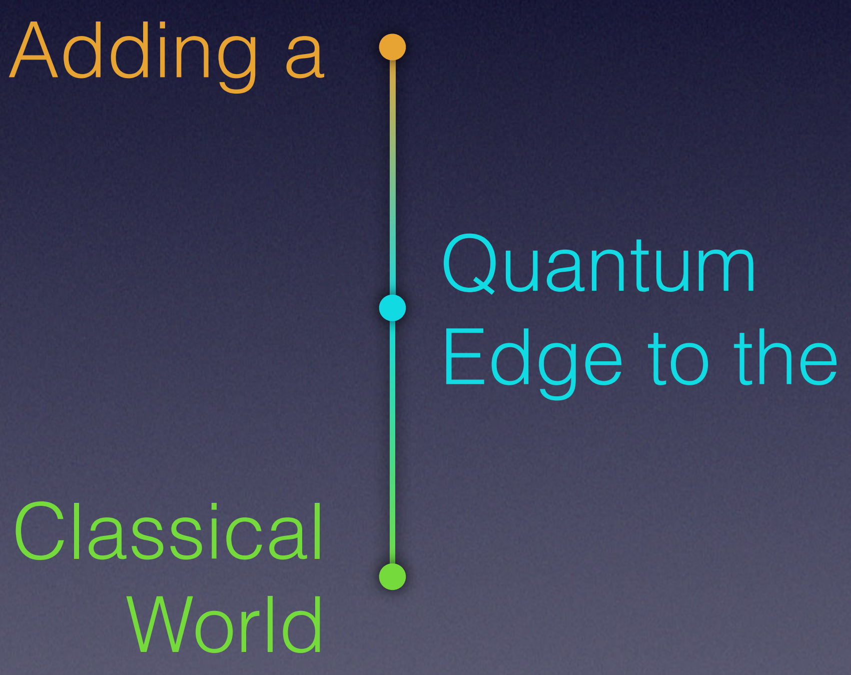
Quantum Computing and Networks

Arahant Ashok Kumar (aak700)



Adding a Quantum Edge to the Classical World

- Quantum network design
  - Network Stack
  - Protocols
  - Simulation
- Classical computing Potential problems
  - SPAM
  - Security
- Quantum communication applications
  - Remote voting
- Quantum advantage
- Classical remote voting
  - Protocol
  - Problems
- Quantum Voting
  - Protocol Design

Classical Networking

Spam & Security

Authenticity

Confidentiality

Integrity

Privacy

Legal

- SPIT - VoIP spam (Issue of Authenticity and Privacy)
- Privacy - One of the biggest concern with exponential digitisation
- Denial of Service constantly plagues the internet and is 2nd most popular vulnerability.
  - TCP SYN flooding - DoS attack on servers
- Data breach is the 5th most popular attack. While this is still damaging at the corporate level, it has serious consequences on govt institutions.
  - Bangladesh Central bank in NYC hacked in 2016
- Vote by Mail: With the Covid-19 pandemic, in-person voting is become a fatal choice and vote by mail has its own set of problems

Quantum Computing applications

- Central bank Quantum encryption
  - Central banks, Intra-govt communication, Election commissions, Intelligence agencies
  - Critical data to protect.
- Quantum Voting
  - Authenticity of vote
  - Integrity and Confidentiality of the ballot.
  - Privacy of citizens
  - Avoids legal disputes.
  - Upholds Democracy
- End-to-end Quantum encryption
  - Quantum crypto based encryption through QKD

Spam (SPIT)	Authorised quantum-based access	Teleportation (Entanglement)	QKD
DoS attack	Authorised quantum-based access	Teleportation (Entanglement)	No-cloning principle
TCP SYN flooding	QKD	Entanglement timeout	
Remote Quantum Voting	QKD	Quantum Money	Superdense coding
Data breach	Authorised quantum-based access	QKD	
Privacy	OKD		

Quantum Computing

Concepts

- Qubit
- No-cloning principle
- Superposition and Measurement
- Entanglement (Channel)
- Fidelity & Purification
- Decoherence
- (Entanglement) Channel degradation
- Bit flip error

Communication protocols

- Entanglement Channel
- CHSH experiment
- Superdense coding
- Quantum Teleportation
- Quantum Key Distribution
- Qubit Error Correction

Classical remote voting (by mail)

Protocol

- Register online/ in-person
- VBM packets are mailed
  - Secrecy envelope
  - Ballot return envelope
  - Ballot
- Cast your vote
- Turn in ballot enclosed in secrecy envelope

