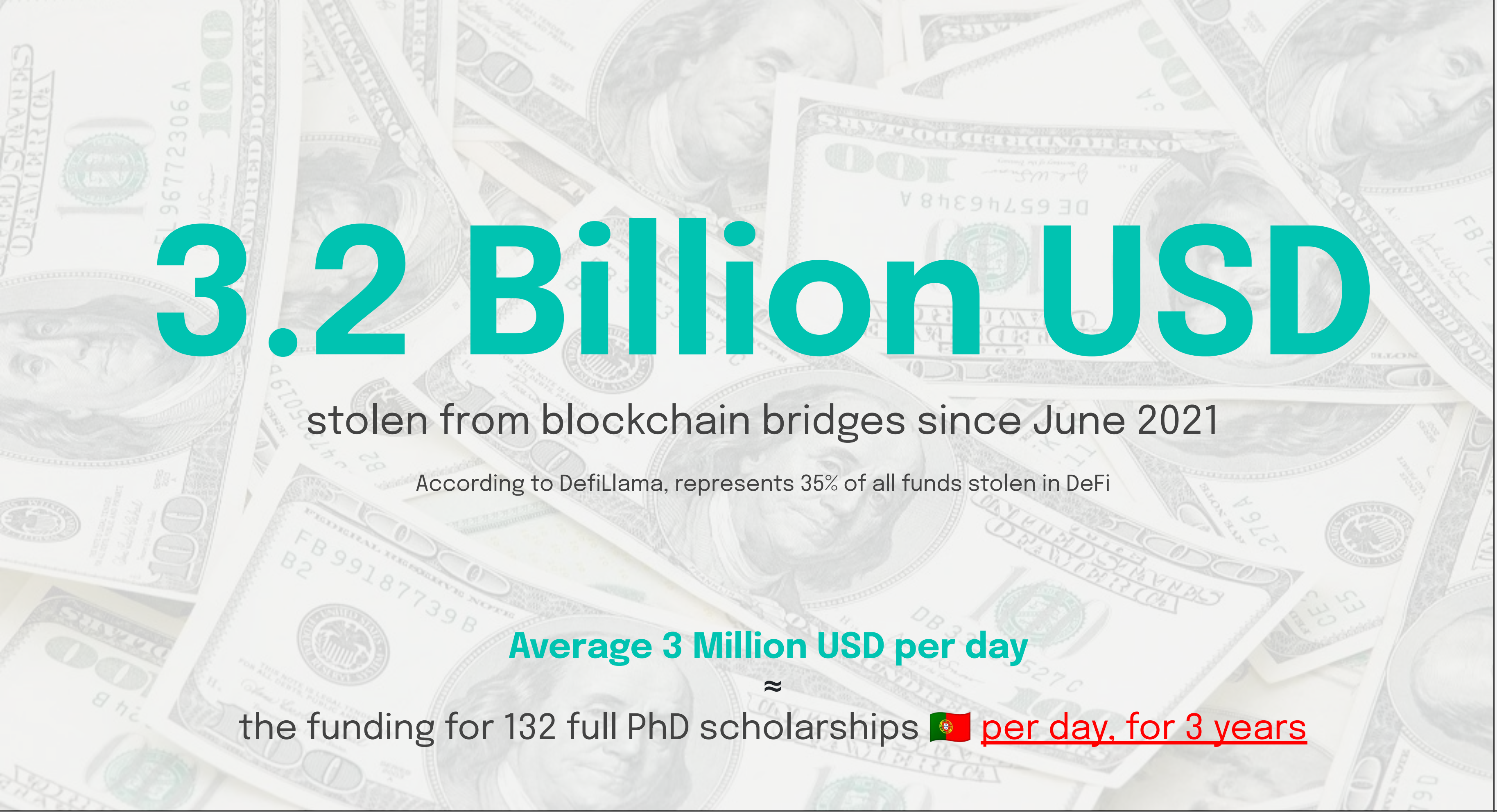
Distributed Ledger Interoperability Security

Rafael Belchior (INESC-ID, Instituto Superior Técnico)

Supervisor: Prof. André Vasconcelos
Co-supervisor: Prof. Miguel Pupo Correia

24 September 2024, Lisboa



3.2 Billion USD

stolen from blockchain bridges since June 2021

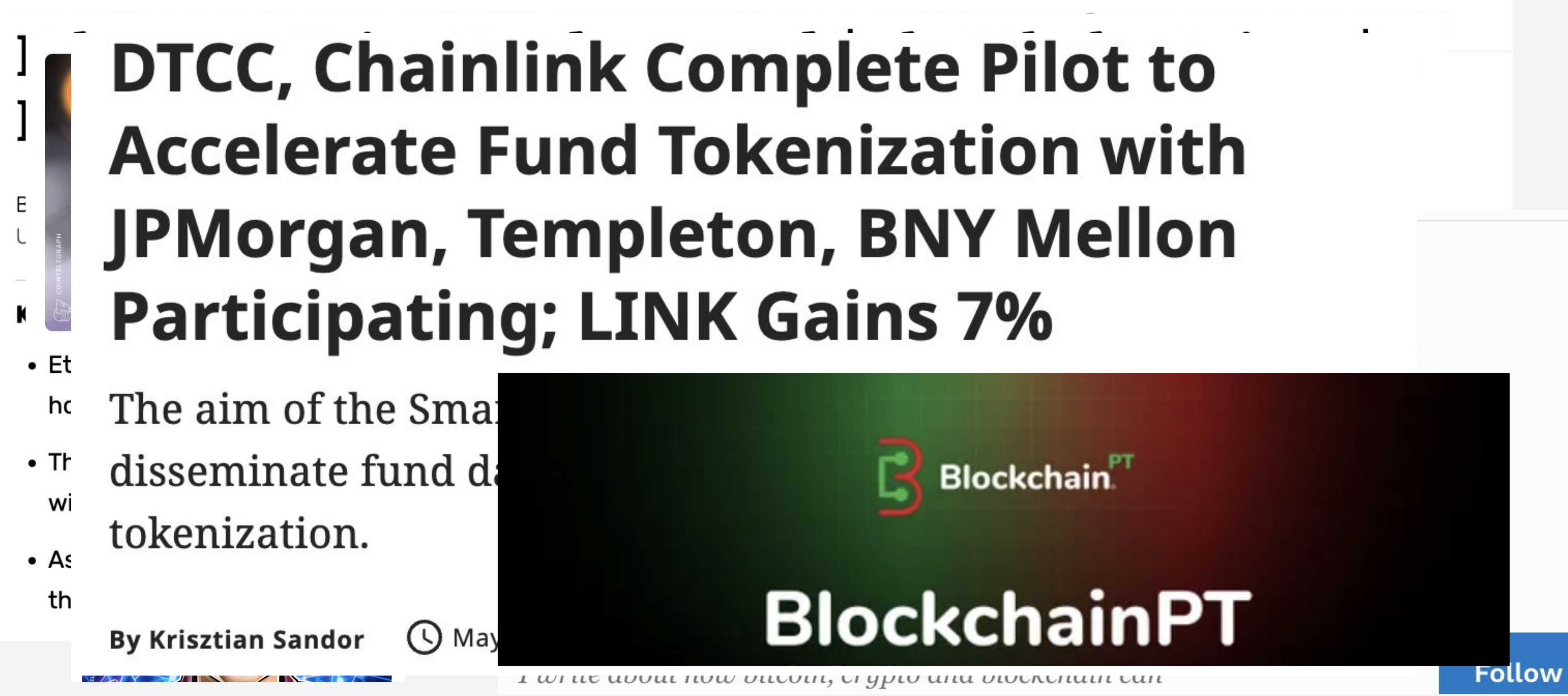
According to DefiLlama, represents 35% of all funds stolen in DeFi

Average 3 Million USD per day

≈

the funding for 132 full PhD scholarships 🇵🇹 per day, for 3 years

Why do we care about DLT



- Et
  ho
- Th
  wi
- As
  th

DTCC, Chainlink Complete Pilot to Accelerate Fund Tokenization with JPMorgan, Templeton, BNY Mellon Participating; LINK Gains 7%

The aim of the Sma
disseminate fund d
tokenization.

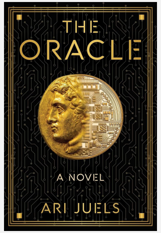
By Krisztian Sandor May

I write about how bitcoin, crypto and blockchain can

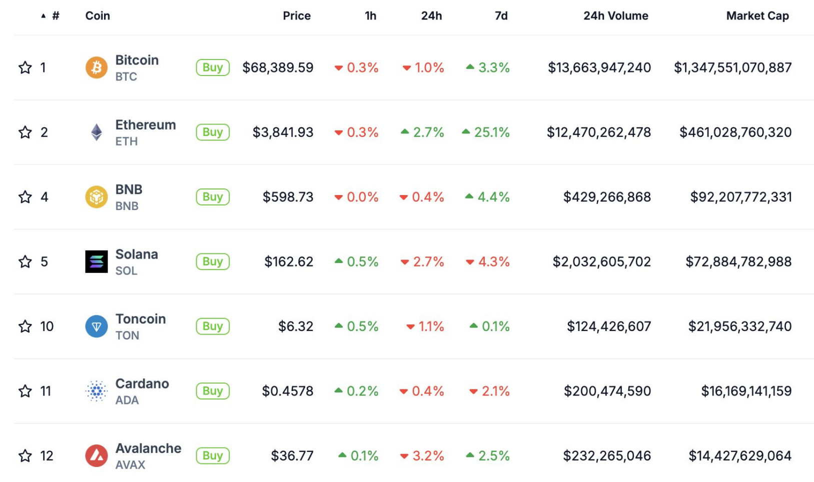
Before oracles came along, practically the only thing anyone did with blockchains was ***move money around*** *and breed ugly digital blockchain cats called CryptoKitties.*

When oracles first came on line, it felt like living in a primitive city ***that finally got electricity****.*

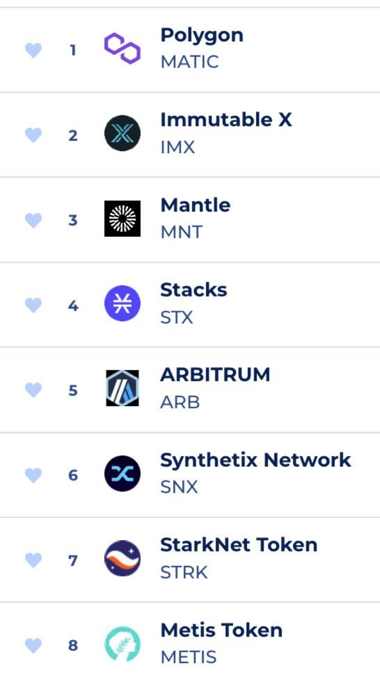
from "The Oracle: A Novel" by Ari Juels



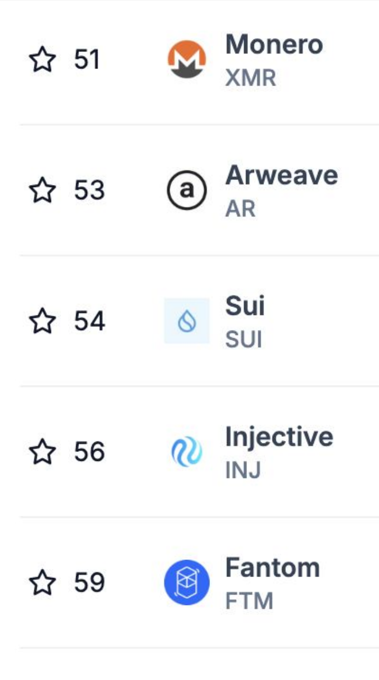
The rise of Interoperability



▲ #	Coin		Price	1h	24h	7d	24h Volume	Market Cap
☆ 1	Bitcoin BTC	Buy	$68,389.59	▼ 0.3%	▼ 1.0%	▲ 3.3%	$13,663,947,240	$1,347,551,070,887
☆ 2	Ethereum ETH	Buy	$3,841.93	▼ 0.3%	▲ 2.7%	▲ 25.1%	$12,470,262,478	$461,028,760,320
☆ 4	BNB BNB	Buy	$598.73	▼ 0.0%	▼ 0.4%	▲ 4.4%	$429,266,868	$92,207,772,331
☆ 5	Solana SOL	Buy	$162.62	▲ 0.5%	▼ 2.7%	▼ 4.3%	$2,032,605,702	$72,884,782,988
☆ 10	Toncoin TON	Buy	$6.32	▲ 0.5%	▼ 1.1%	▲ 0.1%	$124,426,607	$21,956,332,740
☆ 11	Cardano ADA	Buy	$0.4578	▲ 0.2%	▼ 0.4%	▼ 2.1%	$200,474,590	$16,169,141,159
☆ 12	Avalanche AVAX	Buy	$36.77	▲ 0.1%	▼ 3.2%	▲ 2.5%	$232,265,046	$14,427,629,064



♥	1	Polygon	MATIC
♥	2	Immutable X	IMX
♥	3	Mantle	MNT
♥	4	Stacks	STX
♥	5	ARBITRUM	ARB
♥	6	Synthetix Network	SNX
♥	7	StarkNet Token	STRK
♥	8	Metis Token	METIS



