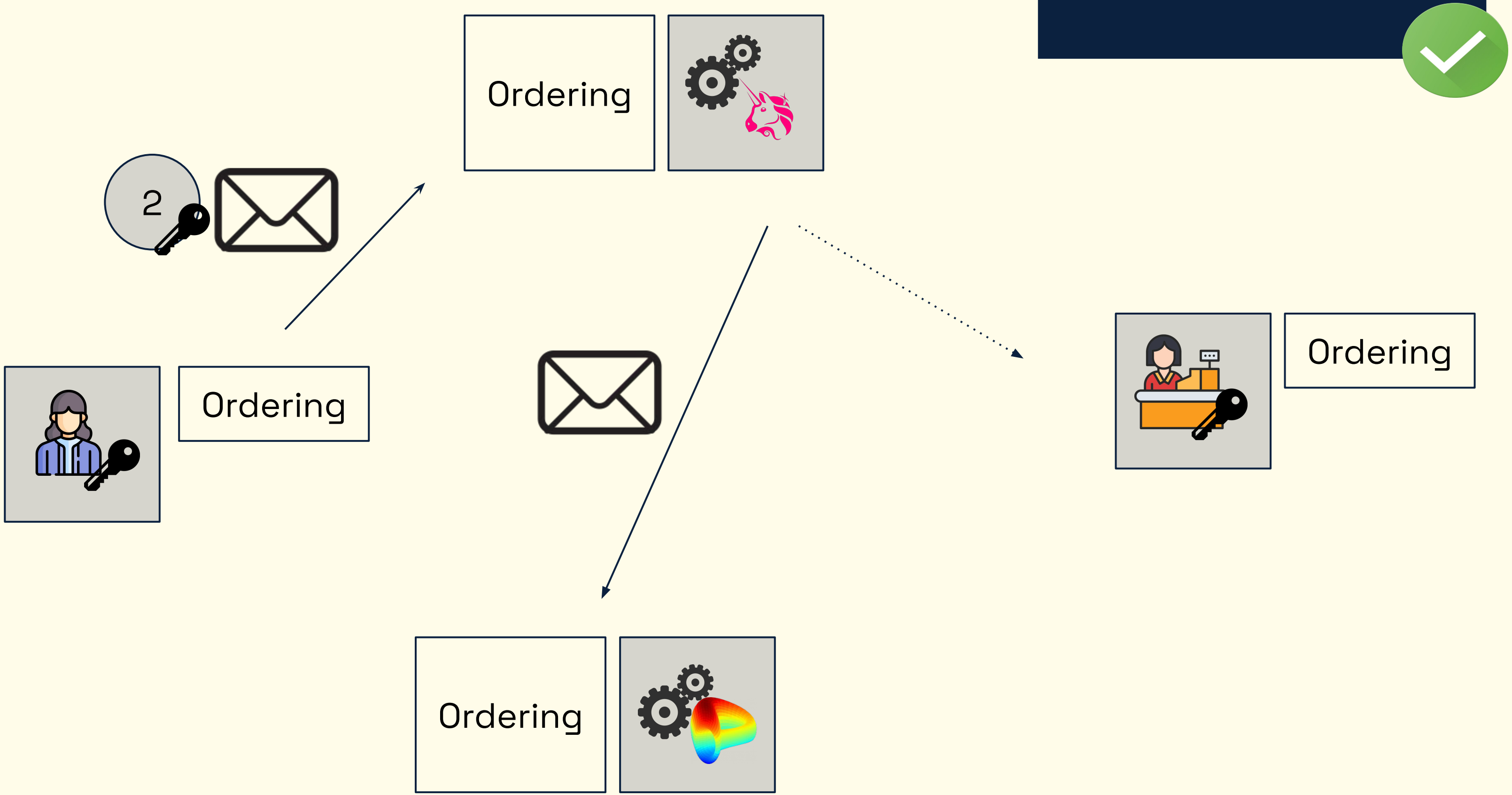


Replicated Actor Model



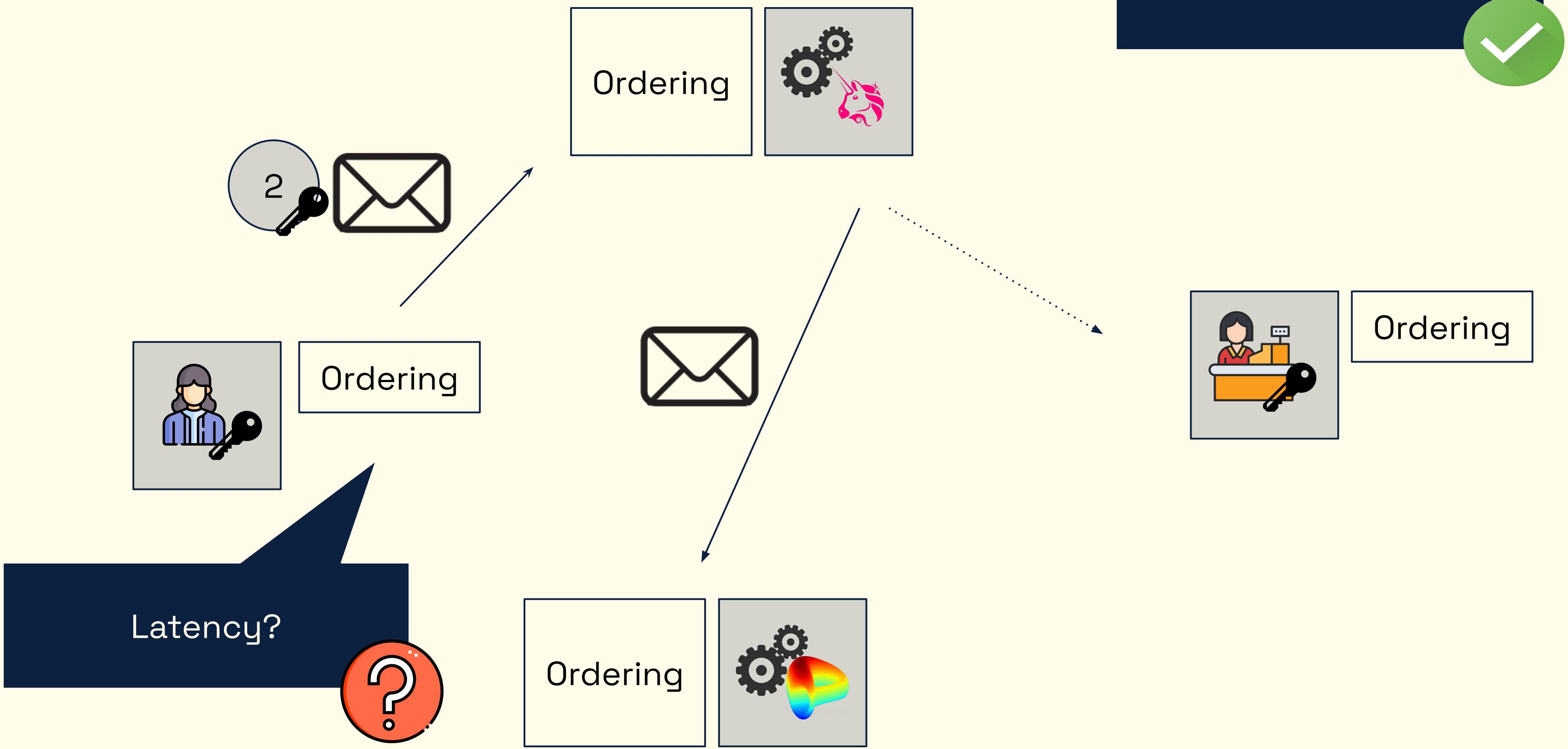
Replicated Actor Model

Parallelizability → Throughput

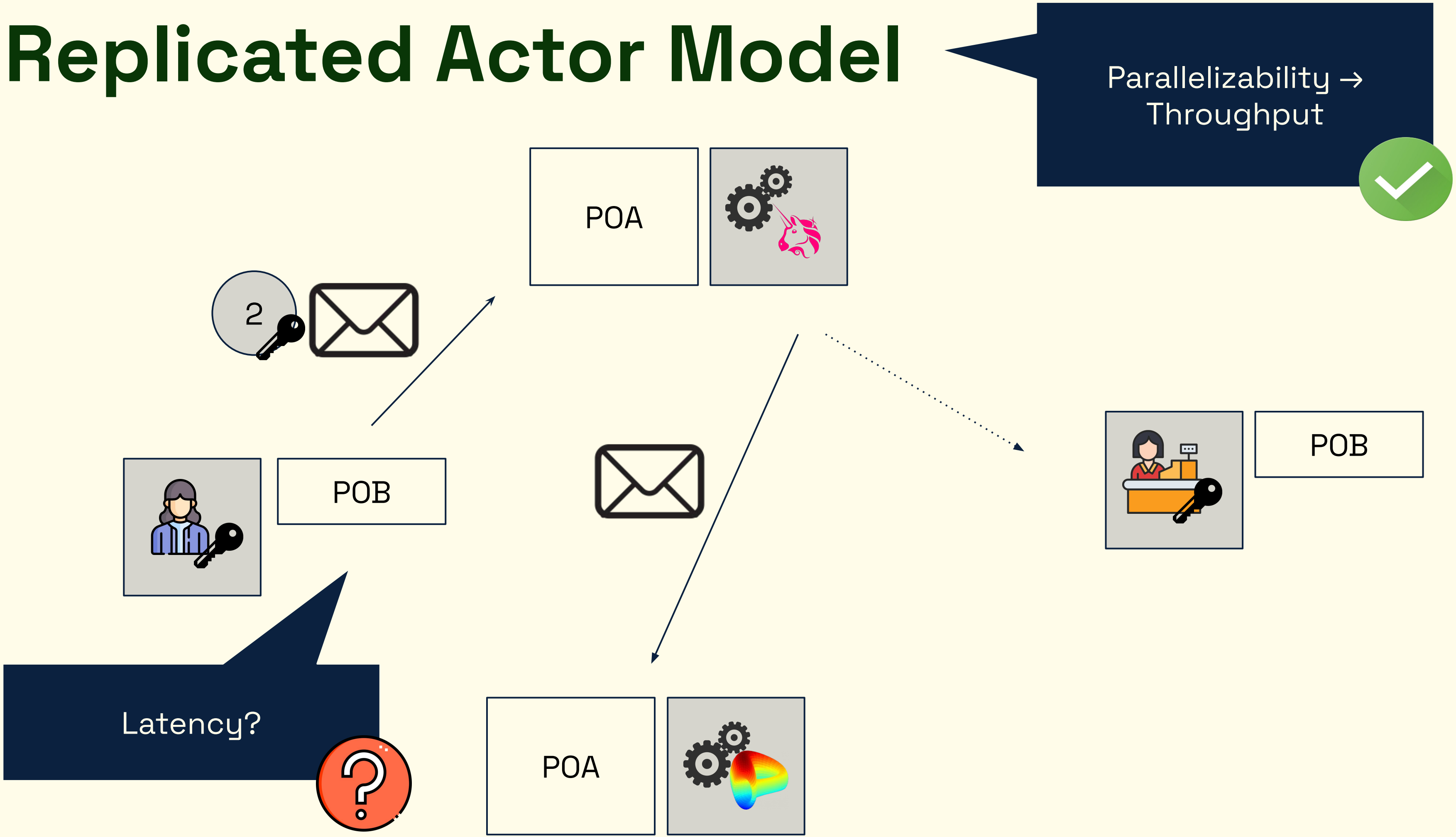


Replicated Actor Model

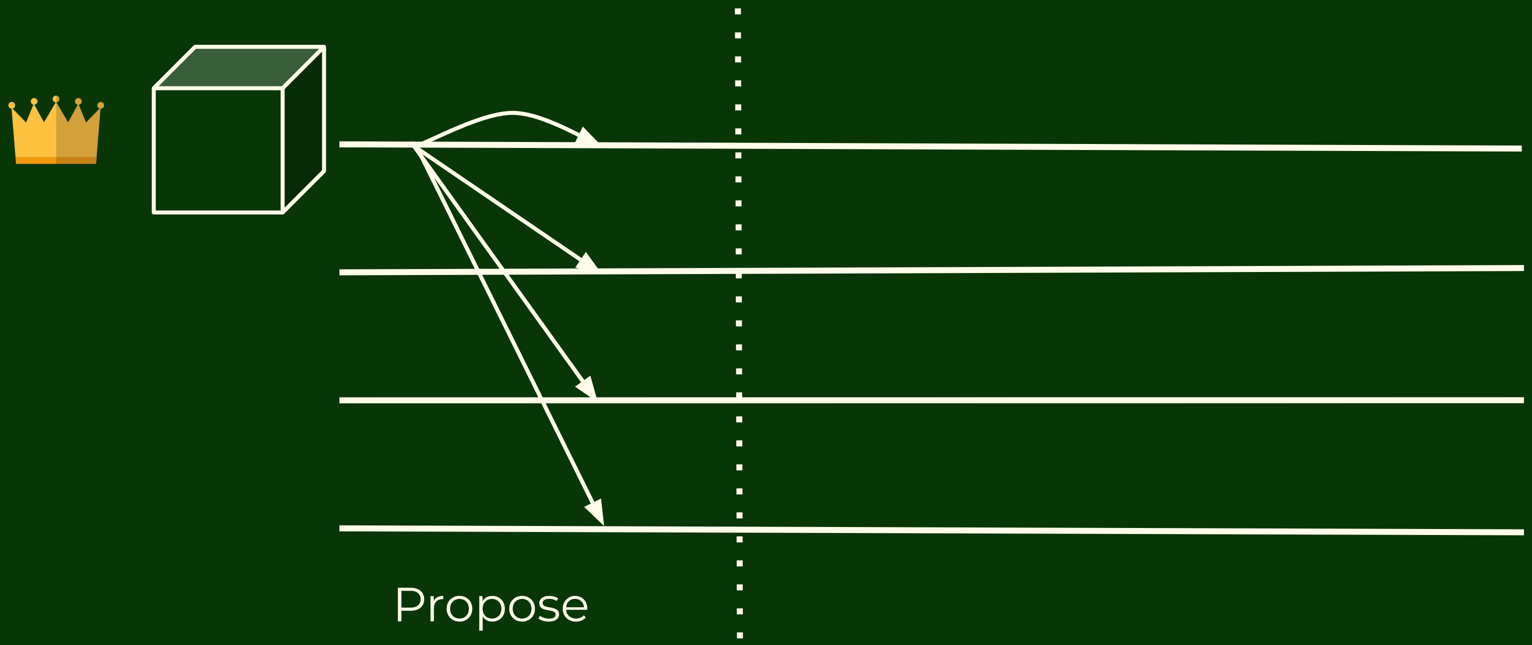
Parallelizability → Throughput



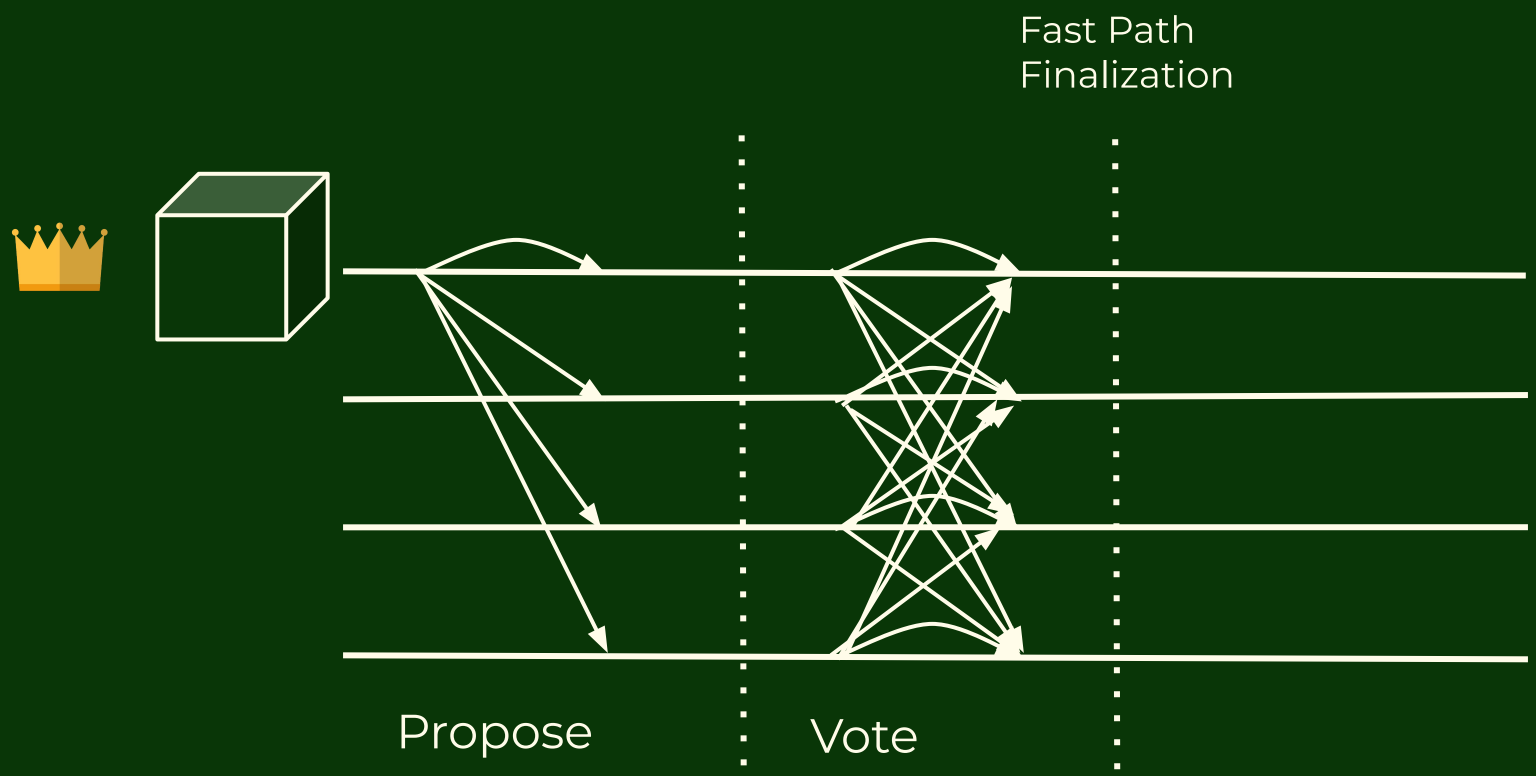
Replicated Actor Model



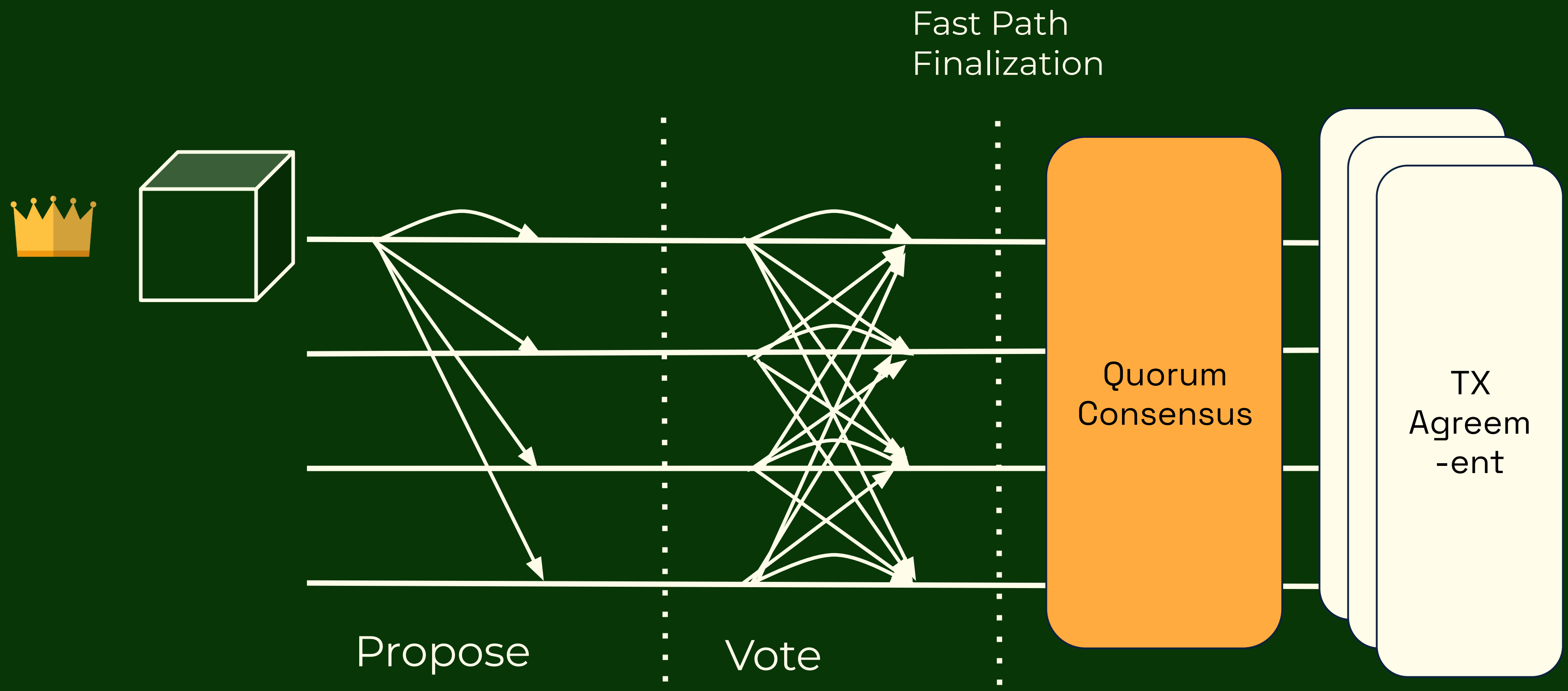
Parallel Optimistic Agreement



