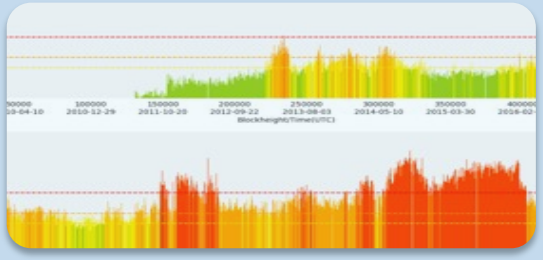
universität wien

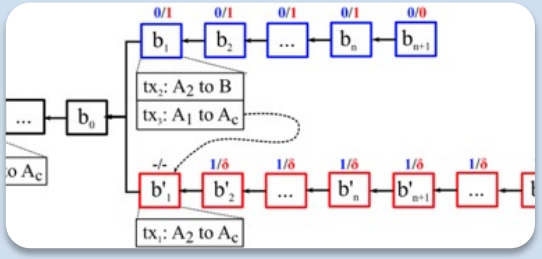
Distributed Ledger Technology, Blockchain & Crypto Currencies

Edgar.Weippl@univie.ac.at

Research



Exploring Reality

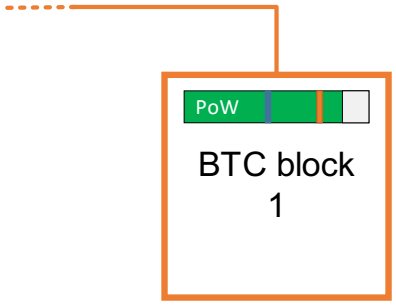


Theoretical Foundations, Algorithms

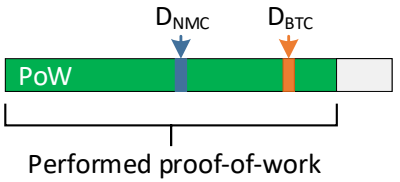
Real-World Impact

TLP White

Exploring Reality

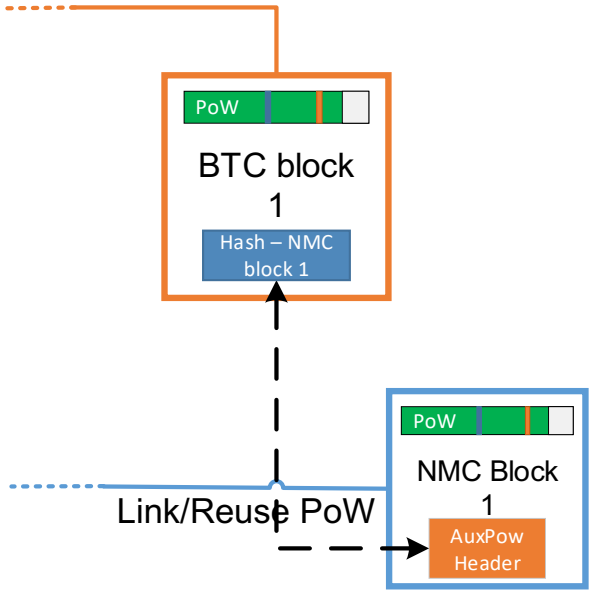


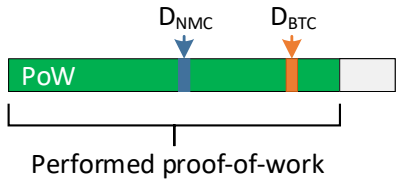
Echoes of the past: Recovering blockchain metrics from merged mining. Financial Crypto 2019.



