K-Chains: A New Class of Blockchains and Related Turing Machines Based on Quantum Mechanics

Hegadekatti, Kartik

13 January 2017

K-CHAINS: A NEW CLASS OF BLOCKCHAINS AND RELATED TURING MACHINES BASED ON QUANTUM MECHANICS

Dr.Kartik H

Author's email: dr.kartik.h@gmail.com

ABSTRACT

Quantum Mechanical principles have brought about a revolution in the way we perceive our world and use technology. One of the possible impacts and usage of Quantum mechanics is in the field of economics. Quantum mechanics can be applied to build a new class of Blockchain systems. This paper explores that possibility. It deals with how Quantum Mechanics can be best implemented to bring into existence a new class of Blockchain systems. These Quantum Blockchains (called K-Chains) will have several advantages like possible Faster-Than-Light (FTL) communication of Transactions, Unlimited network capacity and the revolutionary prospect of an Off-line Blockchain which will not need to be connected to the internet for transactions to occur. Extrapolation of this likelihood can lead to the designing of Quantum Turing Machines which are based on Quantum Blockchain (K-Chain) Technology. Real time information and communication systems spanning distances across light-years will most likely be probable. This can allow Mankind to instantly exchange value and information across vast distances of space almost instantly.

The paper starts by briefly explaining the basics of Blockchains, cryptocurrencies and relevant Quantum mechanical concepts. Then

we discuss how Quantum mechanics can be amalgamated with Blockchain Technology to achieve K-Chains. Later we delve into the various impediments that make achieving a Quantum Blockchain (K-Chain) difficult with present day hardware technology. The paper concludes by discussing the various aspects of Quantum Technology, Blockchain Systems and the possibilities of constructing Blockchain based Quantum Turing Machines.

INTRODUCTION

A cryptocurrency is a medium of exchange using cryptographic techniques to safeguard transactions and also manage the formation of additional units of the currency.

A Blockchain is a widely disseminated archive of data that maintains a continually-expanding register of records fully and reliably protected from any alteration or modification. Each block has a timestamp and link to the preceding block.

A Crypto wallet is an encrypted electronic device that allows an individual to make electronic cryptocurrency transactions. Each wallet will have a public key visible to anyone. But it can be operated by only a person who has a private key. Transactions on the cryptocoin network are usually anonymous.

When people send cryptocoins to each other, someone has to keep account of who spent how much at what time. In case of fiat money (or paper money) it is done by banks (known as Trusted Third Parties, for which they charge a commission).But in case of Cryptocoins, it is registered on a ledger called Blockchain (with nil or minimal fees).

The cryptocoin network makes this possible by detailing all the transactions made during a certain timeframe into a list. This list is known as a block. A certain set of people called 'miners' verify these transactions mathematically and register them on the Blockchain. Those bona-fide miners who have successfully verified the transactions are paid freshly created Cryptocoins. This is how miners are rewarded, and new cryptocoins are generated. This is also the reason why no transaction costs are levied, as the network (in the form of miners) verifies the transactions.

Bitcoin is a peer-to-peer based cryptocoin which is not backed by any commodity and (unlike fiat money) carries no sovereign guarantee whatsoever.

Regulated and Sovereign Backed Cryptocurrencies (RSBC), on the other hand are government backed cryptocurrency akin to paper currency, but in digital form. In this system, the cryptocoins (known as NationCoins) are backed by Sovereign Guarantee.

They are run on a highly secure Controlled BlockChain (CBC) [1] in which Sovereign backed Cryptocurrencies will be transacted without any hassles. NationCoins are completely managed by the Sovereign Authority i.e the Government.

This system is based on the K-Y Protocol [2]. The K-Y Protocol is a set of rules and instructions to implement the Regulated and Sovereign Backed Cryptocurrency (RSBC) system.

Double-spending is the process of successfully spending the same money more than once.

A 51% attack indicates an attack on a blockchain – usually on bitcoin's blockchain, by a group of miners controlling more than 50% of the network's mining capacity, or computing power.

The attackers can then prevent new transactions from being confirmed, permitting them to stop payments between all or some users. They can also undo transactions that take place while they are in control of the network, implying that they can double-spend coins.

It is more difficult to conduct a 51% attack on a Controlled Blockchain (like RSBC) compared to an unregulated one (like Bitcoin's).

Quantum superposition is a fundamental principle of quantum mechanics. It states that, much like waves in classical physics, any two (or more) quantum states can be added together ("superposed") and the result will be another valid quantum state; and conversely, that every quantum state can be represented as a sum of two or more other distinct states.

Quantum entanglement [3] is a Quantum mechanical physical phenomenon. It takes place when pairs or groups of particles are created or interact in a manner such that the quantum state of each particle cannot be explained independently of the others, even when the particles are separated by large distances. Alternatively, a quantum state must be defined for the system as a whole.

Quantum Decoherence[4] is the loss of quantum coherence. Particles (e.g.-electrons) behave like waves and are defined by a

wave function. These waves can interact, leading to the 'strange' behaviour of quantum particles. As long as there is definite phase relation between different states, the system is said to be coherent.

