Turing Test Blockchains and Economics

Torbellino Tech

Juan Díez

12.11.23

Outline I

Outline II

Disclaimer

I am not an economist. . . nor do I pretend to be one.

Disclaimer

The king says I am an engineer.

$\vdash$ I am an engineer.

Disclaimer

The devil is in the details.

Turing Machines and Information

1. Turing Machine as universal model of computation. Theory of Computation.
2. Conceptualized around 1940s, still relevant today.
3. At around the same time, Mathematical Theory of Communication (Shannon). Leads to Informatics.
4. Turing vs. Shannon anecdote.
5. Not clear how to unify the fields. Why two theories inside “Computer Science”?

80 years later...

1. In 80 years: many developments, theoretical and technological, programming, cryptography, computer's architecture, computer networks, distributed systems, cryptography, ...
2. Very exciting but... the fundamental concepts and theories are still the same. Not a lot of truly scientific breakthrough.

80 years later...

1. As a general rule, development has focused in technologies, scalability, products, business models, etc.
2. Technological saturation. Big players in the market already established. Hard to continue innovating.
3. Quantum Computing: spooky probabilities.
4. Today: turning point in this dynamic (apparently, seems necessary...).
5. Blockchain as a scientific revolution (more than a technological one).

Blockchain...

1. Today: turning point in this dynamic (apparently, seems necessary...).
2. Blockchain: the "universal" data structure.
3. Change the data structure, change the game, change the market.
4. Embracing the concept of replication. Somehow, bringing Computer Science to its limits.
5. The climate is changing, the Clouds start to leak...

Cryptography...

1. Unification CS and Inf.
2. Principles vs. theory.
3. General philosophical framework.

MMT and Blockchain

1. Current economic-political paradigm: Social liberalism/Market Socialism/State-Corporate Capitalism.
2. Current monetary paradigm: Modern Monetary Theory (MMT).
    1. Treasury "prints" money (ledger annotations in a computer system).
    2. Treasury channels credit to the economy via: central banks $\rightarrow$ banks $\rightarrow$ corporations $\rightarrow$ companies $\rightarrow$ individuals.
3. Credit $\iff$ Risk.
4. Blockchain:
    1. Decentralize risk.
    2. Delegate risk.
    3. Capillarization.
    4. New markets.

Overview of the field/market...

1. A lot of technologies already well developed. Market established.
2. Possible to start commercializing very abstract concepts.
3. Blockchain still quite immature field though. Bitcoin and Ethereum are just the beginning.
4. Conceptual work (research) is required to clarify. Systematize, classify, clarify, distinguish....
5. This conceptual work is a precondition to establish long-term, profitable business models.