TLP White

Exploring Reality

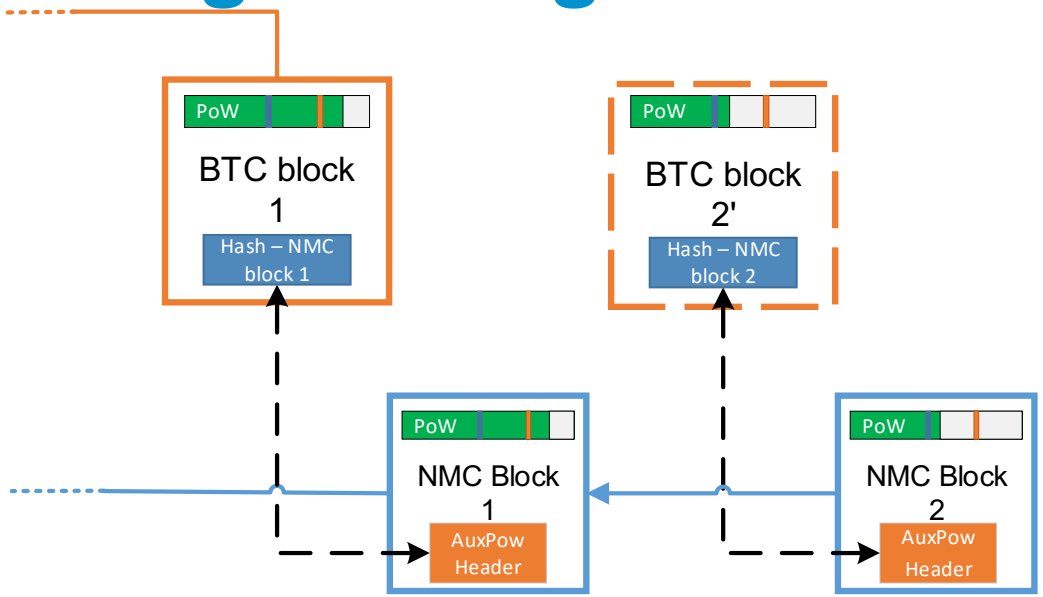




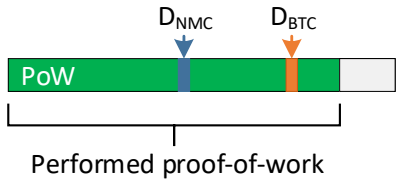
TLP White

Exploring Reality

Merged Mining



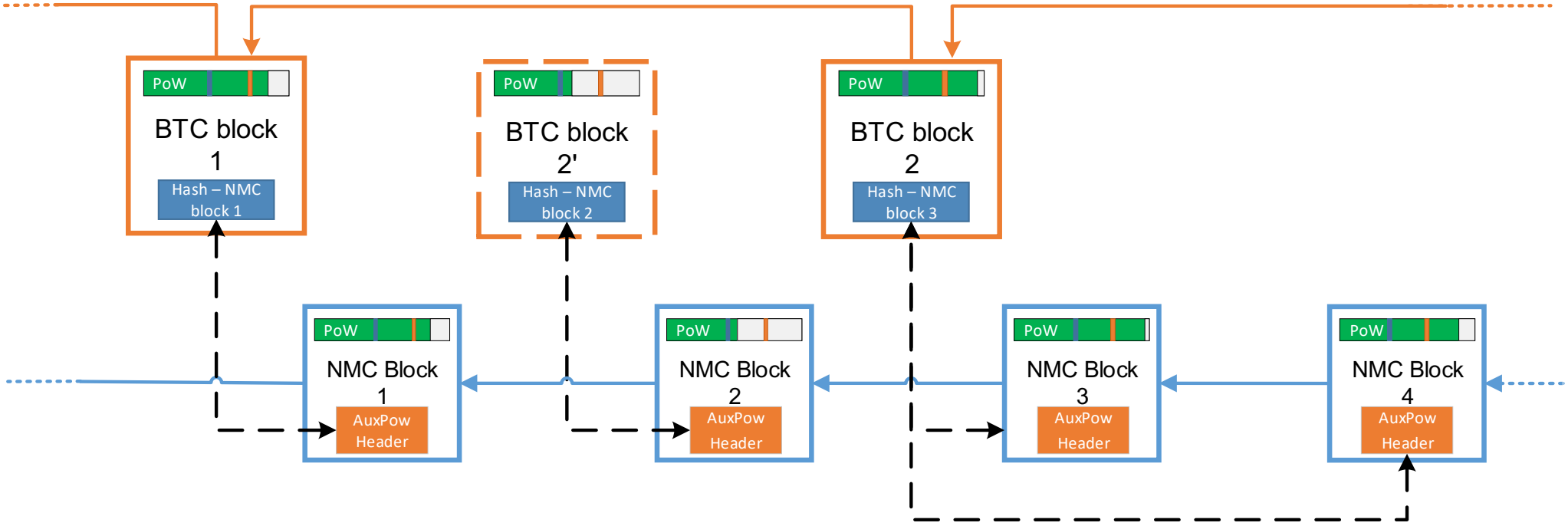
Reuse possible **even if PoW not enough for parent**