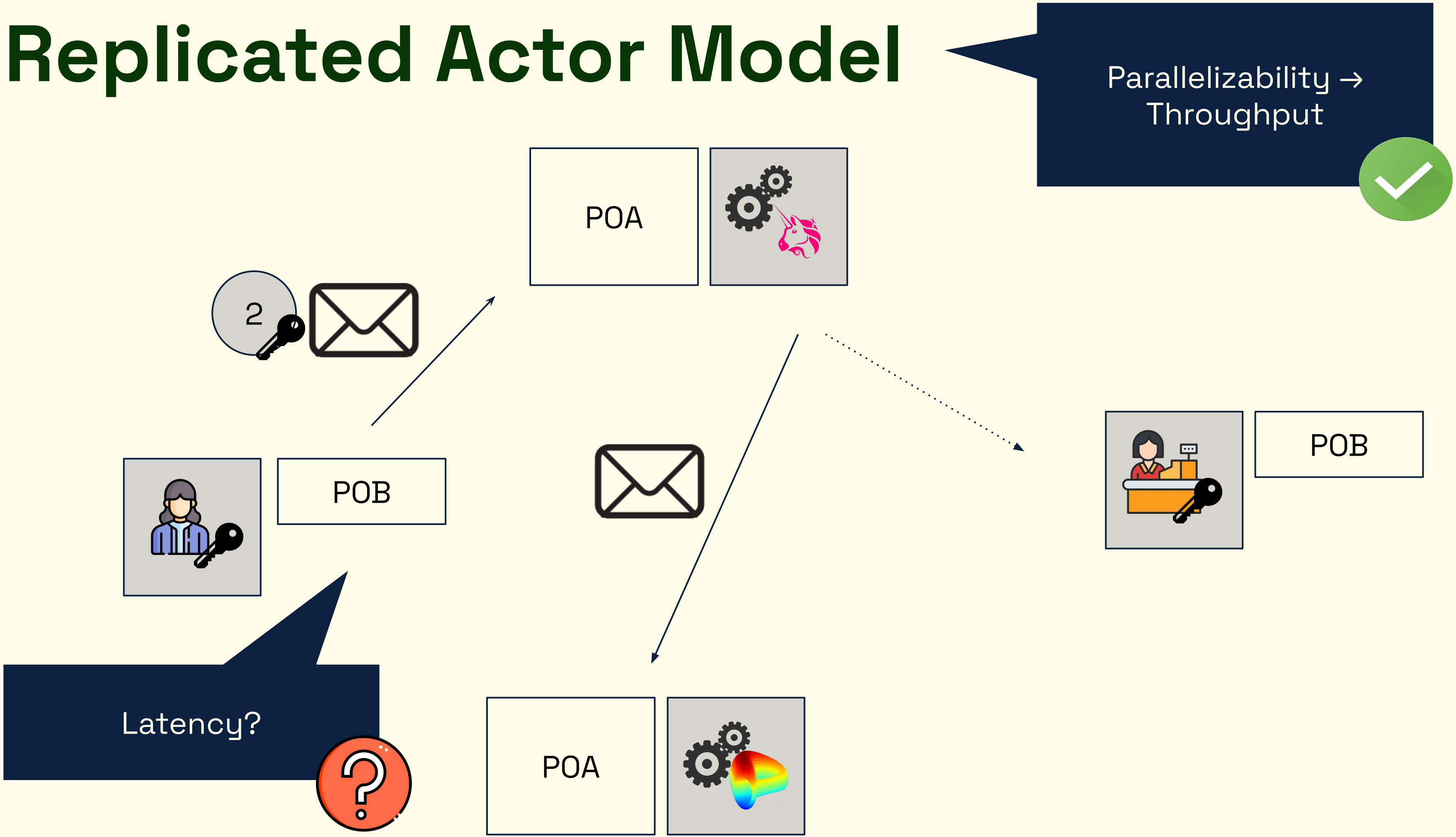
Parallel Optimistic Agreement



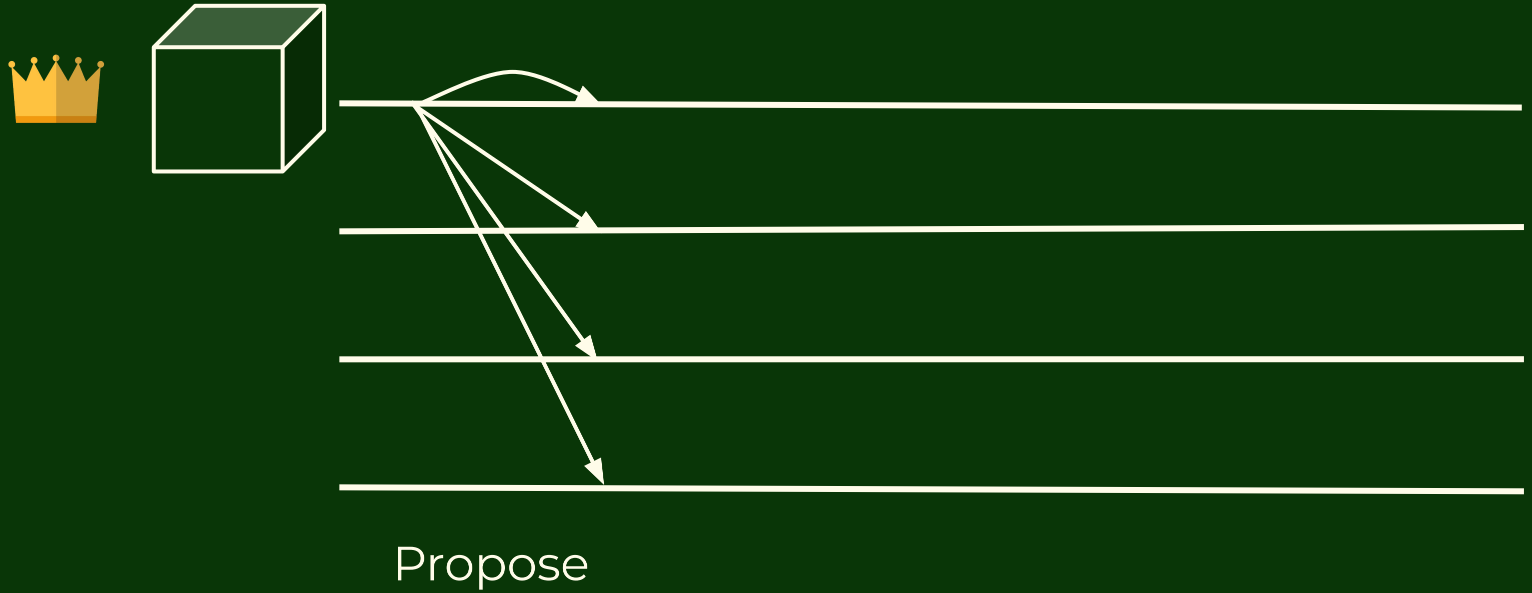
Parallel Optimistic Agreement



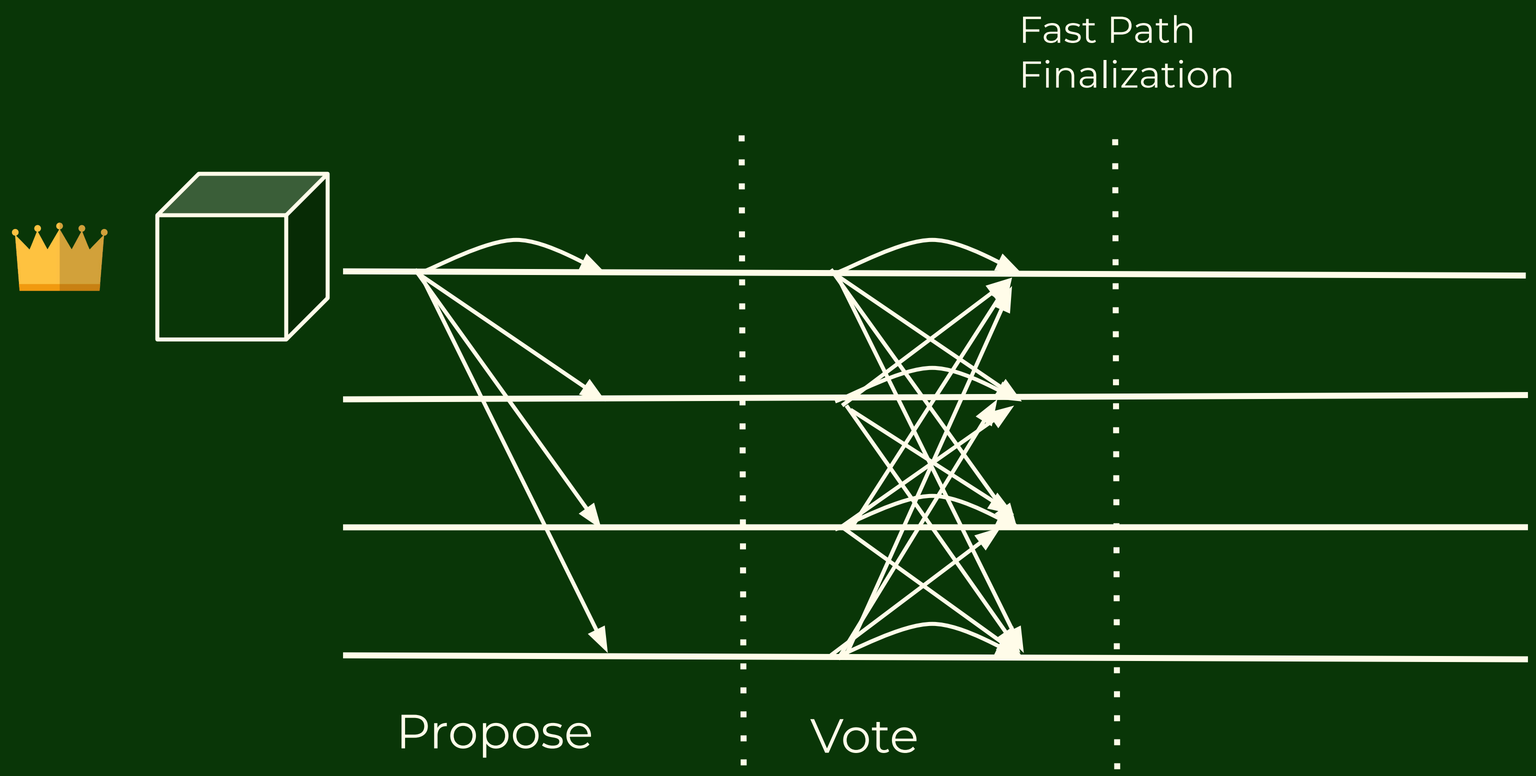
Replicated Actor Model



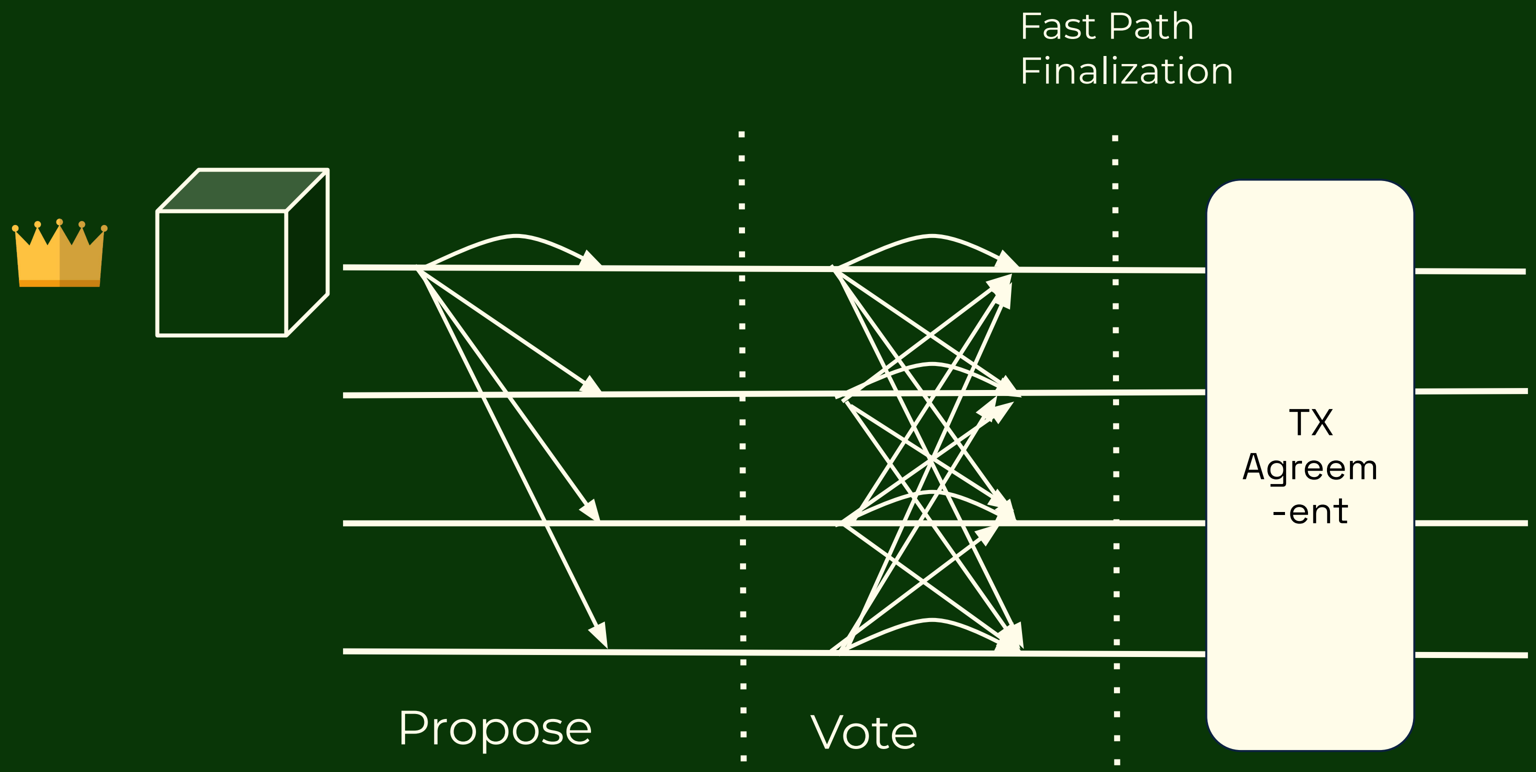
Parallel Optimistic Broadcast



Parallel Optimistic Broadcast



Parallel Optimistic Broadcast



Mangrove Recap

Low Latency

- **2 step commit (optimal)**
- **Resilience (optimal)**
