MONDAY 27TH JUNE 2022

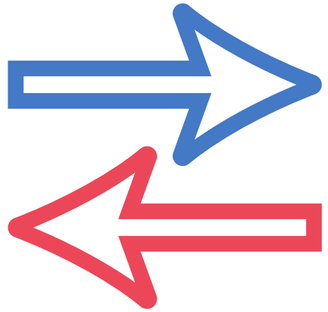
Imperial College London

Exploring the Relationship Between Speed and Security of Cross-chain Transactions

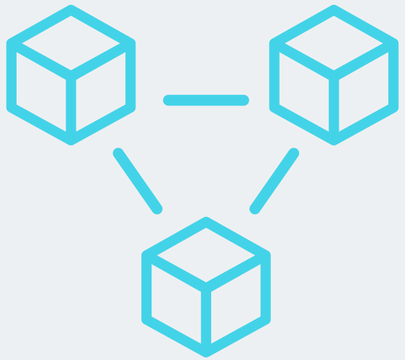
Reece Jackson

Surpervisor
Dr. Arthur Gervais

Second Marker
Dr. Mark Wheelhouse



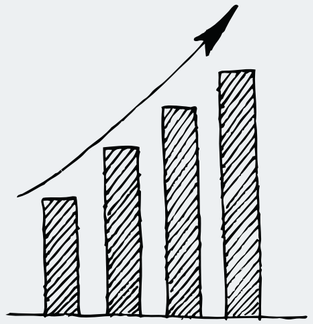
Cross-chain Transfer



Blockchain

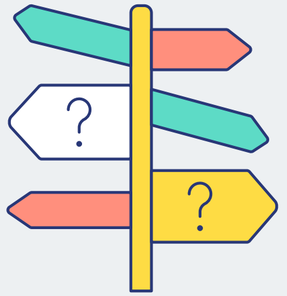
Back to Overview

The Problem



Rapid Growth
and
Popularity

Lack of
Communication
and Interconnectivity



Unfocused
and Sub-optimal
Expanison

How the problem helps to form my question

1

Why does the problem exist?

- Lack of research?
- Technical difficulty?
- Priority?

