

Blockchain Interoperability: From Vulnerabilities to Attacks

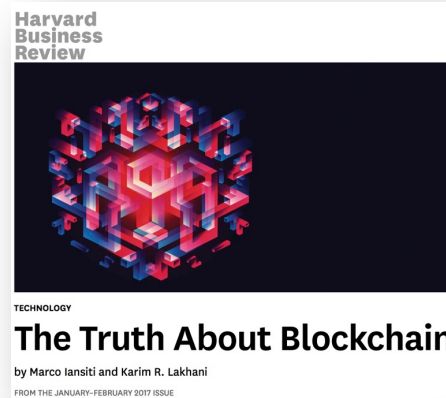
Miguel Pupo Correia

joint work with André Augusto, Rafael Belchior, André Vasconcelos, etc.



EICC 2025



Motivation: blockchain



Cryptos: 16.34M Exchanges: 822 Market Cap: \$3.31T

Name	Price	1h %	24h %	7d %	Market Cap 
 Bitcoin BTC <a data-bbox="842 1289 909 1327" href="#">Buy	\$105,357.25	▲ 0.37%	▼ 2.95%	▼ 5.17%	\$2,093,658,004,669

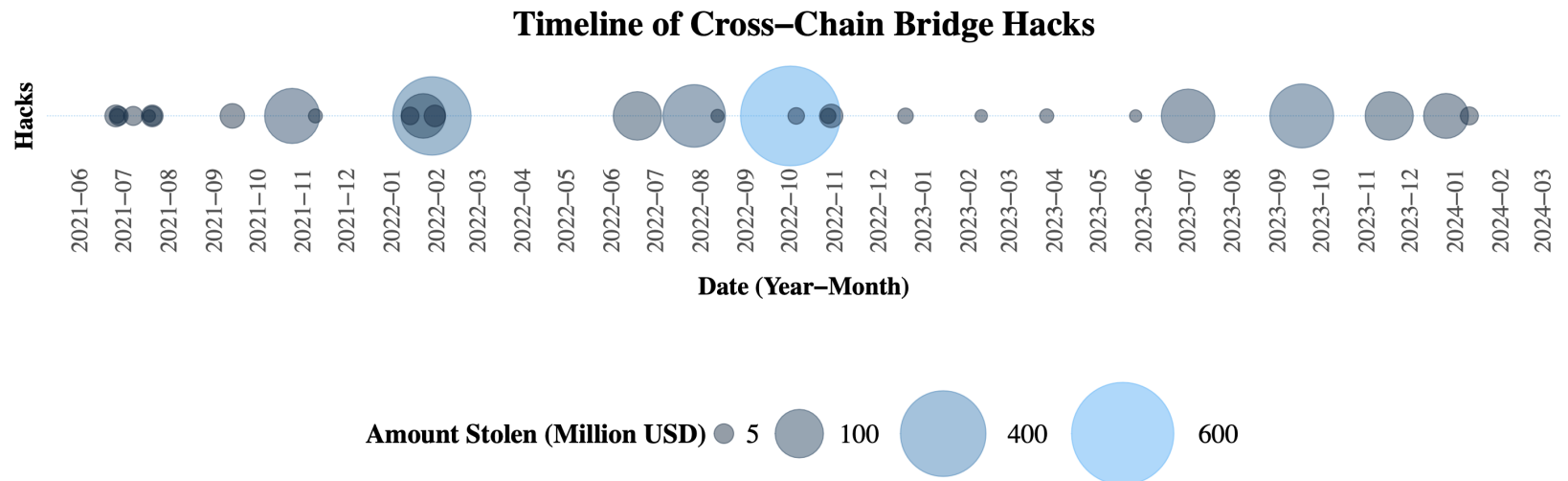
Motivation: blockchain

A blockchain is a distributed infrastructure that
is cybersecure by construction

*Not the usual question: not “how to secure it?”
but “what can we do with something that is secure?”*

Motivation: interoperability

- Interoperability is being widely adopted
- 10s billions of USD locked in cross-chain bridges



Motivation: interdisciplinarity

- **Computer Science** – distributed syst., crypto, security, programming,...
- **Economics** – investment, incentives, game theory,...
- **Law** – MICA, Pilot DLT, eIDAS 2, DAC8/taxes,...
- **Sociology** – decentralization, DAOs, adoption,...

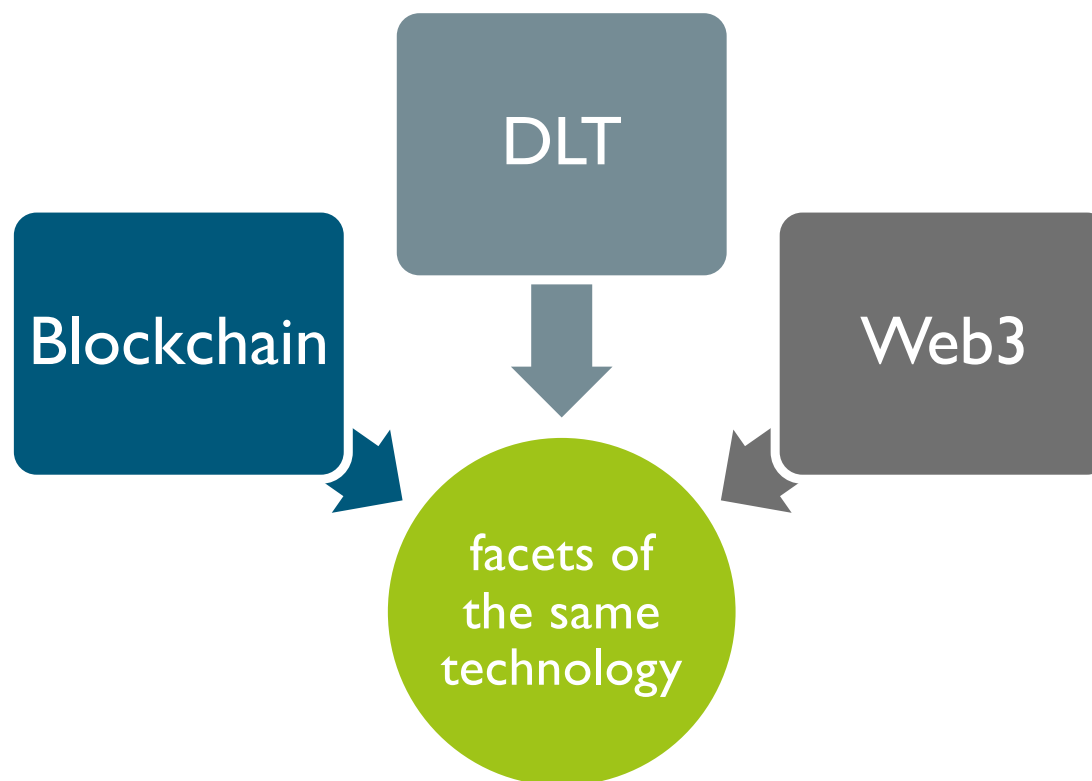
Schedule

- Blockchain in a nutshell
- Blockchain interoperability
- Security of interoperability
- Security mechanisms: Hephaestus and XChainWatcher

