BLOCKCHANGE

Blockchain Technologies for Social Change

FIELD REPORT

On the Emergent Use of Distributed Ledger Technologies for Identity Management

Stefaan G. Verhulst and Andrew Young

AUTHORS

Stefaan G. Verhulst and Andrew Young

(with support from Raul Zambrano, Joyce Zhang,
Michelle Winowatan, Juliet McMurren, and Olivia Clark)

ADVISORY GROUP

Andrew Hoppin, Arun Sundarajan, Audrey Tan, Cara Lapointe, Carlos Santiso, and Marta Piekarska

PEER REVIEWERS

Alexey Musatov, Camilo Urbano, Christos Tsolkas, Kaliya Young, Manuel Vicente Zometa, and Marco Konopacki

METHODS

Case Study; Extensive Literature Review, Interviews and Additional Desk Research

GOVLAB

BLOCKCHANGE

Blockchain Technologies for Social Change

FIELD REPORT

On the Emergent Use of Distributed Ledger Technologies for Identity Management

Stefaan G. Verhulst and Andrew Young

CONTENTS

6
Foreword
–
Blockchain Technologies, Information Asymmetries and Social Change

12
Introduction
–
Blockchain for Social Change

18
Blockchange Primer
–
Introduction to a Rapidly Evolving Technology and Its Potential for Enabling Social Change

28
Blockchange Attributes and Use Cases
–
A More Nuanced View

40
Blockchange and Identity
–
The Foundational Use Case

58
Lessons Learned
–
Cross-Cutting Challenges and Operational Conditions

72
Conclusion: GENESIS
–
Design Principles for Blockchange

FOREWORD: BLOCKCHAIN TECHNOLOGIES, INFORMATION ASYMMETRIES AND SOCIAL CHANGE 6

INTRODUCTION — BLOCKCHAIN FOR SOCIAL CHANGE 12

- Purpose of this Field Report 14
- Summary of Findings 16

PART 1: BLOCKCHANGE PRIMER – INTRODUCTION TO A RAPIDLY EVOLVING TECHNOLOGY AND ITS POTENTIAL FOR ENABLING SOCIAL CHANGE 18

- Narratives Associated with Blockchain for Social Change 20
- Glossary of Terms 22
- Blockchain Guides 24

PART 2: BLOCKCHANGE ATTRIBUTES AND USE CASES — A MORE NUANCED VIEW 28

- Matrix of Blockchain Technologies 30
- Blockchain Core Attributes: Immutability, Integrity, and Resilience 32
- Blockchain Optional Attributes: Disintermediation, Transparency and Accessibility 34
- Three Types of Blockchange Applications: Track and Trace, Smart Contracts, Identity 36

PART 3: BLOCKCHANGE AND IDENTITY — THE FOUNDATIONAL USE CASE 40

- Why Identity Matters for Social Change 44
- Why Identity Matters for Blockchange 46
- Beyond Attributes – Challenges and Opportunities Across the Identity Lifecycle 48
- Stages of the Identity Lifecycle 48
- Current Challenges Throughout the Identity Lifecycle 50
- Promise of Blockchain for Addressing Challenges Across the Identity Lifecycle 52
- The Blockchain Identity Paradigm Change 54
- Maturity of Blockchange Experiments Across the Identity Lifecycle 56

PART 4: LESSONS LEARNED – CROSS-CUTTING CHALLENGES AND OPERATIONAL CONDITIONS 58

- Cross-Cutting Challenges: User Interfaces, Incentives, Legal and Policy Uncertainty, Technical Inefficiencies, Risk and Impact Measurement 62
- Enabling Operational Conditions: Problem, Data & Tech, and Ecosystem 66

PART 5: CONCLUSION: GENESIS – DESIGN PRINCIPLES FOR BLOCKCHANGE 72

FOREWORD

Blockchain Technologies, Information Asymmetries and Social Change[1]

We live in a data age, and it has become common to extol the transformative power of data and information. It is now conventional wisdom to assume that many of our most pressing public problems—everything from climate change to terrorism to mass migration—are amenable to a "data fix."

The truth, though, is a little more complicated. While there is no doubt that data—when analyzed and used responsibly—holds tremendous potential, many factors affect whether, and to what extent, that potential will ultimately be fulfilled.