2

Factors that may contribute

- Cost of transfer
- Speed of transfer
- Security of transfer
- Scalability

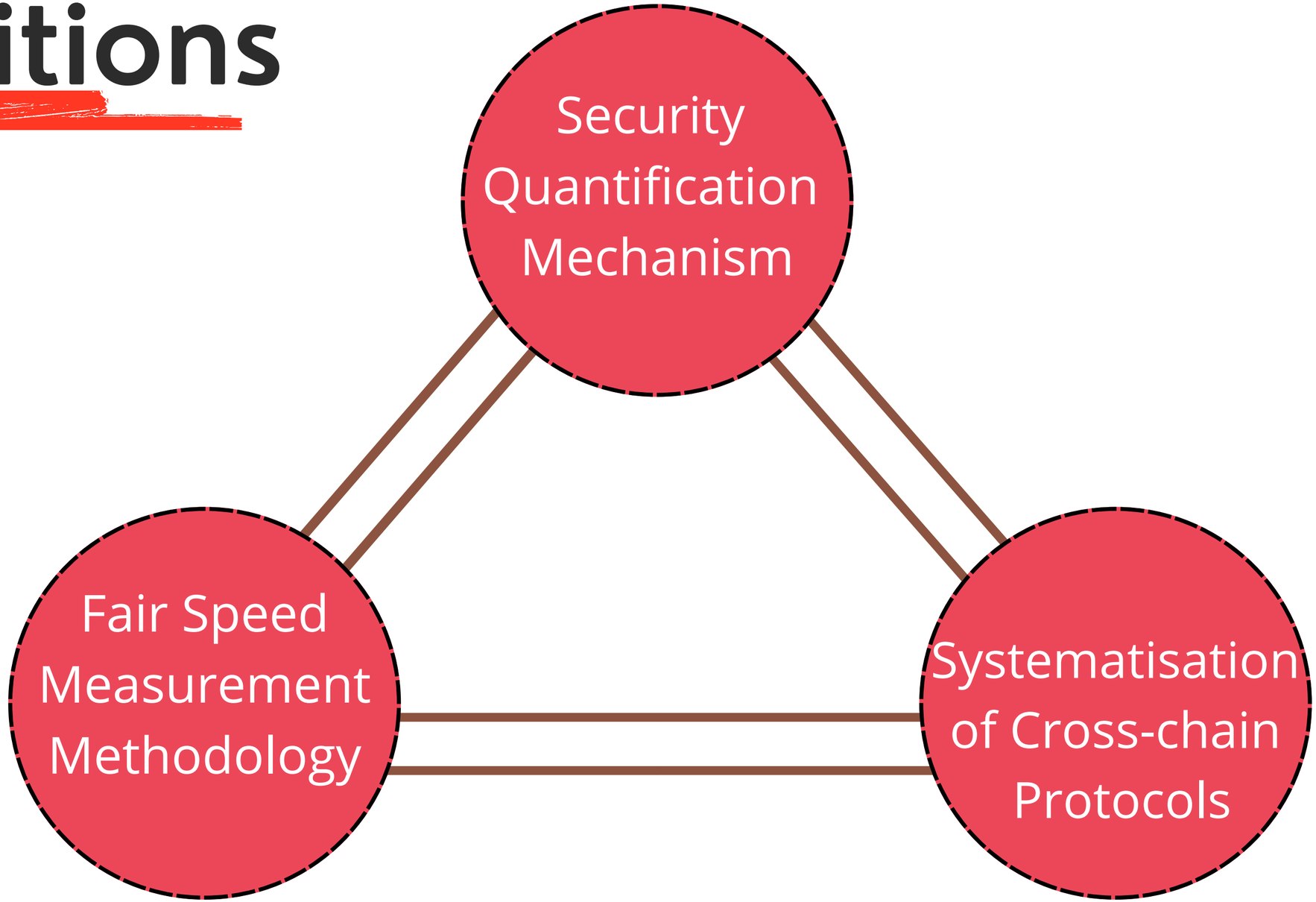
3

What stage are current solutions at?

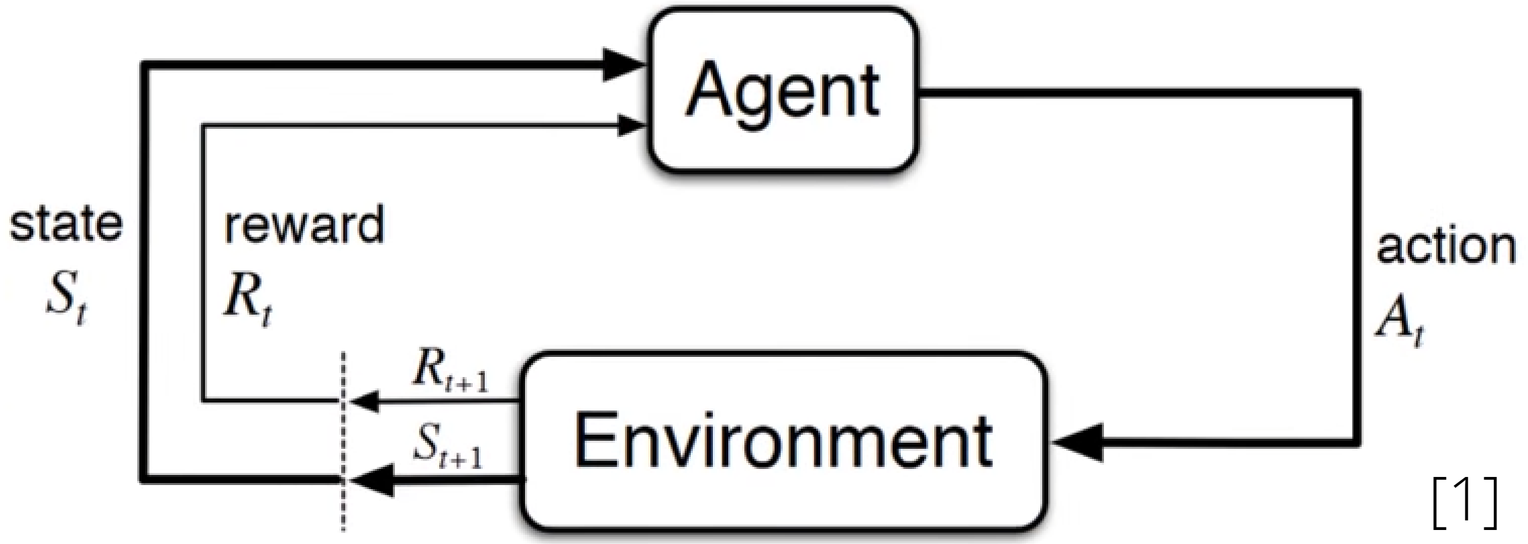
- How many blockchains are facilitated?
- Are transfers bi-directional?
- Can transfers be chained together?

