BLOCKCHAIN TIME AND HEISENBERG UNCERTAINTY PRINCIPLE

RICARDO PÉREZ MARCO

Abstract. We observe that the definition of time as the internal blockchain time of a network based on a Proof-of-Work implies Heisenberg Uncertainty Principle between time and energy.

1. Introduction.

The role of time in Physics remains mysterious. A proper and unified formalization of time (and of observer's time) is lacking in modern physical theories. In General Relativity time has a geometric meaning as the fourth coordinate in the $3+1$ Lorenzian spacetime. The status of time in Quantum Theory is uncertain and subject to controversies. A fundamental observation by W. Pauli [10] is that there is no well behaved observable operator representing time, thus it is not an observable in the classical sense. There are indeed various interpretations of time. One can consult the classical references [5], [15], and [6] [7] for more information and an updated bibliography.

Time in Quantum Mechanics is not just another spacetime coordinate as is particularly visible in Heisenberg Uncertainty Principle [4]. Usually stated for the standard deviation of corresponding canonical Hamiltonian variables, as position and momentum,

$$\Delta q \,.\, \Delta p \sim \hbar \ ,$$

where $\hbar$ is the reduced Planck constant.We have sometimes a similar relation between energy and time,

$$\Delta t \,.\, \Delta E \sim \hbar \ ,$$

but, as is often observed (see [8], [4]), this is usually proved in Quantum Mechanics in situations where t is a proxy for another canonical Hamiltonian variable. There is no general proof of this type of uncertainty relation since time does not appear as

2010 *Mathematics Subject Classification.* Primary: 91B55, 91B82, 91B80, 81S99, 92C20.

Key words and phrases. Blockchain, Bitcoin, Proof-of-Work, quantum mechanics, Heisenberg Uncertainty Principle, neuroscience.

an observable. The natural result in Quantum Mechanics is the Mandelstam-Tamm inequality for an observable R which states that

$$\tau_R \, . \, \Delta E \geq \hbar/2 \ ,$$

where τ_R is the characteristic time variation of R,

$$\tau_R = \frac{\Delta R}{\left| \frac{d<R>}{dt} \right|} \ .$$

Other more general interpretations have been proposed of time and energy uncertainty relation in general Quantum Systems, as stated by J. Von Neumann in [15] (p. 353): If we want to measure the energy of a system with precision ΔE we need a minimal time Δt and

$$\Delta t \, . \, \Delta E \sim \hbar \ .$$

Some criticisms and controversy surround this interpretation, as for instance the one in [4] assuming the that no minimum time would be necessary for measurements of observables in Quantum Systems. An example of this is given by Aharonov-Bohm energy measurement model [1]. However, more recently, Aharonov and Reznik [2] reviewed the result when the time measurement is made internally, with an internal time. Then the uncertainty of the internal clock provides the time-energy Uncertainty Relation, exactly as in the situation considered here with the "blockchain time" defined in this article. A nice account of this research and more information about quantum clocks can be found in [3].

For all these reasons, we believe that it is not without interest to have some non-standard models for time that shed some light on these problems and the nature of time, energy, and their Heisenberg Uncertainty Relation.

2. Bitcoin network.

On January 9th 2009 the Bitcoin network started operating as the first decentralized peer-to-peer (P2P) payment network, using bitcoin as the virtual currency. The protocol was presented by an anonymous author (or group of authors) by the name of Satoshi Nakamoto in the paper [9] *"Bitcoin: A peer-to-peer electronic cash system"*. The protocol relies on a major breakthrought: The first *Decentralized Consensus Protocol* (DCP): An open group of anonymous and unrelated individuals can reach honest consensus if a majority of the resources are provided by honest participants[1]

[1]We don't use nor give here a precise definition for "consensus", as for example exists in the theory of Distributed Systems. What we mean by "consensus" is the empirically observed agreement of the participants in the network, that allows a "trust system" to function. Very much in the Quantum Theory spirit, the "consensus" reached in the Bitcoin network is not deterministic but probabilistic, with certainty improving with time.

