How Quantum Computing Threatens the Security of Your Digital Assets

DR. VIKTOR POLIC

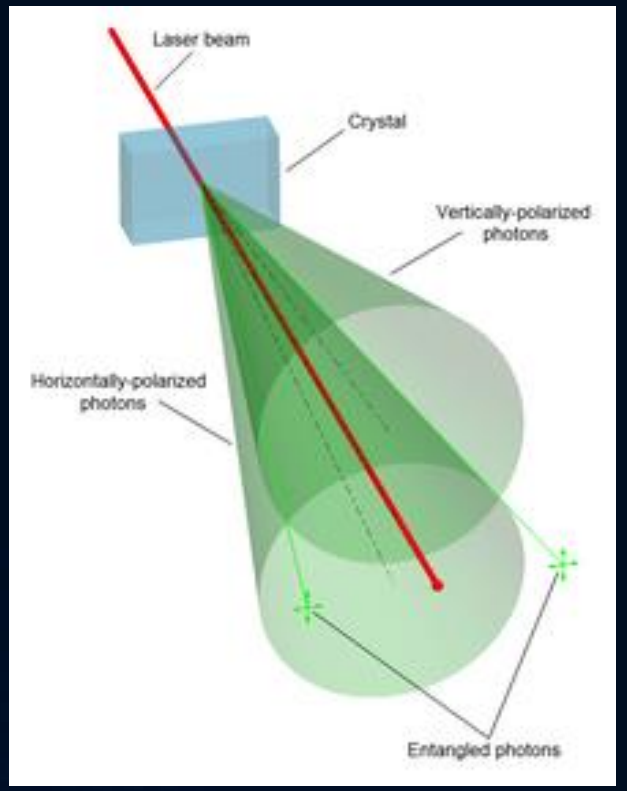
Quantum Computing 101

How it differs from today's computers

Why quantum computing?

THE WORLD IS QUANTUM

SPOOKY ACTION AT A DISTANCE



Let’s flip a coin on a 2-bit classic computer

ONE BIT CAN REPRESENT EITHER HEADS OR TAILS AT A TIME

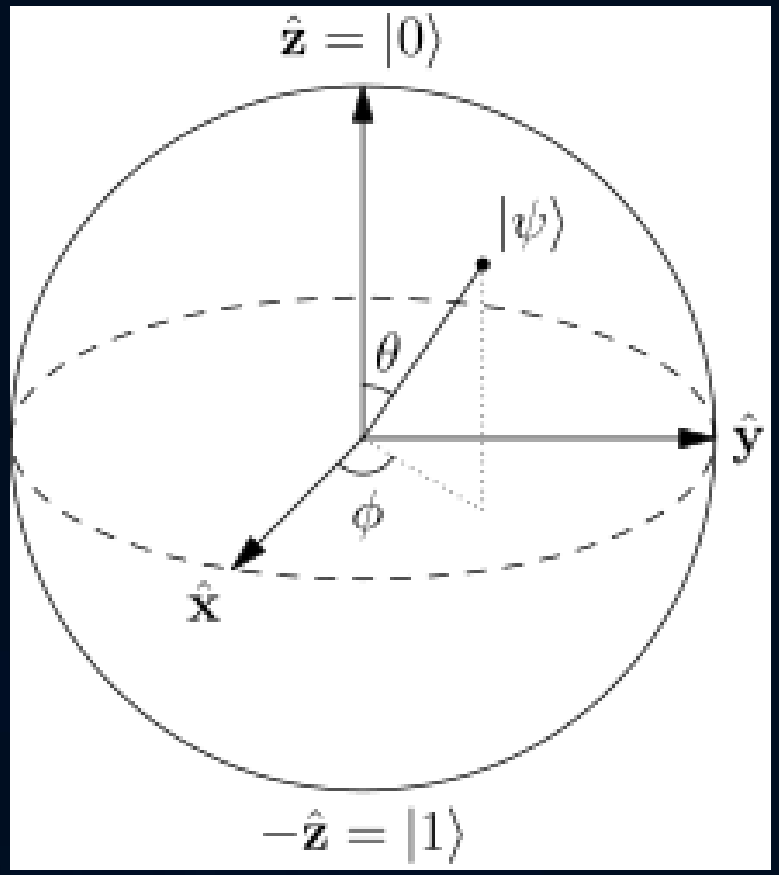
Let’s flip a coin on a 2-qbit quantum computer

SUPERPOSITION

ONE QBIT CAN REPRESENT BOTH HEADS AND TAILS AT THE SAME TIME

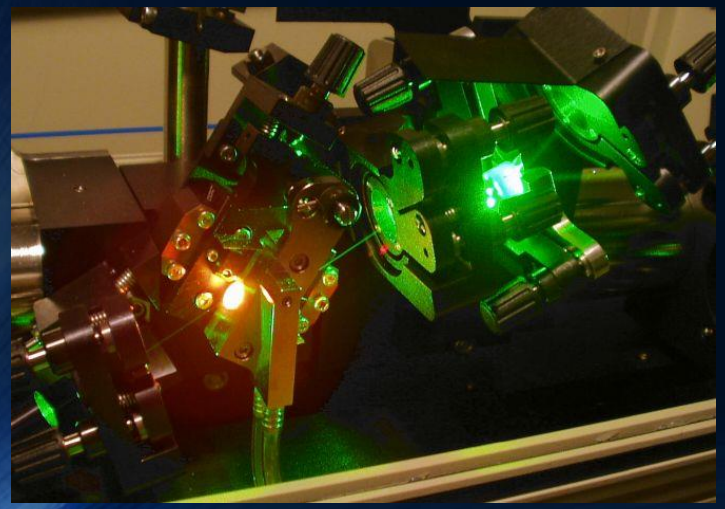
What is a quantum computer?

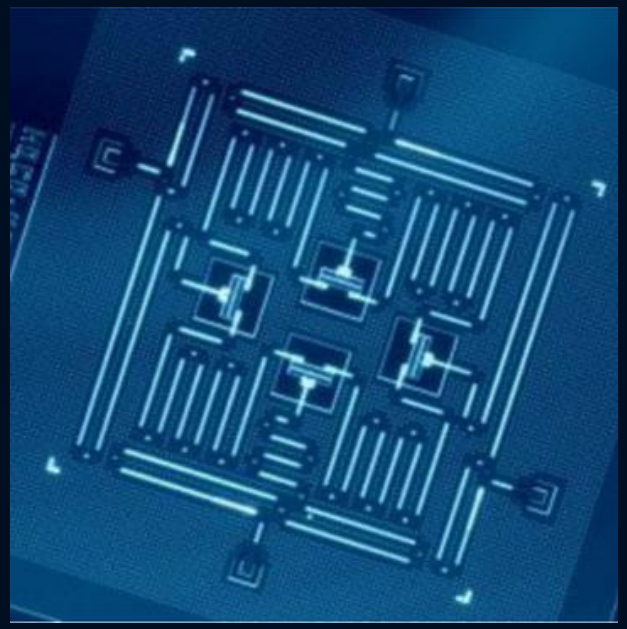
- A common misconception about quantum computing is that a qubit is always in state 1 or state 0, we just don't know which one until we "measure" it. That is not the case.
- A qubit in a superposition is in a linear combination of the states 0 and 1. When a qubit is measured, it is forced to collapse into one state or the other - in other words, measuring a qubit is an irreversible process that changes its initial state.

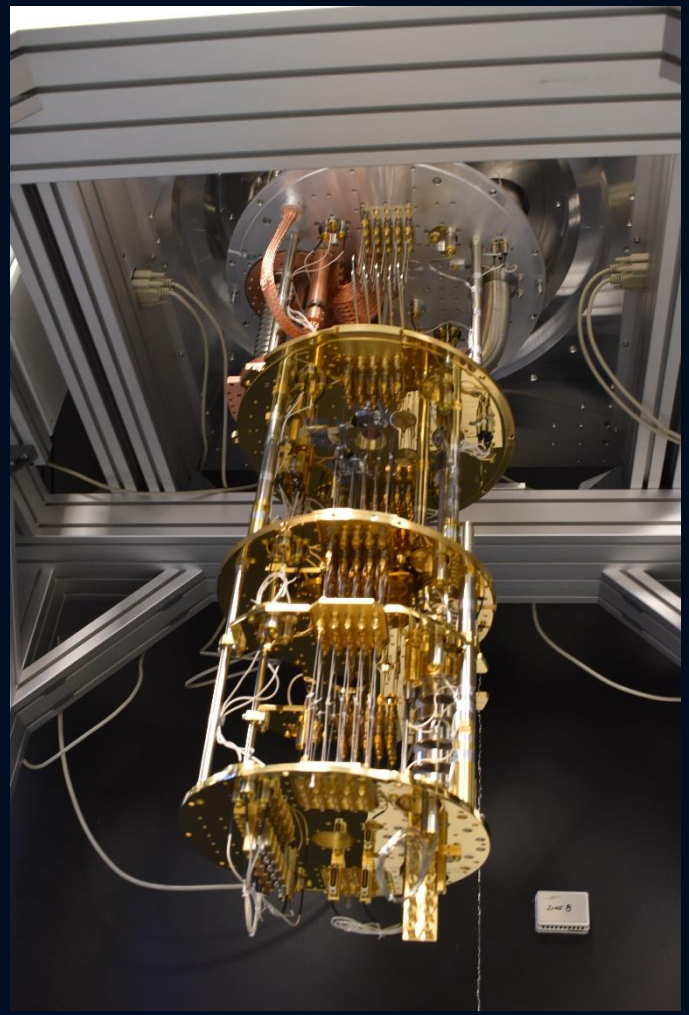


Hardware implementations

- Superconducting quantum computing
- Trapped ion quantum computing
- Linear optical quantum computing
- Diamond-based quantum computer








HOW'S YOUR QUANTUM COMPUTER PROTOTYPE COMING ALONG?
GREAT!
THE PROJECT EXISTS IN A SIMULTANEOUS STATE OF BEING BOTH TOTALLY SUCCESSFUL AND NOT EVEN STARTED.
CAN I OBSERVE IT?
THAT'S A TRICKY QUESTION.