Back to Overview

Ambitions



Markov Decision Problems (MDP) and Markov Chains

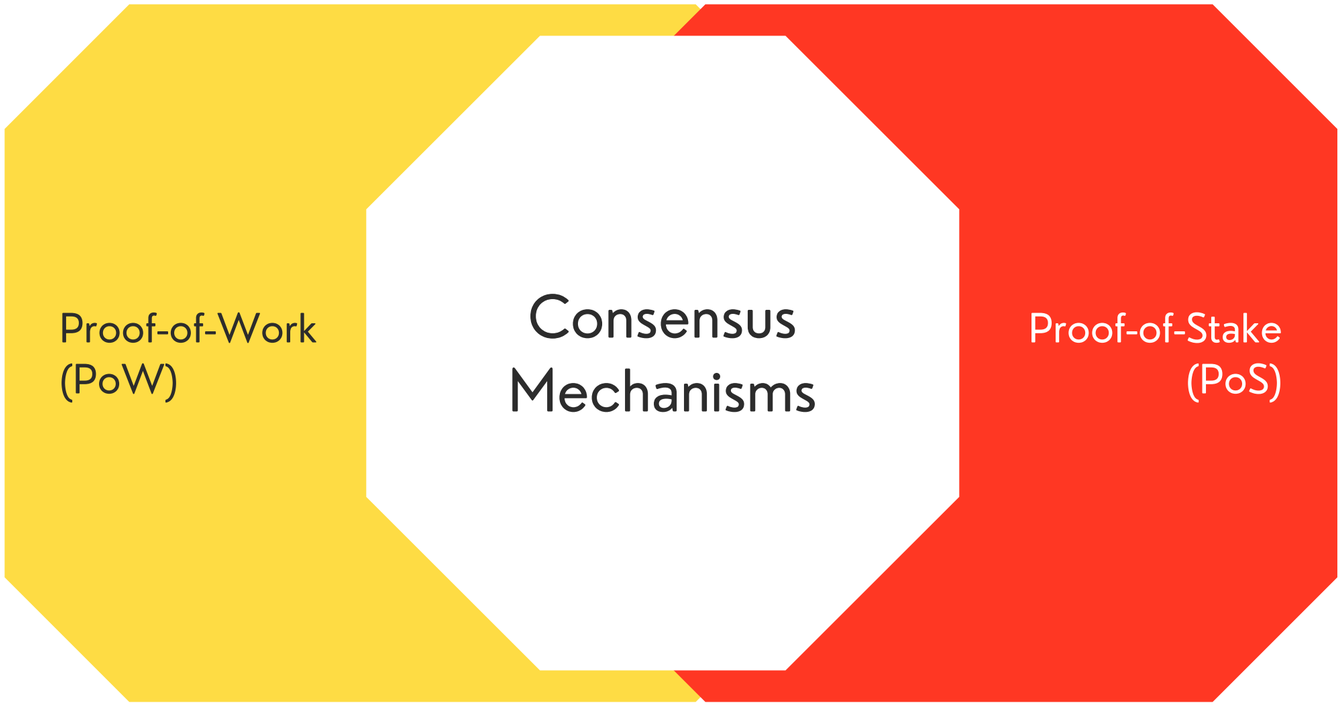


[1]

[1] Deeplizard. Markov Decision Processes (MDPs) - Structuring a Reinforcement Learning Problem; 2018. Available from: https://deeplizard.com/learn/video/my207WNoeyA.

Back to Overview

Blockchain Validation



PoW Blockchains Discussed

Proof-of-Work (PoW)

Consensus Mechanisms

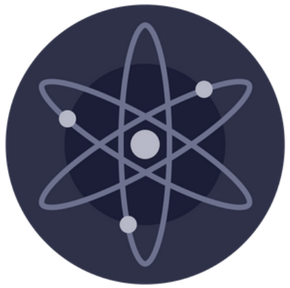
Bitcoin

Litecoin

PoS Blockchains Discussed

Consensus Mechanisms

Proof-of-Stake (PoS)

