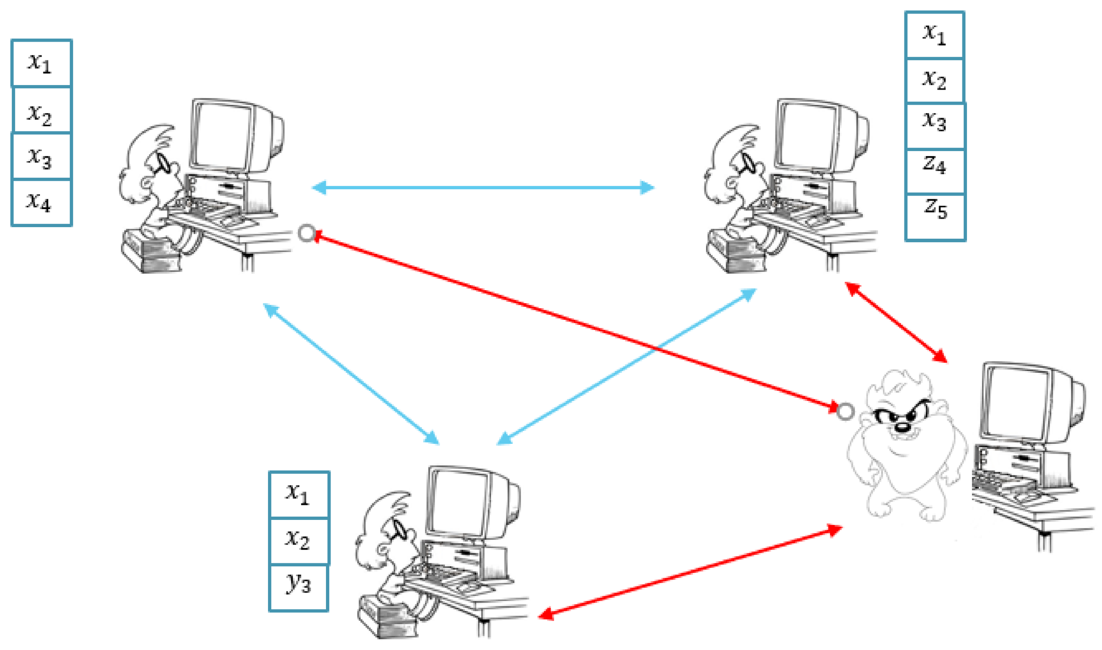
The Bitcoin Backbone Protocol Against Quantum Adversaries

Alexandru Cojocaru, Juan Garay, Aggelos Kiayias, Fang Song, Petros Wallden

Bitcoin Backbone Protocol



- All honest parties and adversaries are classical;
- t adversaries, $n - t$ honest parties – honest majority assumption;
- In a single round, in order to break a PoW, each party (honest or adversary) has q queries to H
- H is modelled as a Classical Random Oracle;
- **PoW** - Party convinces others he invested effort for solving a task: Find witness y such that $H(x, y) < D$, where x - hash of the last block.

Our Results

Security against Quantum Adversaries holds by bounding:
Quantum adversarial hashing power relative to honest classical hashing power

1. Quantum queries so that each quantum query is worth $O(p^{-1/2})$ classical ones
2. Wait time for safe settlement is expanded by a factor of $O(p^{-1/6})$

where p = probability of success of a single classical query

Underlying Abstract Problem

- Quantum Adversary tries to produce a chain longer than honest chain;
- Translates to a search problem where output is a chain of hashes (output of one hash is fed as input to next hash).

> Problem Π_G: Chain-of-PoWs
> **Given**: N, $x_0 \in X$, δ and $h_0, \dots, h_{N-1}$ as (quantum) random oracles, where each $h_i : X \times Y \to X$ is independently sampled.
> **Goal**: Using N total queries find a sequence $y_0, \dots, y_{k-1}$ such that $x_{i+1} := h_i(x_i, y_i)$ and $x_{i+1} \leq D \ \forall \ i \in \{0, \cdots, k-1\}$ such that the length of the sequence $k \leq N$ is the maximum that can be achieved with success probability at least δ.