Problems

- Mail under threat in transit - not tamper-proof
- Confidentiality -
- Integrity -
- Authenticity - Voter Fraud, Ballot Harvesting
- Privacy
- Legal issues
- Archaic

Quantum Voting

Protocol

- QKD shares Key between Voter and Govt server
  - Key encoding (N qubits + N bits)
  - Correlated randomness (Bell pair) (2N qubits)
  - CHSH (2N qubits)
  - Key encoding with Error (QBEC) (3N qubits)
- Govt server generates a Bell pair with the Voter
  - Bell pair encrypted with QKD shared before
  - Voter performs QBEC
- Voter cast votes (in classical bits)
- Voter encodes bits into received Bell pair qubit
- Voter sends encoded Bell pair qubit to govt server
- Govt server receives encoded Bell pair qubit
  - QBEC on received encoded qubit
- Measures votes

Advantages

- Double security
  - QKD - using SSN, biometric or ad-hoc random choice of personal data
  - Entanglement-based voting encrypted with QKD
- Authentic
  - QKD only distributed to registered citizens/ voters
  - QKD qubit guarded by any ID - SSN, DOB etc. private to citizen
  - QKD/ Vote qubit cannot be cloned
- Confidentiality
  - Eavesdropping destroys qubit and information within
  - All or nothing
  - Ensures Privacy
- Integrity - Tamper-proof qubit (QKD, Entanglement and votes)

Design - Network stack and Components

Network Stack design

Physical Layer

- Generating qubits
- Qubit Error Correction
- Quantum Teleportation
  - Entanglement Swapping
- Quantum Computing operations

Connectivity layer

- Entanglement generation service
  - Heralded signal generation
- Node state maintenance
- Quantum Repeaters
- Long distance P2P entanglement
- Entanglement purification

Quantum N/W components

- Quantum Computer
- Quantum Nodes
- Entanglement channel
- Quantum OS
- Quantum resource manager
- Quantum Network state
  - Quantum Computing state
  - Quantum Nodes state
  - Entanglement channel state

Implementation - Simulation

QuTech's SimulaQron simulator

Topology	Description	Entanglement Channel	Teleportation	Entanglement Swapping	Superdense coding	Qubit Err correction (QBEC)	QKD
Dual	2 nodes 1:1	Establishing an entanglement channel between nodes for every qubit of information transfer	1:1 teleportation		Encoding classical info (bits) into Bell pair bit and transferring	Measuring qubit Error rate through N simulation runs	
Line	N nodes End to end Max degree: 2	Establishing an entanglement channel between nodes. Ad-hoc channel between nodes	Serial teleportation between nodes	Teleporting qubits swapping them between entangled channels through quantum operation	Serial transfer of bits end to end using Bell pair qubit. Measurement at each node	Measuring End to end & Node to node Bit flip error	
Random	Adjacency matrix Dijskstra's routing Dynamic, ad-hoc	Establishing an entanglement channel between nodes. Ad-hoc & dynamic route channel	Sequential teleportation between nodes by dynamic routing	Teleporting qubits through swapping between entanglement channels	Sequential transfer of bits using Bell pair qubit. Measurement at each node	End to end & Node to node Bit flip error based on node degree	Node to node QKD for critical applications ad-hoc routing
Voting	1 (voter) :1 (Govt) N (voters):1 (Govt)	Establishing an exclusive entanglement channel between client (voter) and server (govt)	Teleporting qubits between Govt. and a voter		Encoding Votes (classical bits) into entangled qubit and transferring them on channel	QBEC by voter for QKD qubit. QBEC BY govt for vote qubit	Generating Secret keys for every voter. Distributing them to voters

Implementation - Quantum Voting

1. QKD
    - SimulaQron's cqc.pythonLib to create and share Entangled qubits and info qubits
    - Shell script wrappers for each python module
    - Protocols: CHSH, Correlated randomness, Key encoding
    - Key encoding: Can encode personal data - SSN, biometric data, etc.
    - QKD with system error (bit flips)
        - QBEC by Voter
    - Size of QKD secret key ranges [10-50]
    - QKD govt - QKD voter pair
    - QKD is one-time; destroyed after use

2. Quantum Voting
    - Random vote generator (to simulate)
    - List of Govt and voters in a file
        - N (voters) :1 (Govt) topology
    - The Voter's vote in classical bits
    - Quantum and classical connections
        - No actual transfer of classical bits in superdense coding

