On the insecurity of quantum Bitcoin mining
arXiv:1804.08118

Or Sattath, Ben-Gurion University

QCrypt 2018

SUMMARY

- The Bitcoin network will become less secure once Bitcoin miners use a quantum computer.
- Quantum Bitcoin mining ➔ a high stale-rate in the Bitcoin blockchain.
- A higher stale-rate is known to have negative implications on Bitcoin's security
  - double-spending (51% attack) requires less computational power
  - selfish mining becomes profitable with a smaller hash-rate
  - longer confirmation times
- We proposed a countermeasure for this concern, by changing the Bitcoin protocol

HOW DOES BITCOIN WORK?

FIRST ATTEMPT

- Suppose you have an **append only, globally available** public bulleting board. How can such a bulletin board be used to construct a money system?

Attempt 1

- Distribution: Alice, Bob and Chalie get 10 coins each
- Alice sends 2 coins to David.
- Charlie sends 1 coin to Eve
- ~~Alice sends 20 coins to Francis.~~

Insufficient funds, ignored

Problem: David can append the message “Bob sends 10 coins to David”, and steal Bob’s coins.

Attempt 2: Digital signatures

- Distribution: Alice with pk_A, Bob with pk_B and Chalie with pk_C get 10 coins each
- Alice sends 2 coins to David with pk_d. Signature: 0110001010.
- ~~Bob sends 10 coins to David with pk_d. Signature: 11101101011~~

invalid signature.

Everyone checks that the signature is valid:
Verify(message,signature,public-key)=True?

IMPLEMENTING AN APPEND ONLY PUBLIC BULLETIN BOARD

- A cryptographic hash function H, such as SHA256 is modeled like a random function (random oracle model) $H: \{0,1\}^* \to \{0,1\}^{256}$.
- Transactions are flooded to a peer-to-peer network.
- Miners try to create a block by finding a "nonce" x such that H(prev_block_hash,time,x, transactions)<t .
- The threshold t is adjusted so that a block is mined every 10 minutes on average. The time is used to adjust the difficulty every 2016 blocks (~2 weeks): $t_{new} = t_{old} \cdot \frac{days\ for\ last\ 2014\ blocks}{14}$.
- This mechanism is called Proof-of-Work. Classically, it is progress free: the time you spent so far on finding a block does not affect your chances in finding a block in the next minute. The number of proofs / blocks found per minute has a Poisson distribution.

IMPLEMENTING AN APPEND ONLY PUBLIC BULLETIN BOARD (2)

- A miner who finds a valid block gets some bitcoins (started at 50, slashed in half every 4 years) from thin air.
- Honest miners keep evaluating the hash-function, until they win the lottery.

Target t=00400

Block hash	00214
Previous block	-
Miner's address	Satoshi2ff
Nonce	21231321
Time	8:00

Block hash	00312
Previous block	00214
Miner's address	miner2fsfsa
Nonce	5268363
Time	8:12
Tx1	Sat → usr1

Miner 1

Miner 2

Miner 3

Block hash	00214
Previous block	-
Miner's address	Satoshi2ff
Nonce	21231321
Time	8:00

Block hash	00312
Previous block	00214
Miner's address	miner2fsfsa
Nonce	5268363
Time	8:12
Tx1	Sat → usr1

Block hash	00108
Previous block	00312
Miner's address	miner1kds
Nonce	3729963
Time	8:19

Block hash	00223
Previous block	00312
Miner's address	miner3lqw
Nonce	3219411
Time	8:19
	usr1→usr2

Miner 1

Miner 2

Miner 3

FORKS

- Once in a while, there may be a fork: two miners, who haven't heard of each other's block, find two blocks.
- **Longest chain rule:** Honest users & miners follow the longest chain of blocks (hence, block-chain). In case of ties, they mine on top of the tip which they have heard first (this is subjective: two honest miners may mine on top of two different longest tips). Symmetry-breaking mechanism.

Block hash	00214
Previous block	-
Miner's address	Satoshi2ff
Nonce	21231321
Time	8:00

Block hash	00312
Previous block	00214
Miner's address	miner2fsfsa
Nonce	7421168
Time	8:12
Tx1	Sat → usr1

Block hash	00223
Previous block	00312
Miner's address	miner3lqw
Nonce	3219411
Time	8:19
	usr1→usr2

Block hash	00108
Previous block	00223
Miner's address	miner2fsfsa
Nonce	1183462
Time	8:31

Miner 1 | Miner 2 | Miner 3

IMPLEMENTING AN APPEND ONLY PUBLIC BULLETIN BOARD (3)

- Miners invest money (to buy mining rigs) & electricity and get Bitcoins in return.
- Why does the Bitcoin network "spend" so much "money" (bitcoins) on mining?
- Miners secure the network. The more computational power invested, the harder it is for an attacker to perform a double-spend attack, AKA a 51% attack.