This coherence is essential for the function of quantum computers. But if a quantum system is not totally isolated, the coherence decays with time through quantum decoherence resulting in loss of quantum behaviour

In quantum information theory, superdense coding [5] [6] is a technique used to send two bits of classical information using only one Qubit.

Quantum teleportation [7] is a process by which quantum information (i.e the precise state of an electron or photon) can be communicated (exactly, in principle) from one location to another, with the help of classical communication and formerly shared quantum entanglement between the receiving and sending location.

A quantum Turing machine (QTM) [8], also known as a universal quantum computer, is an abstract device which can be used to simulate the effects of a quantum computer. It offers a simplistic explanation which summarizes all of the power of quantum computation. Any quantum algorithm can be expressed as a quantum Turing machine.

Electron Spin: An electron spin is an intrinsic property of electrons. Spin "up" and "down" permits two electrons for each set of spatial quantum numbers. Electrons have intrinsic angular momentum characterized by a quantum number i.e 1/2. Spin is an intrinsic

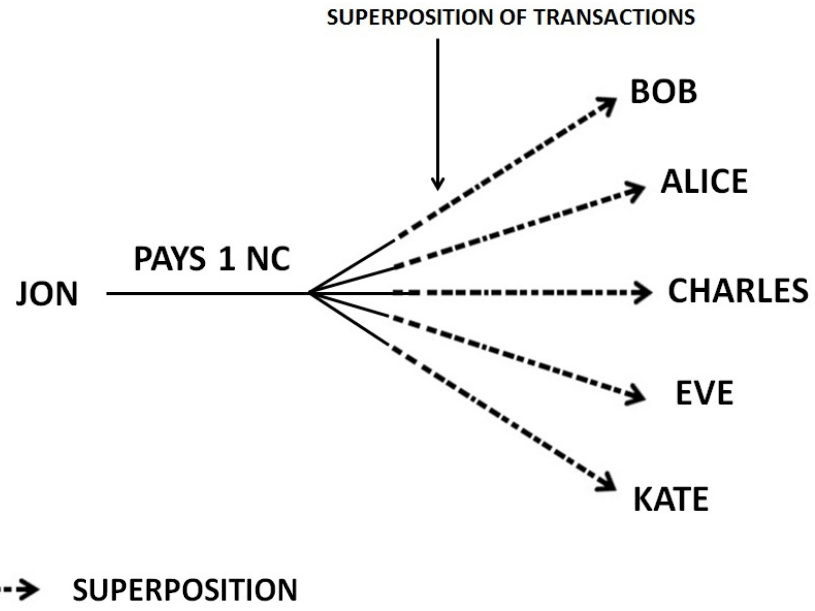
property of a Quantum particle which can be used for representational and computational purposes (it is similar to Switch 'on' or 'off' property used to represent classical binary bits.)

Jon, Bob, Alice, Eve, Kate, Charles, and Harry are 7 people who use a Quantum (Kuantum) Blockchain (or K-Chain).

Jon can pay Bob and attempt to Double-spend the same money with Alice or Kate. To overcome this problem, current Blockchain technology i.e. Classical Blockchain technology uses a process called 'Broadcasting' where the act of Jon paying Bob is announced to all the 'Nodes' on the network. This way, the network ensures that Joe cannot pay the same money twice (or thrice) to Alice or Kate. In case he does, only one transaction is validated and all other transactions (with the same money) are invalidated.

Let us examine how the problem of Double-spending is overcome on a K-Chain.

Jon Attempts to pay one NationCoin to Bob. At the Same time, he tries to transact the same money to Alice, Eve,Charles and Kate. (One Important feature of a K-Chain is that it will allow only one transaction at a time to and from only one device). But because the K-Chain Protocol will be based on Quantum Principles the following will happen-



1) Transactions to all the wallets will take place simultaneously.

2) All transactions will be in a superposition of states i.e. all transactions will have occurred and yet not have occurred at the same time.

3) When the transactions are to be made part of the K-Chain (Quantum Blockchain), only one transaction will have occurred, the others being 'automatically invalidated'. Simply put, the superposition of transactions will 'collapse' into one valid transaction.

4) Thus the transaction that actually goes through can be deemed to have been 'automatically verified'.

5) Because there is a Risk that Jon's payment might go to any of the five people (if he tries to Double-spend or Multi-spend) and the probability of it going to Bob will be 1/5 i.e. 20%. If there are a Billion wallets, probability of the Money actually ending up with Bob will be 10^{-9}. Therefore, if Jon tries to Double-spend, he will be 'Penalised' as he will most probably lose his money and also fail to

pay Bob (Which Bob will later try to collect from Jon). Thus, there is an inherent penalty if Jon tries to Double-spend.

How K-Chain Transactions can be achieved?

K-Chains can be attained by using 2 different (yet opposing) principles of Quantum Mechanics. One is by Superdense Coding and the other is through Quantum Teleportation.

K-Chains By Supersense Coding

Each of the Seven persons mentioned above will have a K-Device (*Kuantum* Device) which is a hypothetical device enabling transactions on the K-Chain.