☆	51	Monero	XMR
☆	53	Arweave	AR
☆	54	Sui	SUI
☆	56	Injective	INJ
☆	59	Fantom	FTM

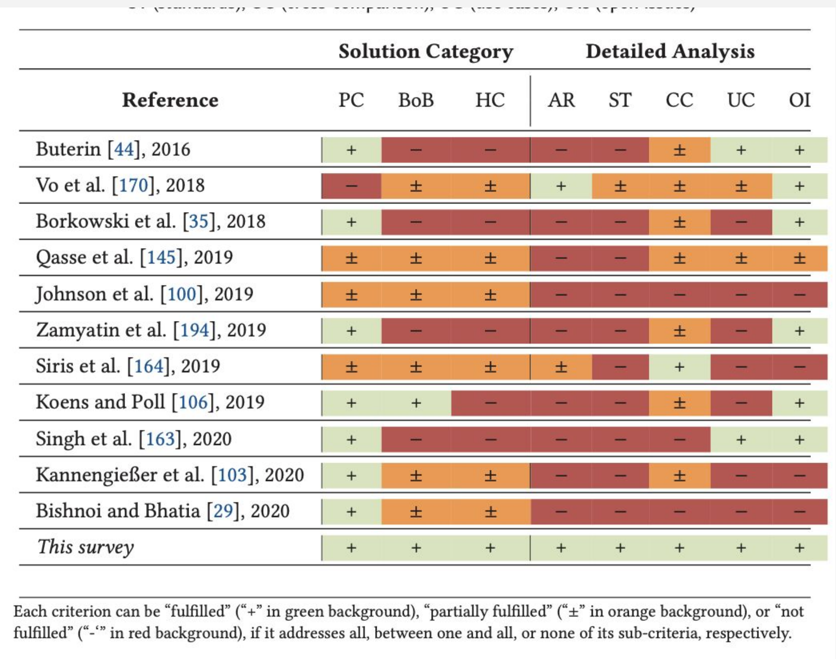
New generation of financial infrastructure

Secure Asset Transfer Protocol (SATP)

SWIFT Chainlink Integration Explained

Cross-Chain DvP Settlement

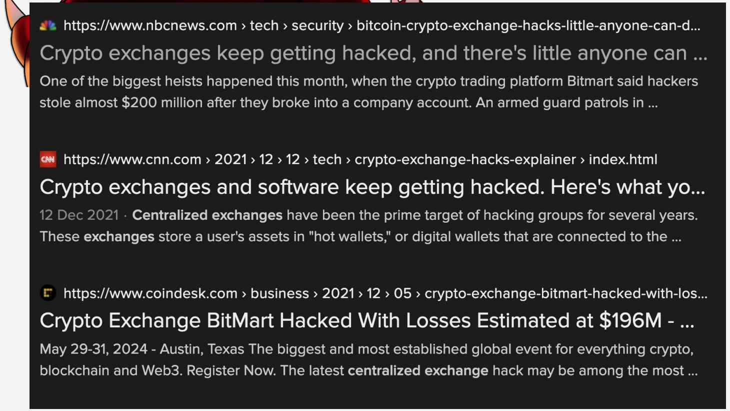
Current Problems



ST (standards), CC (cross-comparison), UC (use cases), OI (open issues)

	Solution Category			Detailed Analysis				
Reference	PC	BoB	HC	AR	ST	CC	UC	OI
Buterin [44], 2016	+	−	−	−	−	±	+	+
Vo et al. [170], 2018	−	±	±	+	±	±	±	+
Borkowski et al. [35], 2018	+	−	−	−	−	±	−	+
Qasse et al. [145], 2019	±	±	±	−	−	±	±	±
Johnson et al. [100], 2019	±	±	±	−	−	−	−	−
Zamyatin et al. [194], 2019	+	−	−	−	−	±	−	+
Siris et al. [164], 2019	±	±	±	±	−	+	−	−
Koens and Poll [106], 2019	+	+	−	−	−	±	−	+
Singh et al. [163], 2020	+	−	−	−	−	−	+	+
Kannengießer et al. [103], 2020	+	±	±	−	−	±	−	−
Bishnoi and Bhatia [29], 2020	+	±	±	−	−	−	−	−
This survey	+	+	+	+	+	+	+	+

Each criterion can be "fulfilled" ("+" in green background), "partially fulfilled" ("±" in orange background), or "not fulfilled" ("-‵" in red background), if it addresses all, between one and all, or none of its sub-criteria, respectively.



https://www.nbcnews.com › tech › security › bitcoin-crypto-exchange-hacks-little-anyone-can-d...

Crypto exchanges keep getting hacked, and there's little anyone can ...

One of the biggest heists happened this month, when the crypto trading platform Bitmart said hackers stole almost $200 million after they broke into a company account. An armed guard patrols in ...

https://www.cnn.com › 2021 › 12 › 12 › tech › crypto-exchange-hacks-explainer › index.html

Crypto exchanges and software keep getting hacked. Here's what yo...

12 Dec 2021 · **Centralized exchanges** have been the prime target of hacking groups for several years. These **exchanges** store a user's assets in "hot wallets," or digital wallets that are connected to the ...

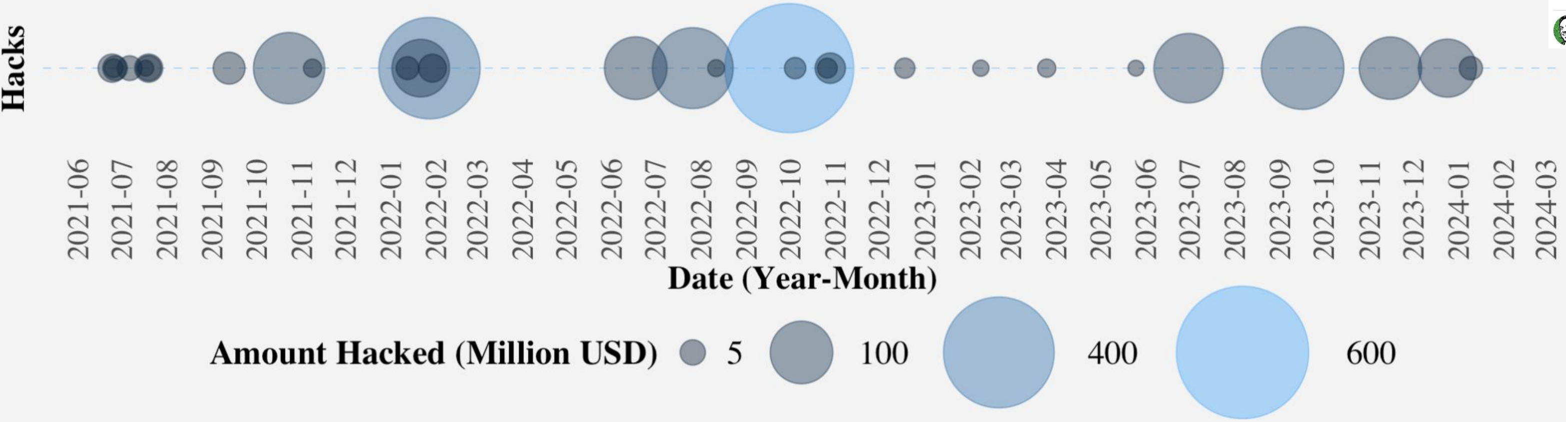
https://www.coindesk.com › business › 2021 › 12 › 05 › crypto-exchange-bitmart-hacked-with-los...

Crypto Exchange BitMart Hacked With Losses Estimated at $196M - ...

May 29-31, 2024 - Austin, Texas The biggest and most established global event for everything crypto, blockchain and Web3. Register Now. The latest **centralized exchange** hack may be among the most ...

Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2021. A Survey on Blockchain Interoperability: Past, Present, and Future Trends. ACM Comput. Surv. 54, 8, Article 168 (November 2022), 41 pages. https://doi.org/10.1145/3471140

Timeline of attacks



EXPLAINED: THE RONIN NETWORK HACK (AUGUST 2024)

ROB BEHNKE
August 8th, 2024

Defi Protocol LI.FI Struck by $11M Exploit

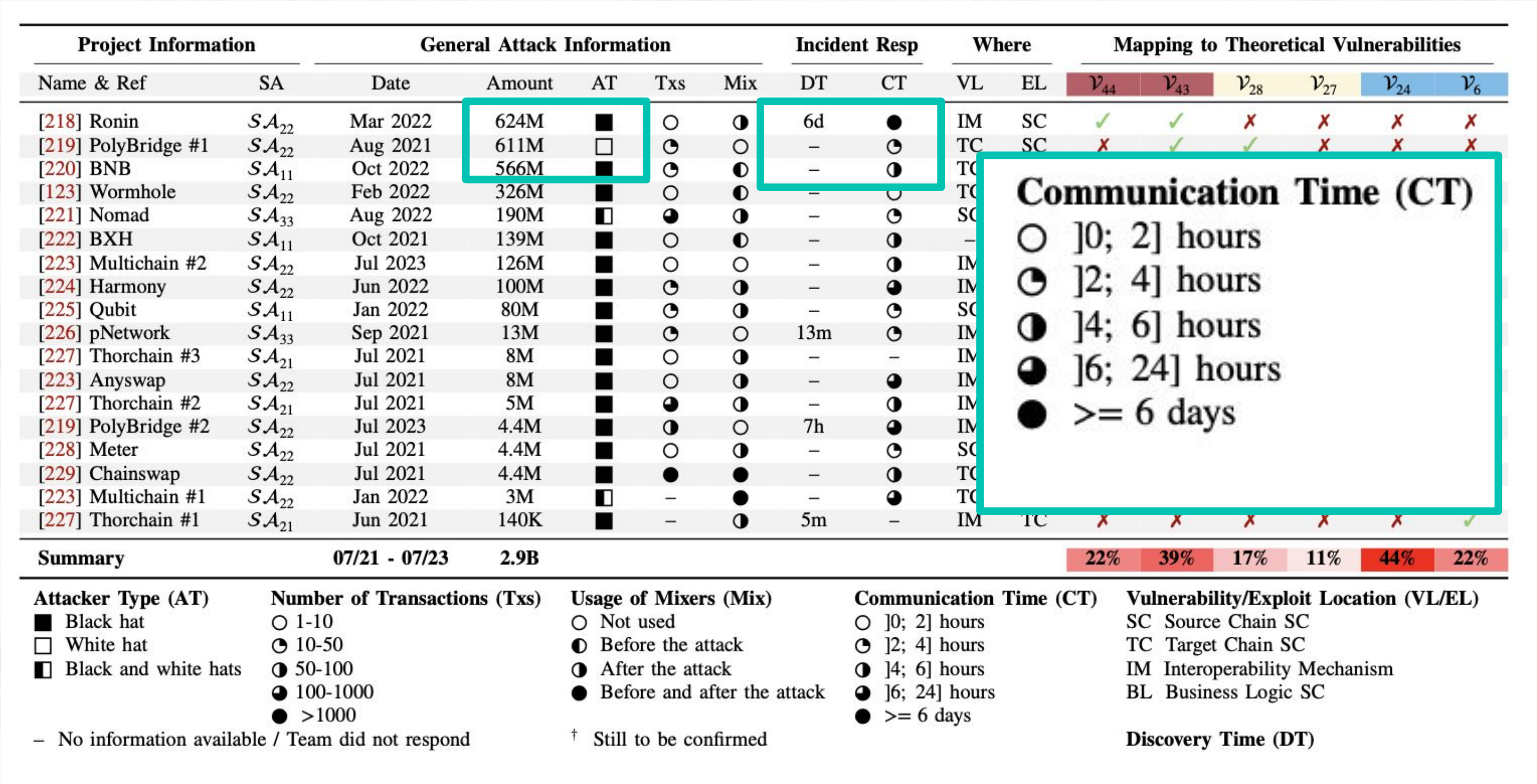
The exploit is reported to be related to the LI.FI bridge.

By Oliver Knight Jul 16, 2024 at 4:30 p.m. Updated Jul 16, 2024 at 10:45 p.m.

... 2024 july, august

These are recurrent,
not just a few isolated events!!!

