Quantum Consensus

By Quantum Disconsensus

Team Members

- Matthias Hudobnik
- Marc Gaensler
- Oleksandr Mykhalevych
- Anton Karazeev
- Takahiko Satoh
- Anders Rehult
- Takaaki Matsuo
- Bram Dobbelaar
- Wojciech Kozlowski

Motivation

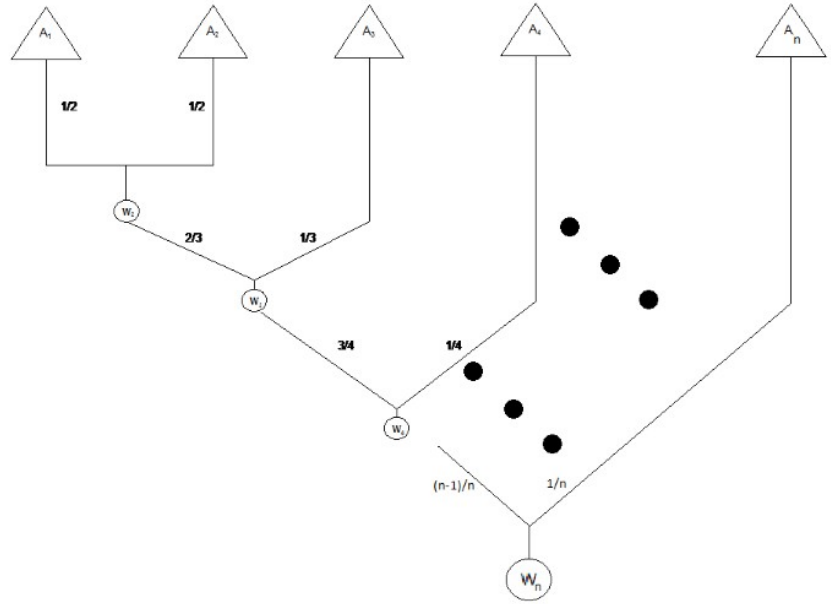
- BitCoin runs a leader election algorithm to elect the next node to add a block to the blockchain
- These nodes do not trust each other
- This algorithm is very CPU intensive and has some known vulnerabilities (51% attack)
- Can we do better using quantum?

Coin Flipping Leader Election

arXiv:0910.4952v2

2.4.1 Protocol:

1. Let $W_1 = A_1$.
2. For $i = 2$ *to* n
   (a) W_{i-1} plays A_i a $P_{\frac{i-1}{i}',\epsilon'}$ unbalanced weak coin flipping protocol. Namely, $P_{q',\epsilon'}$ such that $\left|q' - \left(\frac{i-1}{i}\right)\right| \leq \epsilon'$. Except when $i = 2$, then the protocol is simply $P_{\epsilon'}$.
   (b) W_i is the winner.
3. W_n is declared as the leader.



W State Leader Election

- Let the processors share the state

$$W_n = |10\ldots0\rangle + |010\ldots0\rangle + \cdots + |0\ldots01\rangle$$

$$W_n = |2^{n-1}\rangle + |2^{n-2}\rangle + \cdots + |2\rangle + |1\rangle$$

- Algorithm
  - Let each processors measure its qubit
  - If measurement is 1, then elect itself as leader

First W state created in SimulaQron!

Success!

- Both have been merged into the main SimulaQron repository earlier today
- https://github.com/SoftwareQuTech/SimulaQron/pull/90

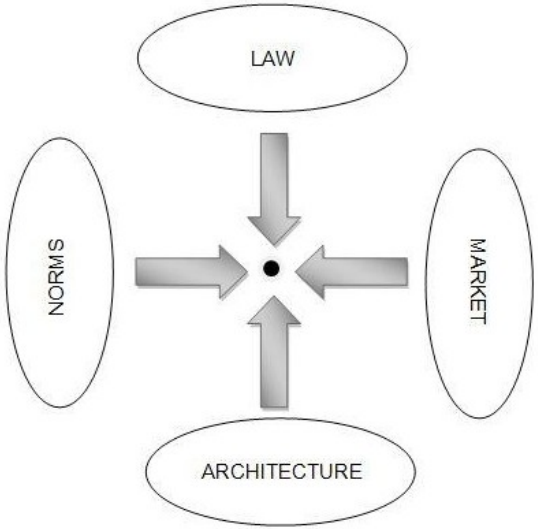
Byzantine Leader Election

- An algorithm already exists:

  https://en.wikipedia.org/wiki/Quantum_Byzantine_agreement
- Too challenging for hackathon
- Uses qutrits – need to port to qubits
- Uses quantum verifiable secret sharing
- Means Quantum BitCoin as intended is possible

Exploring the Legal Side

- Can Quantum BitCoin make cryptocurrency a better candidate for legal tender?
- Increased security leads to auto-regulation by social norms due to increased trust



Lessig – four modalities of regulation

Lessons Learned

- Main difficulty is preparing the quantum state
- Not trivial to prepare W state
- Preparing the state for the biased coin flip was the most challenging part of that algorithm