Each device will have 4 Registers. A register is a set of Qubit Cohorts performing a specific function, primary among them, as indicators of transactions.

Cohort: Several Electrons (Qubits) will be brought into a state of entanglement. We categorize these electrons into sets called Cohorts. If there is a Cohort A, all electrons belonging to a cohort will be found in every K-Device in the universe.

Similarly there will be Cohorts like B, C, D, E etc.

Electrons of Cohort A will be A_1, A_2, A_3, A_4 etc.

Electrons of Cohort B will be B_1, B_2, B_3, B_4 etc.

Electrons A_1, A_2, A_3, A_4 are entangled. Similarly Electrons B_1, B_2, B_3, B_4 are entangled. No two electrons from different cohorts are entangled. Only electrons from the same cohort are entangled i.e A_1 and B_1 are NOT entangled A_1 and A_2 are entangled.

Imagine there are 3 Qubits (made of 3 Electrons each) in each Register (number of Qubits in each register can vary. In this example we will take 3 Qubits). Up-spin is taken as 1 and Down-Spin is taken as Zero. As such each Qubit can either be 1 or 0 or a Superposition of Both. 3 Qubits can represent a total of 2^3=8 entities. If we take Spin of electrons to be representational then 'up' indicates '1' and 'down' indicates '0'

Let the people mentioned above have following representations:

Jon: 101 [Qubit- up, down, up]

Bob: 111 [Qubit- up, up, up]

Alice: 011 [Qubit- down, up, up]

Eve: 010 [Qubit- down, up, down]

Kate: 110 [Qubit- up, up, down]

Charles: 001 [Qubit- down, down, up]

Harry: 100 [Qubit- up, down, down]

K-Chain Network: 000 [Qubit- down, down, down]

The K-Chain Network is represented by the Register 000

7 Units of NationCoins can be transacted using a 3 Qubit register (Zero NationCoins cannot be transacted- see further; it is a rule of the K-Chain Protocol)

NationCoins	Representation
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

Each K-Device will have at least 4 Registers.

