Sybatcoin

Sybatcoin: A next generation quantum powered trust authority for the quantum web.

AntimonyIQ

antimonyiq@gmail.com

www.sybat.network

Abstract

The prevailing model of quantum computation describes the computation in terms of a network of quantum logic gates. Entanglement is an intrinsically quantum effect that involves nonclassical correlations, usually between spatially separated quantum systems. This phenomenon was described by Einstein as "spooky action at a distance", and yet it forms the basis of nearly all quantum information platforms, such as quantum computers and quantum networks. In particular, quantum networks distribute quantum information between any two nodes on the network. This allows the distributed system to carry out valuable tasks such as quantum key distribution (QKD), which guarantees secure communication through the laws of physics. Significant progress is currently being made towards the creation of a global quantum network, and it is becoming an increasing priority to find further applications that can be built on such a platform.

A more desirable solution would be an intrinsically quantum blockchain, which is constructed out of quantum information, and whose design is fully integrated into a quantum network. This would provide the benefit of a QKD layer as well other potential quantum advantages over a classical blockchain.

Classical Blockchain: The classical blockchain is composed of a blockchain data structure and a network consensus protocol; the former is the database, while the latter provides the decentralization feature. The aim of a blockchain is to have a single database of records about the past that every node in the network can agree on. Furthermore, it should not require a centralized management node.

Table of Contents

Introduction

Scientist around the world are working on a quantum internet to communicate by teleportation and data storage through photons. This may sound like a sci-fi concept, but building quantum networks is key ambition for many countries around the world. At least in a very preliminary form, The US department of Defense (DoE) published the first blueprint of its kind.

The quantum internet is a network that will let quantum devices exchange some information within an environment that harnesses the laws of quantum mechanics. In theory, this would lend the quantum internet unprecedented capabilities that are impossible to carry out with today's web applications.

In the quantum world, data can be encoded in the state of qubits, which can be created in quantum devices like quantum computer or quantum processors. And the quantum internet in simple terms, will involve sending qubits across a network of multiple quantum devices that are physically separated. All of this would happen using the properties of quantum states.

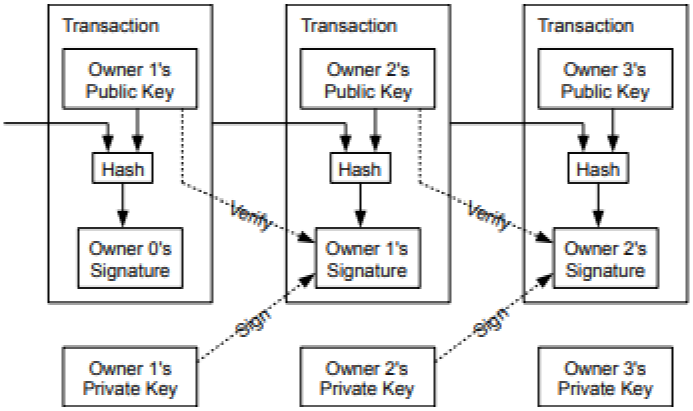
That might sound similar to the standard internet. But sending qubits around through a quantum channel, rather than a classical one, effectively means leveraging the behavior of particles when taken at their smallest scale so-called "quantum states", which have caused delight and dismay among scientists for decades.

And the laws of quantum physics, which underpin the way information will be transmitted in the quantum internet, are nothing short of unfamiliar. In fact, they are strange, counter-intuitive, and at times even seemingly supernatural.

And so, to understand how the quantum ecosystem of the internet 2.0 works, you might want to forget everything you know about classical computing. Because not much of the quantum internet will remind you of your favorite web browser.

Transactions

According to the Bitcoin definition of electronic cash system, electronic coin as a chain of digital signatures each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.



Unlike the classical process of transaction validation process the quantum electronic coin transaction system is no different, regardless a quantum transaction process follows the quantum coin flipping.

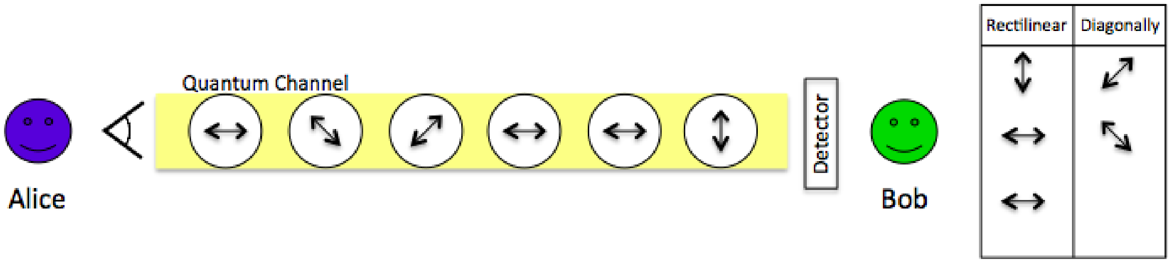
Quantum coin flipping is when random qubits are generated between two participants in which there is no trust, to establish a trusted transaction. The essence of coin flipping occurs when the two transacting participants issue a sequence of instructions (receiver's public key, transacting owner public and private key) over a communication channel that then eventually results in an output.

A basic quantum coin flipping protocol involves two people: Alice and Bob.

Alice sends Bob a set number of **K** photon pulses in the quantum states. Each of these photon pulses is independently prepared following a random choice by Alice of basis α_i and bit c_i where i = 1, 2, 3...K.