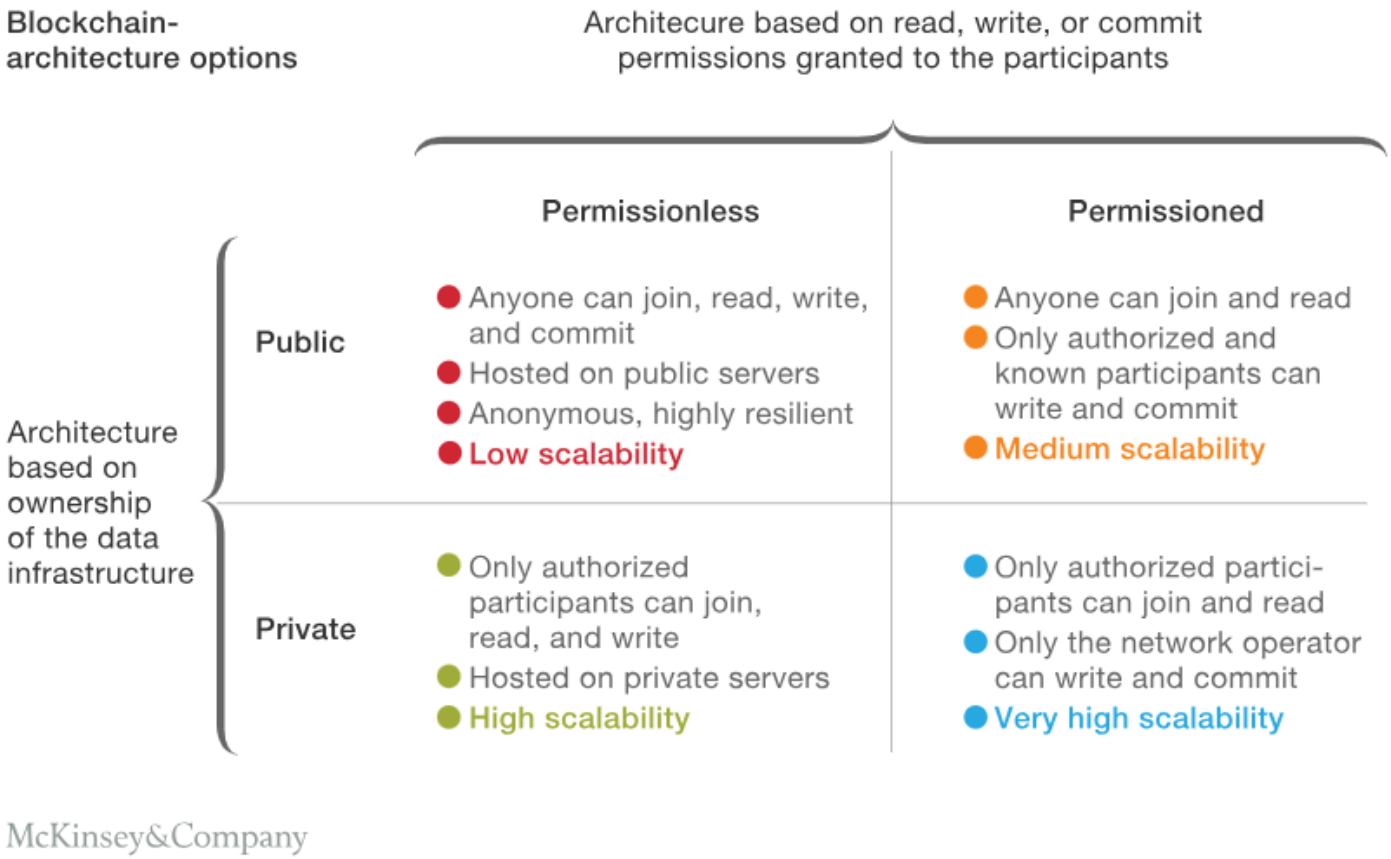
Strategic Value of Blockchain

(McKinsey, 2018) insights:

1. Blockchain does not have to be a disintermediator to generate value $\Longrightarrow$ permissioned commercial applications.
2. Blockchain's short-term value will be predominantly in reducing cost before creating transformative business models.
3. Blockchain is still three to five years away from feasibility at scale (standards is the main obstacle).

Permissionless vs. Permissioned

Most commercial blockchain will use private, permissioned architecture to optimize network openness and scalability.



(McKinsey, 2018)

Hot topics (research)

(Boneh, 2022):