Margaret Hamilton

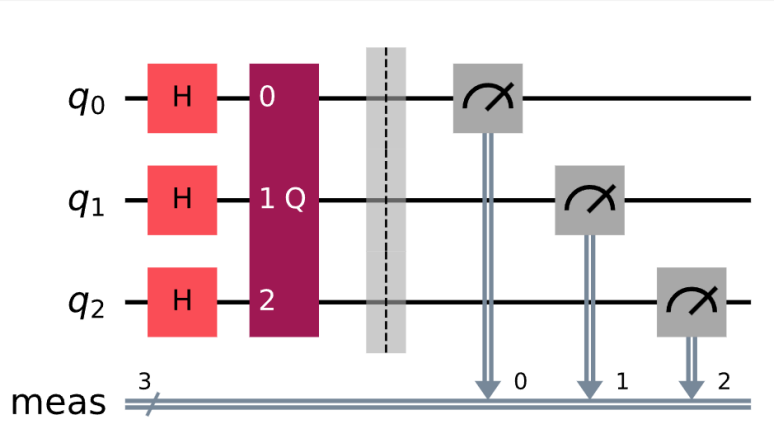
Apollo Guidance Computer

Quantum computing software

```
1  qc = QuantumCircuit(grover_op.num_qubits)
2  # Create even superposition of all basis states
3  qc.h(range(grover_op.num_qubits))
4  # Apply Grover operator the optimal number of times
5  qc.compose(grover_op.power(optimal_num_iterations), inplace=True)
6  # Measure all qubits
7  qc.measure_all()
8  qc.draw(output="mpl", style="iqp")
```

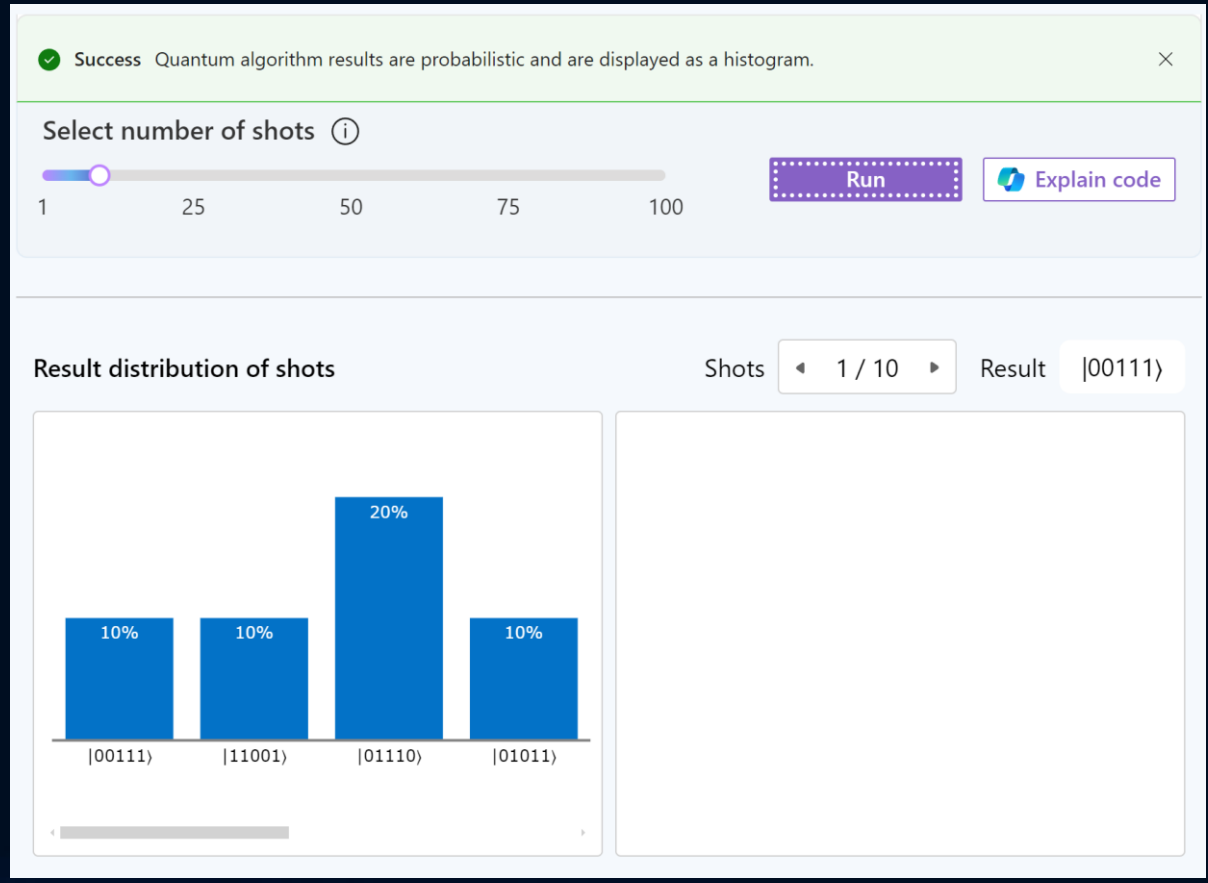
Run

Output:



IBM Qiskit

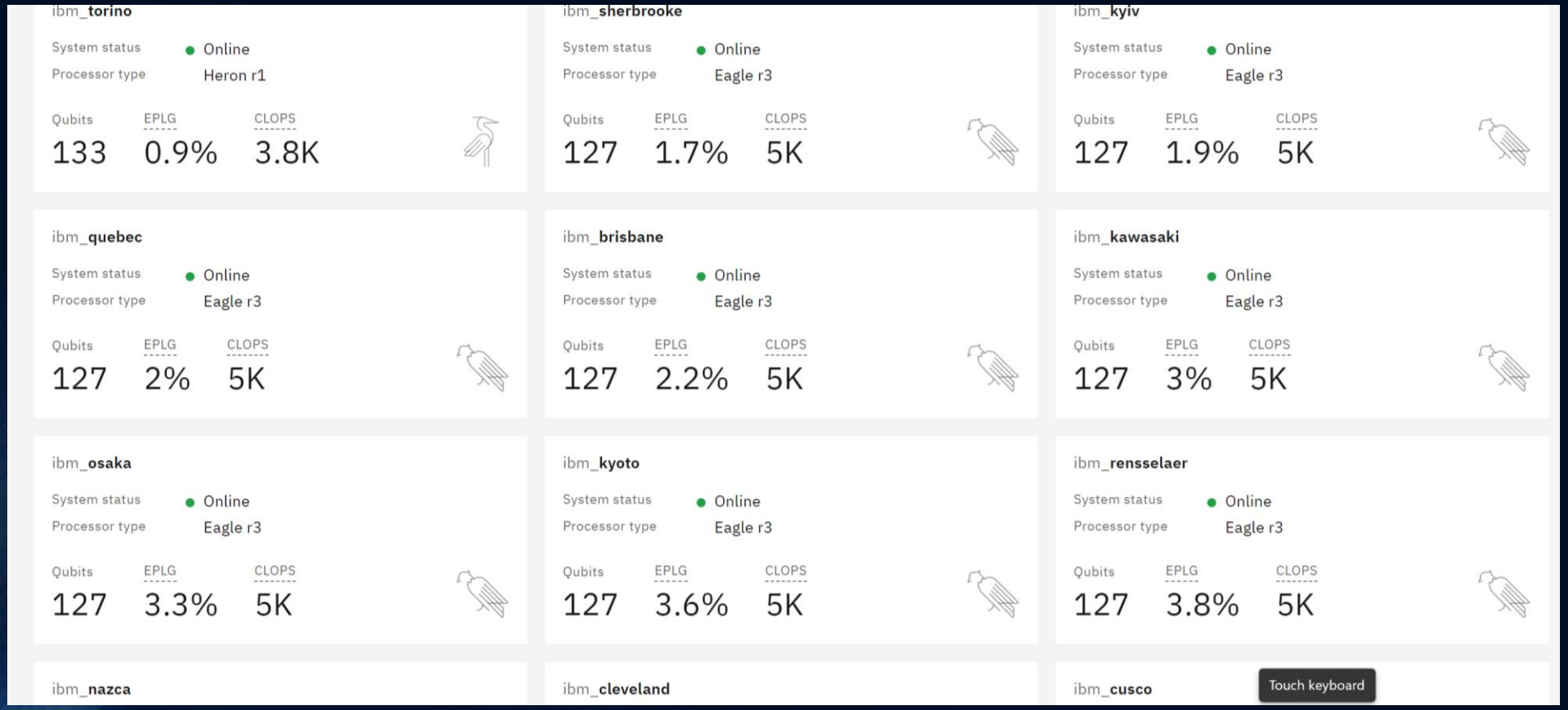
https://learning.quantum.ibm.com/tutorial/grovers-algorithm#full-grover-circuit



Microsoft Q#

https://quantum.microsoft.com/en-us/experience/quantum-coding

Are quantum computers available commercially?



Are quantum computers available commercially?

Quantinuum's System Model H2 includes numerous hallmark features that set it apart from other quantum computers, including:

56
fully-connected qubits

262,144 (2^{18})
Quantum Volume

99.997%
single-qubit gate fidelity

99.87%
two-qubit gate fidelity

- Highest commercially available two-qubit gate fidelity
- All-to-all connectivity
- Qubit reuse
- Mid-circuit measurement with conditional logic

What can they do better?

