Thunderdome

Timelock-Free Rationally-Secure Virtual Channels

Zeta Avarikioti
TU Wien &
Common Prefix

Yuheng Wang
TU Wien

Yuyi Wang
CRRC Zhuzhou Institute &
Tengen Intelligence Institute

USENIX Security 2025

Background

- Blockchain is known for its **scalability limitation**
  - Visa: 1,700 TPS
  - Ethereum: 142 TPS[1] (given its current 36M gas limit, 12s blocks, and 21k gas cost for ETH transfers)

[1] "Ethereum", Wikipedia, https://en.wikipedia.org/wiki/Ethereum, accessed July 2025.

Background

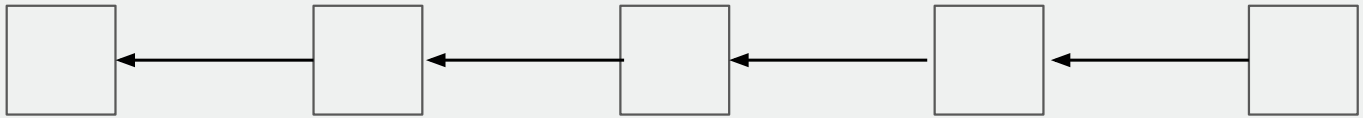
- Blockchain is known for its **scalability limitation**
  - Visa: 1,700 TPS
  - Ethereum: 142 TPS[1] (given its current 36M gas limit, 12s blocks, and 21k gas cost for ETH transfers)

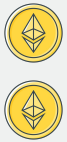
- Current solutions to this challenge
  - Blockchain sharding
  - Efficient consensus scheme
    - Causing hard fork
  - Layer 2 protocols: **Payment Channel Network (PCN)**, Sidechain, Rollup etc.

[1] "Ethereum", Wikipedia, https://en.wikipedia.org/wiki/Ethereum, accessed July 2025.