Our ability to address complex public problems using data depends vitally on how our data ecosystems are designed (including how questions over representation, power and data stewardship are addressed). Design shortcomings may prevent us from addressing complex public problems and may also be responsible for many societal failures and inequalities. Information asymmetries are among the most common, and most persistent, of these shortcomings. They manifest when:

- some actors have better access to data than others;
- data is of poor quality (or even "fake"), contains implicit bias, and/or is unvalidated and thus not trusted;
- information is stove-piped, siloed, and generally difficult to access.

1 Originally published at: Stefaan Verhulst, "Information Asymmetries, Blockchain Technologies, and Social Change," Medium, July 24, 2018, https://medium.com/@sverhulst/information-asymmetries-blockchain-technologies-and-social-change-148459b5ab1a

Consider, for instance, examples of some of the transaction costs, power inequities and other obstacles that may result from information asymmetries:

- At the individual level, someone who is trying access services, for example opening a bank account, or signing up for new cell phone service, is often unable to provide all the requisite information, such as credit history, proof of address or other confirmatory and trusted attributes of identity. Information asymmetries are in effect limiting this individual's access to financial and communications services.
- At the corporate level, a vast body of literature[2] in economics has shown how uncertainty over the quality and trustworthiness of data can impose transaction costs, limit the development of markets for goods and services, or shut them down altogether. This is the well-known "market for lemons" problem[3] made famous in a 1970 paper of the same name by George Akerlof.
- At the government or societal level, information asymmetries don't just affect the efficiency of markets or social inequality. They can also incentivize unwanted behaviors that cause substantial public harm. Tyrants and corrupt politicians thrive on limiting their citizens' access to information (e.g., information related to bank accounts, investment patterns or disbursement of public funds). Likewise, criminals operate and succeed in the information-scarce corners of the underground economy.

These problems are now becoming more widely recognized. Several observers have for example pointed to the relationship between information asymmetries and corruption,[4] financial exclusion,[5] global pandemics,[6] forced mass migration,[7] human rights abuses,[8] and electoral fraud.[9] In many ways, in virtually all parts of the world, the potential of our data economy and society is being severely limited by design shortcomings that cause or in some cases exacerbate existing information asymmetries. We need a solution—a better way to handle information.

2 "Secrets and agents." The Economist, July 23, 2016. https://www.economist.com/economics-brief/2016/07/23/secrets-and-agents

3 George A. Akerlof. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." The Quarterly Journal of Economics, August 1970. https://www.jstor.org/stable/1879431?seq=1#page_scan_tab_contents

4 Melanie Manion. "Corruption by Design: Bribery in Chinese Enterprise Licensing." The Journal of Law, Economics, and Organization, April 1996. https://academic.oup.com/jleo/article/12/1/167/896197

5 George Okello Candiya Bongomin, et al. "Financial intermediation and financial inclusion of poor households: Mediating role of social networks in rural Uganda." Cogent Economics & Finance, 2017. https://www.tandfonline.com/doi/pdf/10.1080/23322039.2017.1362184

6 Harvey Rubin. "Future Global Shocks: Pandemics." Organisation for Economic Co-operation and Development, 2011. https://www.oecd.org/gov/risk/46889985.pdf

7 Kelly M. Greenhill. "Weapons of Mass Migration: Forced Displacement, Coercion, and Foreign Policy." Cornell University Press, 2010. http://www.cornellpress.cornell.edu/book/?GCOI=80140100627270

8 Yonatan Lupu. "Best Evidence: The Role of Information in Domestic Judicial Enforcement of International Human Rights Agreements." Department of Political Science, University of California-San Diego, 2013. https://pdfs.semanticscholar.org/b8cb/cfa41b4fc07927db8d0393f8e722ad3128a0.pdf

9 Nadia Heninger. "Computational Complexity and Information Asymmetry in Election Audits with Low-Entropy Randomness." Princeton University. https://www.cis.upenn.edu/~nadiah/papers/election-auditing/election-auditing.pdf

Blockchain Technologies and Information Asymmetries

This is where blockchain comes in. At their core, blockchain technologies offer new capacity for increasing the immutability, integrity, and resilience of information capture and disclosure mechanisms, fostering the potential to address some of the information asymmetries described above. By leveraging a shared and verified database of ledgers stored in a distributed manner, blockchain seeks to redesign information ecosystems in a more transparent, immutable, and trusted manner. Solving information asymmetries may turn out to be the real contribution of blockchain, and this—much more than the current enthusiasm over virtual currencies—is the real reason to assess its potential.