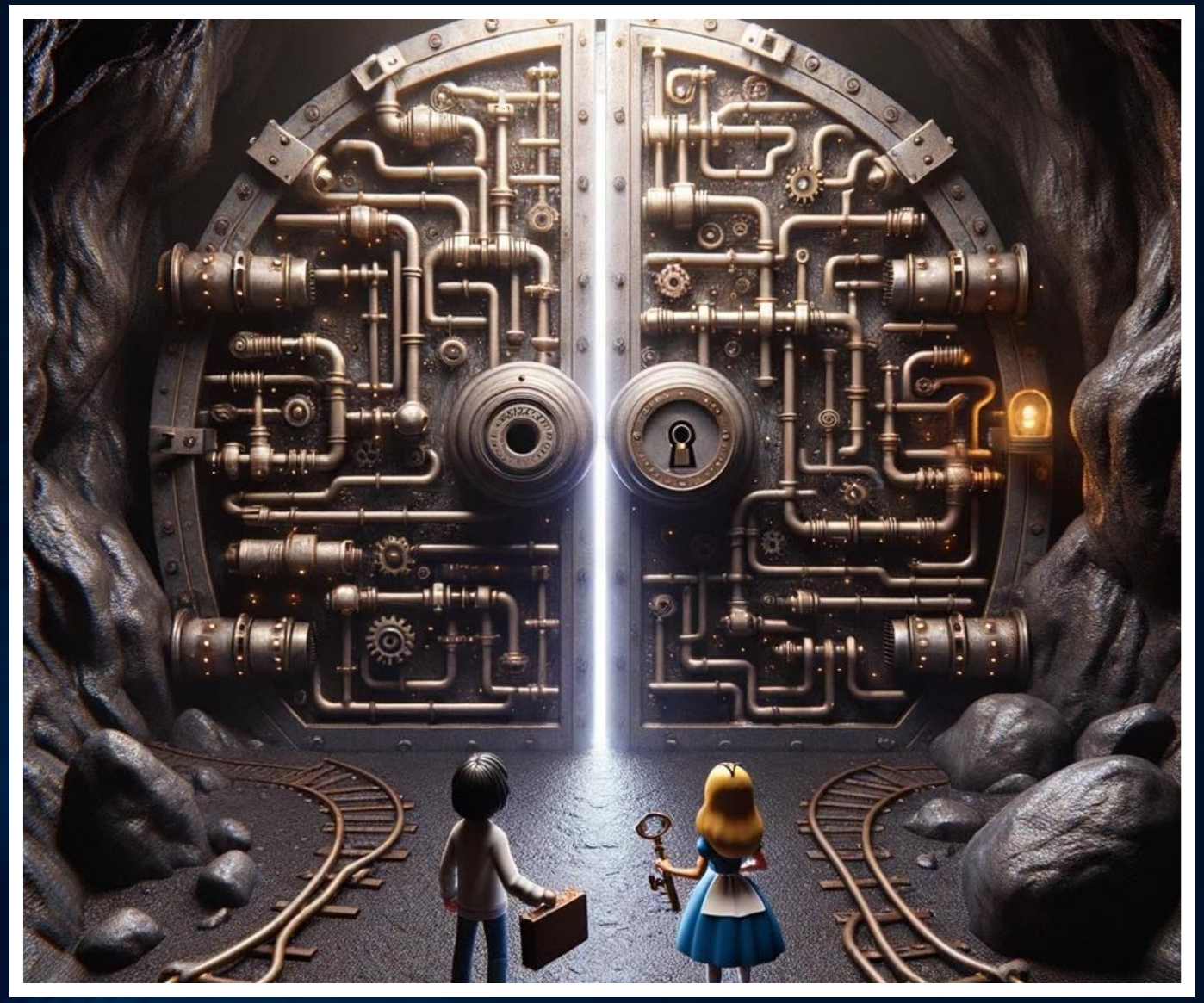
- portfolio optimization and derivatives pricing
- collateral optimization for use cases such as securities lending, which involves cross-optimizing multiple sets of variables
- credit-decision algorithms
- risk level of loans by credit scoring

Ref: IMF, McKinsey

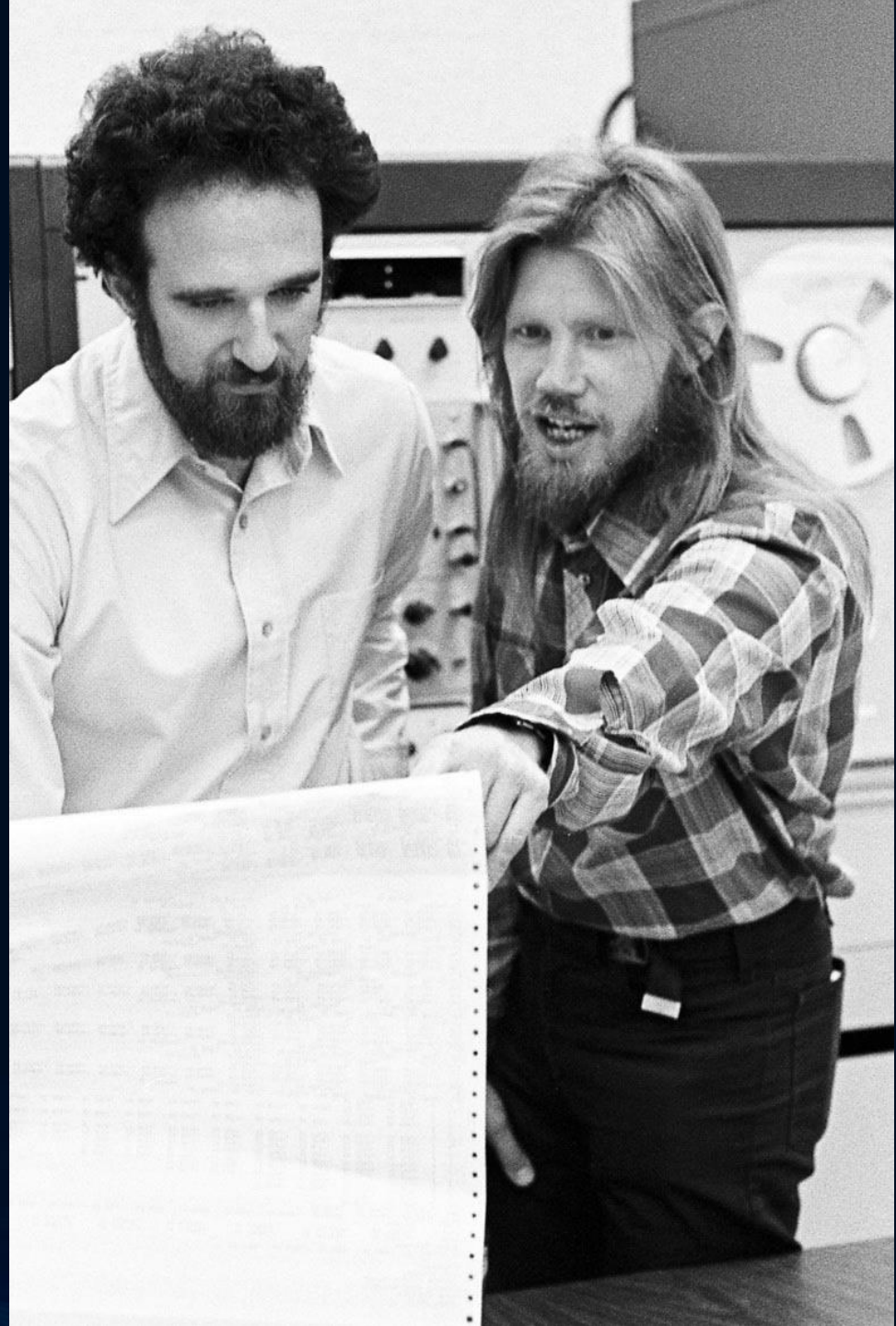
- We present the Quantum Monte Carlo Integration (QMCI) engine developed by Quantinuum. It is a quantum computational tool for evaluating multi-dimensional integrals that arise in various fields of science and engineering such as finance

Ref: https://arxiv.org/abs/2308.06081

Why Cryptography Matters?



Public key cryptography

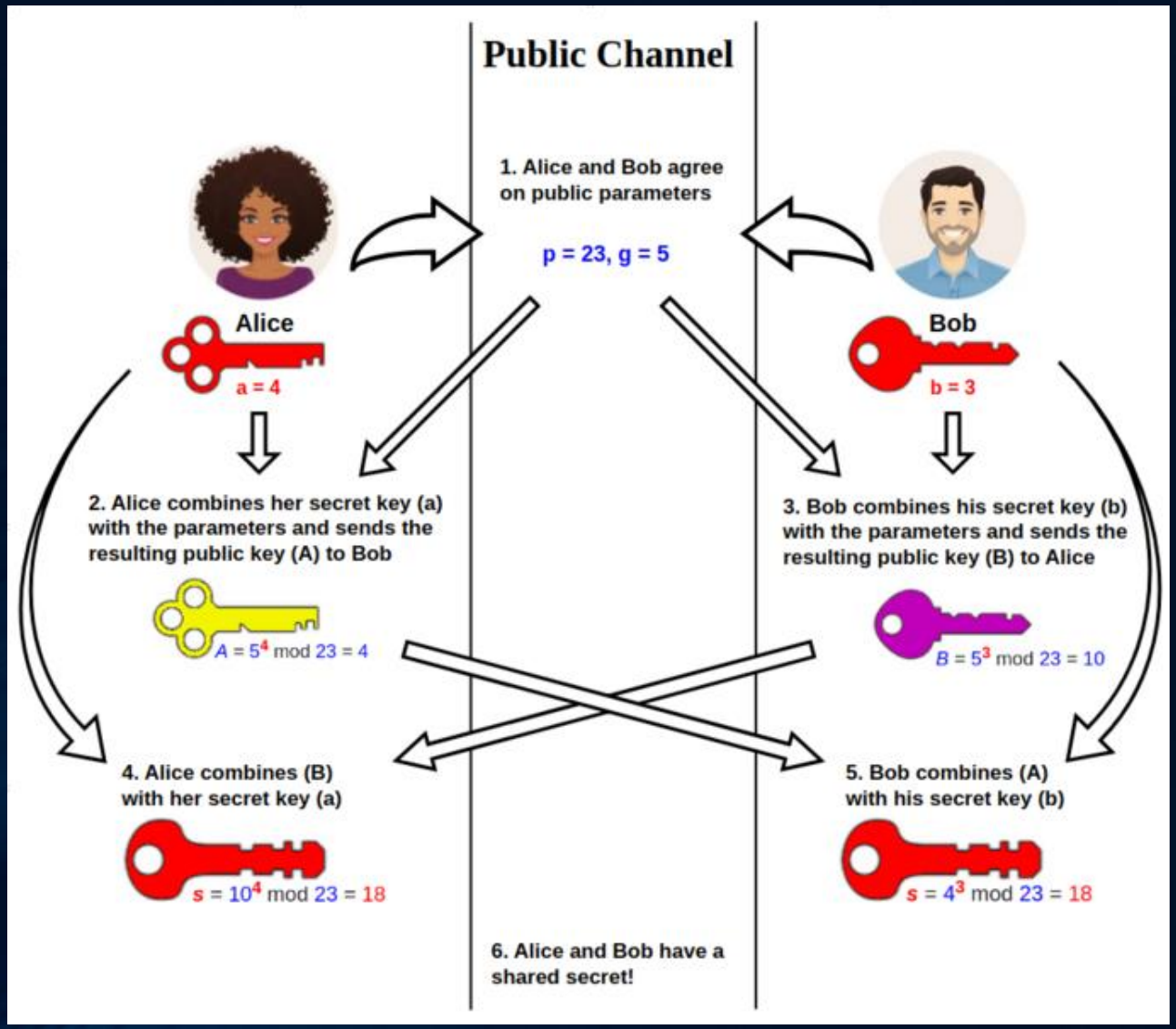


Stanford's Martin Hellman, left, and Whitfield Diffie, shown in 1977, were awarded the 2015 A.M. Turing Award this week. (Image credit: Chuck Painter/Stanford News Service)