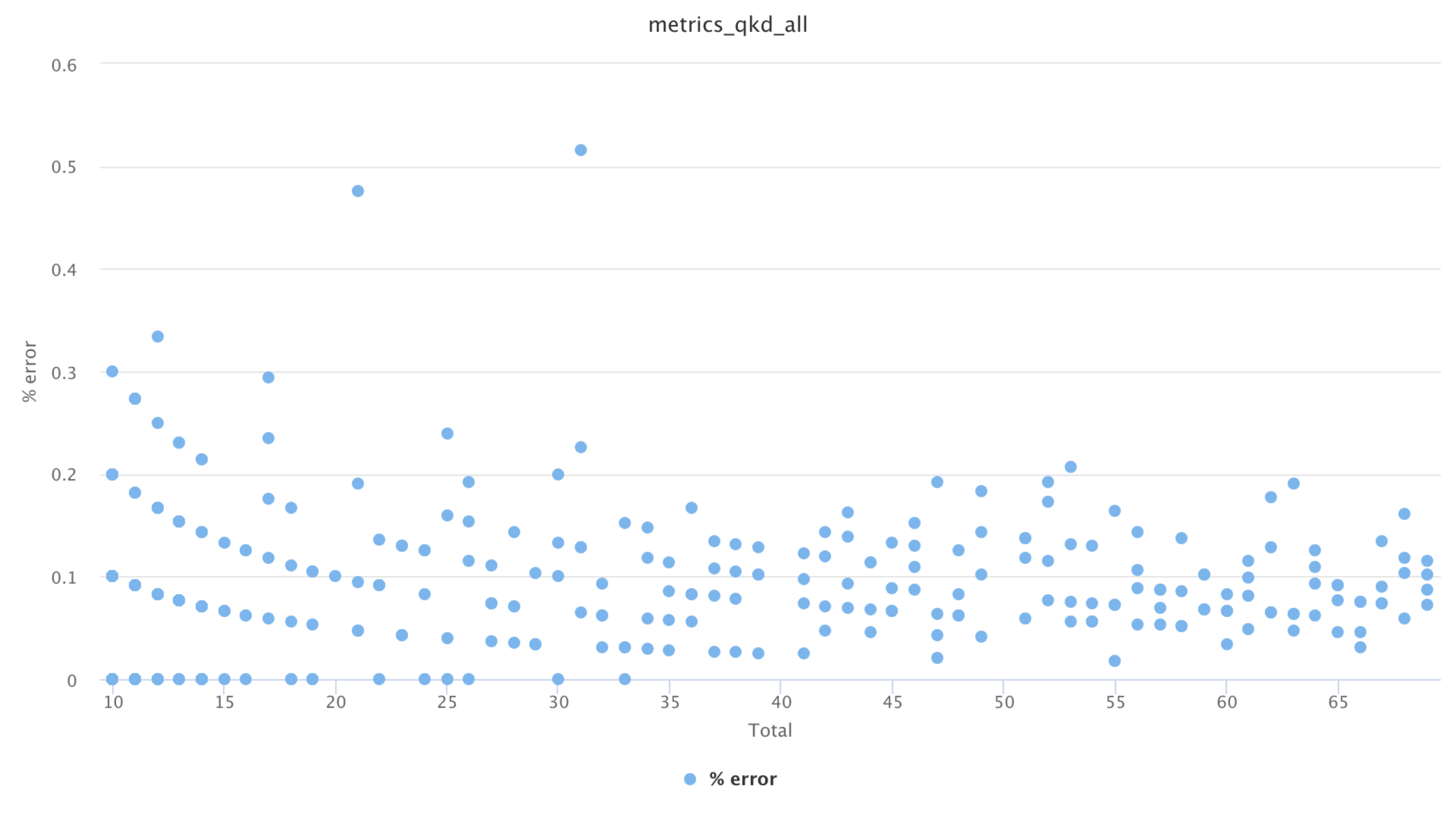
3. Metrics
    - Compares cast votes and recorded votes to calculate voting errors
        - # qubit(s) (1-2 qubits)
        - % Err (of 1 and 2 qubits)
    - % loss in QKD key size compared to original
    - Transmission delay at nodes
        - High delay in case of QBEC