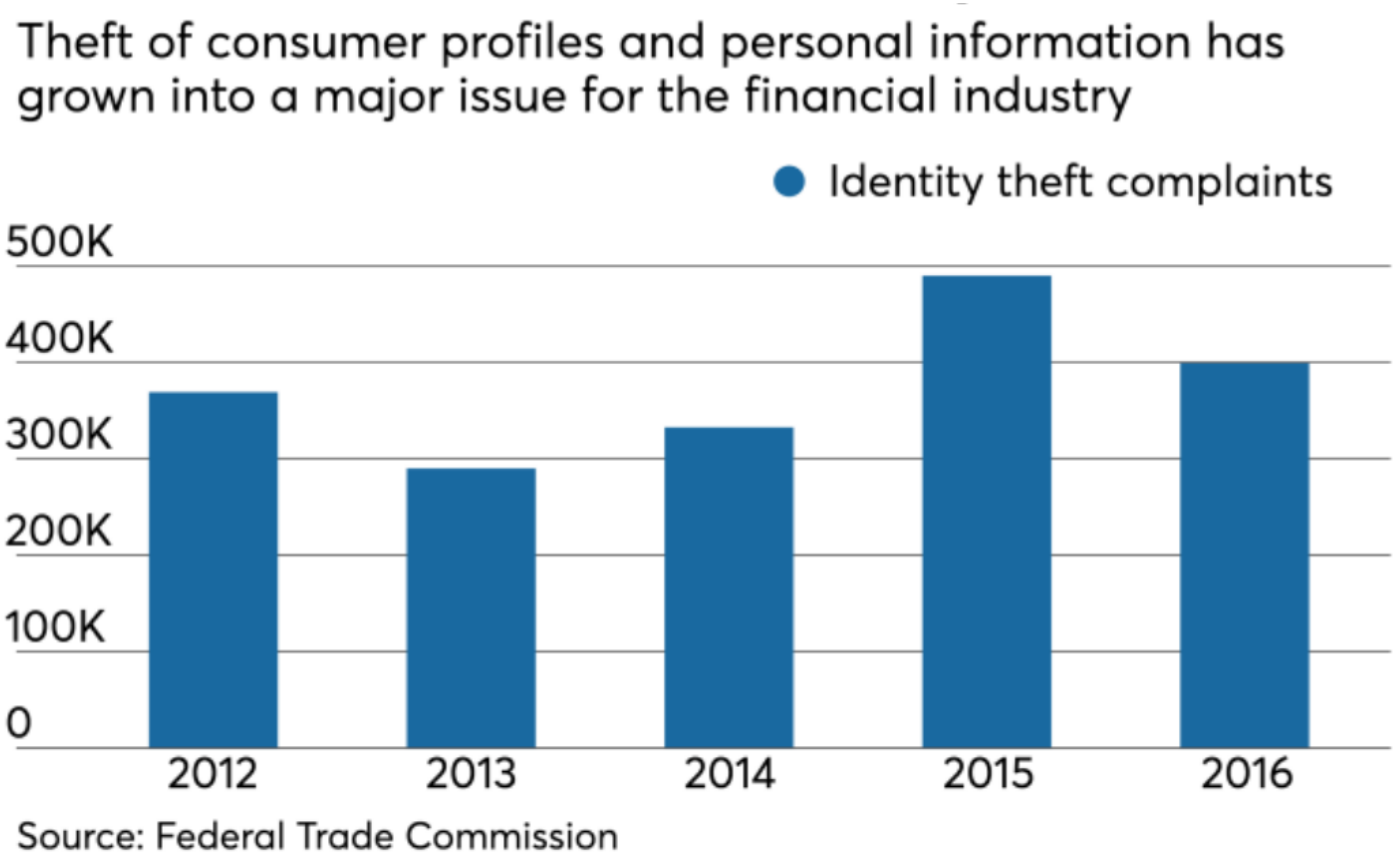
1. Scaling the blockchain (Ethereum too expensive).
2. Privacy on the blockchain. Businesses cannot use if all transactions are public.
3. Interoperability between blockchains.

IAM Challenges

IAM Challenges (Gensler, 2018):

1. Privacy and Security.
2. Identity Theft and Forged Credentials.
3. Credentials –Physical Documents often with Images.
4. Updating Personal Identity Information (PII) for life changes.
5. Costs and Timeliness of Attestation.
6. Trade-Offs or Digital vs. Physical Credentials.
7. Centralization (Targets for Cyber Attacks, Jurisdictional Segmentation, Monopolistic Behavior, Censorship and Inclusion).

Identity Theft in Financial Industry



(Gensler, 2018)

Institutional identity

1. Government ID.
   - Issues: privacy, low granurality, bureaucracy, limited geography, single point of failure, (scalability).
2. Government Passport.
   - Issues: privacy, low granurality, bureaucracy, limited geography, single point of failure, (scalability).
3. Healthcare system: Medical records, biometrics.
   - Issues: privacy, ethics, high cost, bureaucracy, limited geography, single point of failure, local regulations, standards, scalability.

