Turing Test Blockchains and Economics

Juan Díez García
diezgjuan@gmail.com

DOI: 10.13140/RG.2.2.14951.62882

November 2, 2023

1 General idea of this research project

Roughly speaking, the field of this research project can be characterized by the following hypothesis:

1. There is a fundamental connection between Computer Science and Economics, in the fundamental concepts of the disciplines but also in the problems they try to solve, in the following sense: Computer Science provides a solution to the main problem of Economics (the "problem of value") via a solution to one of the fundamental problems of Computer Science (the Turing test).
2. The concepts of Economics involved in said problem can be coordinated (not necessarily reduced in the strict scientific sense) to concepts in Computer Science. The question of reduction is a matter of research also.
3. Inside the field of Computer Science, the modern theory of cryptography is a great candidate to address this coordination.

There are some other important ideas that will have to be addressed at some point during this project, in connection with the above hypothesis:

- The scientific status of Economics. Generally speaking, the field of Economics cannot be considered a strict science, even though it may have some scientific characteristics and presupposes different sciences and technologies.
- Relationship between the Turing test and CAPTCHAs. Typical CAPTCHAs today may be considered a practical, limited, specific case of a Turing test.
- The Turing test and its relationship to AI today.

- The idea that it is sound to take the Turing test (a test to differentiate humans from machines) as a conducting idea for the investigation, and to test how far we can get in this direction.
- The principles of modern cryptography as some sort of unification (or start of unification) of Computer Science (or the theory of computation and the theory of computational complexity) and Informatics (or the mathematical theory of communication).
- Economics as a "human science" or "social science" (the human element is part of its constitution and cannot be completely segregated).
- On the nature of "human being", or the lack of its scientific determination.

The general idea of this project is to extend the modern principles of cryptography to a broader scientific field that incorporates in a more systematic manner the relationships with different political and economical institutions, communities and, ultimately, humans. For instance, one of the core ideas this new theory would have to address is the idea of identity.

In order to do this, new concepts will probably have to be introduced that name these relationships or the elements behind them. I am working on this and have some intuitions already of what some of the core concepts may be, but further research is required to test these intuitions and present them formally.

This is a very general description and many efforts are already been made in this or similar directions. The direction that this project would take in this general context is yet to be determined, and would probably be clarified after a systematic state of the art is developed.

2 How this project is novel compared to related work/SoA

According to my research, which is still limited, there are a few issues to address. On the one hand, the modern theory of cryptography [1] tends to be very abstract. This is a good feature in the sense that the theory can be applied to a broad range of phenomena, but it is an undesirable feature because of a general lack of precision, explainability, implementability, etc.

On the other hand, the dynamic relationship that exists between technology and "traditional" economical and political institutions is complex and advancing at a faster pace. This implies uncertainty and lack of comprehension. Because of all this, the gap this project would try to address is to account for these relationships, that are already there, taking place, but that have not been systematised yet. This project would try to develop further and implement some ideas I have found in the literature in this direction, but rather disconnected, and that have

[1] Actually, at this point it is not clear that there is a theory of cryptography, but some principles of cryptography. In a sense, this work would try to derive from these principles a theory, in the context of distributed systems.

not seen widespread adoption compared to other already functioning systems that have already gained worldwide popularity.

AI would probably be one important idea and technology in this investigation. It would probably be necessary in dealing with massive amounts of data, uncertainty and implementing an interface for the end users. From a more theoretical point of view, I think the reason of the necessity of AI lies at the very foundations of computer science, economics, and what a coin is.

There is already research being made in this intersection between AI and cryptography. Nevertheless, this intersection is in principle big, and it will be part of the research to qualify exactly how AI and cryptography are relevant to this project. Furthermore, many ideas in the literature and industry are still very immature or disconnected; this project would try to systematize them. For instance, AI is being implemented as part of cryptographic systems but only at a secondary layer, not as part of the core of the design of the system.

Another important difference with respect to what I have seen in the literature is the general philosophical perspective from which the question is approached. As far as I know, there is a relatively narrow conception (specially in terms of economical and political concepts). In this respect, I refer the reader to the first section of this text and to the list of references at the end (the references are a starting point/rough idea).

3 How to derive the research gap from the literature

In order to account for these relationships, I think we must start from the principles of cryptography, that is, this science is for the most part accepted as given. On the other hand, there is a scientific corpus of the fields of economics and politics that shall also be considered. Furthermore, there is a scientific corpus that addresses, to a certain extent, part of the relationships between these two fields, via theories of the institutions or via more general philosophical theories (e.g. theories of identity). The idea is that the theory of cryptography is general enough such that it can incorporate concepts from the other fields. Some modifications and reinterpretations are expected to be necessary.

For further details on this and the research methodology do not hesitate to contact me at the email provided[2].

[2] If I do not answer in a couple of days assume there has been a problem with the service, the email has been classified as spam, etc.

References

Awerbuch, B., & Scheideler, C. (2004). Group spreading: A protocol for provably secure distributed name service. In J. Díaz, J. Karhumäki, A. Lepistö, & D. Sannella (Eds.), *Automata, languages and programming* (pp. 183–195). Berlin, Heidelberg: Springer Berlin Heidelberg.

Boneh, D., & Shoup, V. (2023). *Principles of Modern Cryptography.*

Bueno, G. (1993). *Teoría del cierre categorial.* Pentalfa Oviedo.

Dupré, J. (n.d.). (various works, tbd)..

European Commission. (2021). Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS.

Idena. (2019). Idena. Retrieved from `https://docs.idena.io/docs/wp/summary/`

Innis, H. A., & Innis, M. Q. (1950). *Empire and Communications.* University of Toronto Press. Retrieved 2023-10-16, from `http://www.jstor.org/stable/10.3138/j.ctv31nzkn3`

Levine, B. N., Shields, C., & Margolin, N. B. (2006). A survey of solutions to the sybil attack.

Lovejoy, J., Fields, C., Virza, M., Frederick, T., Urness, D., Karwaski, K., ... Narula, N. (2022). *A High Performance Payment Processing System Designed for Central Bank Digital Currencies.* Cryptology ePrint Archive, Paper 2022/163. Retrieved from `https://eprint.iacr.org/2022/163` (`https://eprint.iacr.org/2022/163`)

Modulus Labs. (2023). The Cost of Intelligence. Retrieved from `https://www.moduluslabs.xyz/`

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*.

TURING, A. M. (1950, 10). I.—COMPUTING MACHINERY AND INTELLIGENCE. *Mind*, *LIX*(236), 433-460. Retrieved from `https://doi.org/10.1093/mind/LIX.236.433` doi: 10.1093/mind/LIX.236.433