UNCEFACT Chain

Quantum Communication Workgroup

PRESENTED BY
Alan Kuresevic

PRESENTED ON
2020-07-09

Quantum Communication Workgroup

- Workgroup objective:

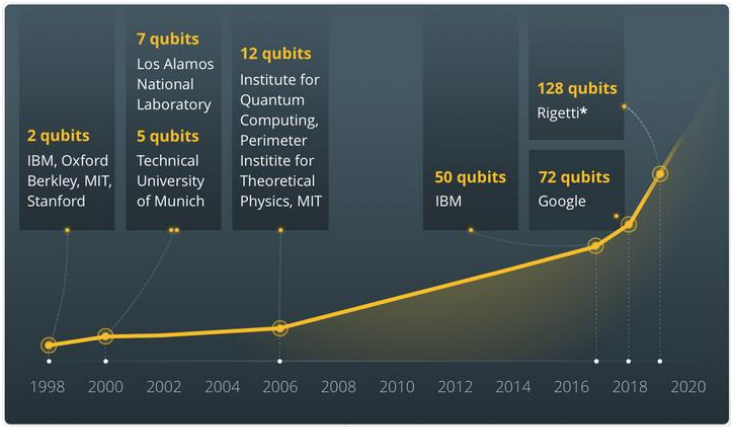
  Asses the impact of quantum computing on blockchain and its interoperability.

- Workgroup members:

  Dean Rakić (blockcontrol.de)
  Josip Maričević (HashNet)
  Tadej Slapnik (Tolar)
  Alan Kurešević (SES)

Quantum Computing

- Quantum computer is a computational device that is based on the principles of quantum mechanics
- Classical computers are based of exploitation of bit's binary states of and using 1s and 0s to represent numbers and perform calculations
- Quantum computers use qubits (anything that exhibits quantum behavior) that can have multiple states (i.e. molecule with 20 electrons has 1 million states)
- Key quantum mechanics aspects: superposition and entanglement
- Quantum computers are million times faster then classical computers (i.e. latest Google experiment: 260 sec vs. 1000 years)
- The quest for **"quantum supremacy"** – tipping point at which quantum computer can demonstrate performances and/or functionality that exceed classical computers
- Good progress but still 5-10 years from commercial reality



Quantum Computing Impact on Cryptography (1/2)

- Cryptography is set of processes and algorithms to protect data and communication
- Three families of cryptographic algorithm:
  - Symmetric (private) key cryptography – considered as “old school” algorithms. Require secure exchange of same encryption keys between parties.
  - Asymmetric (public) key cryptography - most modern every day’s encryption based on asymmetric algorithms. Uses public/private key pairs to establish initial keys.
  - Hash functions (“keyless cryptography”) – used to create theoretically unique fingerprint of the message so we can tell if message was modified
- Cryptography is largely based on “one way” mathematical computational challenges. Easy to do in one direction, practically impossible to do in other direction using classical computers.
- Shor’s and Grover’s algorithms are quantum computing algorithms used to simplify reverse mathematical operations of factoring and hashing using quantum computers

Quantum Computing Impact on Cryptography (2/2)

- Using quantum computer processing power and Shor's and Grover's algorithms makes one direction mathematical problems breakable in a reasonable amount of time
- **Asymmetric cryptography** is **vulnerable** to "quantum attacks" facilitated by quantum computers can make the most of the current encryption systems obsolete
- Pure **symmetric cryptography** with the right key length is still considered **quantum secure**, but requires **symmetric keys** to be shared by both parties

Quantum Computing Impact on Blockchain/DLT

- Blockchain's widely accepted immutability and security is an essential element of public trust in digital assets
- Quantum computers could threaten the public key cryptography, which is the backbone of blockchain security
- Main blocks used for providing security in a blockchain are
  - Hash functions currently used, which are not invertible with regular computing
  - Public private key systems which rely on hidden subgroup problems

… both are the backbone of blockchain security and are under the threat from quantum computing algorithms.

- Today no practical quantum computer implementation that has enough processing power to break encryption
- Current research estimates availability of practical instances of quantum computers in 5-10 years, while latest studies shows that successful replacement of compromised encryption algorithm takes around 10 years

Quantum Resistant Cryptography

- Quantum Resistant Cryptography are cryptographical methods that are secure against the attack of quantum computers

Two approaches to the problem:

Post Quantum Cryptography (PQC)

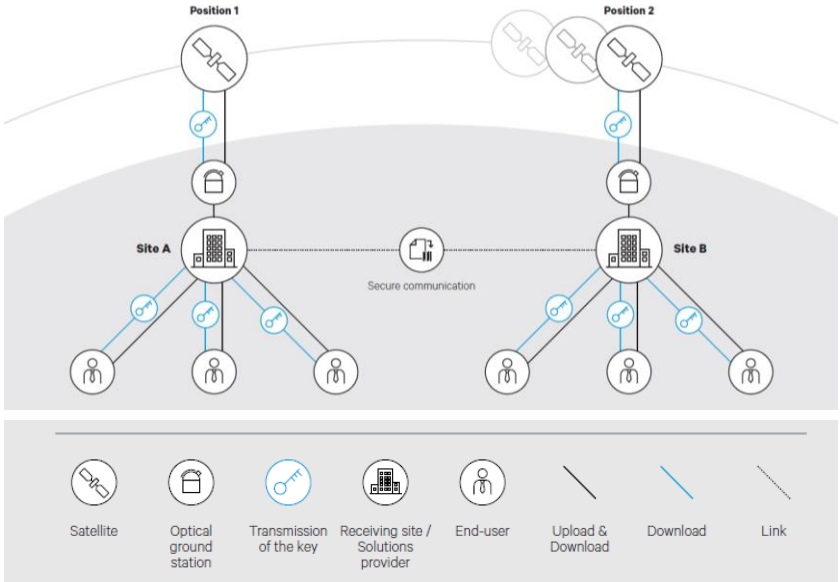
- Replacing underlying mathematical functions with those that are not solvable by quantum computing
- Several family of algorithms are under considerations
- Requires very longs keys (several KB to MB) which makes them impractical for use
- Still require mathematical proof of being unbreakable
- Can be software or hardware based

