Towards Building Secure and Efficient Decentralized Systems

Dr. Yuzhe Tang

EECS, Syracuse University

Towards Building Secure & Efficient **Decentralized Systems**

Modern infrastructures evolves to be more open and decentralized.

- Financial ledgers: blockchains
- Web infrastructures: transparency logs
- Cloud computing: decentralized storage

Towards Building Secure & Efficient **Decentralized Systems**

Intention of decentralization & open-membership designs:

- Trustworthy & more accountable

Towards Building **Secure** & Efficient Decentralized Systems

But two consequences of decentralized & open systems:

- Larger attack surface …

Towards Building **Secure** & Efficient Decentralized Systems

But two consequences of decentralized & open systems:

- Larger attack surface …

Theme 1: How to understand & harden security?

Towards Building Secure & **Efficient** Decentralized Systems

But two consequences of decentralized & open systems:

- Larger attack surface …

Theme 1: How to understand & harden security?

- Higher unit cost for basic operations …

Towards Building Secure & **Efficient** Decentralized Systems

But two consequences of decentralized & open systems:

- Larger attack surface …

Theme 1: How to understand & harden security?

- Higher unit cost for basic operations …

Theme 2: How to optimize the application cost?

Example Projects Presented in this Talk

- Theme 1: How to understand & harden the security in emerging large-scale systems?
    - Project P1: Securing blockchains under DoS vectors (CCS'21, NDSS'21, IMC'21)
- Theme 2: How to analyze & optimize perf./costs in security-centric large-scale systems?
    - Project P2: Cost-optimizing DApps without losing security (FSE'21, Middleware'20, ICDE'19)

Talk Outline

Project P1: Securing blockchains under DoS vectors

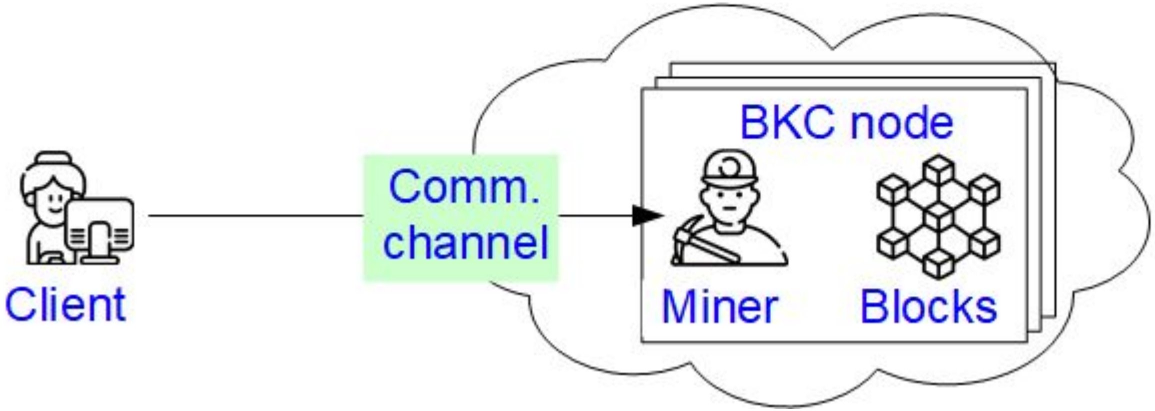
- RQ1: DoS security on TxRelay (published in NDSS’21)
- RQ2: DoS security on Tx propagation (ACM IMC’21)
- RQ3: DoS security on Mempool (ACM CCS’21)

Project P2: Optimizing the DApp cost without losing security

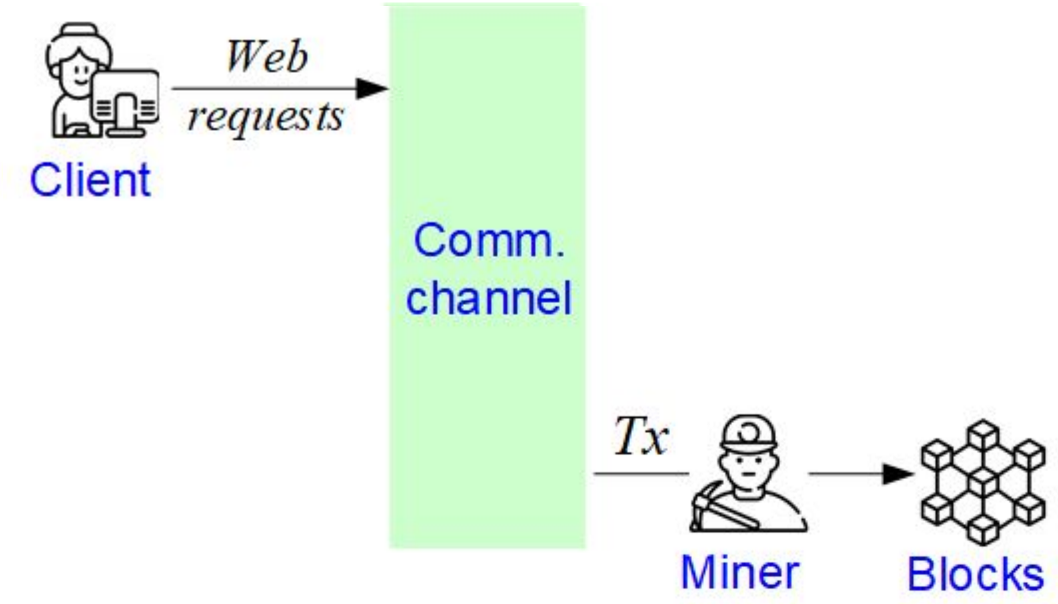
Overview of Other Research Projects

Future Research Directions

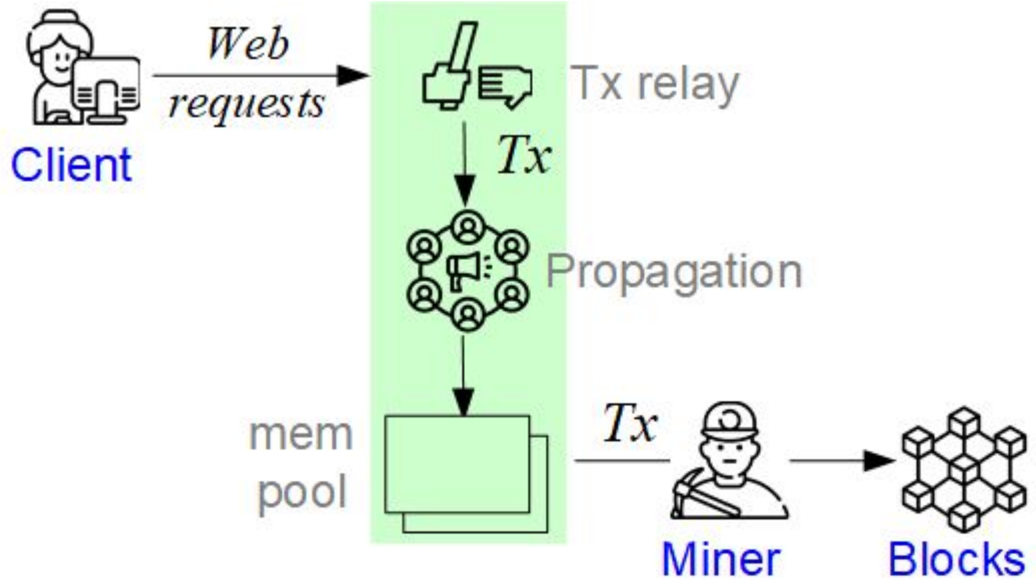
P1: Blockchain Security under DoS



P1: Blockchain Security under DoS



P1: Blockchain Security under DoS



P1: Blockchain Security under DoS

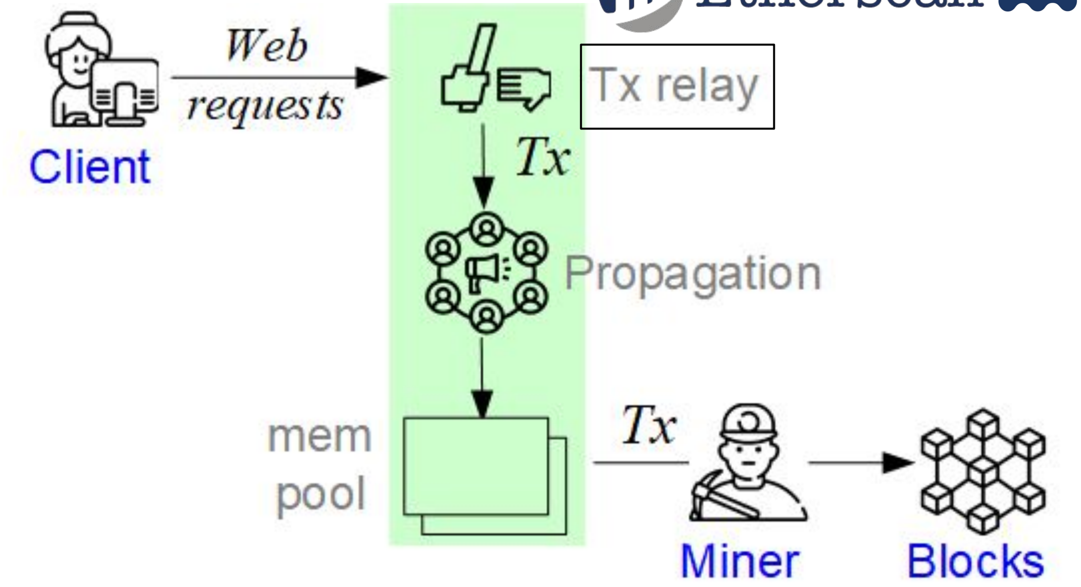
INFURA

QuikNode

BLOCKDAEMON

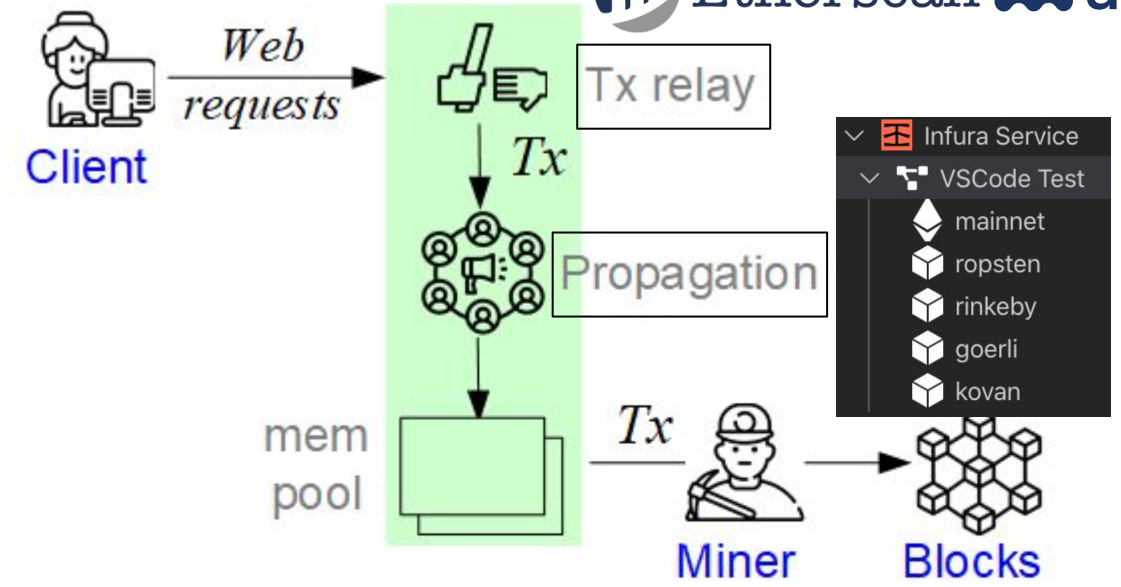
Etherscan

amberdata



P1: Blockchain Security under DoS

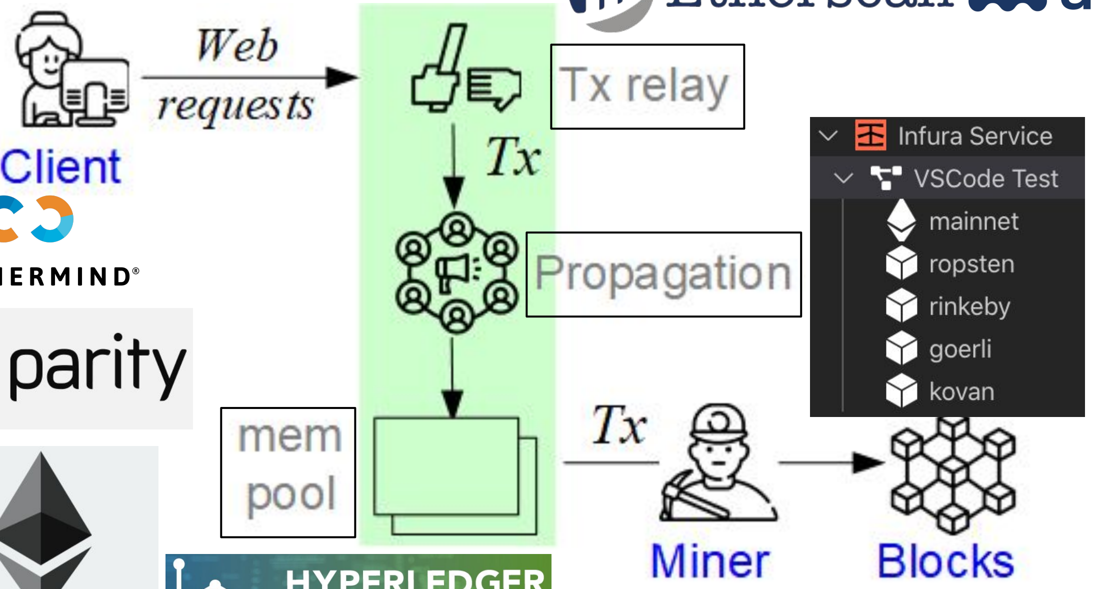
INFURA QuikNode BLOCKDAEMON Etherscan amberdata



Infura Service
- VSCode Test
  - mainnet
  - ropsten
  - rinkeby
  - goerli
  - kovan