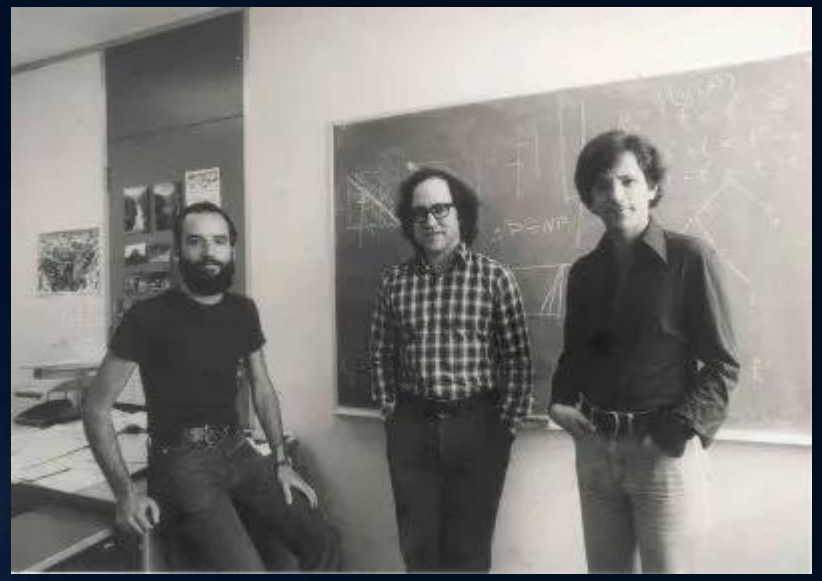
Diffie-Hellman key exchange

1976, New directions in cryptography

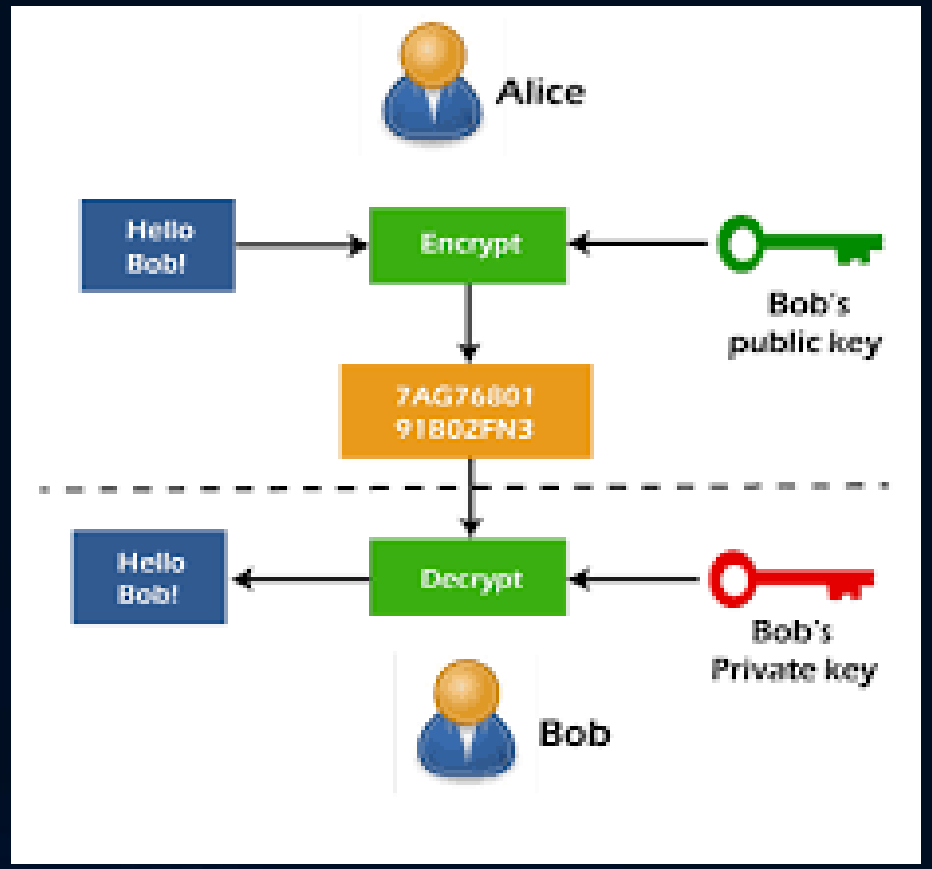
https://www-ee.stanford.edu/~hellman/publications/24.pdf



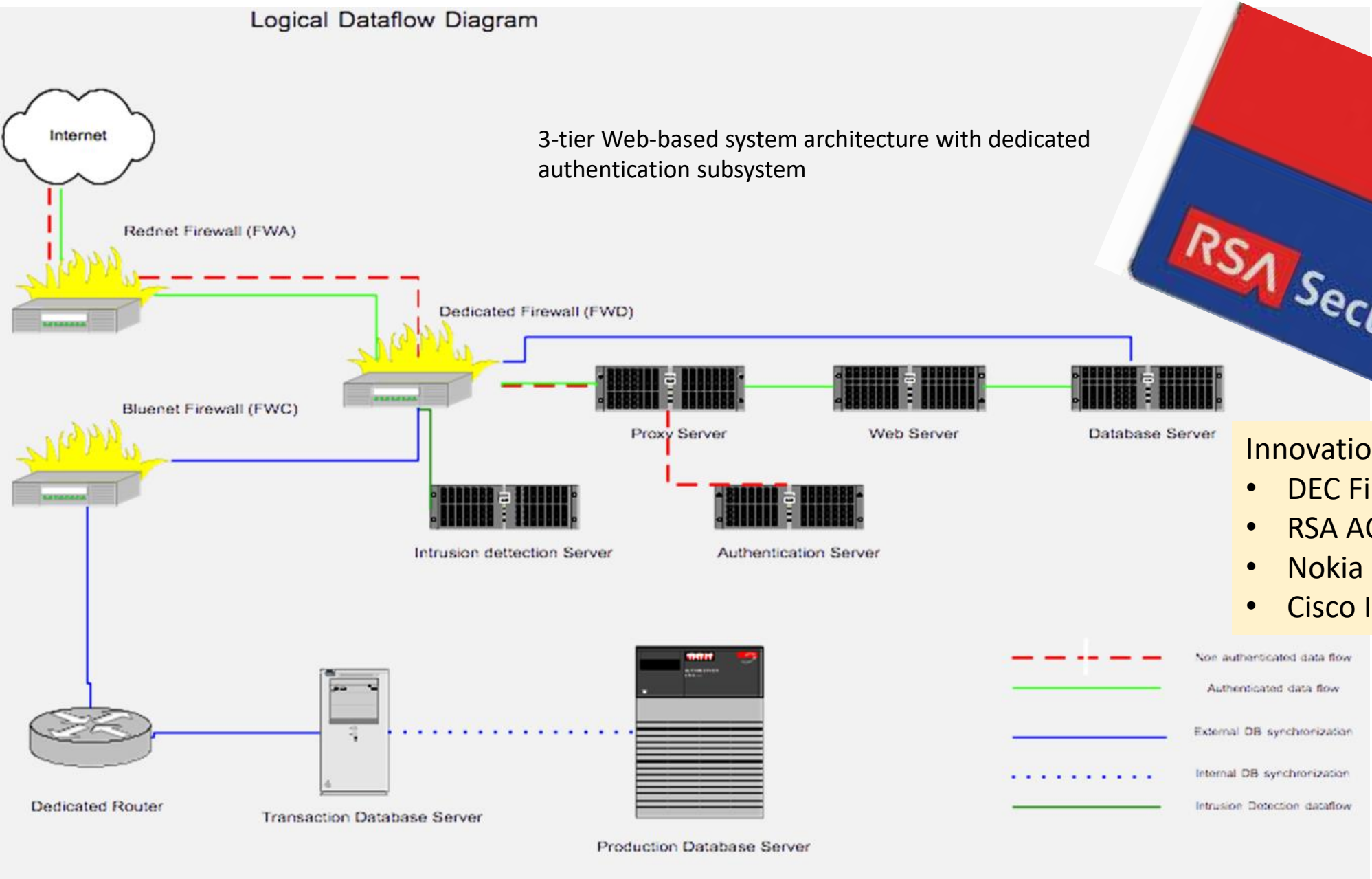
Public key cryptography



1983, "Cryptographic communications system and method."
The three inventors, which the patent is named after, are Ronald Rivest, Adi Shamir, and Leonard Adleman.
2002, Turing Award



2001 Online Claims Payment Tracking System



3-tier Web-based system architecture with dedicated authentication subsystem

Innovation used

- DEC Fiber channel
- RSA ACE/Server
- Nokia Firewall
- Cisco Intrusion Detection server