Background

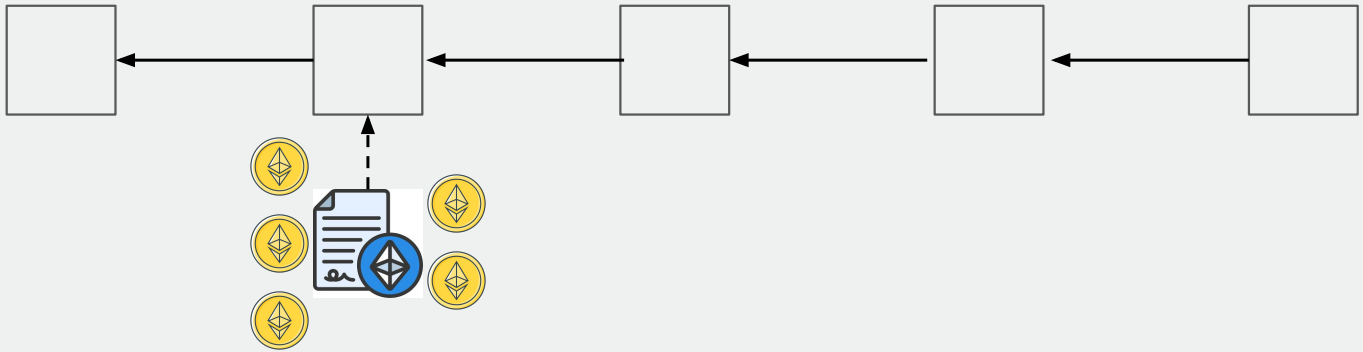
- Fundations of Channels

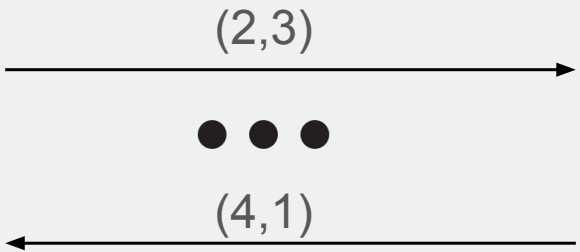




Background

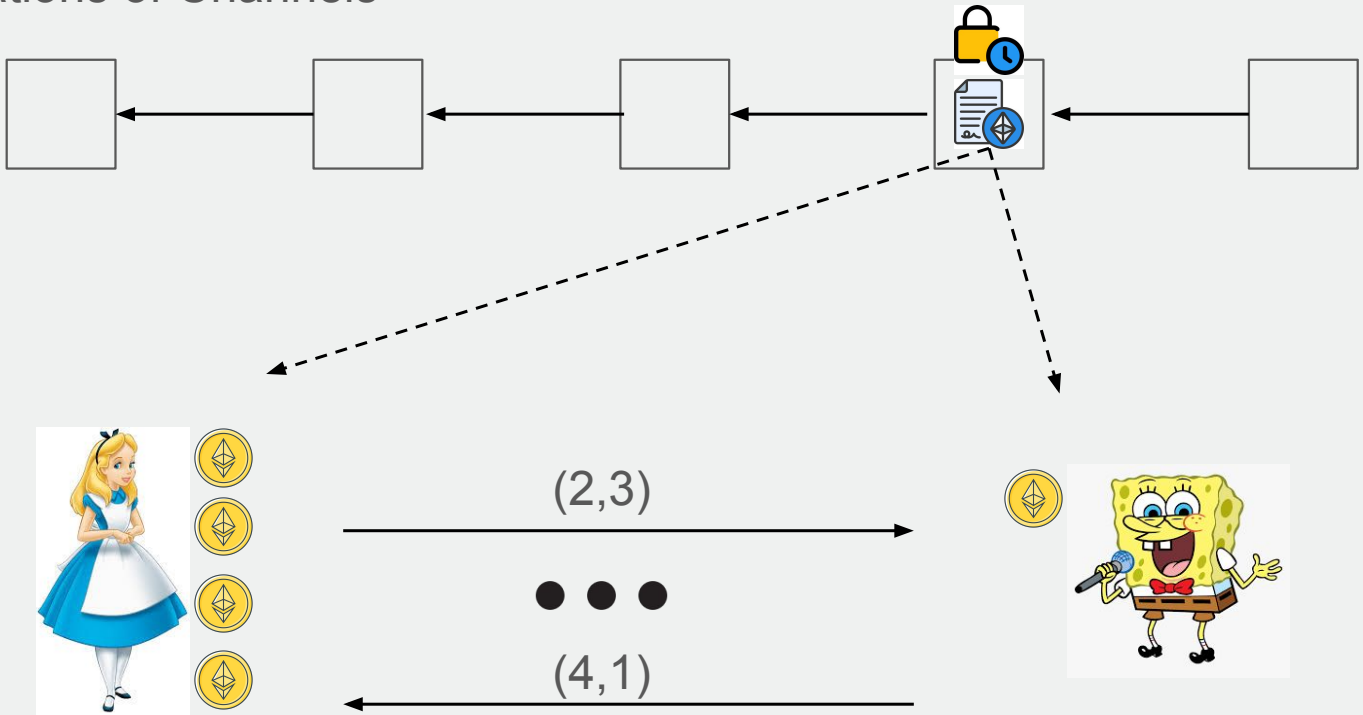
- Fundations of Channels





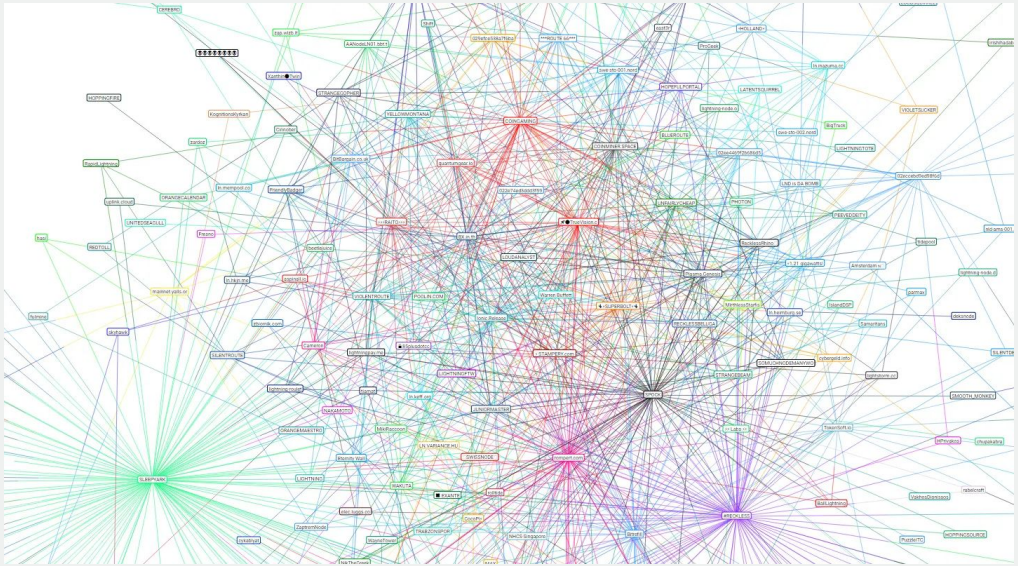
Background

- Fundations of Channels



Background

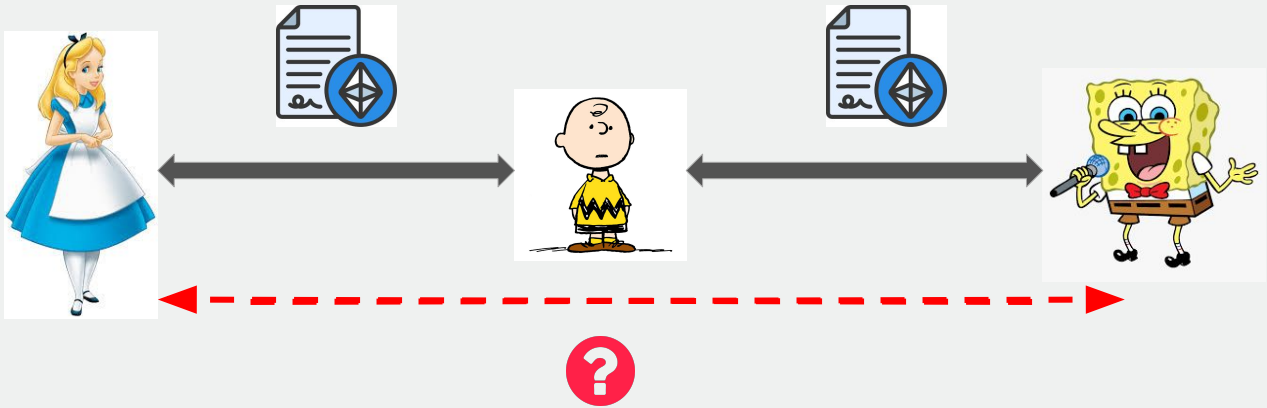
- Payment Channel Networks



[2] Lim, "Lightning Network: Last Mile Solution", Medium, July 6, 2020.

