Turing Test Blockchains and Economics

Torbellino Tech

Juan Díez

15.01.23

Esquema I

Esquema II

- Main deliverables
- Schedule

7 Regulatory framework
- Human rights
- Finance
- Artificial Intelligence

8 References

Some context

1. Blockchain ∩ AI.
    1. Turing Test Blockchains.
    2. Digital identity.
    3. Proof of Personhood/Proof of Humanity.

About me

1. Computer Science (University of Sevilla).
2. Master Logic and Philosophy of Science (University of Granada).
3. M.Sc. Data Engineering and Analytics (Technical University of Munich) (*).
4. Master Cybersecurity (Universidad Nacional de Educación a Distancia).
5. Mostly, interested in AI and Cybersecurity (cryptography).

State of the art...

1. Scientific work required to systematize, classify, clarify field.
2. This conceptual work is fundamental to establish new, serious, long-term sustainable business models.
3. Yet immature field, Blockchain has yet a lot of potential.
4. Blockchain has proven its potential in some applications (mostly DeFi).
5. This project: specifically exploring the concept of digital identity.

Strategic value of Blockchain

(McKinsey, 2018):

1. Blockchain value not necessarily reduced to disintermediator $\Longrightarrow$ permissioned model.
2. Blockchain will provide value short-term mostly in reduction of costs.
3. Still years from scalability (main obstacle is standardization).

Hot topics (research)

(Boneh, 2022):

1. Scalability (Ethereum expensive).
2. Privacy Blockchain.
3. Interoperability.

IAM

Problems/challenges IAM (Gensler, 2018):

1. Privacy and security.
2. Identity theft, fake credentials.
3. Updating personal information.
4. Attestation.
5. Centralization (cyberattacks, jurisdictional segmentation, monopoly, censorship, inclusion).

Institutional identity

1. ID/Passport.
   - Issues: privacy, low granurality, bureaucracy, limited geography, scalability, centralization, fragmentation, ...
2. Health system: health records, biometrics.
   - Issues: privacy, ethics, cost, bureaucracy, fragmentation, regulations, scalability, ...

Institutional identity

1. Telecommunications infrastructure: telephone.
   - Issues: privacy, second order dependency, low granurality, centralization. . . .
2. Banking infrastructure:
   - Issues: . . .

In process of institutionalization...

1. Cryptocurrencies.
   - Issues: PKI centralization, second order dependency, cybersecurity, scalability, not user friendly, . . .
2. CAPTCHAs.
   - Issues: scalability, abstraction, uncertainty, technical/scientific challenge, . . .

(Idena, 2019)

1. Technically, same idea that this project (scientific coincidence).
2. Very interesting project, first prototype/reference of SoA.
3. However (yet to be studied in detail):
    1. Insufficient documentation.
    2. Philosophy/principles/scope of the project unclear.
    3. Still many technical challenges (development).
    4. Business model unclear.
    5. ...

(Modulus Labs, 2023)

1. AI in Blockchain.
2. Technical study on scalability, performance, IoT limitations, etc.
3. Still to clarify how exactly relevant to this project.

Self-sovereign identity

1. Power of individuals/communities to control their identities (digital footprint), in their interactions with others.
2. Identity and money are two separate things in principle:
   - (Gensler, 2018): “Decentralized identity does not necessarily require decentralized money”.

Decentralized Identity Foundation

Decentralized Identity Foundation.

Research hypothesis...

Main research hypothesis:

1. There is a fundamental connection between Computer Science and Economics: Computer Science provides a solution to one of the fundamental problems of Economics (the "**problem of value**") via a solution to one of the main problems of Computer Science (the **Turing test**).

Secondary hypothesis/topics derived from the main one...

1. Relationship between Turing test and CAPTCHAs today.
2. Turing test and AI SoA today.
3. Modern theory of cryptography as a start of unification of Computer Science and Informatics.
4. The scientific status of Economics as a discipline of knowledge ("human science" or "social science").
5. The connection of this with the concept of identity.

