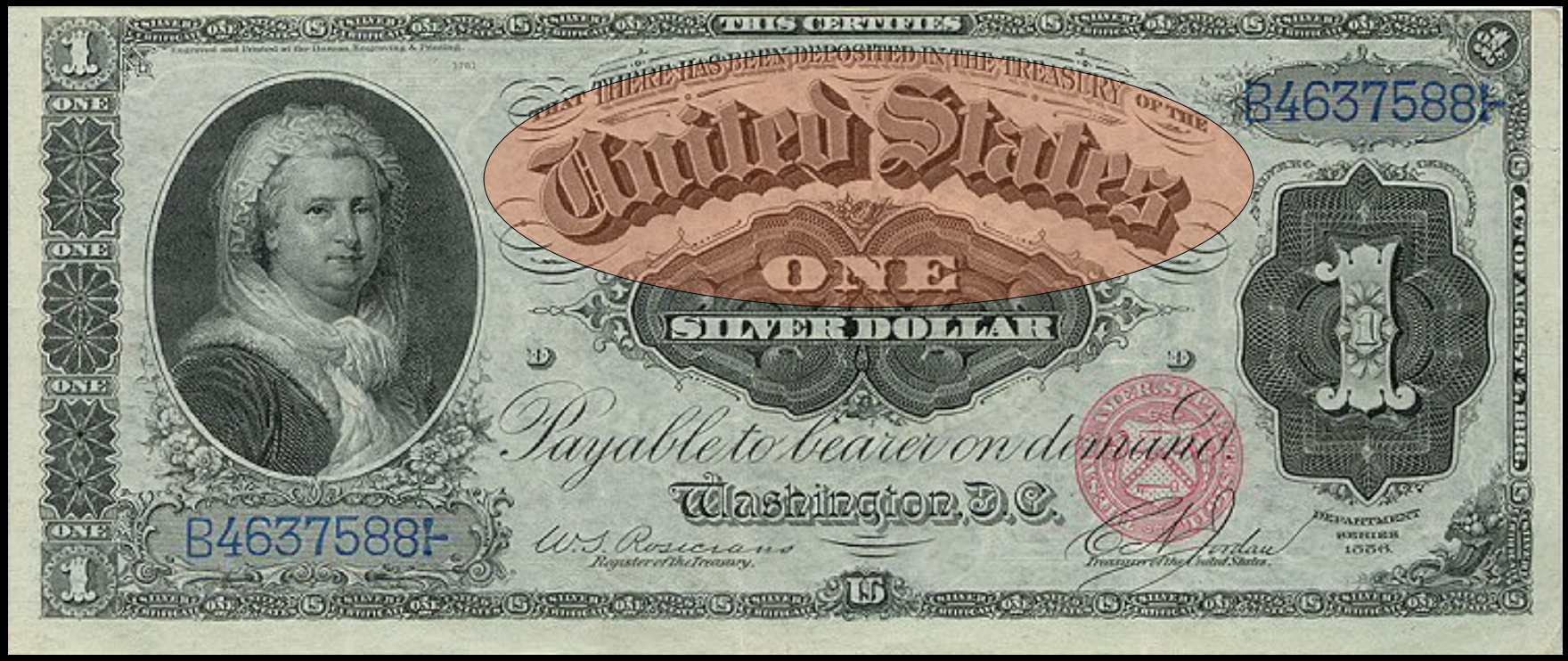
Breaking and making quantum money: toward a new quantum cryptographic protocol

Andrew Lutomirski, MIT
with: Scott Aaronson, Edward Farhi, David Gosset, Avinatan Hassidim, Jon Kelner, and Peter Shor



US $1 1886 Silver Certificate.jpg

What is a quantum state?

$$n \text{ qubits}$$

$$\text{State is in a } 2^n \text{ dimensional Hilbert space}$$

$$|\psi\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle$$

Unknown states cannot be copied!