It is important to emphasize, of course, that blockchain's potential remains just that for the moment—only potential. Considerable hype surrounds the emerging technology, and much remains to be done and many obstacles to overcome if blockchain is to achieve the enthusiasts' vision of "radical transparency[10]."

Blockchain Technologies and Traditional Means of Addressing Information Asymmetries

To date, information asymmetries needed to be overcome through a variety of institutional and 'signalling'[11] means. These include the enforcement of liability and traceability provisions[12] and/or disclosure requirements or monitoring[13] by well-known and trusted institutions; the establishment of industry standards or professional norms; reputation-based mechanisms[14]; or even "outcome-contingent" contracts[15] (where the buyer does not pay until the outcome of the service is known). Recent developments toward "open data[16]" or "open contracting[17]" as part of the move toward "open government[18]" can also be portrayed as efforts to prevent or address information (and power) asymmetries.

10 Marshall Brown. "Will Blockchain Unchain The World?" Forbes, November 16, 2017. https://www.forbes.com/sites/marshallbrown/2017/11/16/will-blockchain-unchain-the-world/#2fe52864224f

11 Tamilla Mavlanova, et al. "Signaling theory and information asymmetry in online commerce." Information and Management, July 2012. https://www.sciencedirect.com/science/article/pii/S0378720612000444

12 Jill E. Hobbs. "Information asymmetry and the role of traceability systems." Agribusiness, October 4, 2004. https://onlinelibrary.wiley.com/doi/abs/10.1002/agr.20020

13 Ferdinand A. Gul and Han Qiu. "Legal Protection, Corporate Governance and Information Asymmetry in Emerging Financial Markets." February 8, 2002. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=298169

14 Gerald Bloom, et al. "Markets, information asymmetry and health care: Towards new social contracts." Social Science and Medicine, May 2008. https://www.sciencedirect.com/science/article/pii/S0277953608000592

15 "Contingent contract." Wikipedia. https://en.wikipedia.org/wiki/Contingent_contract

16 "Open Data's Impact." The Governance Lab. http://odimpact.org/

17 Open Contracting Partnership. https://www.open-contracting.org/

18 "Opening Governance." The Governance Lab. http://opening-governance.org/

These institutional solutions, however, are dependent not just upon strong and trusted societal intermediaries but also upon an individual's ability to access those intermediaries, or leverage the data made available. This in large part explains why information asymmetries tend to affect less developed countries[19], and already marginalized populations, more. Such groups simply have a harder time accessing and leveraging traditional methods to mitigate information asymmetries.

Blockchain technologies may offer a more distributed, more egalitarian and democratic alternative to these institutional solutions. In doing so, they may serve as mechanisms not just to reduce information asymmetries, but also to address powerful and deeply entrenched social and economic inequalities. At the moment, however, this remains mere potential, and it is entirely possible that blockchain may itself ultimately rely on the same types of institutions and trust-providing mechanisms[20] (i.e., in the form of new information-verification intermediaries). Similarly, recent developments toward more private and permission-based blockchains may actually create new or reinforce existing information asymmetries instead of dismantling them (as we have seen with certain identity[21] and smart contracting[22] initiatives). Thus, while the potential is clear, the jury is still out on what blockchain's actual impact will be.

This Field Report seeks to collect and organize what is known about blockchain and its capacity for creating positive social change by addressing information asymmetries, especially in the field of identity. The report is intended to contribute to a more sophisticated exploration and dialogue regarding the promise and practice of Blockchain to achieve social change. Even as the technology continues to develop rapidly, big questions remain about its potential and actual applicability. This document marks the first of a wider set of conversations and examinations that the GovLab hopes to facilitate as the technology (and our understanding of it) continue evolving. As such, we would be delighted to hear from you if you have any ideas on how we can expand and improve the current state of insights into blockchain and its potential for social impact.

