

A Quantum Money solution to the Blockchain Scalability Problem

Andrea Coladangelo, Or Sattath

QCrypt 2020



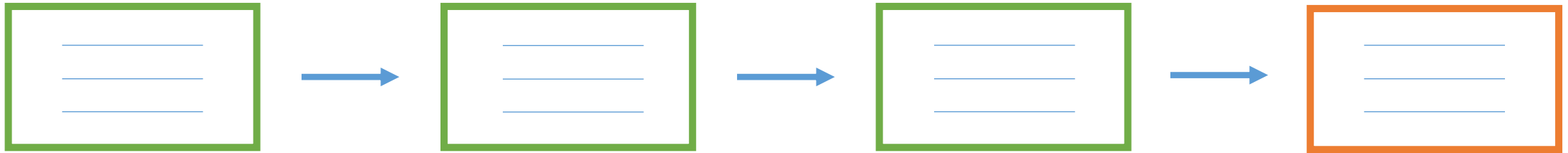
Berkeley
UNIVERSITY OF CALIFORNIA

The scalability problem

The amount of resources or time needed per transaction grows with the number of users.

e.g. Long waiting times for Bitcoin transactions, and limited throughput.

What is *a blockchain*



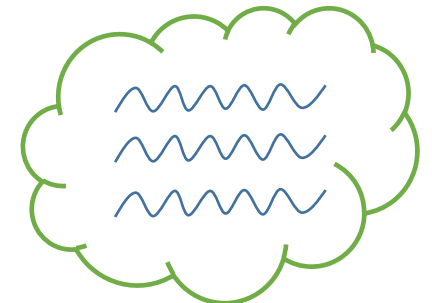
- A sequence of blocks.
- Each block contains data about previous transactions.



How does a user add a new transaction?



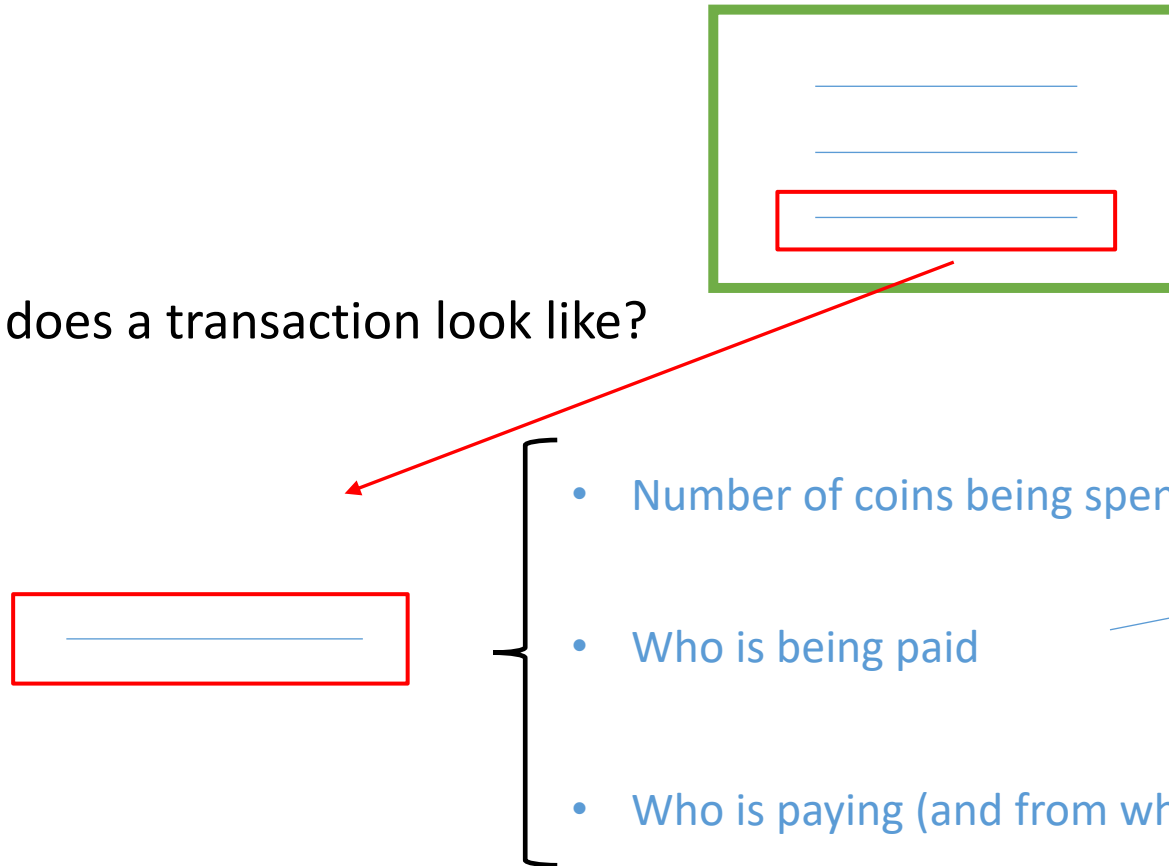
“Alice pays 4 coins to Bob”



Pool of pending transactions

What is a blockchain

What does a transaction look like?