Properties of quantum money

- The bank can print it
- Anyone can verify it (public-key)
- No one can copy it

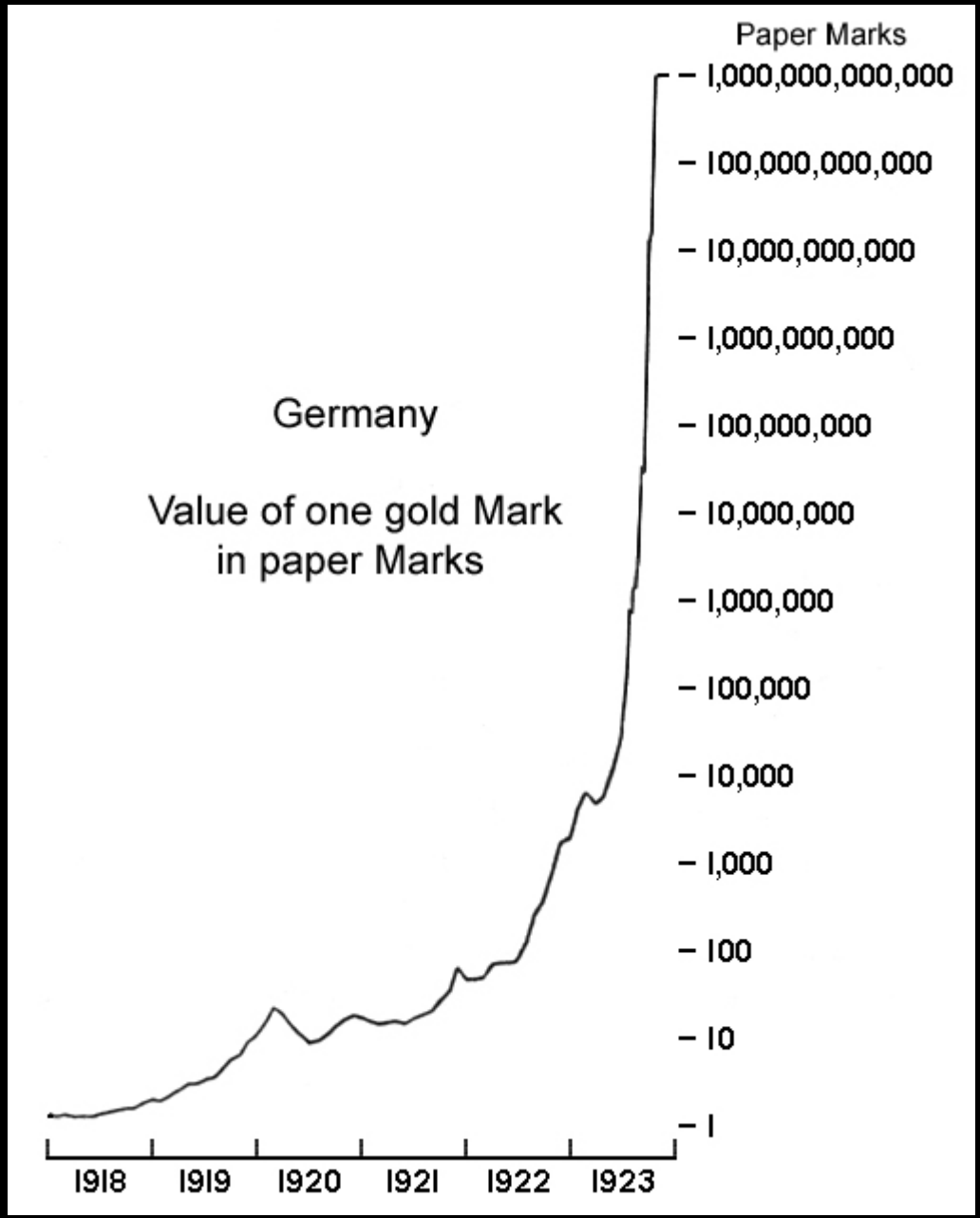

THIS CERTIFIES
THAT THERE HAS BEEN DEPOSITED IN THE TREASURY OF THE
United States
ONE
SILVER DOLLAR
Payable to bearer on demand
Washington, D.C.
B4637588I
B4637588I
W. S. Rosecrans
Register of the Treasury.
Treasurer of the United States.
ONE

