Year in Academic Blockchain Research 2018/2019

Dominik Harz
Imperial College London
@nud3l

14 August 2019

Methodology

Selected papers from academic conferences in years 2018/2019 with their open access link

- IEEE S&P 2019
- ACM CCS 2018
- Usenix 2019
- NDSS 2018
- PODC 2019
- Crypto 2018
- Financial Cryptography 2019
- EuroCrypt 2019
- AsiaCrypt 2018

Disclaimer

While I tried to keep the selection of papers diverse and mainly picked papers from the top-tier conferences, this summary is not a complete review of all papers in the space. Rather, it is my personal selection of papers. If a paper is not included here, it does not mean that it is not interesting or relevant. If you wish your paper to be included, feel free to reach out to me via DM on Twitter (@nud3l_) or email via d.harz at ic.ac.uk

Agenda - Part 1

Agenda - Part 2

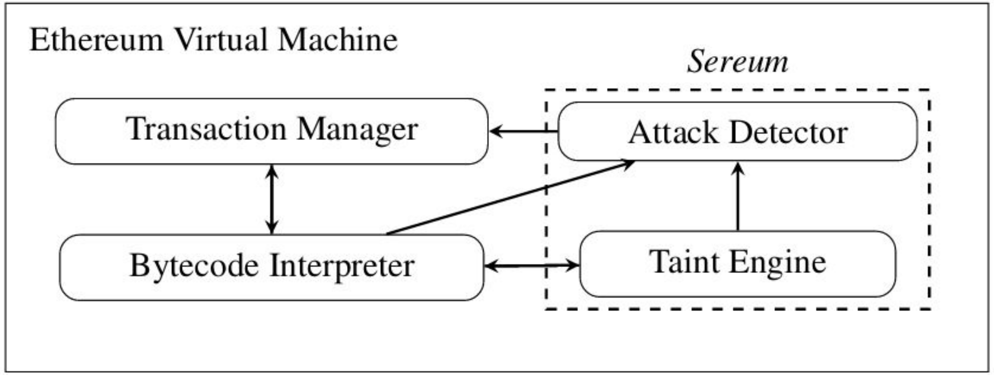
Improving clients

Sereum: Protecting Existing Smart Contracts Against Re-Entrancy Attacks

---

Integrate re-entrancy attack detection into EVM implementation (geth)

Higher detection rates than other tools (Securify, Oyente etc.) and backwards compatible

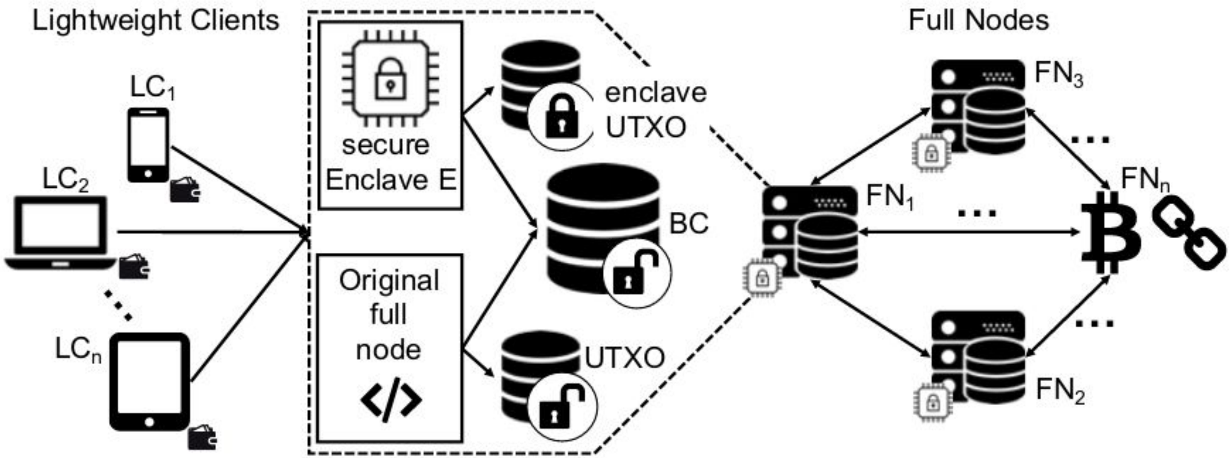


https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_09-3_Rodler_paper.pdf

BITE: Bitcoin Lightweight Client Privacy using Trusted Execution

---

Prevent privacy leakage in Bitcoin light clients



https://www.usenix.org/system/files/sec19fall_matetic_prepub.pdf

Biased Nonce Sense: Lattice Attacks against Weak ECDSA Signatures in Cryptocurrencies

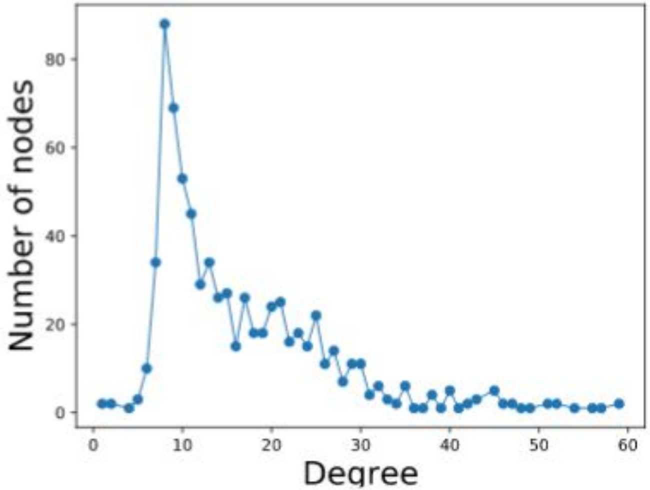
Computed 300 Bitcoin private keys, dozens of Ethereum private keys and one Ripple key

Weak randomness generation for key generation as root cause

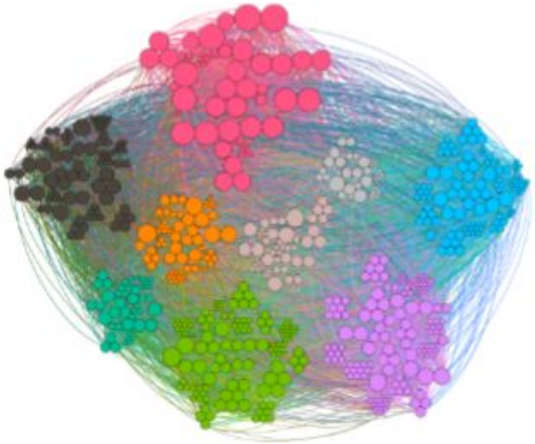
https://fc19.ifca.ai/preproceedings/104-preproceedings.pdf

Discovering and improving P2P networks

TxProbe: Discovering Bitcoin's Network Topology Using Orphan Transactions



(a) Degree distribution of nodes in the testnet snapshot.

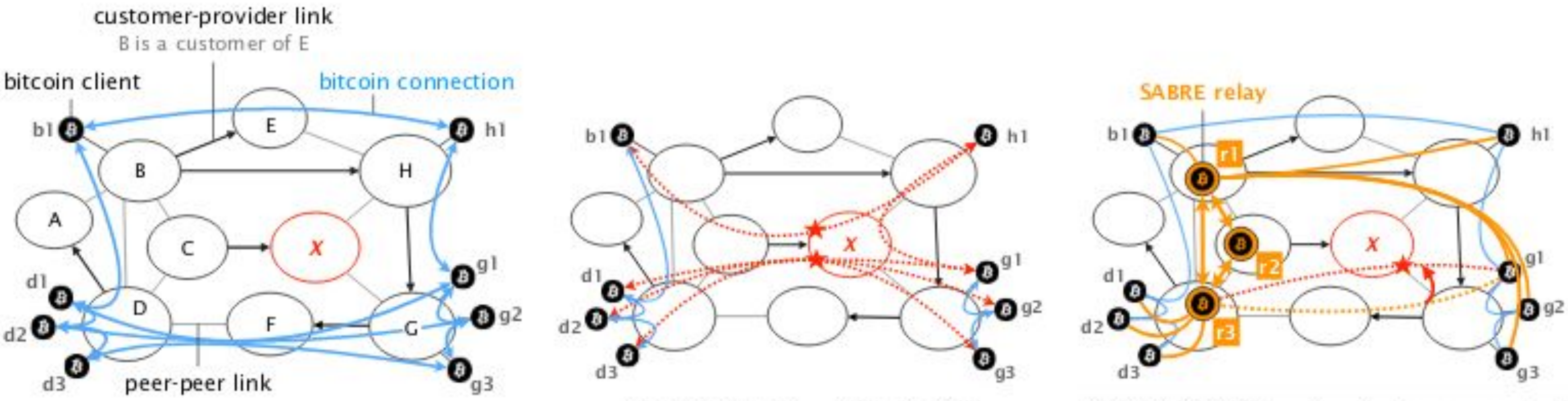


(b) Communities detected in the testnet snapshot.