- Number of coins "deposited" in the transaction.
- **A set of instructions φ .** (e.g. Anyone who provides a value w such that $\varphi(w) = 1$ can release and spend the deposited coins).
- **Reference to a previous transaction,** (and a valid witness for that transaction).

In general, φ could be **any set of instructions**.

Such generic transactions are referred to as ***smart contracts***.

Pros and Cons of a blockchain



Decentralized. Requires no trusted third party.





Digital.



Some consensus mechanism is required for each new block.
This takes time.

What is *Quantum Money*

- Form of money proposed by Wiesner in 1970, based on the No-Cloning Theorem.
- A banknote is a quantum state.
- A Quantum Money scheme is specified by:
 1. A generation procedure **Gen**: $\longrightarrow \left| \text{ \right\rangle, s$
 2. A verification procedure **Ver**: $\left| \text{ \right\rangle, s \longrightarrow \text{“accept” or “reject”}$
- Security: Given **1** valid banknote with serial number s , it is hard for an adversary to produce **2** banknotes with serial number s that both pass verification.

Public key quantum money: state of the art

Public key Quantum Money: **Ver** is a public procedure
(it does not require any secret parameters).

- [Zhandry '18], [Aaronson, Christiano '12], from hidden subspaces. Secure assuming iO .
- [Farhi et al. '12], from knots.
- [Kane '19], from modular forms.
- [Shor '20], from LWE? (unpublished)

Pros and Cons of Public Key Quantum Money



Cannot be counterfeited.



Can be transferred very quickly (via quantum channels or teleportation).
It does not require a consensus mechanism.



Requires a bank, a trusted third party.

Quantum Lightning!




- Formalized in [Zhandry '18]. Informally introduced by [Lutomirski et al. '09].
- Public key quantum money, with an added feature: **no generation procedure** (not even the honest one) **can produce 2 banknotes with the same serial number** (except with negligible probability).

Sketch of a quantum lightning construction

- H a (non-collapsing) Hash function.
- **Gen:** 1. Create a uniform superposition over inputs.
2. Compute H.
3. Measure the image register.

$$\sum_x |x\rangle \longrightarrow \sum_x |x\rangle |H(x)\rangle \longrightarrow \sum_{x:H(x)=y} |x\rangle, y$$

 serial number

↓


↓

The diagram illustrates the generation process. It starts with a uniform superposition over all inputs x , $\sum_x |x\rangle$. This is followed by applying a hash function H , resulting in a superposition over all pairs $(x, H(x))$, $\sum_x |x\rangle |H(x)\rangle$. Finally, the image register $|H(x)\rangle$ is measured, yielding a specific serial number y . The resulting state is a superposition over all pre-images x that hash to y , $\sum_{x:H(x)=y} |x\rangle, y$. Blue arrows indicate the flow from the first state to the second, and from the second state to the final state. A blue arrow also points from the 'serial number' label to the y in the final state.

- **Ver:** (a) Compute Hash H and check that outcome is y .
(b) Distinguish a single pre-image from a superposition over pre-images.

Sketch of a quantum lightning construction

- Why is it hard to produce two valid quantum banknotes with the same serial number?

$$\sum_x \alpha_x |x\rangle \otimes \sum_x \beta_x |x\rangle$$


The diagram shows two blue arrows pointing downwards from the summation indices x in the equation above to the variables x and x' below.

(x, x') is a **collision** with noticeable probability.

Removing the trusted third party?

Quantum lightning: No one can generate two valid banknotes with the same serial number (not even the bank).

This opens to the possibility of removing the trusted third party.

Question: how do you prevent people from printing many banknotes with different serial numbers?

Blockchain



No trusted third party.



Digital.



Some consensus mechanism required. Long waiting times.

Quantum Money/Lightning



Cannot be counterfeited.



Can be transferred very quickly.



Requires a trusted third party.