  $n >= 3f + 2p + 1$

Horizontal Scalability

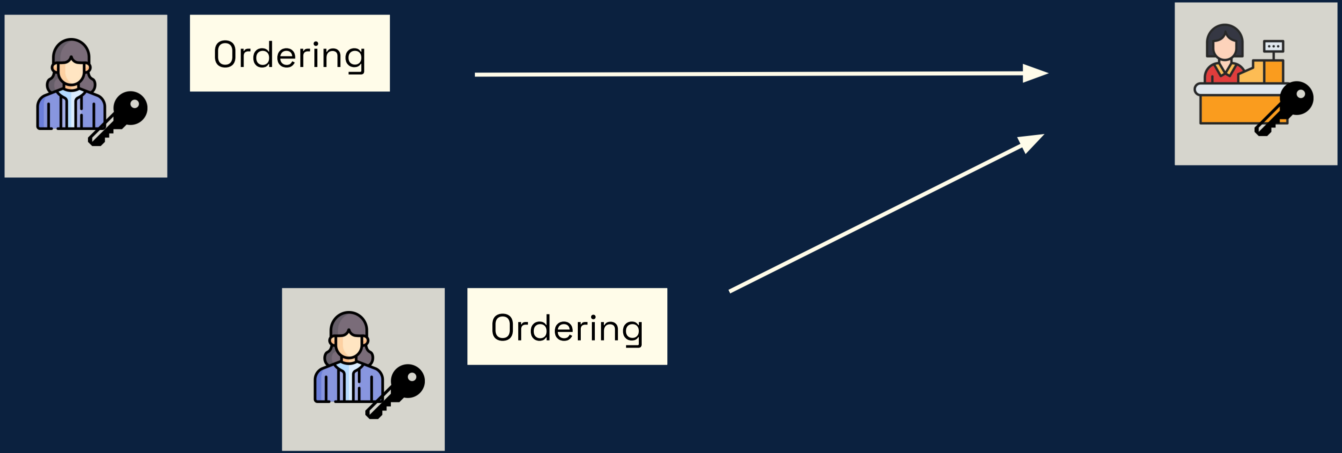
- **No limit to throughput!** every component runs in parallel
- **Congestion pricing is made easy**
- **Incentivizes scalable smart contract design**

Drawbacks

- **Complex transactions** are slower
- **Communication complexity** is high
- **Slow path** is slow

No-Consensus Payment Systems

No-Consensus Payment Systems



No-Consensus Payment Systems

