DOI 10.26886/2414-634X.1(53)2022.3

UDC: 51-37

TO SAVE MANKIND: PROPOSED IS AN ALTERNATIVE TO MINING BLOCKCHAINS

Mykola Stukach

https://orchid.org/0000-0002-2001-6937

e-mail: mykola.stukach@npp.nau.edu.ua

National Aviation University, Ukraine, Kyiv

The concept of blockchains arouses an admiration due to its reasonableness and ease of implementation within existing infrastructure of Internet. The essential flawisan unacceptably big (from the point of view of ecology and common sence) power waste. The matter concerns the destinies of mankind, because uncontrollably expanding mining blockchains inevitably leads to overheating of Earth and thendeath of all living things. The solution being proposed is based on that follows: mining blockchains is not the goal in itself. The end goal is the reliable safekeeping of some valued constant (invariable) file. We propose not to RESIDE this file in the usual storage medium but to GENERATE it by a proper finite-state automaton. The principal singularity of the automaton circuit is an exeptional testability with respect to all multiple stuck-at faults. It is due to building the circuit according to the Theory of widened long flip-flop. The availis that mining is EXCLUSED as well as consumption of any significant power.

Keywords: *miningblockchains, synthesis of finite-state automaton, easily testable logical circuit, theory of widened long flip-flop, multiple stuck-at faults.*

Introduction. To speak in terms to which people are accustomed, we

will regard the previous coin [1] like “soft” while the new one like “hard”. A hard coin is an electronic device that looks like a small thin box with a small socket and with QR display on the side surface. The display is consist of light-emitting diodes.

Our main offer is publicating a hard coin like a Widened long flip-flop [2; 3]. I.e. at the beginning we design a finite-state automaton that performs 3 function: (1) easy testing of the hard coin, (2) an authentification of the hard coin, and (3) showing the digital content of the hard coin. The design must results with getting a program in the language Verilog. Finelly we publicate the hard coin by mean of making multiple copies of the hard coin of metal. You supply part of copies to customers and part of copies to a public library. It’s clear that the program of the hard coin in the language Verylog must be destroyed.

In the beginning the content of the hardcoin, where included are transactions; bank coins (here they are not creaning by a cryptocurrency miner, instead they are realised at the decretion of some bank-emitent in the form of proper announcements); NFT are accumulated by the responsible publisher of the hardcoin (it can be a monetary yard). The monet of the hardcoin when formed is described in te language of Verilog and is regarded like an original. After the original of the hardcoin is formed, it publishes by the responsible publisher in form of the electronic devices in quantity let us say 1000 copies, of which some are for sale, some are for the public library, and some remains in reserve. The original of the hardcoin the language Verilog should be deleted.

Using of a hard coin begins with cheking of its consistency. You must watch if its surfacehas no visual damages. Then you plug the hard coin into the slot for simple testing and fully test it against all stuck-at faults. After making sure the hard coin is working properly, you check if the hard coin is not a fake. Two copies of the same hardcoin are used for this. The two

copies check each other by mean of an as long as desired procedure of request-response pseudo-random passwords.

Then you read the content of the hardcoin if needed. The contend is shown at the QR-display. The showing sequence of QR-codes is reading by camera of any smartfone, notebook, or by any web-camera.

Merits of the hardcoin concept:1) it can't be forgedin order to change its content; 2) its defense against faults is full; 3) the maintenance of its integrity doesn't need a cent. If your copy of a hardcoin is out-of-service, you can replace it by a properly functioning one in the office of the responsible publisher if it is present in the reserve. It's possible to borrow it from somebody who has such copy or from the public library. All copies of any hardcoin are equivalent. The hardcoin number is sew in its content and is typed on its surface.

If all properly functioning copies of a hardcoin are ending, nothing prevents the hardcoin publisher from publicating a new hardcoin in which a part of old hardcoin can be included.

The cost, the operating speed, and the power input of a hardcoin copy are expected to be moderate. At present no one can see the reasons that they will become empyreal.

Our planet is in danger

Many humans were surprised by what happened to Iceland. As known in it there are super cheap sources of geothermal energy. They used to be enough to heat the home of the Icelanders, for heating all greenhouses, and generation of all necessary electricity. So the light in Iceland was not turned off at night, it used to smelt almost free aluminum, and even for massive carbon dioxide binding and turning it to stone. But that was before there appeared business of mining blockchains. Now the electricity became catastrophically lacking! Because all humans who are not lazy are mining

blockchains. It is a simple business. You must buy the right hardware, configure it with software from Internet and don't turn it off ever. You will earn small but stable money.