Blockchain + Quantum Lightning allows to get the best of both worlds.



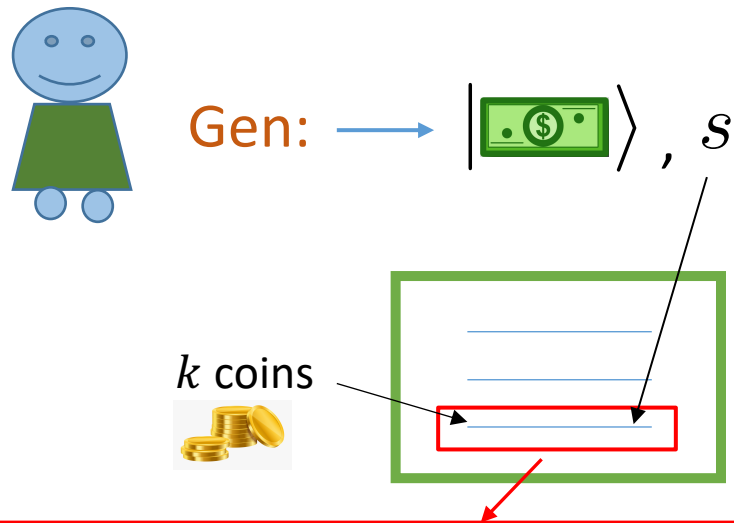
No trusted third party.



Payments are as quick as sending a quantum state.
(no consensus mechanism involved)

1. Mechanism to control generation of quantum banknotes

Recall: A **smart contract** allows to “deposit” a number of coins, with respect to a set of instructions φ .



(i) Generate a new quantum lightning state.

(ii) Deposit some number k of coins in a smart contract. Write the serial number “ s ” in the instructions.

“This is the contract for a quantum banknote:”

Serial number: s

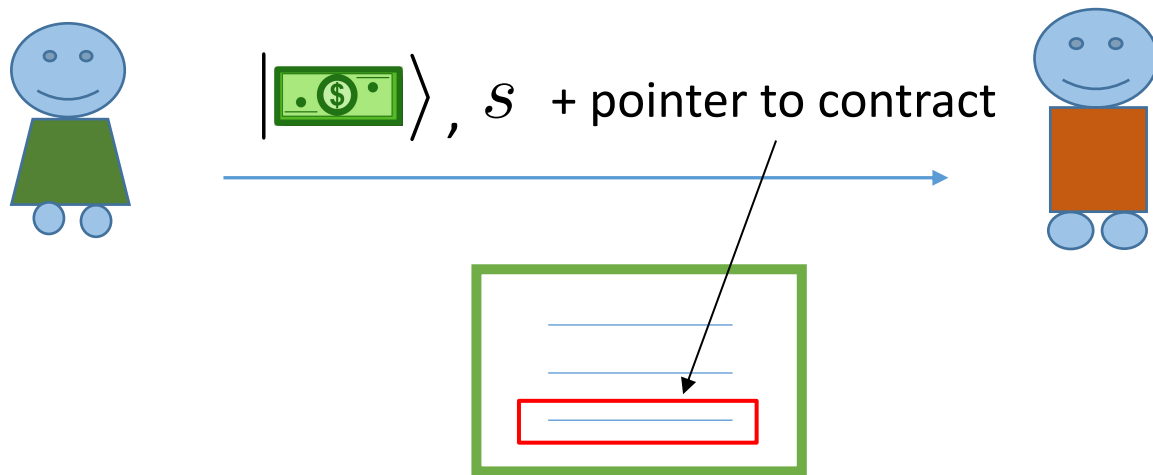
Coins deposited: k

• • •

Interpret this as the quantum banknote having “acquired” value k .

Payments

- After s has been recorded in a “quantum banknote” contract, Alice can spend the quantum state to Bob:



“Value” of banknote determined by number of coins deposited in contract

- Alice sends the banknote state and serial number to Bob, and references the “quantum banknote” contract containing s .
- Bob checks validity of contract. And checks that
$$\text{Ver} \left(|\text{banknote}\rangle, s \right)$$
 returns “accept”.

Payments

What is the point?

Bob can later spend the banknote to Charlie, Charlie can spend it to Dana, etc.. **without** any new transaction posted on the blockchain.

Crucially, **the blockchain is updated only when the banknote is created.**
All subsequent transactions happen “off-chain”.

1. Mechanism to generate quantum banknotes:

Classical coins \longrightarrow Quantum banknotes

2. Mechanism to go back.

Quantum banknotes \longrightarrow Classical coins

For this, we formalize a natural property of Quantum Lightning schemes, which we call ***banknote-to-certificate*** property.