Public key cryptography use cases

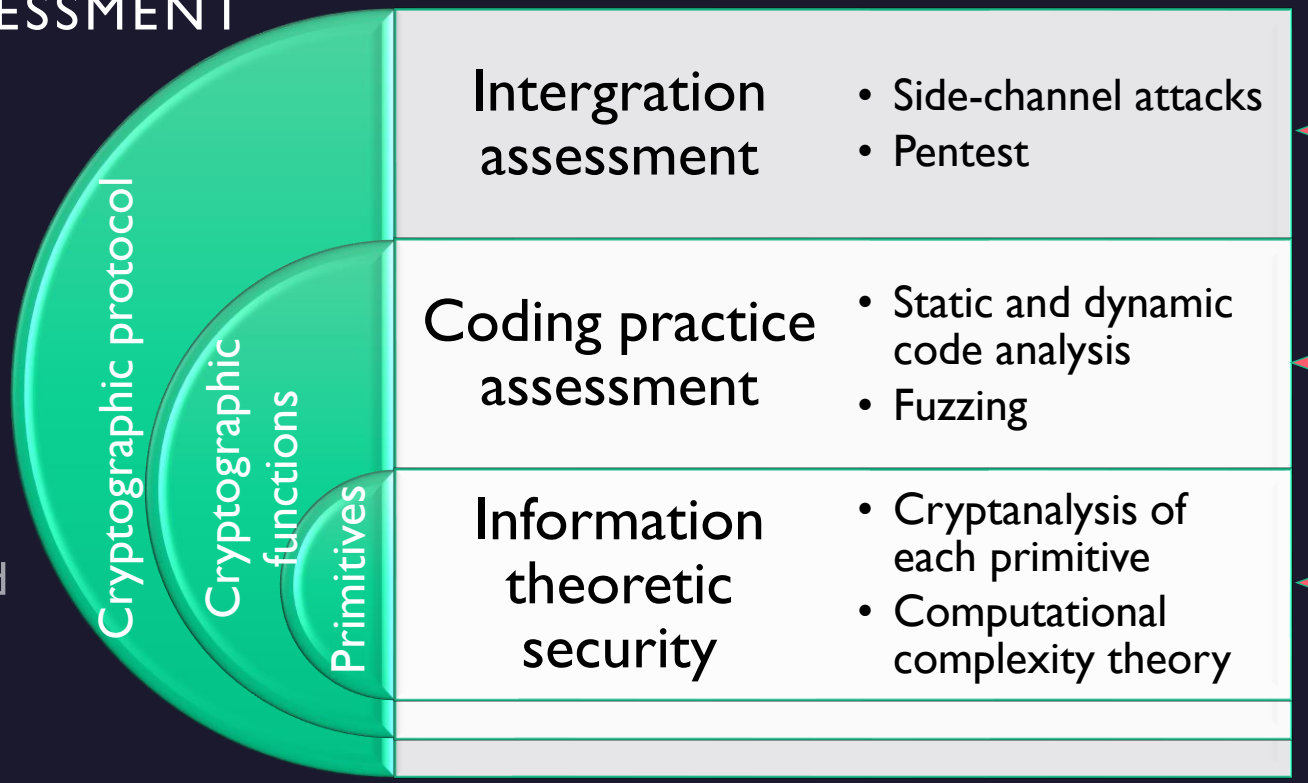
- Confidentiality: Encrypted information can only be accessed by the person for whom it is intended and no one else.
- Integrity: Encrypted information cannot be modified in storage or in transit between the sender and the intended receiver without any alterations being detected.
- Non-repudiation: The creator/sender of encrypted information cannot deny their intention to send the information.
- Authentication: The identities of the sender and receiver—as well as the origin and destination of the information—are confirmed.
- Key management: The keys used in encrypting and decrypting data and associated tasks like key length, distribution, generation, rotation, etc. are kept secure.

The Quantum Threat

Cryptographic controls risk analysis

CODING PRACTICE ASSESSMENT

- Static analysis: Examines source code without executing the program.
- Dynamic analysis: Examines software while running.
- Fuzzing uncovers vulnerabilities by injecting malformed or unexpected data.



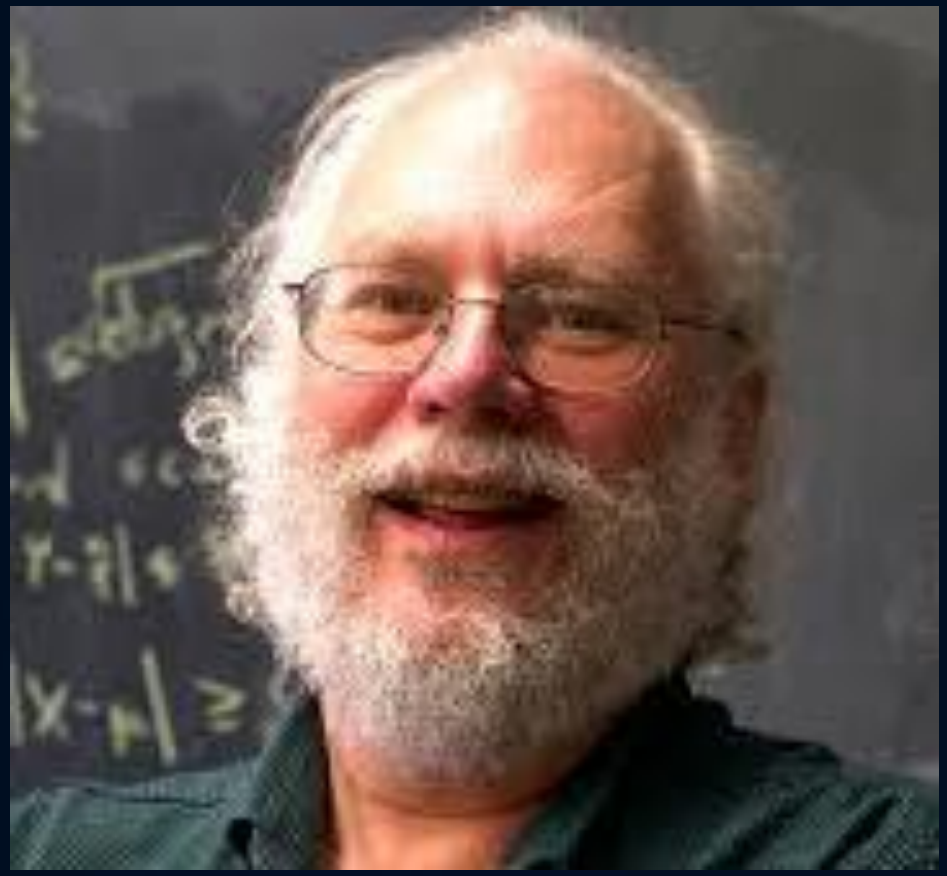
RSA Challenge

- 2020
- RSA-250 solved (829bits)
- The total computation time was roughly 2700 core-years, using Intel Xeon Gold 6130 CPUs as a reference (2.1GHz)
- RSA-250 sieving: 2450 physical core-years
- RSA-250 matrix: 250 physical core-years
- Ref: https://sympa.inria.fr/sympa/arc/cado-nfs/2020-02/msg00001.html

- We used computer resources of the Grid'5000 experimental testbed in France (INRIA, CNRS, and partner institutions) [3], of the EXPLOR computing center at Université de Lorraine, Nancy, France [4], an allocation of computing hours on the PRACE research infrastructure using resources at the Juelich supercomputing center in Germany [5], as well as computer equipment gifted by Cisco Systems, Inc. at UCSD.

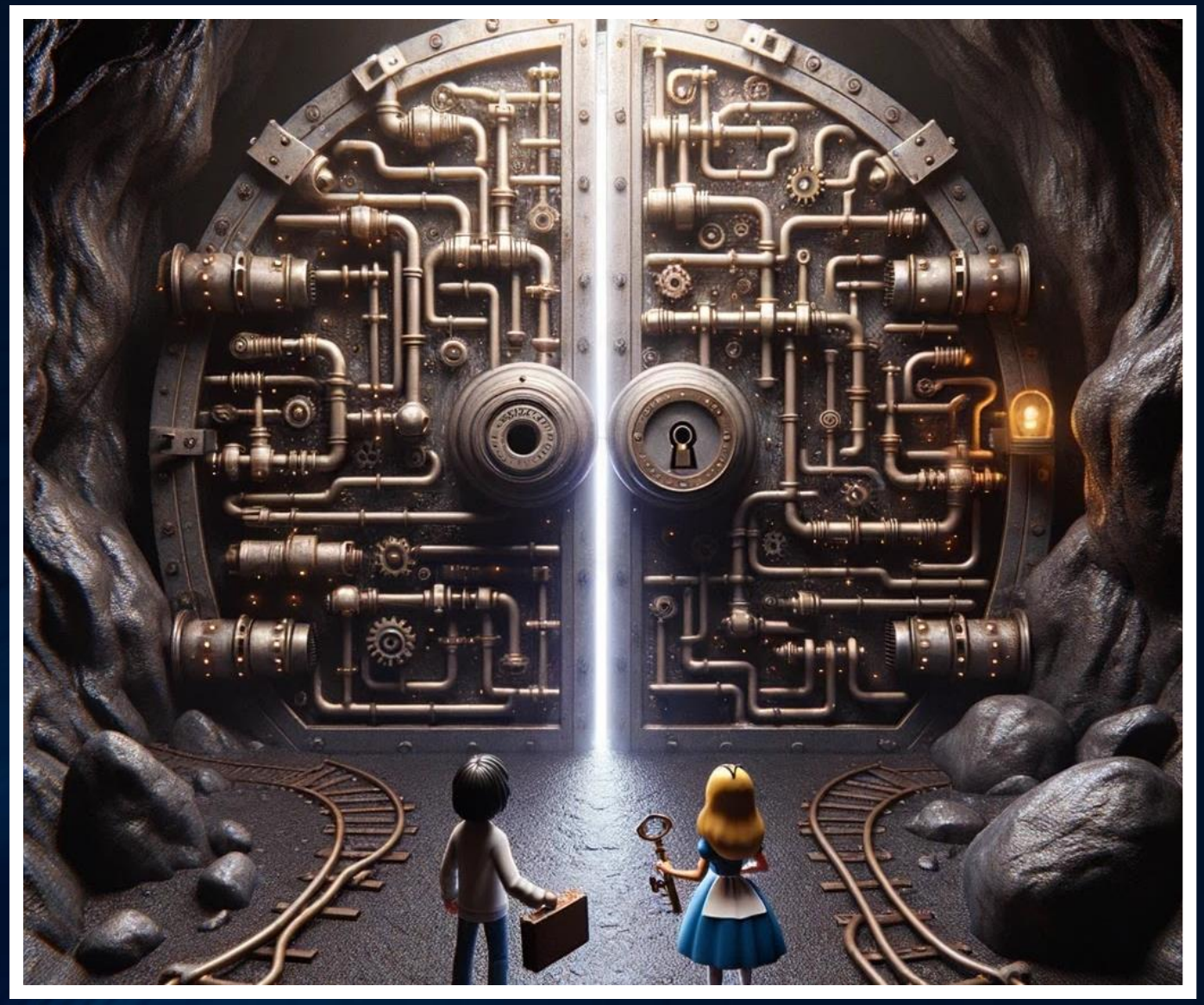
Shor’s algorithm

- Shor's algorithm is a quantum algorithm for finding the prime factors of an integer.
- “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits.“
- In August 2023, an IBM team showed an error correction technique that could control the errors in a 12-qubit memory circuit using an extra 276 qubits, a big improvement over the thousands of extra qubits required by surface codes.