Jon's K-Device Address: 101

Bob's K-Device Address: 111

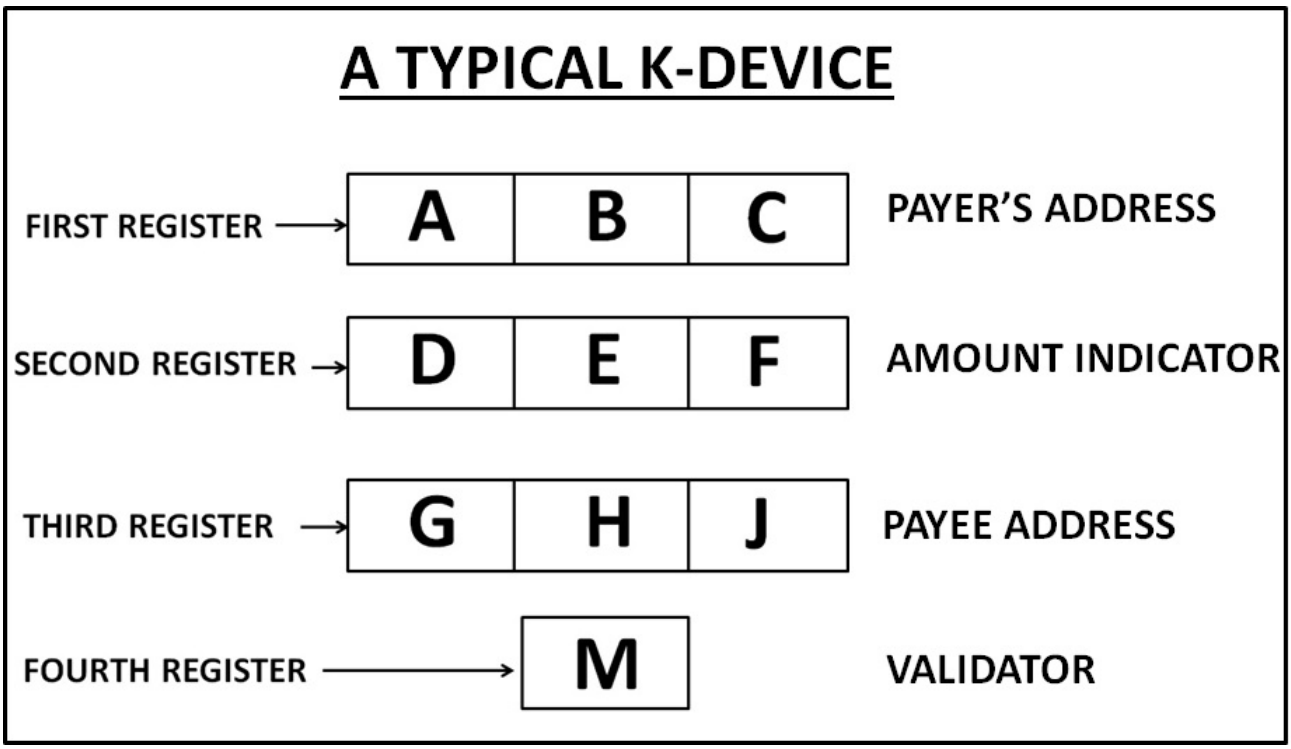
1 NationCoin(NC): 001

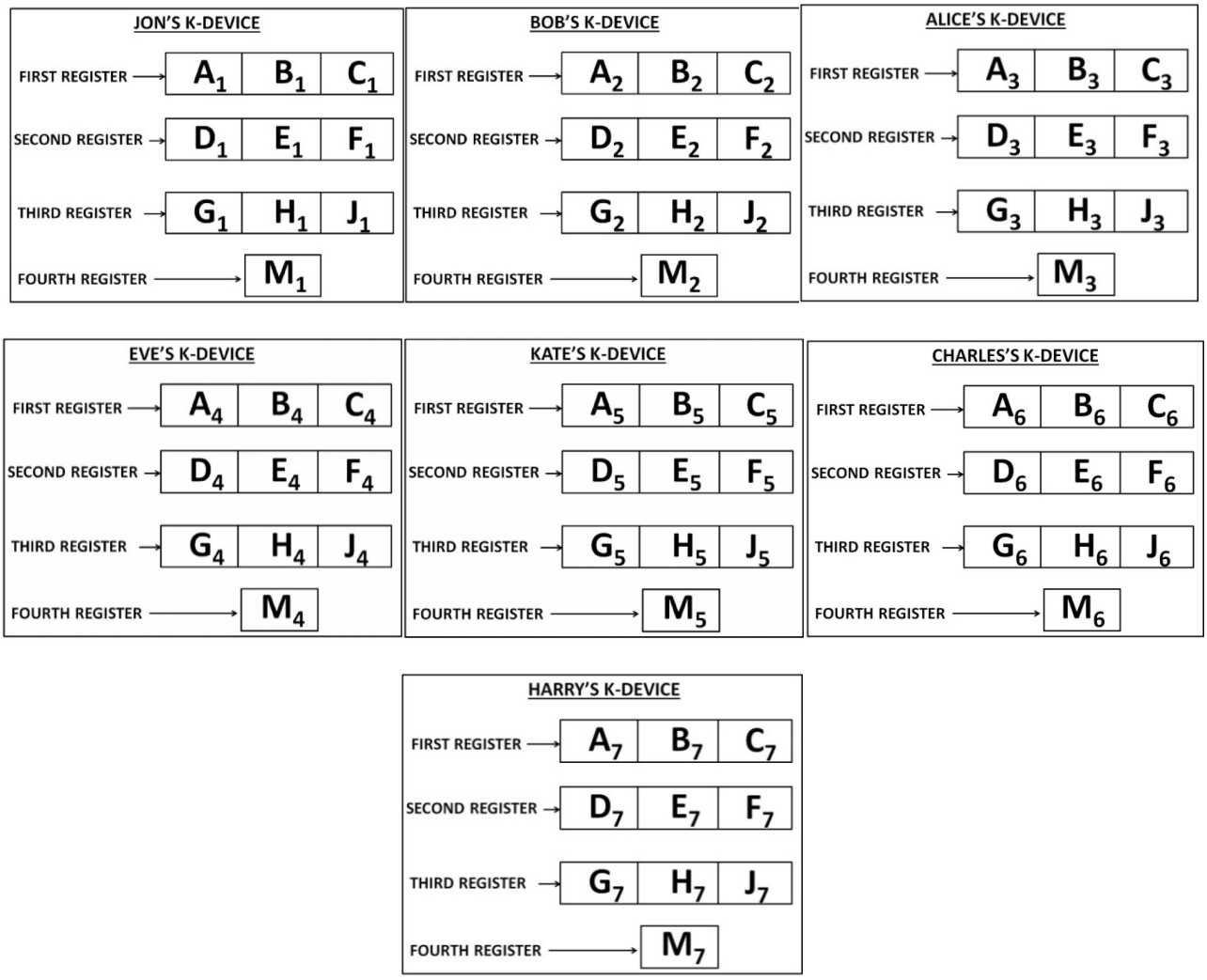
"Jon pays Bob 1 NationCoin" is indicated in the K-Device as

First Register -Jon's Address : 101

Second Register- Amount Indicator (1 NC): 001

Third Register- Bob's Address: 111


A TYPICAL K-DEVICE
FIRST REGISTER
A
B
C
PAYER'S ADDRESS
SECOND REGISTER
D
E
F
AMOUNT INDICATOR
THIRD REGISTER
G
H
J
PAYEE ADDRESS
FOURTH REGISTER
M
VALIDATOR