https://fc19.ifca.ai/preproceedings/58-preproceedings.pdf

SABRE: Protecting Bitcoin against Routing Attacks

BGP level attacks leads to eclipse and fork attacks



(a) AS-level topology (b) AS X hijacks ASH & ASG (c) With SABRE, network stays connected

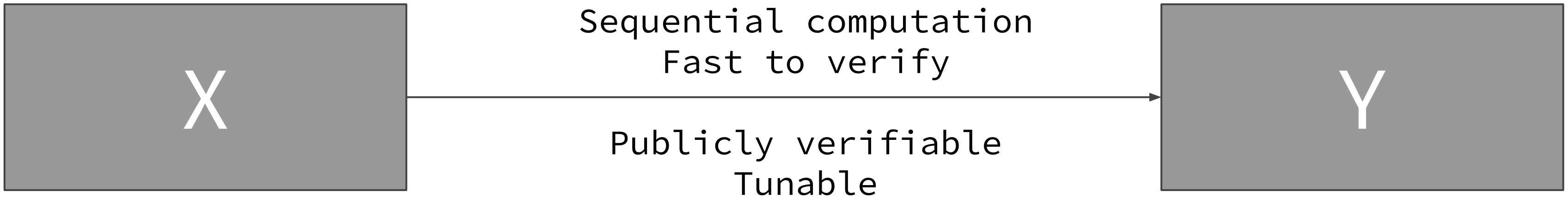
https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-1_Apostolaki_paper.pdf

Crypto means Cryptography

Verifiable Delay Functions

Compute a function that requires wall-clock time to compute with a random output

Use random output for random beacons, leader election,or proof of replication



https://eprint.iacr.org/2018/601.pdf
https://www.youtube.com/watch?v=qUoagL7OZ1k&feature=youtu.be

Compact Multi-Signatures for Smaller Blockchains

Decrease the size of blockchains by signature aggregation

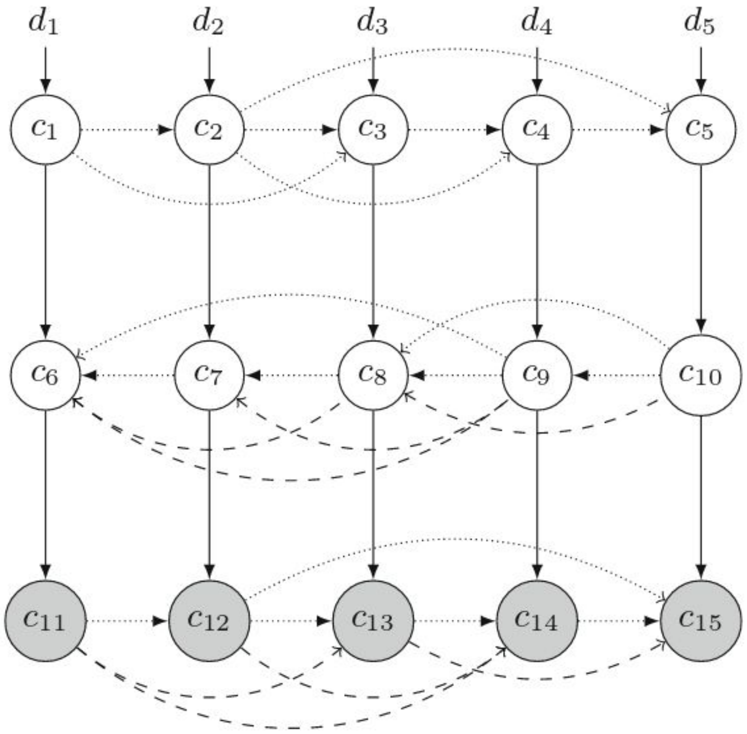
	Combined public key size	Combined signature size	Total size (KB)	Threshold support
Bitcoin	$tx \cdot inp \cdot n \cdot \lvert\mathbb{G}\rvert$	$tx \cdot inp \cdot n \cdot 2 \cdot \lvert\mathbb{Z}_q\rvert$	1296	linear
MuSig ([35])	$tx \cdot inp \cdot \lvert\mathbb{G}\rvert$	$tx \cdot (\lvert\mathbb{G}\rvert + \lvert\mathbb{Z}_q\rvert)$	240	small
$\mathcal{MSDL}$ (Sec. 5)	$tx \cdot inp \cdot \lvert\mathbb{G}\rvert$	$tx \cdot (\lvert\mathbb{G}\rvert + \lvert\mathbb{Z}_q\rvert)$	240	small
$\mathcal{MSP}$ (Sec. 3.1)	$tx \cdot inp \cdot \lvert\mathbb{G}_2\rvert$	$tx \cdot \lvert\mathbb{G}_1\rvert$	360	small
$\mathcal{AMSP}$ (Sec. 3.3)	$tx \cdot inp \cdot \lvert\mathbb{G}_2\rvert$	$\lvert\mathbb{G}_1\rvert$	216	small
$\mathcal{ASM}$ (Sec. 4)	$tx \cdot inp \cdot \lvert\mathbb{G}_2\rvert$	$tx \cdot inp \cdot (\lvert\mathbb{G}_1\rvert + \lvert\mathbb{G}_2\rvert)$	864	any

https://eprint.iacr.org/2018/483.pdf

Tight Proofs of Space and Replication

Efficient proofs for providing and storing files

Depth robust graph (DRG) as basis structure for proofs



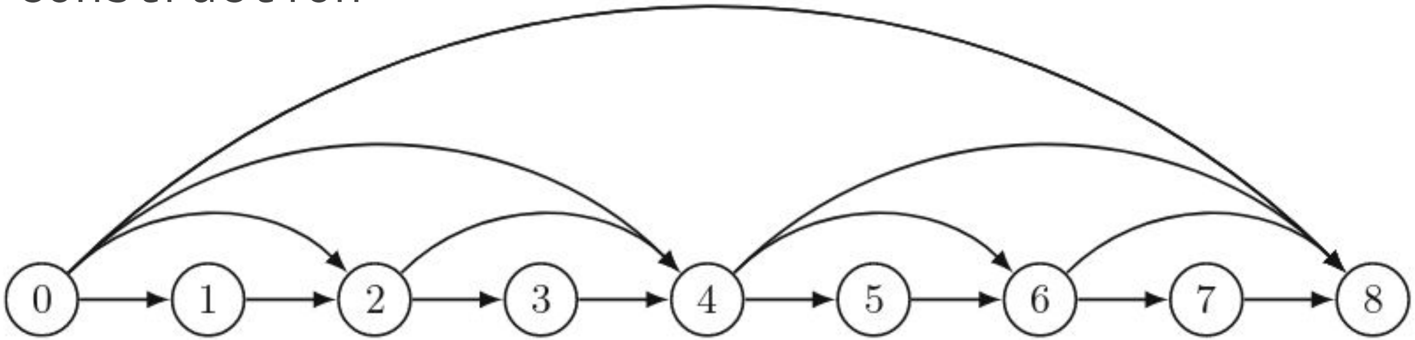
https://link.springer.com/content/pdf/10.1007%2F978-3-030-17656-3_12.pdf

Reversible Proofs of Sequential Work

Skip list as underlying structure

Application to proof of replication

Efficient construction



https://link.springer.com/content/pdf/10.1007%2F978-3-030-17656-3_10.pdf

Understanding existing ledgers

Lay Down the Common Metrics: Evaluating Proof-of-Work Consensus Protocols' Security

Compared Nakamoto consensus with other (academic) PoW protocols

No protocol better in all areas than Nakamoto

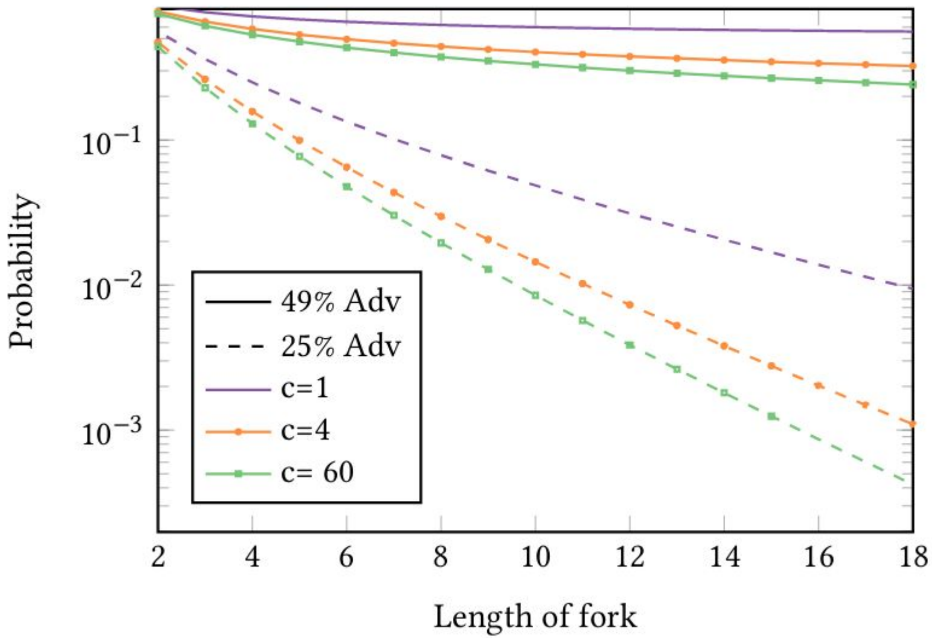
Group	Protocol	Designers' analysis	Our results
Better-chain-quality	SHTB [12]	None	New protocol-specific attack strategy
Better-chain-quality	UDTB [18], [21]	Analysis against one attack strategy	New protocol-specific attack strategy
Attack-resistant: reward-all	Fruitchains [20]	Formal analysis against selfish mining assuming some parameters are large enough	Vulnerable to selfish mining and double-spending attacks with reasonable parameters
Attack-resistant: punishment	RS [12], [21]	Analysis against one attack strategy	Vulnerable to censorship attack
Attack-resistant: reward-lucky	Subchains [11]	None	Vulnerable to all three attacks