As everyone will want a business like this, our planet in fact is fated – there will be its overheating and death of all living things. The way out is seen in the creating an alternative to mining blockchains.

The concept of blockchains [1] is very beautiful, it enthralls your mind. Especially how it utilizes an infrastructure of Internet. It was needen to finish write only soft that turns all interested people into miners of blockchains. Very goodly it was offered to provide safety preservation of data (miners keep in there computers the plurality of copies of data, correct mistakes, generate blockchains, check transactions, pay thereselfs for work and so on).

But futher there begins a horror: a wild expense of energy for executing these functions. For example, to earn 5 dollars on mining blockchains, you must consume about 2 kilowatt-hour of electroenergy – it is a daily energy consumption for family of 4 persons.

Mining blockchains is not the goal in itself. The end goal is the reliable safekeeping of some valued constant (i.e. invariable) file. Because now the task of reliable safekeeping an information like that is solving not easy. Let's consider examples:

1. Not long ago there was a scandal: it turned out that compactdisks reliably store information not for at least 10 years as promised by the manufacturers, but for essentially shorter time.
2. A storing information in clowds in practice turned out very risky. Many a man got burned on that they fully believed the advertisement.
3. A storing information in RAID (i.e. Redundant Array of Independent Disks). One would think that at such a low average failure rate, which is

inherent in modern hard disks, there is no perceived danger of losing information. But this is not the case. The risk is noticeable due to effect of “cool data”: a stored in a hard disk information can be viewed, in order to correct mistakes using colossal redundancy inherent in RAID, but this must be done continuously, with no major stops. Otherwise the data “gets cool”, to the effect that errors get accumulated and become uncorrectable.

Very expressive is that a 10 terabyte RAID of level 5, available to the author for observation, continuously performs the following cycle: the RAID performs a data consintency check for 4 days, then rests for 3 days, then performs a patrol read of all hard disks for 4 days, then rests for 3 days, then starts the cycle over. Sometimes the RAID recognizes any hard disk as broken (though usually it is wrongly). In this case the RAID launches the rebuild procedure lasting for 5 days. During such rebuild the RAID of level 5 is fully defenceless to any failures. To prevent the defenceless like this, instead of RAID of level 5 there can be used RAID of level 6 or higher, though it means much more redundancy.

4. Separate care must be taken for the file protection from hackers. The best way is hiding the file in secret places and rehiding it often. Doing this is French police in regard to its archives.
5. In fact we have little knowledge about behavior of probabilities. For example, recently unraveled was the mystery of waves-killers [4]: often there were noticed ocean-going ships marked with terrible blow to the body which could be made by 30-meter vawe only, although it is well known that the ship sailed among 3-meter vawes. But 3-meter – it is an average height. There appeared a surmise that among 3-meter vawes there are 30-meter ones. This assumtion due to contemporary technologies turned out to be easy to check, as satellites send photos

of oceans incessantly. The search program for 30-meter vawes on photos was launchedand and it turned out that there are a lot of such high vawes. The above goes to show that we may not our weak understanding of probabilities ascribe to the reality we see. For example, to how will faults in files appear. Or to that it is enaugh to defend from single faults of digital circuits. Really needen (if possible!) is defence from all faults (included multiple), like us in our theory of the Widened long flip-flop.

6. Our another example of our misunderstanding how do probabilities behave concerns the river Nile. They watch the river Nile for thousands of years and so there are records about floods of Nile. An analysis of this records showed that sometimes Nile is flooding for unknowing reasons as if it went crazy for a moment. And it happens at every time scale: 10 years, 100 years, 1000 years, 10000 years.
7. They recommend to make backups. But not without reason there came into being a black humor joke: “The state of whatever backup remains a mystery until they try to restore this backup”. To say the same thing in other terms, you need to backup, but you must understand that it does not give the full assurances of data preservation.
8. In the blockchains technology, the safety of data is achieved due to keeping the data copies by huge number of the miners. When there are differencies in copies, the miners take the ballot: they recognizes the correct a copy that has more matches with the others copies. It is the moment when is it convenient for hackers to intervene: they can use the notorius and well rolled in technology of “well-managed chaos”. About this the folk wisdom says: “Everybody’s business is nobody’s business”. In other words, it only seems so that the more people performs management and check functions, the more is the order. It maybe vice versa.

It is important to note that suffering from mining blockchains refusal does not relate to humans who make money due to they have strong intuition about market movements or similar subtle matters. (Making money on mining blockchains are ordinary doers which are not required to have any talentes.) If you have the proper intuition, ardour and money, you can trade in objects of NFT instead of mining blockchains. It will be cool! It will give more income and will not harm nature.