Schedule

- Blockchain in a nutshell
- Blockchain interoperability
- Security of interoperability
- Security mechanisms: Hephaestus and XChainWatcher

A cautionary note



“Blockchain” has two meanings

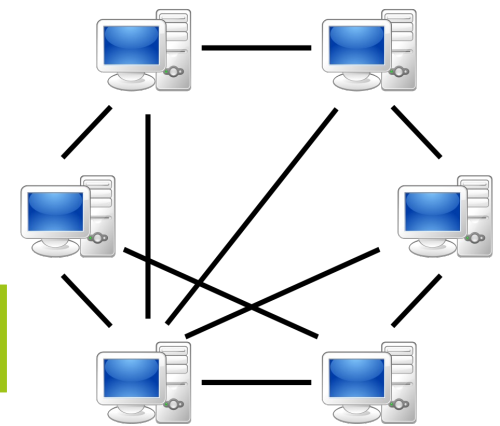
I) Data structure – append-only, chain of blocks of transactions – ledger



“Blockchain” has two meanings

2) Distributed system – set of Internet nodes/peers

- They execute software and keep a copy of the chain
- They run a consensus algorithm to agree on the next block to append to the data structure



Today I will use the term Blockchain always in this sense

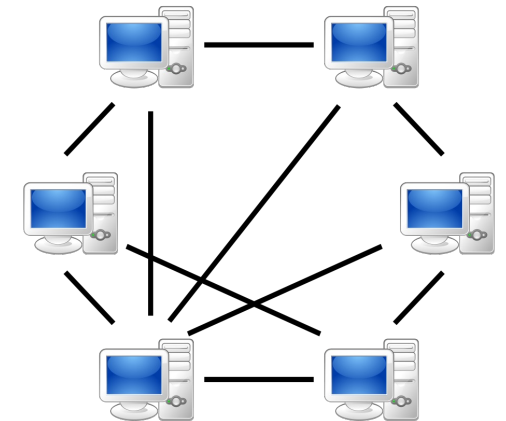
Blockchain relevant properties

- **Availability & integrity** – works 24/7 even if some nodes are compromised (intrusion tolerance, Byzantine fault tolerance)
- **Auditability** – the ledger is visible to “everyone”, so it can be verified
- **Immutability** – once a transaction is appended, it’s not removed
- **Programmability** – transactions cause the execution of code, enabling automation
- **Decentralization** – properties above without trust on a third party – this is what is new in Blockchain!

Bitcoin



- Bitcoin is a **cryptocurrency**
 - a **digital asset**
 - \approx fiat currencies (e.g., Euro), but not issued by a central bank
- Who issues the coin? Who ensures we can trust it?
 - A blockchain system (thousands of nodes)
 - that execute Bitcoin software
 - and keeps copies of the blockchain (data structure)
 - Decentralized!



- Another blockchain that implements a cryptocurrency (ether)
 - Introduced the notion of **smart contract**
- A **smart contract** is:
 - Software, i.e., a program
 - Stored & executed in the blockchain nodes (thousands)
 - May involve asset transfers (in ether)
 - Not usually smart or (legal) contracts



Tokens

- **Token**: a blockchain-based abstraction that represents something that can be owned; examples:
 - Digital assets, e.g., ERC-20
 - Equity (part of some entity)
 - Collectibles (NFTs)
 - Real World Assets (also NFTs)
- Tokens are generated, stored and transferred in **smart contracts**

Blockchain variants

- **Permissionless** for **public** use
 - ex.: Bitcoin and Ethereum
 - any server can join the network (no permission needed)
- **Permissioned** for **consortium** or **private (?)** use
 - ex.: instances of Hyperledger Fabric, Hyp. Besu, Quorum, Corda
 - servers must have permission to join
 - *participants already have some degree of trust among them, but want to simulate the services of a neutral third party*

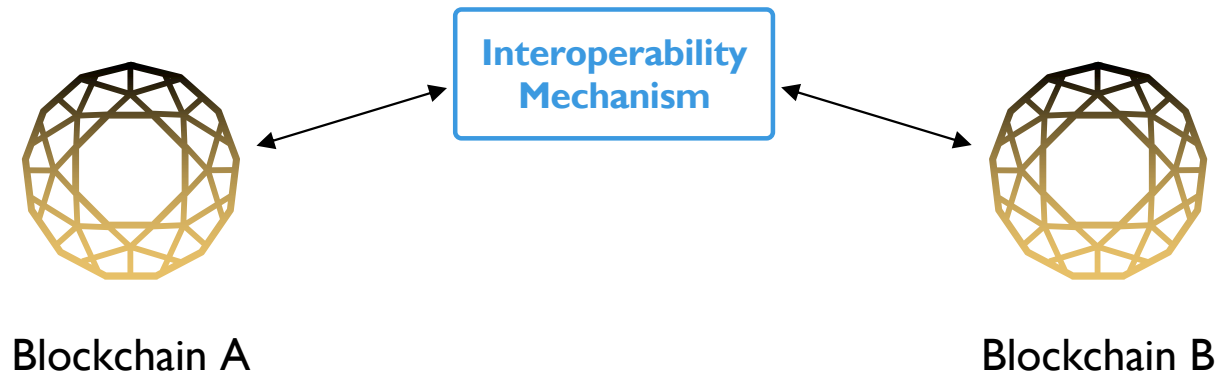
Schedule

- Blockchain in a nutshell
- Blockchain interoperability
- Security of interoperability
- Security mechanisms: Hephaestus and XChainWatcher

Why Blockchain Interoperability?

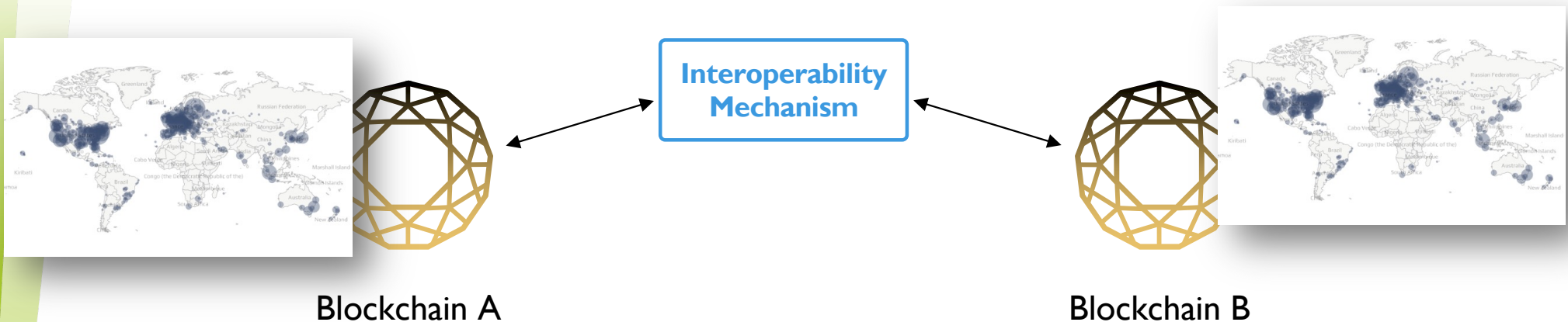
- Scalability – L1-L1 and L1-L2
- Exchange tokens in a public blockchain by tokens in another
- Unwillingness to share data in a common private/consortium blockchain