19 Lawrence Lessig. "Thinking Through Law and Code, Again." COALA's Blockchain Workshops, 2015. https://www.youtube.com/watch?v=pcYJTIbhYF0

20 Dominika Latusek and Alexandra Gerbasi. "Trust and Technology in a Ubiquitous Modern Environment: Theoretical and Methodological Perspectives." IGI Global, 2010. https://www.igi-global.com/book/trust-technology-ubiquitous-modern-environment/37347#table-of-contents

21 Ananya Bhattacharya. "Blockchain is helping build a new Indian city, but it's no cure for corruption." Quartz, July 17, 2018. https://qz.com/india/1325423/indias-andhra-state-is-using-blockchain-to-build-capital-amaravati/

22 Primavera De Filippi and Samer Hassan. "Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code." First Monday, University of Illinois at Chicago Library, 2016. https://arxiv.org/abs/1801.02507

INTRODUCTION – BLOCKCHAIN FOR SOCIAL CHANGE

Purpose of This Field Report

Blockchain technologies are digital ledgers that provide one or more permanent and validated records in a distributed manner, with the possibility to provide a level of guaranteed privacy and security, data integrity, and increased trust. The disruptive potential of blockchain technologies (hereafter referred to simply as ‘blockchain’), and distributed ledger technologies (DLTs) more generally,[23] extends beyond private-sector innovation in products, services, revenue streams and industry operating systems. Blockchain is increasingly believed to be capable of positively empowering underserved populations in a myriad of ways,[24] including by providing a means for establishing a trusted digital identity. As such, blockchain is seen as an avenue for creating positive social change, or “Blockchange.”

Yet for all the enthusiasm, we in fact know very little about how blockchain can impact social change — what kinds of applications serve what needs, what technological attributes matter most, what risks are involved, and under what conditions blockchain can have maximum impact. This Blockchange Field Report shares early findings from the GovLab’s research initiative on blockchain’s potential for improving people’s lives, with a particular focus on the emergent universe of Blockchange as it relates to identity. This focus is based on the need for trusted identifiers in accessing a number of rights and services, from banking to the ballot box, as well as identity’s role as an enabler of blockchain-enabled smart contracting and track and trace interventions. As we explain further below, identity is in effect emerging as a core aspect of blockchain and Blockchange, a nexus for many of the associated issues and a vital lever for positive social change.

23 Anthony Stevens. “Gaining clarity on key terminology: Bitcoin versus blockchain versus distributed ledger technology.” Hacker Noon, April 23, 2018. https://hackernoon.com/gaining-clarity-on-key-terminology-bitcoin-versus-blockchain-versus-distributed-ledger-technology-7b43978a64f2

24 David Hessekiel. “The Future Of Social Impact Is…Blockchain.” Forbes, April 3, 2018. https://www.forbes.com/sites/davidhessekiel/2018/04/03/the-future-of-social-impact-is-blockchain/2/#5b7260de264f

This field report was developed through a yearlong research project, supported by the Rockefeller Foundation. Our methodology took the form of desk research and literature analysis of current theory, practice and dominant narratives in the blockchain and identity spaces – and at the nexus of the two – as well as the development of eight case studies on specific Blockchange for identity projects and pilots. Those case studies, included in Appendix 1, were developed through in-depth interviews with stakeholders involved in their implementation.

The report has five parts. The first provides a curated primer on key narratives, terms, and guides to blockchain and its potential for creating social change. Part two highlights blockchain's core and optional attributes and describes three categories of social change use cases.[25] The third part dives into the area of identity, analyzing the current and potential value of blockchain across the identity lifecycle, and highlighting findings from case studies completed by the research team. Part four brings all of the above together by discussing lessons learned related to operational conditions that can help to enable successful Blockchange initiatives, as well as cross-cutting challenges. Finally, part five concludes with a set of principles aimed at providing guidance on how to design Blockchange interventions in the identity space that are legitimate, effective, ethical, and impactful.

25 Our study is not focused on cryptocurrency systems, like the Bitcoin blockchain, that could be put to use to achieve social change objectives; rather, our inquiry is uniquely interested in uses of blockchain as a potential protocol for good.

Summary of Findings

PREMISE 1:

Blockchain technologies are rapidly evolving and subject to constant innovation but also facing deep constraints that impede widespread adoption and broad application.

PREMISE 2:

The core attributes of immutability, (guaranteed) integrity and distributed resilience of blockchain and other Distributed Ledger Technologies (DLTs) have potential for social impact that extends far beyond merely transforming the way industry records and manages transactions.

PREMISE 3:

Blockchains and DLTs are not monolithic concepts, and different types (e.g., private vs. public and permissioned vs. permissionless blockchains) possess varying, optional attributes, which include disintermediation, transparency, and accessibility.

PREMISE 4:

The combination of these core and optional attributes allows for three broad types of blockchain applications that could benefit social change or "blockchange applications": Identity Management, Track and Trace, and Smart Contracting.

