MIT Connection Science
the technology of innovation

2/23/22

Prevention of Digital Crime and Corruption in a Web3.0 World

Prof. Alex Pentland, MIT

MIT Connection Science Whitepaper 1/23/2022 based on conversations with senior leadership of multinational companies (Mastercard, Visa, EY, Deloitte, IBM, Ferrovial, Barclays, China Construction Bank), nations (Treasury and Commerce departments of US, EU, Korea, Singapore, Indonesia, Australia, Denmark) and multilaterals (World Bank, OECD, UN Sec. General office, World Economic Forum, World Leadership Alliance). The views in this paper do not necessarily represent those of the discussion participants.

The Web 3.0 Security Challenge

New "web 3.0" technologies….the combination of artificial intelligence (AI), blockchain, and Internet of Things (IoT)…have created new challenges for institutions and governments in combatting digital crime and corruption, as well as creating the potential for enormous inequality [1]. Blockchain systems may be the world's largest path for ransom, money laundering, and illegal funds transfer. AI is used within every sector to discover private, proprietary data and even national secrets, and IoT allows mass tracking of the behavior of private individuals, corporations, and organizations at a very high level of granularity.

Today there are no generally accepted standards for monitoring or auditing these flows of money, material, environmental conditions or data, despite the obvious and serious risk these problems pose to individuals, corporations, governments, and even the entire world. While there are historical systems and regulations in the domain of finance, and proposals for some aspects of these new all-digital financial systems, there is no framework for a world-wide anti-fraud and anti-corruption framework that could be applied to all digital transactions.

As much promise web 3.0 holds, the reality is that the technical means that would enable good governance and crime prevention don't yet exist. Without the ability to monitor and audit digital transactions we will not have an effective, reliable Environmental, Social and Governance (ESG) measurement [2], reduction in large-scale financial fraud [3], monitoring of logistics chain risk [1,2,3], or early detection of pandemics.

Development of standards and norms for these new Web 3.0 systems should happen before they are widely deployed, which means that discussions need to happen very soon. Discussions between nations, multinationals, and civil society organizations should focus on establishing norms of interaction, auditing, accountability and governance. Payments and some other types of financial transactions are examples of systems where this sort of interoperability and shared norms has been achieved.

This suggests that a new "Digital Bretton Woods" multilateral effort is required, with the goal of developing a multilateral body to provide guidance for Web 3.0 platforms both for industry-developed platforms and those developed by China, Singapore and Switzerland. Unlike the World War II Bretton Woods effort, such coordination must not only be centered around banking and finance but must be intimately dependent on digital technical standards for trade and the unified risk-assessment science needed to measure and forecast interactions between finance, sustainability and social factors. Such a body need not be expensive or large, as illustrated by the governance oversight platforms developed for the Internet and the World Wide Web.

An Architecture for Web 3.0 Governance and Audit

Transparency, accountability and fairness are the basis for justice and good governance. These public goods are in tension with individual privacy, proprietary business data, and state secrets. Historically personal, company, and state secrets were protected by physically hiding them and by norms prohibiting discussion. In the modern era we have developed more formal governance and crime prevention methods, such as the census (which puts certain information in the public domain), regular reporting of summary information (tax forms, company reports) that guide financial investment and potentially signal problems, and rules for maintaining private records for investigative audit.

The tension between making information available and keeping it secret is everywhere in these systems, and is usually solved by either trusting the state to hold the data secret (e.g., tax records) or making them public (e.g., census and financial performance data). Unfortunately, new technologies such as blockchain, AI and IoT make existing solutions outdated. The Web 3.0 world may end up being a very lawless place, where the quick and the powerful rule with impunity and the rest of us are "mined" for our resources

This whitepaper will lay out technical capabilities and system architecture that allow balancing the needs of individuals and the public while at the same time reducing risks of crime, corruption, and unintended consequences. Our approach is based on two recent mathematical advances. The first is development of methods for constructing aggregate census-like data, including public performance and impact reports from companies and nations, without risk of exposing personal, company, or state data and without having to trust third parties such as government agencies. The second is a method of proving that your operations are conforming to laws and are property reflected in your reports without revealing private, proprietary, or secret data. Both methods have the separate advantage that they are very sensitive and quick methods to detect and isolate fraud or attack by third parties.