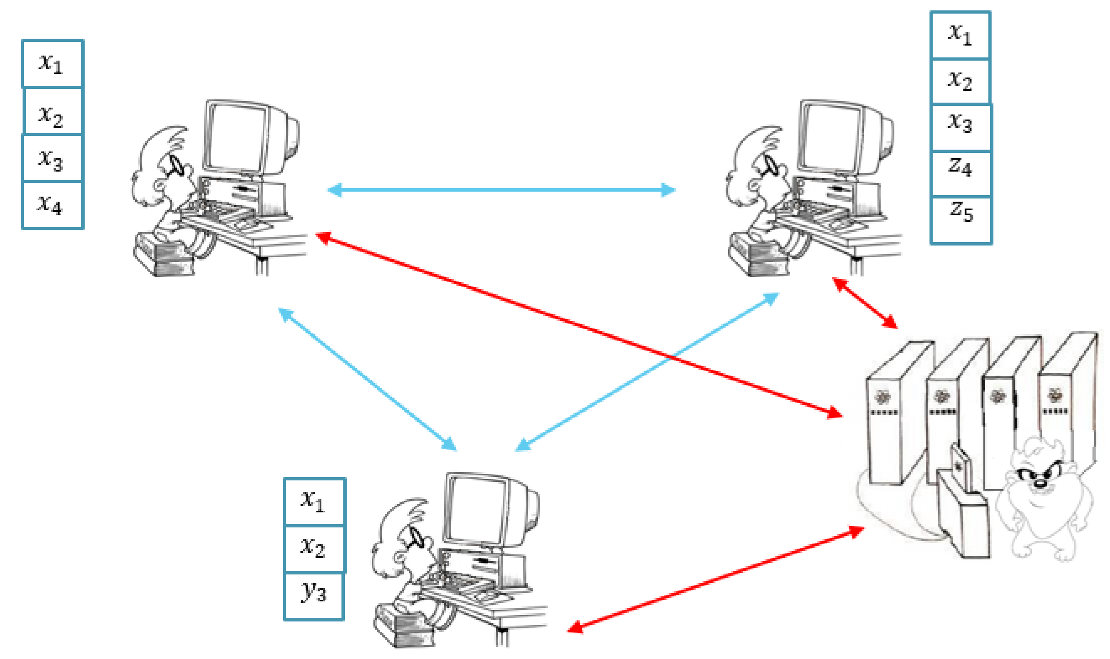
Sequential Measurements Strategy (SMS) for Bag-of-PoWs

Adversary that given N queries solves Bag-of-PoWs in a sequential way (following an order). Number of queries K_i spent for each oracle h_i satisfy:

1. $\sum_{i=1}^{N} K_i = N$
2. Choice of K_i depends only on:
   (a) Number of left queries $N - (K_1 + \cdots + K_{i-1})$
   (b) Previous searches outcomes $[w_1, \cdots, w_{i-1}]$ - w_i indicates if a PoW was solved using i-th oracle

- SMS are **optimal** for Bag-of-PoWs
- For the most general SMS adversaries, variables are dependent:
- $\Rightarrow$ To bound number of adversarial PoWs using the maximal expectation value we need to use an **alternative concentration theorem**.

Post-Quantum Backbone



- Adversary is quantum;
- He is allowed to query H in superposition:

$$|y_1\rangle + \cdots |y_n\rangle \otimes |0\rangle \xrightarrow{O_H} |y_1\rangle\,|H(y_1)\rangle + \cdots + |y_n\rangle\,|H(y_n)\rangle$$

- We model the adversary as a single quantum adversary with N total queries, joint computational effort of the parties under his control