P1: Blockchain Security under DoS

INFURA QuikNode BLOCKDAEMON Etherscan amberdata



Infura Service
VSCode Test
mainnet
ropsten
rinkeby
goerli
kovan

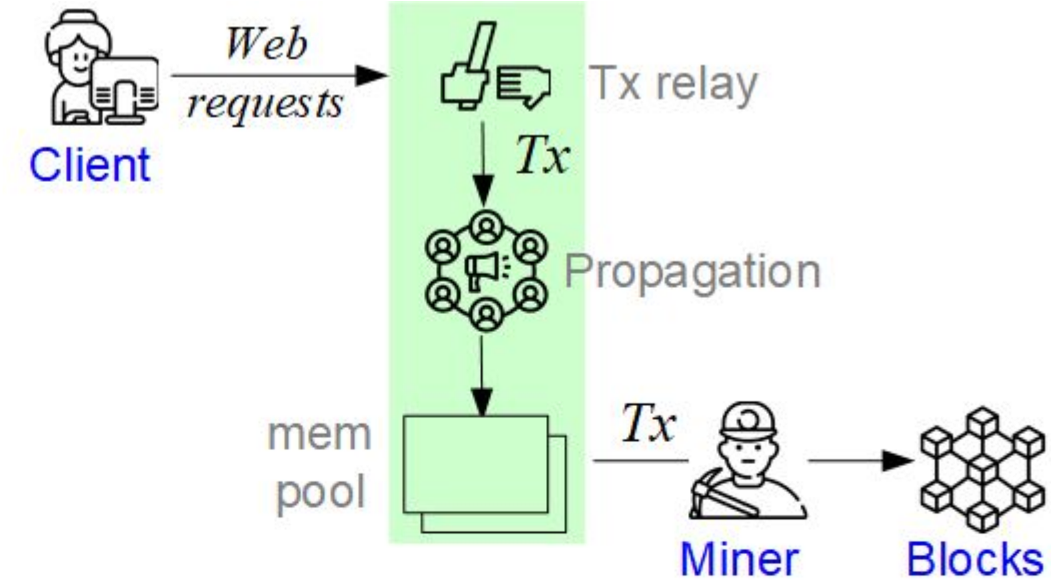
NETHERMIND®

parity

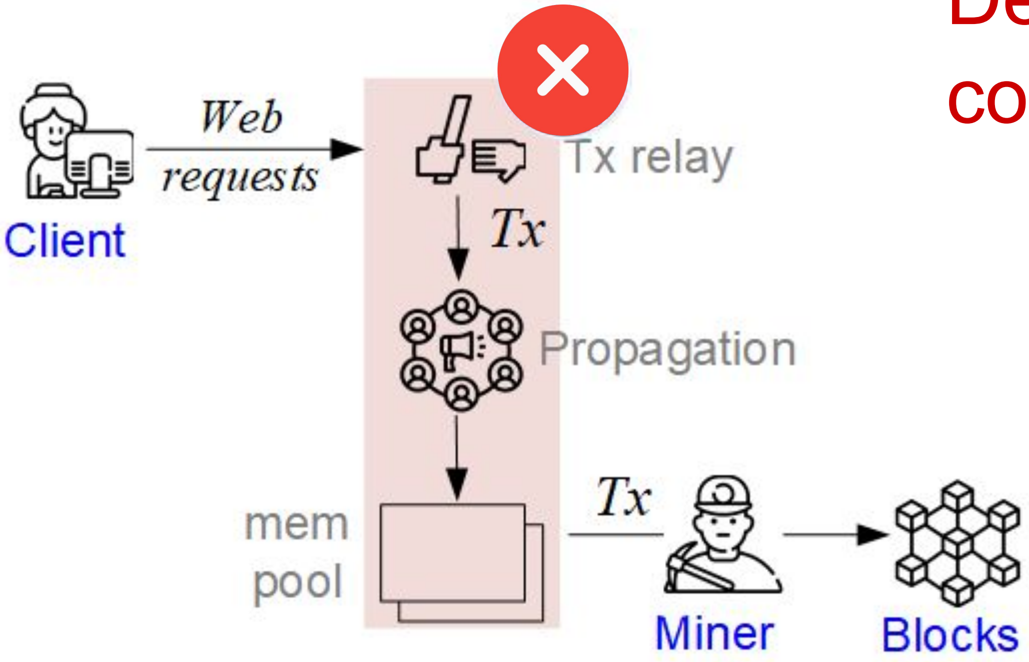
Go Ethereum

HYPERLEDGER BESU

P1: Blockchain Security under DoS

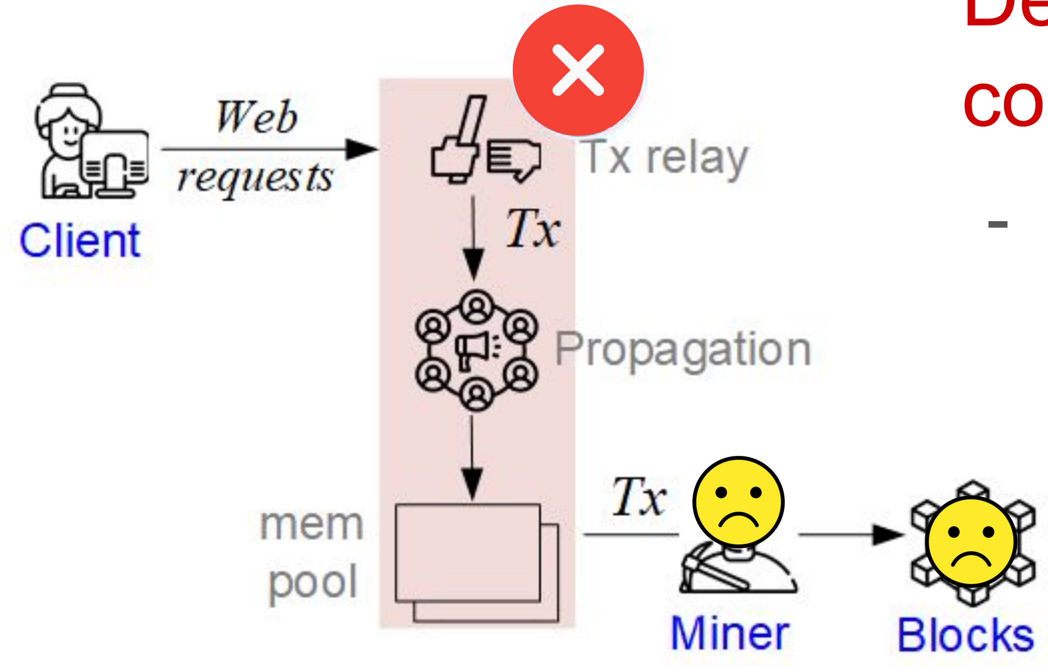


P1: Blockchain Security under DoS



Denial of Blockchain comm. channel service?

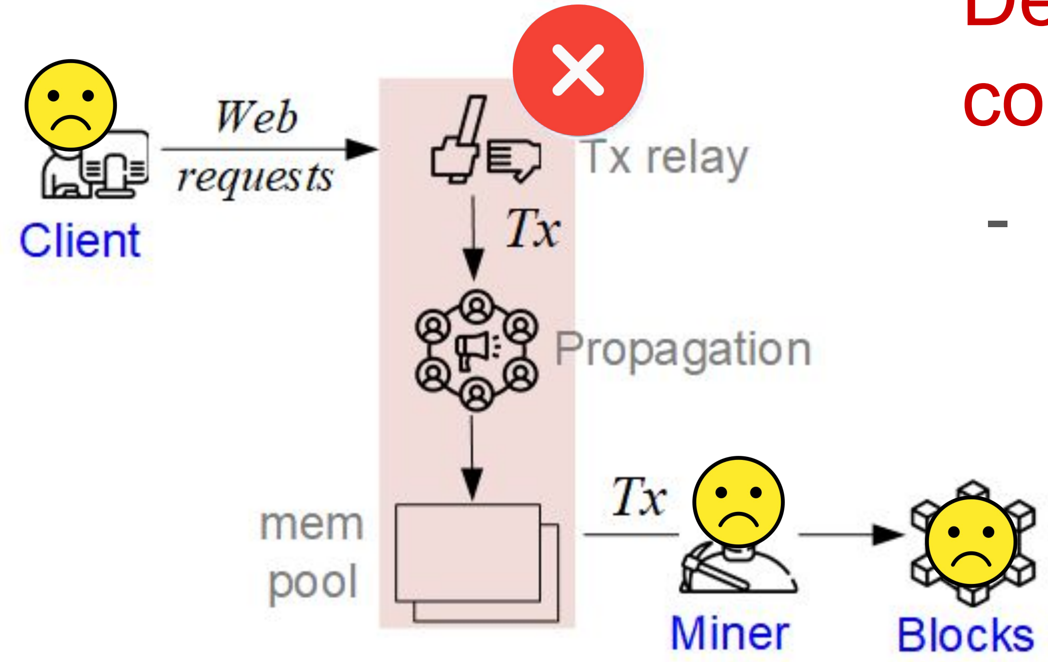
P1: Blockchain Security under DoS



Denial of Blockchain comm. channel service?

- Miner unable to include txs; empty blocks.
  - low revenue, lose miners, 51% attacks

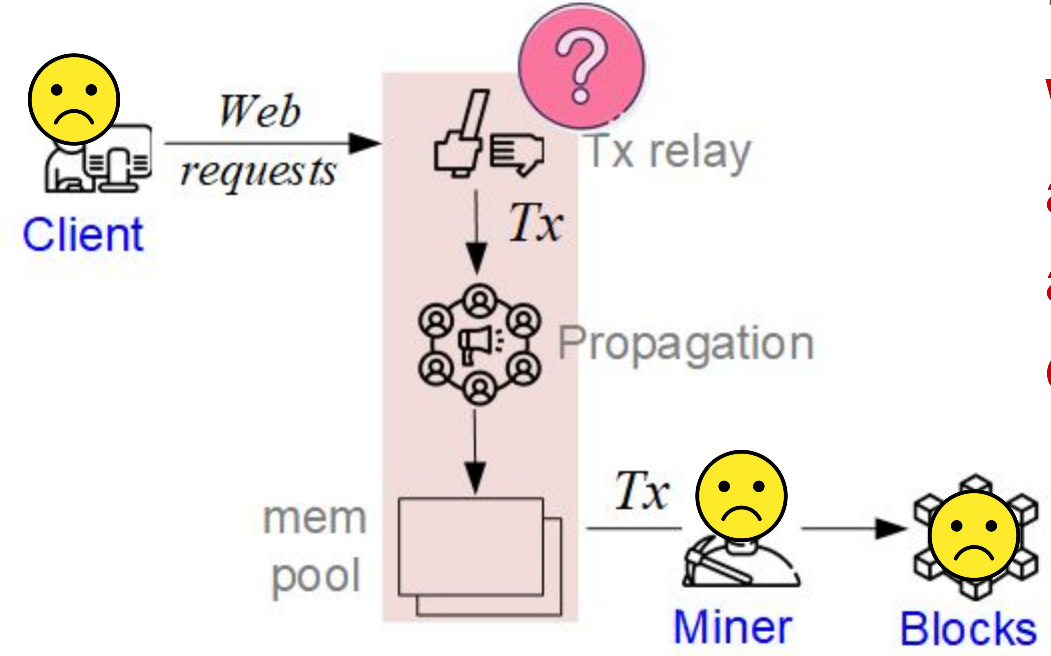
P1: Blockchain Security under DoS



Denial of Blockchain comm. channel service?

- Miner unable to include txs; empty blocks.
  - low revenue, lose miners, 51% attacks
- Clients cannot send txs.
  - Frontrunning, lose clients

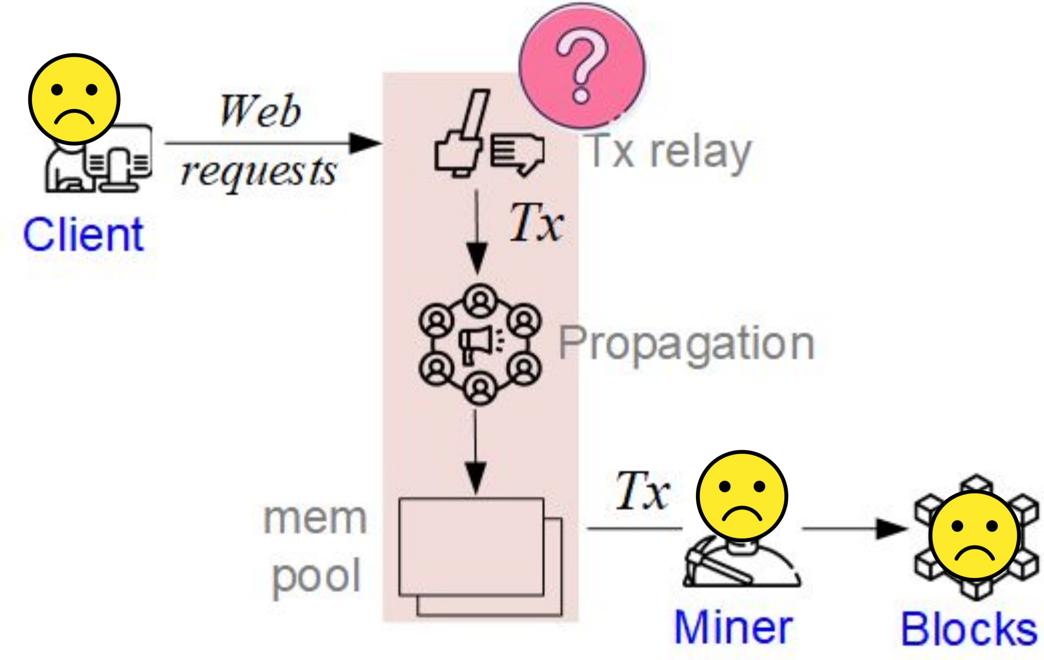
P1: Blockchain Security under DoS



Research statement:

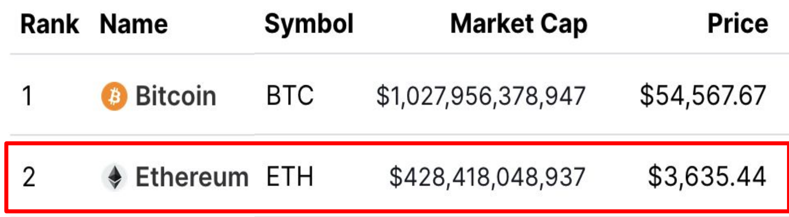
Whether & how resilient are Ethereum blockchains against denial of comm. channel service?

P1: Blockchain Security under DoS



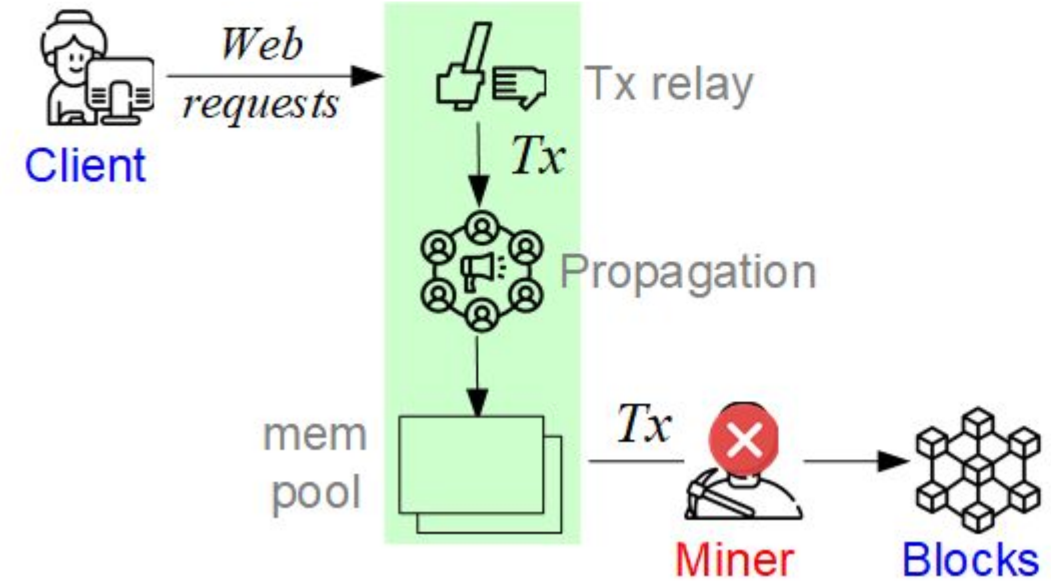
Research statement:

Whether & how resilient are Ethereum blockchains against denial of comm. channel service?