Blockchain Interoperability



Blockchain Interoperability challenges

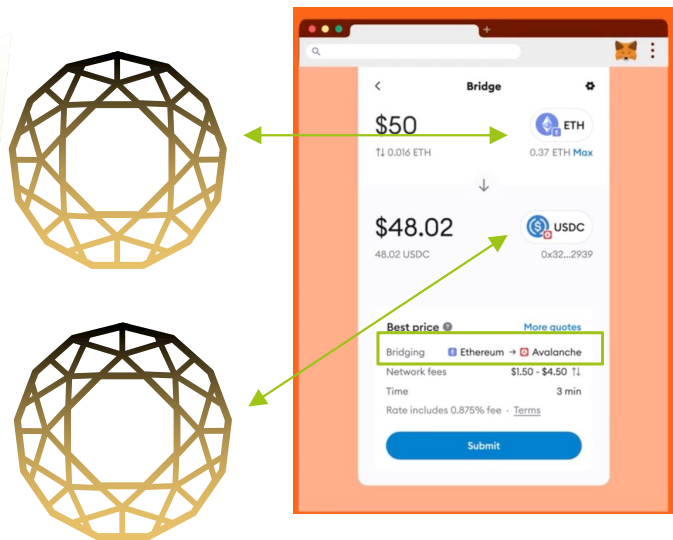
- Not 2 nodes but 2 decentralized infrastructures!



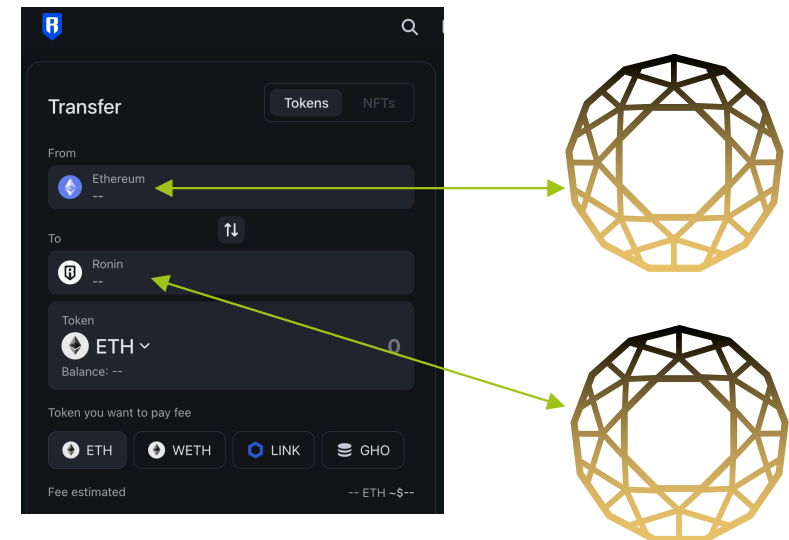
- Technical: No single node to contact and contacting one is not enough
- Technical: Consensus finality may be uncertain and require time (minutes)
- Sociologic: Created by young enthusiastic people focused on products, not security

Example: Blockchain Bridges

Metamask



Ronin



Example: how a token bridge works?

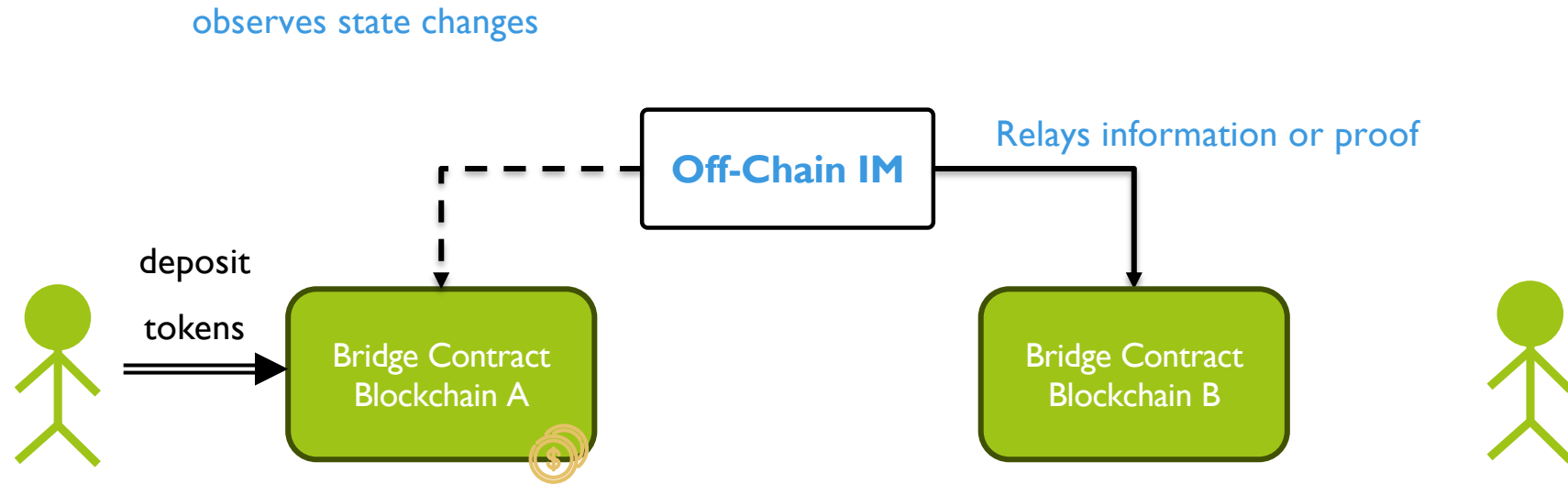


IM = Interoperability Mechanism

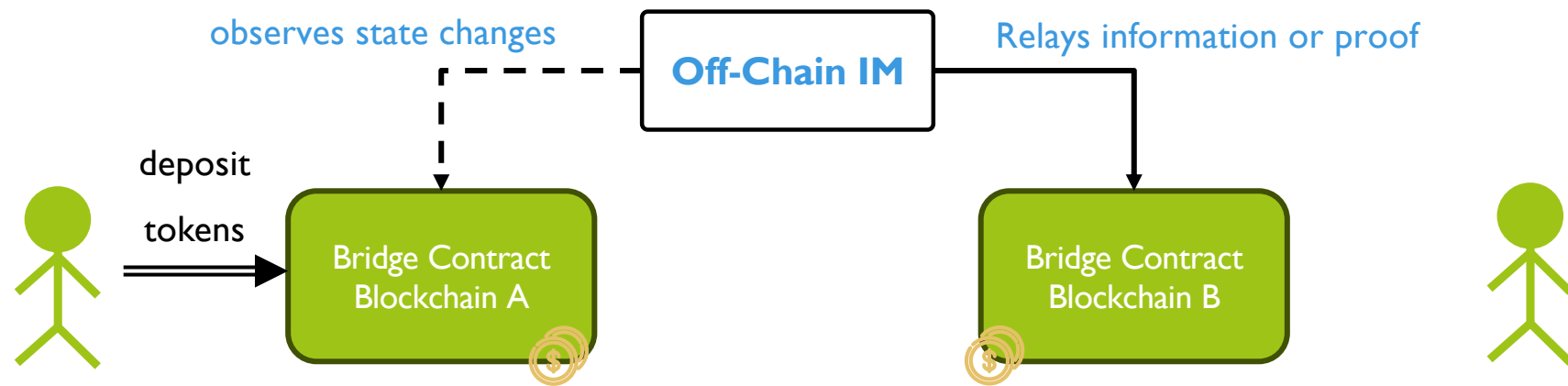
Example: how a token bridge works?