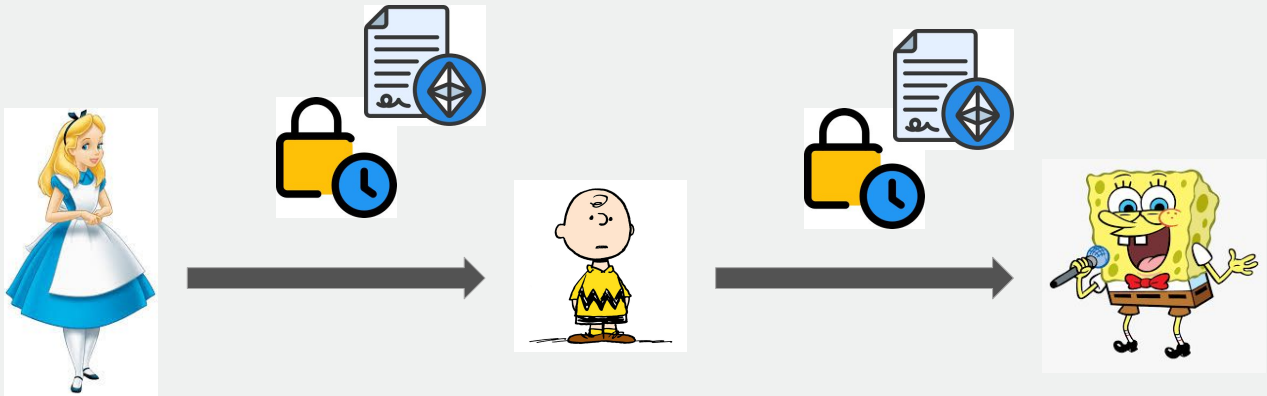
Background

- Payment Channel Networks
  - Two-hop Example



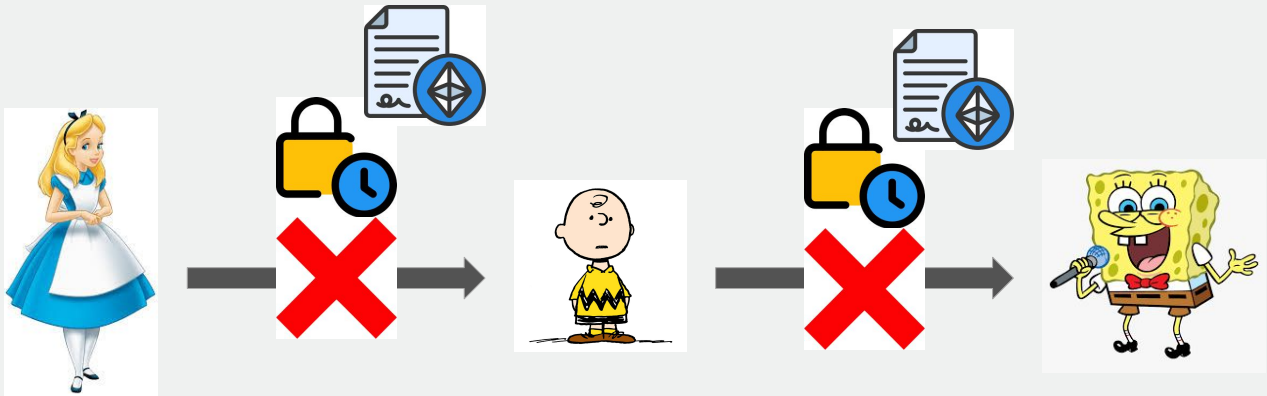
Previous Works

- Multi-hop Payment based on **Timelock Channel**
  - Transactions between *Alice / Charlie*, *Charlie / Bob* should executed **atomically** within certain **time period**
  - Hash Timelock Contracts, Verifiable Timed Signatures …



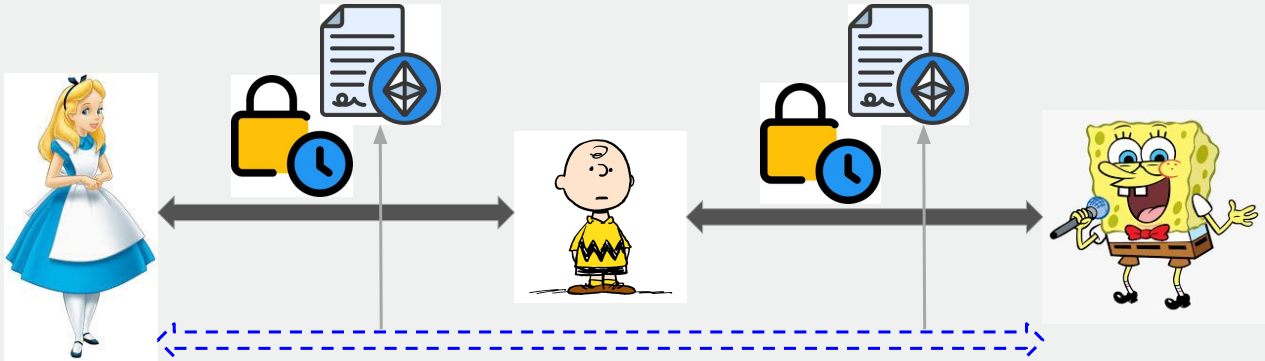
Previous Works

- Multi-hop Payment based on **Timelock Channel**
  - Transactions between *Alice / Charlie*, *Charlie / Bob* should executed **atomically** within certain **time period**
  - Hash Timelock Contracts, Verifiable Timed Signatures …
  - Require participation of intermediary party all the time
  - Rely on time-related assumptions