Rank	Name	Symbol	Market Cap	Price
1	Bitcoin	BTC	$1,027,956,378,947	$54,567.67
2	Ethereum	ETH	$428,418,048,937	$3,635.44

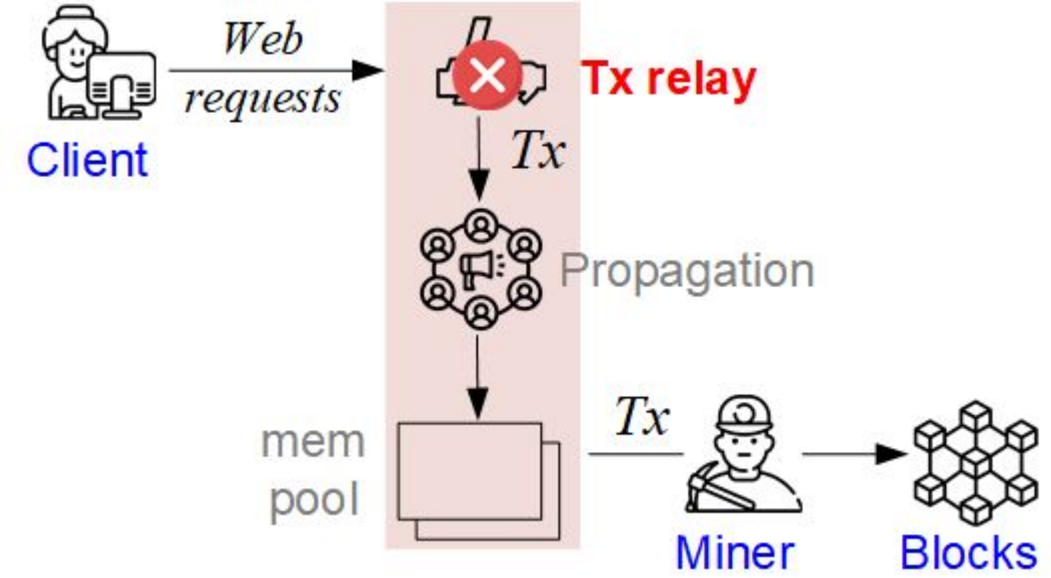
P1: Blockchain Security under DoS: Related Works

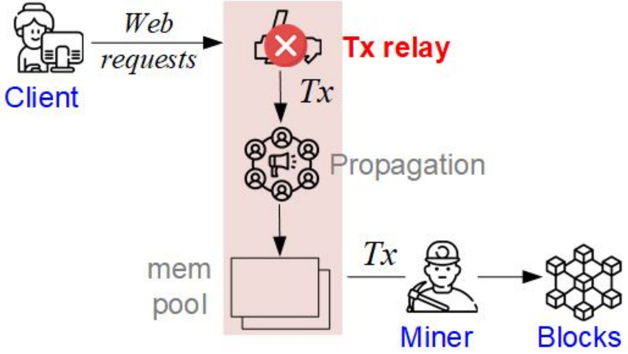


Existing works

- BDoS (CCS'20), selfish mining (FC'14), 51% attacks
- Smart-contract DoS (NDSS'20), Bribery (SP'21)

RQ1. Blockchain Security under DoS Tx Relay

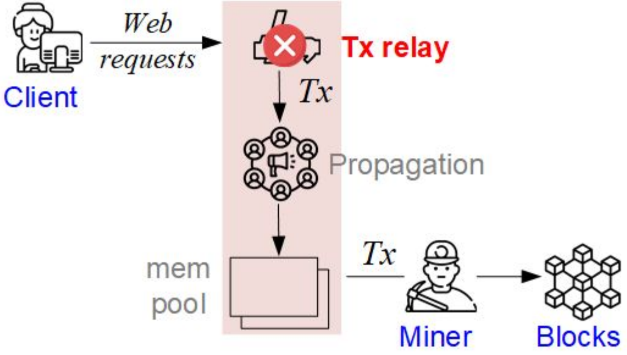




RQ1. Security under DoS Tx Relay

Formulated problem:

- Observe a vulnerable relay API (eth_call)
- If exposed, straightforward DoS exploiting eth_call



RQ1. Security under DoS Tx Relay

Formulated problem:

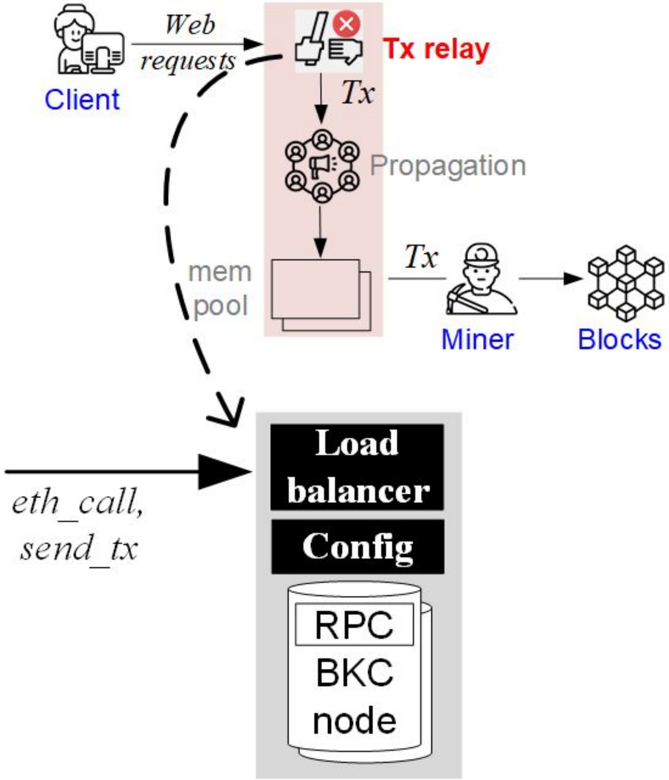
- Observe a vulnerable relay API (eth_call)
- If exposed, straightforward DoS exploiting eth_call

RQ1 (Exploitability measurement): Under the DoS exploiting the vulnerable API, how exploitable are real-world blackbox relay services are?

RQ1. Security under DoS Tx Relay

Proposed method (intuition)

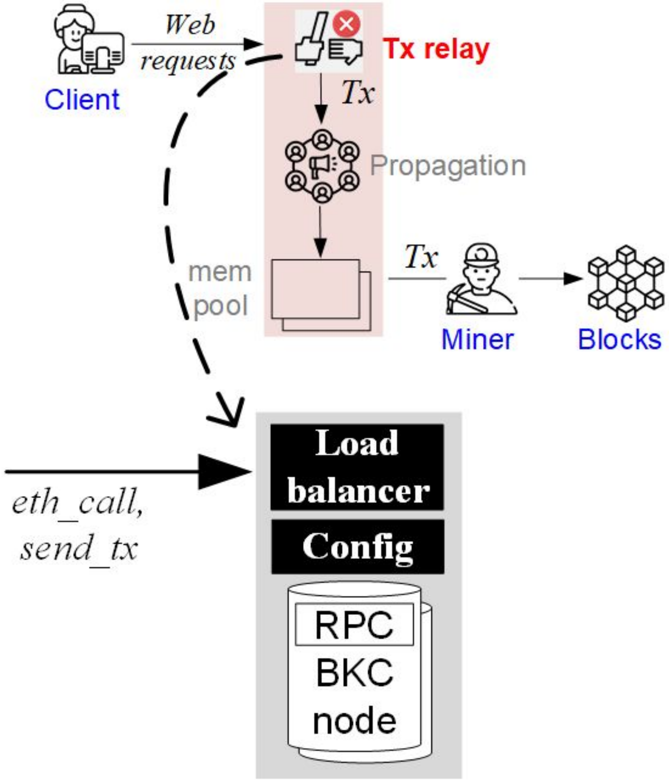
- Detect presence of load balancing inside tx relay services.



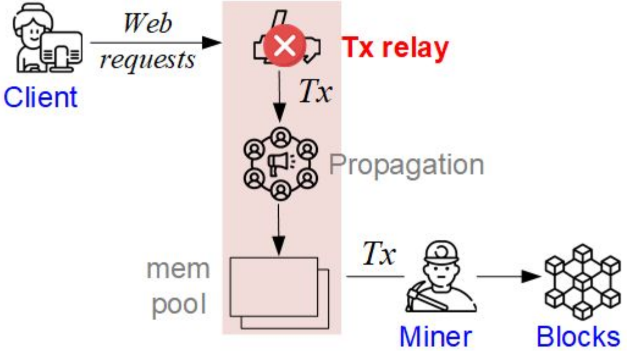
RQ1. Security under DoS Tx Relay

Proposed method (intuition)

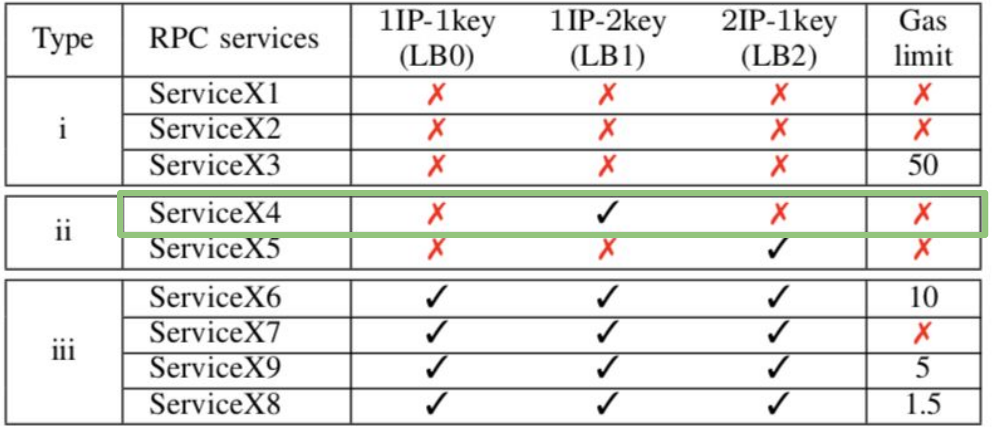
- Detect presence of load balancing inside tx relay services.
- Send two double-spending txs to a RPC service & observe if both requests succeed.
  - Both requests succeed ⇒ load balancing detected.
  - One request fail ⇒ No load balancing detected.



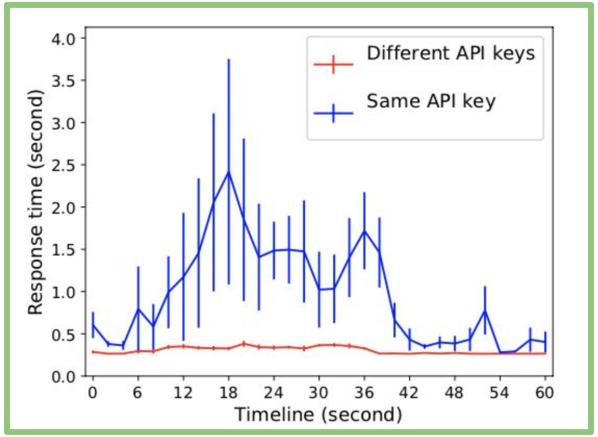
RQ1. Security under DoS Tx Relay



Results: on mainnet services

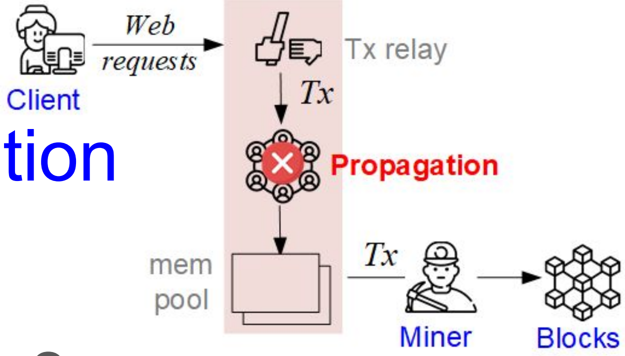


Type	RPC services	1IP-1key (LB0)	1IP-2key (LB1)	2IP-1key (LB2)	Gas limit
i	ServiceX1	✗	✗	✗	✗
	ServiceX2	✗	✗	✗	✗
	ServiceX3	✗	✗	✗	50
ii	ServiceX4	✗	✓	✗	✗
	ServiceX5	✗	✗	✓	✗
iii	ServiceX6	✓	✓	✓	10
	ServiceX7	✓	✓	✓	✗
	ServiceX9	✓	✓	✓	5
	ServiceX8	✓	✓	✓	1.5



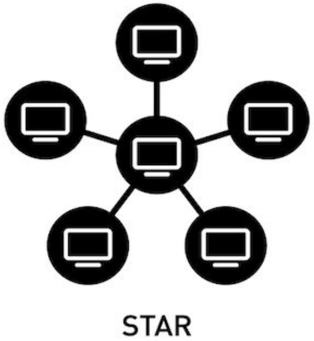
Publication: **NDSS 2021**

"As Strong As the Weakest Link: How to Break and Fix Blockchain DApps at RPC Service?"
Kai Li, Jiaqi Chen, Xianghong Liu, Yuzhe Tang, XiaoFeng Wang, Xiapu Luo.

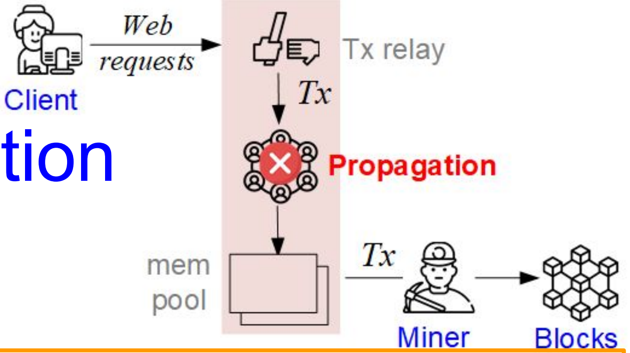


RQ2. Security under DoS Tx Propagation

Motivation: How resilient is Ethereum's Tx Propagation under single-point-of-failure?