Augusto, R. Belchior, M. Correia, A. Vasconcelos, L. Zhang and T. Hardjono, "SoK: Security and Privacy of Blockchain Interoperability," 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024, pp. 3840-3865,



Project Information		General Attack Information					Incident Resp		Where		Mapping to Theoretical Vulnerabilities					
Name & Ref	SA	Date	Amount	AT	Txs	Mix	DT	CT	VL	EL	$\mathcal{V}_{44}$	$\mathcal{V}_{43}$	$\mathcal{V}_{28}$	$\mathcal{V}_{27}$	$\mathcal{V}_{24}$	$\mathcal{V}_{6}$
[218] Ronin	$\mathcal{SA}_{22}$	Mar 2022	624M	■	○	◑	6d	●	IM	SC	✓	✓	✗	✗	✗	✗
[219] PolyBridge #1	$\mathcal{SA}_{22}$	Aug 2021	611M	□	◔	○	–	◔	TC	SC	✗	✓	✓	✗	✗	✗
[220] BNB	$\mathcal{SA}_{11}$	Oct 2022	566M	■	◔	◐	–	◑	TC	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[123] Wormhole	$\mathcal{SA}_{22}$	Feb 2022	326M	■	○	◐	–	○	TC	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[221] Nomad	$\mathcal{SA}_{33}$	Aug 2022	190M	◧	◕	◑	–	◔	SC	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[222] BXH	$\mathcal{SA}_{11}$	Oct 2021	139M	■	○	◐	–	◑	–	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[223] Multichain #2	$\mathcal{SA}_{22}$	Jul 2023	126M	■	○	○	–	◑	IM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[224] Harmony	$\mathcal{SA}_{22}$	Jun 2022	100M	■	◔	◑	–	◕	IM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[225] Qubit	$\mathcal{SA}_{11}$	Jan 2022	80M	■	◔	◑	–	◔	SC	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[226] pNetwork	$\mathcal{SA}_{33}$	Sep 2021	13M	■	◔	○	13m	◔	IM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[227] Thorchain #3	$\mathcal{SA}_{21}$	Jul 2021	8M	■	○	◑	–	–	IM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[223] Anyswap	$\mathcal{SA}_{22}$	Jul 2021	8M	■	○	◑	–	◕	IM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[227] Thorchain #2	$\mathcal{SA}_{21}$	Jul 2021	5M	■	◕	◑	–	◑	IM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[219] PolyBridge #2	$\mathcal{SA}_{22}$	Jul 2023	4.4M	■	◑	○	7h	◕	IM	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[228] Meter	$\mathcal{SA}_{22}$	Jul 2021	4.4M	■	○	◑	–	◔	SC	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[229] Chainswap	$\mathcal{SA}_{22}$	Jul 2021	4.4M	■	●	●	–	◑	TC	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[223] Multichain #1	$\mathcal{SA}_{22}$	Jan 2022	3M	◧	–	●	–	◕	TC	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[227] Thorchain #1	$\mathcal{SA}_{21}$	Jun 2021	140K	■	–	◑	5m	–	IM	TC	✗	✗	✗	✗	✗	✓
Summary		**07/21 - 07/23**	**2.9B**								22%	39%	17%	11%	44%	22%

Communication Time (CT)
○]0; 2] hours
◔]2; 4] hours
◑]4; 6] hours
◕]6; 24] hours
● >= 6 days

Attacker Type (AT)
■ Black hat
□ White hat
◧ Black and white hats

Number of Transactions (Txs)
○ 1-10
◔ 10-50
◑ 50-100
◕ 100-1000
● >1000

Usage of Mixers (Mix)
○ Not used
◐ Before the attack
◑ After the attack
● Before and after the attack

Communication Time (CT)
○]0; 2] hours
◔]2; 4] hours
◑]4; 6] hours
◕]6; 24] hours
● >= 6 days

Vulnerability/Exploit Location (VL/EL)
SC Source Chain SC
TC Target Chain SC
IM Interoperability Mechanism
BL Business Logic SC

– No information available / Team did not respond

† Still to be confirmed

Discovery Time (DT)

Augusto, R. Belchior, M. Correia, A. Vasconcelos, L. Zhang and T. Hardjono, "SoK: Security and Privacy of Blockchain Interoperability," 2024 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2024, pp. 3840-3865,

Outline

01 Hypothesis

02 Overview of problem and solution space

03 C1: Systematization

04 C2: Blockchain Gateways (SATP)

05 C3: New Interoperability Security Method

06 Future Work and Conclusions

Outline

01 Hypothesis

02 Overview of problem and solution space

03 C1: Systematization

04 C2: Blockchain Gateways (SATP)

05 C3: New Interoperability Security Method

06 Future Work and Conclusions

Outline

01 Hypothesis

02 Overview of problem and solution space

03 C1: Systematization

04 C2: Blockchain Gateways (SATP)

05 C3: New Interoperability Security Method

06 Future Work and Conclusions

Thesis chapter **2 and 3** :
Do You Need a Distributed Ledger Technology Interoperability Solution?

BUNGEE: Dependable Blockchain Views for Interoperability

Outline

01 Hypothesis

02 Overview of problem and solution space

03 C1: Systematization

04 C2: Blockchain Gateways (SATP)

05 C3: New Interoperability Security Method

06 Future Work and Conclusions

Outline

Thesis chapter **4** : *Hermes: Fault-Tolerant Middleware for Blockchain Interoperability*

01 Hypothesis

02 Overview of problem and solution space

03 C1: Systematization

04 C2: Blockchain Gateways (SATP)

05 C3: New Interoperability Security Method

06 Future Work and Conclusions

Thesis chapter **5 and 6** :
Harmonia: Securing Cross-Chain Applications using ZKP

Hephaestus: Modelling, Analysis, and Performance Evaluation of Cross-Chain Transactions

Outline

01 Hypothesis

02 Overview of problem and solution space

03 C1: Systematization

04 C2: Blockchain Gateways (SATP)

05 C3: New Interoperability Security Method

06 Future Work and Conclusions

Outline

01 Hypothesis

02 Overview of problem and solution space

03 C1: Systematization

04 C2: Blockchain Gateways (SATP)

05 C3: New Interoperability Security Method

06 Future Work and Conclusions

01

Hypothesis

[There can be] Interoperability mechanisms providing interoperability across the technical, semantic, (and organizational) layers can securely implement the requirements of both centralized and decentralized organizations.

Centralized orgs.: have enterprise-grade requirements (privacy - confidentiality, auditability, monitoring and availability). There is an emphasis on **Compliance and interoperability with legacy infrastructure -> Type User Enterprise-Grade**

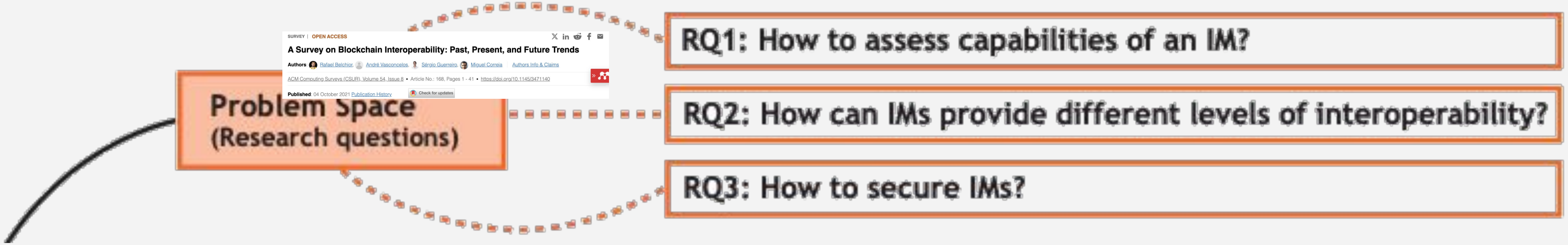
[There can be] Interoperability mechanisms providing interoperability across the technical, semantic, (and organizational) layers can securely implement the requirements of both centralized and decentralized organizations.

Centralized orgs.: have enterprise-grade requirements (privacy - confidentiality, auditability, monitoring and availability). There is an emphasis on **Compliance and interoperability with legacy infrastructure -> Type User Enterprise-Grade**

Decentralized orgs.: focus on the retail investor or Web3 “crypto-native” institutions; **Prioritize more decentralized solutions and privacy-preserving features (anonymity) -> Type User Crypto-Native**

02

Overview of problem and solution space



RQ1: How to assess capabilities of an IM?

RQ2: How can IMs provide different levels of interoperability?

RQ3: How to secure IMs?

SURVEY | OPEN ACCESS

A Survey on Blockchain Interoperability: Past, Present, and Future Trends

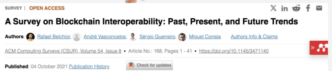
Authors: Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, Miguel Correia | Authors Info & Claims

ACM Computing Surveys (CSUR), Volume 54, Issue 8 • Article No.: 168, Pages 1 - 41 • https://doi.org/10.1145/3471140

Published: 04 October 2021 Publication History

Thesis

Problem Space
(Research questions)



SURVEY | OPEN ACCESS

A Survey on Blockchain Interoperability: Past, Present, and Future Trends

Authors: Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, Miguel Correia | Authors Info & Claims

ACM Computing Surveys (CSUR), Volume 54, Issue 8 • Article No.: 168, Pages 1 - 41 • https://doi.org/10.1145/3471140

Published: 04 October 2021 Publication History

RQ1: How to assess capabilities of an IM?

RQ2: How can IMs provide different levels of interoperability?

RQ3: How to secure IMs?

Solution Space
(Contributions)

Principles and algorithms
(Completed work)

C1

...

C8

BUnGee

HARMONIA

Secure Asset Transfer Protocol (SATP)

Future work
(Roadmap)

SURVEY | OPEN ACCESS

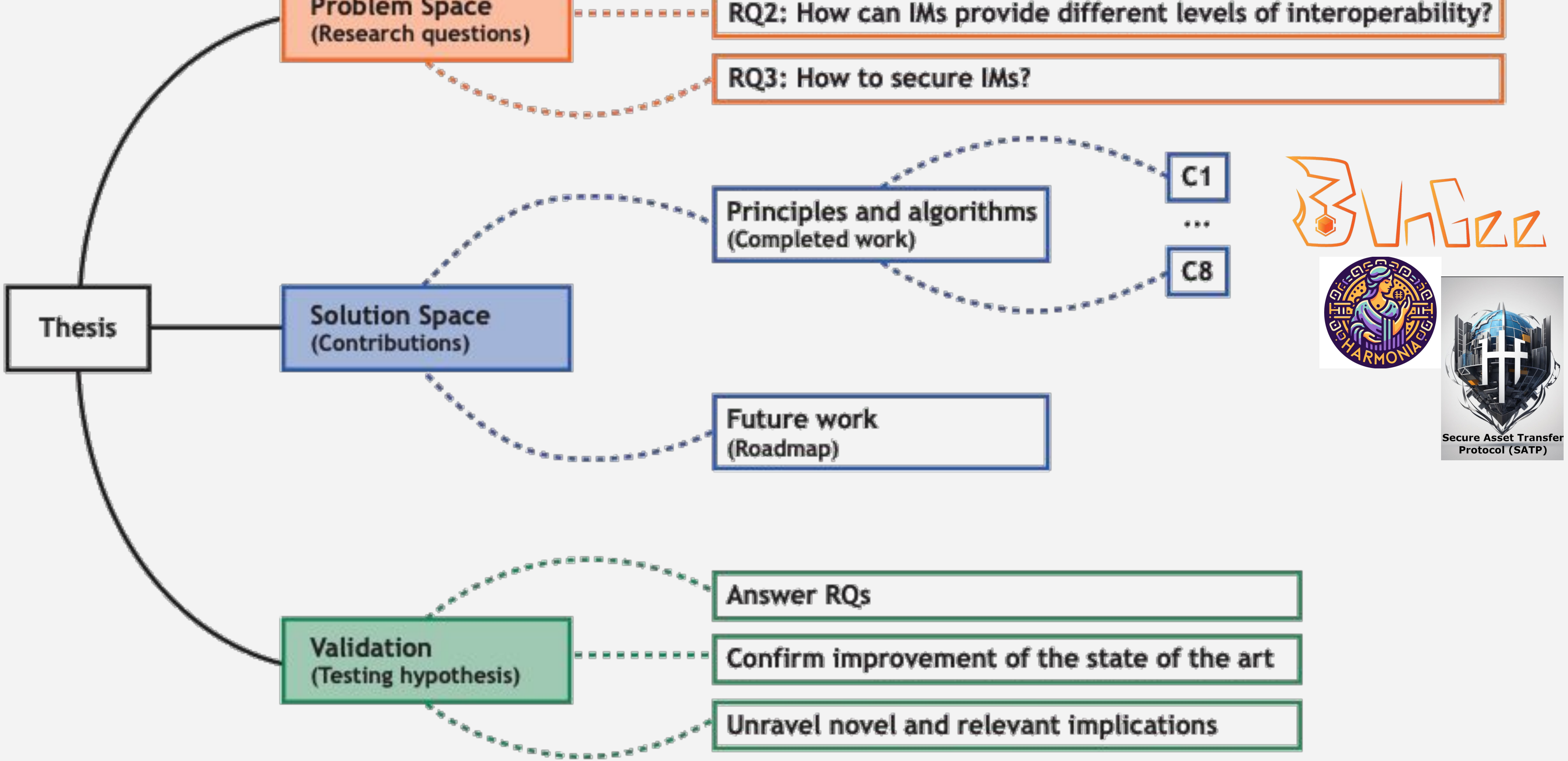
A Survey on Blockchain Interoperability: Past, Present, and Future Trends

Authors: Rafael Belchior, André Vasconcelos, Sérgio Guerreiro, Miguel Correia | Authors Info & Claims

ACM Computing Surveys (CSUR), Volume 54, Issue 8 • Article No.: 168, Pages 1 - 41 • https://doi.org/10.1145/3471140

Published: 04 October 2021 Publication History

RQ1: How to assess capabilities of an IM?



Thesis

Problem Space
(Research questions)

RQ2: How can IMs provide different levels of interoperability?

RQ3: How to secure IMs?

Solution Space
(Contributions)

Principles and algorithms
(Completed work)

C1

...