The DCP is made possible by a web of nodes interacting P2P via communication channels through the Internet. Nodes in the network are constantly synchronizing between themselves. The protocol requires computational power, thus energy, to function properly. For a quick introduction to Bitcoin protocol we refer to [11].

3. Blockchain time.

A remarkable consequence of the protocol is the creation of a proper internal chronology to the network. All bitcoin transactions are recorded on a cryptographically secured database called *the blockchain*. This database is regularly updated by the DCP by the validation of new blocks of transactions. Each new validated block provides a "tick" of the internal clock. Since the blockchain is untamperable and unfalsifiable, this clock is a universal untamperable and unfalsifiable clock with a precision of the order of magnitude of the time it takes to validate one new block. The probability to alter the blockchain chronology decreases exponentially with the number of validations [9].

Moreover, the precision of the internal clock is directly related to the average validation time Δt between blocks. If the latency τ_0 of synchronization of the network is negligible compared to Δt, $\tau_0 << \Delta t$, then Δt is directly related to hashrate of the network and the difficulty set by the Proof-of-Work.

4. Proof-of-Work.

The DCP used by the bitcoin protocol is based on a *Proof-of-Work* (PoW) that needs an external input of energy. The *Thermodynamic Conjecture* states that this should be necessary in fairly general conditions, as it follows from general physical thermodynamical principles (see [12]).

The proof of work consists in iterating hashes of the block header of the block in course of validation by some particular nodes of the network (the miners). More precisely he computes $hash(\text{HEADER})$ where $hash(x) = \text{SHA256}(\text{SHA256}(x))$ where HEADER in the block header with a varying nonce. The goal is to find a nonce for which $hash(\text{HEADER}) < d$ where $d \in [0, 2^{256} - 1]$ is the difficulty. The network hashrate H is the number of hashes computed by second by the whole network. In the Bitcoin network the difficulty is adjusted in function of the network hashrate every 2016 blocks so that every block is validated on average in 10 minutes. The pseudorandom properties of $hash$ make that we need an average number of $2^{256}/d$ hashes in order to solve the problem. Hence the average time of validation is on average d/H

where H is the hashrate of the network. If the difficulty is kept constant, then the average time between block validations Δt is variable and is inversely proportional to the hashrate H of the network,

$$\Delta t = \frac{d}{H} \ .$$

In the bitcoin protocol the difficulty is updted for practical reasons. First to avoid long average validation times between blocks that would slow down confirmation of transactions. And the second reason is to avoid a confirmation time that would be close to the critical synchronization time τ_0 of the network. Otherwise there would be a proliferation of orphan blocks and the network would be unable to reach a synchronization regime.

5. PoW and energy.

Since the PoW consists in iterating the same hash function, the input of energy of the network is directly proportional to the hashrate. The energy necessary to reproduce the whole blockchain is proportional to the cumulative amount of work needed to validate the blocks. In that sense we can measure the amount of energy E contained in the cryptographically structured information of the blockchain. This energy is proportional to the computational complexity of the blockchain. At any given time, we have an uncertainty in the measurement of energy ΔE that is proportional to the average energy necessary to validate one block, and this is directly proportional to the hashrate, thus we have

$$\Delta E = k.H \ .$$

6. Heisenberg Uncertainty Principle.

The internal time to the network, obtained by counting blocks in the blockchain, is natural and intrinsic. Any external reference to time, to a clock server, will violate decentralization [11]. It is then natural to define "time" as the network internal time. The above relations imply the Heisenberg Uncertainty Principle, more precisely, with a "reduced Planck constant" for our system $\hbar_0 = k.d$,

Theorem 1. ***(Heisenberg Uncertainty Principle)*** *We have*

$$\Delta E \, . \, \Delta t \sim \hbar_0 \ .$$

We stress that the Heisenberg Uncertainty Principle becomes a corollary with our time definition.

Observe that $\hbar_0 \geq \hbar$ where $\hbar$ is the usual reduced Planck constant[2]. This provides a lower bound for k,

$$k \geq \frac{\hbar}{d} \ .$$

This observation has interesting physical consequences on the relation between energy and computation, and the nature of matter, that are developed in the companion article [13].