- Single-point-of-failure by existing single-node attacks (e.g., eclipse attacks, DoERS, DETER)



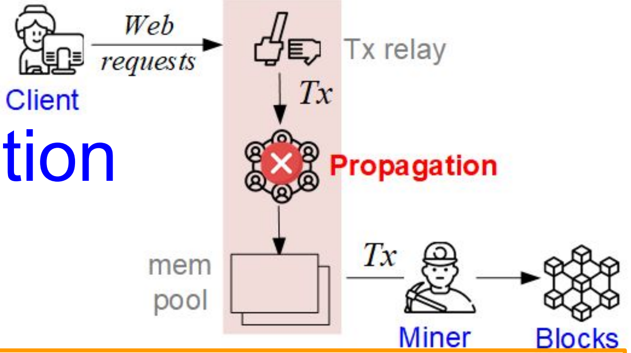
RQ2. Security under DoS Tx Propagation

Formulated problem:

RQ2 (Network measurement): What's Ethereum's network topology?

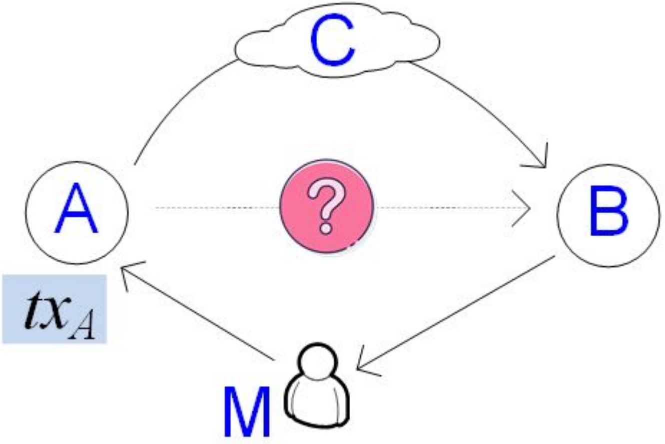
Related works	**Blockchain**	**Measurement Target**
[Neudecker et al. TR'18]	Bitcoin	Nodes
*[Miller et al. TR'**15**], [IEEE ATC'16], TxProbe [FC'19]*	Bitcoin	Edges
[FC'20]	Monero	Edges
[IMC'18], [FC'21]	Ethereum	Nodes
?	**Ethereum**	**Edges**

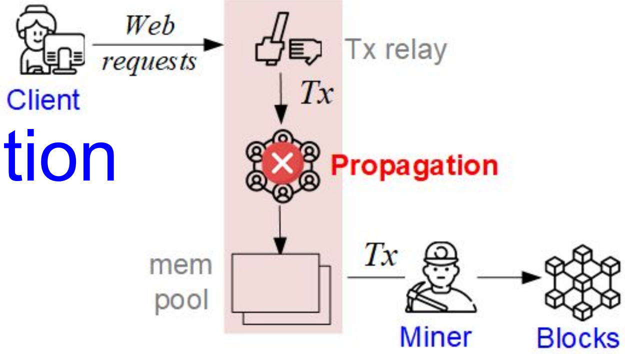
RQ2. Security under DoS Tx Propagation



Formulated problem:

RQ2 (Network measurement):
How to measure if remote Ethereum nodes (A & B) are connected?

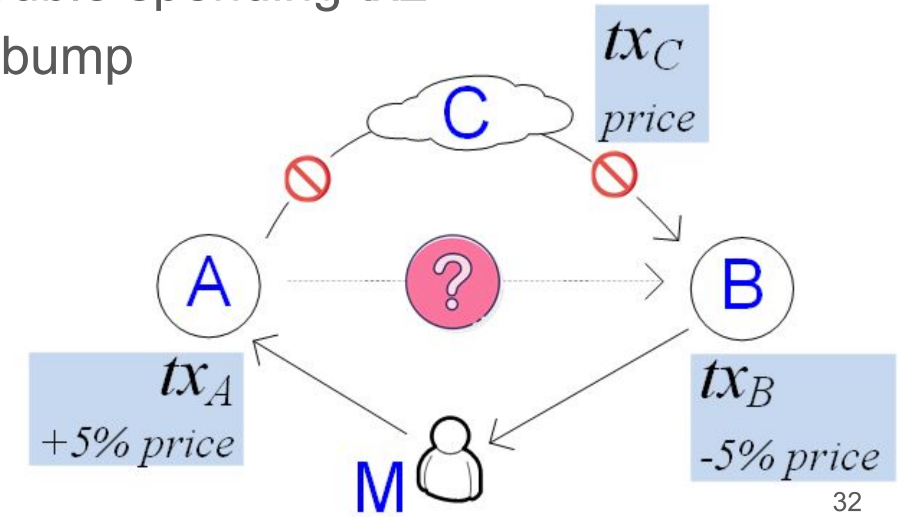


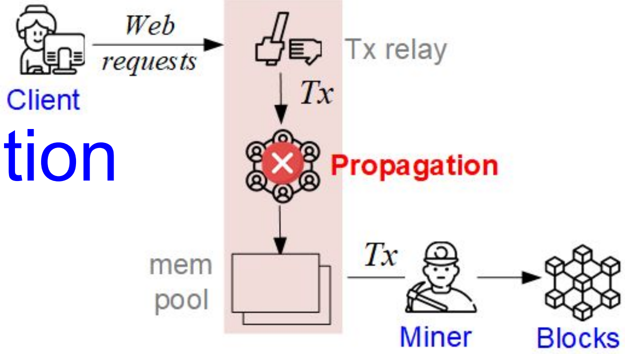


RQ2. Security under DoS Tx Propagation

Proposed method (intuition)

- Preliminary: tx replacement policies
  - Old tx1 replaced by a newer, double spending tx2 if tx2 has sufficient (10%) price bump
- Key insight:
  - Price bump & future txs to enforce isolation.

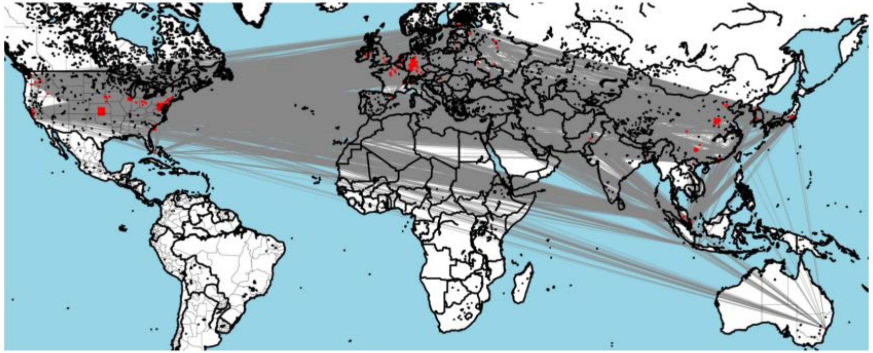




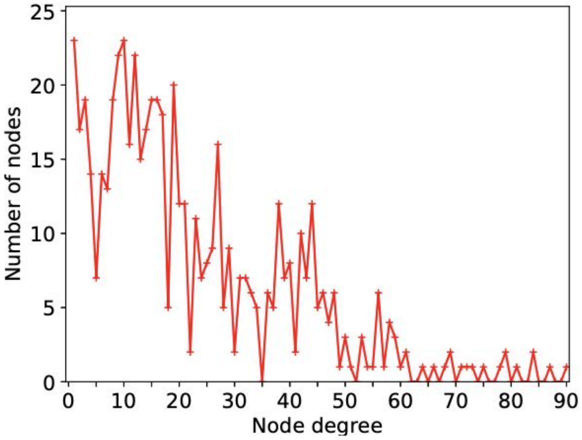
RQ2. Security under DoS Tx Propagation

Results: Full-network topology in testnets

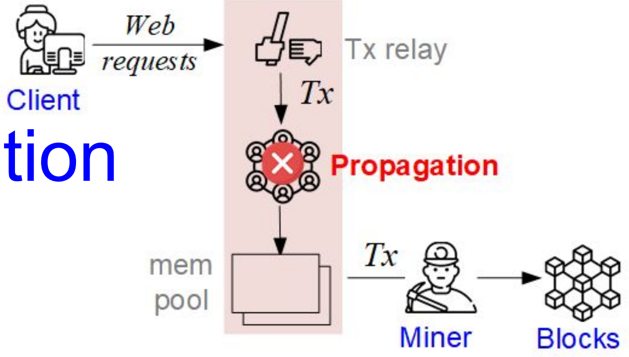
- Lower modularity & fewer cliques than random graphs
- Resilient to single-point-of-failure, but unsecure for low-degree nodes



(b) Geo distribution of Rinkeby



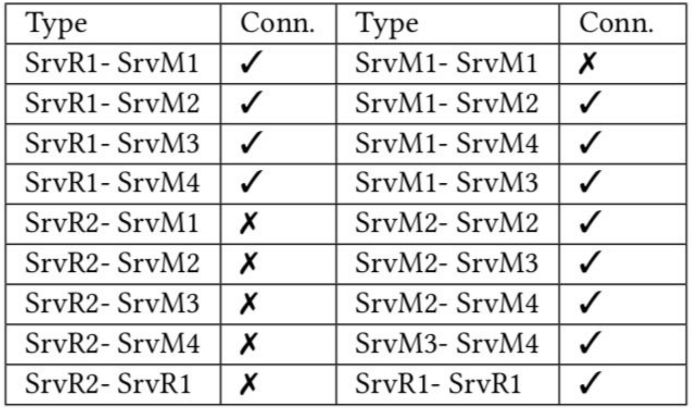
RQ2. Security under DoS Tx Propagation



Results: Critical-node subnet in mainnet

- Biased node connections towards popular services

Table 6: Connections among critical nodes



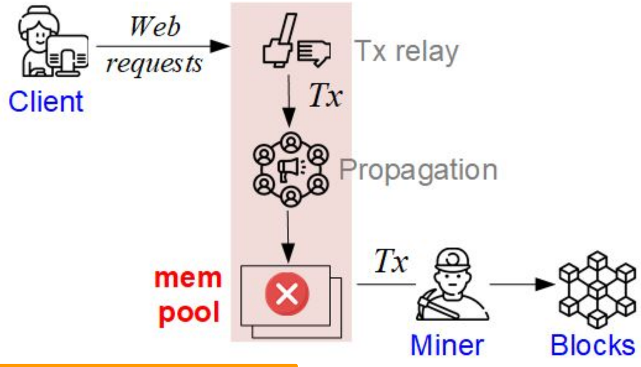
Type	Conn.	Type	Conn.
SrvR1- SrvM1	✓	SrvM1- SrvM1	✗
SrvR1- SrvM2	✓	SrvM1- SrvM2	✓
SrvR1- SrvM3	✓	SrvM1- SrvM4	✓
SrvR1- SrvM4	✓	SrvM1- SrvM3	✓
SrvR2- SrvM1	✗	SrvM2- SrvM2	✓
SrvR2- SrvM2	✗	SrvM2- SrvM3	✓
SrvR2- SrvM3	✗	SrvM2- SrvM4	✓
SrvR2- SrvM4	✗	SrvM3- SrvM4	✓
SrvR2- SrvR1	✗	SrvR1- SrvR1	✓

- Centralization leads to risks

Publication: **ACM IMC 2021**

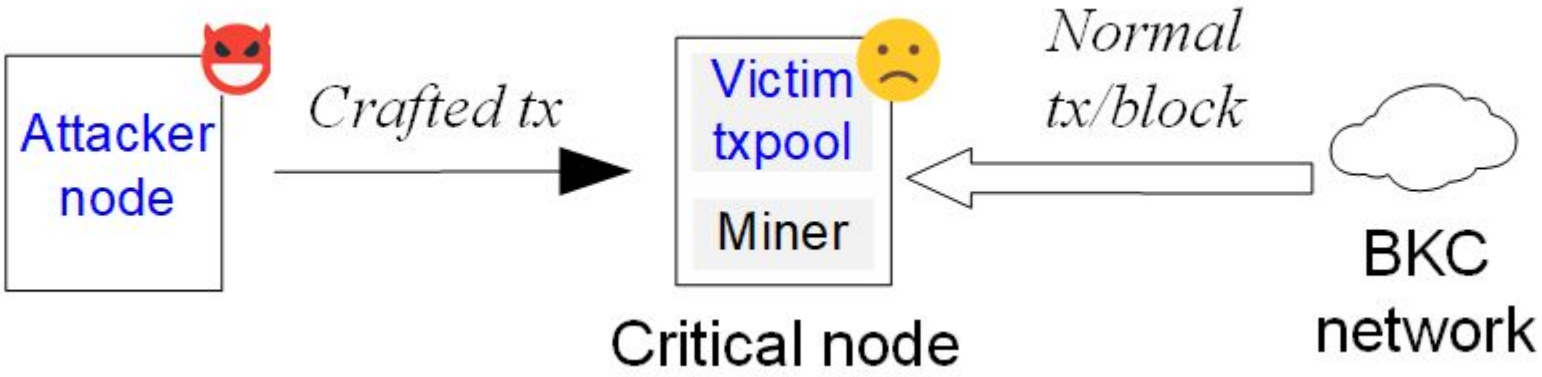
TopoShot: Uncovering Ethereum's Network Topology Leveraging Replacement Transactions.
Kai Li, Yuzhe Tang, Jiaqi Chen, Yibo Wang, Xianghong Liu

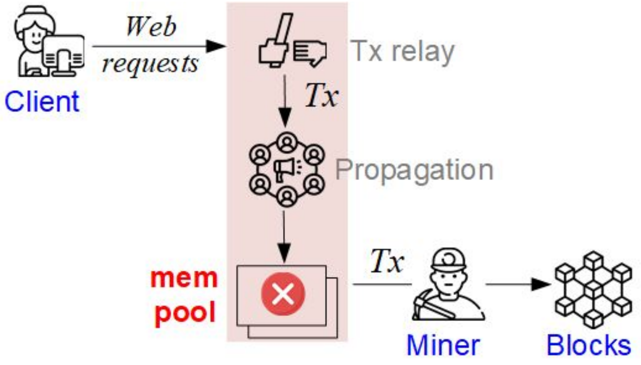
RQ3. Security under DoS Mempool



Formulated problem:

RQ3 (Attack design): Whether possible and how to spam a remote mempool at low cost?

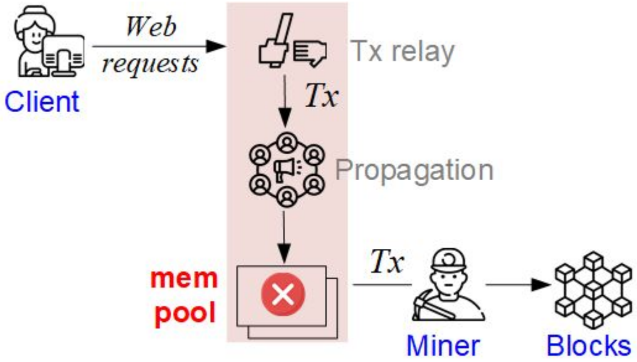




RQ3. Security under DoS Mempool

Proposed method (intuition):

- Exploit the design flaw in auction-based tx admission.
  - Ethereum uses auction to determine tx admission priority.
    - Necessary to mitigate spamming (Bitcoin16)
  - Protocol level: Assume all txs are profitable…
  - Implementation level: False assumption!
    - Unconfirmed Ethereum txs are invalid and unprofitable.
- Idea: Send unprofitable and high-priced txs to occupy an Ethereum node’s mempool.