Banknote-to-certificate property

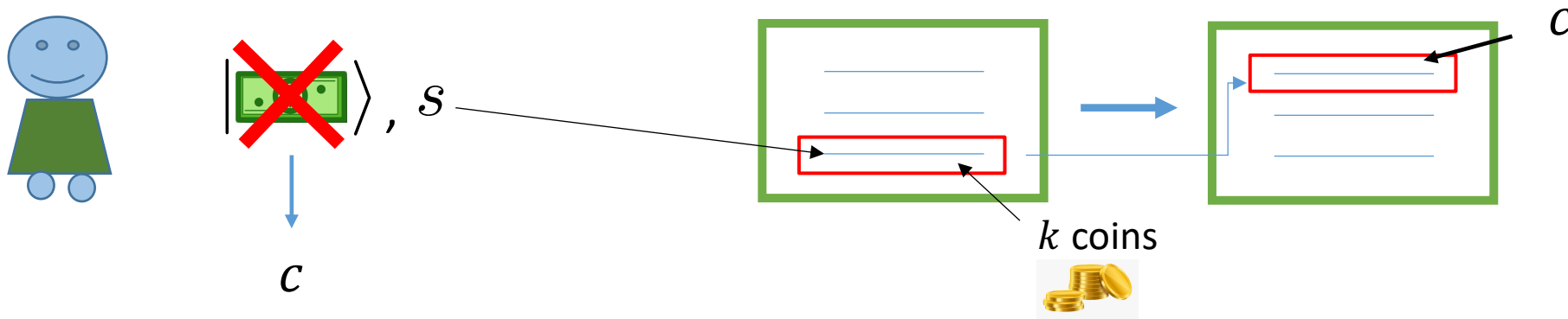
Recall from our quantum lightning sketch: $|\text{banknote}\rangle = \sum_{x:H(x)=y} |x\rangle$

Notice: measuring allows to recover one pre-image. However, this destroys the superposition. It's hard to possess both a valid pre-image and a valid banknote.

Informal definition: A quantum lightning scheme satisfies the **banknote-to-certificate** property, if there is an efficient procedure that extracts a **classical certificate** from a valid banknote.

- The certificate is **efficiently verifiable** given s .
- It is **hard to hold both a valid certificate and a valid banknote** with respect to the same serial number.

2. Quantum Banknotes back to Classical Coins



- The “quantum banknote” contract specifies that **anyone who posts a valid certificate** with respect to s **can recover the deposited coins**.
- Alice posts c to the blockchain to recover the coins in the contract.

Practical considerations

- In an idealized model in which transactions appear on the blockchain in the order that they are submitted by users, we can prove formal security.
- In practice, **a malicious agent could delay certain messages and favor others.**
- Possible attack: wait for a legitimate user to broadcast a valid certificate. “Steal” it and post to the blockchain first.

A resolution: banknote-to-signature property

Banknote-to-certificate:



$$|\text{~~banknote~~\rangle}, s \longrightarrow c$$



Banknote-to-signature:



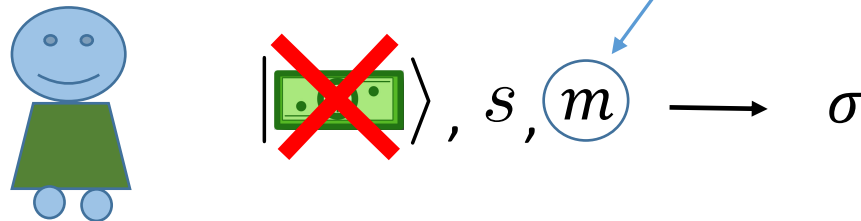
$$|\text{~~banknote~~\rangle}, s, (m) \longrightarrow \sigma$$

A resolution: banknote-to-signature property

- Alice does not broadcast her certificate in the clear. Instead she uses the banknote-to-signature property:

She signs with respect to s the message:

“Alice wishes to convert the banknote back to coins”.



Brief comparison to classical alternatives

- There are some proposed classical solutions, based on the idea of transactions happening “off-chain”:

Lightning Network of Bitcoin, and **Raiden Network** of Ethereum.

- Pros: They don't require quantum technologies.
- Cons: Payments still involve many parties (and hence transaction fees), and some other practical constraints.

Final disclaimer: We don't currently know of a quantum lightning construction secure under standard assumptions!

THANK YOU!