My philosophy of identity

My philosophy of identity:

1. ¿An ID, a DNA string, a bank account number, . . . ? Reductionist.
2. In principle, we have to start from a more general idea.
3. Identity is a philosophical idea (necessarily).
4. Best effort, soft identity, uncertainty, . . .
5. Identity as a process/chain.
6. Identity is social.
7. But societies are heterogeneous.
8. We presuppose societies are build based on:
    1. common technologies,
    2. common scientific disciplines,
    3. common sectors/industries, . . .

Market value

Market value (potential): trillions $[1].

[1] (Preukschat & Reed, 2021)

Potential clients

B2B: 10^2-10^3

B2C: 10^6-10^9

Collaborators

General service providers:

1. Database.
2. Networks.
3. Sysadmin.
4. Cybersecurity.

Specific providers:

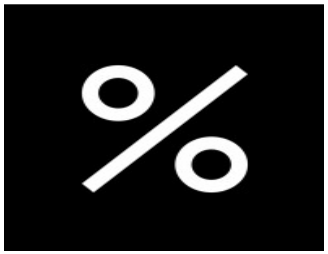
1. Identity Access Management.
2. Blockchain.
   - Identity.
   - Others.
3. Artificial Intelligence.
   - Natural language processing.
   - Image.
   - Audio.
   - ...

Collaborators

Decentralized Identity Foundation.

Collaborators

Collaborators



Clients/collaborators

1. Tech, information, social networks, ...
2. Banks, e-commerce, ...
3. Public administrations, ...
4. Health, ...
5. Logistics, ...
6. Audiovisual, media, ...

Competitors

1. In general, immature field, hard to tell yet.
2. Potentially, organizations working in Blockchain, AI, and digital identity.
3. Potentially, any of the collaborators.

Business model

1. Digital identity in blockchain.
2. Digital identity (in general).
3. Decentralized public key infrastructure (DPKI).
4. Depending on collaborators, clients, and project development:
    1. Database administration.
    2. Computing/information services.
    3. Consulting.

General considerations

In rough terms, project dedication consists of:

1. Research (70%):
    1. Basic research (20%).
    2. Applied research (30%).
    3. Communication (20%)
2. Development (30%).

Main research lines

The project implies the following main research lines:

1. AI: computer vision, natural language processing, signal processing...
2. Distributed systems: consensus, cryptography.
3. Methodology, data life-cycle.

Lines of work

Lines of work/publication ($\sim$ product/service):

1. Distributed systems theory.
2. Clustering applied to digital identity.
    1. Survey/SoA: TornadoCash, Z.Cash, ...
3. AI and consensus algorithms.
    1. Survey/SoA: Idena, ...
4. Methodology, framework, ...
5. Applications by sector: energy, movility, finance...

Software

1. Software prototypes.
2. Simulations/experiments.
3. Application.

Data

1. Simulation/experimentation data.
2. Open source data: internet.
3. Collaboration data.
4. Derived data, aggregates, processed,...

Schedule

The first big iteration of the project would last around 3 to 5 years. The project can be divided in the following phases (illustrative, may overlap/vary):

1. Research: SoA, basic research, applied research (1-2 years).
2. Development: experimentation, simulation, research, implementation, integration, testing (1-2 years).
3. Deployment: scaling, testing, customization, configuration, maintenance, monitoring (1-2 years).

Human resources

1. Computer Scientist/Computer Engineer.
2. Artificial Intelligence Specialist.
3. Distributed Systems Specialist.
4. Cryptography/Cybersecurity Specialist.
5. Computing Services Specialist.
6. Sysadmin Specialist.
7. Sector specialist:
    1. Energy (Electrical Engineer, Industrial Engineer, etc.).
    2. Finance, Economist, etc.
    3. E-commerce Specialist.
    4. Regulations (Lawyer, etc.).
    5. Health (Bio-medical Engineer, Medical Doctor, etc.).
    6. ...