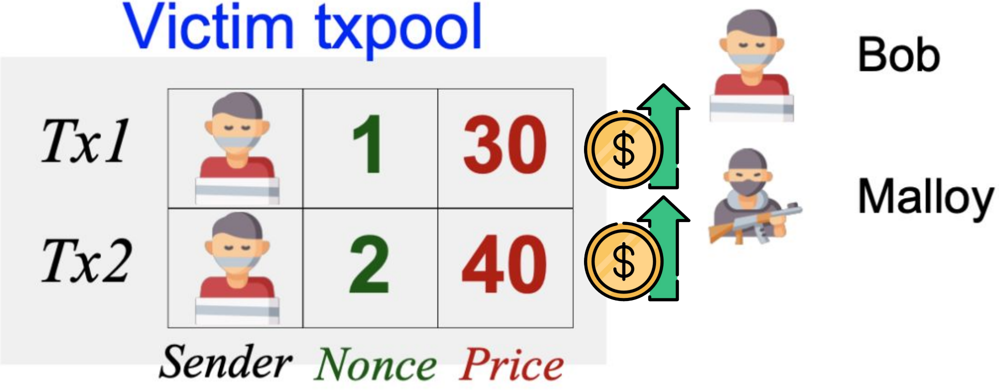


RQ3. Security under DoS Mempool

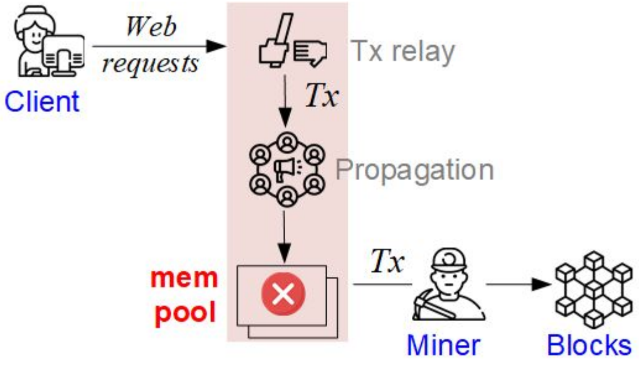
Proposed method (intuition): Attack

Attacker node

Victim txpool

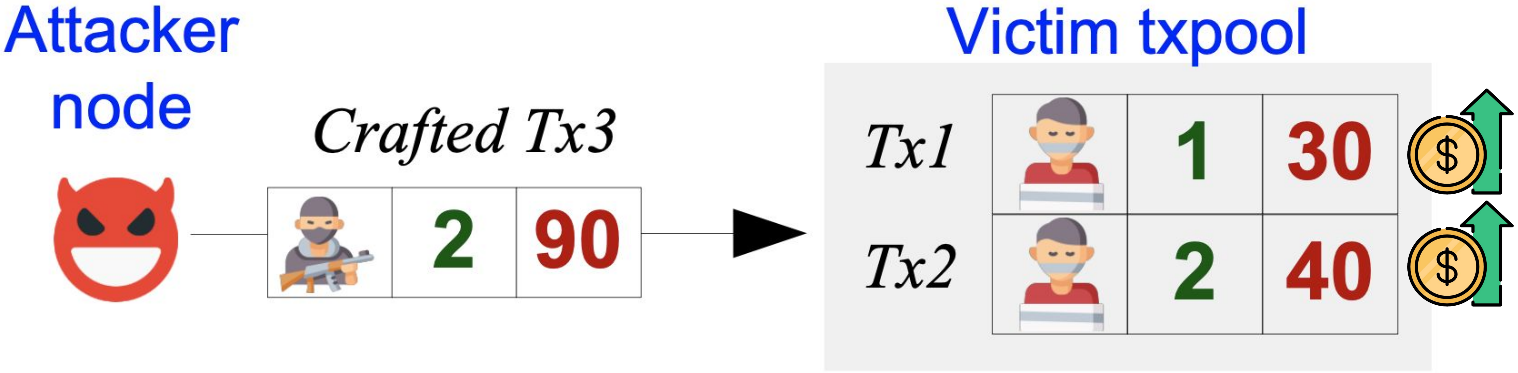


	Sender	Nonce	Price
Tx1		1	30
Tx2		2	40



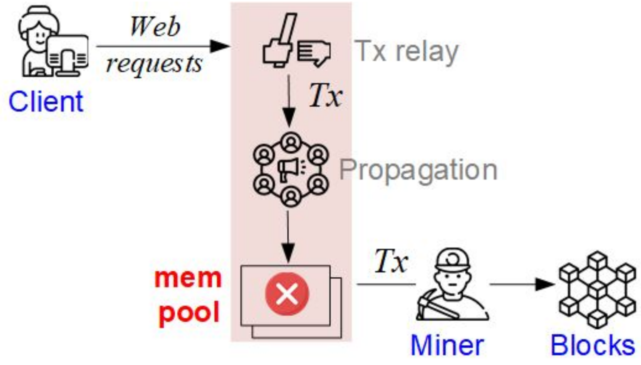
RQ3. Security under DoS Mempool

Proposed method (intuition): Attack



Crafted Tx3		2	90

Tx1		1	30
Tx2		2	40

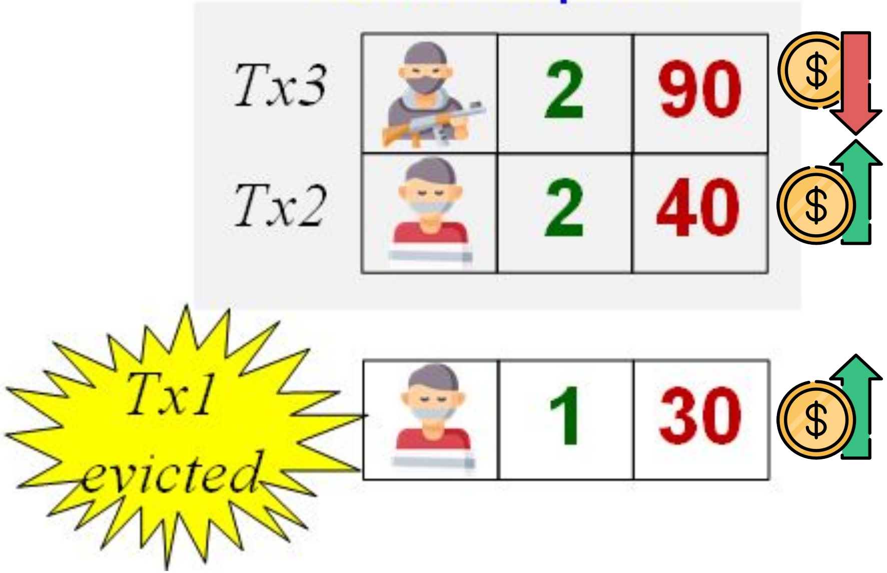


RQ3. Security under DoS Mempool

Proposed method (intuition): Attack

Attacker node

Victim txpool

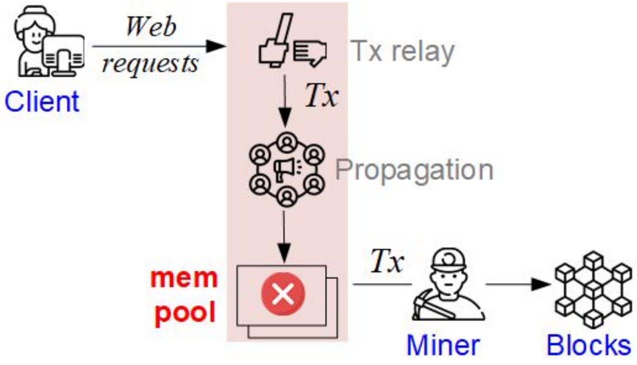


Tx3		2	90
Tx2		2	40
Tx1 evicted		1	30

admitting tx3 leads to

1. evict tx1

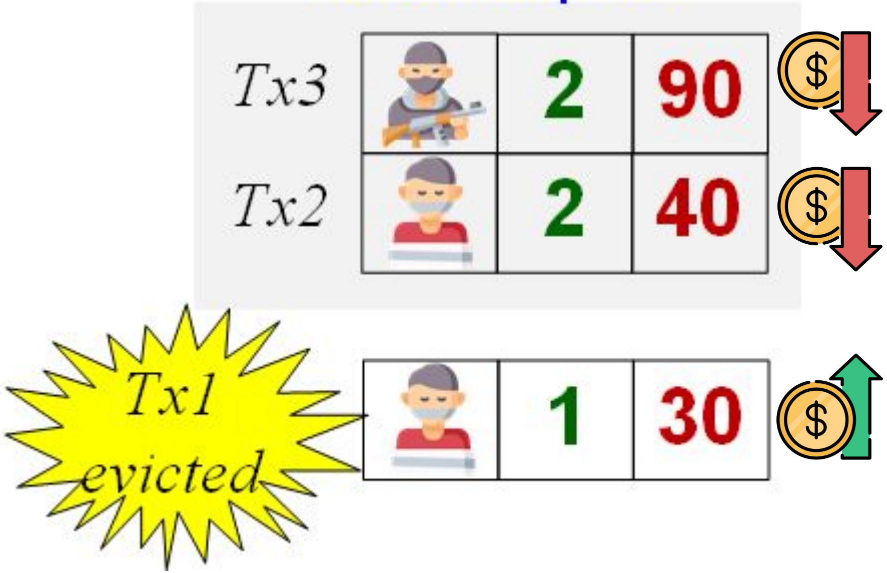
RQ3. Security under DoS Mempool



Proposed method (intuition): Attack

Attacker node

Victim txpool

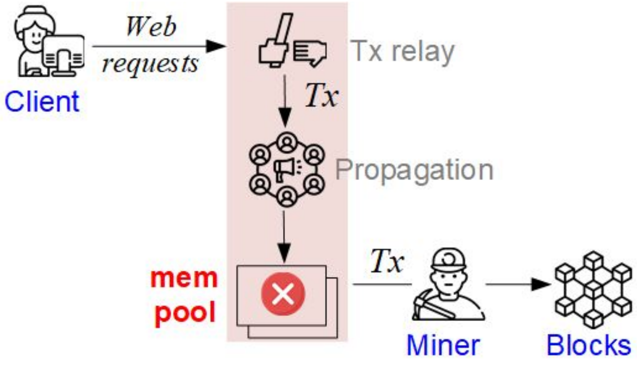


Tx3		2	90
Tx2		2	40
Tx1 evicted		1	30

admitting tx3 leads to

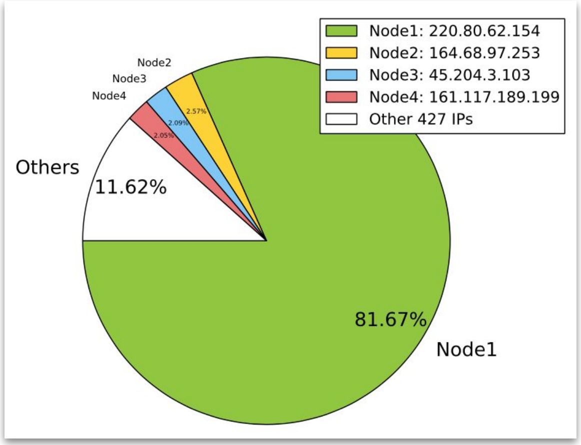
1. evict tx1
2. turn tx2 to future

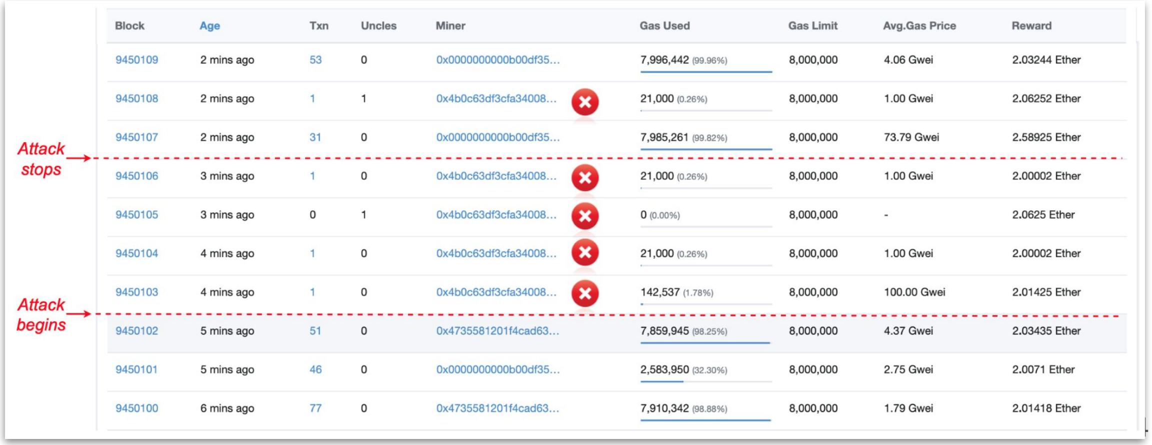
RQ3. Security under DoS Mempool



Results: Attack success & cost in testnets

- Launching two supernodes joining Ropsten testnets.
- Using the node discoverability method to discover top miners.