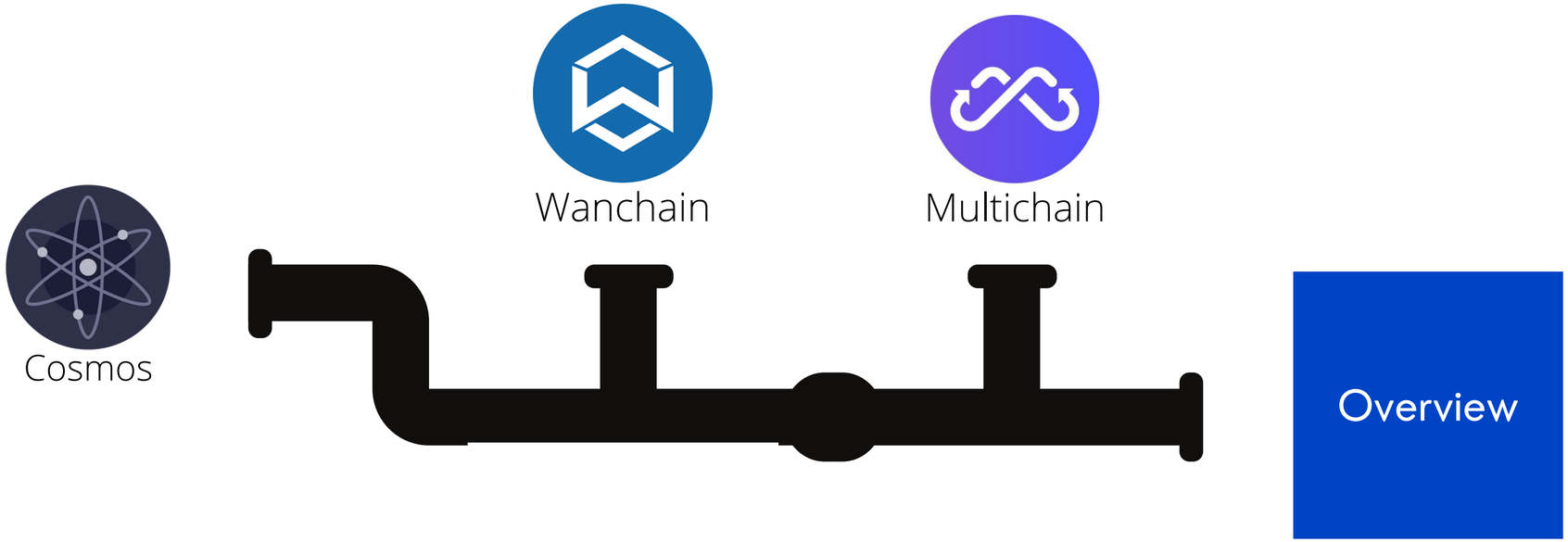


Cosmos

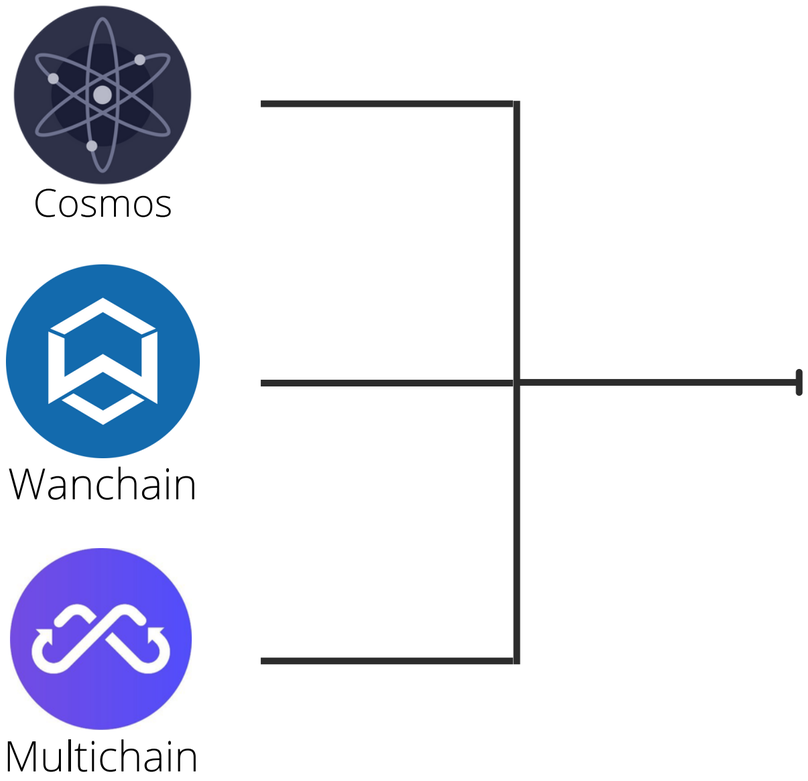
Multichain

Wanchain

The Systematisation of PoS Cross-chain Protocols



Transfer-in Process



