CRYPTO Q

Using quantum in classical crypto

TEAM 2

Alfonso de la Rocha

Álvaro Buendía

Álvaro Reyes

Problems we were trying to tackle

- **Symmetric key distribution**
  - Diffie-Helman: Key exchanged using same channel as data
  - Several interactions to agree about the key

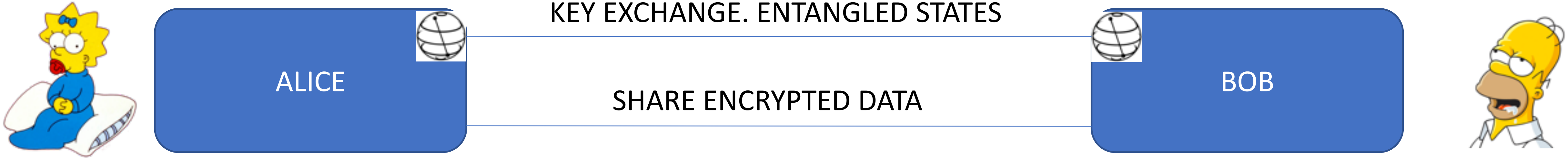
- **Blockchain consensus algorithms**
  - Proof-of-work? Expensive and slow
  - Proof-of-stake? Problem of nothing-at-stake
  - Proof-of-elapsed time? I can cheat selecting my random timer.

Quantum Key Distribution

- Use **quantum entanglement** to share the symmetric key
- **Encrypt using classical cryptography** and send data using classical link.

Quantum Key Distribution

- Use **quantum entanglement** to share the symmetric key
- **Encrypt using classical cryptography** and send data using classical link.



ALICE

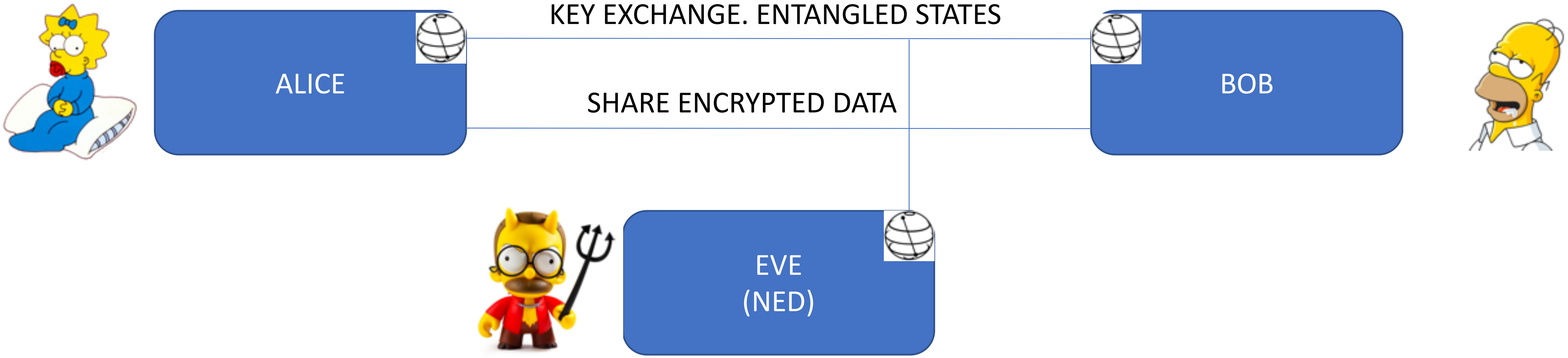
KEY EXCHANGE. ENTANGLED STATES

SHARE ENCRYPTED DATA

BOB

Quantum Key Distribution

- **BUT WAIT!** Our key exchange could be eavesdropped or sabotaged!
- **Simulating Eve’s effect** and adding a parity bit to detect this matter.



KEY EXCHANGE. ENTANGLED STATES

ALICE

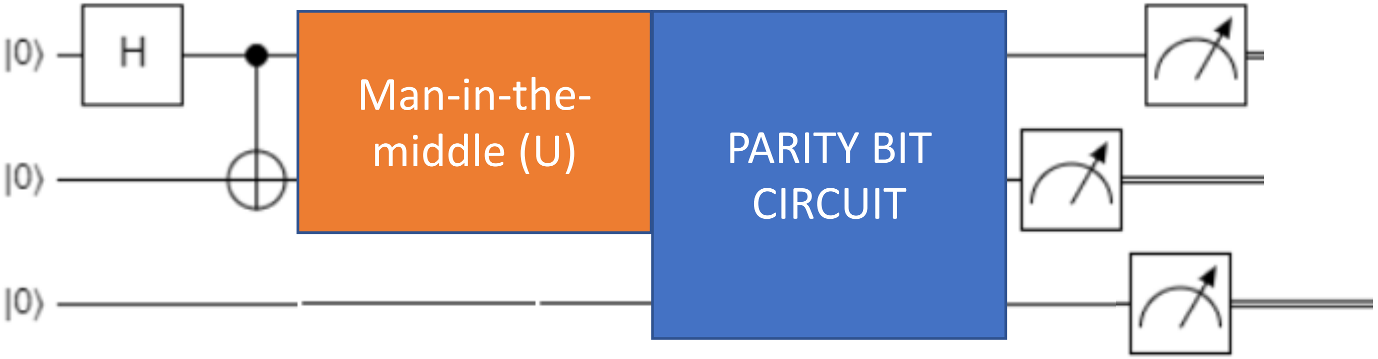
SHARE ENCRYPTED DATA

BOB

EVE
(NED)

How did we do it? Our parity circuit!