C8

Future work
(Roadmap)

Secure Asset Transfer Protocol (SATP)

Validation
(Testing hypothesis)

Answer RQs

Confirm improvement of the state of the art

Unravel novel and relevant implications

03

Systematization

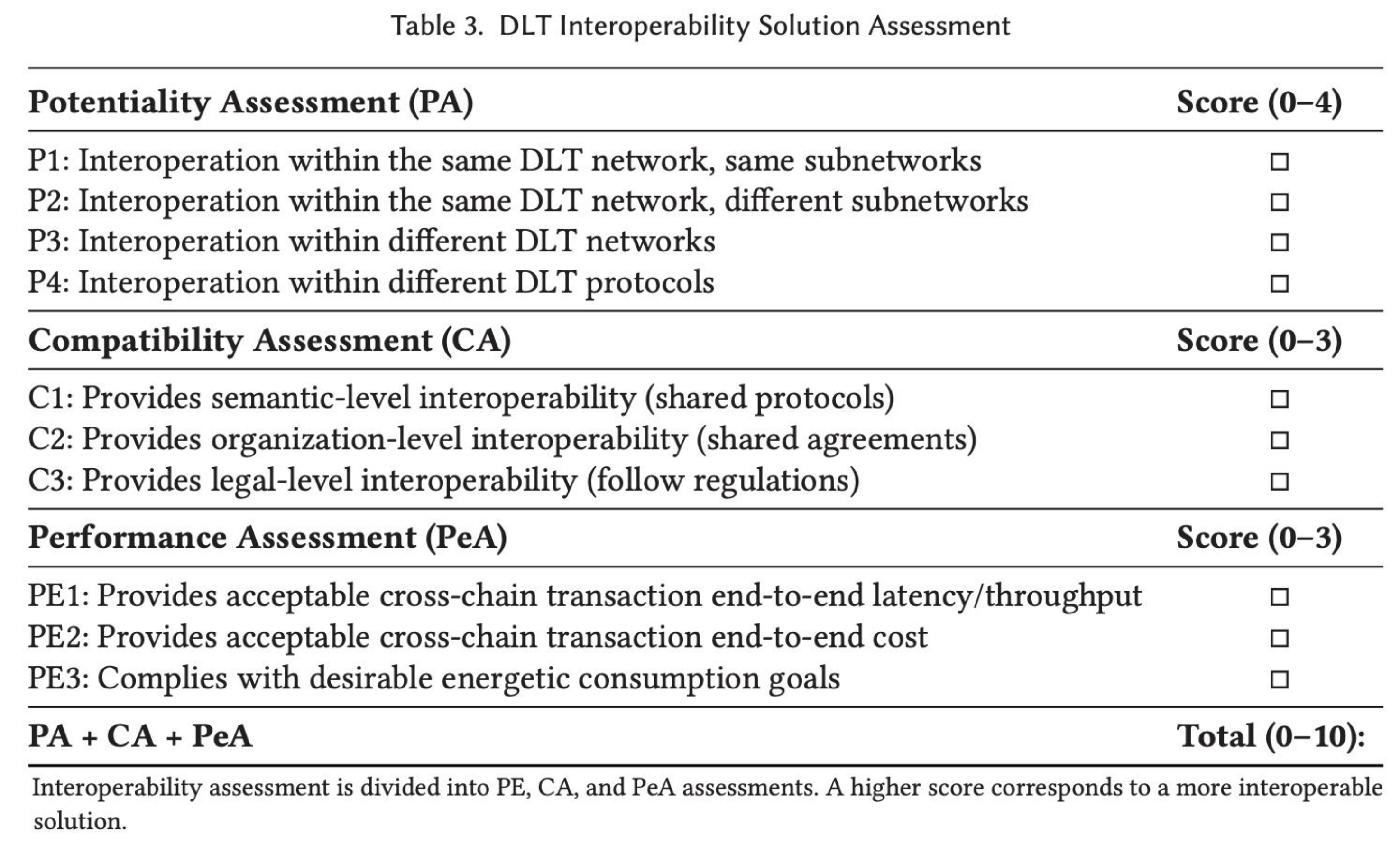


Table 3. DLT Interoperability Solution Assessment

Potentiality Assessment (PA)	**Score (0–4)**
P1: Interoperation within the same DLT network, same subnetworks	□
P2: Interoperation within the same DLT network, different subnetworks	□
P3: Interoperation within different DLT networks	□
P4: Interoperation within different DLT protocols	□
Compatibility Assessment (CA)	**Score (0–3)**
C1: Provides semantic-level interoperability (shared protocols)	□
C2: Provides organization-level interoperability (shared agreements)	□
C3: Provides legal-level interoperability (follow regulations)	□
Performance Assessment (PeA)	**Score (0–3)**
PE1: Provides acceptable cross-chain transaction end-to-end latency/throughput	□
PE2: Provides acceptable cross-chain transaction end-to-end cost	□
PE3: Complies with desirable energetic consumption goals	□
PA + CA + PeA	**Total (0–10):**

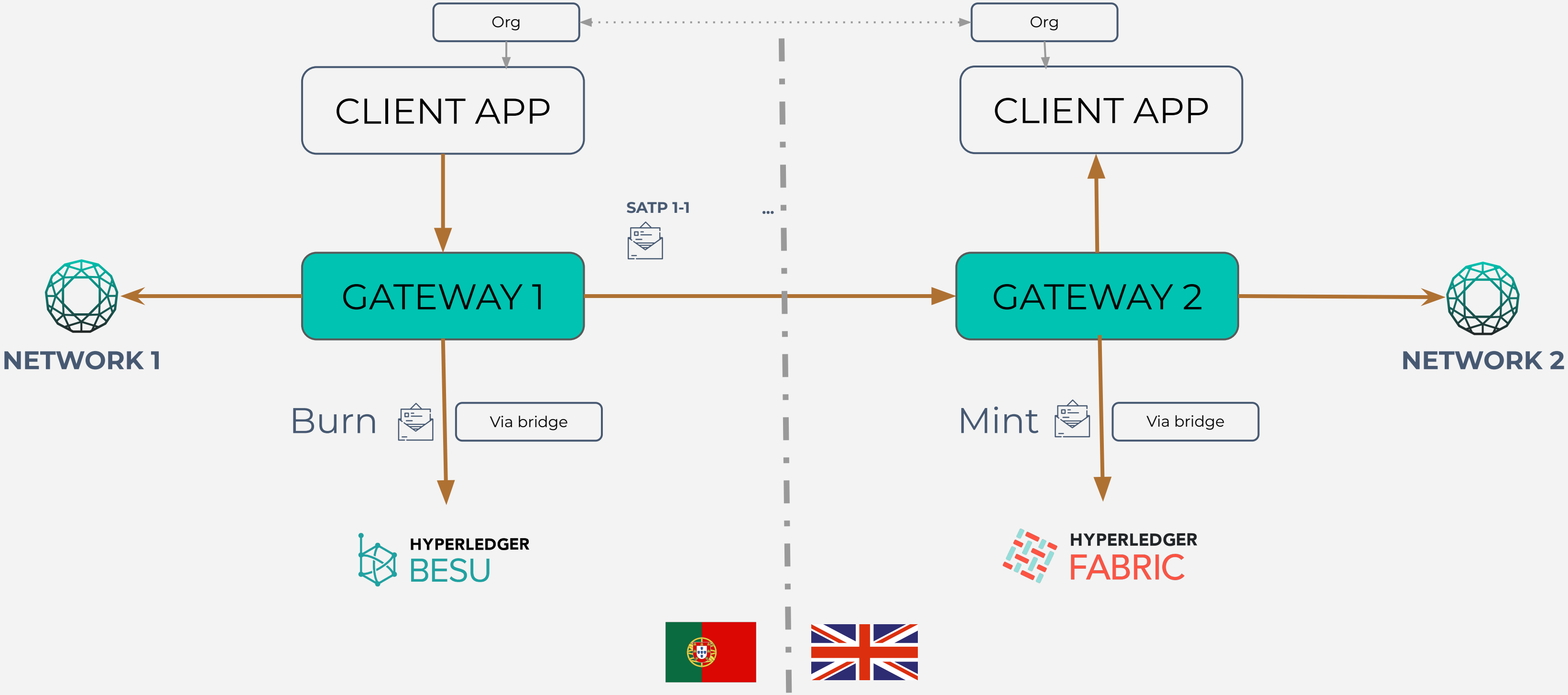
Interoperability assessment is divided into PE, CA, and PeA assessments. A higher score corresponds to a more interoperable solution.

Rafael Belchior, Luke Riley, Thomas Hardjono, André Vasconcelos, and Miguel Correia. 2023. Do You Need a Distributed Ledger Technology Interoperability Solution? Distrib. Ledger Technol. 2, 1, Article 1 (March 2023), 37 pages.

04

Blockchain Gateways (SATP)

SATP Model


Org
Org
CLIENT APP
CLIENT APP
SATP 1-1
...
GATEWAY 1
GATEWAY 2
NETWORK 1
NETWORK 2
Burn
Via bridge
Mint
Via bridge
HYPERLEDGER
BESU
HYPERLEDGER
FABRIC

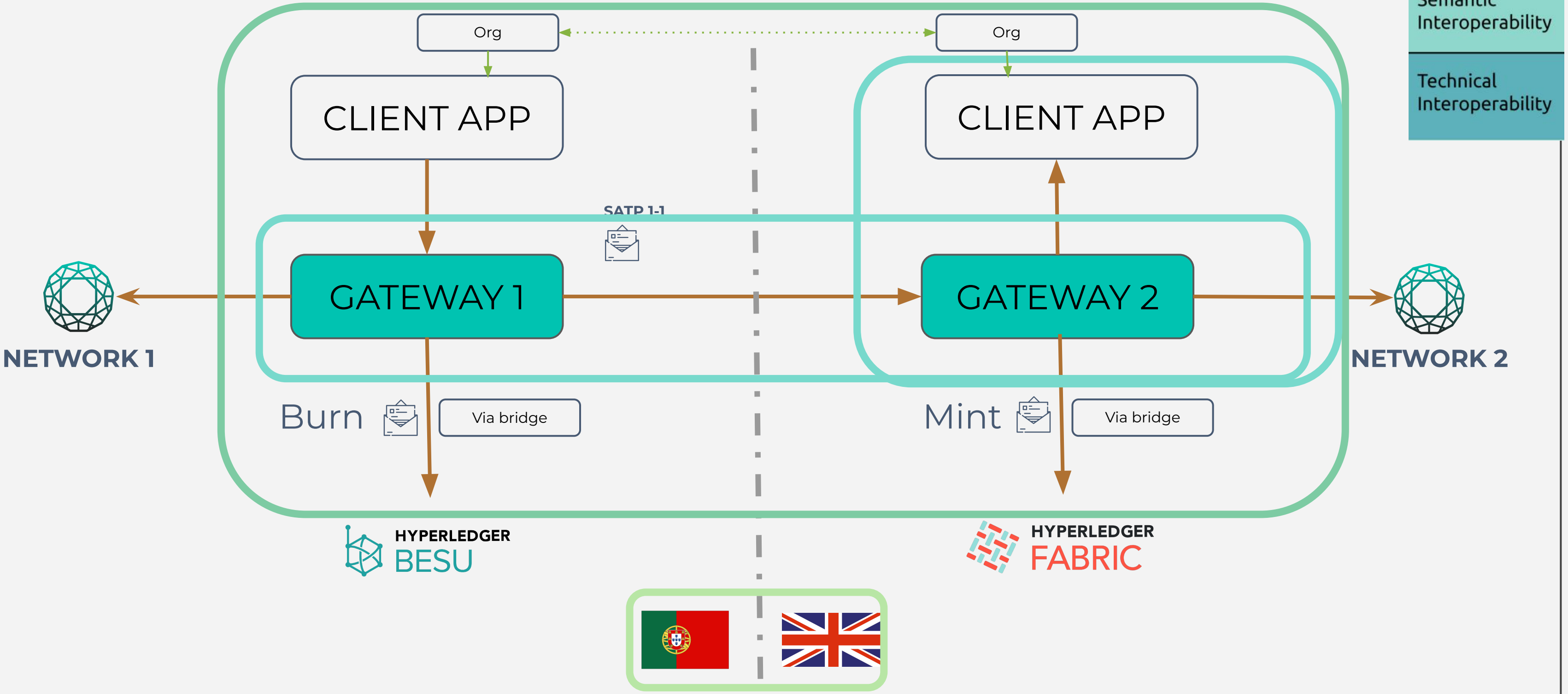
SATP Model

Legal Interoperability

Organizational Interoperability

Semantic Interoperability

Technical Interoperability



Org

Org

CLIENT APP

CLIENT APP

SATP 1-1

GATEWAY 1

GATEWAY 2

NETWORK 1

NETWORK 2

Burn

Via bridge

Mint

Via bridge

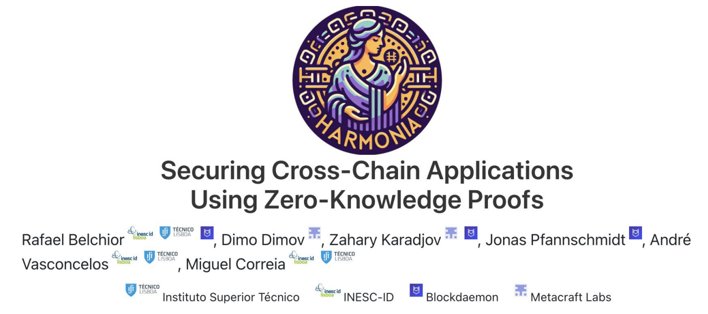
HYPERLEDGER BESU

HYPERLEDGER FABRIC

05

Interoperability Security

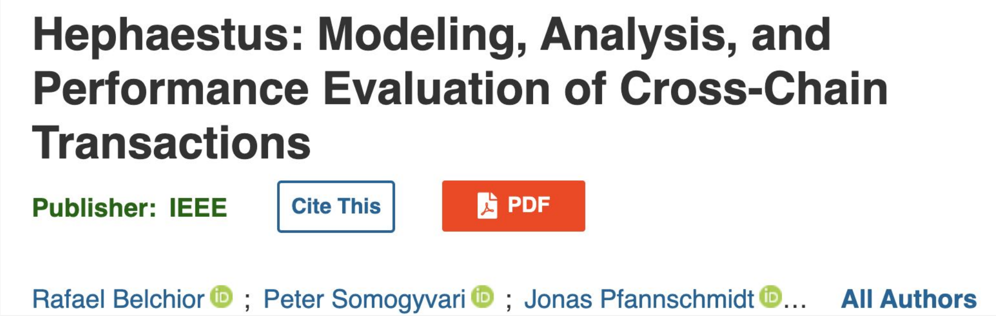
Mitigating the security problem



Securing Cross-Chain Applications Using Zero-Knowledge Proofs

Rafael Belchior, Dimo Dimov, Zahary Karadjov, Jonas Pfannschmidt, André Vasconcelos, Miguel Correia