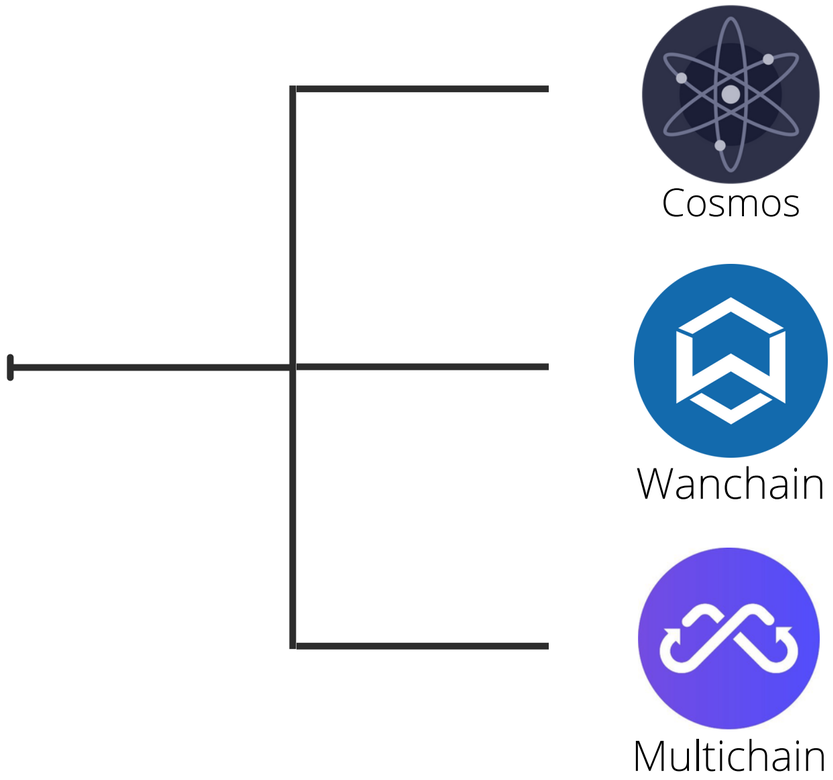
- User sends tokens to a locked account
- Bridge Receipt Verification
- Minting of Wrapped Assets
- User Receives Wrapped Tokens