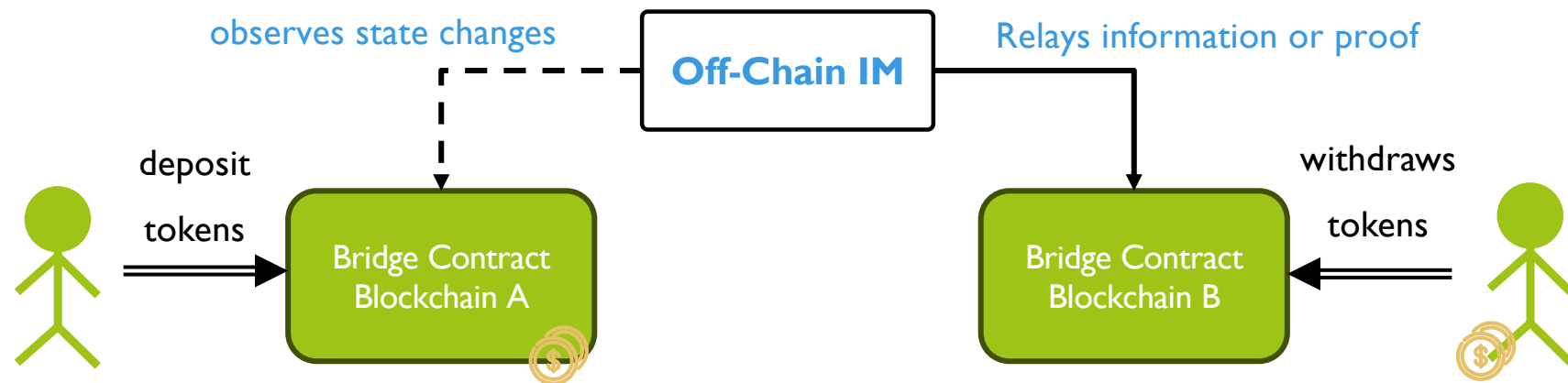
Example: how a token bridge works?



Example: how a token bridge works?



Example: how a token bridge works?



There are multiple modes:

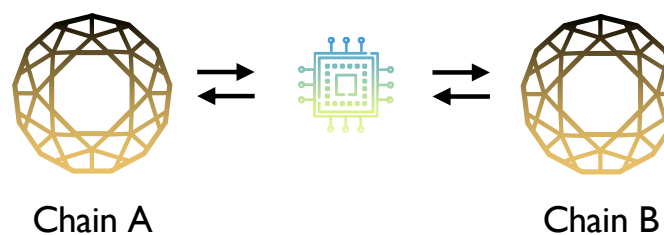
- Lock-mint (in the diagram)
- Burn-mint
- Lock-unlock

IM architectures

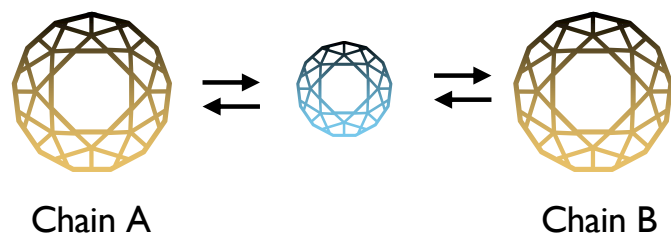
Centralization



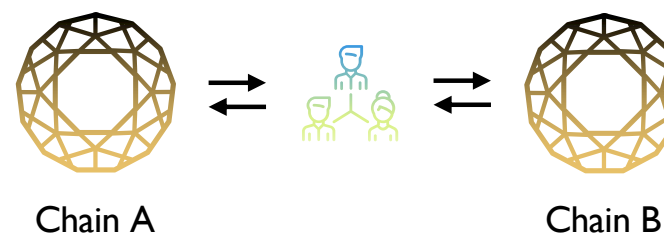
Trusted Computation



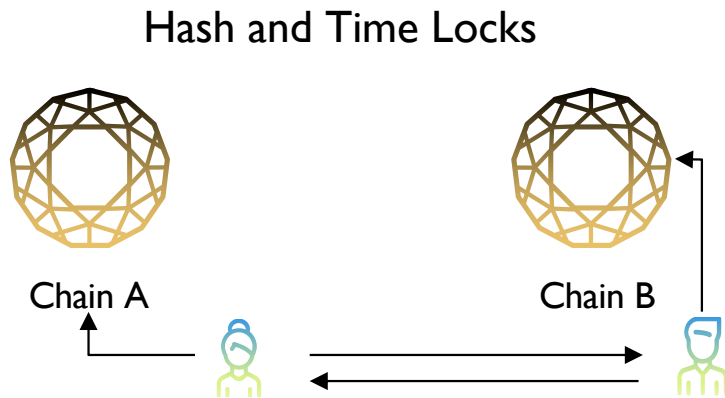
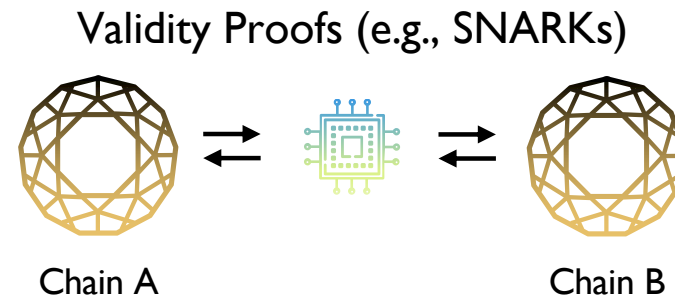
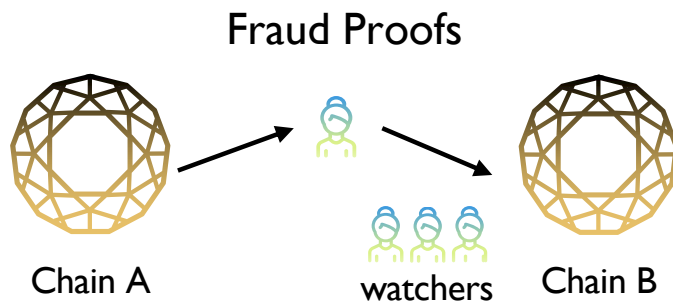
Permissionless Blockchain



Permissioned Blockchain



IM architectures (cont.)



and more...