Instituto Superior Técnico INESC-ID Blockdaemon Metacraft Labs



Hephaestus: Modeling, Analysis, and Performance Evaluation of Cross-Chain Transactions

Publisher: IEEE

Rafael Belchior ; Peter Somogyvari ; Jonas Pfannschmidt... All Authors

Decentralization + Economic inventices

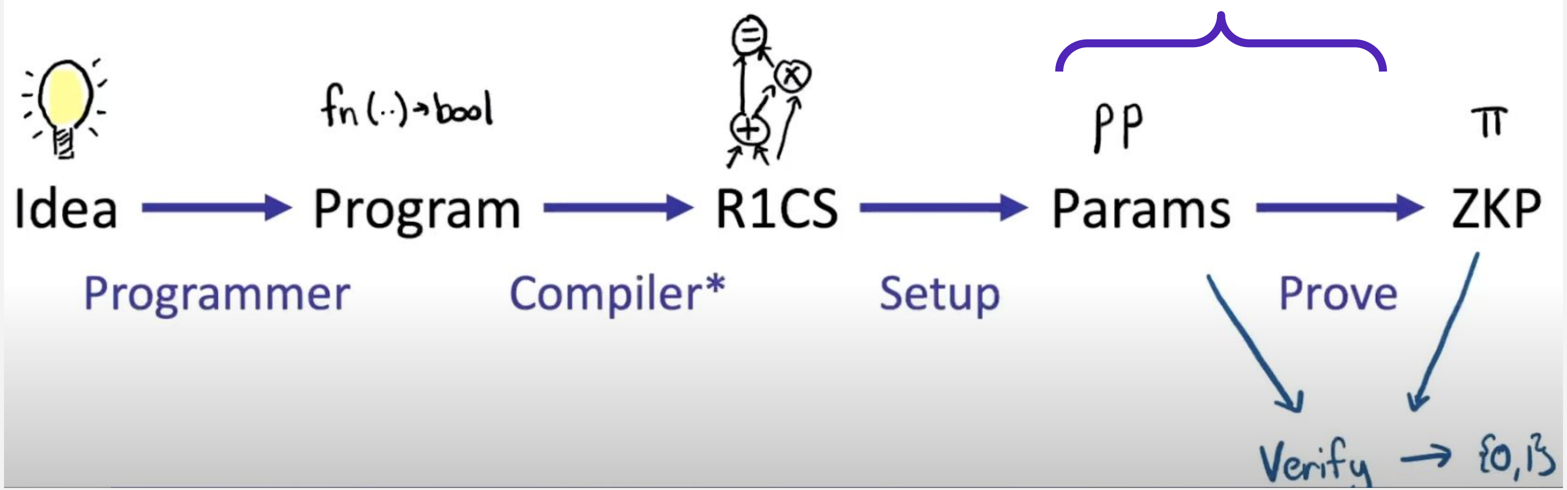
Proactive monitoring + incident response (WIP)

User Crypto-Native

User Crypto-Native or Enterprise-grade

Harmonia

Trusted Setup


Idea → Program → R1CS → Params → ZKP

Programmer

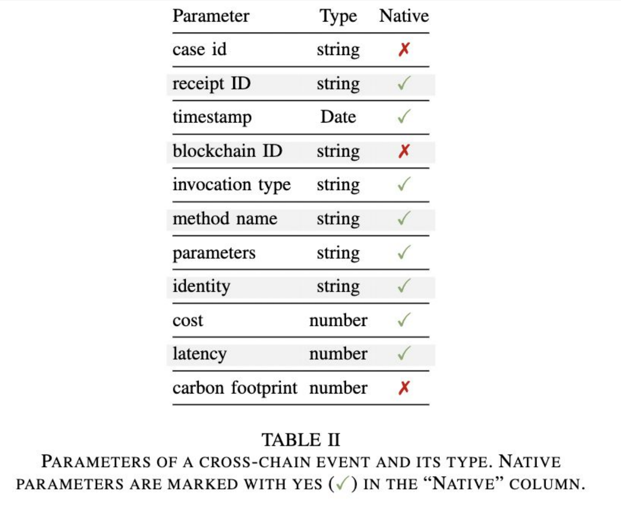
Compiler*

Setup

Prove

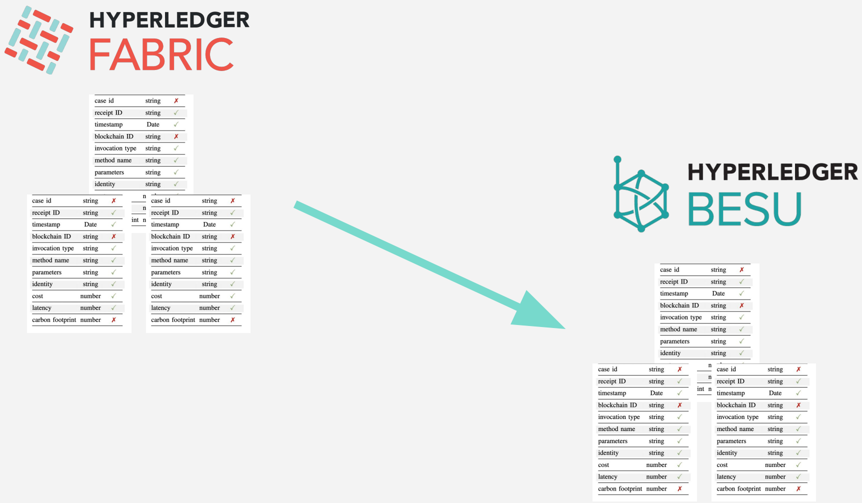
source : https://www.youtube.com/watch?v=UpRSaG6iuks

Proactive monitoring - Hephaestus



Parameter	Type	Native
case id	string	✗
receipt ID	string	✓
timestamp	Date	✓
blockchain ID	string	✗
invocation type	string	✓
method name	string	✓
parameters	string	✓
identity	string	✓
cost	number	✓
latency	number	✓
carbon footprint	number	✗

TABLE II
PARAMETERS OF A CROSS-CHAIN EVENT AND ITS TYPE. NATIVE PARAMETERS ARE MARKED WITH YES (✓) IN THE "NATIVE" COLUMN.

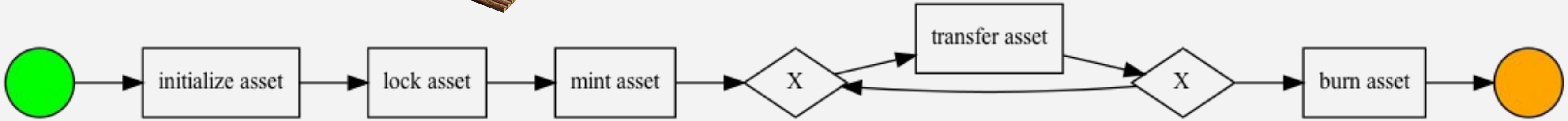


PART 3 = series of cc rules

Key Idea

HYPERLEDGER FABRIC

HYPERLEDGER BESU



initialize asset

lock asset

mint asset

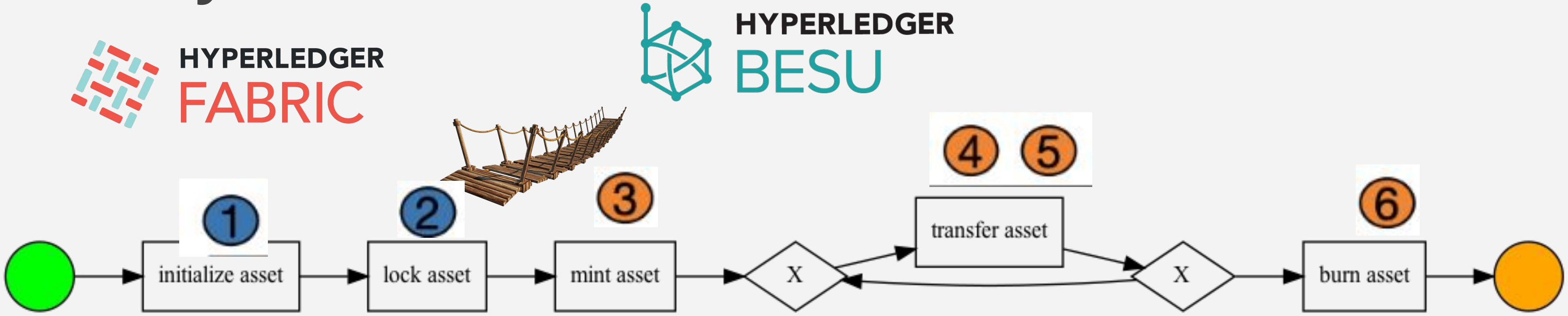
X

transfer asset

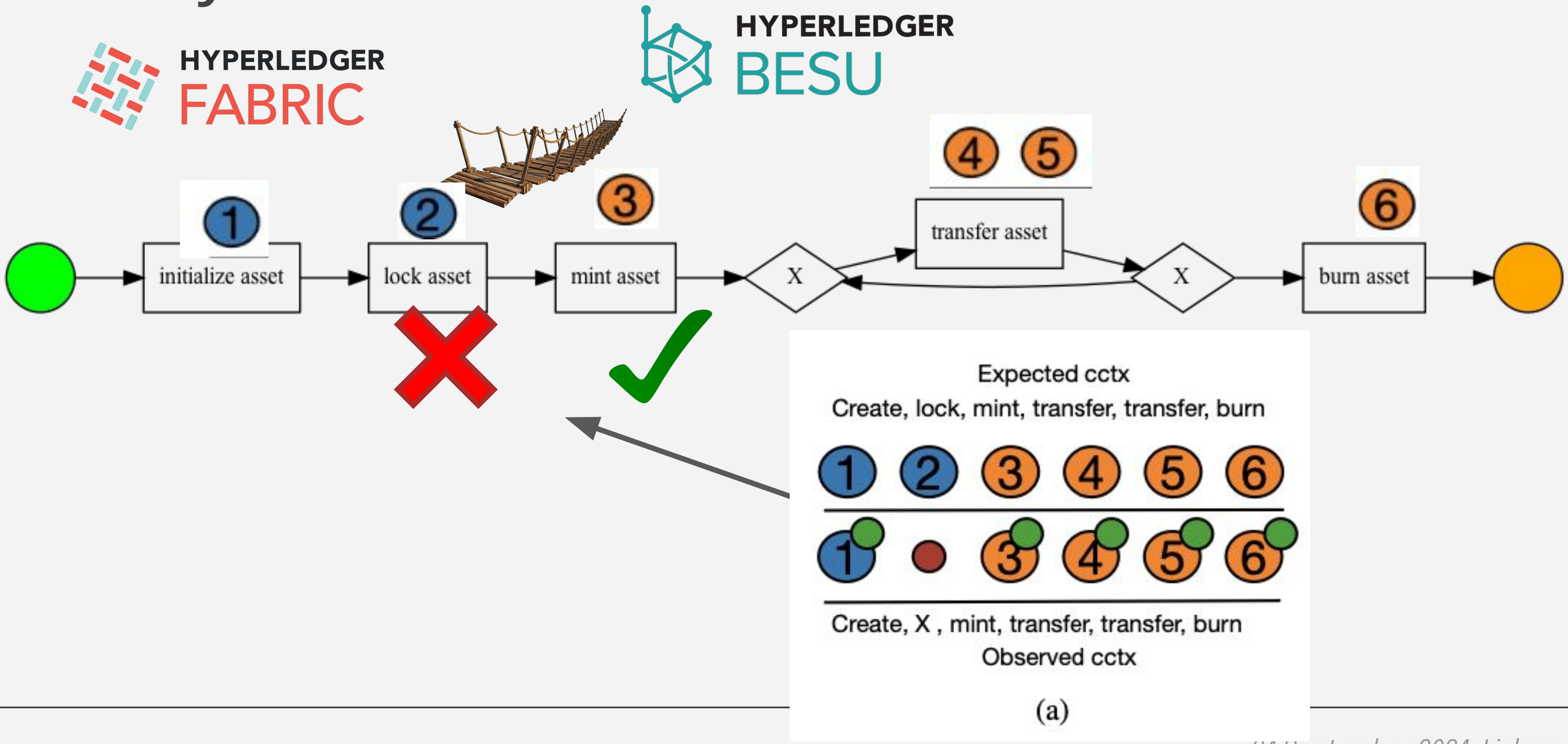
X

burn asset

Key Idea


HYPERLEDGER
FABRIC
HYPERLEDGER
BESU
1
initialize asset
2
lock asset
3
mint asset
X
4
5
transfer asset
X
6
burn asset