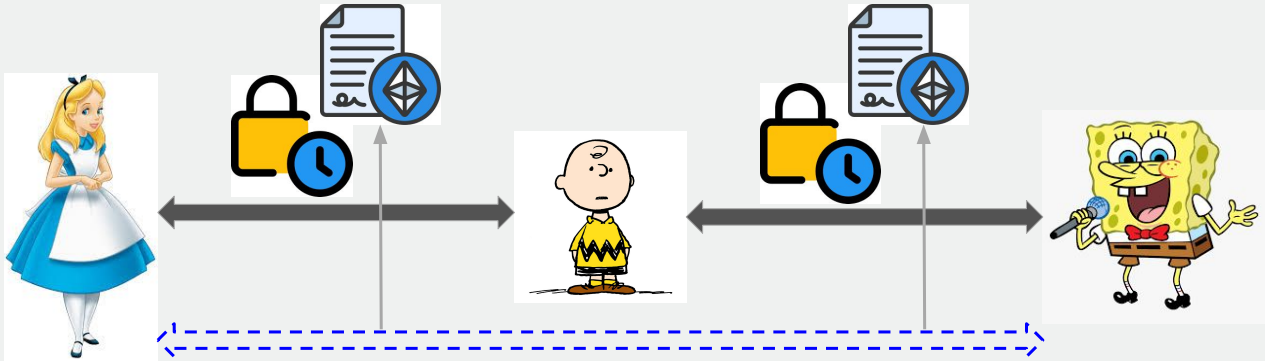
Previous Works

- Virtual Channel
  - Charlie only helps Alice and Bob open/close a virtual channel
  - Rely on time-related assumptions



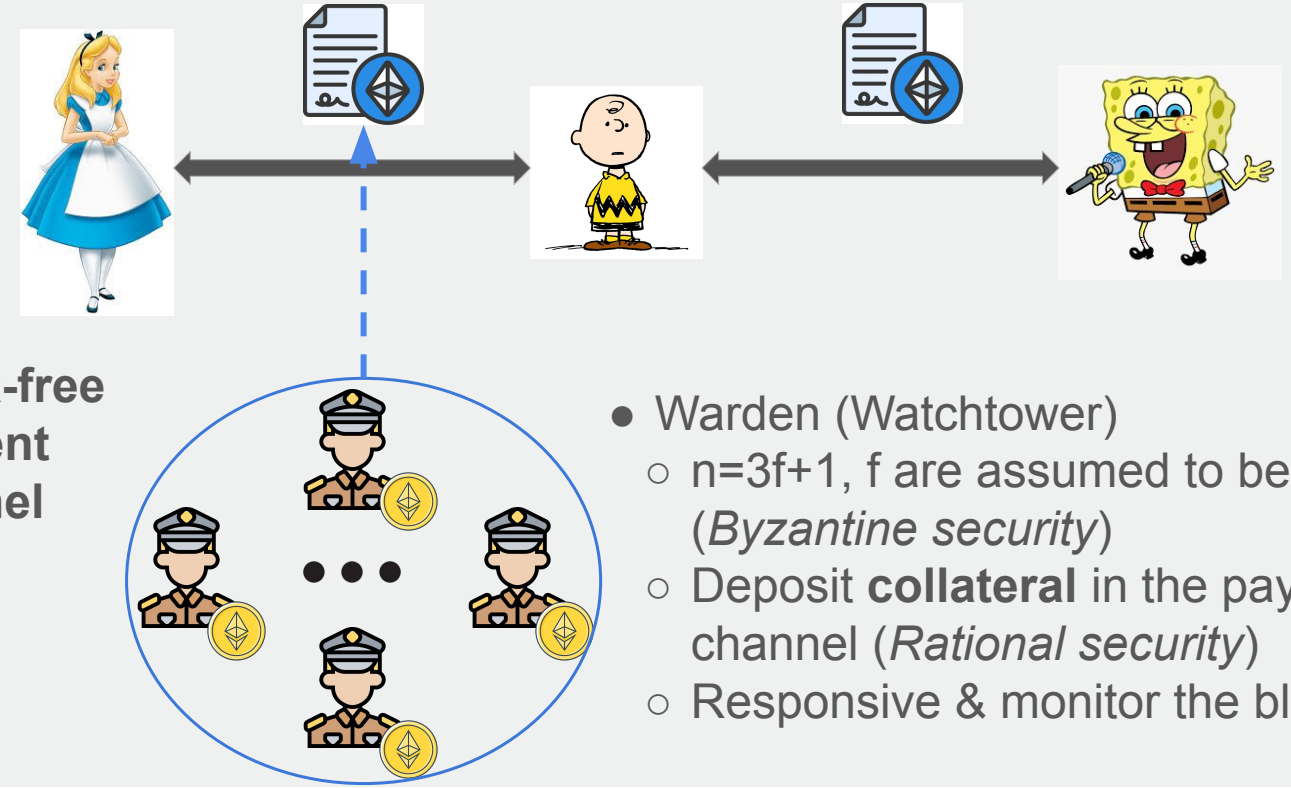
Previous Works

- Virtual Channel
  - Charlie only helps Alice and Bob open/close a virtual channel
  - Rely on time-related assumptions



Can we secure PCNs be designed without the reliance on timelocks?