A Non-Consensus Based Decentralized Financial Transaction Processing Model
with Support for Efficient Auditing

by

Saurabh Gupta

A Thesis Presented in Partial Fulfillment
of the Requirements for the Degree
Master of Science

No-Consensus Payment Systems

A Non-Consensus Based Decentralized Financial Transaction Processing Model with Support for Efficient Auditing

by

Saurabh Gupta

A

The Consensus Number of a Cryptocurrency

Rachid Guerraoui
rachid.guerraoui@epfl.ch
EPFL
Lausanne, Switzerland

Petr Kuznetsov
petr.kuznetsov@telecom-paristech.fr
LTCI, Télécom Paris, IP Paris
Paris, France

Matteo Monti
matteo.monti@epfl.ch
EPFL
Lausanne, Switzerland

Matej Pavlovič
matej.pavlovic@epfl.ch
EPFL
Lausanne, Switzerland

Dragos-Adrian Seredinschi*
dragos-adrian.seredinschi@epfl.ch
EPFL
Lausanne, Switzerland

ABSTRACT

Many blockchain-based algorithms, such as Bitcoin, implement a decentralized *asset transfer system*, often referred to as a *cryptocurrency*. As stated in the original paper by Nakamoto, at the heart of these systems lies the problem of preventing *double-spending*; this is usually solved by achieving *consensus* on the order of transfers among the participants. By treating the asset transfer problem as a *concurrent object* and determining its *consensus number*, we show that consensus is not necessary to prevent double-spending.