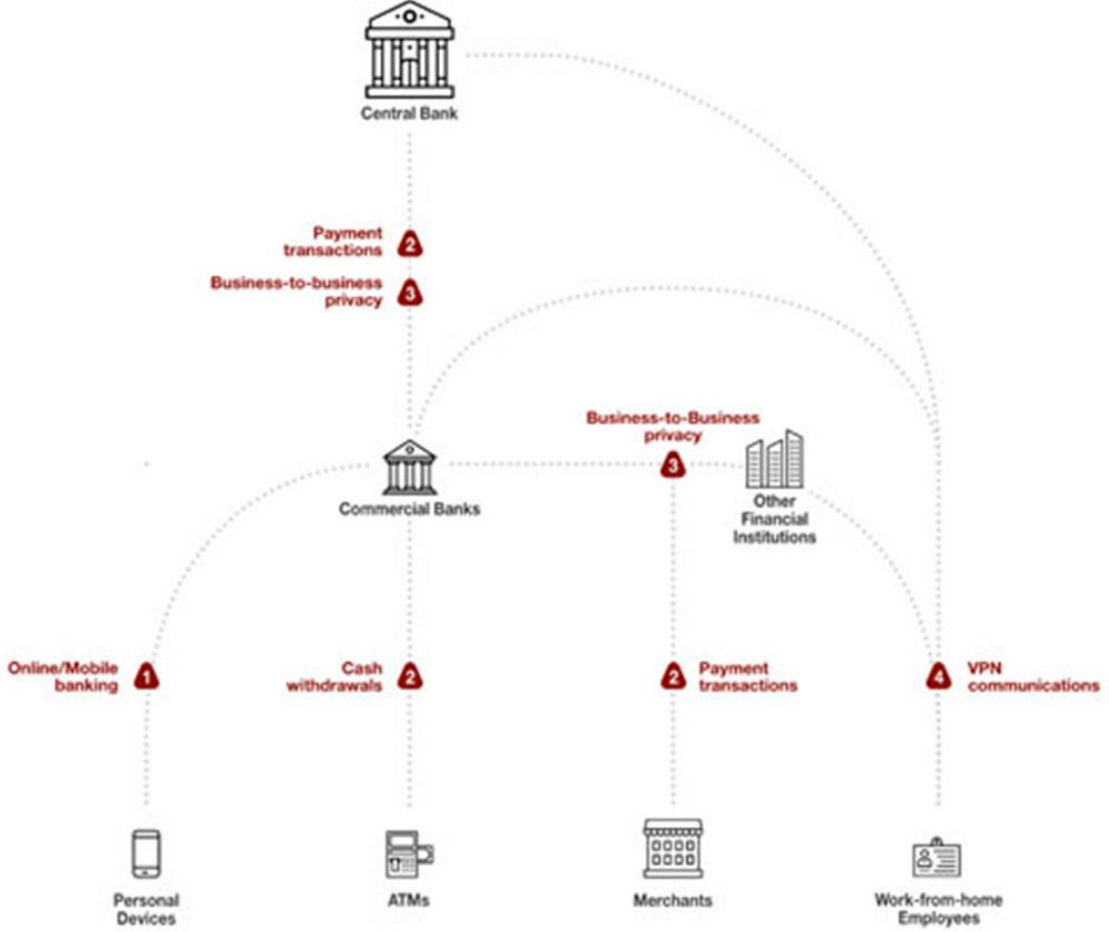
Peter Shor

Risks to Digital Financial Systems



5D – An orchestrated targeted ransomware attack campaign (may include partial data destruction)

- ION provides mission-critical trading and workflow automation software, high-value analytics and insights, and strategic consulting to financial institutions, central banks, governments, and corporates.
- It was hit by ransomware attack in late January 2023. Its cleared derivatives platform was unavailable for a week which disrupted customers that include some of the world's biggest banks, brokerages and hedge funds.
- The Futures Industry Association (FIA) said the situation was improving after some exchanges and clearing houses offered extensions to allow affected firms to meet clearing and reporting deadlines. Clearing is the process of ensuring trades have gone through and the relevant parties are fully settled up. The U.S. Commodity Futures Trading Commission, a regulator, delayed publication of weekly trading statistics because some affected ION customers were not able to collate information fast enough to compile daily positioning reports.
- Lockbit said a ransom had been paid, declining to say how much it was, or offer evidence the money had been handed over. ION declined to comment on Lockbit's statement.



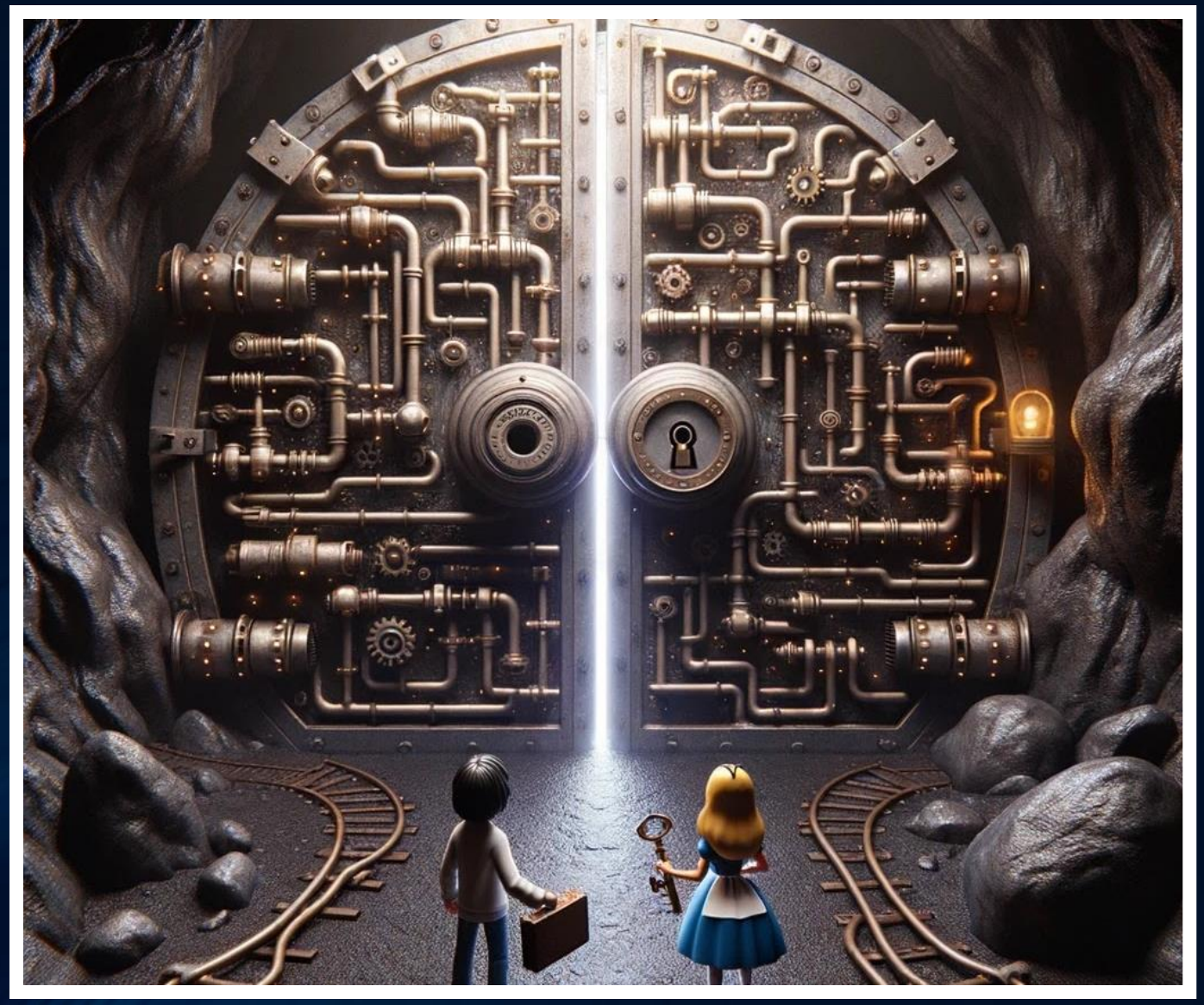
1 **Online/Mobile Banking**
Compromising customer-to-central bank/commercial bank/broker or e-commerce connections to commit unauthorized transactions, including CBDC

2 **Payment Transactions and Cash Withdrawals**
Committing unauthorized transactions against existing payment systems, and ATM machines