https://www.esat.kuleuven.be/cosic/publications/article-3005.pdf

A Better Method to Analyze Blockchain Consistency

Markov-chain to analyse consistency of blockchains

Analyse various protocols including Nakamoto and GHOST

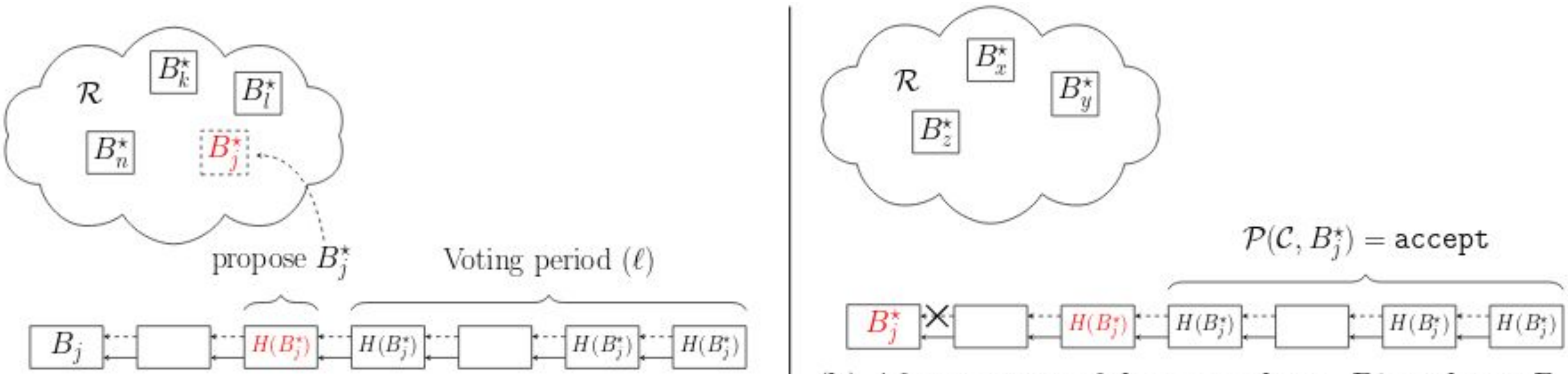


https://shelat.ccis.neu.edu/research/2018-08-01-blockchain-consistency/

Improving and extending ledgers

Redactable Blockchain in the Permissionless Setting

Replace blocks by voting



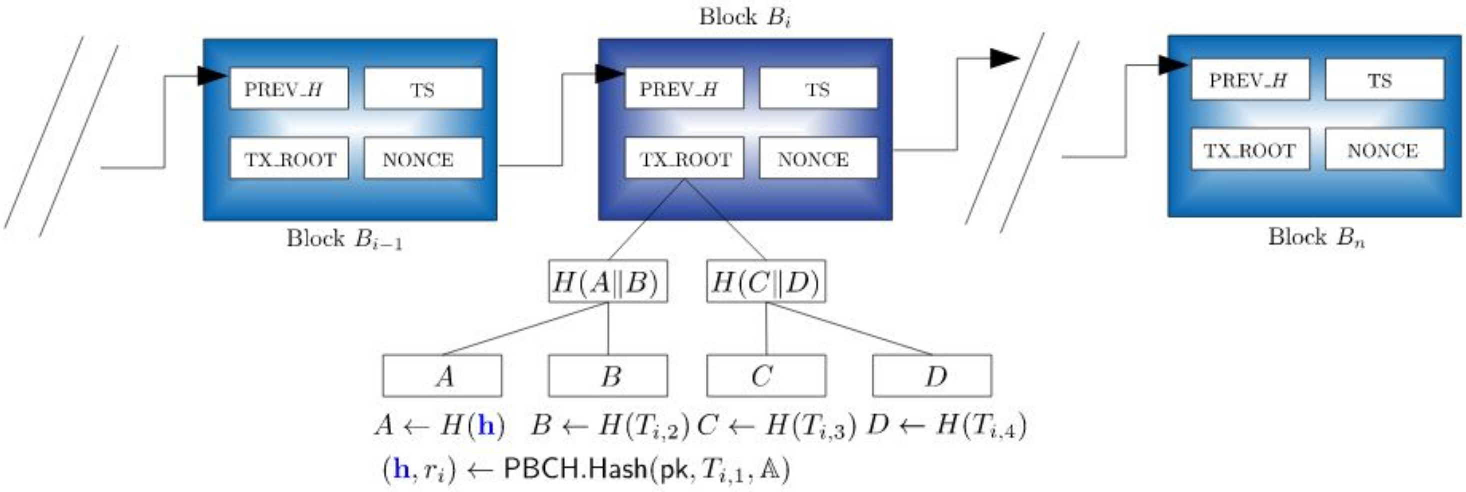
(a) Proposing a redaction $B_j^\star$ for the block B_j

(b) After a successful voting phase, $B_j^\star$ replaces B_j in the chain

https://arxiv.org/abs/1901.03206

Fine-Grained and Controlled Rewriting in Blockchains: Chameleon-Hashing Gone Attribute-Based