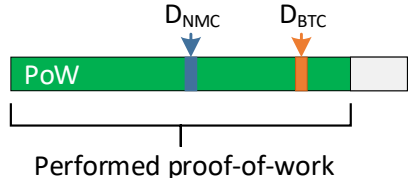
TLP White

Exploring Reality

Merged Mining

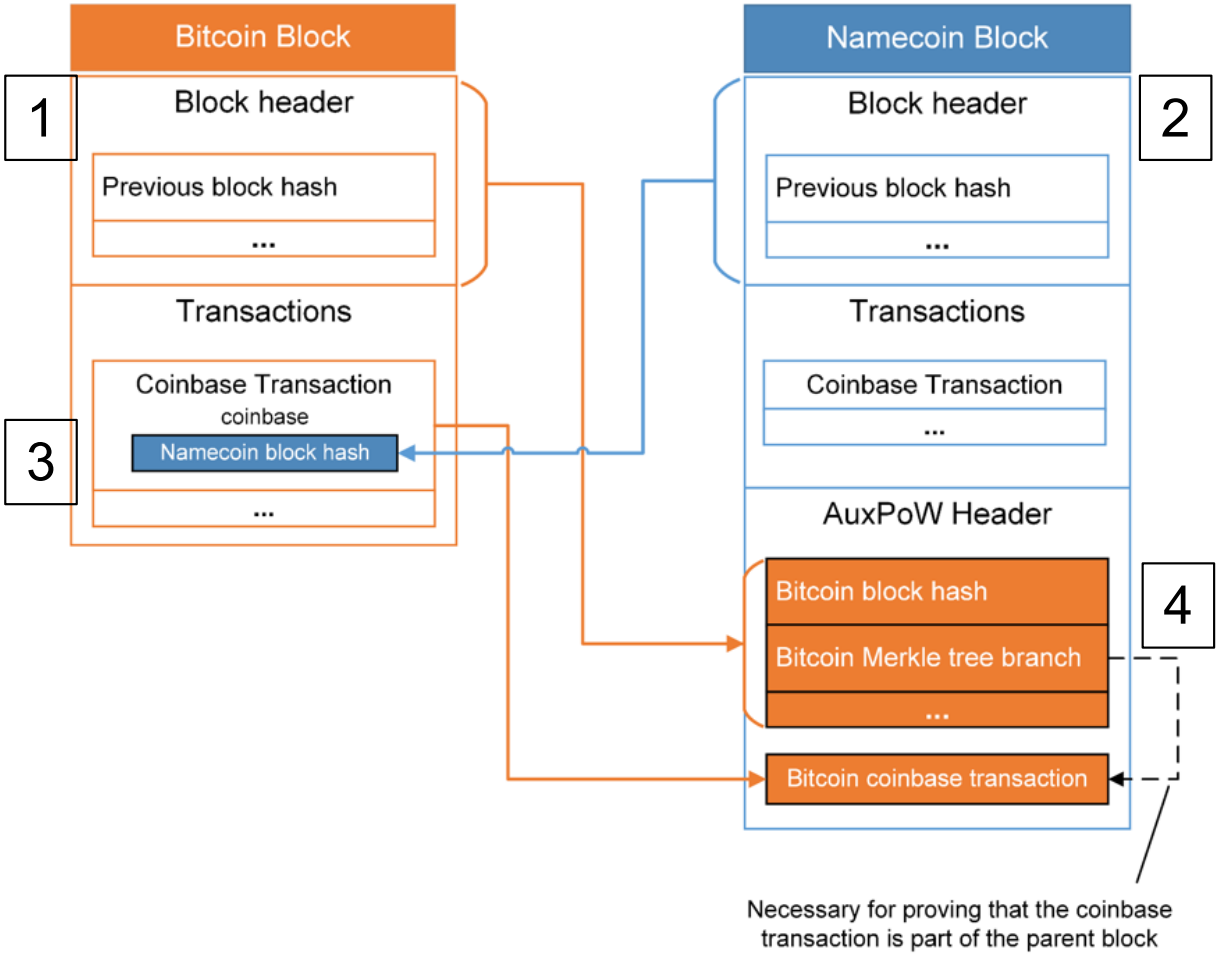


Multi-reuse possible

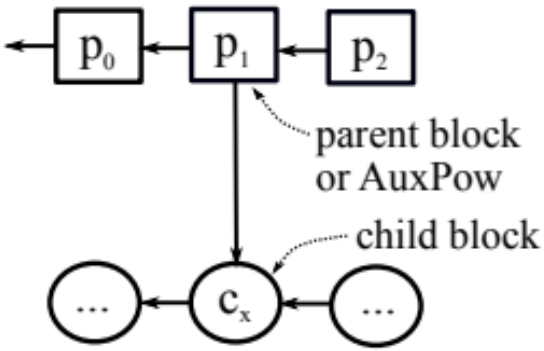


TLP White

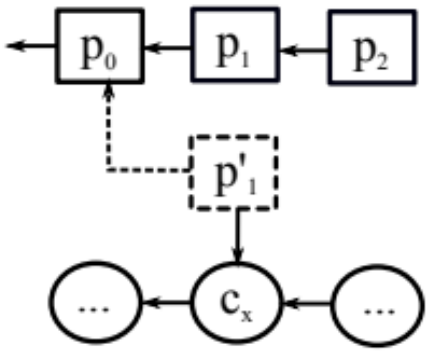
Exploring Reality



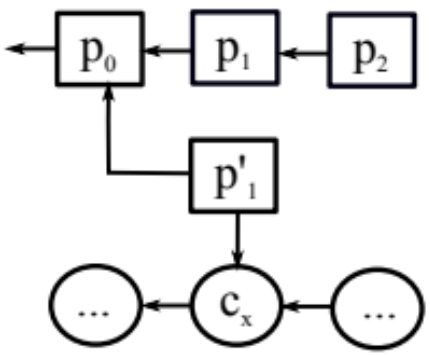
Exploring Reality



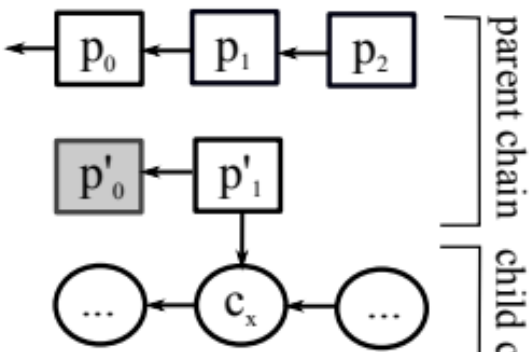
p_1 is a *merge-mined canonical block* if
$p_1 \in$ parent main chain