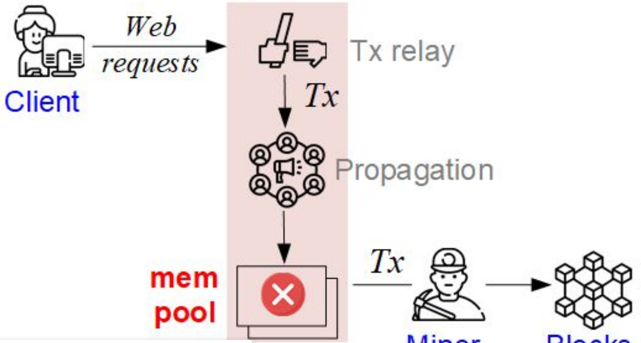


Block	Age	Txn	Uncles	Miner	Gas Used	Gas Limit	Avg.Gas Price	Reward
9450109	2 mins ago	53	0	0x0000000000b00df35...	7,996,442 (99.96%)	8,000,000	4.06 Gwei	2.03244 Ether
9450108	2 mins ago	1	1	0x4b0c63df3cfa34008... ✖	21,000 (0.26%)	8,000,000	1.00 Gwei	2.06252 Ether
9450107	2 mins ago	31	0	0x0000000000b00df35...	7,985,261 (99.82%)	8,000,000	73.79 Gwei	2.58925 Ether
9450106	3 mins ago	1	0	0x4b0c63df3cfa34008... ✖	21,000 (0.26%)	8,000,000	1.00 Gwei	2.00002 Ether
9450105	3 mins ago	0	1	0x4b0c63df3cfa34008... ✖	0 (0.00%)	8,000,000	-	2.0625 Ether
9450104	4 mins ago	1	0	0x4b0c63df3cfa34008... ✖	21,000 (0.26%)	8,000,000	1.00 Gwei	2.00002 Ether
9450103	4 mins ago	1	0	0x4b0c63df3cfa34008... ✖	142,537 (1.78%)	8,000,000	100.00 Gwei	2.01425 Ether
9450102	5 mins ago	51	0	0x4735581201f4cad63...	7,859,945 (98.25%)	8,000,000	4.37 Gwei	2.03435 Ether
9450101	5 mins ago	46	0	0x0000000000b00df35...	2,583,950 (32.30%)	8,000,000	2.75 Gwei	2.0071 Ether
9450100	6 mins ago	77	0	0x4735581201f4cad63...	7,910,342 (98.88%)	8,000,000	1.79 Gwei	2.01418 Ether

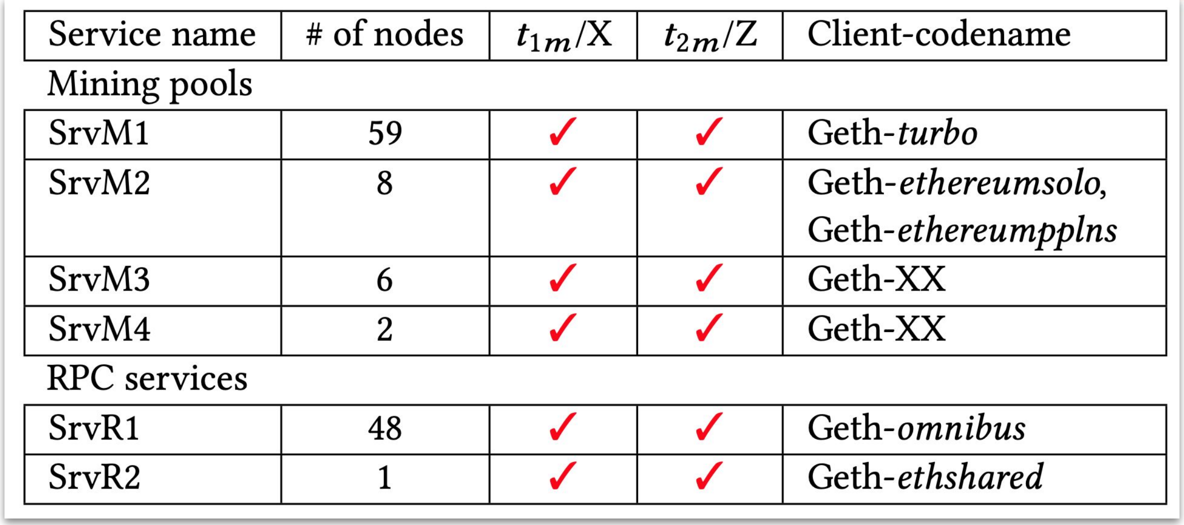
Attack stops

Attack begins

RQ3. Security under DoS Mempool



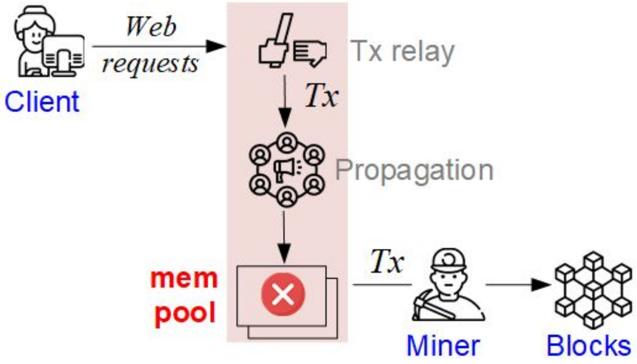
Results: Exploitability probes in mainnet



Service name	# of nodes	t_{1m}/X	t_{2m}/Z	Client-codename
Mining pools				
SrvM1	59	✓	✓	Geth-*turbo*
SrvM2	8	✓	✓	Geth-*ethereumsolo*, Geth-*ethereumpplns*
SrvM3	6	✓	✓	Geth-XX
SrvM4	2	✓	✓	Geth-XX
RPC services				
SrvR1	48	✓	✓	Geth-*omnibus*
SrvR2	1	✓	✓	Geth-*ethshared*

Publication: **ACM CCS 2021**

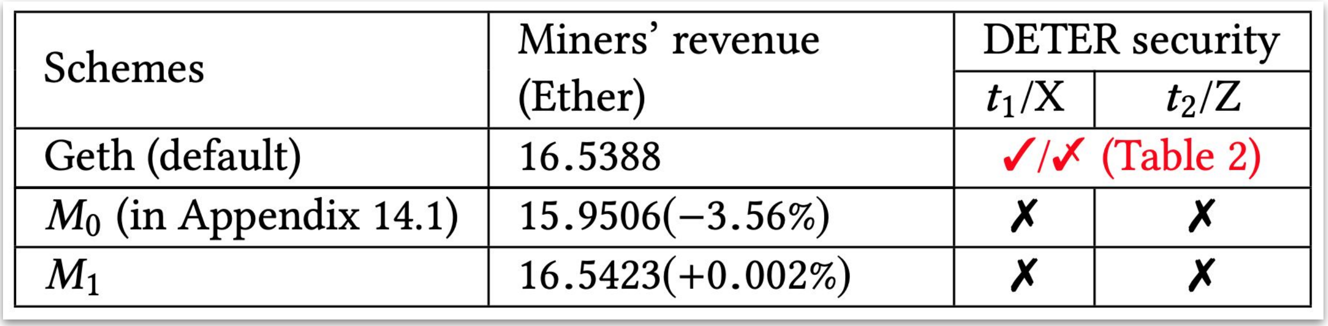
DETER: Denial of Ethereum's Txpool Service.
Kai Li, Yibo Wang, Yuzhe Tang



RQ3. Security under DoS Mempool

Mitigation scheme: Eliminate the attack

- Goal: DETER security versus miner revenue.
- Ideal: Decline any unprofitable txs.
- But profitability cannot be known upon admission?
- Heuristics: decline future txs (M0), decline exploitable tx eviction (M1).
- Evaluation: M0/M1 impl.'ed as middleware on mempool



Schemes	Miners' revenue (Ether)	DETER security	
		t_1/X	t_2/Z
Geth (default)	16.5388	✓/✗ (Table 2)	
M_0 (in Appendix 14.1)	15.9506(−3.56%)	✗	✗
M_1	16.5423(+0.002%)	✗	✗

Bug Reporting

- DETER/DoERS bugs confirmed by Ethereum client developers, RPC services & mining pools.

Go Ethereum

parity

NETHERMIND®

HYPERLEDGER BESU

INFURA

QuikNode

BLOCKDAEMON

Etherscan

amberdata

Bug Reporting

- DETER/DoERS bugs confirmed by Ethereum client developers, RPC services & mining pools.
- Bug bounty rewarded: >$22,000

Go Ethereum

parity

NETHERMIND®

HYPERLEDGER BESU

INFURA

QuikNode

BLOCKDAEMON

Etherscan

amberdata

Bug Reporting

- DETER/DoERS bugs confirmed by Ethereum client developers, RPC services & mining pools.
- Bug bounty rewarded: >$22,000
  - ○ Acknowledgements https://bounty.ethereum.org/

Go Ethereum

parity

NETHERMIND®

HYPERLEDGER BESU

INFURA

QuikNode

BLOCKDAEMON

Etherscan

amberdata

Bug Reporting

- DETER/DoERS bugs confirmed by Ethereum client developers, RPC services & mining pools.
- Bug bounty rewarded: >$22,000
  - Acknowledgements https://bounty.ethereum.org/
- Quick code fix deployed, and advanced fixes in progress.

Go Ethereum

parity

NETHERMIND®

HYPERLEDGER BESU

INFURA

QuikNode

BLOCKDAEMON

Etherscan

amberdata

Talk Outline

Project P1: Securing blockchains under DoS vectors

Project P2: Optimizing DApp costs w.o. losing security

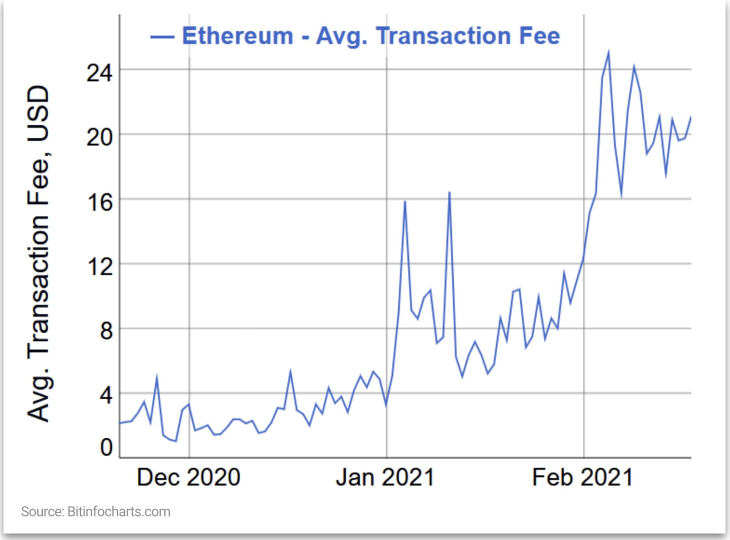
Overview of Other Research Themes

Future research directions

P2: DApp Cost Efficiency

Observation: Blockchain’s expensive!

- Consequence: fewer customers



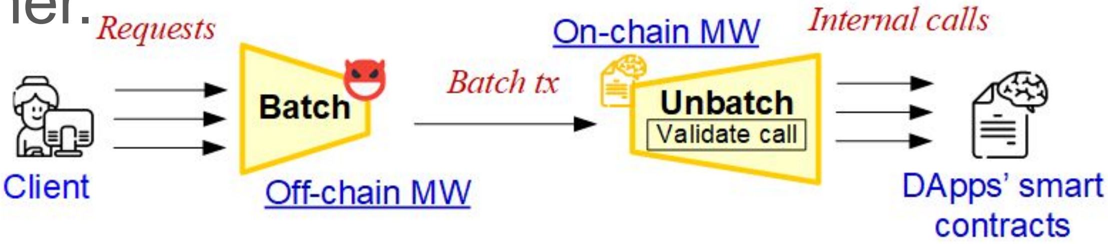
Source: Bitinfocharts.com

Goal: Reduce the use of blockchains per DApp (instead of designing “more efficient yet less trustworthy blockchains”).

RQ4. Reduce Transaction Uses

Motivation (Idea): Batch multiple txs in a block into one big tx to amortize tx fees.

Problem (RQ4): Cost-effective defense against the replay attacks by off-chain batcher.

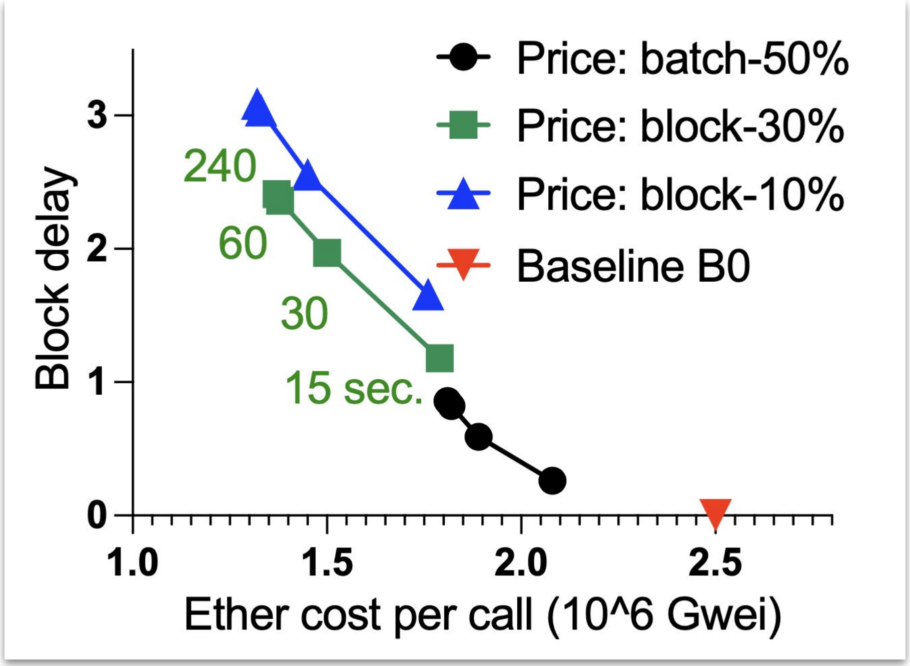


Approach: Security protocol with offchain collective signing & verification using stateless SC

RQ4. Reduce Transaction Uses

Results:

- Middleware prototype on Ethereum/Geth
- Tx replay engine for realistic evaluation
- Significant cost saving at small delay
    - e.g., -60% cost at 2 mins



Publication: **ESEC/FSE 2021**

iBatch: Saving Ethereum Fees via Secure and Cost-Effective Batching of Smart-Contract Invocations
Yibo Wang, Kai Li, Yuzhe Tang, Jiaqi Chen, Qi Zhang, Xiapu Luo, Ting Chen

Talk Outline

Project P1: Securing blockchains under DoS vectors

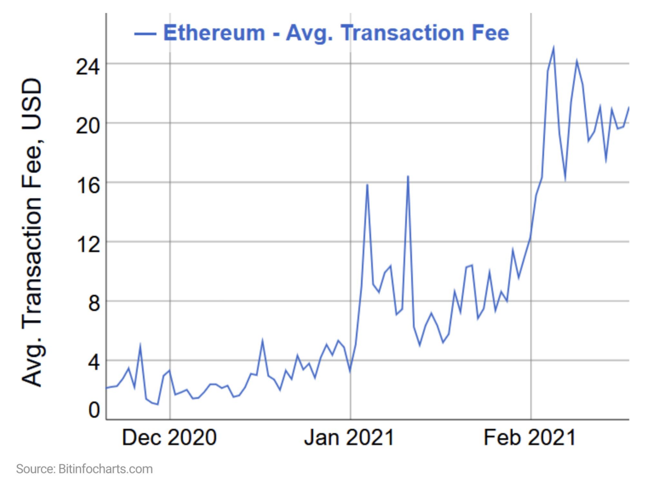
Project P2: Optimizing DApp costs w.o. losing security

- **RQ4: Reducing transaction costs (FSE’21)**
- RQ5: Reducing data movement costs (Middleware’20)

Overview of Other Research Themes

Future research directions

P2^{3M}: DApp Cost Efficiency

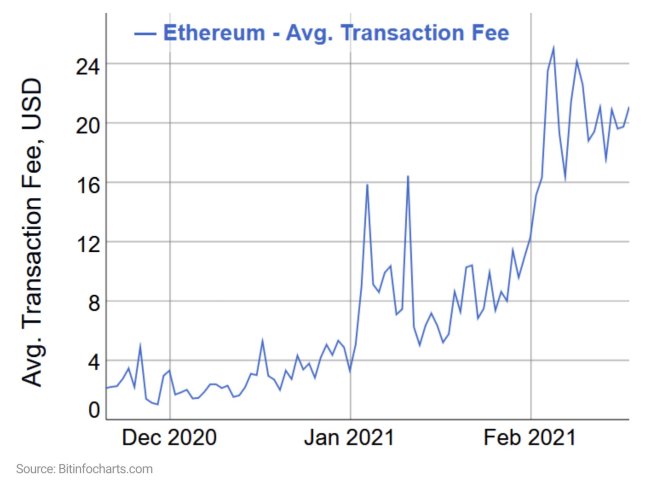


Source: Bitinfocharts.com

Observation: Blockchain's expensive!