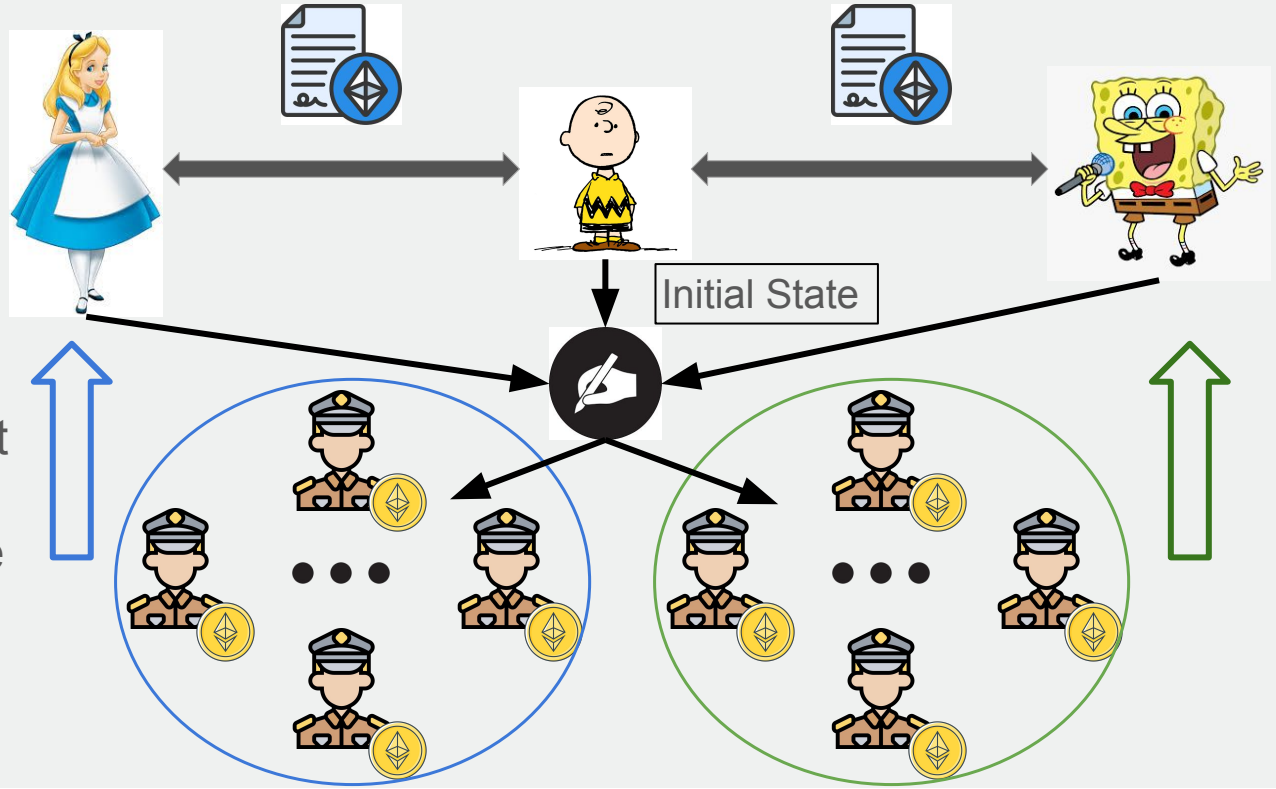
Overview of Thunderdome



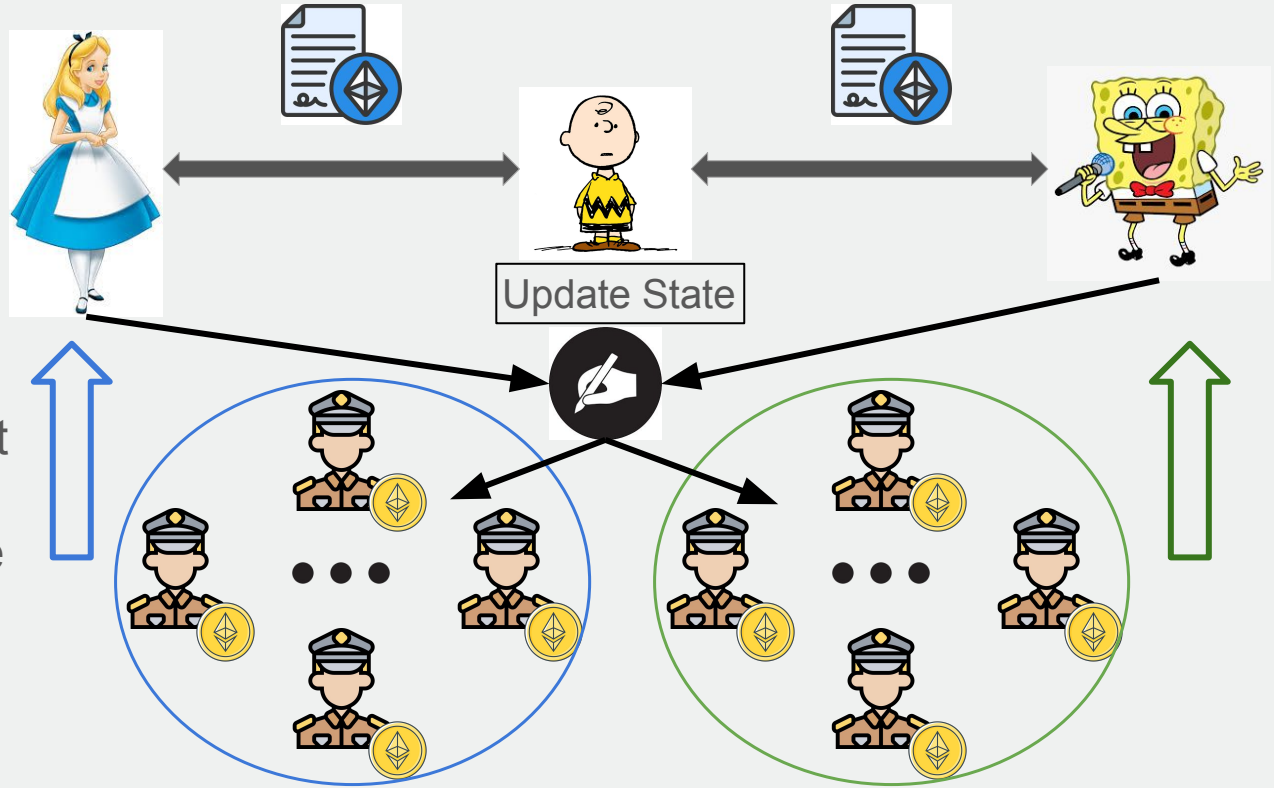
Timelock-free Payment Channel

- Warden (Watchtower)
  - n=3f+1, f are assumed to be **corrupted** (*Byzantine security*)
  - Deposit **collateral** in the payment channel (*Rational security*)
  - Responsive & monitor the blockchain