Schedule

- Blockchain in a nutshell
- Blockchain interoperability
- Security of interoperability
- Security mechanisms: Hephaestus and XChainWatcher

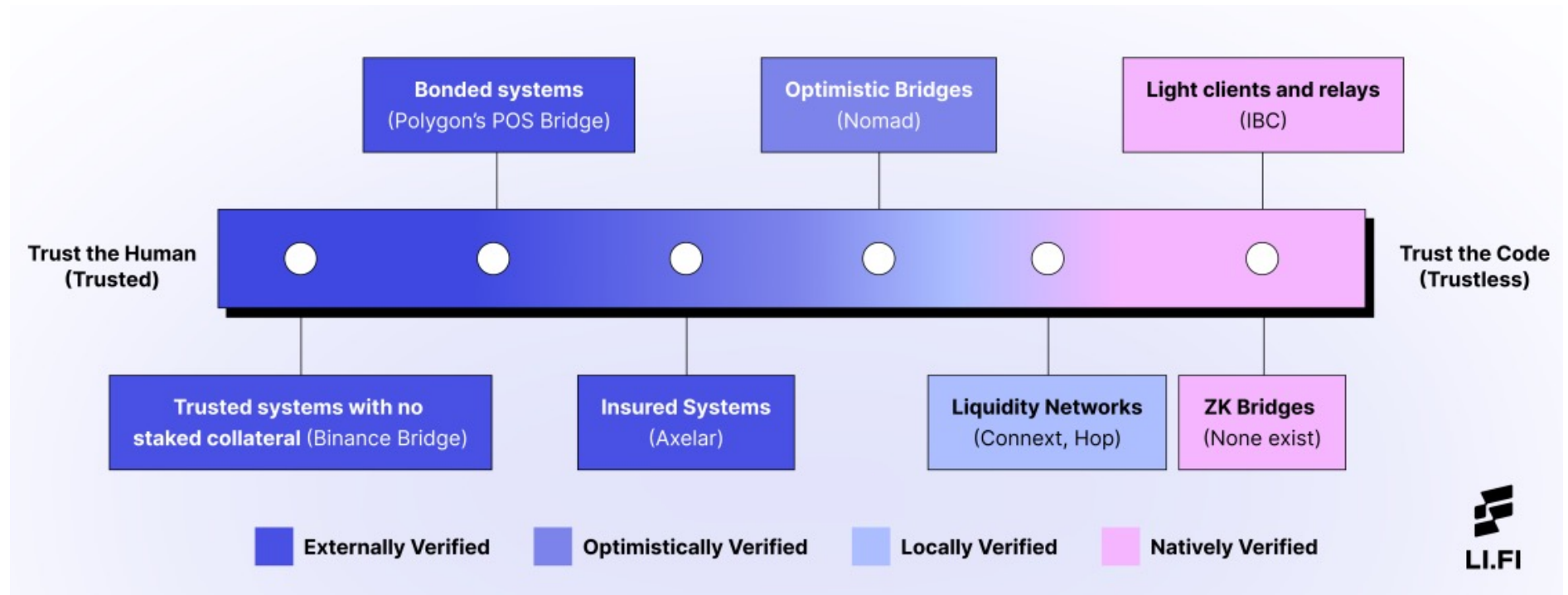
How to classify IMs based on security guarantees?

Impossibility result

*There exists no asynchronous **cross-chain communication protocol** that is tolerant to misbehaving nodes without a **trusted third party**.*

(the problem can be reduced to fair exchange)

Trust spectrum for bridges



The Trust Spectrum doesn't say all we need

A set of properties



Integrity

of the system, data, and assets



Accountability

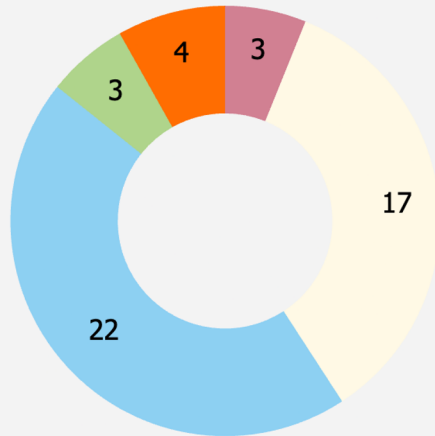
of participants for integrity breach attempts



Availability

of system to process cross-chain transactions

Vulnerabilities in Interoperability



● Operational Layer
 ● Implementation Layer
 ● Protocol Layer
 ● Network Layer
 ● Privacy Leaks

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]	$\mathcal{M}_{40}, \mathcal{M}_{41}$

• • • •

Attacks against Cross-Chain Bridges

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					
[193] Ronin	SA_{22}	Mar 2022	624M	■	○	●	6d	●	IM	SC	✓	✓	✗	✗	✗	✗					
[194] PolyBridge #1	SA_{22}	Aug 2021	611M	□	●	○	–	●	TC	SC	✗	✓	✓	✗	✗	✗					
[195] BNB	SA_{11}	Oct 2022	566M	■	●	●	–	●	TC	TC	✗	✗	✗	✗	✓	✗					
[108] Wormhole	SA_{22}	Feb 2022	326M	■	○	●	–	○	TC	TC	✗	✗	✓	✗	✓	✗					
[196] Nomad	SA_{33}	Aug 2022	190M	□	●	●	–	●	SC	SC	✗	✗	✗	✗	✓	✗					
[197] BXH	SA_{11}	Oct 2021	139M	■	○	●	–	●	–	SC	✓	✓	✗	✗	✗	✗					
[198] Multichain #2	SA_{22}	Jul 2023	126M	■	○	○	–	●	IM	SC	✓ [†]	✓ [†]	✗	✗	✗	✗					
[199] Harmony	SA_{22}	Jun 2022	100M	■	●	●	–	●	IM	SC	✓	✓	✗	✗	✗	✗					
[200] Qubit	SA_{11}	Jan 2022	80M	■	●	●	–	●	SC	TC	✗	✗	✗	✓	✓	✗					
[201] pNetwork	SA_{33}	Sep 2021	13M	■	○	○	13m	○	IM	SC	✗	✗	✗	✗	✗	✓					
[202] Thorchain #3	SA_{21}	Jul 2021	8M	■	○	●	–	–	IM	SC	✗	✗	✗	✗	✗	✓					
[198] Anyswap	SA_{22}	Jul 2021	8M	■	○	●	–	●	IM	TC	✗	✓	✗	✗	✗	✗					
[202] Thorchain #2	SA_{21}	Jul 2021	5M	■	●	●	–	●	IM	TC	✗	✗	✗	✗	✓	✓					
[194] PolyBridge #2	SA_{22}	Jul 2023	4.4M	■	●	○	7h	●	IM	TC	✗	✓	✗	✗	✗	✗					
[203] Meter	SA_{22}	Jul 2021	4.4M	■	○	●	–	●	SC	TC	✗	✗	✗	✗	✓	✗					
[204] Chainswap	SA_{22}	Jul 2021	4.4M	■	●	●	–	●	TC	TC	✗	✗	✓	✗	✓	✗					
[198] Multichain #1	SA_{22}	Jan 2022	3M	□	–	●	–	●	TC	BL	✗	✗	✗	✓	✓	✗					
[202] Thorchain #1	SA_{21}	Jun 2021	140K	■	–	●	5m	–	IM	TC	✗	✗	✗	✗	✗	✓					
Summary		07/21 - 07/23		2.9B												22%	39%	17%	11%	44%	22%