We first consider the problem as defined by Nakamoto, where only a single process—the account owner—can withdraw from each

KEYWORDS

distributed computing, distributed asset transfer, blockchain, consensus

ACM Reference Format:
Rachid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovič, and Dragos-Adrian Seredinschi. 2019. The Consensus Number of a Cryptocurrency. In *2019 ACM Symposium on Principles of Distributed Computing (PODC'19), July 29–August 2, 2019, Toronto, ON, Canada.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/3293611.3331589

No-Consensus Payment Systems

A Non-Consensus Based Decentralized Financial Transaction Processing Model with Support for Efficient Auditing

by

Saurabh Gupta

A

The Consensus Number of a Cryptocurrency

Rachid Guerraoui
rachid.guerraoui@epfl.ch
EPFL
Lausanne, Switzerland

Petr Kuznetsov
petr.kuznetsov@telecom-paristech.fr
LTCI, Télécom Paris, IP Paris
Paris, France

Matteo Monti
matteo.monti@epfl.ch
EPFL
Lausanne, Switzerland

Matej Pavlovič
matej.pavlovic@epfl.ch
EPFL
Lausanne, Switzerland

Dragos-Adrian Seredinschi*
dragos-adrian.seredinschi@epfl.ch
EPFL
Lausanne, Switzerland

ABSTRACT

KEYWORDS

istributed computing, distributed asset transfer, blockchain, con-
nsus

CM Reference Format:
chid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovič, and Dragos-
rian Seredinschi. 2019. The Consensus Number of a Cryptocurrency. In
*19 ACM Symposium on Principles of Distributed Computing (PODC'19),
ly 29–August 2, 2019, Toronto, ON, Canada.* ACM, New York, NY, USA,
pages. https://doi.org/10.1145/3293611.3331589

ABC: Asynchronous Blockchain without Consensus

Jakub Sliwinski and Roger Wattenhofer

ETH Zurich
{jsliwinski,wattenhofer}@ethz.ch

Abstract. There is a preconception that a blockchain needs consensus. But consensus is a powerful distributed property with a remarkably high price tag. So one may wonder whether consensus is at all needed.
We introduce a new blockchain architecture called ABC that functions despite not establishing consensus, and comes with an array of advantages: ABC is permissionless, deterministic, and resilient to complete asynchrony. ABC features finality and does not rely on costly proof-of-work.
Without establishing consensus, ABC cannot support certain applica-

No-Consensus Payment Systems

A Non-Consensus Based Decentralized Financial Transaction Processing Model with Support for Efficient Auditing

by

Saurabh Gupta

A

The Consensus Number of a Cryptocurrency

Rachid Guerraoui
rachid.guerraoui@epfl.ch
EPFL
Lausanne, Switzerland

Petr Kuznetsov
petr.kuznetsov@telecom-paristech.fr
LTCI, Télécom Paris, IP Paris
Paris, France

Matteo Monti
matteo.monti@epfl.ch
EPFL
Lausanne, Switzerland

Matej Pavlovič
matej.pavlovic@epfl.ch
EPFL
Lausanne, Switzerland

Dragos-Adrian Seredinschi*
dragos-adrian.seredinschi@epfl.ch
EPFL
Lausanne, Switzerland

ABSTRACT

KEYWORDS
...stributed computing, distributed asset transfer, blockchain, con-...nsus

...CM Reference Format:
...chid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovič, and Dragos-...rian Seredinschi. 2019. The Consensus Number of a Cryptocurrency. In ...19 ACM Symposium on Principles of Distributed Computing (PODC'19), ...ly 29–August 2, 2019, Toronto, ON, Canada. ACM, New York, NY, USA, ... pages. https://doi.org/10.1145/3293611.3331589

ABC: Asynchronous Blockchain without Consensus

Jakub Sliwinski and Roger Wattenhofer

ETH Zurich
{jsliwinski,wattenhofer}@ethz.ch

Abstract. There is a preconception that a blockchain needs consensus. But consensus is a powerful distributed property with a remarkably high price tag. So one may wonder whether consensus is at all needed.
We introduce a new blockchain architecture called ABC that functions despite not establishing consensus, and comes with an array of advantages: ABC is permissionless, deterministic, and resilient to complete asynchrony. ABC features finality and does not rely on costly proof-of-work.
Without establishing consensus, ABC cannot support certain applica-

Online Payments by Merely Broadcasting Messages
(Extended Version)

Daniel Collins, Rachid Guerraoui, Jovan Komatovic, Matteo Monti, and Athanasios Xygkis
EPFL

Matej Pavlovic
IBM Research

Petr Kuznetsov
LTCI, Télécom Paris
Institut Polytechnique Paris

Yvonne-Anne Pignolet
DFINITY

Dragos-Adrian Seredinschi
Informal Systems

Andrei Tonkikh
National Research University
Higher School of Economics

...bstract—We address the problem of online *payments*, ...ere users can transfer funds among themselves. We ...oduce *Astro*, a system solving this problem efficiently in ...centralized, deterministic, and completely asynchronous ...nner. Astro builds on the insight that consensus is ...ecessary to prevent double-spending. Instead of consen-... Astro relies on a weaker primitive—Byzantine reliable ...adcast—enabling a simpler and more efficient implemen-...on than consensus-based payment systems.
...n terms of efficiency, Astro executes a payment by merely ...adcasting a message. The distinguishing feature of Astro ...hat it can maintain performance robustly, i.e., remain ...ffected by a fraction of replicas being compromised or ...ved down by an adversary. Our experiments on a public ...d network show that Astro can achieve near-linear ...ability in a sharded setup, going from $10K$ payments/sec ...hards) to $20K$ payments/sec (4 shards). In a nutshell, ...ro can match VISA-level average payment throughput, ... achieves a $5x$ improvement over a state-of-the-art ...sensus-based solution, while exhibiting sub-second 95^{th} ...centile latency.

I. Introduction

...nline payment systems promise secure financial trans- ... continue to do so (Facebook's Libra and many others [32], [35], [45], [46], [58], [63], [68], [78]).

We introduce *Astro*, a decentralized payment system capable of matching the performance of the largest centralized solutions (e.g., $65K$ peak, $7K$ average transactions per second, as recently reported by VISA [77]) for payments.