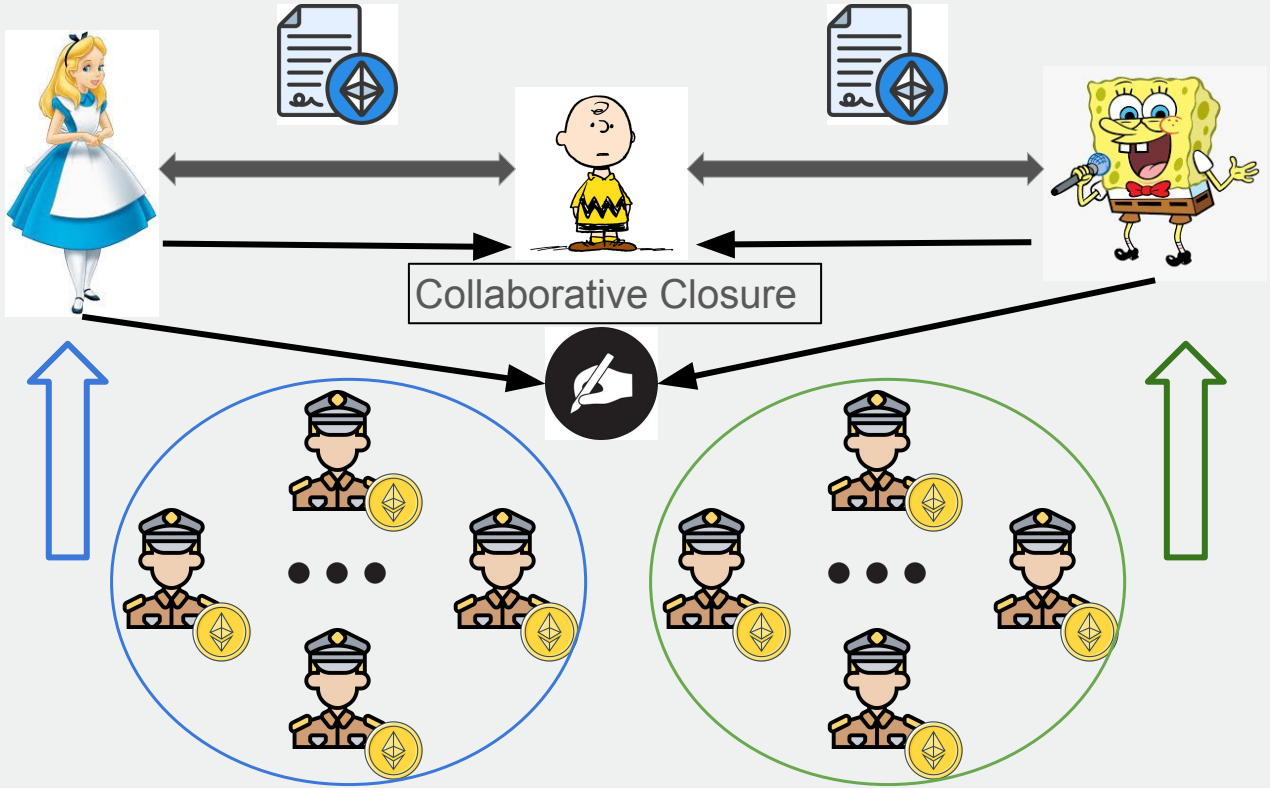
Overview of Thunderdome



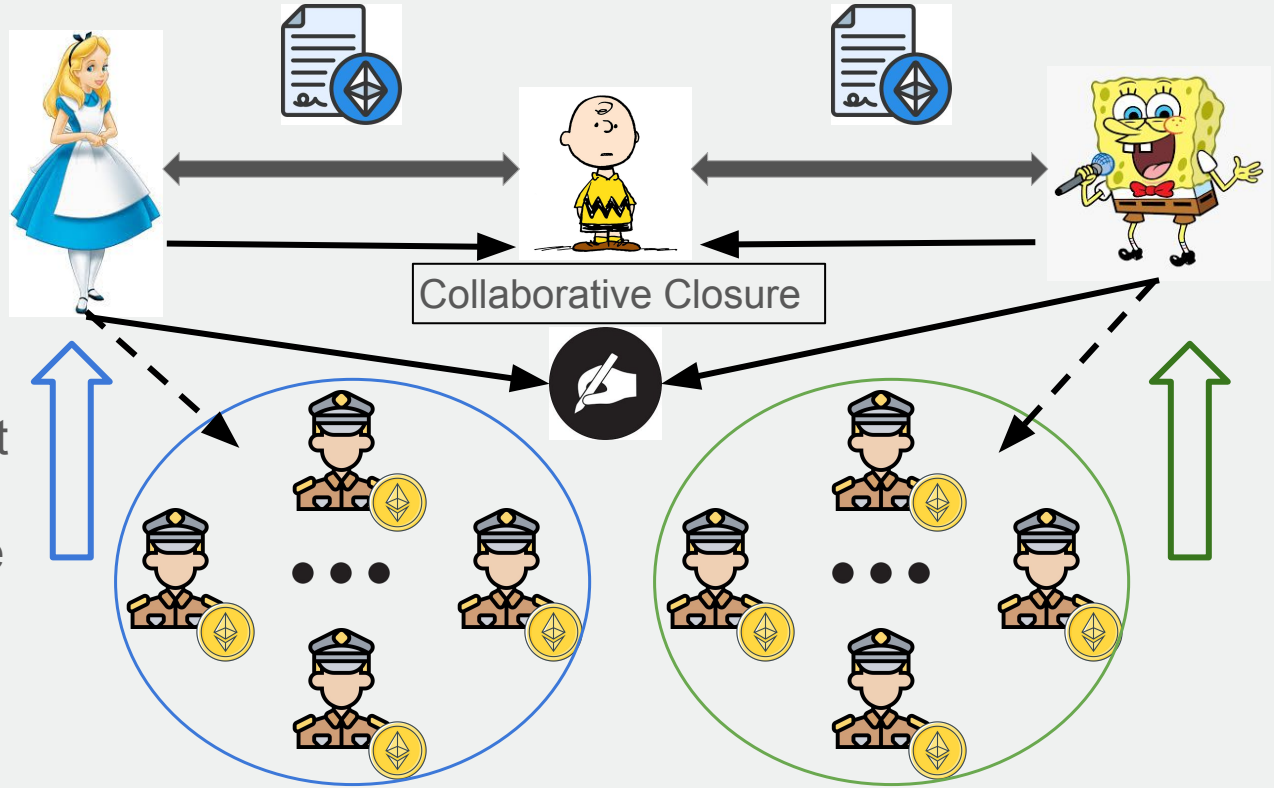
Overview of Thunderdome



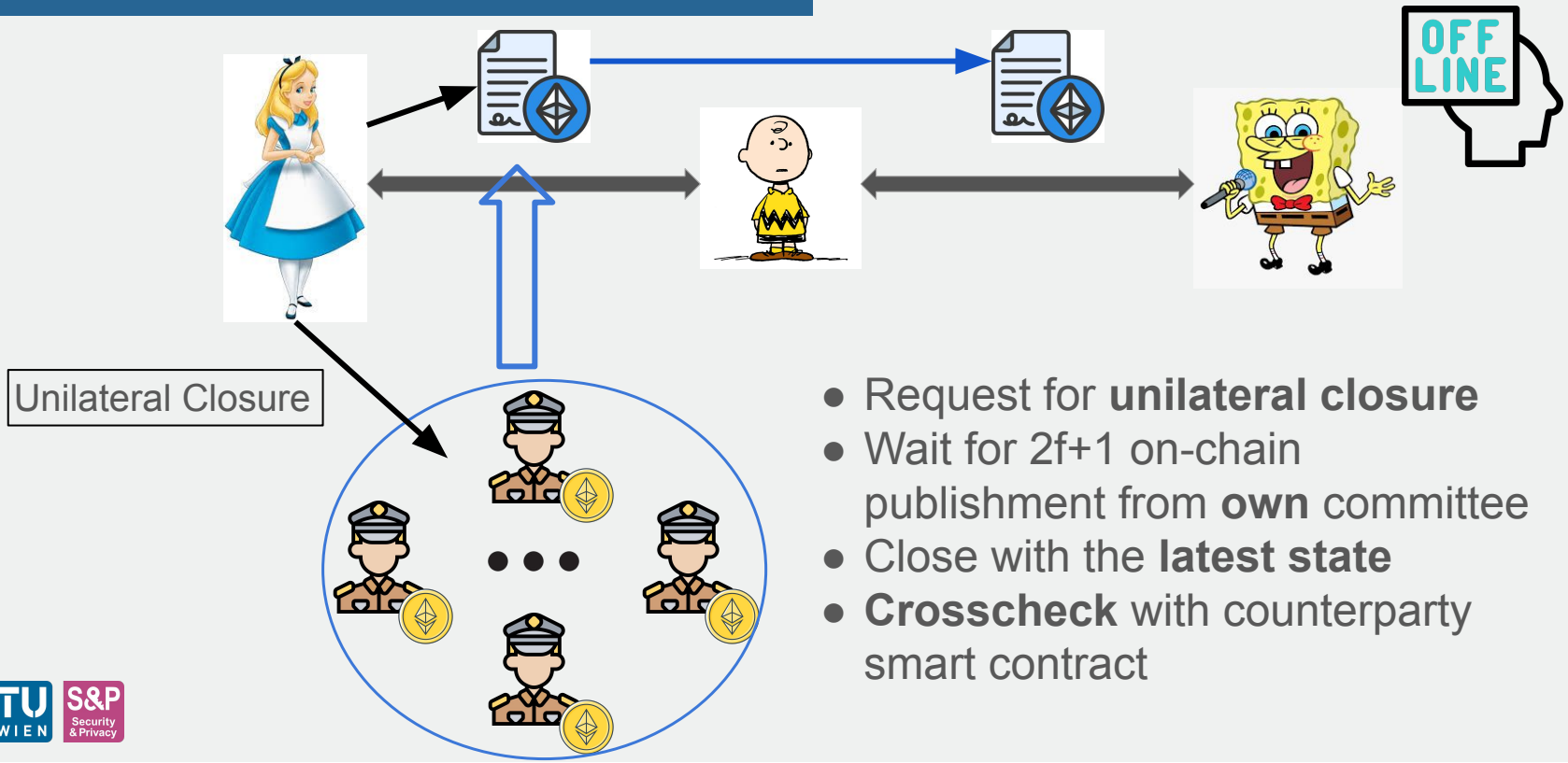
Overview of Thunderdome



Overview of Thunderdome



Overview of Thunderdome



- Request for **unilateral closure**
- Wait for 2f+1 on-chain publishment from **own** committee
- Close with the **latest state**
- **Crosscheck** with counterparty smart contract

Security Analysis

- Byzantine Security Model
  - Main Parties: Among Alice, Bob and Charlie, there should be **at most two parties** are corrupted.
  - Wardens: **No more than *f*** wardens are corrupted.

Security Analysis

- Byzantine Security Model
  - Main Parties: Among Alice, Bob and Charlie, there should be **at most two parties** are corrupted.
  - Wardens: **No more than *f*** wardens are corrupted.

Theorem 1 (Balance security).
Thunderdome achieves balance security for honest parties under asynchrony, assuming at most *f* Byzantine wardens in each committee.

Theorem 2 (Liveness).
Thunder dome achieves liveness for honest parties under asynchrony, assuming at most *f* Byzantine wardens in each committee.

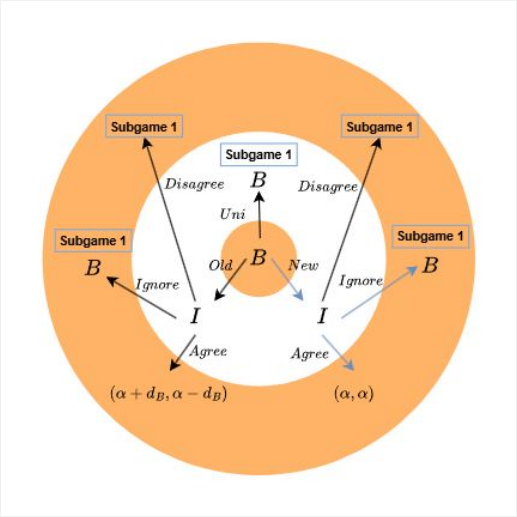