Transfer-out Process

User Triggers
Transfer-back Request

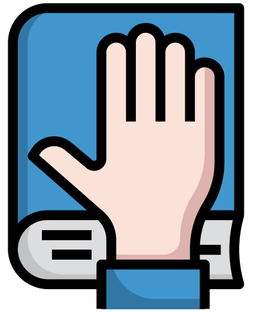
Wrapped Assets are Burned

Locked Assets are Unlocked
and Distributed



Back to Overview

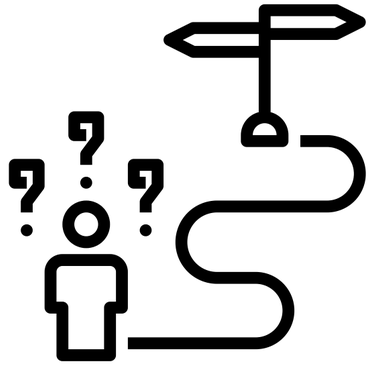
Assumption - Bridge Model



Adversary is rational	Irrational behaviour presents itself to new possibilities
Bridge begins transfer-in process immediately	Delays mean longer confirmation time is needed
Bridge assumed to be an honest participant	Expands the problem space

Back to Overview

Assumption - Native or Non-Native



- Transfer-in and Transfer-out processes differ
- This is depends on whether the token is Native or Non-Native
- Extend for the exploration between Nativity, in relation to Speed and Security