Policy-based chameleon hashes to change existing transactions in blockchains

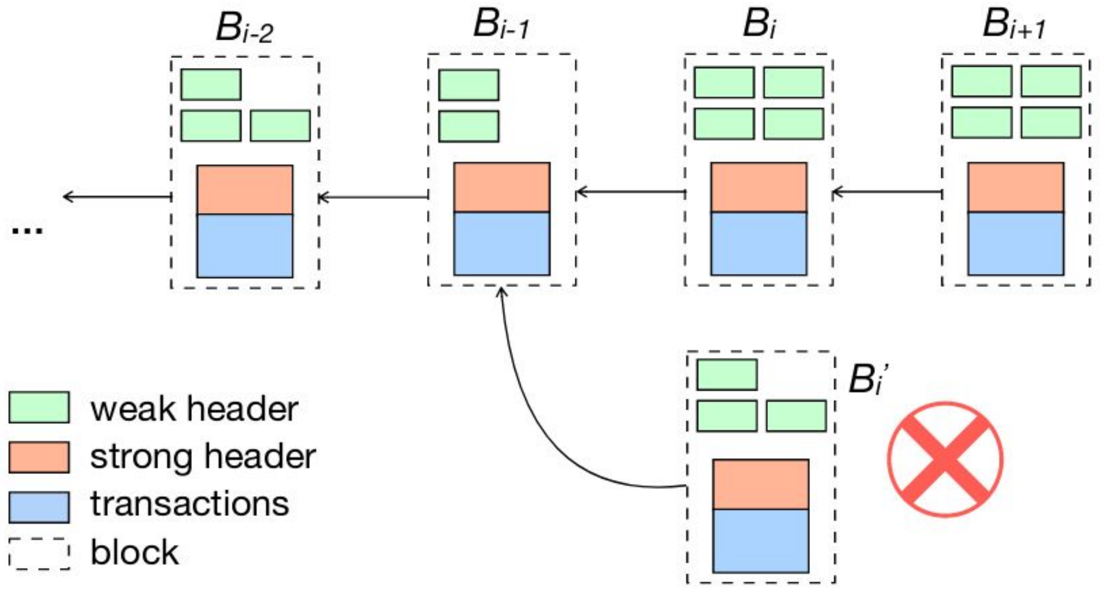


https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-3_Derler_paper.pdf

StrongChain: Transparent and Collaborative Proof-of-Work Consensus

Include weak results in blocks

Provide an incentive to collaborate instead of compete



https://arxiv.org/pdf/1905.09655v1.pdf

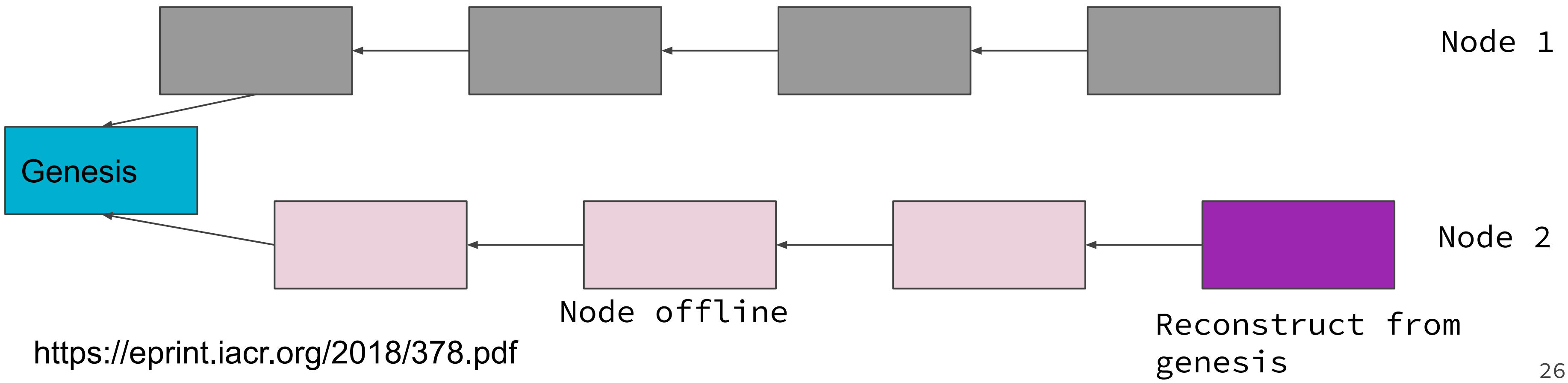
Reaching consensus

Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability

---

Secure bootstrap a blockchain from the Genesis block

Proven in Global Universally Composable (GUC) model



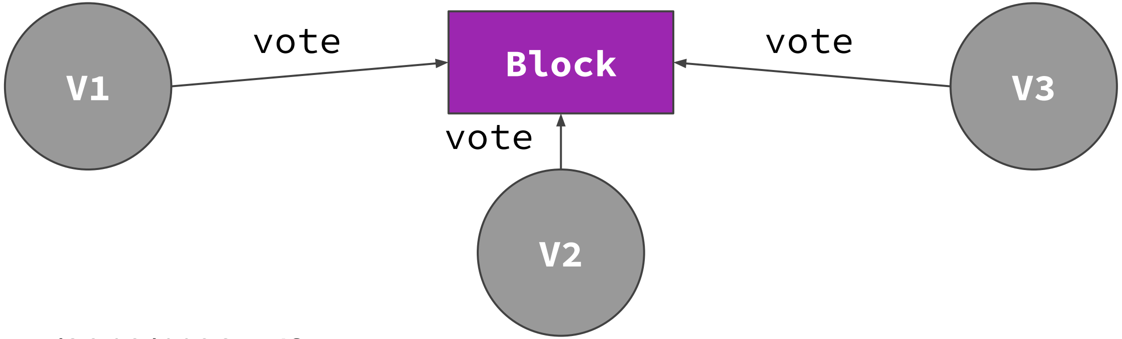
https://eprint.iacr.org/2018/378.pdf

Ouroboros Crypsinous: Privacy-Preserving Proof-of-Stake

Privacy-preserving ledger with strong security proofs

SNARK extension to allow privacy-preserving staking

Builds on Ouroboros Genesis and Zerocash



https://eprint.iacr.org/2018/1132.pdf

Communication Complexity of Byzantine Agreement, Revisited

Reduce communication complexity below n^2 nodes (i.e. subquadratic)

- After-the-fact removal of messages should not be allowed
- Near-optimal subquadratic communication with multicasts
- Requirement of setup phase for Public-Key Infrastructure (PKI)

Formal proofs on upper and lower bounds of communication

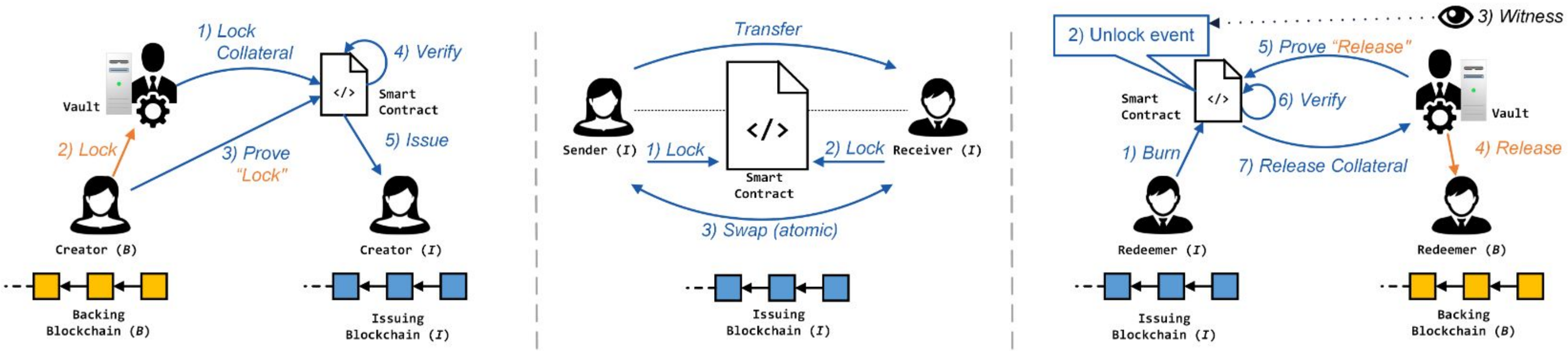
https://arxiv.org/pdf/1805.03391.pdf

Connecting chains

XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets

---

Interoperability through issuing and redeeming cross-chain assets



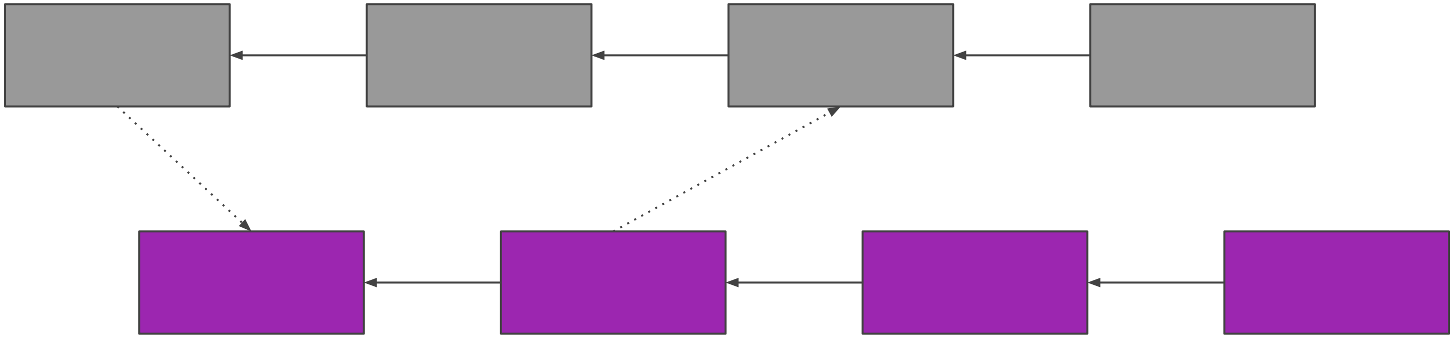
Issue　　Transfer / Swap　　Redeem

https://eprint.iacr.org/2018/643.pdf

Proof-of-Stake Sidechains

Cross-chain special transactions to transfer assets

Different chains can have different properties



https://eprint.iacr.org/2018/1239.pdf

Tracing Transactions Across Cryptocurrency Ledgers

Identify matching transactions across Bitcoin, Ethereum, Litecoin, Bitcoin Cash, Dogecoin, Dash, Ethereum Classic, and Zcash

Data source from Changelly and ShapeShift

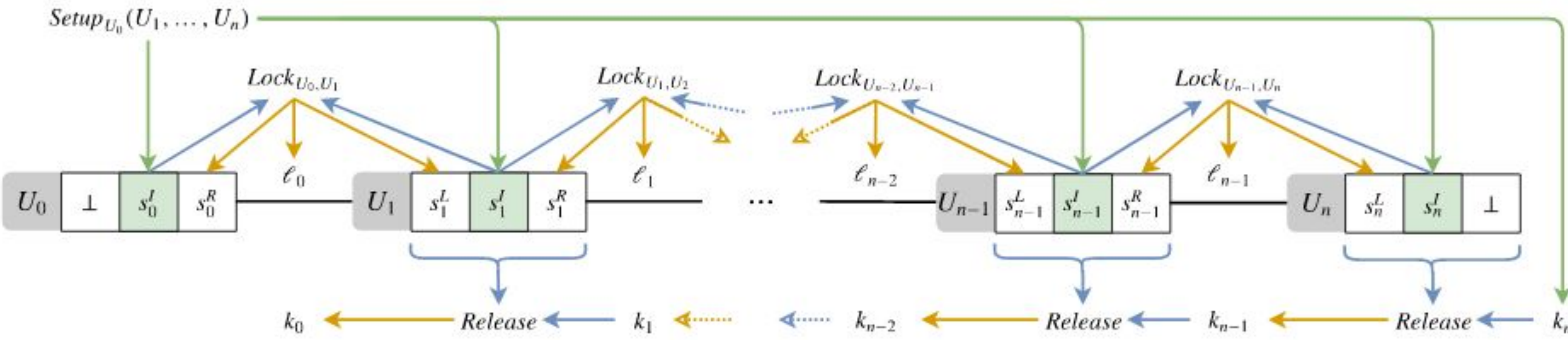
Currency	Parameters		Basic %	Augmented %
	δ_b	δ_a		
BTC	0	1	65.76	76.86
BCH	9	4	76.96	80.23
DASH	5	5	84.77	88.65
DOGE	1	4	76.94	81.69
ETH	5	0	72.15	81.63
ETC	5	0	76.61	78.67
LTC	1	2	71.61	76.97
ZEC	1	3	86.94	90.54

https://arxiv.org/pdf/1810.12786.pdf

Making blockchains scale

Anonymous Multi-Hop Locks for Blockchain Scalability and Interoperability

AMHL construction on ECDSA signatures (compatible with Bitcoin and Ethereum)