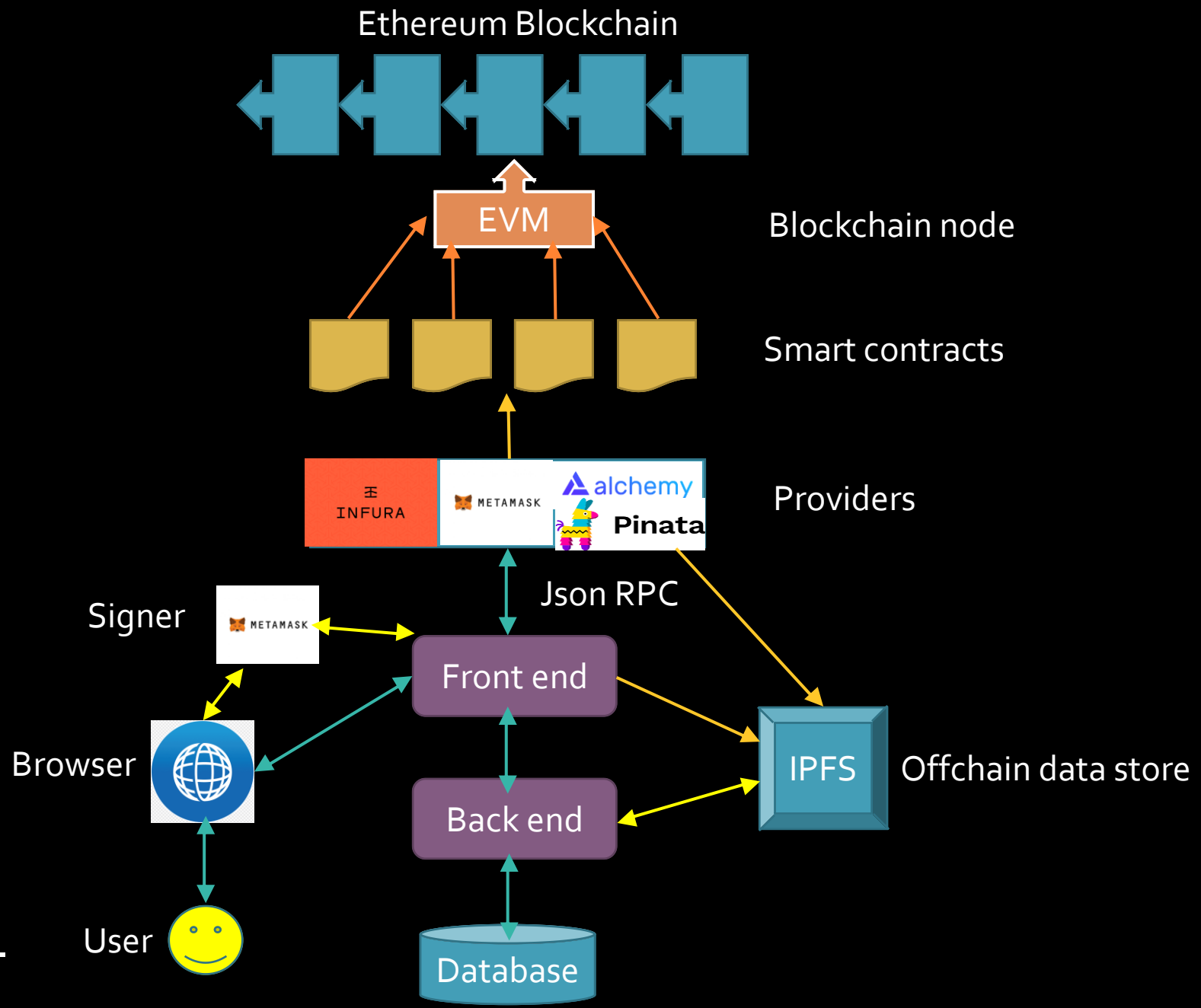
3 **Business to Business Privacy**
Compromising widely used point-to-point secure communications between financial institutions, brokers and businesses

4 **VPN Communications**
Compromising VPN connections used for staff to work-from-home to access organizational internal and sensitive resources

Impact on Cryptocurrencies and Blockchain



A typical decentralized financial application architecture



Off-chainEthereum throughput scaling

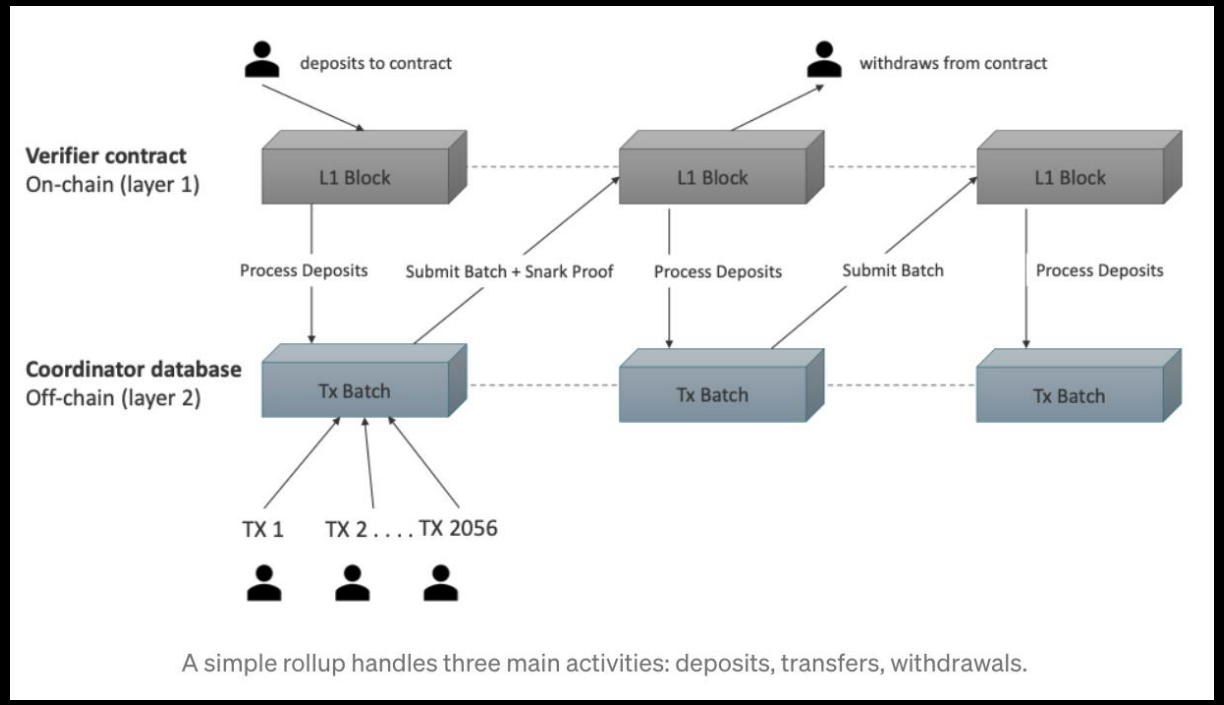
Off-chain scaling is achieved through Layer 2 (L2) rollup chains.

L2 rollup chains process large number of transactions that are "rolled-up" to L1 chain for verification.

The verification is performed using either optimistic or zero-knowledge proof (ZKP) based consensus.

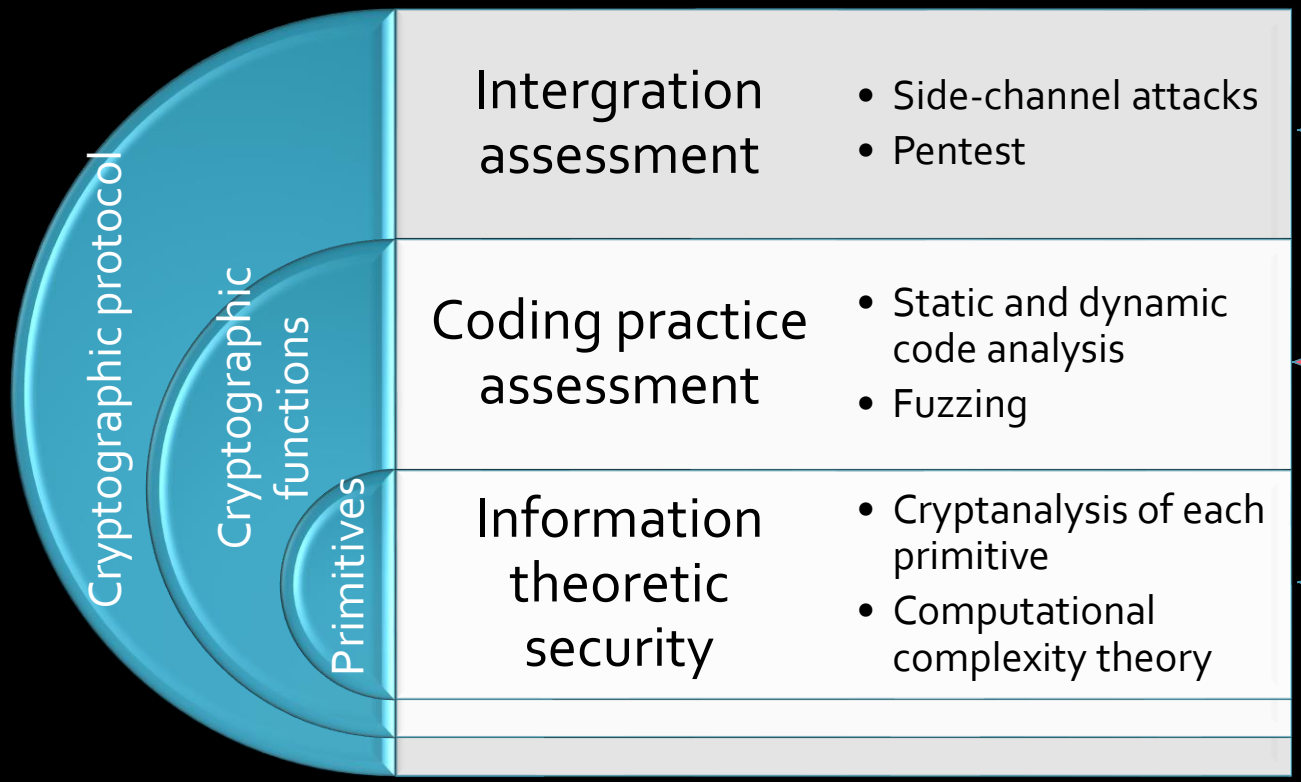
ZKRollup technology is in our focus because of its maturity, performance, transparency and availability.