Key Idea



Expected cctx
Create, lock, mint, transfer, transfer, burn

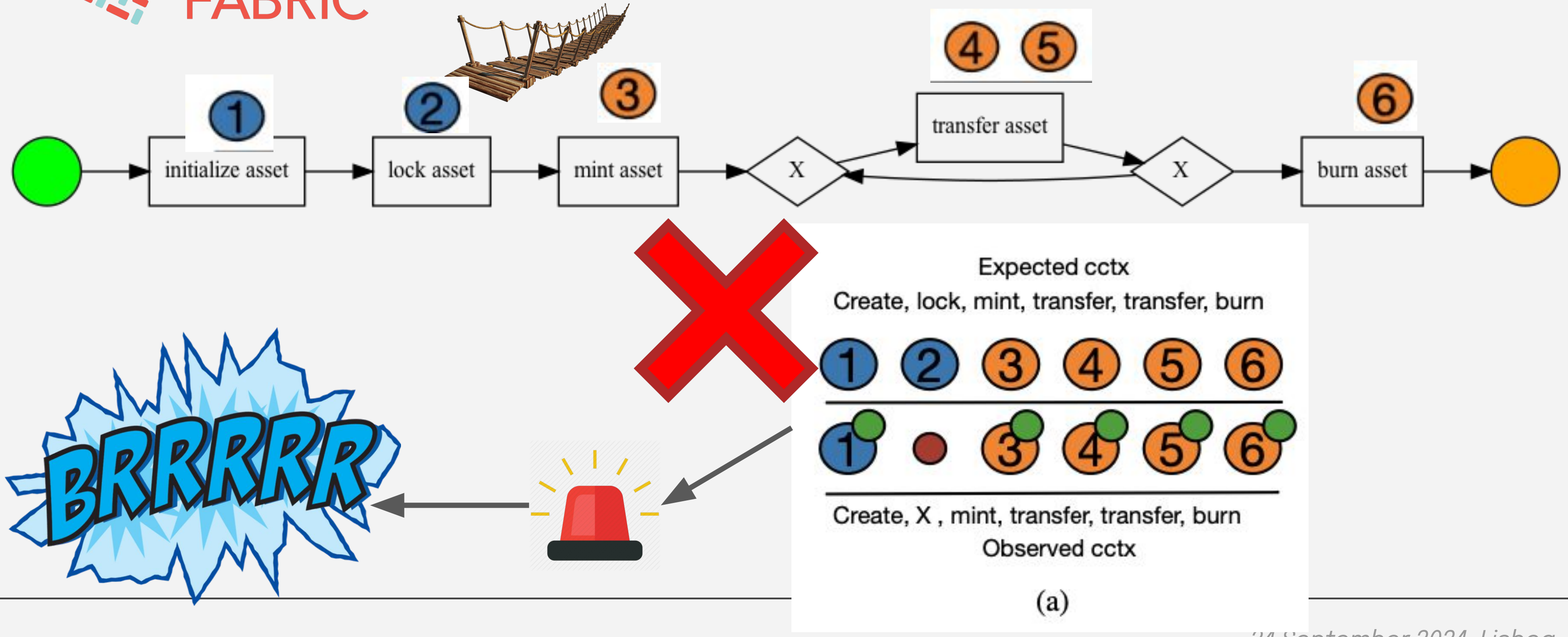
Create, X , mint, transfer, transfer, burn
Observed cctx

(a)

Key Idea

HYPERLEDGER FABRIC

HYPERLEDGER BESU



Future Work

SoK: Security and Privacy of Blockchain Interoperability

André Augusto (INESC-ID, Instituto Superior Técnico)
Rafael Belchior (INESC-ID, Instituto Superior Técnico)
André Vasconcelos (INESC-ID, Instituto Superior Técnico)
Miguel Correia (INESC-ID, Instituto Superior Técnico)
Luyao Zhang (Duke Kunshan University)
Thomas Hardjono (MIT Connection Science)

The paper in tables

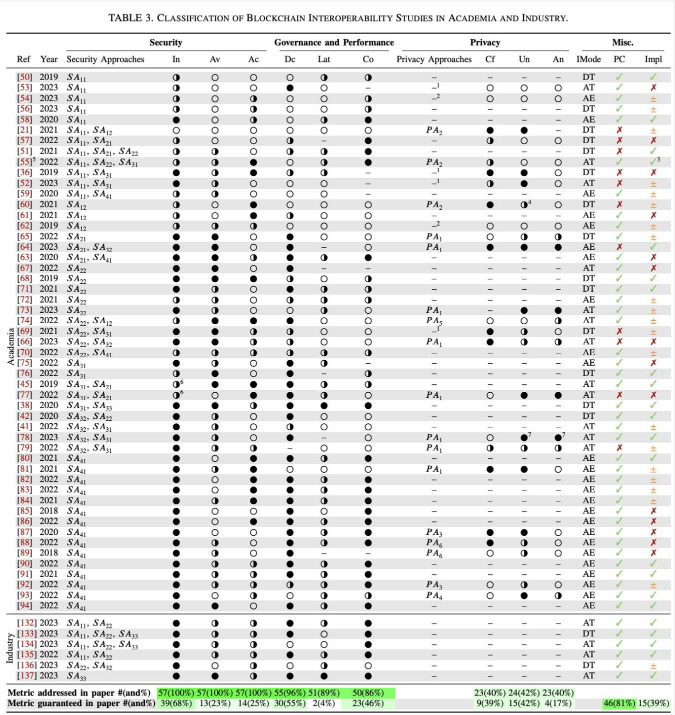
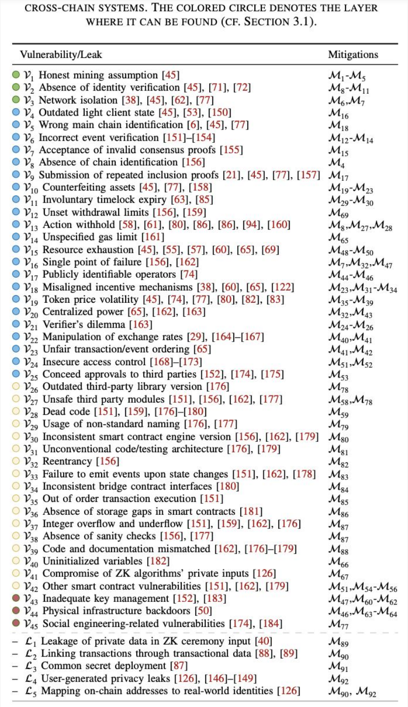


TABLE 3. Classification of Blockchain Interoperability Studies in Academia and Industry.

			Security				Governance and Performance			Privacy				Misc.		
	Ref	Year	Security Approaches	In	Av	Ac	Dc	Lat	Co	Privacy Approaches	Cf	Un	An	IMode	PC	Impl
Academia	[50]	2019	SA_{11}	◑	○	○	○	◑	◑	–	–	–	–	DT	✓	✓
	[53]	2023	SA_{11}	◑	○	○	●	○	–	–[1]	○	○	○	AT	✓	✗
	[54]	2023	SA_{11}	◑	○	◑	○	○	◑	–[2]	○	○	○	AE	✓	±
	[56]	2023	SA_{11}	◑	○	◑	○	○	◑	–	–	–	–	DT	✓	±
	[58]	2020	SA_{11}	●	○	◑	○	◑	●	–	–	–	–	AE	✓	✓
	[21]	2021	SA_{11}, SA_{12}	○	○	○	○	○	○	PA_2	●	●	–	DT	✗	±
	[57]	2022	SA_{11}, SA_{21}	◑	○	○	◑	–	●	–	◑	○	○	DT	✗	✗
	[51]	2021	SA_{11}, SA_{21}, SA_{22}	◑	◑	○	◑	◑	●	–	–	–	–	DT	✗	✓
	[55][5]	2022	SA_{11}, SA_{22}, SA_{31}	◑	◑	●	○	◑	●	PA_2	◑	○	○	AT	✓	✓[3]
	[36]	2019	SA_{11}, SA_{31}	●	◑	●	◑	◑	–	–[1]	●	●	○	DT	✗	✗
	[52]	2023	SA_{11}, SA_{31}	●	◑	○	○	○	–	–[1]	◑	●	○	AT	✗	±
	[59]	2020	SA_{11}, SA_{41}	◑	◑	○	○	○	–	–	–	–	–	AE	✓	±
	[60]	2021	SA_{12}	◑	○	●	○	○	○	PA_2	●	◑[4]	○	DT	✗	±
	[61]	2021	SA_{12}	◑	○	●	◑	○	○	–	–	–	–	AE	✓	✗
	[62]	2019	SA_{12}	◑	◑	◑	○	○	○	–[2]	○	○	○	AE	✓	±
	[65]	2022	SA_{21}	●	●	○	●	○	○	PA_1	○	◑	◑	DT	✓	±
	[64]	2023	SA_{21}, SA_{32}	●	●	○	●	–	○	PA_1	●	●	●	AE	✗	✓
	[63]	2020	SA_{21}, SA_{41}	●	●	◑	●	◑	●	–	–	–	–	AE	✓	✗
	[67]	2022	SA_{22}	●	●	○	●	–	–	–	–	–	–	AT	✓	✗
	[68]	2019	SA_{22}	●	●	●	◑	○	◑	–	–	–	–	DT	✓	✓
	[71]	2021	SA_{22}	●	◑	○	●	◑	◑	–	–	–	–	DT	✓	✓
	[72]	2021	SA_{22}	◑	◑	○	◑	◑	◑	–	–	–	–	AE	✓	±
	[73]	2023	SA_{22}	●	◑	○	○	◑	○	PA_1	–	●	●	AT	✓	±
	[74]	2022	SA_{22}, SA_{12}	◑	●	●	●	○	○	PA_5	○	○	◑	AT	✓	±
	[69]	2021	SA_{22}, SA_{31}	●	●	◑	◑	○	○	–[1]	●	◑	○	DT	✗	±
	[66]	2023	SA_{22}, SA_{32}	●	●	◑	◑	○	○	PA_1	●	◑	◑	AT	✗	✗
	[70]	2022	SA_{22}, SA_{41}	◑	◑	◑	◑	◑	◑	–	–	–	–	AE	✓	±
	[75]	2022	SA_{31}	●	◑	○	●	◑	–	–	–	–	–	AE	✓	✗
	[76]	2022	SA_{31}	◑	●	○	●	–	◑	–	–	–	–	DT	✓	✓
	[45]	2019	SA_{31}, SA_{21}	◑[6]	●	●	●	◑	◑	–	–	–	–	AT	✓	✓
	[77]	2022	SA_{31}, SA_{21}	◑[6]	○	●	●	◑	○	PA_1	○	●	●	AT	✗	✗
	[38]	2020	SA_{31}, SA_{33}	●	●	◑	●	●	●	–	–	–	–	DT	✓	✓
	[42]	2020	SA_{32}, SA_{22}	●	◑	○	●	○	○	–	–	–	–	DT	✓	✓
	[41]	2022	SA_{32}, SA_{31}	●	◑	○	◑	○	○	–	–	–	–	AT	✓	±
	[78]	2023	SA_{32}, SA_{31}	●	◑	○	●	–	○	PA_1	○	●[7]	●[7]	AT	✓	✓
	[79]	2022	SA_{32}, SA_{31}	●	◑	◑	–	○	○	PA_1	◑	◑	◑	AT	✗	±
	[80]	2021	SA_{41}	●	○	●	●	◑	●	–	–	–	–	AE	✓	✓
	[81]	2021	SA_{41}	●	◑	●	○	○	○	PA_1	●	●	○	AE	✓	±
	[82]	2022	SA_{41}	●	○	●	●	◑	●	–	–	–	–	AE	✓	±
	[83]	2022	SA_{41}	●	○	●	●	◑	●	–	–	–	–	AE	✓	±
	[84]	2021	SA_{41}	●	◑	●	●	◑	●	–	–	–	–	AE	✓	±
	[85]	2018	SA_{41}	●	○	○	●	○	●	–	–	–	–	AE	✓	✗
	[86]	2022	SA_{41}	●	○	●	●	◑	●	–	–	–	–	AE	✓	✗
	[87]	2020	SA_{41}	●	○	○	●	◑	●	PA_3	●	●	○	AE	✓	✗
	[88]	2022	SA_{41}	●	◑	○	●	◑	●	PA_6	●	◑	○	AE	✓	✗
	[89]	2018	SA_{41}	●	◑	○	●	–	–	PA_6	○	◑	○	AE	✓	✗
	[90]	2022	SA_{41}	●	◑	◑	●	◑	●	–	–	–	–	AE	✓	✓
	[91]	2021	SA_{41}	●	◑	◑	●	◑	●	–	–	–	–	AE	✓	✓
	[92]	2022	SA_{41}	●	◑	◑	◑	◑	●	PA_3	○	◑	○	AE	✓	±
	[93]	2022	SA_{41}	●	○	◑	○	◑	◑	PA_4	○	●	◑	AE	✓	✓
	[94]	2022	SA_{41}	●	●	○	●	◑	●	–	–	–	–	AE	✓	✓
Industry	[132]	2023	SA_{11}, SA_{22}	●	◑	◑	●	◑	●	–	–	–	–	AT	✓	✓
	[133]	2023	SA_{11}, SA_{22}, SA_{33}	●	◑	◑	●	○	●	–	–	–	–	DT	✓	✓
	[134]	2023	SA_{11}, SA_{22}, SA_{33}	●	◑	◑	○	○	●	–	–	–	–	AT	✓	✓
	[135]	2022	SA_{11}, SA_{22}	●	◑	◑	●	◑	●	–	–	–	–	AT	✓	✓
	[136]	2023	SA_{22}, SA_{32}	●	○	◑	○	◑	○	–	–	–	–	DT	✓	±
	[137]	2023	SA_{33}	●	●	◑	●	●	●	–	–	–	–	AT	✓	✓
Metric addressed in paper #(and%)				57(100%)	57(100%)	57(100%)	55(96%)	51(89%)	50(86%)		23(40%)	24(42%)	23(40%)			
Metric guaranteed in paper #(and%)				39(68%)	13(23%)	14(25%)	30(55%)	2(4%)	23(46%)		9(39%)	15(42%)	4(17%)		46(81%)	15(39%)