- Fees = price * cost
- Costs are high (replicated data)
- prices are skyrocketing (Increasing demand > supply)

Project P2: DApp Cost Efficiency

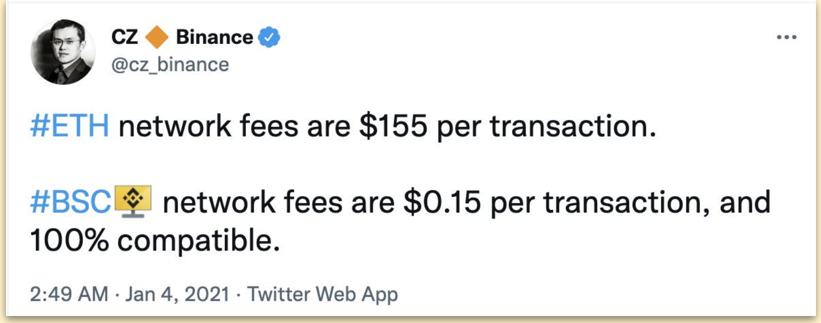


Source: Bitinfocharts.com

Observation: Blockchain's expensive!

- Fees = price * cost
- Costs are high (replicated data)
- prices are skyrocketing (Increasing demand > supply)

Consequence: Scared away customers

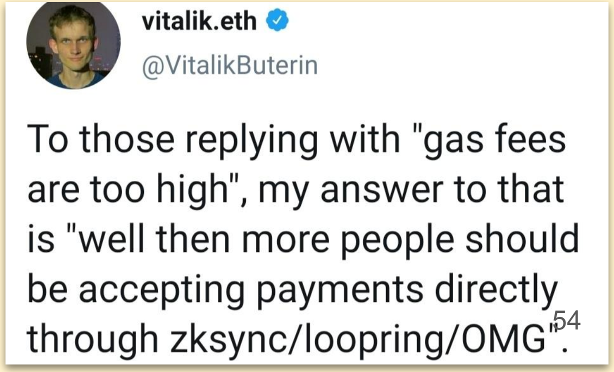


CZ 🔶 Binance
@cz_binance

#ETH network fees are $155 per transaction.

#BSC network fees are $0.15 per transaction, and 100% compatible.

2:49 AM · Jan 4, 2021 · Twitter Web App



vitalik.eth
@VitalikButerin

To those replying with "gas fees are too high", my answer to that is "well then more people should be accepting payments directly through zksync/loopring/OMG".

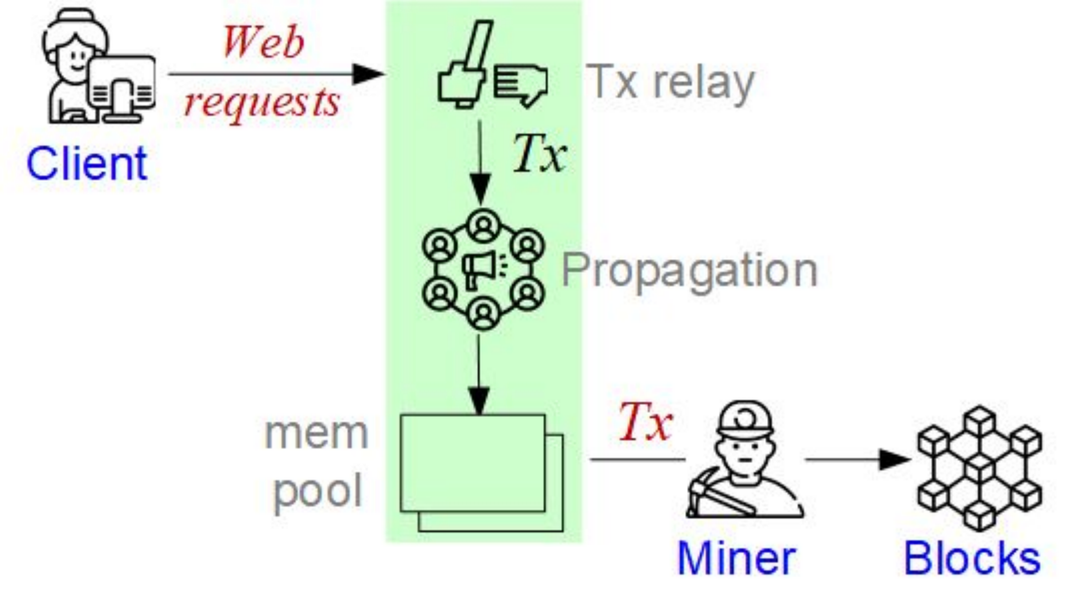
Project P2: DApp Cost Efficiency

Goal: Make DApps'/smart-contracts' use of blockchain efficient, without modifying underlying blockchains.

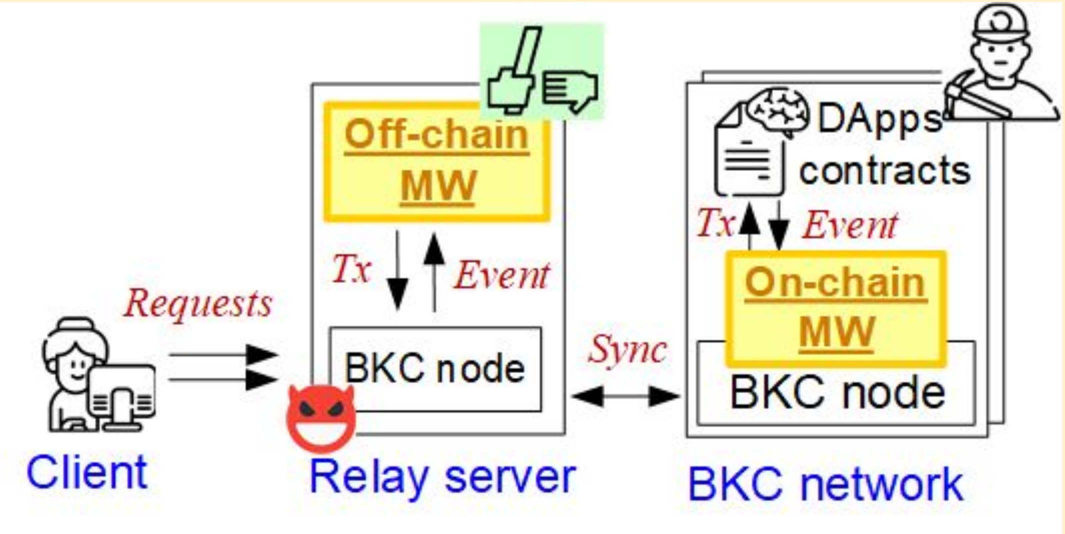
- Ease of deployment as a middleware onto operational blockchain.
- Distinct from research on "more efficient blockchains"

Project P2: DApp Cost Efficiency

Recall the communication-channel view of blockchain ecosystem



Project P2: DApp Cost Efficiency: System Model



Two middlewares in BKC-client comm. channel.

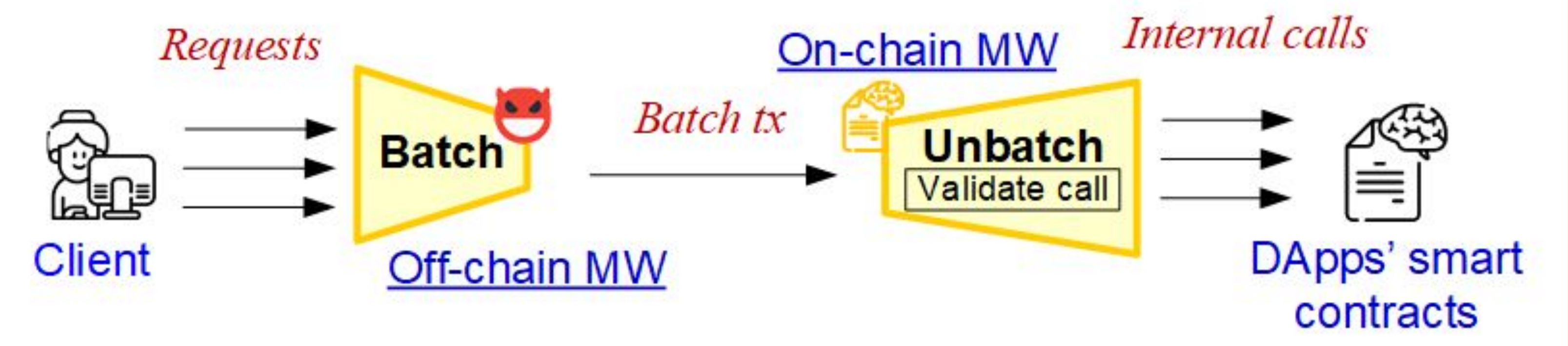
- Untrusted off-chain relay server
- Trusted on-chain smart contract.

Approach: Design & impl. cost-optimization schemes in the two blockchain middlewares.

RQ4. Reduce Transaction Uses

Motivation: There're already multiple txs in one block, why not batch them in one big tx to save/amortize the tx fees?

Threat model:



RQ4. Reduce Transaction Uses

Problem: Fundamental tradeoff between costs and security.

- Off-chain server replays client requests in/across batch txs.
- Baseline design checks replay in smart contracts, incurring costs & offsetting saving by batching.

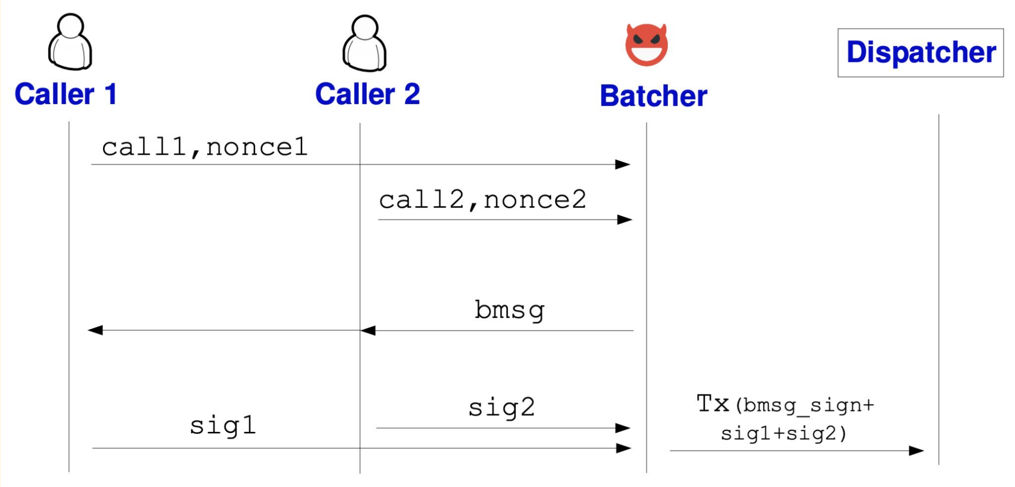
RQ4. How to securely batch against an off-chain replaying server while saving the overall costs?

RQ4. Reduce Transaction Uses

Approach: Key idea:

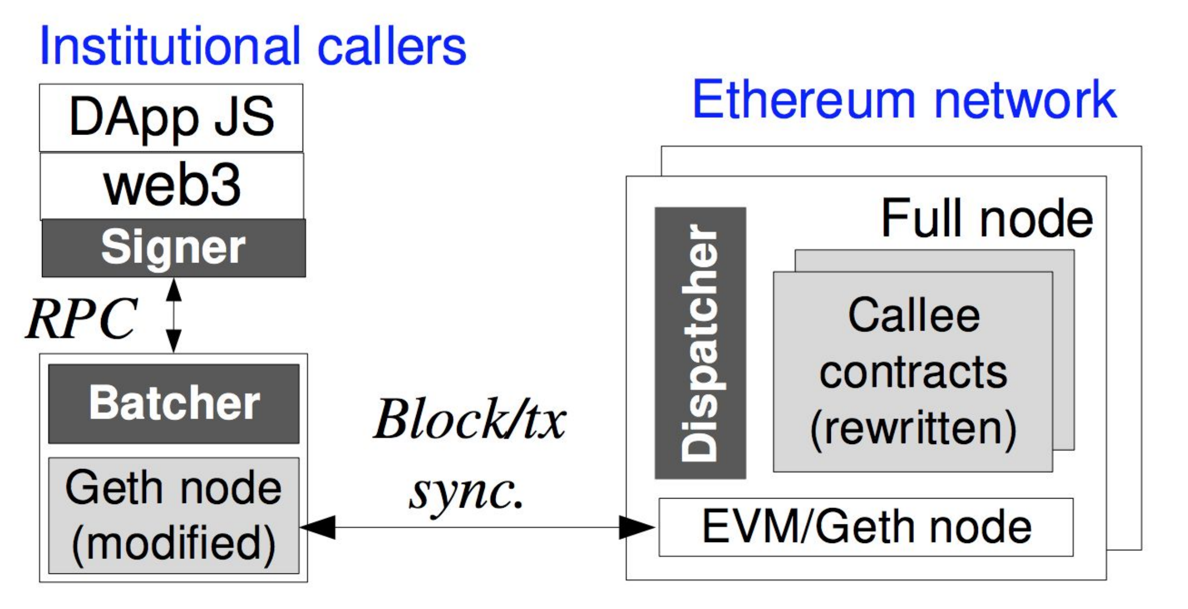
  - ○ ***Reusing tx-wise nonces** to defend against the replays of all N requests in the batch tx.*

- Techniques proposed:
  - ○ Collective signing off-chain
  - ○ Stateless smart-contract on-chain