p'_1 is a *near block* if
$d(p'_1) < d(p_1)$



p'_1 is a *stale block* if
$d(p'_1) \geq d(p_1)$

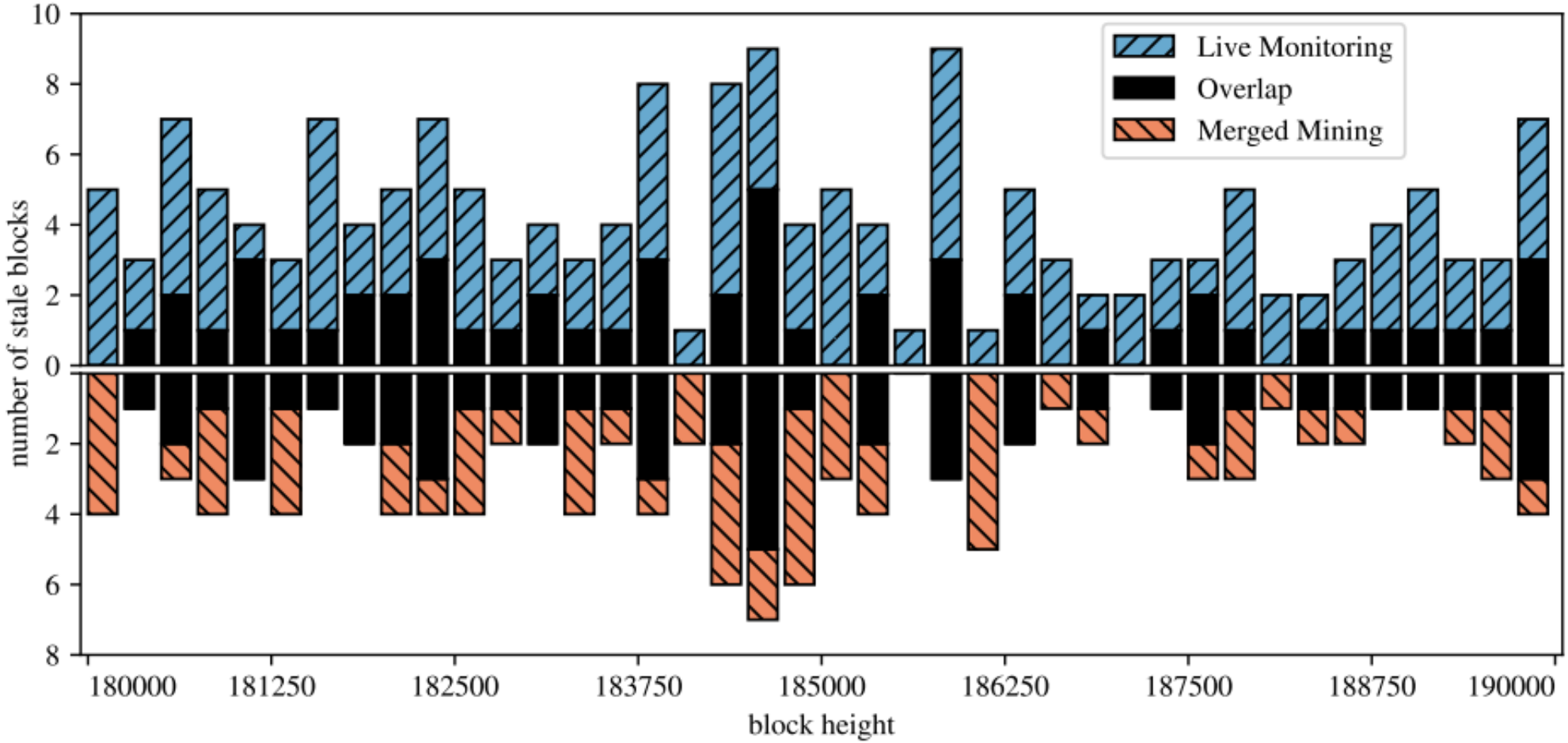


p'_0 is a *shadow bock* if
$d(\text{hash}(p'_0)) \geq d(p_0)$

p'_1 is an *orphan bock* if
$d(p_1) \geq d(p_1)$

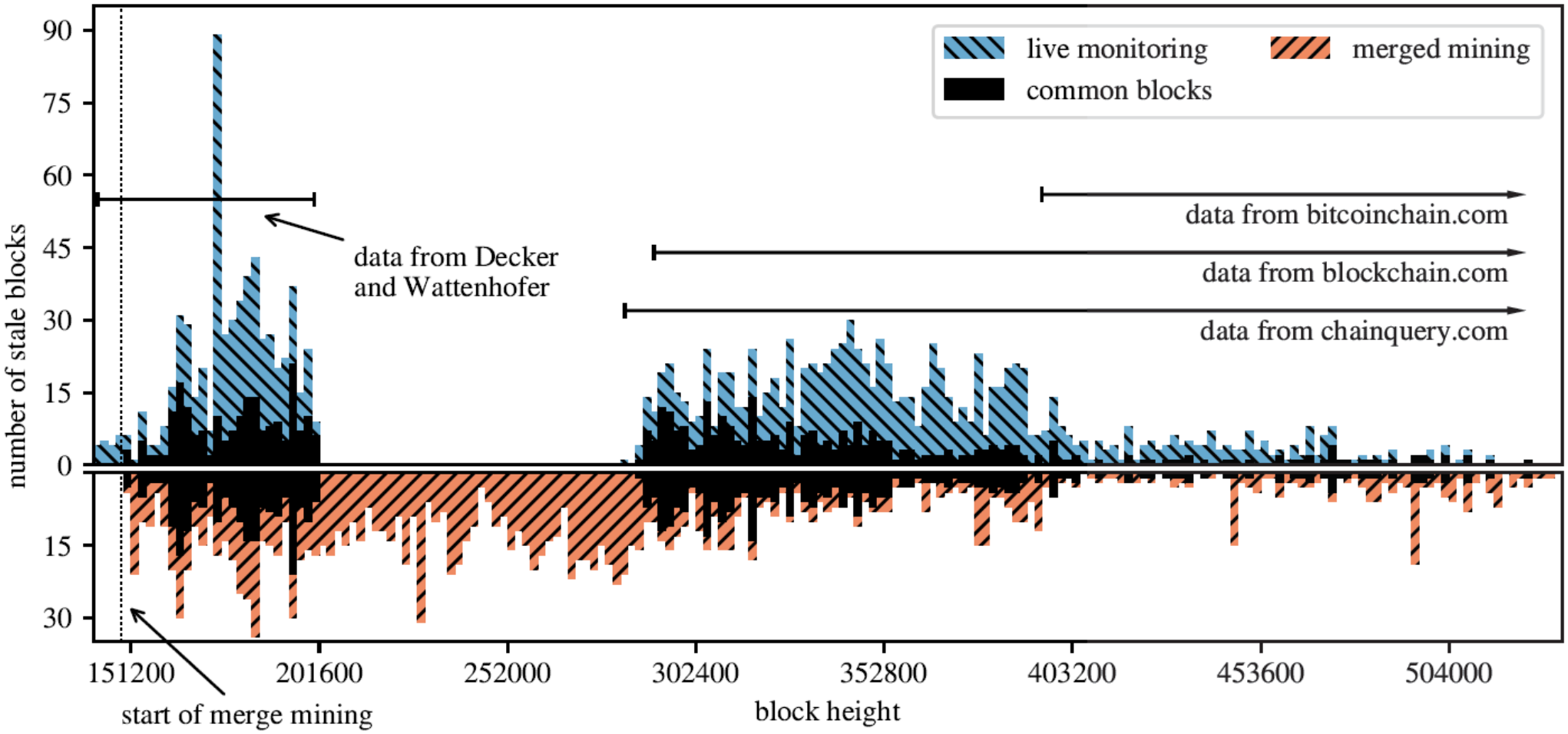
TLP White

Exploring Reality



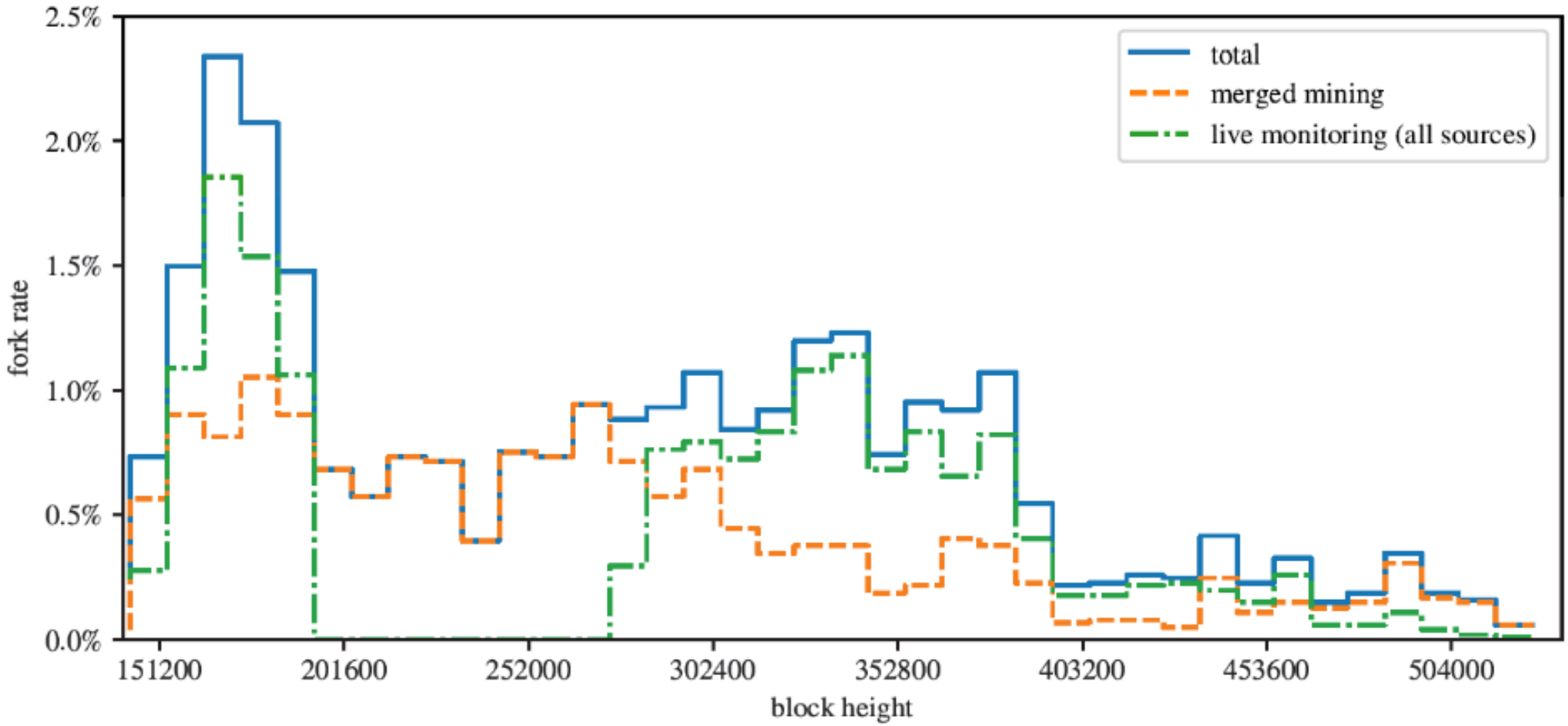
TLP White

Exploring Reality



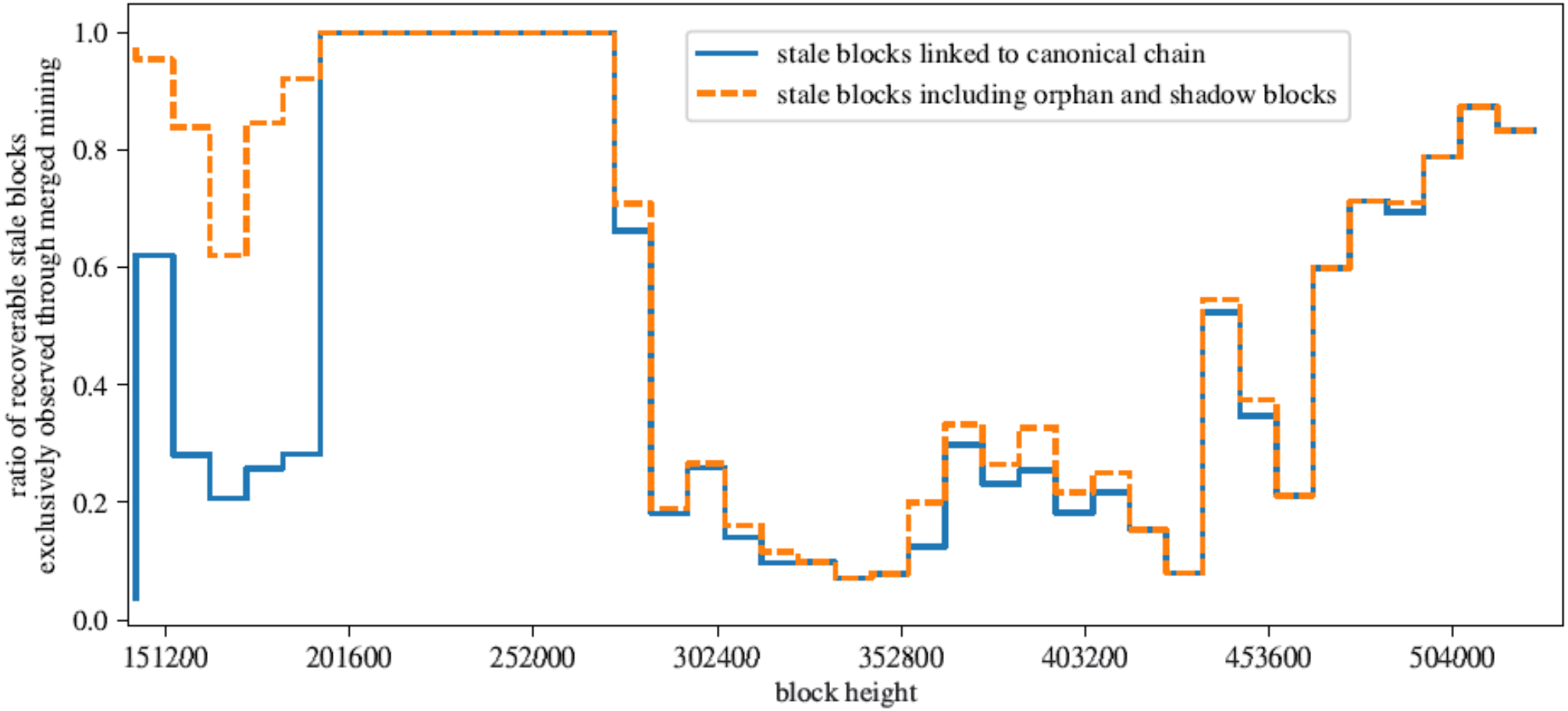
TLP White

Exploring Reality



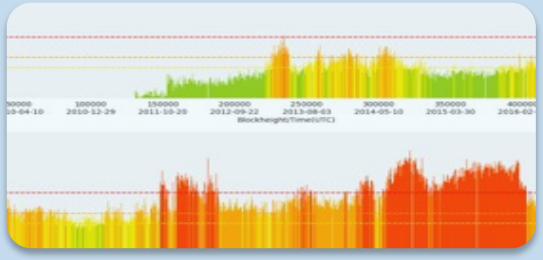
TLP White

Exploring Reality