This is an important fact because it is intuition that should be valued. For example, the queen of exact sciences, i.e. mathematics, is fully based on intuition of mathematicians, for the reason that in mathematics theorems are guessed first and then proven. For example, famous formula “1+2+3+4+… = -1/12”, i.e. “sum of infinite natural sequence equals to minus one divided twelve”. The formula is unbelievable but easy provable within school algebra course, see the figure shown:

$$S_1 = 1 - 1 + 1 - 1 \ldots;$$

$$S_1 + S_1 = + \begin{array}{l} 1 - 1 + 1 - 1 + 1 \ldots \\ +1 - 1 + 1 - 1 \ldots \end{array} = 1; \quad \Rightarrow \quad S_1 = \frac{1}{2};$$

$$S_2 = 1 - 2 + 3 - 4 + 5 \ldots;$$

$$S_2 + S_2 = + \begin{array}{l} 1 - 2 + 3 - 4 + 5 \ldots \\ +1 - 2 + 3 - 4 \ldots \\ \hline 1 - 1 + 1 - 1 + 1 \ldots \end{array} = S_1 = \frac{1}{2}; \quad \Rightarrow \quad S_2 = \frac{1}{4};$$

$$S_3 = 1 + 2 + 3 + 4 + 5 \ldots;$$

$$S_3 - S_2 = - \begin{array}{l} 1 + 2 + 3 + 4 + 5 + 6 \ldots \\ 1 - 2 + 3 - 4 + 5 - 6 \ldots \\ \hline +4 \quad +8 \quad +12 \ldots \end{array} = 4(1 + 2 + 3 \ldots) = 4S_3;$$

$$S_3 = -S_2/3 = -\frac{1}{12};$$

Of course there is a much more sofisticated proof which uses Dirichlet series and Riemann zeta function [5]. The formula is undoubtedly confirmed as a property of the real world (based on it are the Theory of

evaporation of black holes by Stephen Hawking, the Quantum Electrodynamics by Richard Feynman, and the famous Effect of Hendrik Casimir). This formula was first recorded by a brilliant Indian mathematician self-tauht Ramanujan who never used proofs but formulas felt intuitively and as far as is known he was never wrong.

The given figure long ago walks around Internet demanding an attention to itself. And here it came useful us in our article like one more proof that everything brilliant is simple. Don't look for focuses in the method happily described in the figure. Focuses are not there. An using a column sum with shift in the beginning of unfinite series is a quite honest method. It can't get an arbitrary result. It turns out that different variants of this operation give either the same result or nothing result.

Conclusions:

1) Doing no changens is unpossible otherwise the world will die from overheating. Because at present world's power already is being thrown away in unacceptable amount, and in prospects everything will get much worse so as number of willing to make money on mining blockchains (which is quite natural!) will only grow until it's too late to make a decision to refuse mining blockchains. The saved energy is worth to spend on a large-scale carbon dioxide binding with making stable rock (stones) [6]. It will very effectively counteract overheating the Earth.
2) Possibly our way to refuse the mining (based on applying the Widened long flip-flop) is not the best possible, but there are no others yet, and when will they appear then the best way to find the best of them is making both theoretical and experimental studies.

Further action:

Investments and enthusiasts are needen.

References:

1. Blockchain. Retrieved from https://en.wikipedia.org/wiki/Blockchain. (2022, January, 24).

2. Stukach, Nick (2008). Easily testable logical networks based on a “widened long flip-flop”. Retrieved from https://arxiv.org/ftp/arxiv/papers/0808/0808.2602.pdf. (2022, January, 24).

3. Stukach, Mykola (2021). Anadvantage of the theory of the Widened long flip-flop: proposed is formulating in the language Verilog. Frankfurt. TK Meganom LLC, Paradigm of knowledge, 6(50), pp. 33-50, ISSN 2520-7474, www.naukajournal.org/index.php/Paradigm[in English].

4. Freak Wave - programme summary. Retrieved from https://www.bbc.co.uk/science/horizon/2002/freakwave.shtml. (2022, January, 24).

5. Kapadia, Devendra (2014). The ABCD of divergent series. Retrieved from https://blog.wolfram.com/2014/08/06/the-abcd-of-divergent-series. (2022, January, 24).

6. How does Carbfix and Climeworks work? Retrieved from https://www.youtube.com/watch?v=jG7nH2WLxiE. (2022, January, 24).