State Identity Projects

From (Gensler, 2018):

1. Estonia e-identity.
   - State Issued Digital Identity.
   - Started 2002 with ID-cards.
   - Run on X-Road software.
   - Not blockchain technology.
2. India Aadhaar.
   - National Identification System.
   - Social inclusion, wealthfare philosophy.
   - 12 digit ID.
   - Biometrics: fingerprint and iris scan.
   - Not blockchain.
   - Good things, pretty efficient.
   - But also a lot of problems, scary. One national system. Mistakes. Single point of failure. Including suicides.
   - Faster system in the world to reach 1 billion users (not mandatory).

Institutional identity

1. Telecommunications Infrastructure: Telephone.
   - Issues: privacy, governmental second-order dependency, low granurality, bureaucracy, (limited geography), (single point of failure), (scalability).
2. Banking infrastructure: Credit card/bank account.
   - Issues: privacy, governmental second-order dependency, (low granurality), bureaucracy, (limited geography), (single point of failure), scalability.

Non-Institutional identity

1. Cryptocurrencies.
   - Issues: (privacy), (governmental second-order dependency), (low granurality), (bureaucracy), (limited geography).
2. CAPTCHAs.
   - Issues: scalability, technical/scientific (AI).

(Idena, 2019)

1. Technically, same idea as us.
2. Very interesting project. Could be seen as a reference case study.
3. However (yet to be studied systematically):
    1. Poor documentation.
    2. Unclear philosophy/general principles of the project.
    3. Many technical challenges still open...
    4. Permissionless system. What about permissioned?
    5. ...

(Modulus Labs, 2023)

1. Focused on AI in the blockchain.
2. "The Cost of Intelligence" white-paper.
3. Study on scalability, performance of AI, limitations of IoT, embedded devices, new directions in blockchain and AI...
4. Also very interesting project. Reference case study.
5. Better documentation. Seems like a more "professional" project than (Idena, 2019).
6. However (yet to be studied systematically):
    1. Not so clear how it is specifically related to our project (identity).

Self-sovereign identity

1. The concept of central government issued identification is quite modern (one hundred to two hundred years).
2. In the past, other institutions took the place, or there was just a gap of power.
3. The power of the coin as unit of account. Coin is more flexible (e.g. anonymous).
4. The power of individuals or communities to control their identities (digital footprints), while also interacting with other communities.
5. Treat identity and money as two separate things in principle.
   - (Gensler, 2018): “Decentralized identity does not necessarily require decentralized money”.

Decentralized Identity Foundation

Decentralized Identity Foundation members.

Working hypothesis...

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: 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.
3. The modern theory of cryptography is a great candidate to address this coordination.

Some questions to be addressed...

1. Relationship between the Turing test and CAPTCHAs.
2. The Turing test and its relationship to AI today.
3. The principles of modern cryptography as some sort of unification of Computer Science and Informatics.

Turing test and Economics...

1. The scientific status of Economics. Not strictly a science.
2. Economics as a “human science” or “social science”.
3. On the nature of “human being”, or the lack of its scientific determination.
4. The idea that it is sound to take the Turing test as a conducting idea for the investigation, and to test how far we can get in this direction.
5. The connection of all of this with the concept of identity (digital identity).

What is identity?

What is identity?

1. A Government ID, a DNA string, a bank account number, . . . ? Reductionist.
2. In principle, we need to assume a more general idea of identity.
3. Identity is a philosophical idea.
4. Identity is social.
5. Identity as a process/trace (chain).
6. But societies are heterogeneous.
7. We presuppose societies are built on:
    1. common technologies,
    2. common scientific disciplines,
    3. common techniques,
    4. common professions
    5. common industries/sectors,
    6. . . .