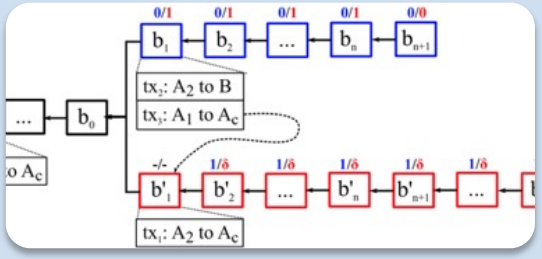


TLP White

Research



Exploring Reality



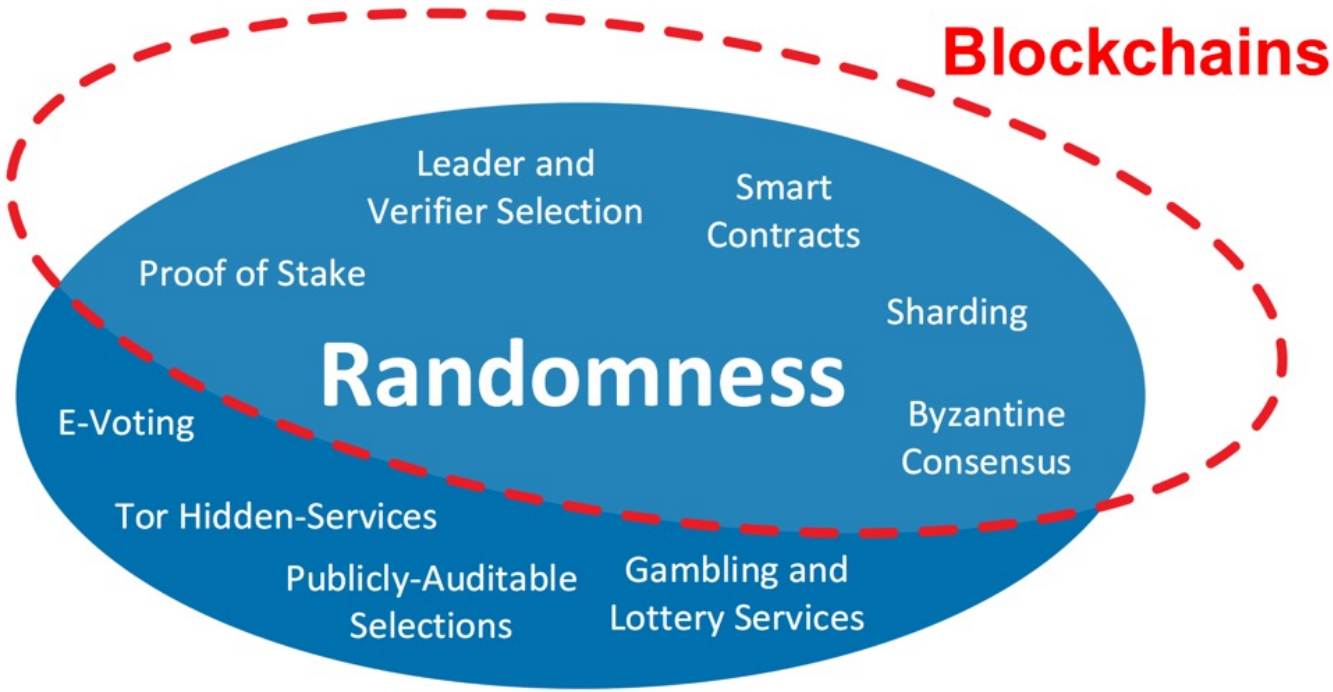
Theoretical Foundations, Algorithms

Real-World Impact

TLP White

Theory

Randomness in Decentralized Systems



TLP White

Theory

HydRand: Practical Continuous Distributed Randomness

- Core building block for PoS protocols and essential primitive in the context of smart contracts
- Can be readily implemented and serve at the core of a Blockchain protocol
- Applicable to both permissioned and permissionless Blockchains

