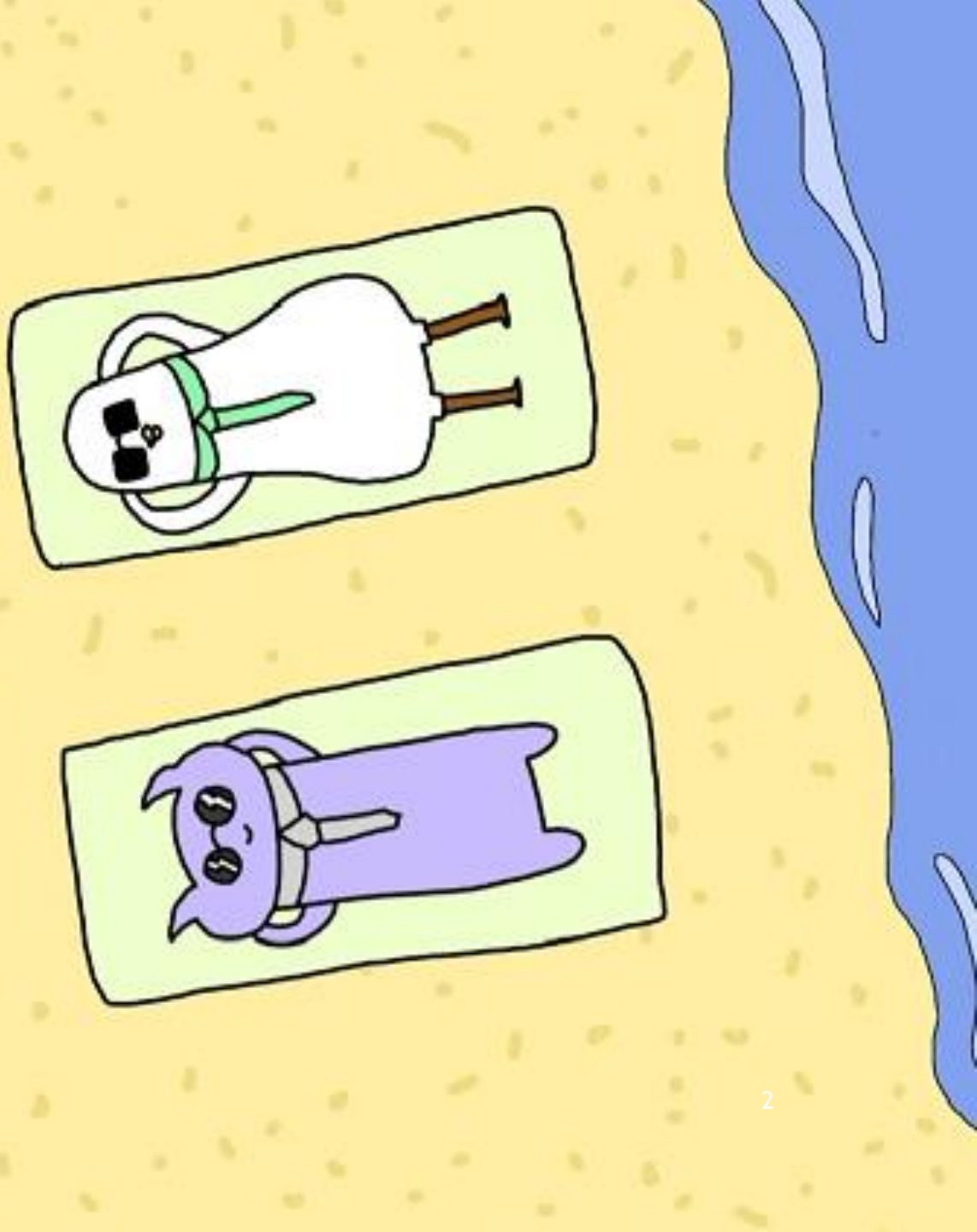
Quantum Contracts

An On-chain Quantum Emulator on Polygon

1

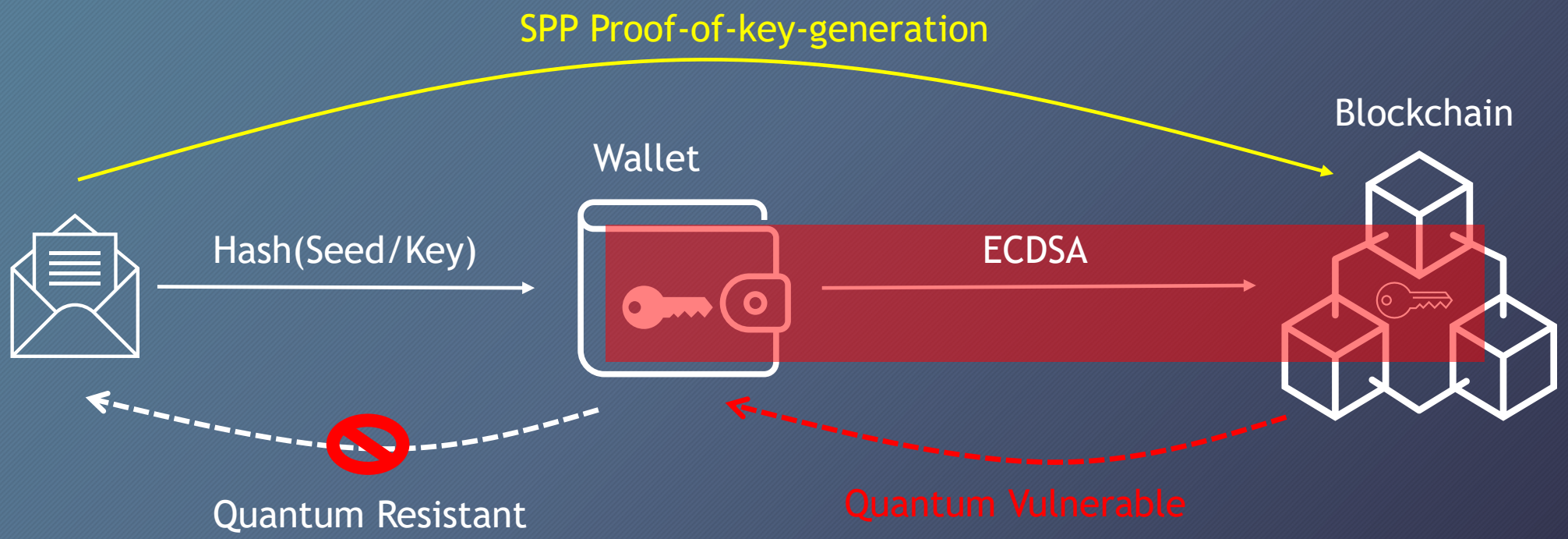
Be Quantum Ready

WE ENVISION A **SECURE** AND **VIABLE** QUANTUM-FUTURE FOR ALL



Making Web3 Quantum-safe

- Layering ECDSA with a MPC-in-the-head Zero-knowledge Proof of Key Generation



https://www.pqcee.com/wp-content/uploads/2022/10/Solving_the_Quantum_Dilemma_in_Public_Blockchains.pdf

Is Web3 Quantum-Ready?

Quantum computing is being used in simulations, optimizations and machine-learning in other industries

Platforms from IBM, Microsoft, AWS, Regetti are already providing quantum tools and services on the cloud

But do we know of quantum use-cases in Web3?

Do Web3 programmers even know where to start?

Introducing QuantumContracts

- A on-chain quantum emulator running in a smartcontract
- runQScript API:
  - Input : Number of Qubits + Quantum circuit
  - Output : Computation result
- On Mumbai testnet
  - Written in solidity as a view function (no gas needed)
  - Source on Github

- v0.1 Features
  - Supports up to 4 Qubits
  - Supports the following gates:
    - I = Identity Gate
    - X = Not Gate
    - H = Hadamard Gate
    - CN = Control-Not Gate
    - CCN = Toffoli Gate
  - Quantum circuit is interpreted (not compiled)

Demo

Entanglement

- 2-Qubit Bell state
- 3-Qubit GHZ

Exponential Speedup

- 2-Qubit Simon

Search

- 2-Qubit Grover
- 3-Qubit Grover

Limitations and Future Extensions

Size of circuit	Universal quantum computer	Production ready	Use cases	Business model
• 4 Qubits to increase to XX Qubits • Need to increase compute and memory	• Phase Gates to be added • Need to support complex numbers & floating-point computation	• Need to make code optimized, secured, audited, etc	• Optimization for DeFi? • Entanglement for DAO? • Superposition API calls	• No figured out yet • Do we need to connect to an actual quantum computer?

Comments/Questions

- Please contact:
  - Teik Guan Tan
  - teikguan@pqcee.com
  - Linkedin.com/in/teikguan
  - @tanteikg