cross-chain systems. The colored circle denotes the layer where it can be found (cf. Section 3.1).

Vulnerability/Leak	Mitigations
🟢 $\mathcal{V}_1$ Honest mining assumption [45]	$\mathcal{M}_1$-$\mathcal{M}_5$
🟢 $\mathcal{V}_2$ Absence of identity verification [45], [71], [72]	$\mathcal{M}_8$-$\mathcal{M}_{11}$
🟢 $\mathcal{V}_3$ Network isolation [38], [45], [62], [77]	$\mathcal{M}_6$,$\mathcal{M}_7$
🔵 $\mathcal{V}_4$ Outdated light client state [45], [53], [150]	$\mathcal{M}_{16}$
🔵 $\mathcal{V}_5$ Wrong main chain identification [6], [45], [77]	$\mathcal{M}_{18}$
🔵 $\mathcal{V}_6$ Incorrect event verification [151]–[154]	$\mathcal{M}_{12}$-$\mathcal{M}_{14}$
🔵 $\mathcal{V}_7$ Acceptance of invalid consensus proofs [155]	$\mathcal{M}_{15}$
🔵 $\mathcal{V}_8$ Absence of chain identification [156]	$\mathcal{M}_4$
🔵 $\mathcal{V}_9$ Submission of repeated inclusion proofs [21], [45], [77], [157]	$\mathcal{M}_{17}$
🔵 $\mathcal{V}_{10}$ Counterfeiting assets [45], [77], [158]	$\mathcal{M}_{19}$-$\mathcal{M}_{23}$
🔵 $\mathcal{V}_{11}$ Involuntary timelock expiry [63], [85]	$\mathcal{M}_{29}$-$\mathcal{M}_{30}$
🔵 $\mathcal{V}_{12}$ Unset withdrawal limits [156], [159]	$\mathcal{M}_{69}$
🔵 $\mathcal{V}_{13}$ Action withhold [58], [61], [80], [86], [86], [94], [160]	$\mathcal{M}_8$,$\mathcal{M}_{27}$,$\mathcal{M}_{28}$
🔵 $\mathcal{V}_{14}$ Unspecified gas limit [161]	$\mathcal{M}_{65}$
🔵 $\mathcal{V}_{15}$ Resource exhaustion [45], [55], [57], [60], [65], [69]	$\mathcal{M}_{48}$-$\mathcal{M}_{50}$
🔵 $\mathcal{V}_{16}$ Single point of failure [156], [162]	$\mathcal{M}_7$,$\mathcal{M}_{32}$,$\mathcal{M}_{47}$
🔵 $\mathcal{V}_{17}$ Publicly identifiable operators [74]	$\mathcal{M}_{44}$-$\mathcal{M}_{46}$
🔵 $\mathcal{V}_{18}$ Misaligned incentive mechanisms [38], [60], [65], [122]	$\mathcal{M}_{23}$,$\mathcal{M}_{31}$-$\mathcal{M}_{34}$
🔵 $\mathcal{V}_{19}$ Token price volatility [45], [74], [77], [80], [82], [83]	$\mathcal{M}_{35}$-$\mathcal{M}_{39}$
🔵 $\mathcal{V}_{20}$ Centralized power [65], [162], [163]	$\mathcal{M}_{32}$,$\mathcal{M}_{43}$
🔵 $\mathcal{V}_{21}$ Verifier's dilemma [163]	$\mathcal{M}_{24}$-$\mathcal{M}_{26}$
🔵 $\mathcal{V}_{22}$ Manipulation of exchange rates [29], [164]–[167]	$\mathcal{M}_{40}$,$\mathcal{M}_{41}$
🔵 $\mathcal{V}_{23}$ Unfair transaction/event ordering [65]	$\mathcal{M}_{41}$,$\mathcal{M}_{42}$
🔵 $\mathcal{V}_{24}$ Insecure access control [168]–[173]	$\mathcal{M}_{51}$,$\mathcal{M}_{52}$
🔵 $\mathcal{V}_{25}$ Conceed approvals to third parties [152], [174], [175]	$\mathcal{M}_{53}$
○ $\mathcal{V}_{26}$ Outdated third-party library version [176]	$\mathcal{M}_{78}$
○ $\mathcal{V}_{27}$ Unsafe third party modules [151], [156], [162], [177]	$\mathcal{M}_{58}$,$\mathcal{M}_{78}$
○ $\mathcal{V}_{28}$ Dead code [151], [159], [176]–[180]	$\mathcal{M}_{59}$
○ $\mathcal{V}_{29}$ Usage of non-standard naming [176], [177]	$\mathcal{M}_{79}$
○ $\mathcal{V}_{30}$ Inconsistent smart contract engine version [156], [162], [179]	$\mathcal{M}_{80}$
○ $\mathcal{V}_{31}$ Unconventional code/testing architecture [176], [179]	$\mathcal{M}_{81}$
○ $\mathcal{V}_{32}$ Reentrancy [156]	$\mathcal{M}_{82}$
○ $\mathcal{V}_{33}$ Failure to emit events upon state changes [151], [162], [178]	$\mathcal{M}_{83}$
○ $\mathcal{V}_{34}$ Inconsistent bridge contract interfaces [180]	$\mathcal{M}_{84}$
○ $\mathcal{V}_{35}$ Out of order transaction execution [151]	$\mathcal{M}_{85}$
○ $\mathcal{V}_{36}$ Absence of storage gaps in smart contracts [181]	$\mathcal{M}_{86}$
○ $\mathcal{V}_{37}$ Integer overflow and underflow [151], [159], [162], [176]	$\mathcal{M}_{87}$
○ $\mathcal{V}_{38}$ Absence of sanity checks [156], [177]	$\mathcal{M}_{87}$
○ $\mathcal{V}_{39}$ Code and documentation mismatched [162], [176]–[179]	$\mathcal{M}_{88}$
○ $\mathcal{V}_{40}$ Uninitialized variables [182]	$\mathcal{M}_{66}$
○ $\mathcal{V}_{41}$ Compromise of ZK algorithms' private inputs [126]	$\mathcal{M}_{67}$
○ $\mathcal{V}_{42}$ Other smart contract vulnerabilities [151], [162], [179]	$\mathcal{M}_{51}$,$\mathcal{M}_{54}$-$\mathcal{M}_{56}$
🟤 $\mathcal{V}_{43}$ Inadequate key management [152], [183]	$\mathcal{M}_{47}$,$\mathcal{M}_{60}$-$\mathcal{M}_{62}$
🟤 $\mathcal{V}_{44}$ Physical infrastructure backdoors [50]	$\mathcal{M}_{46}$,$\mathcal{M}_{63}$-$\mathcal{M}_{64}$
🟤 $\mathcal{V}_{45}$ Social engineering-related vulnerabilities [174], [184]	$\mathcal{M}_{77}$
– $\mathcal{L}_1$ Leakage of private data in ZK ceremony input [40]	$\mathcal{M}_{89}$
– $\mathcal{L}_2$ Linking transactions through transactional data [88], [89]	$\mathcal{M}_{90}$
– $\mathcal{L}_3$ Common secret deployment [87]	$\mathcal{M}_{91}$
– $\mathcal{L}_4$ User-generated privacy leaks [126], [146]–[149]	$\mathcal{M}_{92}$
– $\mathcal{L}_5$ Mapping on-chain addresses to real-world identities [126]	$\mathcal{M}_{90}$, $\mathcal{M}_{92}$

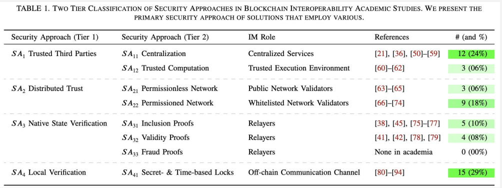


TABLE 1. Two Tier Classification of Security Approaches in Blockchain Interoperability Academic Studies. We present the primary security approach of solutions that employ various.

Security Approach (Tier 1)	Security Approach (Tier 2)	IM Role	References	# (and %)
SA_1 Trusted Third Parties	SA_{11} Centralization	Centralized Services	[21], [36], [50]–[59]	12 (24%)
	SA_{12} Trusted Computation	Trusted Execution Environment	[60]–[62]	3 (06%)
SA_2 Distributed Trust	SA_{21} Permissionless Network	Public Network Validators	[63]–[65]	3 (06%)
	SA_{22} Permissioned Network	Whitelisted Network Validators	[66]–[74]	9 (18%)
SA_3 Native State Verification	SA_{31} Inclusion Proofs	Relayers	[38], [45], [75]–[77]	5 (10%)
	SA_{32} Validity Proofs	Relayers	[41], [42], [78], [79]	4 (08%)
	SA_{33} Fraud Proofs	Relayers	None in academia	0 (00%)
SA_4 Local Verification	SA_{41} Secret- & Time-based Locks	Off-chain Communication Channel	[80]–[94]	15 (29%)

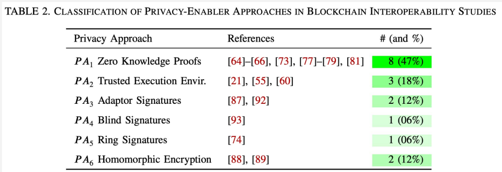
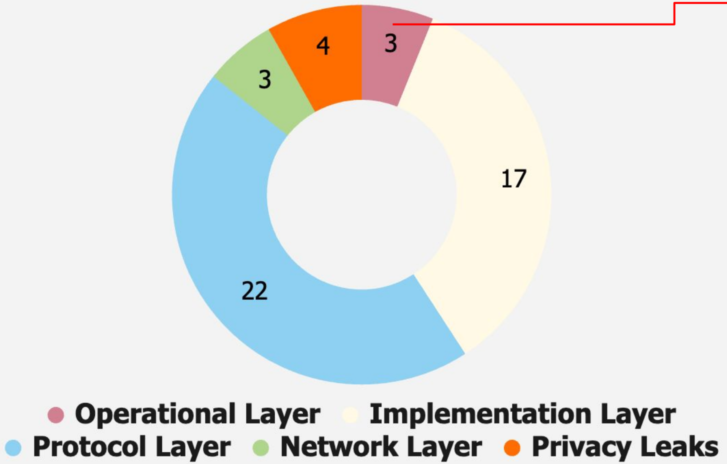


TABLE 2. Classification of Privacy-Enabler Approaches in Blockchain Interoperability Studies

Privacy Approach	References	# (and %)
PA_1 Zero Knowledge Proofs	[64]–[66], [73], [77]–[79], [81]	8 (47%)
PA_2 Trusted Execution Envir.	[21], [55], [60]	3 (18%)
PA_3 Adaptor Signatures	[87], [92]	2 (12%)
PA_4 Blind Signatures	[93]	1 (06%)
PA_5 Ring Signatures	[74]	1 (06%)
PA_6 Homomorphic Encryption	[88], [89]	2 (12%)

Vulnerabilities Found



contrasts with cross-chain hacks!!