ZKRollups are types of proofs submitted to L1 for verification of transaction batches.



A simple rollup handles three main activities: deposits, transfers, withdrawals.

Cryptographic controls risk analysis

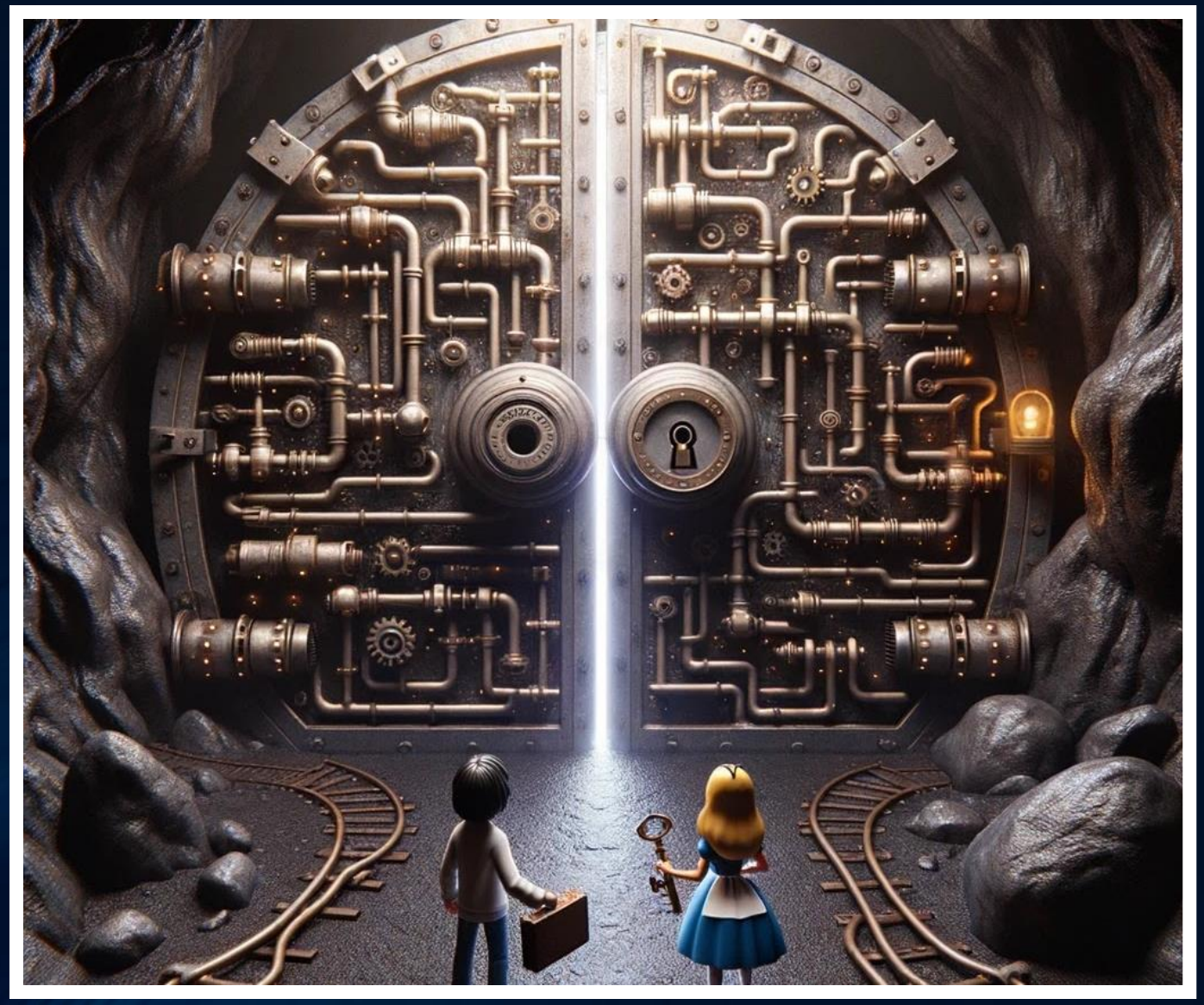


Shellshock BASH
EVM, ZKEVM

Heartbleed buffer over-read in TLS
Smart-contracts

RC4 in SSL 3.0
POODLE
ECDSA, PRNG, SHA256

Protecting Against Quantum Threats



Finding a problem that QCs can't solve rapidly

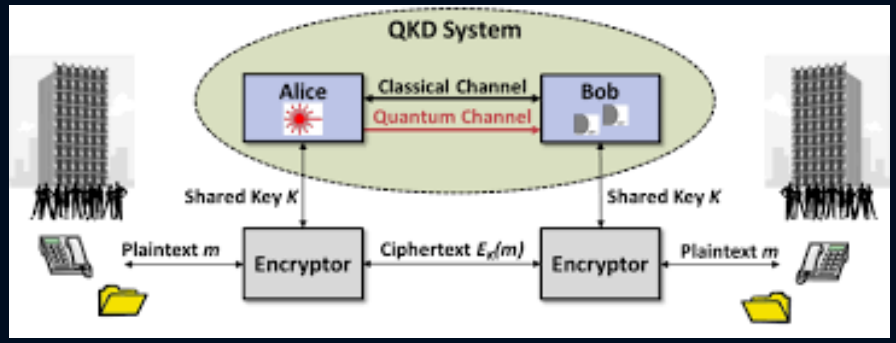
- hash functions and symmetric zero-knowledge proofs
- error correcting codes
- lattices (including the learning with errors (LWE) and NTRU problems)
- multivariate equations
- supersingular elliptic curve isogenies
- Ref: https://pqca.org/about/why-pqca/

- Proposed NIST standards
- CRYSTALS-Kyber (key encapsulation)
- CRYSTALS-Dhilitium (digital signature schema)
- SPHINCS+ (hash based signatures)
- FALCON (hash and sign)

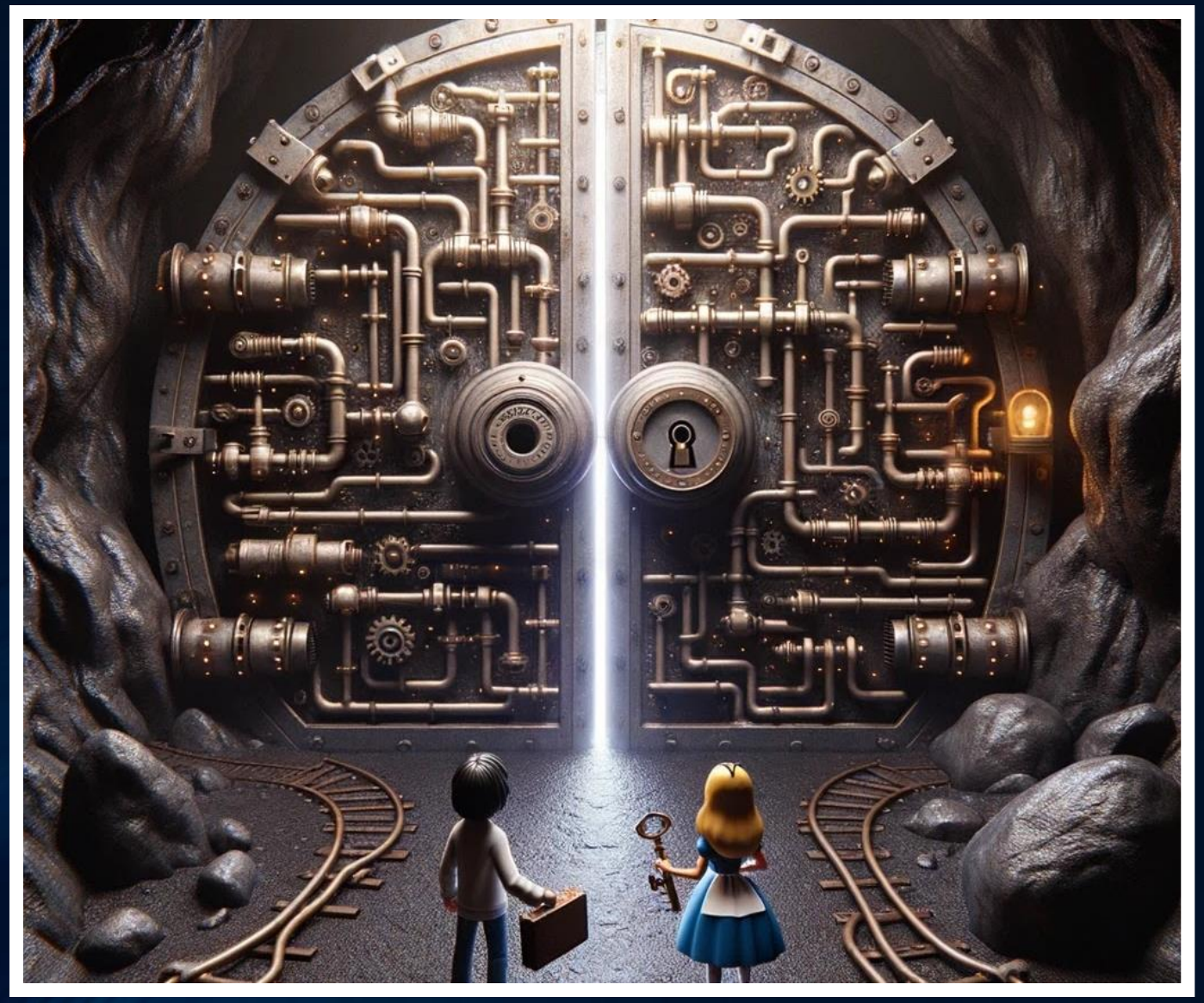
Using quantum against quantum

- Quantum random number generators and one-time pads

- Quantum Key Distribution



What You Can Do



The way forward

- Inventory of cryptographic assets (hardware and software)
  - Cryptography Bill of Materials (CBOM) https://cyclonedx.org/
- Planning: Migrate or Retire?
- Execution

Conclusion:
- Key takeaways.
- Emphasize the need for proactive measures.
- Call to action for awareness and advocacy for secure technology

Dr. Viktor Polic

vpolic@cybersymbiosis.com

https://ch.linkedin.com/in/viktor-polic-891a1a145