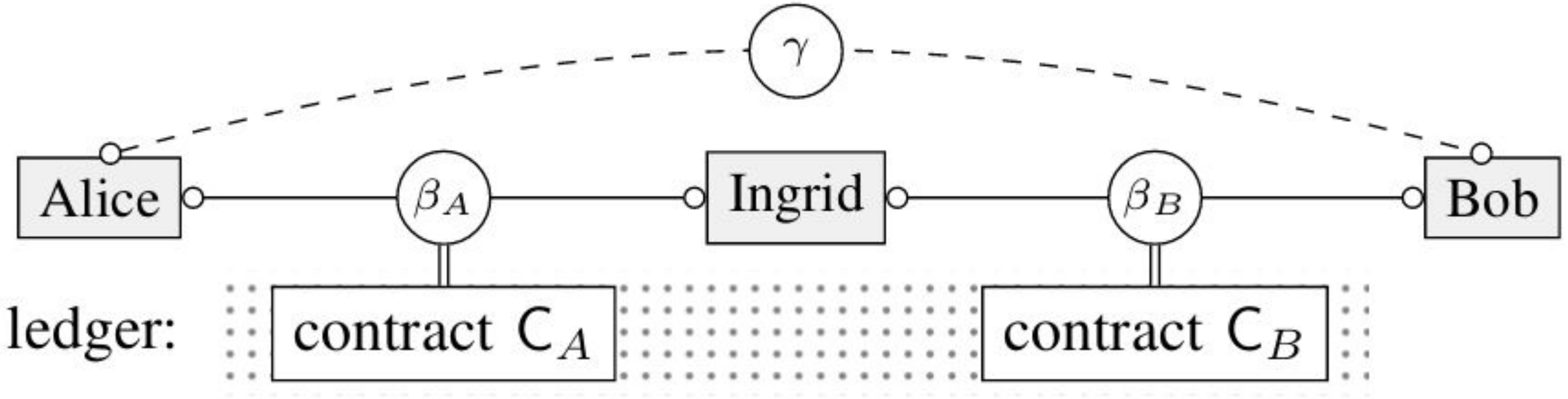


https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_09-4_Malavolta_paper.pdf

Perun: Virtual Payment Hubs over Cryptocurrencies

Perun is an alternative construction to routing schemes

Ingrid does not need to be active

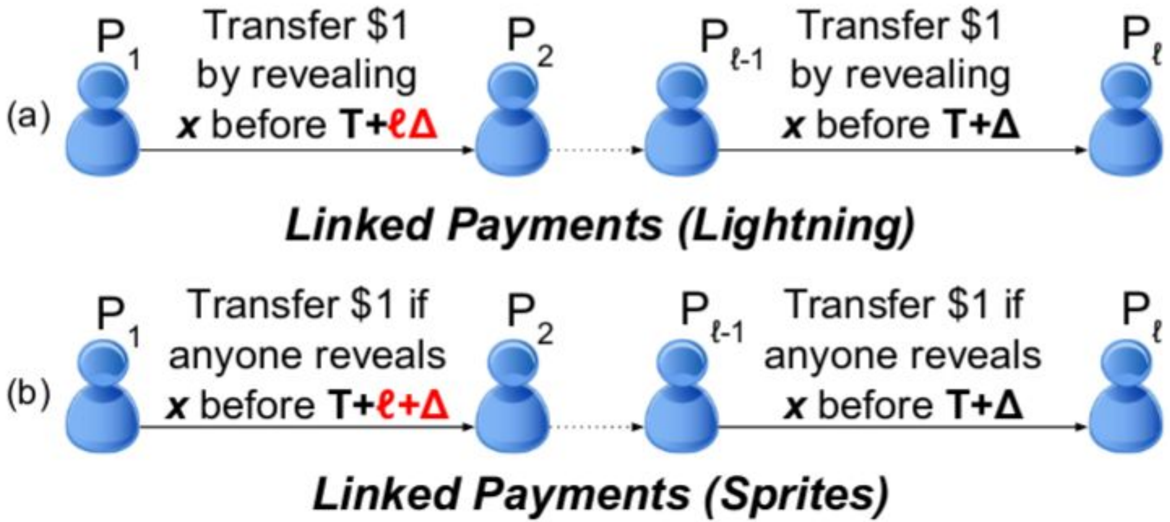


https://eprint.iacr.org/2017/635.pdf

Sprites and State Channels: Payment Networks that Go Faster than Lightning

---

Constant lock time to reduce cost of collateral in channels



https://fc19.ifca.ai/preproceedings/185-preproceedings.pdf

RapidChain: A Fast Blockchain Protocol via Full Sharding

Cross-shard transaction verification technique

Reduces communication overhead in sharding

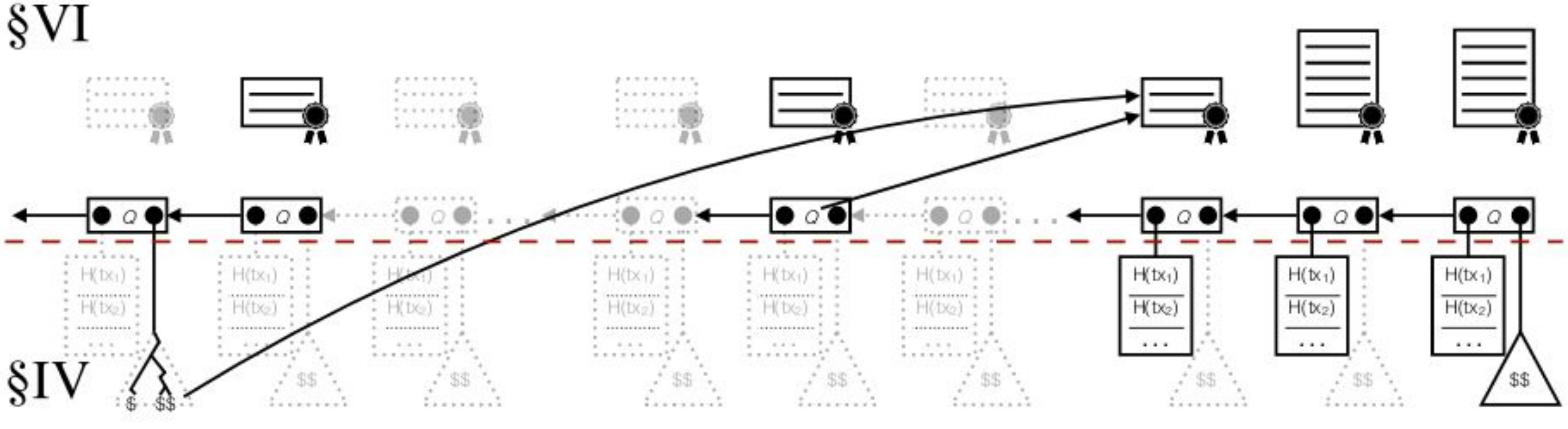
Increases resilience against faults

Protocol	# Nodes	Resiliency	Complexity[1]	Throughput	Latency	Storage[2]	Shard Size	Time to Fail
Elastico [45]	$n = 1{,}600$	$t < n/4$	$\Omega(m^2/b+n)$	40 tx/sec	800 sec	1x	$m = 100$	1 hour
OmniLedger [40]	$n = 1{,}800$	$t < n/4$	$\Omega(m^2/b+n)$	500 tx/sec	14 sec	1/3x	$m = 600$	230 years
OmniLedger [40]	$n = 1{,}800$	$t < n/4$	$\Omega(m^2/b+n)$	3,500 tx/sec	63 sec	1/3x	$m = 600$	230 years
RapidChain	$n = 1{,}800$	$t < n/3$	$O(m^2/b+m \log n)$	4,220 tx/sec	8.5 sec	1/9x	$m = 200$	1,950 years
RapidChain	$n = \mathbf{4{,}000}$	$t < n/3$	$O(m^2/b+m \log n)$	**7,380 tx/sec**	**8.7 sec**	**1/16x**	$m = \mathbf{250}$	**4,580 years**

https://pdfs.semanticscholar.org/55c1/359ef9b2b732643778635dc6182ddaccdb42.pdf

Vault: Fast Bootstrapping for the Algorand Cryptocurrency

Reduce bootstrapping time of new clients by 99.7% compared to Bitcoin and 90.5% compared to Ethereum