Reglamento (UE) 2016/679

- (PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA, 2016).
  1. Definition and classification of infractions.
  2. Definition fines.
  3. Description of relevant institutions in data protection.

Ley Orgánica 3/2018

- (Gobierno de España, 2018).
  1. Personal data definition.
  2. Right to be forgotten.
  3. Right to restriction of processing.
  4. Right to portability.
  5. Right to object.
  6. Right to freedom of expression.
  7. Right to intimacy (e.g. geolocation).
  8. Right to digital will.

Plan de Recuperación

- (Gobierno de España, 2021). Presentación general del plan.
- (Gobierno de España, 2023). Componente 13, específico PYMES.
  1. Reforzar sistema español de garantía recíproca. Dotación al CERSA para garantizar financiación a largo plazo de PYMEs.
  2. Incorporación líneas de especial apoyo y mayor cobertura del riesgo.
  3. Fondos Next Tech.
     1. Fond-ICO Next Tech, F.C.R. ('Next Tech fund').
     2. Financiado a partir de 2022.
     3. Fondos público-privados de inversión en empresas innovadoras en tecnologías disruptivas.

Plan de Recuperación

Calendario inversión Fondos Next Tech.

Inversiones o reformas que conllevarán una inversión específica								
C13.I7	**Fondo para escalar startups tecnológicas: Next Tech**							
Coste	4.000 M€							
Periodificación	2020	2021	2022	2023	2024	2025	2026	Total
Coste del Mecanismo			150	800	1.000	1.050	1.000	4.000
Otra financiación			156	833	1.041	1.072	1.061	4.163

(Gobierno de España, 2023)

4000 M€ adicionales posibles.

Ley de empresas emergentes

- (Gobierno de España, 2022). Ley de empresas emergentes.
  1. Complementa las ayudas de Fondos Next Tech.

Artificial Intelligence

- (European Commission, 2021).

References I

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. (2022). *Cryptocurrencies and Blockchains: the Good, the Bad, and the Future.* Retrieved from `https://www.youtube.com/watch?v=4PHbjESHQME`

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

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

References II

Buterin, V. (2021). *Things that matter outside of defi.* Retrieved from https://www.youtube.com/watch?v=oLsb7clrXMQ

Buterin, V. (2022). *Where to use a blockchain in non-financial applications?* Retrieved from https://vitalik.eth.limo/general/2022/06/12/nonfin.html

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.

References III

Gensler. (2018). *Blockchain and Money.* Retrieved from https://ocw.mit.edu/courses/15-s12-blockchain-and-money-fall-2018/

Gobierno de España. (2018). *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.* Retrieved from https://www.boe.es/eli/es/lo/2018/12/05/3

Gobierno de España. (2021). *Plan de Recuperación, Transformación y Resiliencia.* Retrieved from https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/160621-Plan_Recuperacion_Transformacion_Resiliencia.pdf

References IV

Gobierno de España. (2022). *Ley 28/2022, de 21 de diciembre, de fomento del ecosistema de las empresas emergentes.* Retrieved from https://www.boe.es/eli/es/l/2022/12/21/28/con

Gobierno de España. (2023). *Plan de Recuperación, Transformación y Resiliencia. Componente 13.* Retrieved from https://planderecuperacion.gob.es/sites/default/files/2023-10/0310203_adenda_plan_de_recuperacion_componente13.pdf

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

References V

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)

References VI

McKinsey. (2018). *Blockchain beyond the hype: What is the strategic business value?* Retrieved from https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/blockchain-beyond-the-hype-what-is-the-strategic-business-value/

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*.

PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA. (2016). *Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.*

References VII

Preukschat, A., & Reed, D. (2021). *Self-sovereign identity*. Manning Publications.

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

UMA-ATECH. (2024). *LINK.* Retrieved from https://www.link.uma.es/