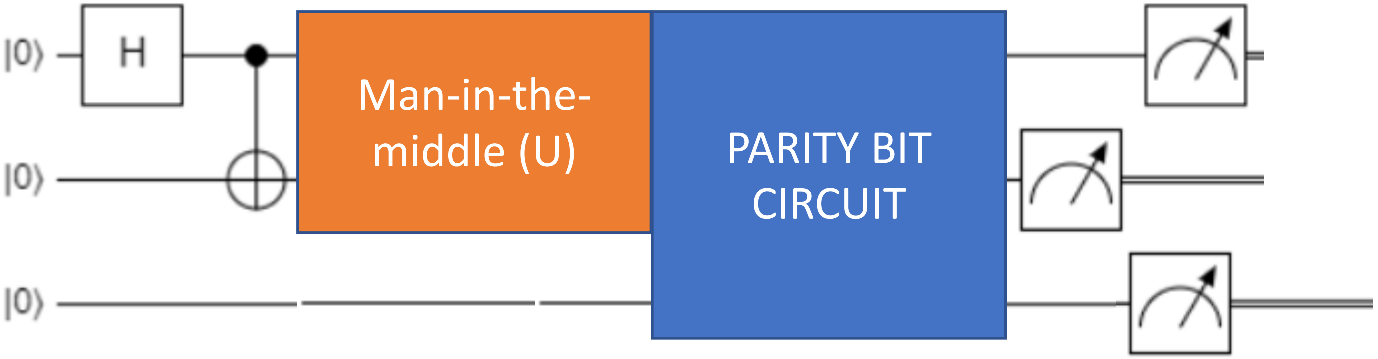
- We implemented a **basic circuit cell to be reused all over the project**.



$$U = R(\theta_A) \otimes R(\theta_B)$$

How did we do it? Our parity circuit!

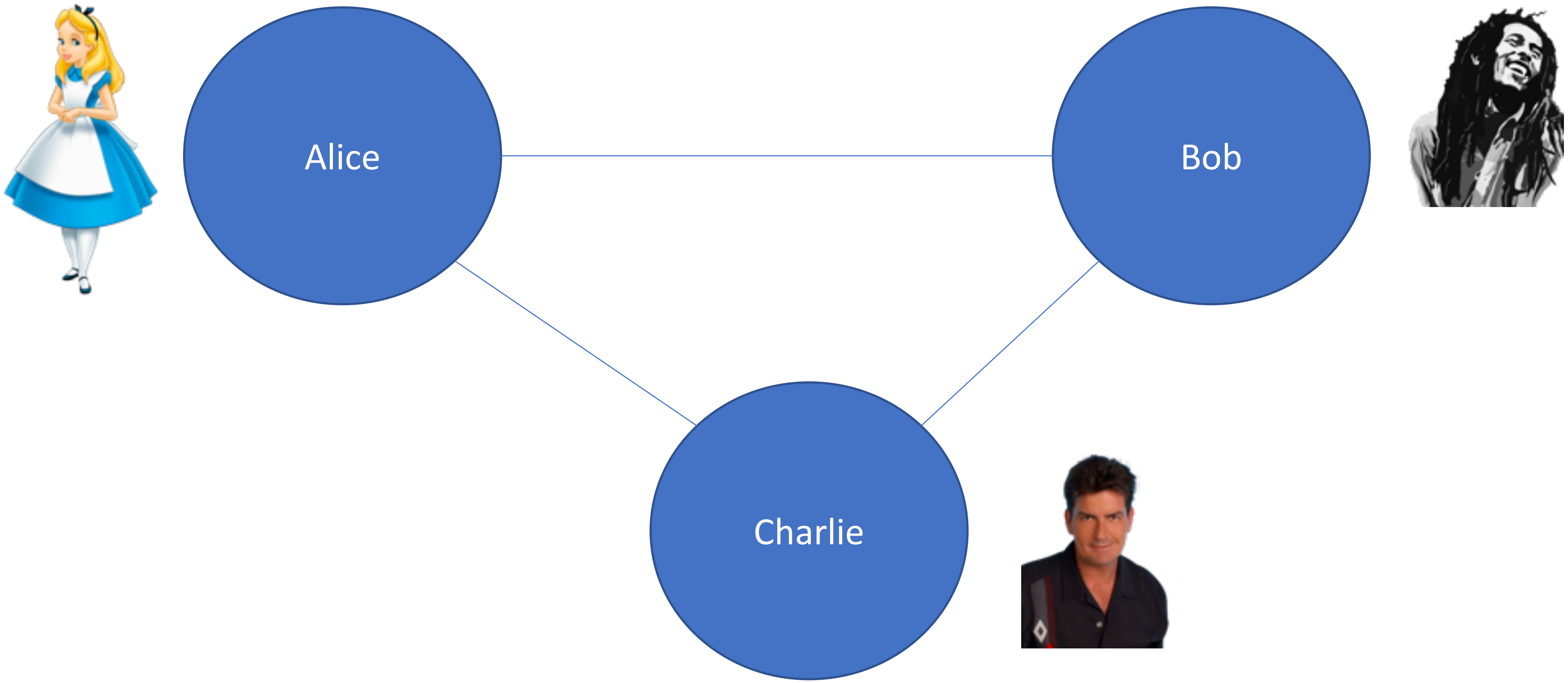
- We implemented a **basic circuit cell to be reused all over the project**.