Astro provides honest participants with *robust* performance, namely stable throughput and latency; this holds independently of network scheduling (i.e., asynchrony) and of compromised replicas, as long as no more than 1/3 of the replicas are affected. Systems building on total order (i.e., agreement), in contrast, are often susceptible to throughput degradation due to a single slow replica, typically the leader. This is an issue that received significant attention in the literature [9], [15], [29], [34], [64], which we discuss in detail (§VII) and also quantify experimentally (§VI-D).

An important insight underlying Astro is that totally ordering all payments can be avoided. Indeed, recent theoretical results show that total order (and hence consensus) is not necessary for preventing double-spending [45], [46]. The main contribution of this paper is to apply this insight by

No-Consensus Payment Systems

A Non-Consensus Based Decentralized Financial Transaction Processing Model with Support for Efficient Auditing

by

Saurabh Gupta

Online Payments by Merely Broadcasting Messages
(Extended Version)

Daniel Collins, Rachid Guerraoui, Jovan Komatovic, Matteo Monti, and Athanasios Xygkis
Matej Pavlovic, *IBM Research*
Petr Kuznetsov, *LTCI, Télécom Paris*
Yvonne-Anne …, *DFINITY*

The Consensus Number of a Cryptocurrency

Rachid Guerraoui, rachid.guerraoui@epfl.ch, EPFL, Lausanne, Switzerland
Petr Kuznetsov, petr.kuznetsov@telecom-paristech.fr, LTCI, Télécom Paris, IP Paris, Paris, France
Matteo Monti, matteo.monti@epfl.ch, EPFL, Lausanne, Switzerland
Matej Pavlovič, matej.pavlovic@epfl.ch, EPFL, Lausanne, Switzerland
Dragos-Adrian Seredinschi*, dragos-adrian.seredinschi@epfl.ch, EPFL, Lausanne, Switzerland

ABSTRACT

KEYWORDS
…istributed computing, distributed asset transfer, blockchain, con…nsus

…CM Reference Format:
…chid Guerraoui, Petr Kuznetsov, Matteo Monti, Matej Pavlovič, and Dragos-…rian Seredinschi. 2019. The Consensus Number of a Cryptocurrency. In …19 *ACM Symposium on Principles of Distributed Computing (PODC'19),* …ly *29–August 2, 2019, Toronto, ON, Canada.* ACM, New York, NY, USA, … pages. https://doi.org/10.1145/3293611.3331589

ABC: Asynchronous Blockchain without Consensus

Jakub Sliwinski and Roger Wattenhofer
ETH Zurich
{jsliwinski,wattenhofer}@ethz.ch

Abstract. There is a preconception that a blockchain needs consensus. But consensus is a powerful distributed property with a remarkably high price tag. So one may wonder whether consensus is at all needed.
We introduce a new blockchain architecture called ABC that functions despite not establishing consensus, and comes with an array of advantages: ABC is permissionless, deterministic, and resilient to complete asynchrony. ABC features finality and does not rely on costly proof-of-work.
Without establishing consensus, ABC cannot support certain applica…

FastPay: High-Performance Byzantine Fault Tolerant Settlement

Mathieu Baudet*, mathieubaudet@fb.com, Facebook Novi
George Danezis, gdanezis@fb.com, Facebook Novi
Alberto Sonnino, asonnino@fb.com, Facebook Novi

ABSTRACT
FastPay allows a set of distributed authorities, some of which are Byzantine, to maintain a high-integrity and availability settlement system for pre-funded payments. It can be used to settle payments in a native unit of value (crypto-currency), or as a financial side-infrastructure to support retail payments in fiat currencies. FastPay is based on Byzantine Consistent Broadcast as its core primitive, foregoing the expenses of full atomic commit channels (consensus). The resulting system has low-latency for both confirmation and payment finality. Remarkably, each authority can be sharded across many machines to allow unbounded horizontal scalability. Our experiments demonstrate intra-continental confirmation latency of less than 100ms, making FastPay applicable to point of sale payments. In laboratory environments, we achieve over 80,000 transactions per second with 20 authorities—surpassing the requirements of current retail card payment networks, while significantly increasing their robustness.

KEYWORDS
distributed system, bft, settlement system, consistent broadcast

ACM Reference Format:
Mathieu Baudet, George Danezis, and Alberto Sonnino. 2020. FastPay: High-Performance Byzantine Fault Tolerant Settlement. In *Proceedings of ACM Conference (Conference'17).* ACM, New York, NY, USA, 15 pages.

1 INTRODUCTION

Real-time gross settlement systems (RTGS) [4] constitute the most …

FastPay is a Byzantine Fault Tolerant (BFT) real-time gross settlement (RTGS) system. It enables authorities to jointly maintain account balances and settle pre-funded retail payments between accounts. It supports extremely low-latency confirmation (sub-second) of eventual transaction finality, appropriate for physical point-of-sale payments. It also provides extremely high capacity, comparable with peak retail card network volumes, while ensuring gross settlement in real-time. FastPay eliminates counterparty and credit risks of net settlement and removes the need for intermediate banks, and complex financial contracts between them, to absorb these risks. FastPay can accommodate arbitrary capacities through efficient sharding architectures at each authority. Unlike any traditional RTGS, and more like permissioned blockchains, FastPay can tolerate up to f Byzantine failures out of a total of $3f+1$ authorities, and retain both safety, liveness, and high-performance.

FastPay can be deployed in a number of settings. First, it may be used as a settlement layer for a native token and crypto-currency, in a standalone fashion. Second, it may be deployed as a side-chain of another crypto-currency, or as a high performance settlement layer on the side of an established RTGS to settle fiat retail payments. In this paper we present this second functionality in detail, since it exercises all features of the system, both payments between FastPay accounts, as well as payments into and out of the system.

Contributions. We make the following contributions:

- The FastPay design is novel in that if forgoes full consensus; it leverages the semantics of payments to minimize shared state between accounts and to increase the concurrency of asynchronous operations; and supports sharded authorities.

No-Consensus Payment Systems

1. Low-latency (2-step)

2. Parallelizable / Horizontally Scalable

No-Consensus Payment Systems

1. Low-latency (2-step)
2. Parallelizable / Horizontally Scalable

Only if sender doesn't misbehave!

No smart contracts!

No-Consensus Payment Systems

1. Low-latency (2-step)

2. Parallelizable / Horizontally Scalable

Only if sender doesn't misbehave!

No smart contracts!

Mangrove solves both!

Thank You

Fast and Parallelizable State Replication for Blockchains

Anton Paramonov, Yann Vonlanthen, Quentin Kniep, Jakub Sliwinski, and Roger Wattenhofer

*ETH Zurich - **Dis**tributed **Co**mputing Group*