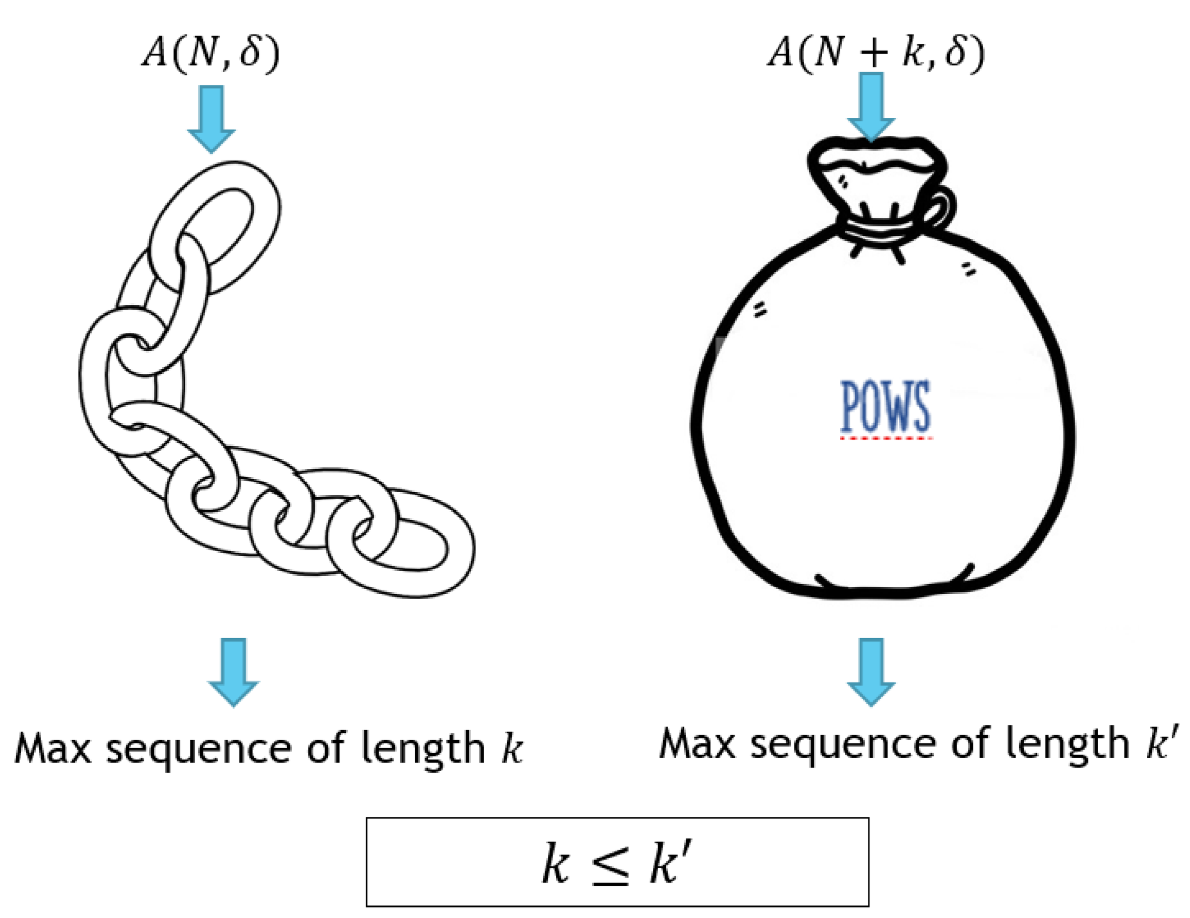
Bag-of-PoWs

Simplified problem asking for maximum cardinality of "*independent*" PoWs given fixed number N of queries and success probability δ

> Problem Π'_G: Bag-of-PoWs
> **Given**: N, δ and $h_0, \dots, h_{N-1}$ as oracles, where each $h_i : X \times Y \to X$ is independently sampled.
> **Goal**: Using N total number of queries find a set of pairs $\{(x_{i_1}, y_{i_1})_1, \dots, ((x_{i_k}, y_{i_k})_k)\}$ so that $h_{i_l}(x_{i_l}, y_{i_l}) \leq D$, for all $l \in \{1, \dots, k\}$, such that the cardinality $k \leq N$ of the set of pairs is the maximum that can be achieved with success probability at least δ. Note that in the set, each pair should correspond to different oracle.

Different blocks are neither sequential nor chained (they are independent)

Relation



Full paper: `https://eprint.iacr.org/2019/1150`