JON'S K-DEVICE
FIRST REGISTER A_1 B_1 C_1
SECOND REGISTER D_1 E_1 F_1
THIRD REGISTER G_1 H_1 J_1
FOURTH REGISTER M_1
BOB'S K-DEVICE
FIRST REGISTER A_2 B_2 C_2
SECOND REGISTER D_2 E_2 F_2
THIRD REGISTER G_2 H_2 J_2
FOURTH REGISTER M_2
ALICE'S K-DEVICE
FIRST REGISTER A_3 B_3 C_3
SECOND REGISTER D_3 E_3 F_3
THIRD REGISTER G_3 H_3 J_3
FOURTH REGISTER M_3
EVE'S K-DEVICE
FIRST REGISTER A_4 B_4 C_4
SECOND REGISTER D_4 E_4 F_4
THIRD REGISTER G_4 H_4 J_4
FOURTH REGISTER M_4
KATE'S K-DEVICE
FIRST REGISTER A_5 B_5 C_5
SECOND REGISTER D_5 E_5 F_5
THIRD REGISTER G_5 H_5 J_5
FOURTH REGISTER M_5
CHARLES'S K-DEVICE
FIRST REGISTER A_6 B_6 C_6
SECOND REGISTER D_6 E_6 F_6
THIRD REGISTER G_6 H_6 J_6
FOURTH REGISTER M_6
HARRY'S K-DEVICE
FIRST REGISTER A_7 B_7 C_7
SECOND REGISTER D_7 E_7 F_7
THIRD REGISTER G_7 H_7 J_7
FOURTH REGISTER M_7

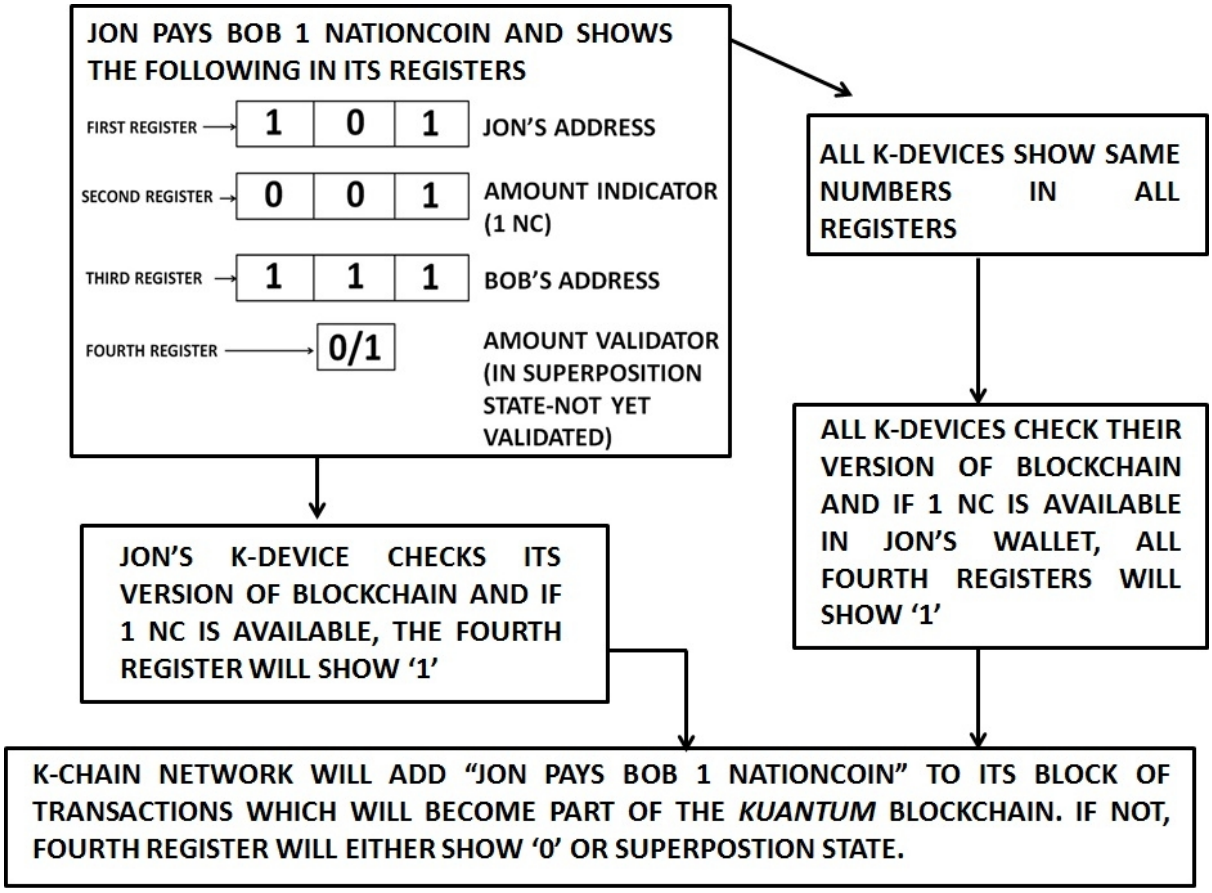
Now, the K-Chain Protocol will immediately verify (by checking the Blockchain) whether Jon actually has the amount that he intends to pay Bob. Once it is verified, the Fourth Register will show 1 (up) if Yes or 0 (down) [and in superposition state] if no.

All electrons in their respective cohorts will align as shown above in all such K-Devices in the universe. Alice's K-Device will alert her that "Jon Pays Bob 1 NationCoin"

In case Jon tries to tamper with the Qubit cohort of the Fourth Register (i.e. he attempts to pay Bob in spite of not having 1 NC), then the Qubits (electrons in this case) will be in a state of superposition (due to entanglement) in all such K-Devices in the universe, essentially invalidating the transaction. (Only the quantum state '1' of the Fourth Register can validate that Jon (or any person) has the requisite amount to pay in his/her wallet.