The first new mathematical advance that we will make use of is the recent development of distributed computing technologies such as Secure Multiparty Computation (SMC) and distributed ledgers employing cryptographic constructs such as Merkle trees. These technologies allow trusted, auditable computing that can automatically compute legal reports (e.g., tax, legal compliance, medical treatment data) and public, census-like data without endangering privacy, security, or state secrets. For instance, in [4] we developed a protocol that turns a blockchain into an automated access-control manager that does not require trust in a third party. Transactions in this system are used to carry instructions, such as storing, querying and sharing data, making it possible to create a trusted, privacy-preserving system for the full range of reporting requirements without exposing the underlying data.

The second new mathematical advance is development of Cryptographic Proofs (CP) that guarantee that transactions and ledgers conform to legal guidelines, and which allow immediate identification of suspicious transactions and accumulations for more detailed auditing. For instance, we have demonstrated in [5] a system that uses cryptographic proofs on distributed ledgers to ensure the secure cooperation of large groups of actors (individuals, companies, nations) by encapsulating transactions in an authenticated data structure known as a Merkle tree. With this method, regulators can provide a legal "blueprint" for the economy without specifying data or details. In other words, transaction verification can be separated from data itself, by having economic actors "prove" their integrity to their peers by exchanging cryptographic proofs. This allows continuous compliance guarantees for transactions in areas ranging from finance, to environmental and healthcare monitoring.

Supporting these publishing and compliance elements must be a ledger technology that immutably records each transaction for risk reduction through legal compliance, fraud or corruption detection, and ensuring fairness and lack of bias. As new technological solutions emerge to manage increased data utilization within an organization – such as logical data warehousing, cloud data, data-hubs, etc. – there is a corresponding need for organizations to incorporate *data auditing* as a core part of the data management lifecycle.

The need for audit is driven not only by internal Enterprise data-consistency requirements, but also from regulatory compliance requirements notably when organizations obtain and utilize personal data (e.g. EU GDPR [6] and EU Data Governance [7]). Included is data provenance tracking (e.g., data use permissions), data derivation (for instance, decisions of an AI system), and tracking of direct access and indirect access to data.

The goal of a *data audit infrastructure* is to collect, organize and maintain evidence of data ingestion, usage and archiving across the various business units of an organization. The data audit infrastructure must be agnostic as to user/employee, applications and the data types. The advent of *hash-chains* and blockchain technology provides a core building-block for trace & audit, around which other data audit functions can be developed.

Computer code development platforms such as GitHub [8] have been using many of these methods for nearly a decade now. Periodically the change-logs and access-logs are further summarized into a hash tree structure (e.g. Merkle tree) anchored to a distributed ledger, and summary statistics published for regulatory compliance or financial reporting, using techniques like Secure Multiparty Computation (SMC) and Cryptographic Proofs (CP), which guarantee protection of the underlying data. This SMC, CP and Merkle tree approach provides important benefits to data management systems employed by many organizations today, including independence from information type, lightweight anchors, persistence and privacy-preservation, and enables automated post-event audit.

Modern organizations in the digital economy will not only rely more on its own data, but it will also rely increasingly on data held by other entities. This dependence opens many opportunities for fraud and corruption which needs mitigation. New methods to share insights and perform joint-computations between parties without disclosing plaintext data, such as SMC and CP are being developed, and will reach the market in the next 3-5 years. This inter-dependence for data among business partners also introduces challenges from the perspective of audit, taxation and regulatory compliance. For example, organizations which share insights (e.g. using the OPAL paradigm [9]) must be able to prove to auditors of the interactions between them through the appropriate APIs. Thus, the notion of a lightweight audit-log blockchain discussed above lends itself for utilization also for cross-enterprise interactions, whether in the context of the sharing of insights, or in asset-related transactions.