- **It worked like a charm in simulation!** We detected man-in-the-middle effects and fixed it. Security level of keys may be set.
- However… things started breaking in a real device. **Noice affected our parity bit** (we could fix it with a classical processing after measurement)

Quantum Distributed Consensus

- Things get a bit messier to explain…



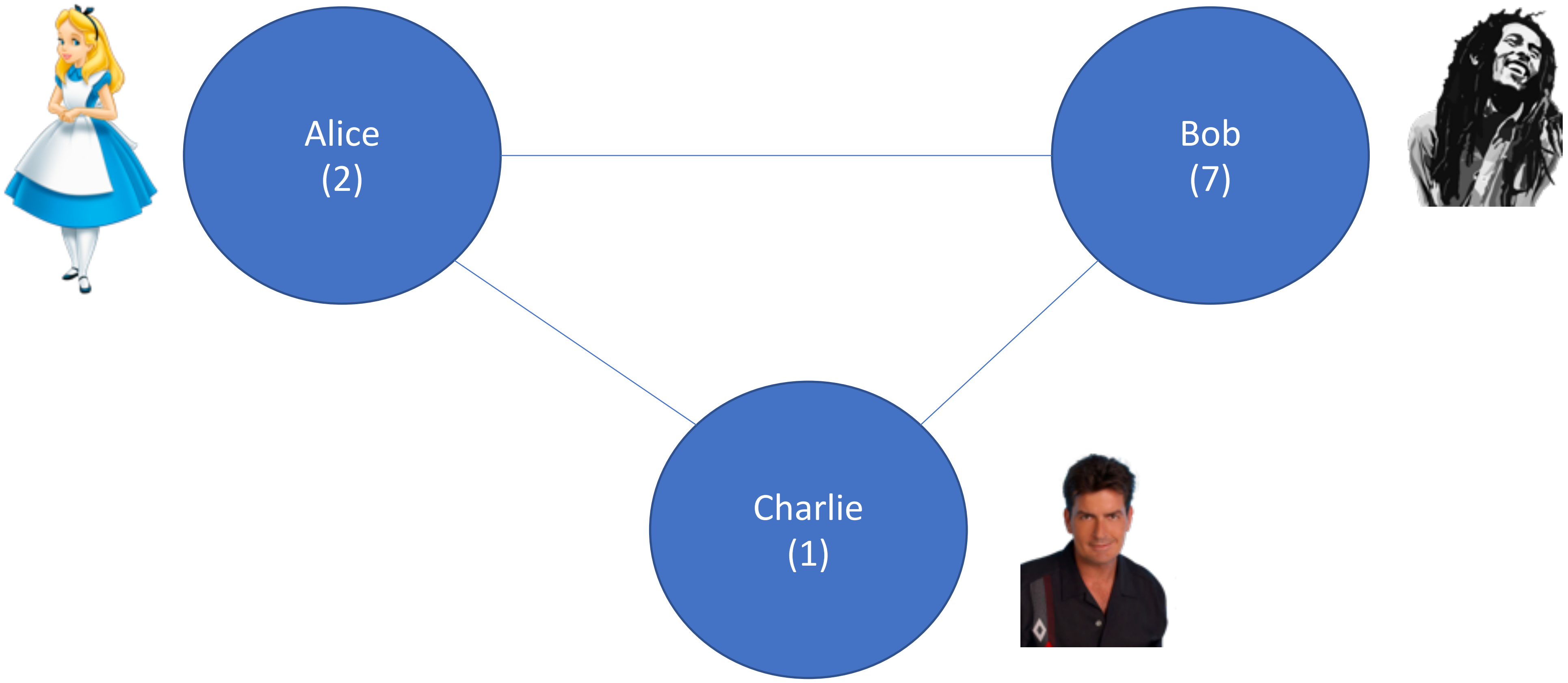
Alice

Bob

Charlie

Quantum Distributed Consensus

- Things get a bit messier to explain…



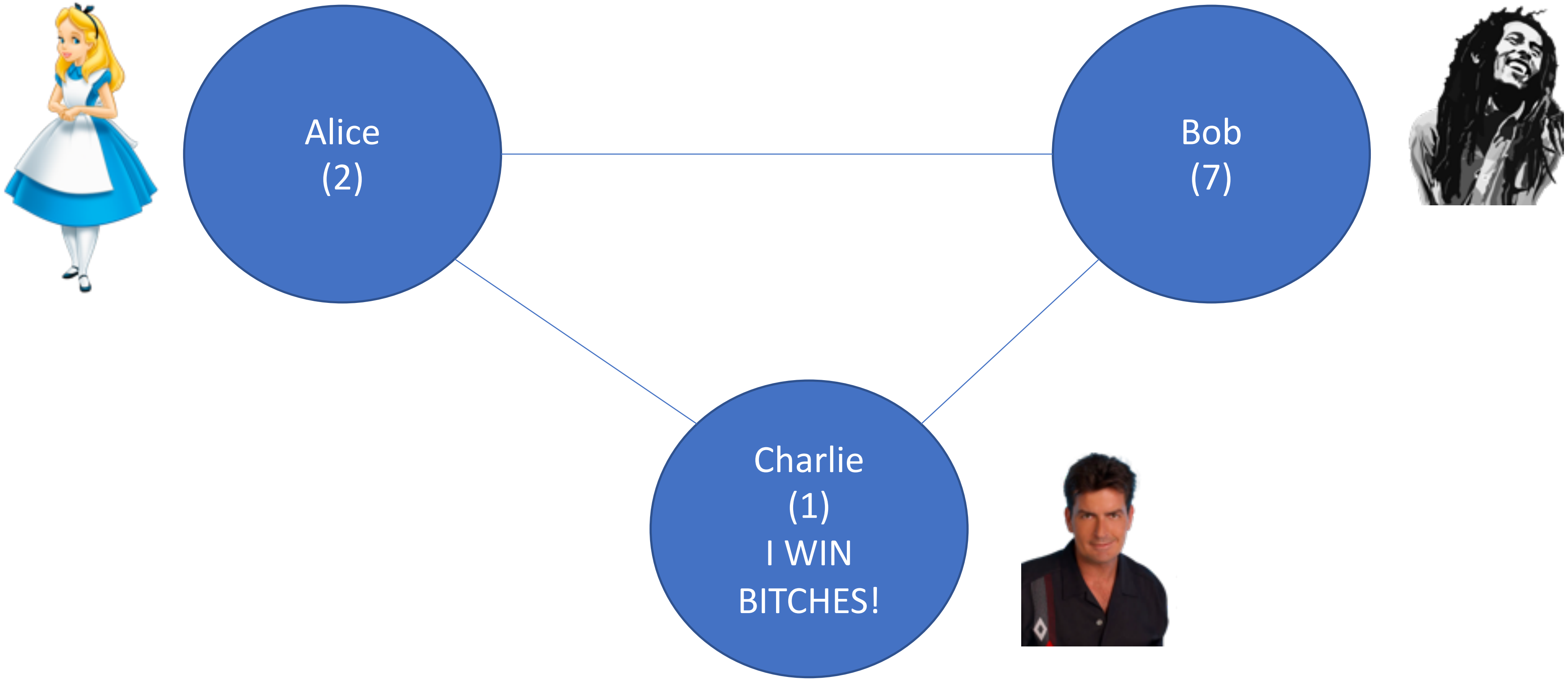
Alice
(2)

Bob
(7)

Charlie
(1)

Quantum Distributed Consensus

- Things get a bit messier to explain…



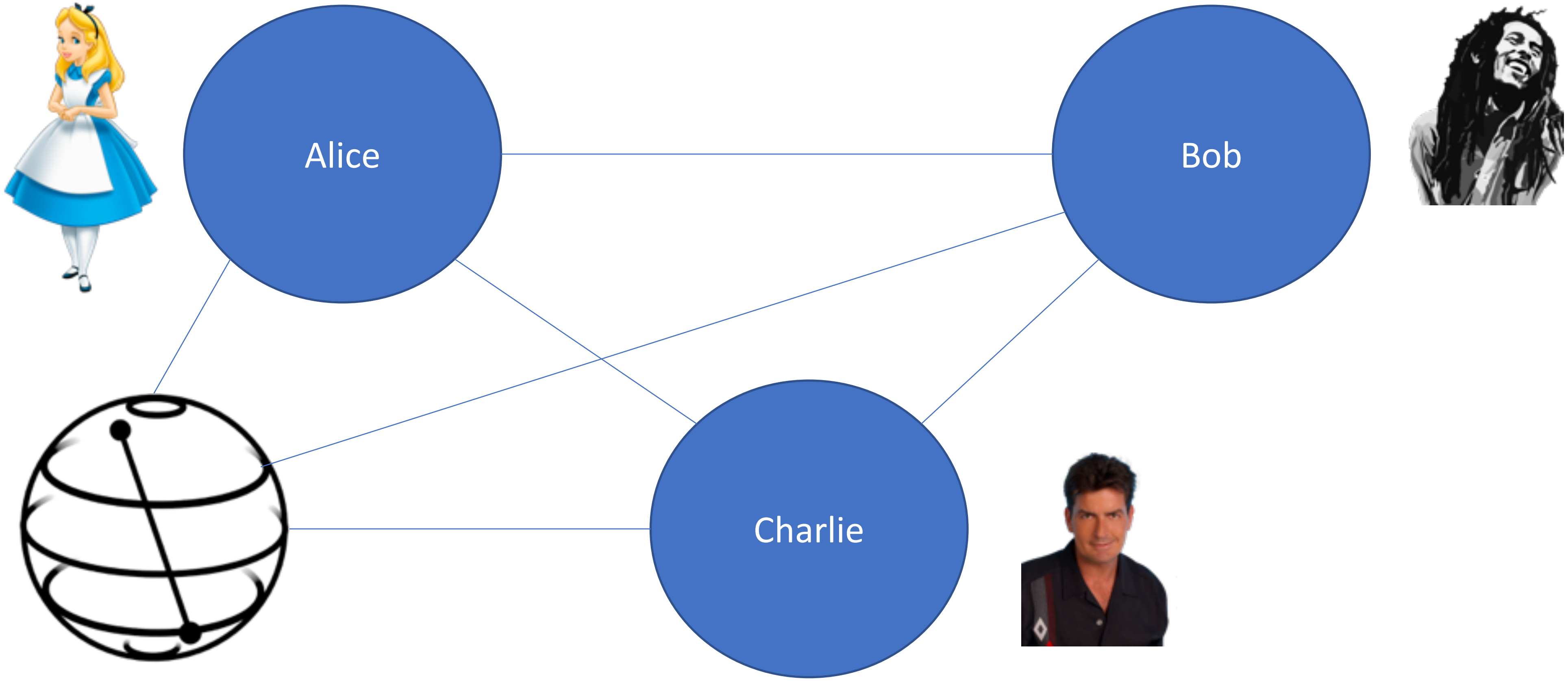
Alice
(2)