Industry and Academia diverge in this topic

We map each vulnerability to a set of mitigations

XChainWatcher : Monitoring and Identifying Attacks in Cross-Chain Bridges

André Augusto (INESC-ID, Instituto Superior Técnico)
Rafael Belchior (INESC-ID, Instituto Superior Técnico)
André Vasconcelos (INESC-ID, Instituto Superior Técnico)
Miguel Correia (INESC-ID, Instituto Superior Técnico)

24 September 2024, Lisboa

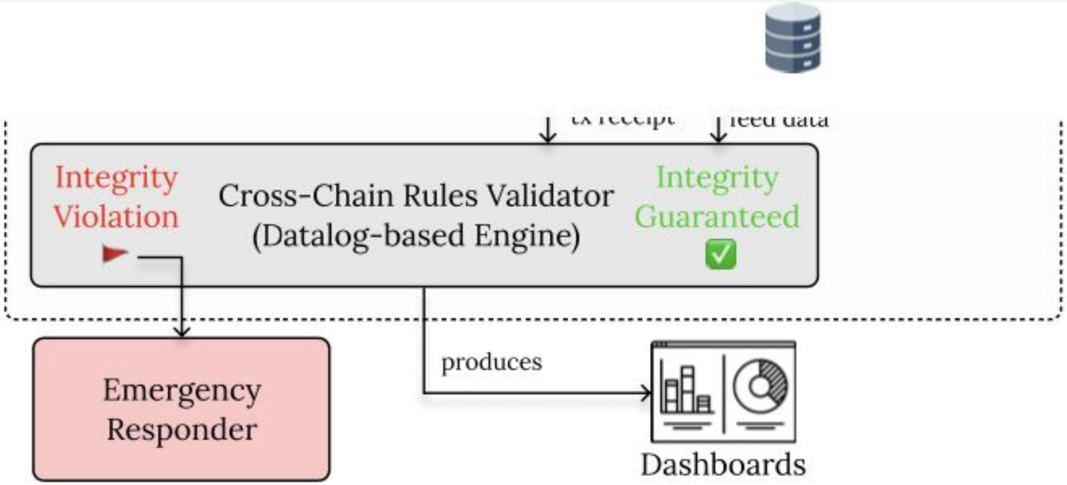
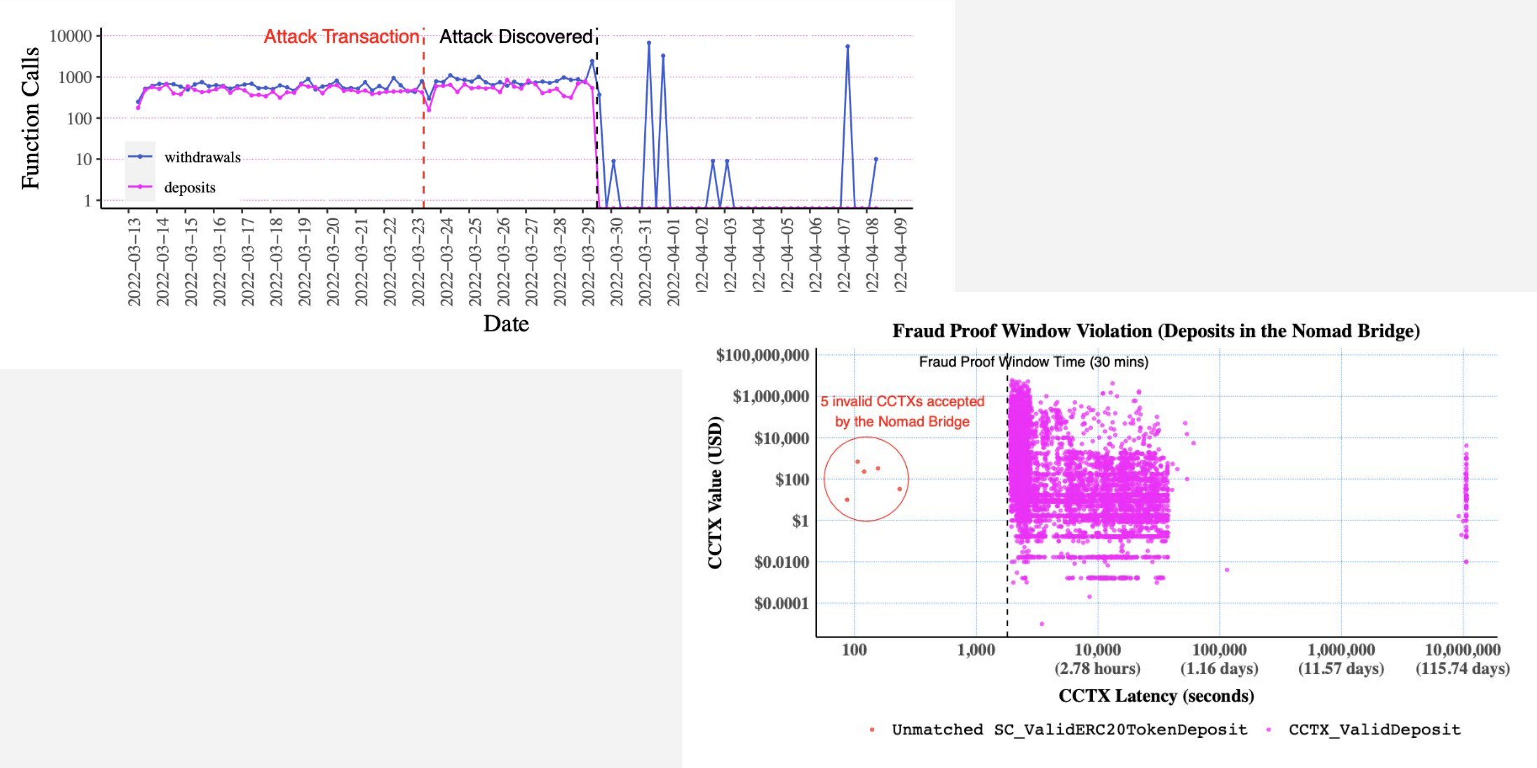


Figure 3: Architecture of XChainWatcher.


Function Calls
10000
1000
100
10
1
Attack Transaction
Attack Discovered
withdrawals
deposits
2022–03–13
2022–03–14
2022–03–15
2022–03–16
2022–03–17
2022–03–18
2022–03–19
2022–03–20
2022–03–21
2022–03–22
2022–03–23
2022–03–24
2022–03–25
2022–03–26
2022–03–27
2022–03–28
2022–03–29
2022–03–30
2022–03–31
2022–04–01
Date
Fraud Proof Window Violation (Deposits in the Nomad Bridge)
Fraud Proof Window Time (30 mins)
5 invalid CCTXs accepted
by the Nomad Bridge
CCTX Value (USD)
$100,000,000
$1,000,000
$10,000
$100
$1
$0.0100
$0.0001
100
1,000
10,000
(2.78 hours)
100,000
(1.16 days)
1,000,000
(11.57 days)
10,000,000
(115.74 days)
CCTX Latency (seconds)
Unmatched SC_ValidERC20TokenDeposit
CCTX_ValidDeposit

Benchmarking Blockchain Bridge Aggregators

UMassAmherst

Manning College of Information & Computer Sciences

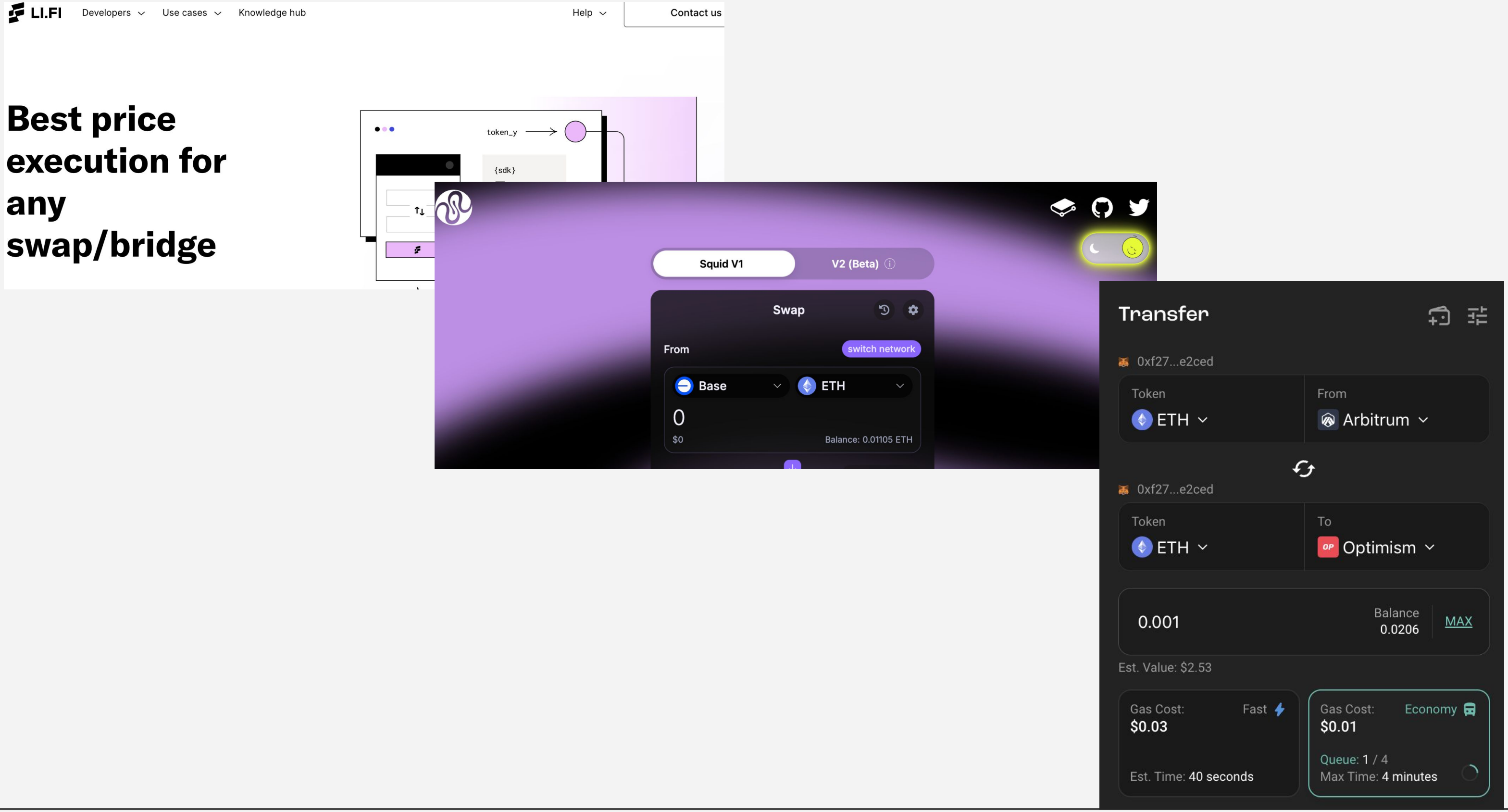
inesc id lisboa

TÉCNICO LISBOA

Shankar Subramanian[1]
André Augusto[2]
Rafael Belchior[2]
André Vasconcelos[2]
Miguel Correia[2]

University of Massachusetts, Amherst
INESC-ID, Instituto Superior Técnico

XX August 2024



Best price execution for any swap/bridge

From

Base ETH

0

$0 Balance: 0.01105 ETH

Transfer

0xf27...e2ced

Token: ETH

From: Arbitrum

0xf27...e2ced

Token: ETH

To: Optimism

0.001

Balance 0.0206 MAX

Est. Value: $2.53

Gas Cost: $0.03 Fast
Est. Time: 40 seconds

Gas Cost: $0.01 Economy
Queue: 1 / 4
Max Time: 4 minutes

Conclusions

Conclusion (Part 1/3)

Implications:

1. Advances in theoretical foundations for blockchain interoperability
   a. Unified model and classification framework
   b. Guidelines to systematically evaluate solutions
2. Propose a data model for heterogeneous blockchains based on views
   a. Common data format for heterogeneous chains
   b. Privacy-preserving friendly data format
3. Gateway paradigm
   a. Technical foundation for organizational interoperability
   b. Privacy-preserving asset transfers that are auditable,

Conclusion (Part 2/3)

Implications:

4. New interoperability framework based on ZKP
   a. dApp framework using ZKP
   b. Decentralized and cost-efficient bridge implementation on Ethereum
5. Monitoring tools for automatic incident response
   a. Cross-chain rules and model
   b. Provide first process mining implementation

Hypothesis

“IMs providing interoperability across the technical, semantic, and organizational layers can securely implement the requirements of both centralized and decentralized organizations”.

Conclusion (Part 3/3)

Conclusion

“We foresee “the development and enhancement of incident response infrastructure, the development of organizational and legal interoperability in DLTs, and the flourishing of new use cases using hybrid blockchain applications, particularly where the thesis statement is verified.”

Future Work

A. Extend cross-chain models
B. Privacy-preserving interoperability solutions
C. S&P of bridge aggregators

Thank you

Rafael Belchior

✉ *rafael.belchior@tecnico.ulisboa.pt*

@RafaelAPB

https://tinyurl.com/gscholar-rb