Security Methodology - Double-Spend Attack

α - Attacker Hashrate Fraction

γ - Propagation Factor

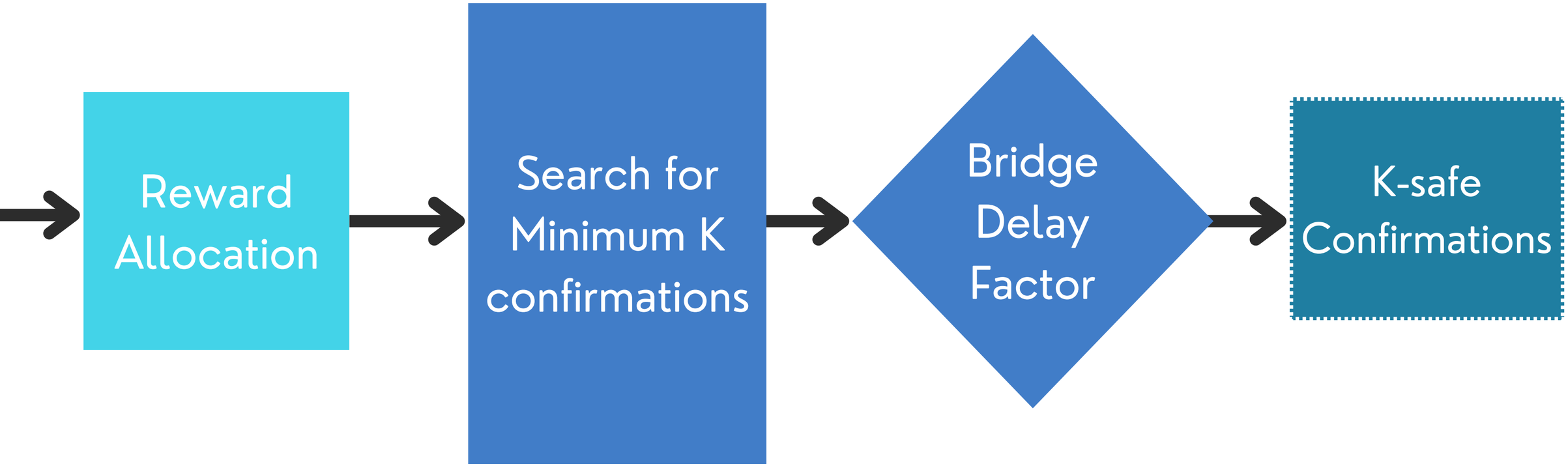
r_s - Stale Block Rate

→ Formation of State-Action Space → Probability Assignment →

[2]

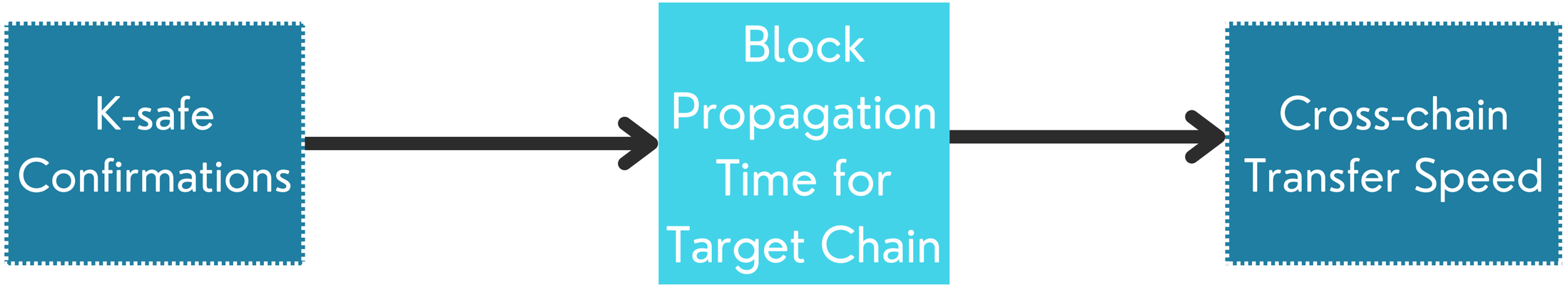
[2] Gervais A, Karame GO, Wüst K, Glykantzis V, Ritzdorf H, Capkun S. On the security and performance of proof of work blockchains. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security; 2016. p. 3-16.

Security Methodology - Double-Spend Attack



[2]

Speed Methodology



Data collection [2]

	Bitcoin	Litecoin
Block Propagation Time	8.7 s	1.02 s
Block Propagation Time	6.73 s (Currently)	1.02 s
Average Block Size	533.1 KB	6.11 KB
Average Block Size	913.2 KB (Currently)	147.8 KB
Stale Block Rate	1.41%	0.273%
Stale Block Rate	3.17% (Currently)	1.13%

Evaluation of Stable Block Rate Estimation

Previous measurements indicated instability [3]

Updated parameters used for Blockchain Simulator [3]

Justified trade-off between time and accuracy

[3] Gervais A, Bitcoin Simulator - Experimental Results, 2017. Available from: http://arthurgervais.github.io/Bitcoin-Simulator/results.html

Evaluation of Average Block Size Choice

Previous research [...] full history [2]

Market dynamics and protocol restructuring have occurred

Opted with using only previous year history

Back to Overview

Summary and Conclusion

First Bridge Security Quantification, Including K-confirmations

Cross-chain Systematisation

Security and Speed Comparison Methodology