Security Analysis

- Rational Security Model
  - All participants are assumed to be **rational.**
  - Model the protocol into **Extensive Form Game (EFG)**

Security Analysis

- Rational Security Model
  - All participants are assumed to be **rational.**
  - Model the protocol into **Extensive Form Game (EFG)**

Theorem 3 (Rational security).
Rational main parties will open, update and close Thunderdome correctly.



Bob starts the closure

Implementation & Evaluation

	On-chain transaction	off/on-chain message			Thunderdome Cost			Perun Cost		
		Alice (Bob)	Ingrid	Warden (10)	Gas	ETH	USD	Gas	ETH	USD
Deploy & Open PC	2+10	1+10 / 1	1+10 / 1	$14 \leq m \leq 20$ / 10	4444861	0.0089	14.83	2819448	0.0057	9.54
Update PC	0	1+10 / 0	1+10 / 0	$14 \leq m \leq 20$ / 0	0	0	0	0	0	0
Open VC	0	3+30 / 0	2+40 / 0	$35 \leq m \leq 50$ / 0	0	0	0	0	0	0
Update VC	0	1+20 / 0	0 / 0	$14 \leq m \leq 20$ / 0	0	0	0	0	0	0
Optimistic VC close	0	1+10 / 0	1+10 / 0	$14 \leq m \leq 20$ / 0	0	0	0	0	0	0
Optimistic PC close	2	1 / 1	1 / 1	0 / 0	252760	0.0005	0.84	147788	0.0003	0.49
Pessimistic VC close by Alice	$2+7 \leq m \leq 2+10$	0 / 2	0 / 0	$0 / 7 \leq m \leq 10$	1217307	0.0024	4.06	418318	0.0008	1.40