PREMISE 5:

Of those three types of "blockchange applications," Identity Management – as it relates to people, tangible objects, and intangible objects – appears to be foundational because it a) plays a prominent role in social change; b) underpins most other blockchange applications; c) provides a necessary missing ID protocol layer on the Internet.

PREMISE 6:

Identity is not just a set of attributes; it involves a process composed of provisioning, authentication, administration, authorization, and auditing. Each stage has its own unique challenges, each of which may be addressed by mobilizing relevant blockchain attributes.

PREMISE 7:

Blockchange use cases are not equally applicable or mature across the identity lifecycle. It appears that blockchain provides the most potential to improve the authorization and auditing stages of the identity lifecycle – with implications for human rights, national security, voting, and financial services, among many other topic areas.

PREMISE 8:

Blockchange implementations are better suited for success when they are responsive to a number of operational conditions spread across four categories:

- **Problem**
  - Is there a clear problem definition?
  - Do information asymmetries and high transaction costs incentivize change?
- **Data & Tech**
  - Are accurate and high-quality digital records available?
  - Is there no availability of credible and alternative disclosure technologies?[26]
- **Ecosystem**
  - Are there trusted intermediaries active in the space and does their efficiency (or lack thereof) incentivize change?
  - Is there a level of cooperation (or 'co-opetition') among players?
- **Capacity**
  - Are the parties involved technology aware and data literate?

26 George A. Akerlof. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." The Quarterly Journal of Economics, August 1970. https://www.jstor.org/stable/1879431?seq=1#page_scan_tab_contents

PREMISE 9:

Blockchain can promote positive social change by improving the way we provide and manage identity, yet more effort will be required to address some of its current cross-cutting challenges, including: governance structure(s), technological interoperability, scalability, generalized adoption, user experience, and a rights-based approach.

PREMISE 10:

Moving forward, it will be essential for the social change field to define and adopt design principles to maximize the benefits of blockchain while preventing possible risks or harms. A preliminary list of foundational design principles would include:

- **G**overnance Legitimacy
- **E**thically Sound
- **N**ot Technology, But Solutions
- **E**cological Footprint
- **S**ynchronized with Existing Initiatives
- **I**nteroperability and Open Standards
- **S**ecuring first block accuracy

BLOCKCHANGE PRIMER

Blockchain is a complex and emerging technology, and its potential for creating positive social change has led to innovation, optimism, hype, and confusion in equal order. In Part 1, we seek to provide a brief primer on blockchain and the potential for using the technology to create Blockchange. This primer comprises a curation of illustrative quotes from experts regarding blockchain's capacity to create social change, a glossary of key terms relevant for this Blockchange study (with a focus on identity), and a curation of blockchain guides to provide the type of technical and operational understanding needed to engage with the field.

Narratives Associated with Blockchain for Social Change

The following quotes seek to provide an illustrative sample of expert viewpoints regarding the potential of blockchain to succeed (or fail) in creating positive social change.

“The blockchain is a disruptive technology with a tremendous transformative potential for our societies. Risks and benefits related to its possible applications, however, must be carefully weighted, avoiding utopian expectations, as well as the pitfalls of technocratic reasoning and determinism.[27]

MARCELLA ATZORI, PH.D.
UCL Center for Blockchain Technologies

“While blockchain’s best-known, most used and highest-impact application is Bitcoin, the potential impact of the technology is much greater and wider than virtual currencies. Indeed, since other applications can ‘piggyback’ the Bitcoin blockchain, the biggest impacts of Bitcoin may be found outside the currency domain.[28]

PHILIP BOUCHER, SUSANA NASCIMENTO, AND MIHALIS KRITIKOS
European Parliamentary Research Service

“Blockchain technology could simplify the management of trusted information, making it easier for government agencies to access and use critical public-sector data while maintaining the security of this information.[29]

STEVE CHENG, MATTHIAS DAUB, AXEL DOMEYER, AND MARTIN LUNDQVIST
McKinsey & Company

27 Marcella Atzori. “Blockchain Technology and Decentralized Governance: Is the State Still Necessary?” Journal of Governance and Regulation, March 2017. https://www.researchgate.net/publication/315919685_Blockchain_technology_and_decentralized_governance_Is_the_state_still_necessary

28 Philip Boucher, Susana Nascimento, and Mihalis Kritikos. “How blockchain technology could change our lives.” European Parliamentary Research Service, February 2017. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