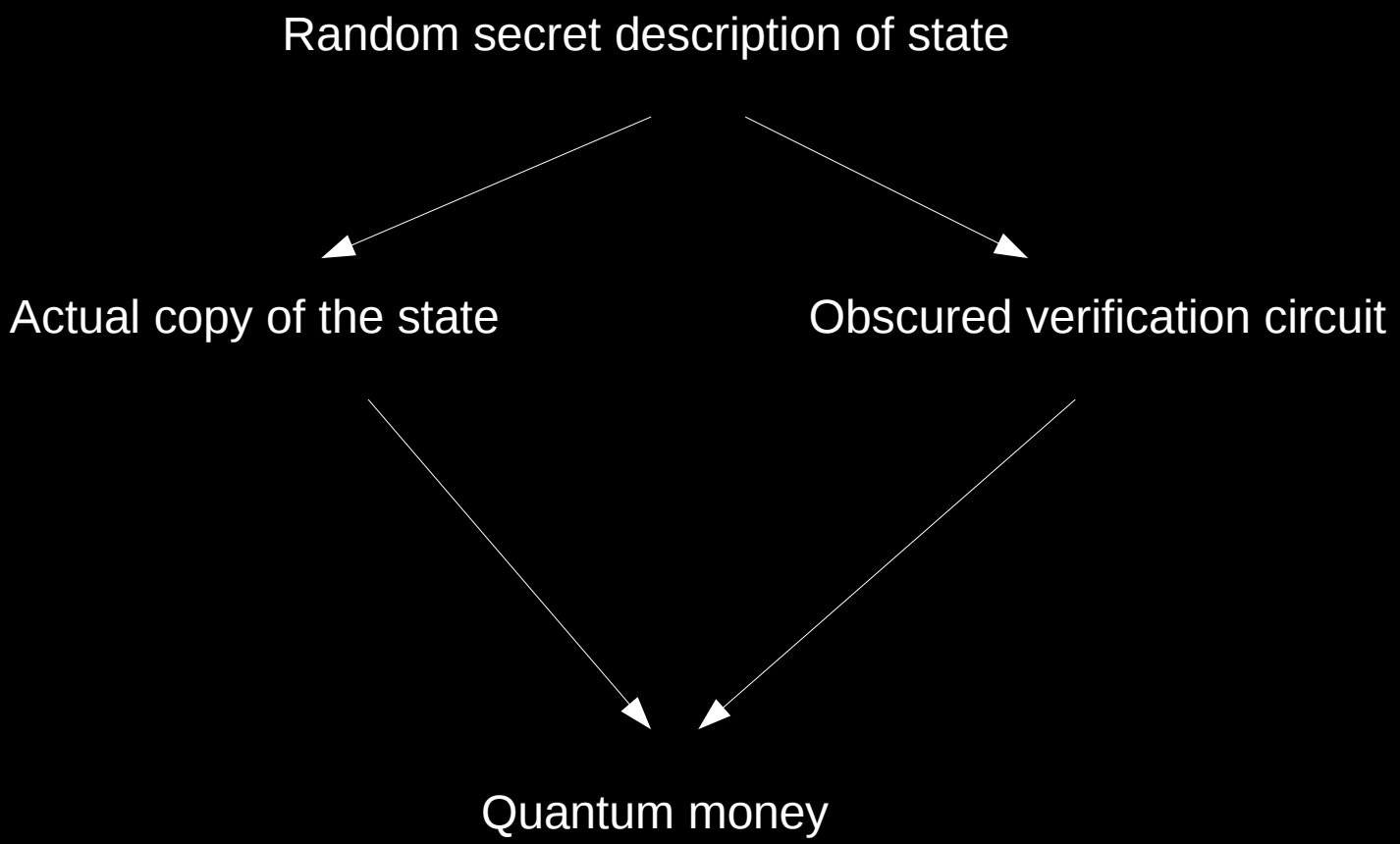
A single piece of quantum money

- A quantum state
- A “serial number” that encodes a circuit to verify the state
- A digital signature of the serial number

Properties of quantum money

- The bank can print it
- Anyone can verify it (public-key)
- No one can copy it
- Collision-free: *no one* can produce two states with the same serial number


Paper Marks
1,000,000,000,000
100,000,000,000
10,000,000,000
1,000,000,000
100,000,000
10,000,000
1,000,000
100,000
10,000
1,000
100
10
1
Germany
Value of one gold Mark
in paper Marks
1918
1919
1920
1921
1922
1923


Random secret description of state
Actual copy of the state
Obscured verification circuit
Quantum money

Postselection money

Labeling function: $L : S \to T$ $\qquad \|S\| \gg \|T\|$

$$|\psi_\ell\rangle = \frac{1}{\sqrt{\|L^{-1}(x)\|}} \sum_{x \text{ s.t. } L(x)=\ell} |x\rangle$$

Verification

Markov chain that mixes rapidly over states with the same label

$$M|\psi_\ell\rangle = |\psi_\ell\rangle$$

$$M^r \approx \sum_\ell |\psi_\ell\rangle\langle\psi_\ell|$$

Verification

Markov matrix has a special form: $U = \sum_i P_i \otimes |i\rangle\langle i|$

$$\left(I \otimes \frac{1}{\sqrt{N}} \sum_{i=1}^{N} \langle i| \right) U \left(I \otimes \frac{1}{\sqrt{N}} \sum_{i=1}^{N} |i\rangle \right)$$

$$= \frac{1}{N} \sum_{i=1}^{N} P_i$$

$$= M$$

Breaking stabilizer money

- Secret is a description of a list of stabilizer states
- A parameter controls the strength of the verifier
- Weak verifiers accept non-stabilizer states
- Strong verifiers allow us to recover the secret