The potential benefit of a lightweight blockchain that carries minimal information – consisting of records of a hash-value and tag (as a context identifier) – is increasingly being recognized by the industry. It is often referred to as a ``witness blockchain'' denoting its main task as a time-stamp for hash-values. European Blockchain Service Infrastructure (EBSI) project [10] refers to something similar as its “notarization” blockchain.

This same model may also be utilized for cross-border transactions (e.g. digital trade [11]), which may incorporate the sharing of data and/or the movement of digital assets (e.g. electronic payments). For instance, the entities involved can be private-sector organizations (e.g. commercial banks) or public-sector organizations (e.g. Border Port Authorities)

Conclusion

Both the financial crash of 2008, the current pandemic and attendant supply chain problems have laid bare the inadequacy of current systems, both in terms of their inability to prevent fraud, forecast and manage crises, and to prevent systemic exclusion or bias against of many parts of society. These challenges aren’t solved by current Web 3.0 technologies alone, and without the sort of governance and auditing mechanisms discussed in this whitepaper it is possible that Web 3.0 could actually exacerbate these problems. To build a safer, inclusive, innovative and equitable global economy there needs to be access to robust, timely and comprehensive “rich census data” including aggregated transaction data. As emphasized in the recent G20 meeting, open access to this sort of data will allow stakeholders to more quickly, and with greater certainty, forecast sources of local and global risks, ranging from financial crashes, to climate change, to pandemics, to systemic racial and gender discrimination to other precursors of social unrest.

Coordinated multinational and national systems that allow unified and agile response is required. The need for technologies such as secure, privacy-preserving digital ID, accurate records of cross-border trade, and real-time sharing of health data are becoming urgent. There are of course many relevant initiatives underway, but there is no overarching vision and so gaps and contradictions are everywhere. The technology to build effective systems exists, and industry is willing to lead the way in deployment, and now governments need to enable effective, coordinated detection of attacks, fraud, and rules for proportional response.

References

[1] https://www.weforum.org/agenda/2021/07/the-future-of-sustainable-finance/

[2] https://www.weforum.org/agenda/2021/10/how-decentralized-systems-can-help-rebuild-local-communities/

[3] http://www.clubmadrid.org/wp-content/uploads/2020/11/Digital-Cooperation-and-a-Better-Global-Future-1.pdf

[4] Guy Zyskind, Oz Nathan, Alex Pentland, Decentralizing privacy: Using blockchain to protect personal data (5/2015), 2015 IEEE Security and Privacy Workshops, pp. 180-184

[5] Eduardo Castelló Ferrer, Thomas Hardjono, Alex 'Sandy' Pentland, Marco Dorigo, (2021) Secure and secret cooperation in robotic swarms, Science Robotics, Vol 6, Issue 56, arXiv:1904.09266, DOI: 10.1126/scirobotics.abf1538,

[6] European Commission, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Vol. L119, pp. 1-88, 2016.

[7] European Commission, EU Data Governance Act (DGA), November 2020. Document 52020PC0767. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0767&from=EN

[8] Wikipedia, Github, https://en.wikipedia.org/wiki/GitHub. Accessed 14 Jan 2022.

[9] A. Pentland, Open Algorithms, in Trusted Data: A New Framework for Identity and Data Sharing, MIT Press 2019.

[10] European Commission, European Blockchain Service Infrastructure (EBSI), 2021. https://ec.europa.eu/cefdigital/wiki/display/EBSIDOC/General

[11] Australia DFAT, *Australia-Singapore Digital Economy Agreement – Fact Sheet*, December 2020. https://www.dfat.gov.au/sites/default/files/australia-singapore-digital-economy-agreement-fact-sheet_0.pdf