Attacker Type (AT)

- Black hat
- White hat
- Black and white hats

– No information available / Team did not respond

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

[†] Still to be confirmed

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

Discovery Time (DT)

Vulnerabilities Behind the Attacks

Project Information		General Attack Information					Incident Resp		Where		Mapping to Theoretical Vulnerabilities					
Name & Ref	SA	Date	Amount	AT	Txs	Mix	DT	CT	VL	EL	v_{44}	v_{43}	v_{28}	v_{27}	v_{24}	v_6

Physical
infrastructure
backdoors

Bad key
management

Dead code

Unsafe third-
party software

Lack of access
control

Incorrect
event verification

Ronin bridge attack March 2022



- **Ronin**
 - Multi-signature bridge: transactions approved by several operators (validators)
 - 9 validators in 2022, 4 controlled by a company, Sky Mavis (!)
- **Attack**
 - Nov. 2021: high request load, so Sky Mavis asks another validator (Axie DAO) the **private keys** to sign transactions on its behalf (!); so long decentralization...
 - Mar. 2022: Sky Mavis employees constantly under sophisticated **spear-phishing attacks** on various social channels; one falls into one such attack
 - Attacker penetrates the Sky Mavis IT infrastructure and gains access to the **private keys** of 4+1 validators
 - The attacker signs transactions and steals 624M

Schedule

- Blockchain in a nutshell
- Blockchain interoperability
- Security and of interoperability mechanisms
- Security mechanisms: Hephaestus and XChainWatcher

Problem: long detection time

Project Information		General Attack Information					Incident Resp	
Name & Ref	SA	Date	Amount	AT	Txs	Mix	DT	CT
[193] Ronin	SA ₂₂	Mar 2022	624M	■	○	●	6d	●
[194] PolyBridge #1	SA ₂₂	Aug 2021	611M	□	○	○	—	○
[195] BNB	SA ₁₁	Oct 2022	566M	■	○	●	—	●
[108] Wormhole	SA ₂₂	Feb 2022	326M	■	○	●	—	○
[196] Nomad	SA ₃₃	Aug 2022	190M	□	●	●	—	○
[197] BXH	SA ₁₁	Oct 2021	139M	■	○	●	—	●
[198] Multichain #2	SA ₂₂	Jul 2023	126M	■	○	○	—	●
[199] Harmony	SA ₂₂	Jun 2022	100M	■	○	●	—	●
[200] Qubit	SA ₁₁	Jan 2022	80M	■	○	●	—	○
[201] pNetwork	SA ₃₃	Sep 2021	13M	■	○	○	13m	○
[202] Thorchain #3	SA ₂₁	Jul 2021	8M	■	○	●	—	—
[198] Anyswap	SA ₂₂	Jul 2021	8M	■	○	●	—	●
[202] Thorchain #2	SA ₂₁	Jul 2021	5M	■	●	●	—	●
[194] PolyBridge #2	SA ₂₂	Jul 2023	4.4M	■	○	○	7h	●
[203] Meter	SA ₂₂	Jul 2021	4.4M	■	○	●	—	○
[204] Chainswap	SA ₂₂	Jul 2021	4.4M	■	●	●	—	●
[198] Multichain #1	SA ₂₂	Jan 2022	3M	□	—	●	—	●
[202] Thorchain #1	SA ₂₁	Jun 2021	140K	■	—	○	5m	—
Summary		07/21 - 07/23	2.9B					

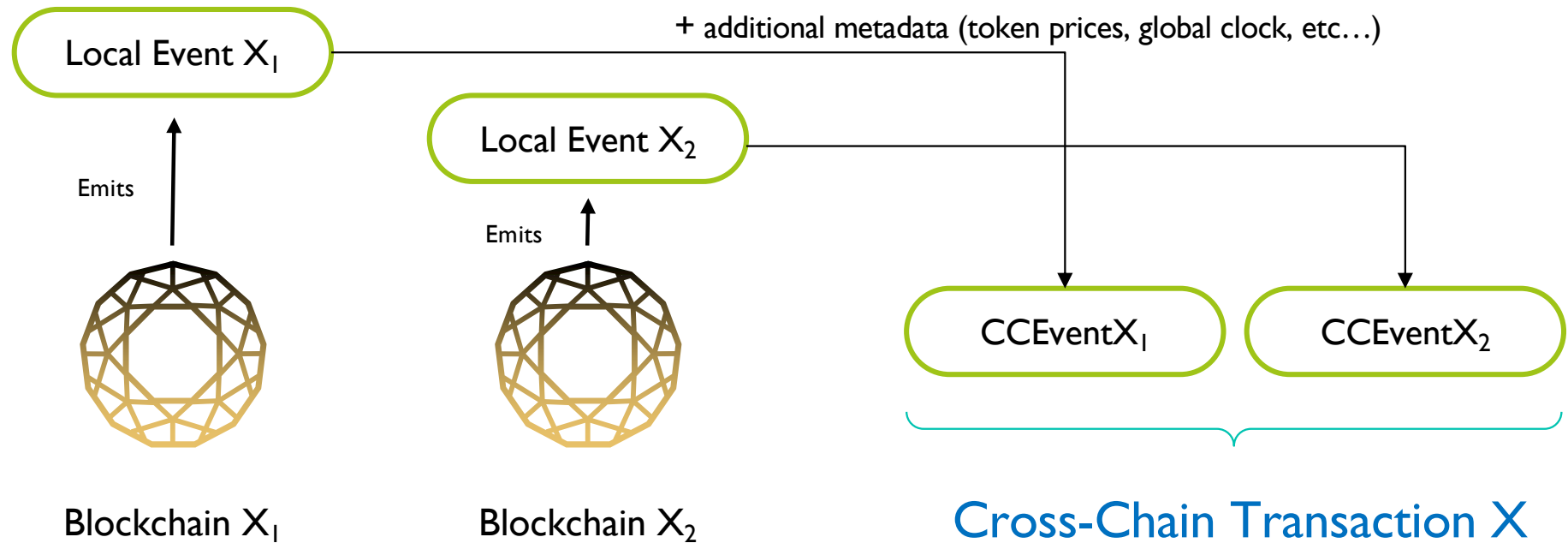
our focus now

Communication Time (CT)

-]0; 2] hours
-]2; 4] hours
-]4; 6] hours
-]6; 24] hours
- >= 6 days

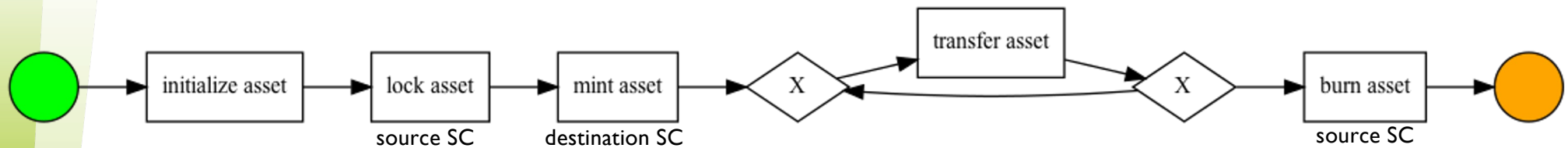
Hephaestus: cross-chain transaction modelling