Block hash	00214
Previous block	-
Miner's address	Satoshi2ff
Nonce	21231321
Time	8:00

Block hash	00312
Previous block	00214
Miner's address	miner2fsfsa
Nonce	21231321
Time	8:12
Tx1	

Block hash	00108
Previous block	00312
Miner's address	miner1kds
Nonce	3219411
Time	8:19
Tx1	mnr3→store1

Block hash	00214
Previous block	-
Miner's address	Satoshi2ff
Nonce	21231321
Time	8:00

Block hash	00312
Previous block	00214
Miner's address	miner2fsfsa
Nonce	21231321
Time	8:12
Tx1	

Block hash	00108
Previous block	00312
Miner's address	miner1kds
Nonce	3219411
Time	8:19
Tx1	mnr3→store1

Block hash	00223
Previous block	00312
Miner's address	miner3lqw
Nonce	3219411
Time	8:19
	mnr3→store2

Miner 1

Miner 2

Miner 3

Block hash	00214
Mine address	
Nonce	
Time	

The more money invested in mining, the cost for this attack increases.

Block hash	
Previous block	
Miner's address	miner3lqw
Nonce	3219411
Time	8:19
	mnr3→store2

	108
block	
Miner's address	miner2fsfsa
Nonce	3219411
Time	8:31

Miner 1

Miner 2

Miner 3

QUANTUM ATTACKS?

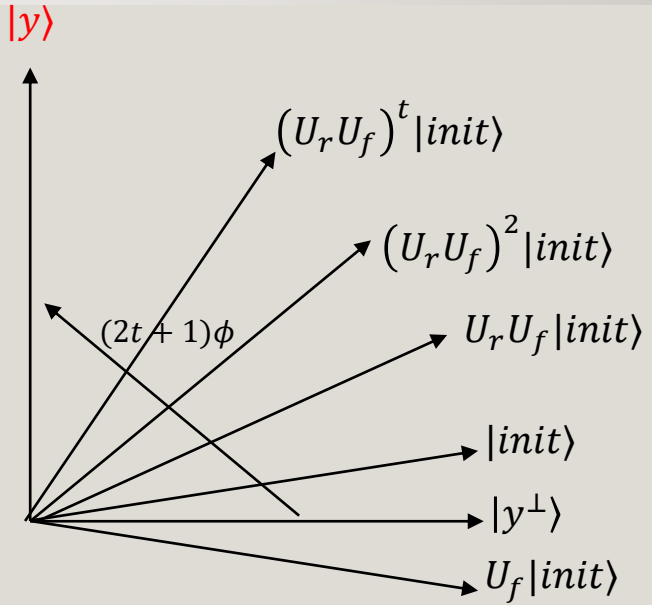
- The current digital signature scheme can be forged using a quantum computer, using (a variant of) Shor's algorithm.
- The proposed solution is to use a post-quantum digital signature scheme – for example, hash-based signature schemes (such as Lamport signatures). Downside: somewhat inefficient. Efficiency is especially important in Bitcoin since a block has a fixed size (larger signatures ➔ less transactions per second).
- This was well known.

IMPLICATIONS OF QUANTUM MINING

- Grover's algorithm can be applied to find solutions for Proof of work puzzles
- Suppose we have quantum miners, that use Grover's algorithm.
- Immediate consequence: the difficulty of mining will increase.
  - Not really a problem.
  - This was well known.

