Publicly Verifiable Argument Systems Through Generic Blockchains

Alessandra Scafuro
NCSU

Luisa Siniscalchi
DIEM - Università di Salerno

Ivan Visconti
DIEM - Università di Salerno

Blockchain and Security Issues

- Blockchains are largely maintained by unknown computers in untrusted countries
- Moreover, we are aware of several spectacular attacks and various security issues
  - The DAO 2016 (recursive call bug)
  - Zcash 2018 (unlimited token printing)
  - QuadrigaCX 2019 (key lost)
  - … and more (stay tuned)

What is Behind the Success of Cryptocurrencies?

Why are we converting real money into cryptocurrencies managed by unknown computers that run potentially flawed protocols using poor key-storage mechanisms?

Public Verifiability

- One of the most supported answers is

Public Verifiability

- Every action on a blockchain is publicly verifiable
- Everyone can check that the system works properly as specified by the rules of the game
- This makes users willing to be involved in transactions recorded in a blockchain even at the point of investing their real-world money
- Public Verifiability is Disruptive

Public Verifiability and GDPR

- The dark side of public verifiability is the obvious conflict with privacy regulations and the private data used in blockchain applications
- At first sight, privacy and public verifiability seem to be mutually exclusive

Privacy-Preserving Cryptography

- Advanced Cryptography can help to mitigate the above tension
- Data can be encrypted in the blockchain, losing public verifiability but protecting privacy
- Privacy-preserving cryptography can add public verifiability while keeping privacy

In Theory: Privacy-Preserving Proofs

Nakamoto

PPP

Verifier

I Know the secret key of Satoshi Nakamoto
OR I know your secret key

In Practice: Non-Interactive Zero-Knowledge Proofs

Nakamoto

NIZK

Verifier

- NIZK guarantees that the secret used to produce the proof remains secret
- NIZK ensures the veracity of the proven statement
- The Cryptocurrency ZCash is based on special NIZK called ZKSnarks

NIZK Proofs are Tough

- NIZK proofs are complicated and quite hard to construct
- The known NIZK proofs are based on
    - Heuristics assumptions
    - Trusted setup
- ZCash builds both on both heuristic assumptions and trusted setup
- Natual open question: can we obtain privacy-preserving publicly verifiable proofs without paying the price of NIZK?

IACR-PKC 2019
Public Verifiability from Blockchains

- In our work we give a positive answer
  - The key point is to introduce a new formulation for public verifiability
  - Public verifiability is still achieved through non-interactive verification
  - Instead the process of computing a proof can be interactive

A Prover Playing with the Blockchain

- The process of computing a proof can be interactive
- The prover interacts with the blockchain in order to compute a proof in multiple steps
- The verifier just reads the multiple pieces and locally decides to accept or reject the proof

Several Technical Challenges

- We extract random bits from the blockchain
- We provide succinct proofs that can fit the space allowed for a transaction in a block of the blockchain

What do We Need from a Blockchain?

- Our assumption: most of the blocks are added by honest miners
- This assumption must hold also in presence of our publicly verifiable ZK proofs

Attack of the Clones

- This is a more general problem
- For any use of the blockchain one should check that this use is safe w.r.t. the blockchain properties (e.g. 6-block confirmation rule in Bitcoin)
- We show a new attack to proof of stake (PoS) blockchains

Part of this work appears in IACR conference PKC 2019, the rest is ongoing work. Feel free to contact us if you want to hear more about it.

Thanks!