Because all the electrons in a particular cohort are in entangled state, all such K-Devices in the universe will show the exact same indicators in all the registers all the time.

Once the Fourth Registry of all devices shows '1', then The K-Chain Network will add "Jon Pays Bob 1 NationCoin" to its Block of transactions which will become part of the *Kuantum* Blockchain.



Total number of Cohorts (all registers combined) needed, C

C= n+m+1

Where,

$$n = \frac{\log x}{\log 2} - 1$$

$$m = \frac{\log y}{\log 2}$$

x= Total number of intended wallets

y= Maximum desired units of currency intended to be transferred from each wallet in one transaction

If total number of intended wallets is 1 trillion and the maximum amount of money in each transaction per wallet is 1 trillion NationCoins, then

Total number of Cohorts needed (C) = n+m+1

n=39; m=40

C=39+40+1=80

Only 80 Qubits can provide for transactions up to 1 Trillion units of currency per wallet per transaction; for a trillion wallets.

Some Salient features of K-Chain Protocol:

1) It will never allow a transaction in which the amount of money is zero. This is necessary so as to eliminate possibilities of spam transactions.

2) A transaction will be a part of the K-Block (Kuantum Block) only if the Fourth Register indicates a definitive '1'.

3) Continued superposition of Qubits in the Fourth Register in spite of stabling (or 'Collapse') of other Cohorts in the first, second and third registers will invalidate the transaction.

4) It will allow only one transaction at a time per device.

5) It will allow for queuing of transactions in the K-Device.

Some important differences between Classical Blockchains

(C-Chains) and *Kuantum* Blockchains (K-Chains)

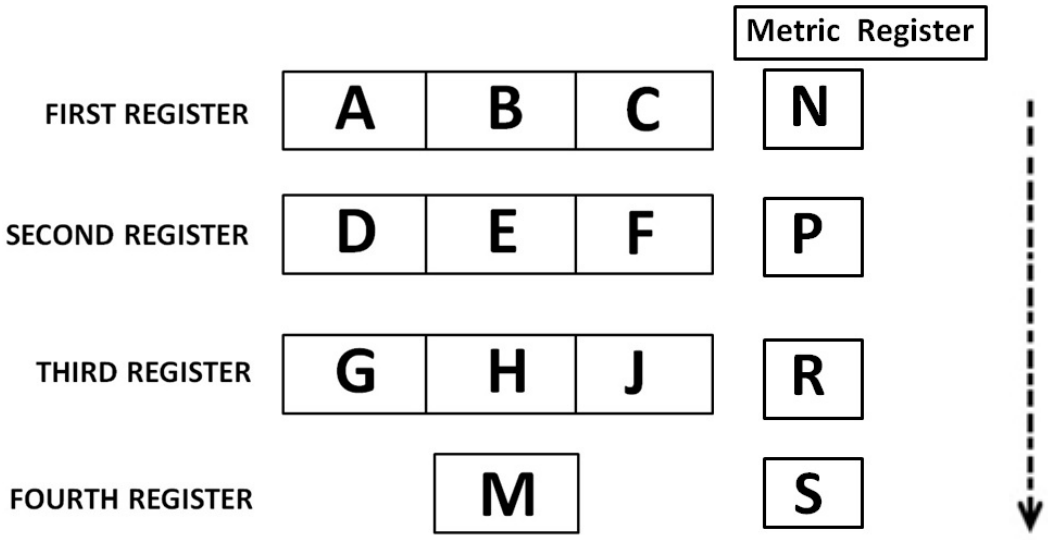
CLASSICAL BLOCKCHAIN (C-Chain)	***KUANTUM* BLOCKCHAIN** (K-Chain)
1) Uses solid-state electronic principles i.e bits for functioning.	Uses Quantum Mechanical principles i.e Qubits for functioning.
2) Broadcasting is needed to prevent Double-Spending.	2) No Broadcasting is necessary; Quantum entanglement ensures that 'Broadcasting' is automatic.
3) Double-spend and 51% Attack can occur.	3) 100% consensus. Double-spend is impossible.
4) There is a finite Block confirmation time.	4) Block confirmation time is essentially Zero due to 'Zero Time Consensus.
5) One Needs to be connected to the internet to conduct transactions.	5) Offline transactions are possible. Internet is not required.
6) Classical encryption is used.	6) Quantum encryption is used.
7) Network capacity is limited; block confirmation time being the primary restraint.	7) Theoretically unlimited Network capacity which is fully secure.

We see that due to quantum entanglement consensus is achieved at faster-than- light speed (in Zero Time) without verification. Thus, Block verification time is cut down to zero and the transactions are immediately updated. This is called "Zero Time Consensus".

REALIZING K-CHAIN TRANSACTIONS THROUGH QUANTUM TELEPORTATION

We can transact on a Blockchain using Quantum Teleportation technique. In this method, two (or many) entangled electrons (or Qubits) are used to measure the state of other non-entangled electrons thus transferring Qubits from one place to another.