Quantum Key Distribution (QKD)

- Using existing symmetric key cryptography with adequate key length is provable to be quantum secure
- Resolving Key Establishment Problem (how to securely share cryptographic keys between parties) by using quantum mechanics properties to generate and distribute encryption key material
- Eavesdropping can be detected and mitigated
- Requires specialized hardware

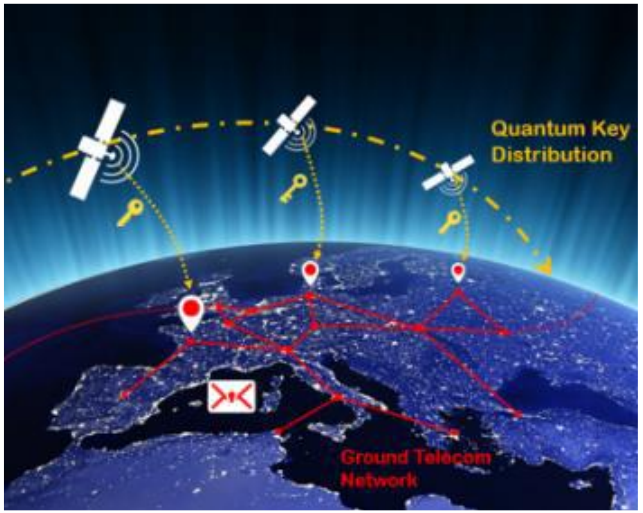
Transnational Quantum Key Distribution (QKD) (1/2)

- Terrestrial QKD is physically limited to a range of 200 km due to attenuation in optical fiber
- Satellite based QKD is therefore required to bridge larger distances
- Terrestrial and satellite based QKD complement each other
- A Low Earth Orbit (LEO) satellite based QKD system can provide a **global service**
- Optical ground terminals are installed at each node in the network to receive the optical quantum channel from the satellite QKD payload
- Truly random key material is securely generated by the QKD payload onboard the satellite and distributed to the network nodes



Transnational Quantum Key Distribution (QKD) (2/2)

- Today there are very few commercially deployed QKD networks across the world (5G South Korea, datacenters in Geneva region)
- Number of national experiments of temporary nature (China, Italy, Germany, Netherlands, USA, …)
- European Commission recognized a strategic importance for Europe to build an independent QCI network as a part of the European Cybersecurity Shield.
  - EuroQCI declaration signed in June 2019 (today 22 states)
  - Integrate quantum secure communication into conventional networks and link critical public communication assets all over the EU
  - Federated EuroQCI network integrating national QCIs
  - Develop technology and fully functional EU infrastructure by 2027



Benefits of Quantum Communication in DLT Interoperability

- There is a limited research done which is focused on post quantum blockchain. Some elements are still in a very early, theoretical domain, lack of practical implementations makes future interoperability assessments very difficult and potentially impossible in some cases. Several areas can have a positive impact on DLT interoperability

1. **Making underlying communication infrastructure quantum resistant**
   Using common secure quantum communication infrastructure (QCI) to protect information exchange between DLT networks

2. **Replacing conventional digital signatures with quantum resistant algorithms**
   Introducing post quantum algorithms to improve security and standardize encryption method across DLTs (Bitcoin Post Quantum, Ethereum 3.0, Tolar HashNET)

3. **Using Quantum Key Distribution (QKD) to implement symmetric cryptography methods**
   Moving to symmetric encryption and QKD to increase transaction speed and standardize encryption methods.

4. **Creating truly quantum based blockchain systems**
   Using entangled qubits to hold transaction records in the form of a single particle's state over time. By using entanglement, transactions would become agnostic of physical distance between entangled particles. Potentially provide an ultimate interoperability as transaction states will be based on the same physical particle state.

Summary

- The accelerated advances in quantum computing and communication present the actual threat to cryptography in general and as such to blockchain security.
- The ongoing research and practical implementations of mechanisms to achieve the post-quantum security are currently developing along two axes, software-based quantum-safe cystography algorithms and quantum physics-based distribution of encryption keys. Early stages of development facing either insufficient mathematical poofs of achieving theoretically secure status or facing challenges of the practical implementation on a wider scale.
- Quantum threat to DLT security and integrity opens opportunity to address and achieve interoperability at new levels.
- Today’s theoretical work and early implementations are still 5-10 years away from practical implementation

Alan Kuresevic

Thank you!