Bob
(7)

Charlie
(1)
I WIN
BITCHES!

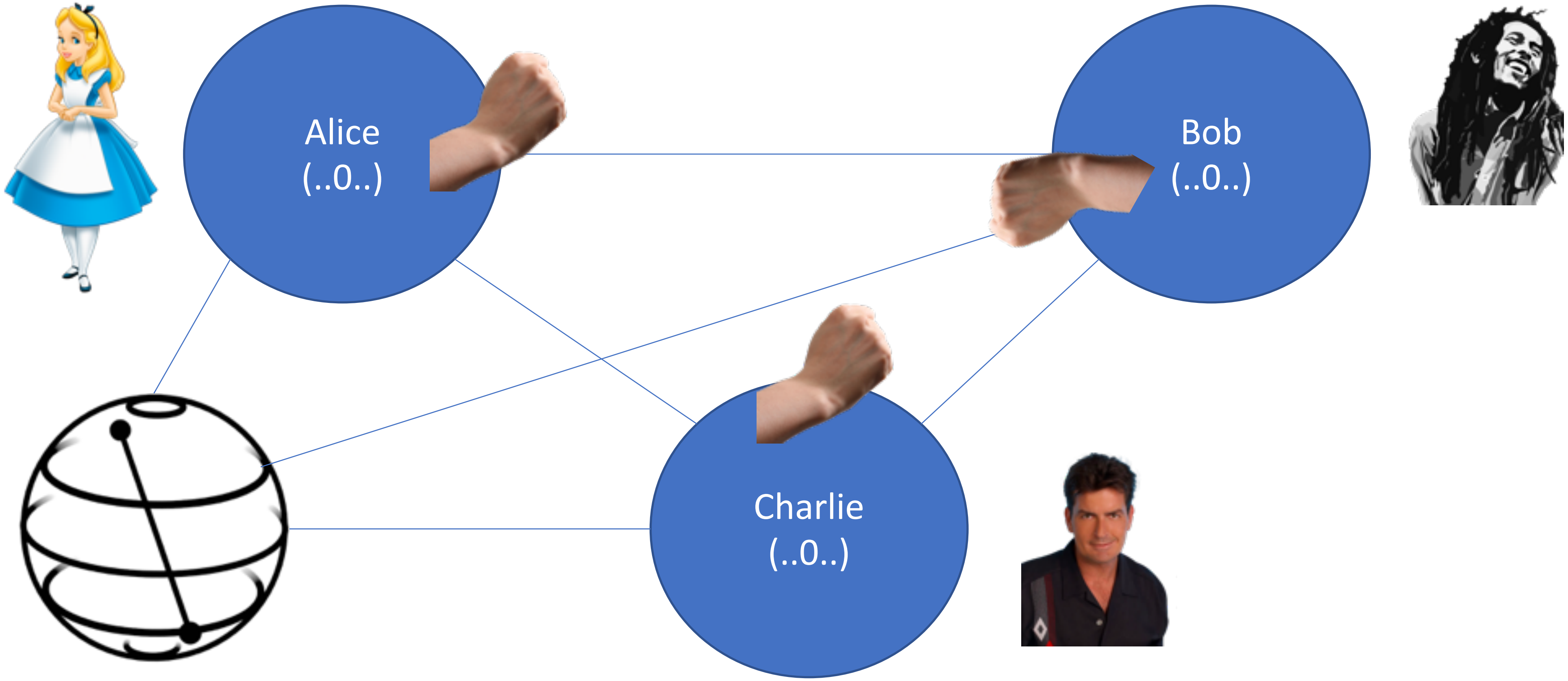
Q Rock-Paper Consensus (QRP-consensus)