The K-Device in Quantum Teleportation technique is slightly different from the one using Superdense coding technique. It contains an extra register called 'Metric Register'. The K-Device in Quantum Teleportation technique appears as follows.

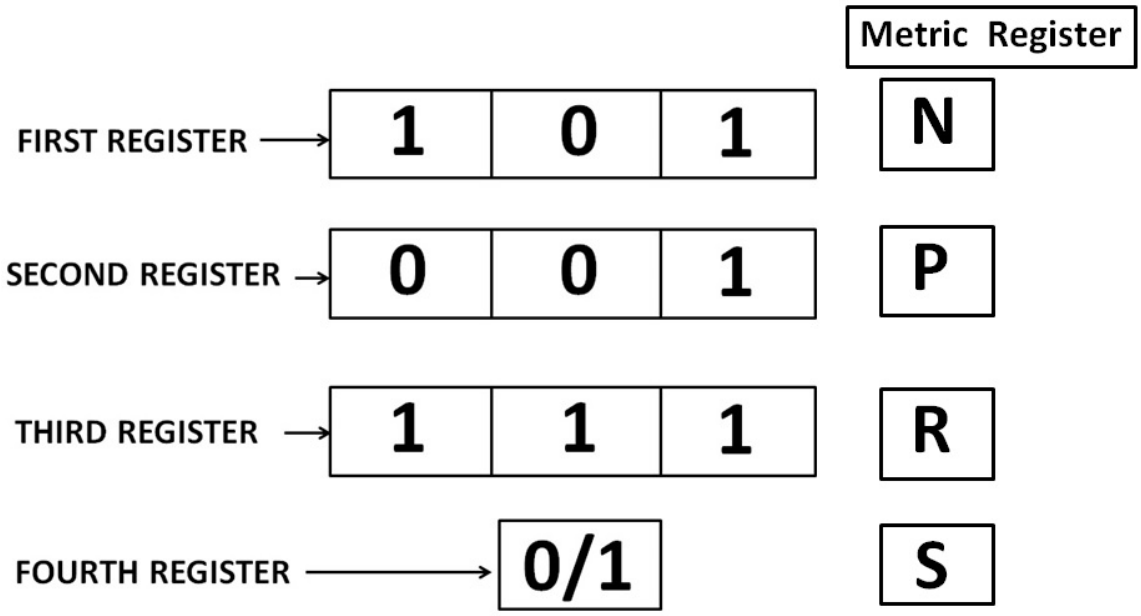


The other 4 Registers are Horizontal Registers, i.e each value in a register represents a transactional entity. A Metric register unlike the 4 registers is a vertical register (Cohorts N, P, R, S are components of the Metric Register). Cohorts in a Metric register are there only for measurement purposes. It means that each row in a Metric register corresponds to an entire row of horizontal registers. I.e. N corresponds to first register; P corresponds to second register and so on.

Moreover, each cohort in a Metric register contains many entangled electrons (usually in numbers proportionate to the number of un-entangled electrons in the horizontal registers whose quantum state is to be measured).

All electrons belonging to cohorts in a Metric register are entangled. Electrons in the 4 registers may or may not be entangled.

The transaction- "Jon pays Bob 1 NationCoin" is coded as -



Now, the measurement of the full first row i.e the first register plus Cohort N is taken, second register plus cohort P is taken and so on.

This information is transferred through classical communication channels using Bits. Whichever K-Device reads this information will decode and output the following as per the principles of Quantum Teleportation [9]-

"Jon pays Bob 1 NationCoin"

The transaction needs no verification. On reaching consensus, it is added to the K-Chain in the same process as explained above. Only difference is that the K-Chain will be a classical blockchain using Quantum principles.

There are some important differences regarding transactions with respect to Superdense Coding and Quantum Teleportation:

K-Chains Based on Superdense Coding	**K-Chains Based on Quantum Teleportation**
1) All Qubits in the 4 Registers (horizontal Registers) must be in entangled state.	1) All Qubits in the 4 Registers (horizontal Registers) may or may not be in entangled state.
2) No Metric registers are needed.	2) Metric registers are a must. This is the single most important differentiating feature.
3) Faster-Than-Light communication takes place as only Qubits are used to transfer information.	3) Information is transmitted through classical channels using Classical Bits.
4)Not necessary to be connected to the Internet (offline blockchain)	4)Internet connection is necessary (online Blockchain)
5) Truly Quantum Blockchain. Fully Quantum in nature.	5) It is a classical Blockchain using Quantum principles. Essentially electronic in nature.
6) Almost instantaneous 'Blocking' (i.e addition to a Block) of transaction.	6) Transaction 'Blocking' is constrained due to the usage of classical bits to transfer information through electronic channels.

The various advantages of K-Chain are as follows:

1) Zero Time Consensus (ZTC). The concept of ZTC theoretically allows for infinite transactions to take place in no time. In reality it will be possible to conduct very large number of real-time transactions in very short time frames across very large distances (possibly light-year distances) in the near future. It will be much faster than the fastest blockchains today.