OBSERVATION

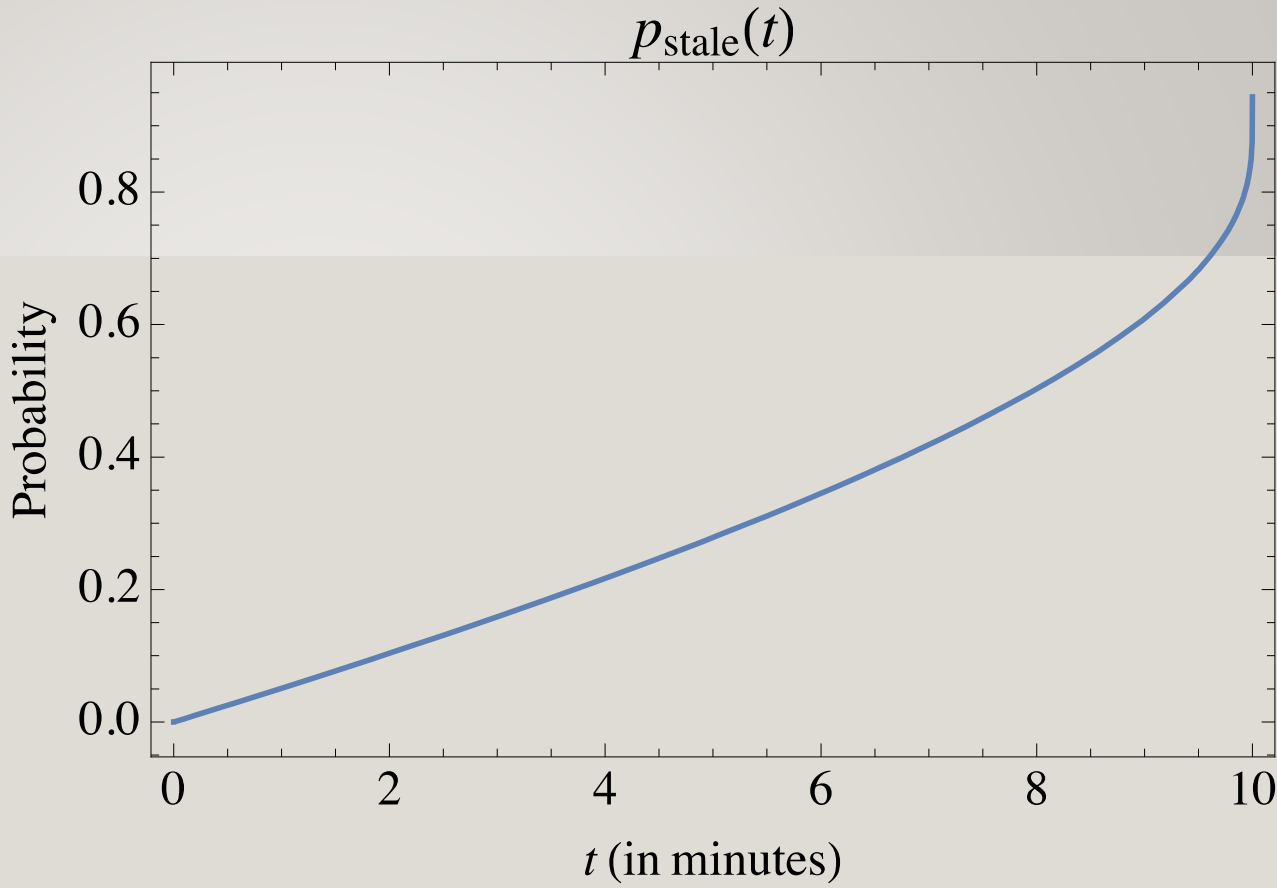
- Grover's algorithm achieves a quadratic speedup even when stopped prematurely.
- We can stop the algorithm prematurely, and still get a quadratic advantage! After t iterations, the success probability is $\sim \frac{t^2}{N}$.
- <u>The number of iterations doesn't need to be chosen in advance!</u>



IMPLICATIONS OF QUANTUM MINING

- Suppose your fellow miner found a block. What do you do?
  - Strategy 1: Stop everything, and start to mine on top of the new block.
  - Strategy 2: Measure the quantum state immediately, hoping to find a block, and to propagate it faster than your fellow miner. If the block becomes part of the longest chain, you win!
- Rational miners will use strategy 2, as it is strictly better.
- Therefore, once one miner finds a block, all others will measure their state. There is strong correlation between the time different miners measure their state.
- This may lead to more forks in the blockchain
  - Classically, forks happen due to propagation time / network effects. Stale rate → 0 as propagation time decreases.
  - In the quantum setting, forks happen for an entirely different reason. Stale rate does not go to zero as propagation time is decreased.

Suppose all miners are symmetric, and they choose the same number of Grover iterations to apply, which takes t minutes. The stale rate (# blocks outside longest chain / total # blocks)



PROPOSED COUNTERMEASURE

- Solution should prohibit the adaptive strategy.
- Intuition: force miners to choose how many Grover iterations they will apply, in advance.
- Proposal:
  - Change the tie-breaking rule.
  - Old rule: follow the tip that was received first. Provides an advantage to well-connected & high-bandwidth miners.
  - New rule: let t_1 and t_2 the times the competing blocks were received (subjective). Let $t = \min\{t_1, t_2\}$. Let s_1 and s_2 the timestamps in the blocks (objective). Honest miners follow the block which minimizes $\min |s_1 - t|, |s_2 - t|$.
  - Honest miners know how many iterations they will apply, and therefore will have a low difference, whereas adaptive miners will usually have a high difference. A miner cannot change the timestamp after starting to mine.

DISCUSSION & OPEN QUESTIONS

- What is the equilibrium strategy for quantum mining? What are its ramifications? Initial unpublished results: "Strategies for quantum races", Troy Lee, Maharshi Ray and Miklos Santha.
- Is the proposed solution secure?
  - Does it introduce other risks, related to timing attacks?
  - Will mining pools work? Perhaps the efficiency of mining pools will be smaller than solo miners
  - Selfish mining, Infiltration attacks and Pool hopping have to be addressed
- Quantum mining is not progress-free. What are the other implications?
  - Obvious ones: Classically, twice-as-fast miner is worth twice. For a quantum miner, twice-as-fast is worth quadruple.
- Is the high-stale rate really a problem in the quantum setting?
  - Classically, a high-stale rate causes problems. I can't see any effect on security or efficiency in the quantum setting. Essentially, a quantum attacker will also have a high stale-rate, whereas a classical miner can decrease its own stale-rate to essentially 0, and get an unfair advantage.

THANK YOU!