Pessimistic PC close by Alice	$1+7 \leq m \leq 1+10$	0 / 1	0 / 0	$0 / 7 \leq m \leq 10$	862459	0.0017	2.88	275049	0.0006	0.92

[3] Stefan Dziembowski, Lisa Eckey, Sebastian Faust, and Daniel Malinowski. *Perun: Virtual payment hubs over cryptocurrencies.* In **2019 IEEE Symposium on Security and Privacy (S&P)**, pages 106–123. IEEE, 2019.

Extension

- **Privacy-preserving protocol**
  - Thunderdome does not protect the virtual channel information to wardens.
  - How to use wardens to guarantee correctness without leaking information.

- **Scaling the multi-hop protocol (more than 3)**
  - How to use less warden and less communication to scale the multi-hop protocol.

- **Extend to state channel**
  - Use Thunderdome to handle more complex execution in addition to payment.

Takeaways

- Virtual channel can works as a **“Layer 3”** and extends the ability of current Payment Channel Network.
- By leveraging **third-party entities** we are able to get rid of the reliance on **timelock** related design.
- **Extensive Form Game** can be useful when analyzing the **game-theoretic security** of Layer 2 protocol.

Thank You!

Questions?

Thunderdome: Timelock-Free Rationally-Secure Virtual Channels