- **Hephaestus**: a framework/software of **cross-chain transaction models**
- Consider a transaction:

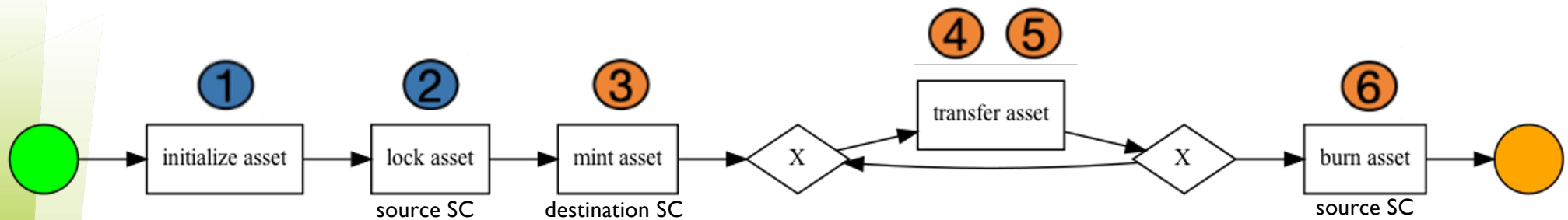


Hephaestus: check if transaction follows model

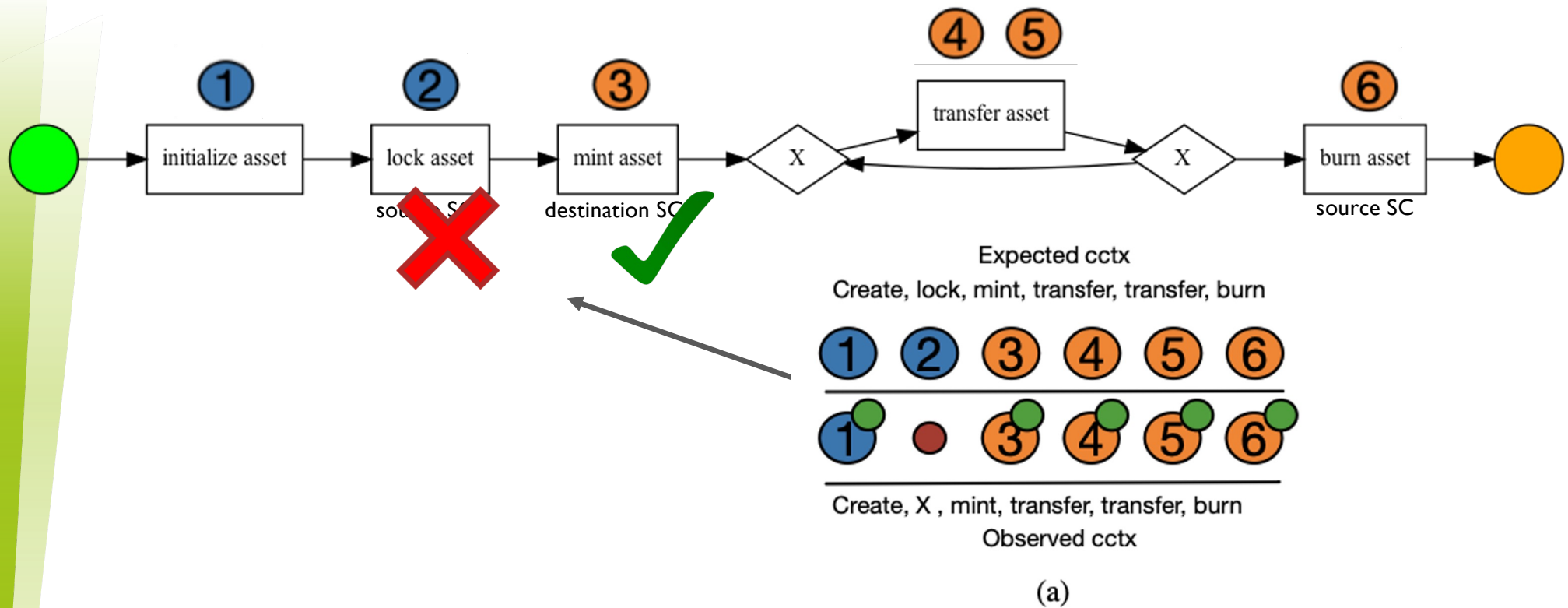
- Example: transaction on the burn-mint model



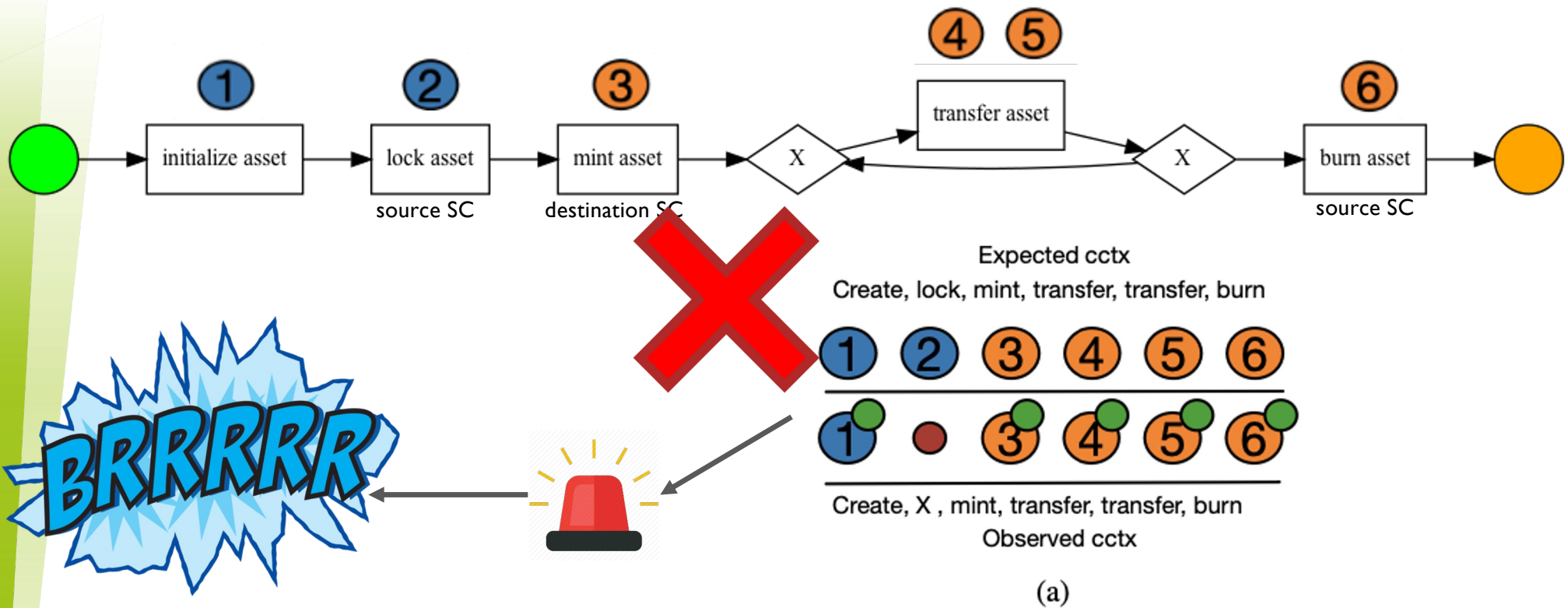
Hephaestus: check if transaction follows model