Bob then measures the pulses from Alice by identifying a random basis β_i. Bob records these photons and then reports back the first successfully measured photon j to Alice along with a random bit *b*.

Alice reveals the basis and bit that she used at the basis Bob gave her. If the two bases and bits match, then both parties are truthful and can exchange information. If the bit reported by Bob is different than that of Alice's, one is not being a trust participant.



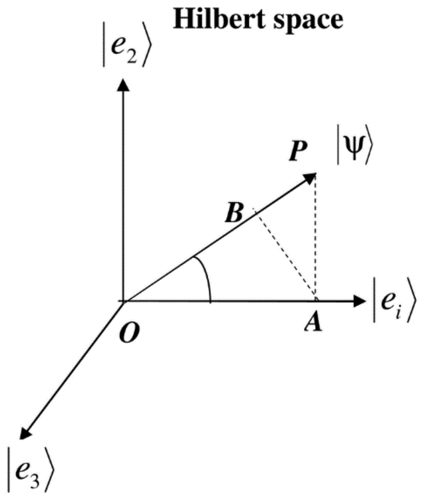
The key issue with coin flipping is that it occurs between two parties with zero trust. These two participating transacting parties are communicating through the communication channel some distance from each other and under a transaction agreement. Since they are individually unknown to one another cheating can occur. In a situation illustrated in the above image, where Alice is the sender and Bob is the receiver of a particular transaction.

For Bob to cheat, he would have to be able to guess Alice's basis with a probability greater than ½. On the other hand, for Alice to cheat, Alice could also send Bob a different original sequence than she actually used in order to beat Bob. The only way to confirm the absence of a transaction is to be aware of all transactions. To accomplish this without a trusted party, transactions must be publicly announced, and we need a system for participants to agree on a single history of the order in which they were received. The payee needs proof that at the time of each transaction and no Third party.

Single photons are used to pass the information from one player to the other (qubits). In this protocol, the information is encoded in the single photons with polarization directions of 0, 45, 90, and 135 degrees, non-orthogonal quantum states. When a third party attempts to read or gain information on the transmission, they alter the photon's polarization in a random way that is likely detected by the two players because it does not match the pattern exchanged between the two legitimate users.

Quantum States

In the science quantum physics, a quantum state is a mathematical entity that provides a probability distribution for the outcomes of each possible measurement on a system. Knowledge of the quantum state together with the rules for the system's evolution in time exhausts all that can be predicted about the system's behavior. A mixture of quantum states is again a quantum state. Quantum states that cannot be written as a mixture of other states are called pure quantum states, while all other states are called mixed quantum states. A pure quantum state can be represented by a ray in a Hilbert space over the complex numbers, while mixed states are represented by density matrices, which are positive semidefinite operators that act on Hilbert spaces.



A pure state here is represented by a two-dimensional complex vector (α, β), with a length of one; that is, with

$$|\alpha|^2 + |\beta|^2 = 1$$

Sybatcoin uses a more complicated case is given (in bra–ket notation) by the singlet state, which exemplifies quantum entanglement:

$$|\psi\rangle = \frac{1}{\sqrt{2}}\big(|\uparrow\downarrow\rangle - |\downarrow\uparrow\rangle\big),$$

Quantum Proof-of-State

A Quantum Proof-of-State (QPoS) protocols are a class of consensus mechanisms for quantum blockchains that work by selecting validators in proportion to validate each singlet state. In a peer-to-peer basis of electronic cash system in quantum state naturally existing in a superposition a singleton transaction is validated by trust third party validator which controls the quantum machine used to carry out the state process.

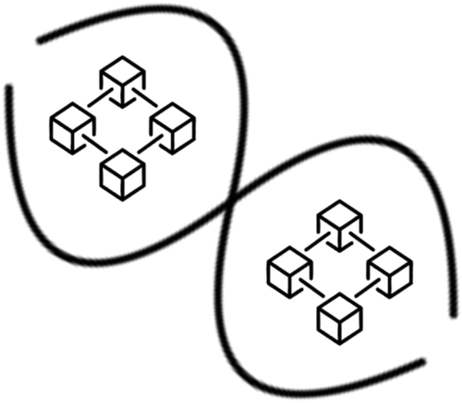
The Proof of State involves scanning for a value that when hashed, and processed through quantum channels the hash begins the resulting computed qubit states returns with a number of zero bits. The average state required is exponential in the number of zero bits required and can be verified by executing a single hash.

Quantum Network

Quantum networks facilitate the transmission of information in the form of quantum bits, also called qubits, between physically separated quantum processors. A quantum processor is a small quantum computer being able to perform quantum logic gates on a certain number of qubits. This pushes the ability to write quantum-based technologies like, Computation, Communication, Etc.

The steps to run the network are as follows:

1) New transactions are broadcast to all Quantum Channels
2) Each Quantum Channels collects new transactions into a block.
3) Each block is validated and collected into a cluster (Quantum Wave).
4) Each channel works on finding a state using quantum Proof-of-State for its block.
5) When a Quantum Channel finds a Proof-of-State, it broadcasts the State to all Cluster.
6) Clusters accept the block only if all transactions in it are valid and not already spent.
7) Quantum Channels express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.



A simple Quantum Blockchain Cluster

Applications

Stateless quantum Blockchain would be applied into the following fields of quantum mechanics:

- Digital Electronic currency for the quantum Internet
- Mapping and Position Identification
- Secure Identification systems (SIS)
- Secure access to a quantum computer