7. Neuroscience thoughts.

Decentralized Consensus Protocols are not an artificial notion. Decentralization provides a resilience of the system which becomes *antifragile* in Taleb's terminology [14]. Natural evolution favors decentralized systems. A hierarchical network can be shut down by destroying the central hierarchy. In a decentralized protocol, destruction or corruption of a minor part of the structure leaves the protocol unaltered. This explains why such networks are superior from the antifragile point of view.

In some sense our brain seems to behave as such system. It is composed by a network of communicating neurones (nodes) and decisions are taken in a decentralized form: As is well known in neuroscience, the failure of a small group of neurones does not affect the normal functioning of the brain. As expected, natural selection favors this type of decentralized structure that has superior antifragile properties. This is not in contradiction with the well-known specialization of parts of the brain since the functioning of these parts remains also unaffected by the failure of a few neurones. Brain waves may correspond to "synchronization pulses" of the neural network as block validations in the Bitcoin network.

It is then natural to conjecture that this type of decentralized structure may be at the origin of the conscience of time. This is supported by the fact the the period of neural waves are of the same order of magnitude than the minimal lapse of time that we are able to perceive, that the conscience of time is perturbed during sleep (or unconsciousness, or epileptic seizures) at the same time than the frequency of neural waves changes.

We believe that this type of considerations deserve further explorations.

[2] $\hbar = 1.05 \ldots 10^{-34} J.s$

References

[1] AHARONOV, Y.;BOHM, D. *Time in the Quantum Theory and the Uncertainty Relation for Time and Energy* , Phys. Rev., **122**, 1961, p.1649.

[2] AHARONOV, Y.;REZNIK, B. *"Weighing" a Closed System and the Time-Energy Uncertainty Principle*, Phys. Rev. Lett., **84**, 2000, p.1668.

[3] BUSCH, P.; *The Time-Energy Uncertainty Relation*, in [6], p. 73, 2008.

[4] HEISENBERG, W.; *The Physical Principles of Quantum Theory*, Dover, NY, 1930.

[5] MESSIAH, A.; *Quantum Mechanics*, Vol. 1 and 2, 2nd edition, Dover, NY, 1995.

[6] MUGA, J.G.; MAYATO, R.S.;EGUSQUIZA,I. *Time in Quantum Mechanics*, **Vol. 1**, Springer, 2008.

[7] MUGA, J.G.; RUSCHAUPT, A.; DEL CAMPO, A. *Time in Quantum Mechanics*, **Vol. 2**, Springer, 2009.

[8] MANDELSTAM, L.I.; TAMM, I.E. *The uncertainty relation between energy and time in non-relativistic quantum mechanics*, Izv. Akad. Nauk SSSR (ser. fiz.) **9**, 1945, p.122128. English translation: J. Phys. (USSR) **9**, 1945, p.249254.

[9] NAKAMOTO, S.; *Bitcoin: A Peer-to-Peer Electronic Cash System*, www.bitcoin.org/ bitcoin.pdf, 2009.

[10] PAULI, W.; *General Principles of Quantum Mechanics*, Springer-Verlag, NY, 1990.

[11] PÉREZ-MARCO, R.; *Bitcoin and decentralized trust protocols*, Newsletter of the European Mathematical Society, **100**, June 2016.

[12] PÉREZ-MARCO, R.; *What is a blockchain?*, Arxiv, 2016.

[13] PÉREZ-MARCO, R.; *Blockchain mass and the nature of matter*, Arxiv, 2016.

[14] TALEB, N.; *Antifragile: Things That Gain from Disorder*, Random House, 2012.

[15] VON NEUMANN, J.; *Mathematical Foundations of Quantum Mechanics*, Princeton Univ. Press, 1955.

CNRS, IMJ-PRG, Labex Réfi[3] , Labex MME-DDII, Paris, France

E-mail address: ricardo.perez.marco@gmail.com

[3]This work was completed through the Laboratory of Excellence on Financial Regulation (Labex ReFi) supported by PRES heSam by the reference ANR10LABX0095. It benefited from a French government support managed by the National Research Agency (ANR) within the project Investissements d'Avenir Paris Nouveaux Mondes (investments for the future Paris New Worlds) under the reference ANR11IDEX000602.