Implementation - Metrics

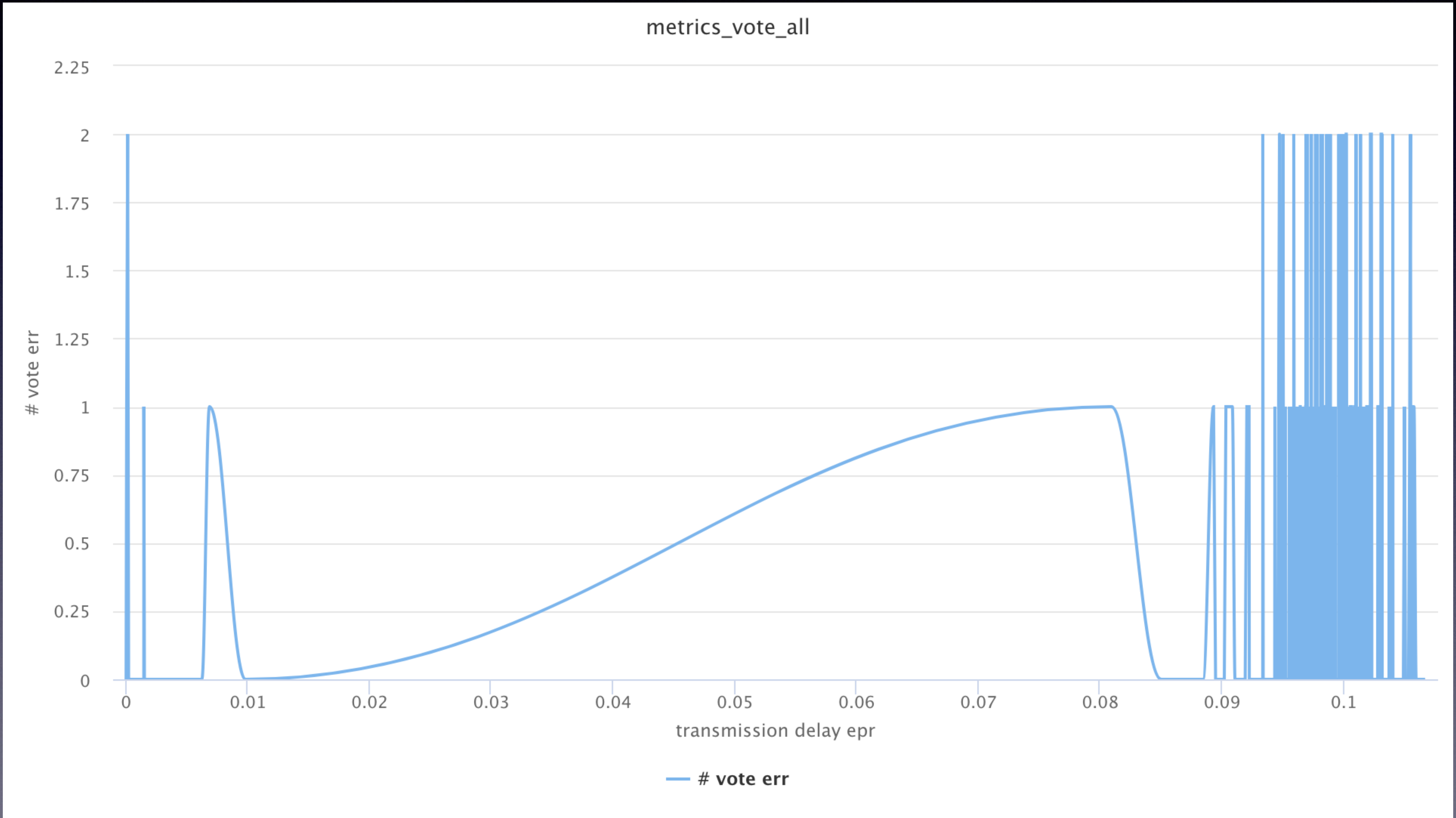
- Information
  - Entropy of votes data (1 and 2 qubit)
  - 1 qubit error rate
  - 2 qubit error rate
  - Information loss
- QKD
  - Threat value
    - (% loss in key size)
    - Vote qubit err rate

- Channel
  - Transmission delay (Entanglement)
  - Qubit flip rate
- Nodes
  - Qubit generation capacity
  - Transmission delay (qubit)
  - QBEC efficiency + rate
- Network
  - Avg QBER
  - Avg. Transmission delay
  - Avg. qubit flip err rate

Data analysis



Data analysis



Future work

- Elaborate simulations
    - Complex topologies
    - Refined metrics
    - Better QBEC
    - Enhanced data analytics
- Quantum Network stack design
    - Quantum packet design
    - Quantum Networking Protocols
- Quantum communication protocols and implementation for remaining use cases
    - SPIT
    - TCP SYN
    - Denial of Service
    - Data breach
    - Simulation demonstration for each use case
- Quantum - Classical integration