Philipp Schindler, Aljosha Judmayer, Nicholas Stifter, and Edgar Weippl. **Hydrand: Practical continuous distributed randomness**. In IEEE S&P, 2020.

Philipp Schindler, Aljosha Judmayer, Markus Hittmeir, Nicholas Stifter, and Edgar Weippl. **RandRunner: Distributed Randomness from Trapdoor VDFs with Strong Uniqueness**, NDSS Symposium 2021

Theory

Protocol Properties


Bias-Resistance


Scalability

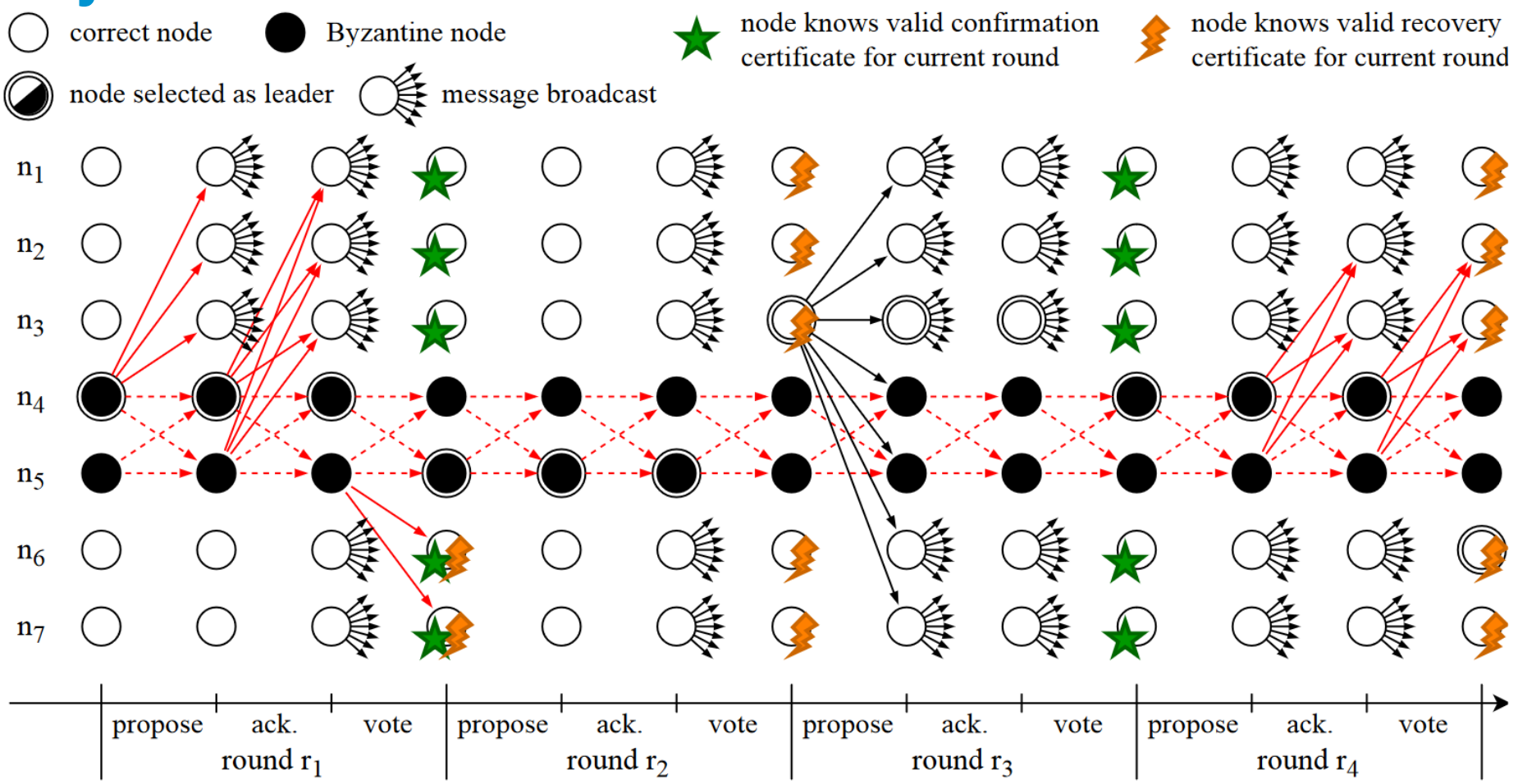

Public-Verifiability


Liveness


Unpredictability

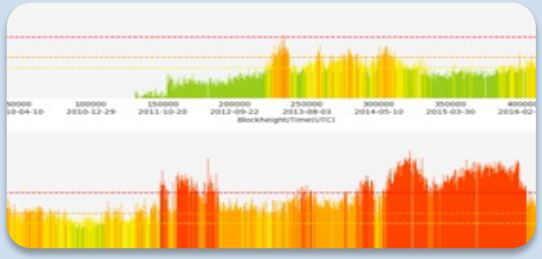
Theory

HydRand:

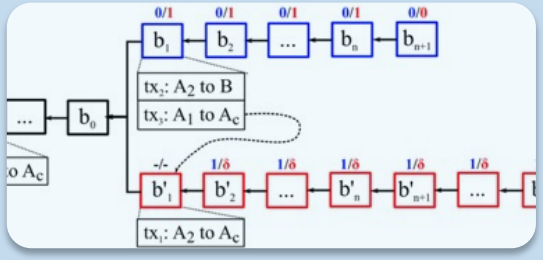


TLP White

Research



Exploring Reality



Theoretical Foundations, Algorithms

Real-World Impact

TLP White

Impact

Opportunistic Algorithmic Double-Spending & Pay To Win: Cheap, Crowdfundable, Cross-chain Algorithmic Incentive Manipulation Attacks on PoW Cryptocurrencies

Opportunistic Algorithmic Double-Spending: How I Learned to Stop Worrying and Love the Fork, Nicholas Stifter, Aljosha Judmayer, Philipp Schindler, and Edgar Weippl. In Computer Security – ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part I. Springer-Verlag, Berlin, Heidelberg, 46–66. https://doi.org/10.1007/978-3-031-17140-6_3

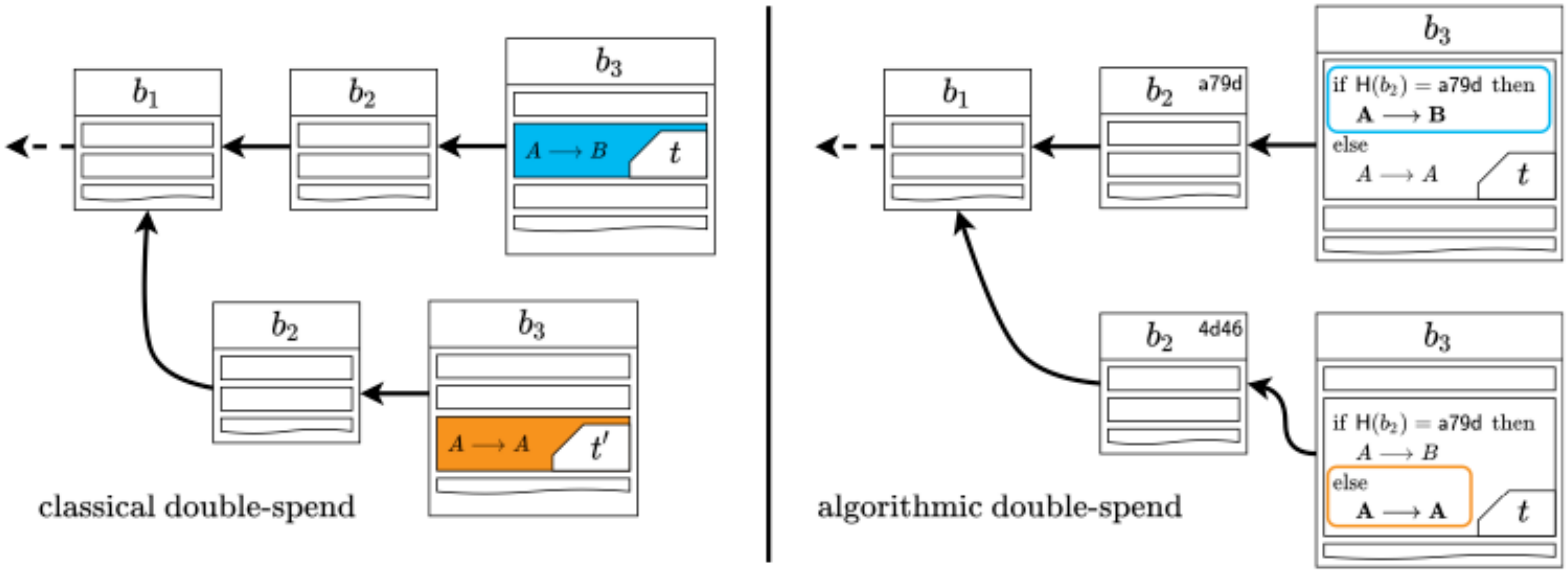
Pay To Win: Cheap, Crowdfundable, Cross-chain Algorithmic Incentive Manipulation Attacks on PoW Cryptocurrencies, Aljosha Judmayer, Nicholas Stifter, Alexei Zamyatin, Itay Tsabary, Peter Gaži, Sarah Meiklejohn, Edgar Weippl, March/2021, Workshop on Trusted Smart Contracts (Financial Cryptography 2021)

Incentive Attacks

- Impact on transactions
  - Transaction revision
  - Transaction ordering
  - Transaction exclusion
- Required interference with consensus
  - Deep fork
  - Near fork
  - No fork
- Attack chain
  - In-band attacks
  - Out-of-band attacks