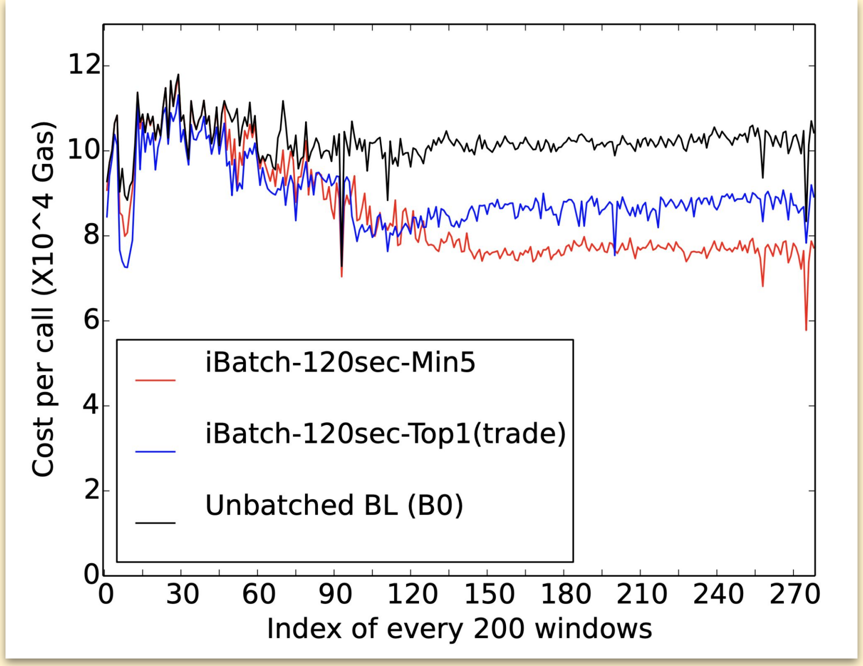
RQ4. Reduce Transaction Uses

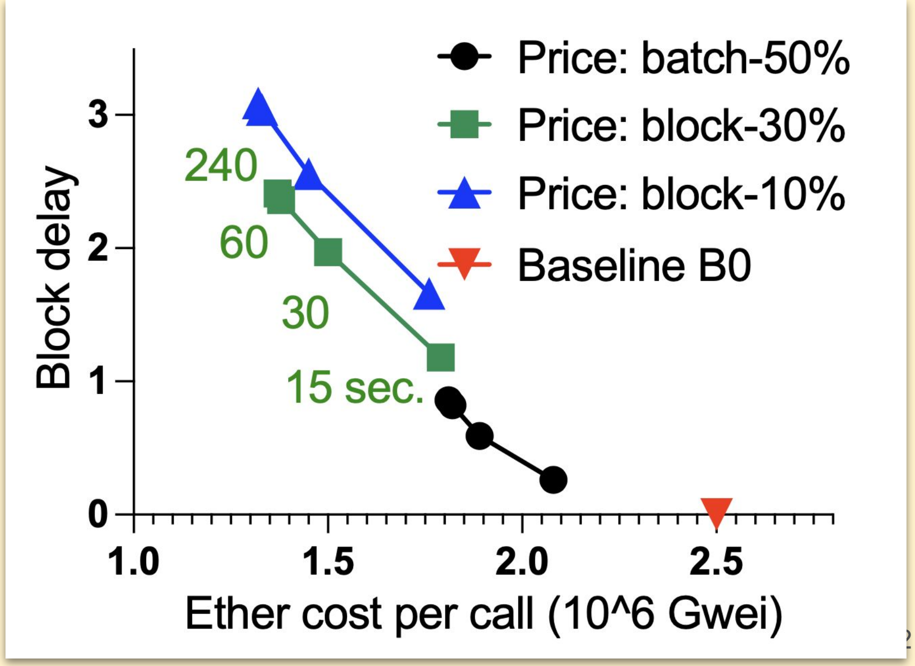
Results: Middleware system prototype on Ethereum/Geth



RQ4. Reduce Transaction Uses

Results: Cost evaluation by replaying real ETH txs

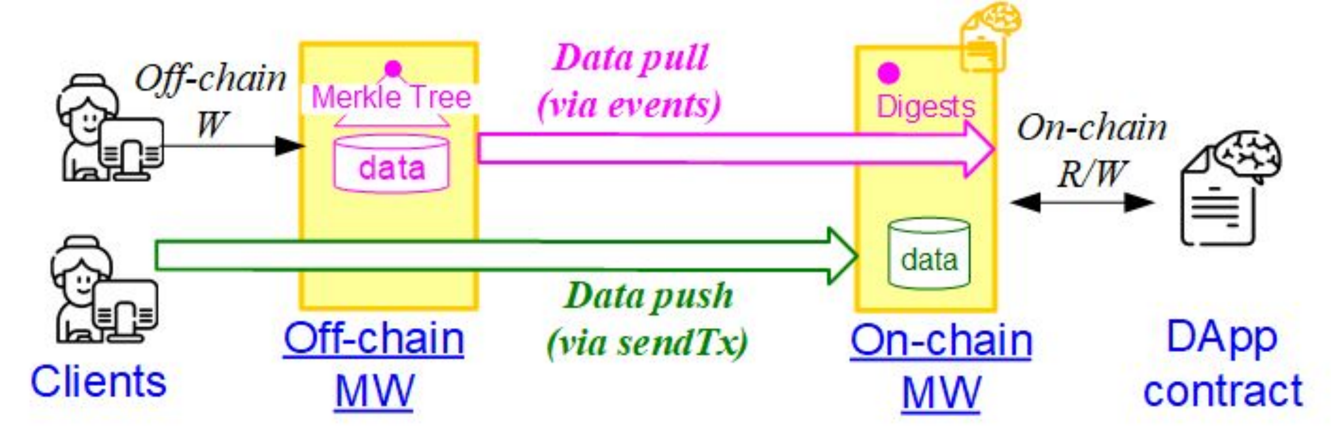




RQ5. Optimize Data Movement Costs

Optimization approach 2:

- Dynamic data replication on/off-chain (Middleware'20)



Talk Outline

Project P1: Securing blockchains under DoS vectors

Project P2: Optimizing DApp costs w.o. losing security

- RQ4: Reducing transaction costs (FSE’21)
- **RQ5: Reducing data movement costs (Middleware’20)**

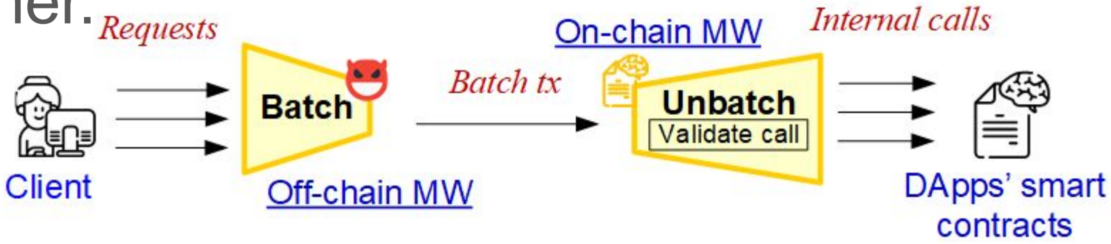
Overview of Other Research Themes

Future research directions

RQ4. Reduce Transaction Uses

Motivation (Idea): Batch multiple txs in a block into one big tx to amortize tx fees.

Problem (RQ4): Cost-effective defense against the replay attacks by off-chain batcher.



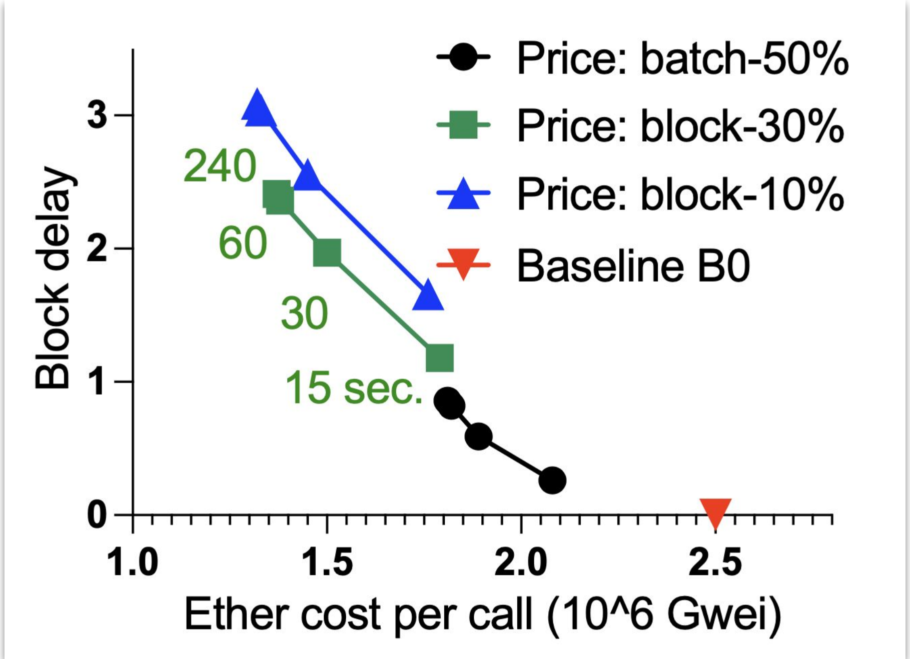
Approach: Security protocol with offchain collective signing & verification using stateless SC

RQ4. Reduce Transaction Uses

Results:

- Middleware prototype on Ethereum/Geth
- Tx replay engine for realistic evaluation
- Significant cost saving at small delay
    - e.g., -60% cost at 2 mins

Publication: **ESEC/FSE 2021**



iBatch: Saving Ethereum Fees via Secure and Cost-Effective Batching of Smart-Contract Invocations
Yibo Wang, Kai Li, Yuzhe Tang, Jiaqi Chen, Qi Zhang, Xiapu Luo, Ting Chen

Talk Outline

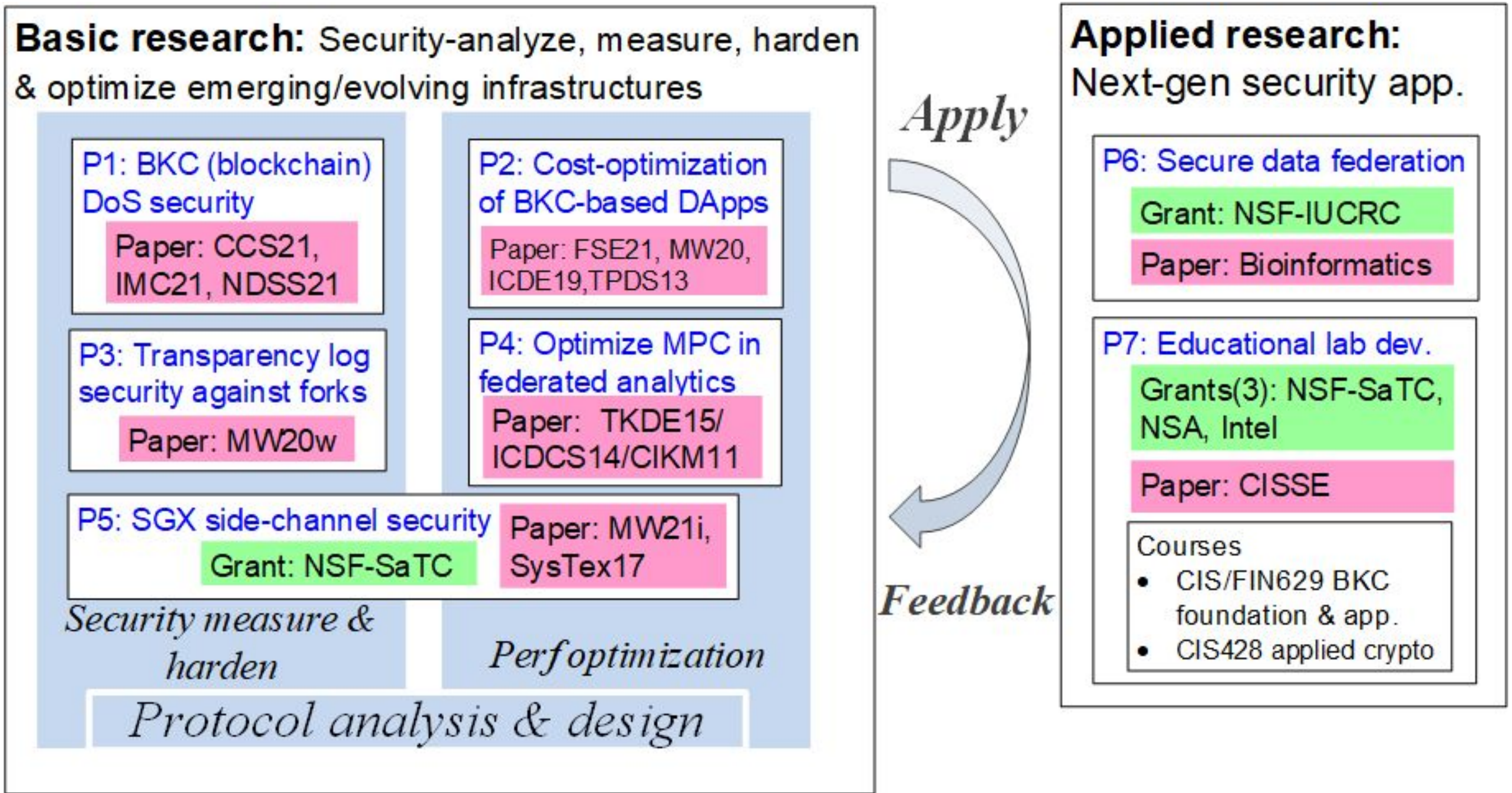
Project 1: Securing blockchains under DoS vectors

Project 2: Optimizing the DApp cost without losing security

Overview of Other Research Themes

Future Research Directions

Current Research: *Methods*, Projects, Grants & Papers.



Basic research: Security-analyze, measure, harden & optimize emerging/evolving infrastructures

P1: BKC (blockchain) DoS security

Paper: CCS21, IMC21, NDSS21

P2: Cost-optimization of BKC-based DApps

Paper: FSE21, MW20, ICDE19,TPDS13

P3: Transparency log security against forks

Paper: MW20w

P4: Optimize MPC in federated analytics

Paper: TKDE15/ ICDCS14/CIKM11

P5: SGX side-channel security

Grant: NSF-SaTC

Paper: MW21i, SysTex17

Security measure & harden

Perf optimization

Protocol analysis & design

Apply

Feedback

Applied research: Next-gen security app.

P6: Secure data federation

Grant: NSF-IUCRC

Paper: Bioinformatics

P7: Educational lab dev.

Grants(3): NSF-SaTC, NSA, Intel

Paper: CISSE

Courses

- CIS/FIN629 BKC foundation & app.
- CIS428 applied crypto

Acknowledgement

- Collaborators: XiaoFeng Wang, Xiapu Luo, Jianliang Xu, etc.

- My students: Kai Li, Yibo Wang, Jiaqi Chen, Yuxuan Zhou, Xianghong Liu, Qi Zhang, Sencer Burak Somuncuoglu, etc.

- Funding support from NSF, NSA, AFRL and industrial gifts from Intel, etc.

	Problem (hardness)	Approach (cleverness)	Results (Significance)
DoERS (NDSS'21)	RQ1. Exploitability measurement on blackbox service	Repurpose double spending tx to detect service load balancer	Bug confirmed by 5 ETH clients; $2K bounty; code fix in Geth >0.1;
TopoShot (IMC'21)	RQ2. Network measurement on blackbox nodes	Repurpose tx replacement to ensure isolation in edge measurement	First work to accurately uncover ETH network topology
DETER (CCS'21)	RQ3. Low-cost DoS on remote mempool	Misuse tx eviction to spam mempool	High severity bugs by 5 ETH clients; $20K bounty
iBatch (FSE'21)	RQ4. Cost-effective defense against tx replays	Off-chain signing protocol with stateless verifier in smart-contracts	Up to 60% lower costs at small delay of 2 min.
GRuB (MW'20)	RQ5. Reduce data movement costs against untrusted service.		

Summary

- Research methodology
  - Target (sub)system: large-scale infrastructures, emerging/evolving features, code in security/cost-critical path.
  - Security research: Understand, measure & harden security?
  - Systems research: Analyze & optimize performance?

- Example research projects in this talk
  - Securing blockchains under DoS vectors (CCS, NDSS, IMC)
    - Hard problem, clever methods, and significant results
  - Cost-optimizing DApps without losing security (FSE, MW, ICDE)