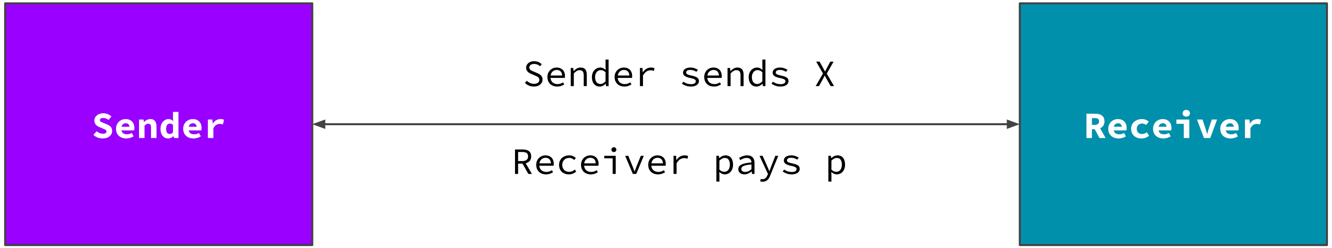
https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_09-2_Leung_paper.pdf

Playing games with money

FairSwap: How to fairly exchange digital goods

Trade digital goods with fair payments

Digital good split up in bits that need to evaluate to true to trigger payment



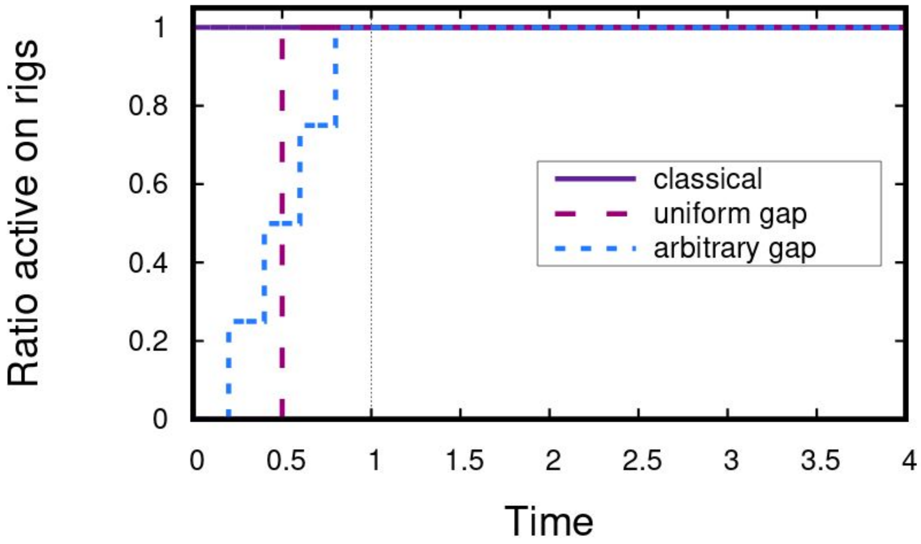
https://eprint.iacr.org/2018/740.pdf

The Gap Game

Fees for transactions play an important role to incentivize miners

Miners switch-off their racks even before fees become the only incentive

Gaps form and are in favour of large mining pools

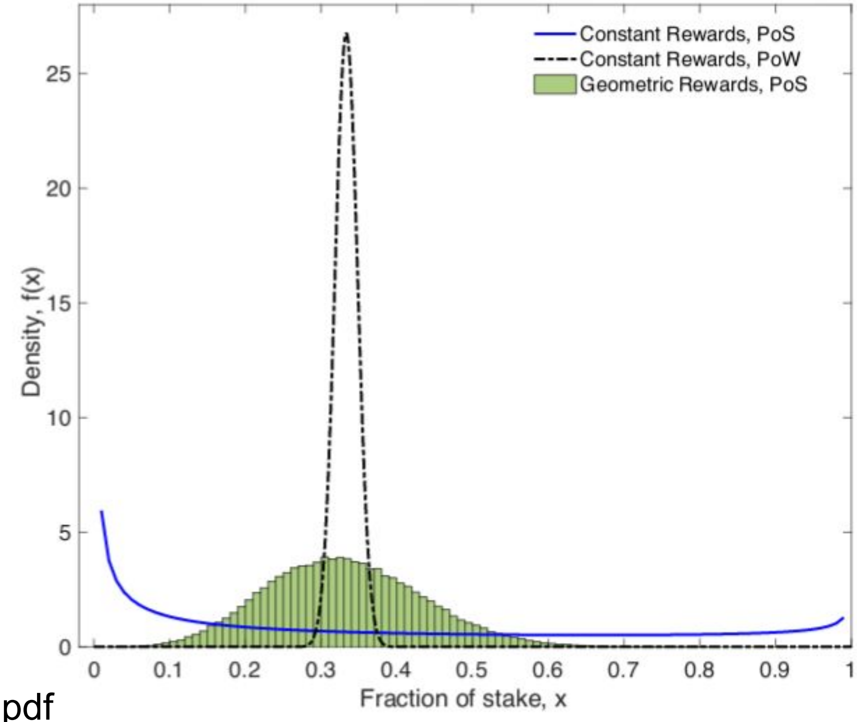


https://arxiv.org/pdf/1805.05288.pdf

Compounding of Wealth in Proof-of-Stake Cryptocurrencies

Constant reward functions in PoS make rich richer and poor poorer

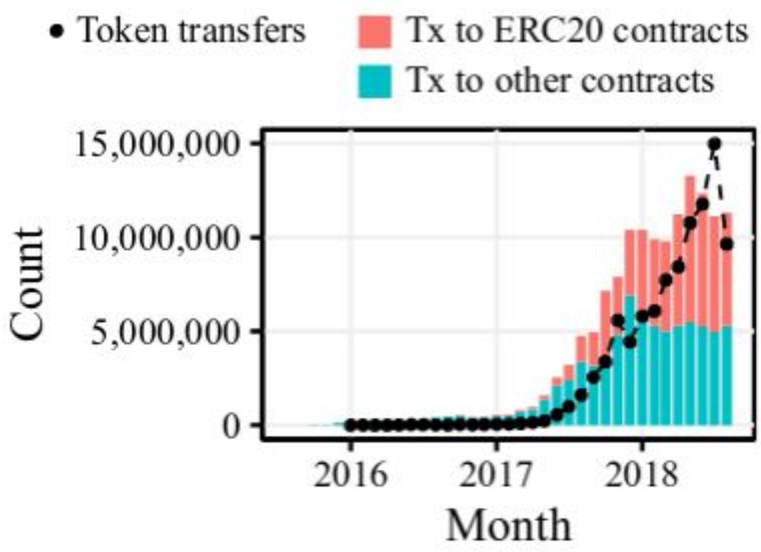
Geometric reward function to achieve similar reward distribution as in PoW