Hephaestus: check if transaction follows model



Hephaestus: check if transaction follows model



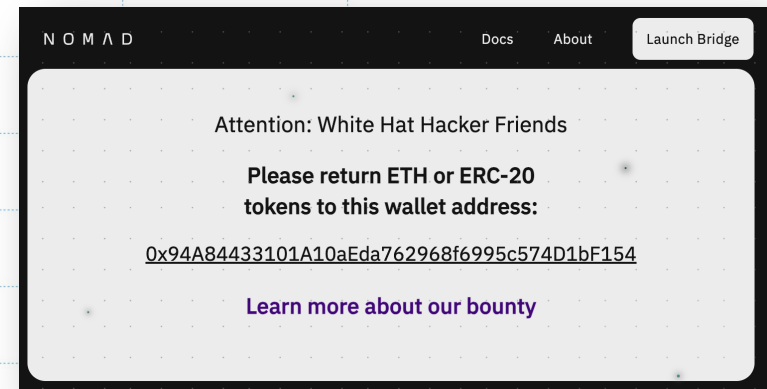
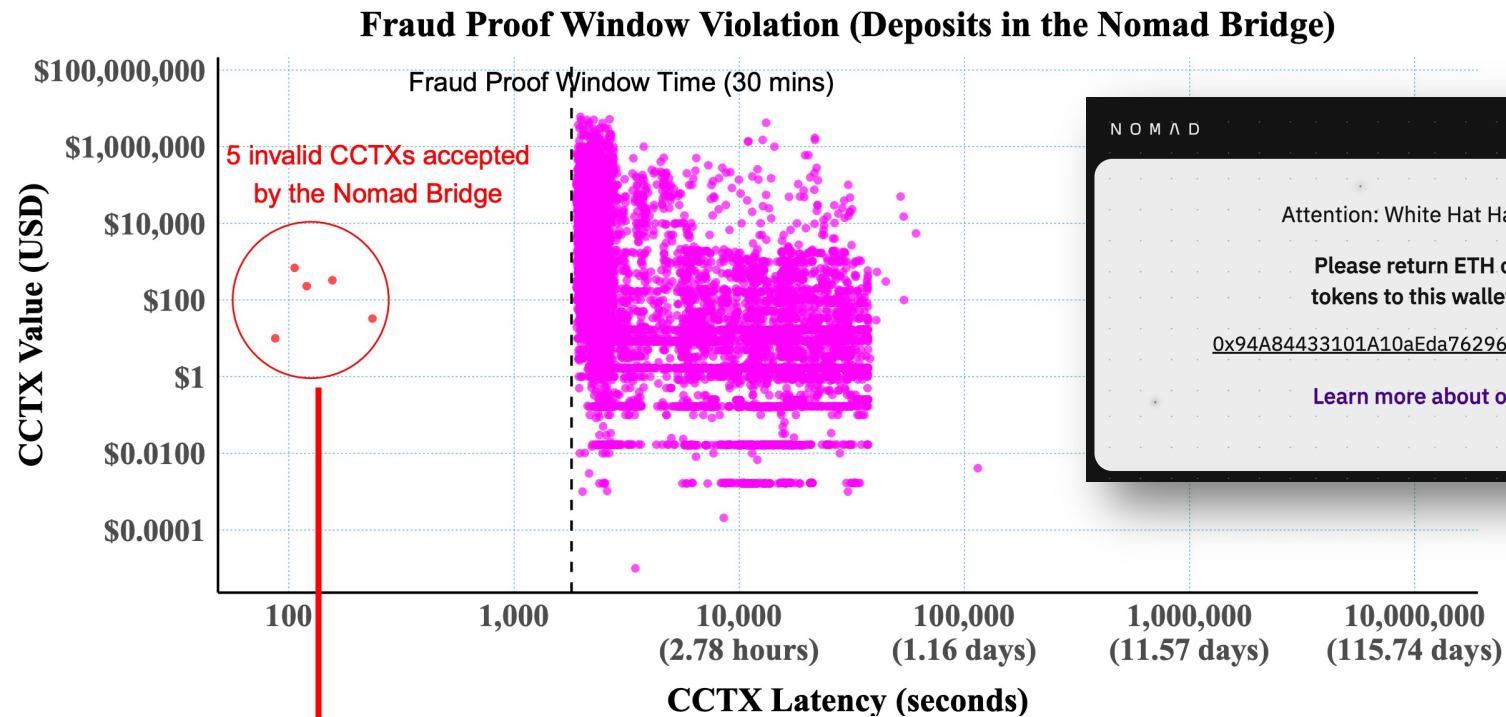
XChainWatcher: cross-chain rules

Finding anomalies in cross-chain protocols through Datalog **cross-chain rules**

Example: **rule** defining that a **valid deposit** of tokens has the same amount, same beneficiary, etc. than what was requested

```
// Rule 4 (D)
CCTX_ValidDeposit(orig_chain_id, orig_timestamp, orig_tx_hash, dst_chain_id, dst_timestamp,
  orig_token, dst_token, sender, benef, amount) :-
  TC_ValidERC20TokenDeposit(dst_timestamp, dst_tx_hash, deposit_id, benef, dst_token,
  (
    SC_ValidERC20TokenDeposit(orig_timestamp, orig_tx_hash, deposit_id, sender, _,
    orig_chain_id, dst_chain_id, _, amount) ;
    SC_ValidNativeTokenDeposit(orig_timestamp, orig_tx_hash, deposit_id, sender, _,
    orig_chain_id, dst_chain_id, _, amount)
  ),
  cctx_finality(orig_chain_id, orig_chain_finality),
  orig_timestamp + orig_chain_finality < dst_timestamp.
```

XChainWatcher: example anomaly



Bridge makes deposit in the destination SC, before deposit in source SC being final

Concluding

Instituto de Engenharia de Sistemas e Computadores
Investigação e Desenvolvimento em Lisboa



Key take-aways

- Blockchain, area for interdisciplinary security research
- Blockchain interoperability is particularly new and interesting
 - Attacks cost billions
 - Security is far from adequate
 - Opportunity to contribute and have impact

Some related publications



- A Augusto et al. **SoK: Security and Privacy of Blockchain Interoperability**. IEEE Symposium on Security and Privacy 2024, S. Francisco, USA, May 2024
- R Belchior et al. **A Survey on Blockchain Interoperability: Past, Present, and Future Trends**. ACM Computing Surveys, Vol. 54, Issue 8, Nov 2022
- R Belchior et al. **Hephaestus: Modelling, Analysis, and Performance Evaluation of Cross-Chain Transactions**. IEEE Transactions on Reliability, 2023
- A Augusto et al. **XChainWatcher: Monitoring and Identifying Attacks in Cross-Chain Bridges**. arXiv preprint arXiv:2410.02029, 2024