- Things get a bit messier to explain…



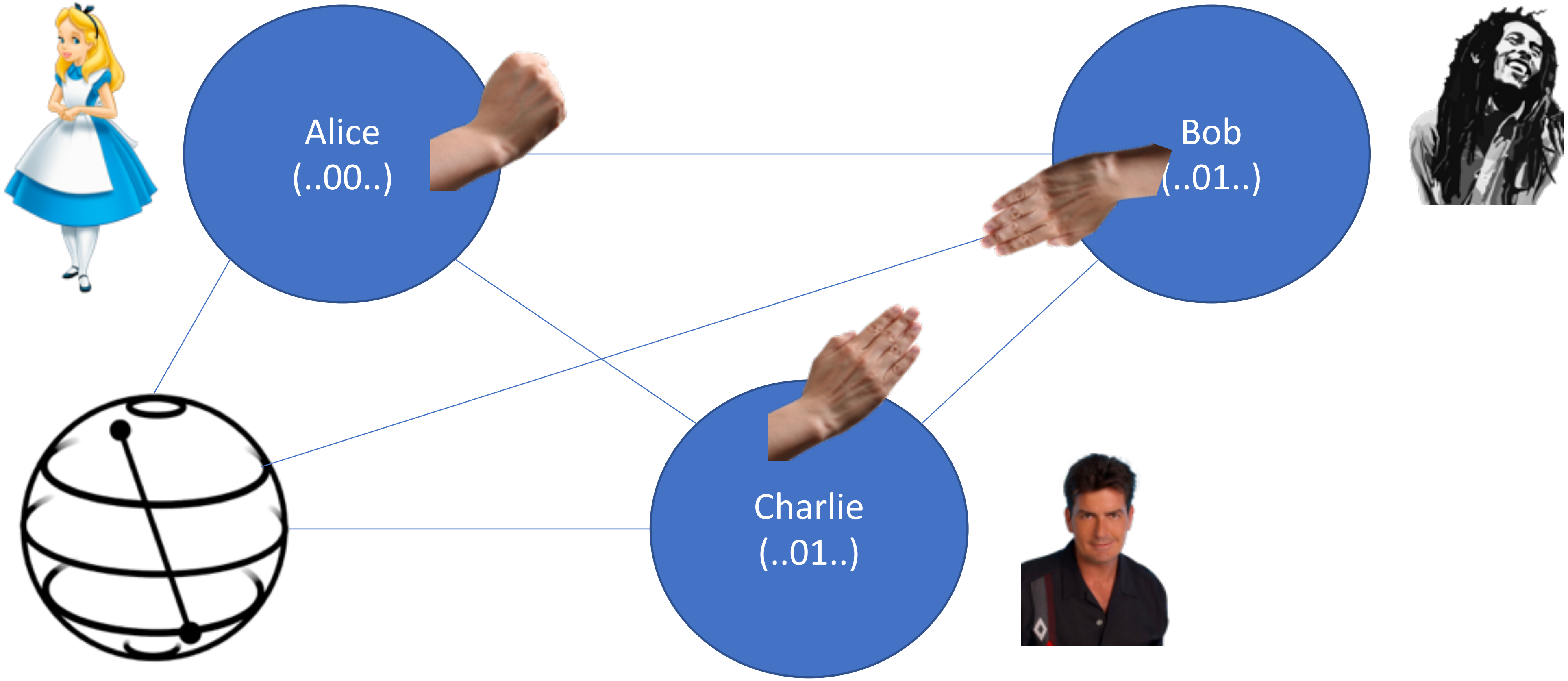
Q Rock-Paper Consensus (QRP-consensus)

- Things get a bit messier to explain…



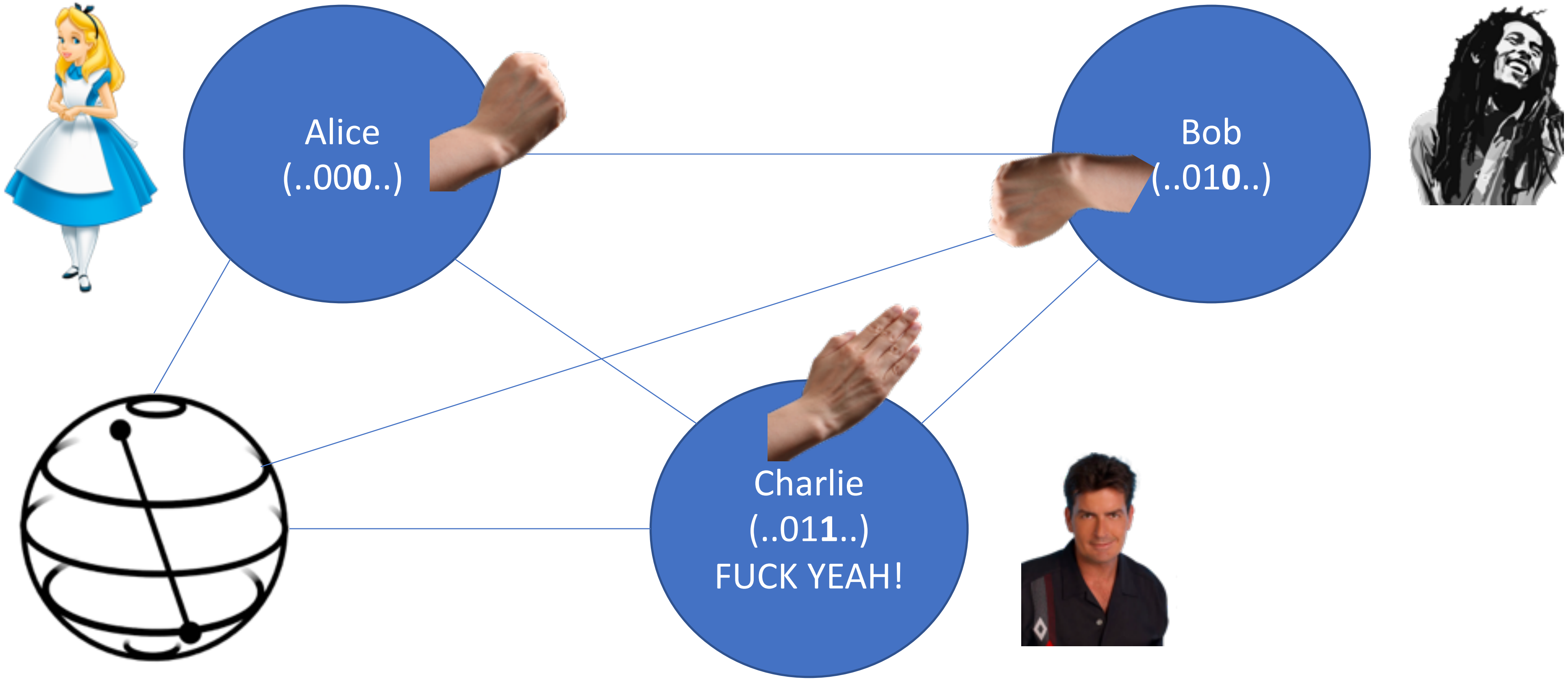
Q Rock-Paper Consensus (QRP-consensus)