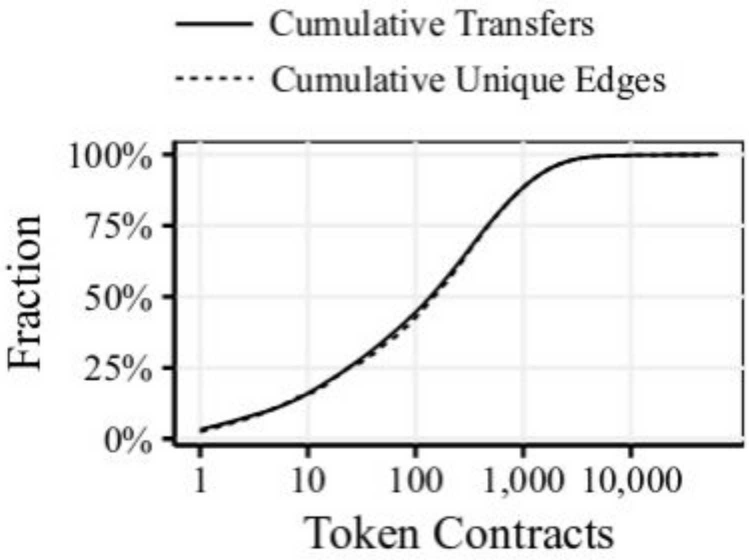


https://fc19.ifca.ai/preproceedings/161-preproceedings.pdf

Tokens and scams

Measuring Ethereum-based ERC20 Token Networks



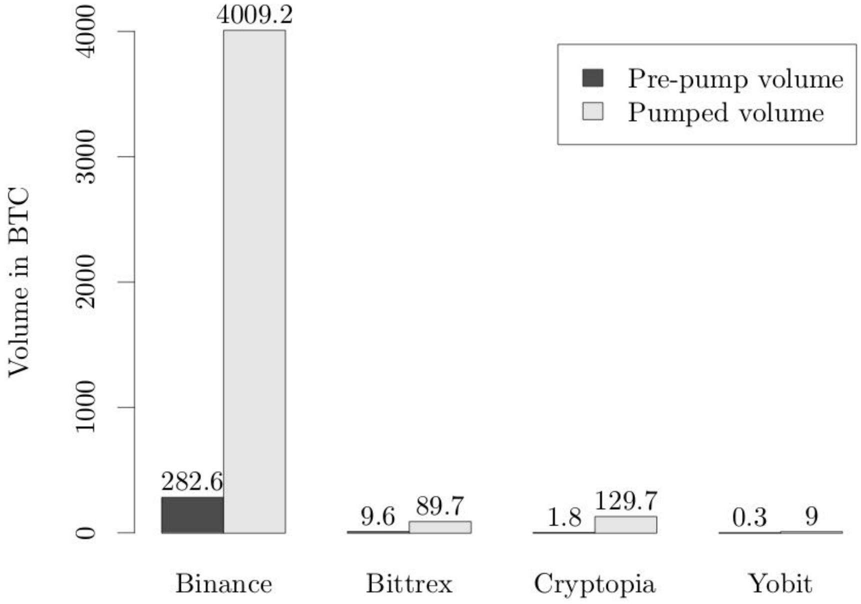


https://fc19.ifca.ai/preproceedings/130-preproceedings.pdf

The Anatomy of a Cryptocurrency Pump-and-Dump Scheme

220 observed pump-and-dump events on Telegram

Up to 80% profits from pump-and-dump trading



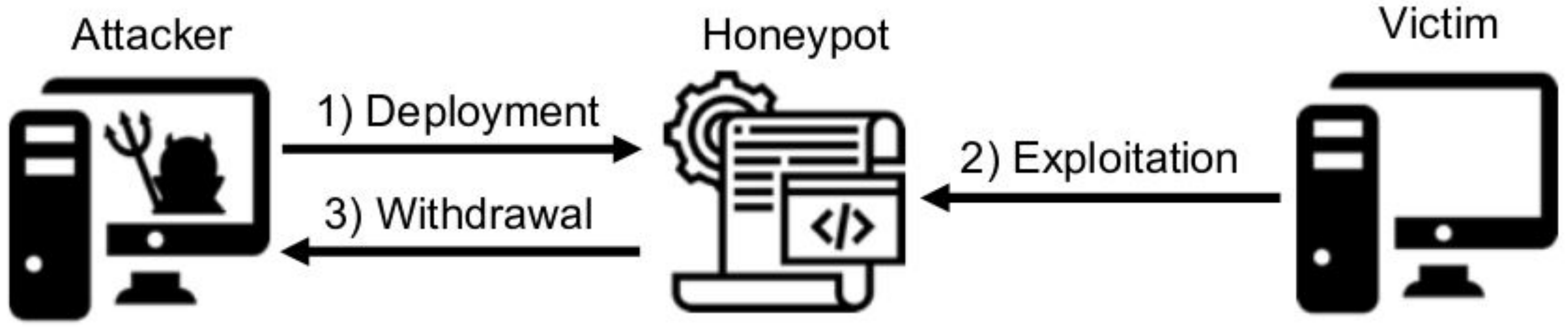
https://arxiv.org/pdf/1811.10109.pdf

The Art of The Scam: Demystifying Honeypots in Ethereum Smart Contracts

---

Identified 690 honeypot contracts on Ethereum (87% accuracy)

Verified 240 victims with 90,000 USD being stolen

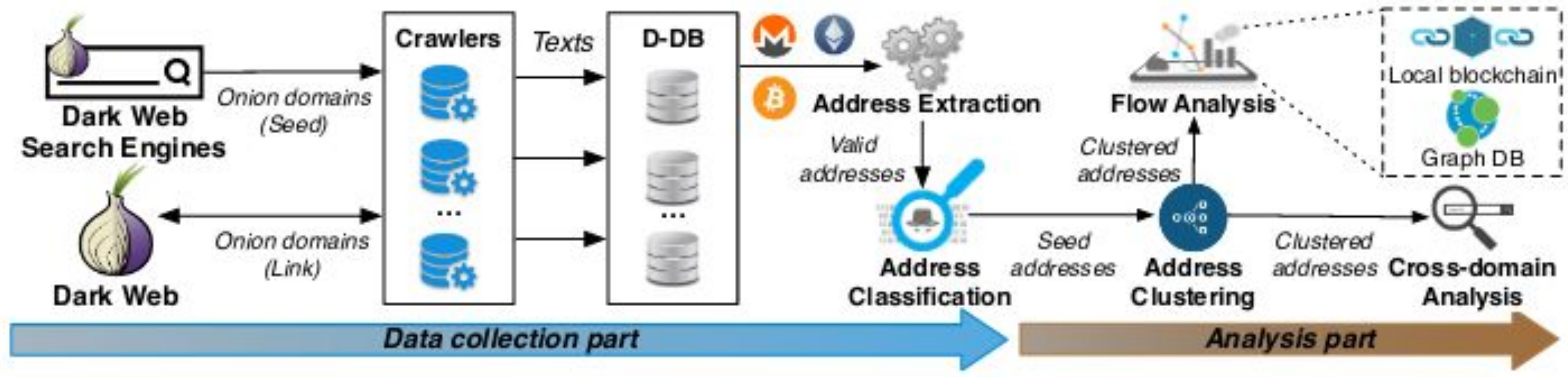


https://arxiv.org/pdf/1902.06976.pdf

Cybercriminal Minds: An investigative study of cryptocurrency abuses in the Dark Web

---

Around 4,500 cryptocurrency addresses are used for illicit activities (83,75%)

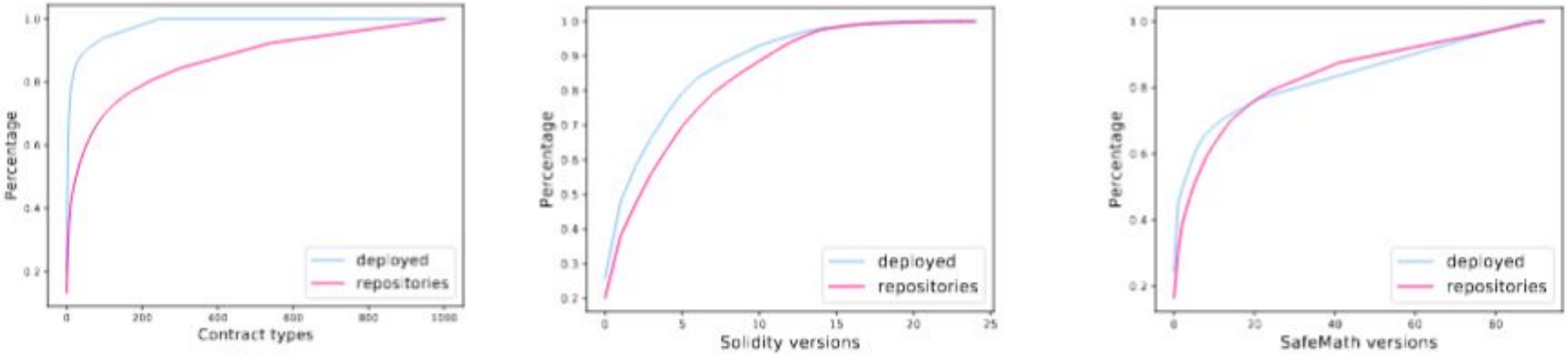


https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_09-1_Lee_paper.pdf

So many crypto projects?

Short Paper: An Exploration of Code Diversity in the Cryptocurrency Landscape

Code for new cryptocurrencies is usually copied from Bitcoin and Ethereum



(a) Types (b) Solidity version (c) SafeMath version

https://fc19.ifca.ai/preproceedings/134-preproceedings.pdf

Improving smart contracts

BitML: A Calculus for Bitcoin Smart Contracts

Write Bitcoin smart contracts in a higher-order logic

Allows construction of contracts over multiple transactions

$$
\begin{aligned}
\mathit{Escrow} &= \mathit{PayOrRefund} + \mathsf{A} : \mathit{Resolve}_{0.1,0.9} + \mathsf{B} : \mathit{Resolve}_{0.1,0.9} \\
\mathit{Resolve}_{v,v'} &= \texttt{split}(v\text{₿} \to \texttt{withdraw}\ \mathsf{M} \\
&\qquad\qquad \mid v'\text{₿} \to \mathsf{M} : \texttt{withdraw}\ \mathsf{A} + \mathsf{M} : \texttt{withdraw}\ \mathsf{B})
\end{aligned}
$$