2) There is no need for verification of transactions. The only thing that needs verification is the amount of money in a wallet (Does Jon have 1 NationCoin in his wallet?). This will be encoded in the K-Chain Protocol where the K-Device itself will validate the amount of money in the wallet.

3) No need for 'Broadcasting' as Double-spending cannot occur (Due to 'collapse' of the Superposition state.)

4) Very high security of wallets due to Quantum encryption.

5) No need for the internet as entanglement ensures instant communication. Essentially, this provides for an offline cryptocurrency, without the need for internet or Wi-Fi. If there comes a time when the Internet fails due to a lack of power (or other reasons), K-Chains can ensure that transactions can still occur.

6) Quantum Teleportation will not only ensure instant communication with Extra-Terrestrial settlements, but will also ensure unified Blockchains enabling instant transactions across vast distances of space.

7) Scalability: 3 cohorts of Qubits can allow for transactions between 7 entities. 35 cohorts can allow for transactions between a trillion entities (people or Devices). Thus, a few Qubits can ensure exponential scalability at a reasonable cost.

IMPEDIMENTS IN REALIZING K-CHAINS AT PRESENT

1) Decoherence- Presently decoherence times are extremely short (in milliseconds). For K-Chains, we need to have decoherence times ranging from a few months to many years.

2) Qubits- Quantum computation is still evolving. We need to choose our Qubits based on the most reliable function vis-a-vis transaction verification and decoherence time.

3) Presently, the hardware for such systems, if built, will be very bulky. Over a period of time we might be able to miniaturize a possible K-Device to the size of a smartphone.

CONCLUSION

We have seen that K-Chain systems provide many advantages like:

1) Instant verification due to Zero Time Consensus. Users need not wait for 'Block Confirmation Time', the bane of Classical Blockchains.

2) Possibilities for an offline Blockchain. In fact by using K-Chains, the whole internet can be brought "offline" where networked communication need not depend on electronic devices and being connected to the network. This provides for very fast, off-line transactions to be conducted in a secure manner.

3) Unlimited Network capacity.

However there are some technological impediments like-

1) Very short decoherence times.

2)Nascent stage in harnessing the power of Quantum computation.

3) Still experimental state of Quantum programming and related technologies.

We can go on increasing the number of Registers and the number of Cohorts in each register (to compute and communicate various values). This will enable us to communicate and execute any complex operation. In this manner, we can also program K-Devices to interpret and execute smart contracts on a Quantum Blockchain (K-Chain). Such an idea can be extended to facilitate the construction of a Quantum Turing Machine (QTM), also known as a Universal Quantum Computer.

It is expected that in a decade or two we may be able to build reliable Quantum computers and scale the above hurdles. K-Chains can then provide a hassle-free, zero-time economic transactional experience to the people.

APPENDIX

K-Chain: Quantum Blockchain. A Blockchain system that uses Quantum mechanical principles to record transactions (or any event) and provide a better and more secure transactional experience. In the Turkish language, Quantum is spelt as *Kuantum*. Quantum Blockchains have been named as K-Chains so as to avoid any possible confusion that might arise due to nomenclatural similarity with other Quantum mechanics or related systems.

Zero Time Consensus (ZTC): Instant consensus between devices having electrons (or Qubits) of the same cohort. ZTC automatically eliminates the possibility of Double-spend and by-passes the need for verification (Machine or Manual). This occurs in the Superdense coding method of K-Chains.

REFERENCES

[1] Hegadekatti, Kartik and S G, Yatish, Roadmap for a Controlled Block Chain Architecture (August 13, 2016). Available at SSRN: https://ssrn.com/abstract=2822667

[2] Hegadekatti, Kartik and S G, Yatish, The K-Y Protocol: The First Protocol for the Regulation of Crypto Currencies (E.G.-Bitcoin) (February 13, 2016). Available at SSRN: https://ssrn.com/abstract=2735267 or http://dx.doi.org/10.2139/ssrn.2735267

[3] Einstein A, Podolsky B, Rosen N; Podolsky; Rosen (1935). "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" Phys. Rev. 47 (10): 777–780.

[4] Schlosshauer, Maximilian (2005). "Decoherence, the measurement problem, and interpretations of quantum mechanics". Reviews of Modern Physics. 76 (4): 1267–1305.

[5] Bennett, C.; Wiesner, S. (1992). "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states". Physical Review Letters. 69 (20): 2881.

[6]Michael A. Nielsen; Isaac L. Chuang (9 December 2010). "2.3 Application: superdense coding". Quantum Computation and Quantum Information.

[7] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, W. K. Wootters, Teleporting an Unknown Quantum State via Dual Classical and Einstein–Podolsky–Rosen Channels, Phys. Rev. Lett. 70, 1895–1899 (1993).

[8] Deutsch, David (July 1985). "Quantum theory, the Church-Turing principle and the universal quantum computer". Proceedings of the Royal Society A. 400 (1818): 97–117.

[9] Rupert Ursin (August 2004). "Quantum teleportation across the Danube". Nature. Retrieved 2010-05-22.