Communities are technologies

1. Blockchain as a scientific revolution (more than a technological one).
2. No such thing as the universal coin.
3. Target communities, discover/adapt to their identity.
4. Their identity is, for the purposes of our project, the technologies that they use.
5. But again, technologies are heterogeneous.
6. Connect this with the idea of AI and the blockchain.
7. In principle:
    1. Permissioned blockchains more profitable, easier to define business model.
    2. Permissionless blockchains easier to deploy.

The adoption problem

1. Systemic problem: adoption.
   1. Adoption cannot be really seen as a “problem” but rather as a guiding principle.
   2. The “problem” of adoption will necessarily need to be tempered by sheer force of technology.
   3. Problem: adoption. Solution: inertia.
   4. Subtly suggested in (Gensler, 2018): “Banks are pushing. . . merchants have no bargaining power. . . ”.
2. Systemic problem: “identity cannot be in the public/wild”.
   1. Solution: actually, that is contradictory.
   2. Solution: apparently, related to narrow conception of the idea of identity.

Collaborators

General service providers:

1. Database infrastructure, implementation, administration.
2. Network infrastructure, implementation, administration.
3. System administration.
4. Cybersecurity.

Specific service providers:

1. Identity Access Management.
2. Blockchain.
   - Identity.
   - Others.
3. Artificial Intelligence.
   - Natural Language Processing.
   - Image Processing.
   - Audio Processing.
   - ...

Collaborators

Decentralized Identity Foundation members.

Clients/collaborators

1. Banks, e-commerce, ...
2. Public administrations, ...
3. Health sector, ...
4. Logistics, ports, ...
5. Audiovisual, media, art, ...

Competitors

1. In general, immature field, hard to tell at this point.
2. Potentially, Blockchain and Artificial Intelligence companies working in the specific area of identity.
3. Potentially, any of the collaborators.
4. General strategy: be everywhere all the time $\Longrightarrow$ be at the right time in the right place.

Business model

1. Digital identity in blockchain.
2. Digital identity (in general).
3. Decentralized Public Key Infrastructure.
4. In general, to be determined in the process.
5. Study competitors/collaborators.
6. Associated (depending on collaborators, client and project):
    1. Database administration.
    2. Computing/information services.
    3. Consultancy.

Main areas/tasks

The project can be divided in the following areas/general tasks:

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

Main technical/scientific lines

The project would involve the following main technical/scientific lines:

1. AI: Computer Vision, Natural Language Processing, Signal Processing.
2. Distributed Systems.
3. Cryptoeconomics: Blockchain services, Interoperability, Cloud services.
4. Human-Computer Interaction: User Interfaces, App Development.

Main deliverables

The project would consist of the following main deliverables:

1. Documentation: articles, research papers, technical documentation, blog, social networks.
2. Software: software prototypes, simulations/experiments, application.
3. Raw data: research, simulations/experiments.

General timeline

The first iteration of the project would last from 3 to 5 years, with the goal of implementing and deploying a first software. Rougly speaking the project could be divided in the following phases:

1. Research: state of the art, basic research, applied research, communication (1-2 years).
2. Development: experimentation, simulation, research, development, integration, testing (1-2 years).
3. Deployment: scale, testing, configuration, deployment, maintenance, monitoring (1-2 years).

Reglamento (UE) 2016/679

- (PARLAMENTO EUROPEO Y EL CONSEJO DE LA UNIÓN EUROPEA, 2016).
  1. Definición y clasificación de infracciones.
  2. Definición cuantías multas.
  3. Descripción de instituciones responsables de la protección de datos.

Ley Orgánica 3/2018

- (Gobierno de España, 2018).
  1. Definición de datos personales.
  2. Derecho de supresión (o derecho al olvido).
  3. Derecho a la limitación del tratamiento.
  4. Derecho a la portabilidad.
  5. Derecho de oposición.
  6. Derecho a la libertad de expresión en Internet.
  7. Derecho a la intimidad frente al uso de geolocalización.
  8. Derecho al testamento digital.

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.

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

References II

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.

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

References III

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

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

References IV

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/

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.

References V

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)

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/

References VI

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.* Retrieved from https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679

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