https://eprint.iacr.org/2018/122.pdf

FASTKITTEN: Practical Smart Contracts on Bitcoin

Execute smart contracts in a Trusted Execution Environment

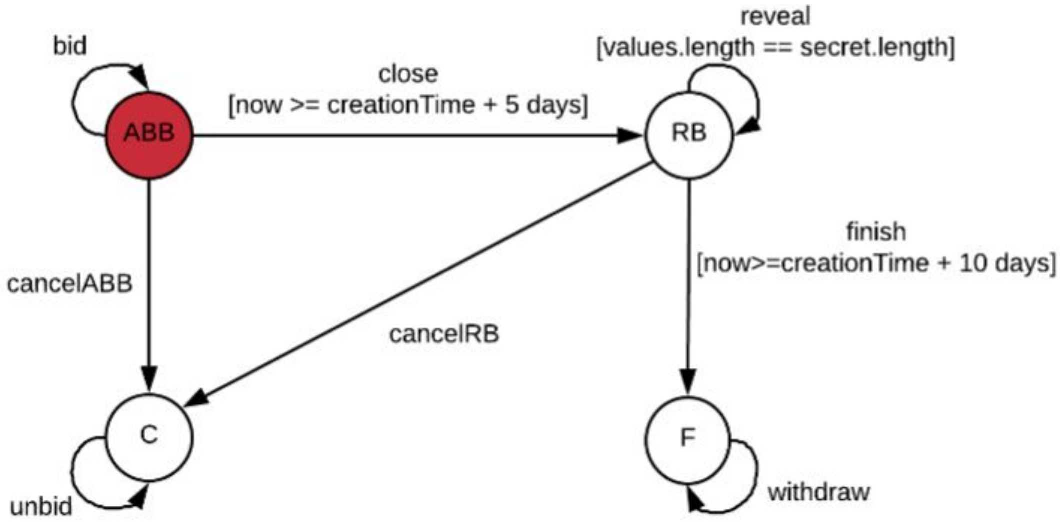
TEE can be hosted by an untrusted operator

Approach	Minimal # TX	Collateral	Generic Contracts	Privacy
Ethereum contracts	$\mathcal{O}(m)$	$\mathcal{O}(n)$	✓	✗
MPC [38–40]	$\mathcal{O}(1)$	$\mathcal{O}\left(n^2 m\right)$	✓	✓
Ekiden [19]	$\mathcal{O}(m)$	no support for money		✓
FASTKITTEN	$\mathcal{O}(1)$	$\mathcal{O}(n)$	✓	✓

https://www.usenix.org/system/files/sec19fall_das_prepub.pdf

VeriSolid: Correct-by-Design Smart Contracts for Ethereum

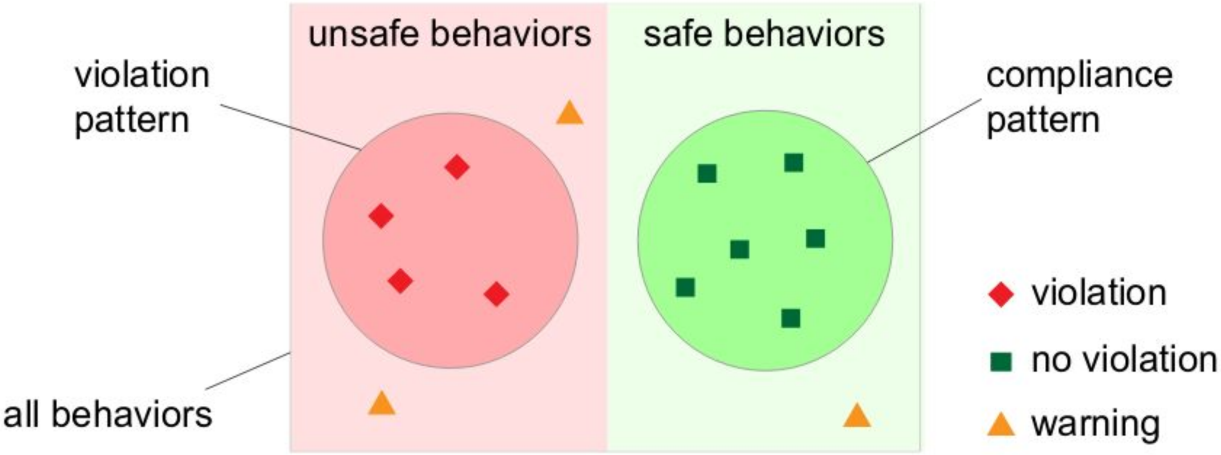
Model Ethereum smart contracts as state machines



https://fc19.ifca.ai/preproceedings/200-preproceedings.pdf

Securify: Practical Security Analysis of Smart Contracts

Use Datalog to reason about smart contract compliance



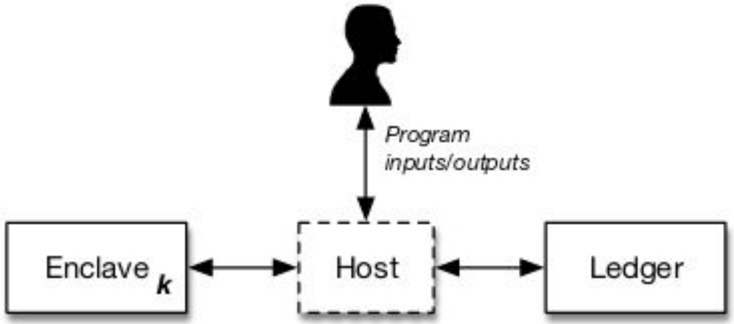
https://arxiv.org/pdf/1806.01143.pdf

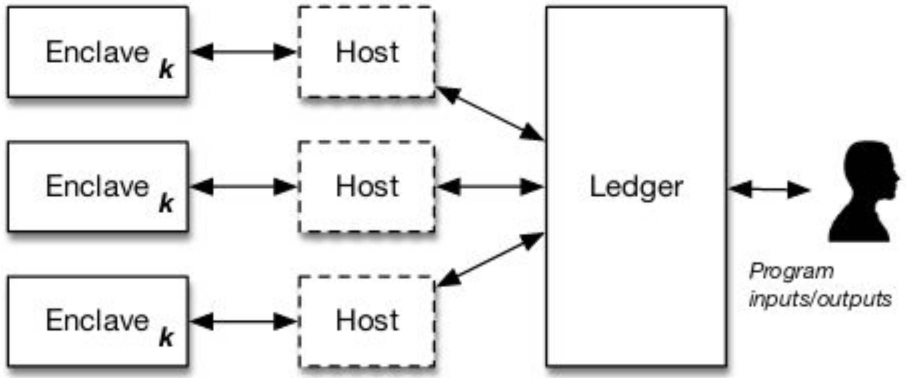
Giving State to the Stateless: Augmenting Trustworthy Computation with Ledgers

---

Use existing TEE (mobile devices, SGX, TrustZone, virtual)

Private smart contracts, mandatory logging, encrypted backups, and fairness in multi-party computation





https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-5_Kaptchuk_paper.pdf

Governance

A Treasury System for Cryptocurrencies: Enabling Better Collaborative Intelligence

---

Formally proven security proofs for voting on projects

Zero-knowledge votes with efficient proof scheme

https://www.ndss-symposium.org/wp-content/uploads/2019/02/ndss2019_02A-2_Zhang_paper.pdf

Applications anyone?

ROYALE: A Framework for Universally Composable Card Games with Financial Rewards and Penalties Enforcement

	Computational Complexity			Communication Complexity		
	Shuffle Cards	Open Private Card (drawer ;others)	Open Public Card	Shuffle Cards	Open Private Card (drawer ;others)	Open Public Card
[3]	$240m(n-1)$ $+161m$	$4n-3;3$	$4n$	$164nm\ \mathbb{G}$, $122nm\ \mathbb{Z}_p$	$45nm\ \mathbb{G}$, $(2n^2+$ $80n+2nm)\ \mathbb{Z}_p$	$n(17m+5)\ \mathbb{G}$, $n(m+18)\ \mathbb{Z}_p$
[7] ([33])	$(44n+1)m$	$4n-3;3$	$4n$	$3(n-1)\ \mathbb{G}$, $2(n-1)\ \mathbb{Z}_p$	$(n-1)\ \mathbb{G}$, $2(n-1)\ \mathbb{Z}_p$	$(n-1)\ \mathbb{G}$, $2(n-1)\ \mathbb{Z}_p$
[7] ([32])	$81m+2n$ $+25$	$4n-3;3$	$4n$	$3n\ \mathbb{G}$, $2n\ \mathbb{Z}_p$	$n\ \mathbb{G}$, $2n\ \mathbb{Z}_p$	$n\ \mathbb{G}$, $2n\ \mathbb{Z}_p$
Royale	$(2\log(\lceil\sqrt{m}\rceil)$ $+4n-2)m$	$4n-3;3$	$4n$	$n(2m+\lceil\sqrt{m}\rceil)\ \mathbb{G}$, $5n\lceil\sqrt{m}\rceil\ \mathbb{Z}_p$	$(n-1)\ \mathbb{G}$, $2(n-1)\ \mathbb{Z}_p$	$n\ \mathbb{G}$, $2n\ \mathbb{Z}_p$

https://fc19.ifca.ai/preproceedings/111-preproceedings.pdf

Thanks!