- Things get a bit messier to explain…



Q Rock-Paper Consensus (QRP-consensus)

- Things get a bit messier to explain…



Alice
(..00**0**..)

Bob
(..01**0**..)

Charlie
(..01**1**..)
FUCK YEAH!

Q Rock-Paper Consensus (QRP-consensus)

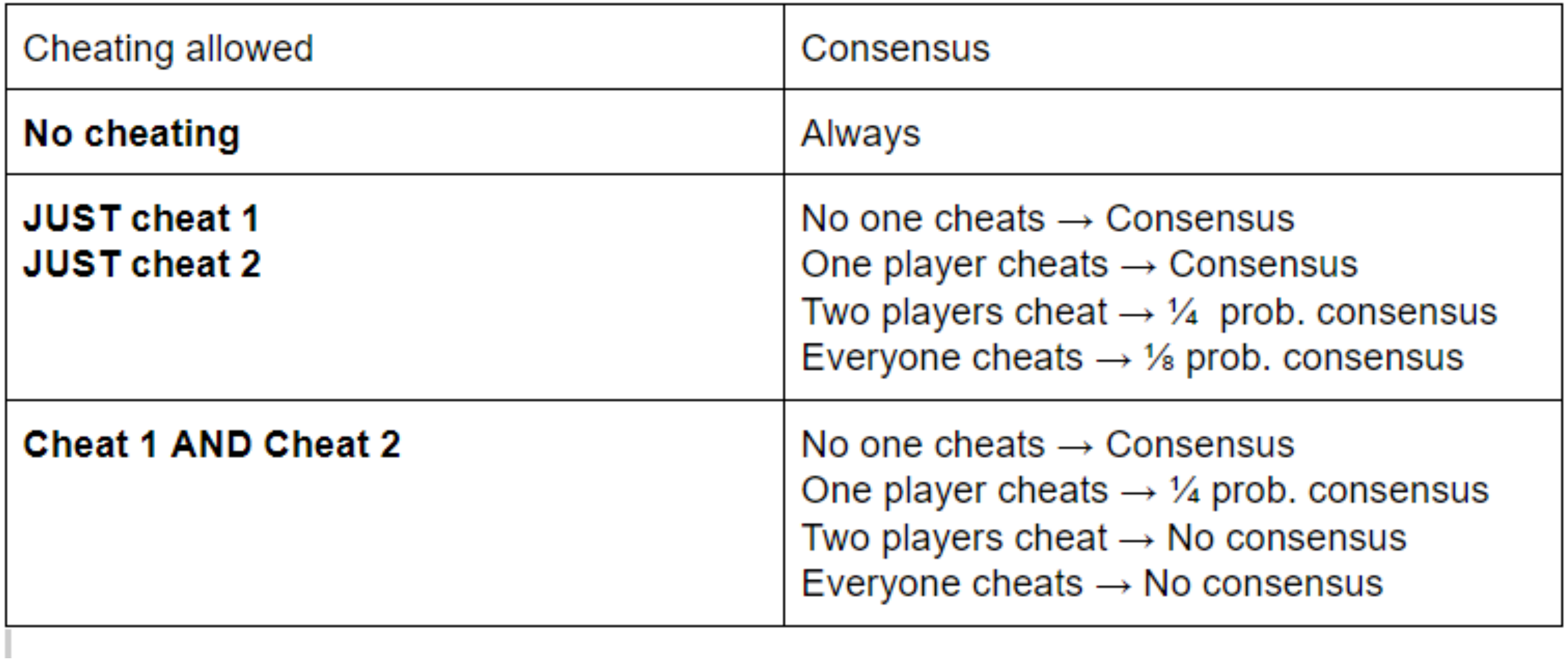
- **Bitwise entanglement** so cheating may be detected (I know my bit and someone else’s)
- But we still can cheat…
- Simulate cheating with “cheating matrices”

$$Ch_1|A, B, C\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |1\rangle$$

$$Ch_2|A_b, B_c, C_a\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |0\rangle$$