Impact

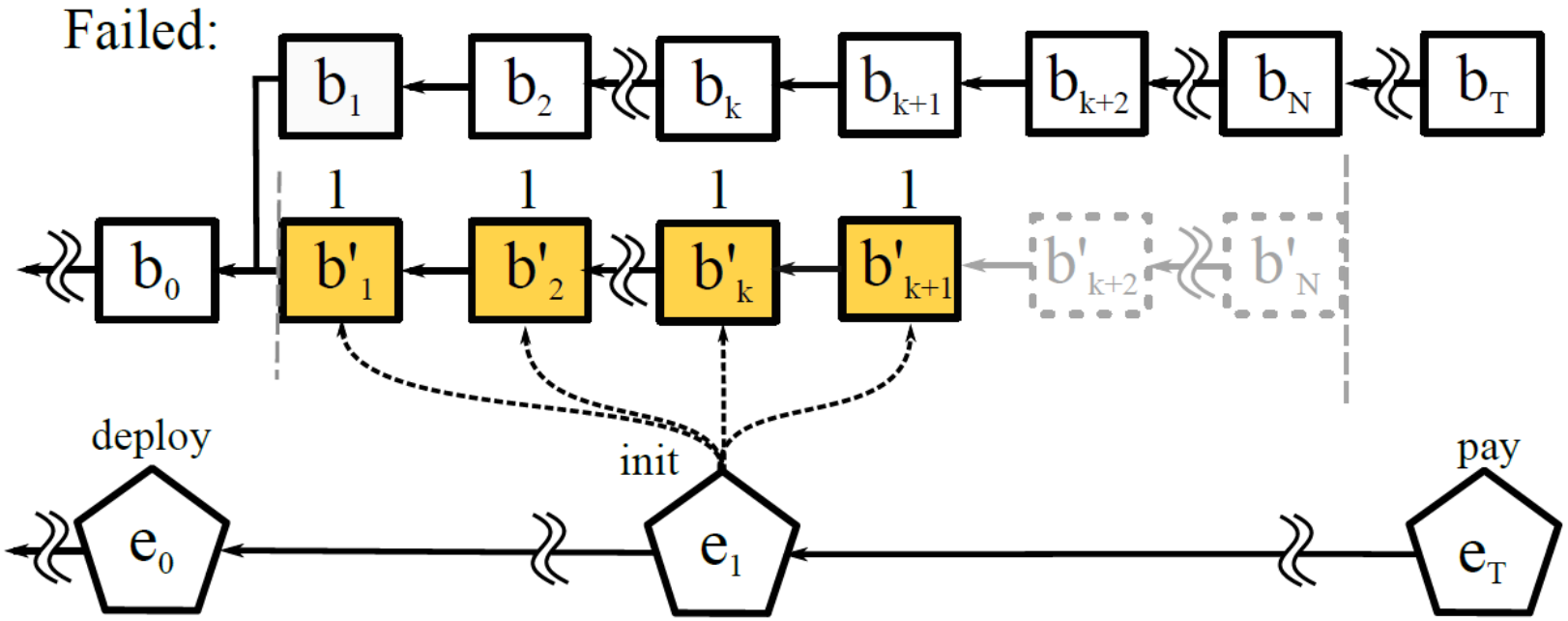
Out-of-Band TX Revision Attack



TLP White

Impact

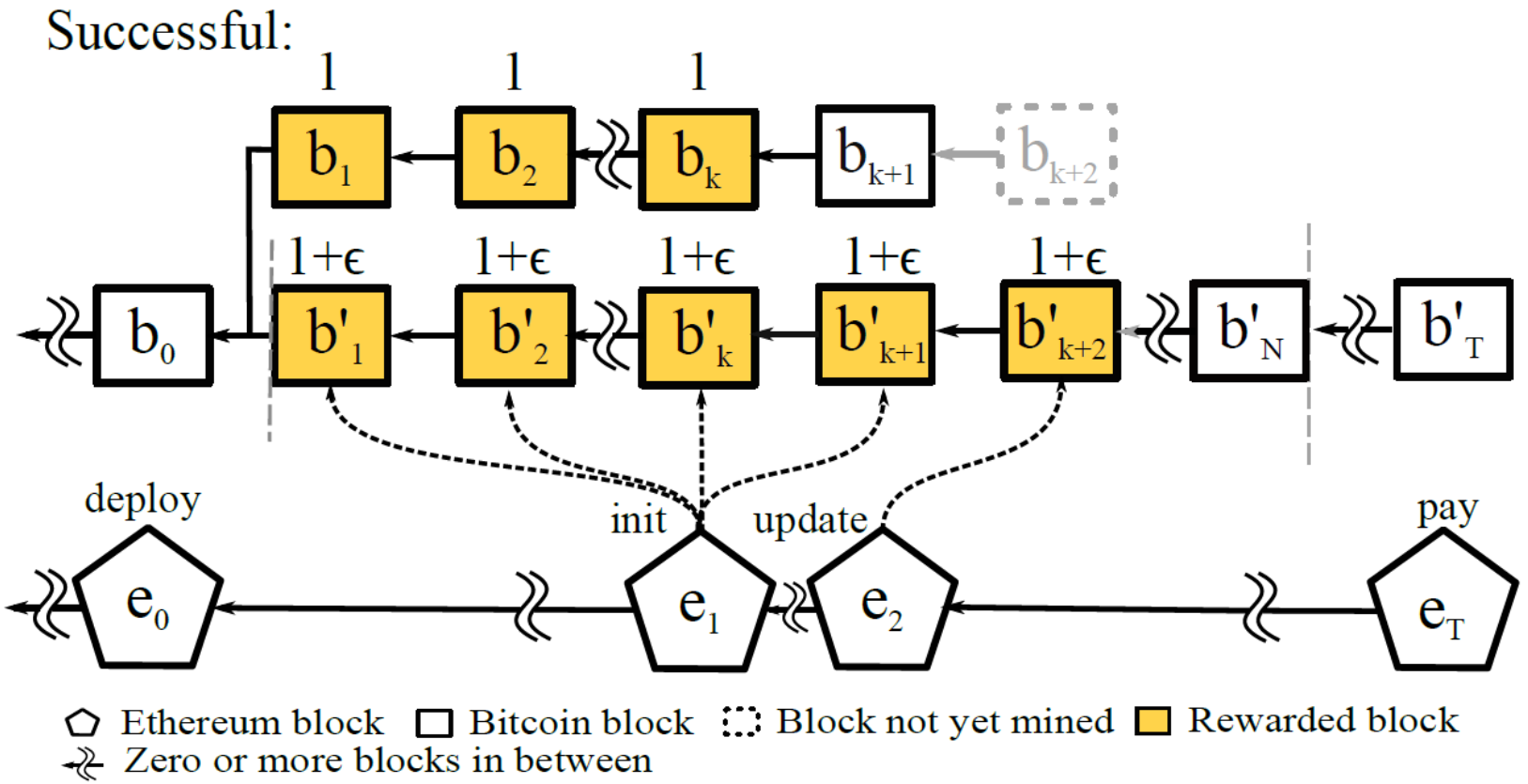
Out-of-Band TX Revision Attack – Failed



TLP White

Impact

Out-of-Band TX Revision Attack – Successful



TLP White

Impact

Outlook

- Incentive Attacks
  - Crowdsourcing
  - Piggybacking
  - Counter Attacks
  - Improved Modeling of Miners
    - rational miners,
    - altruistic miners,
    - merged miners (“pitchfork”)…
- Future Work
  - Who has power? Users, Miners, Software Developers
  - Challenging assumptions (e.g. rationale miner; decentralized network; …)