- We are aiming a **Byzantine Fault Tolerant Consensus** (1/3 can cheat)

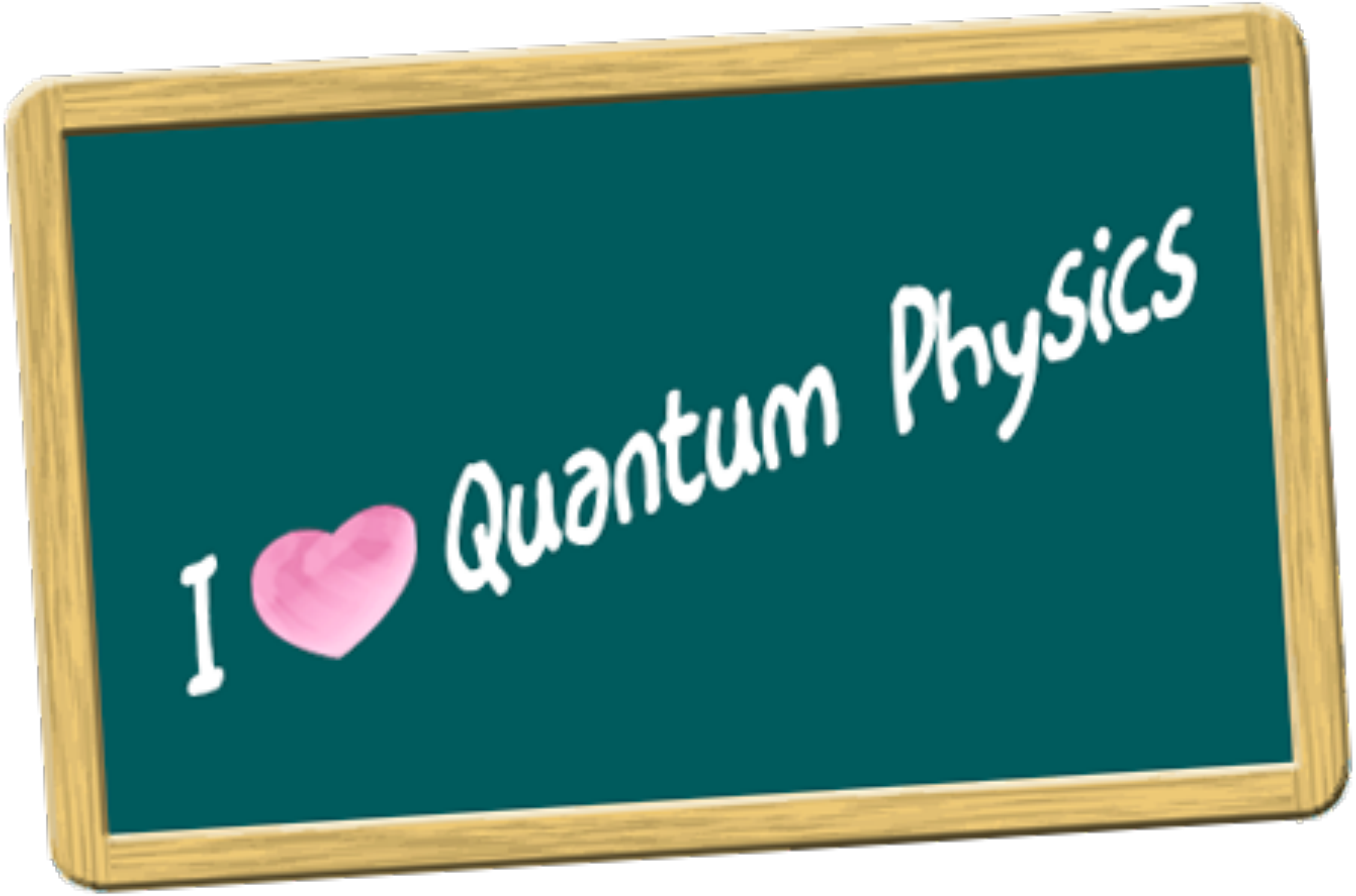
Q Rock-Paper Consensus (QRP-consensus)



Cheating allowed	Consensus
No cheating	Always
JUST cheat 1 **JUST cheat 2**	No one cheats → Consensus One player cheats → Consensus Two players cheat → ¼ prob. consensus Everyone cheats → ⅛ prob. consensus
Cheat 1 AND Cheat 2	No one cheats → Consensus One player cheats → ¼ prob. consensus Two players cheat → No consensus Everyone cheats → No consensus

What else? Future work.

- Quantum Key Distribution in real devices with parity bit.
- **Enhanced QRP consensus** where cheating is penalized. Test it in a real setup.
- **QRPS (Rock-Paper-Scissors) consensus** with encoded 3-D Qudits
- Learn more about quantum and qiskit! And publish a paper? We'll see.


I ♥ Quantum Physics