29 Steve Cheng, Matthias Daub, Axel Domeyer, and Martin Lundqvist. “Using blockchain to improve data management in the public sector.” McKinsey & Company, February 2017. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/using-blockchain-to-improve-data-management-in-the-public-sector?cid=other-eml-alt-mip-mck-oth-1703

> The blockchain could offer people access to alternative currencies, global markets, automated and trustless transactions systems, self-enforcing smart contracts, smart property and cryptographically activated assets, and innovative models of governance based on transparency and corruption-free voting. Combined, these elements could be used to promote individual freedoms and user autonomy. Regardless of nationality, people could be granted equal access to basic digital institutions and infrastructure such as decentralized laws, markets, judiciaries, and payment systems, which can be customized to each country's, group's, and individual's needs.[30]

AARON WRIGHT AND PRIMAVERA DE FILIPPI
Authors, Blockchain and the Law: The Rule of Code

> ...[W]hat if there were not only an Internet of information, but an Internet of value. Some kind of vast, global, distributed ledger running on millions of computers and available to everybody, and where every kind of asset from money to music could be stored, moved, transacted, exchanged, and managed, all without powerful intermediaries.[31]

DON TAPSCOTT
Author, Blockchain Revolution

> Blockchain technology will not solve all government problems, but it can help curb corruption and instill trust in government.[32]

CARLOS SANTISO
Head of Innovation for Citizen Services Division at Inter-American Development Bank

> Blockchain is not going to solve all your problems for you,....You're a hammer-thrower just looking for nails. [When you have technology in search of a use] you end up with crap that we see out there in the enterprise today.[34]

JIMMY SONG
Blockchain Capital

> ...blockchain is one of the most overhyped technologies ever.... Ultimately, blockchain's uses will be limited to specific, well-defined, and complex applications that require transparency and tamper-resistance more than they require speed – for example, communication with self-driving cars or drones. As for most of the coins, they are little different from railway stocks in the 1840s, which went bust when that bubble – like most bubbles – burst.[33]

NOURIEL ROUBINI
New York University
Stern School of Business

30 Aaron Wright and Primavera De Filippi. "Decentralized Blockchain Technology and the Rise of Lex Cryptographia." March 10, 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664

31 Don Tapscott. "How the blockchain is changing money and business." TEDSummit, June 2016. https://www.ted.com/talks/don_tapscott_how_the_blockchain_is_changing_money_and_business

32 Carlos Santiso. "Will Blockchain Disrupt Government Corruption?" Stanford Social Innovation Review, March 5, 2018. https://ssir.org/articles/entry/will_blockchain_disrupt_government_corruption

33 Nouriel Roubini and Preston Byrne. "The Blockchain Pipe Dream." Project Syndicate, March 5, 2018. https://www.project-syndicate.org/commentary/blockchain-technology-limited-applications-by-nouriel-roubini-and-preston-byrne-2018-03

34 Erin Griffith. "When the blockchain skeptic walked into the lions' den". Wired, April 15, 2018. https://www.wired.com/story/when-the-blockchain-skeptic-walked-into-the-lions-den/

Glossary of Terms

This glossary of terms is provided to set the stage for the following sections – particularly our examination of blockchain's potential for creating social change in the identity space – and to clarify a number of important concepts with multiple or contested definitions.

Blockchain	"In layperson's terms, blockchains can be defined as a public spreadsheet that sequentially records transactions among users operating within a decentralized peer-to-peer network. Every network node stores an up-to date copy of the data and updates automatically diffuse among all nodes." **International Development Research Centre**[35]
Distributed Ledger Technology (DLT)	"A distributed ledger is essentially an asset database that can be shared across a network of multiple sites, geographies or institutions. All participants within a network can have their own identical copy of the ledger. Any changes to the ledger are reflected in all copies in minutes, or in some cases, seconds." **United Kingdom Government Chief Scientific Advisor**[36]
Social Change **Synonyms: Social Impact**	"Social change is the significant alteration of social structure and cultural patterns through time." **Oxford Bibliographies**[37]

35 Raúl Zambrano. "Blockchain." International Development Research Centre, August 2017. https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf

36 UK Government Chief Scientific Adviser. "Distributed Ledger Technology: beyond block chain." Government Office for Science, 2016. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf

37 Kevin T. Leicht. "Social Change." Oxford Bibliographies. http://www.oxfordbibliographies.com/view/document/obo-9780199756384/obo-9780199756384-0047.xml

Identity **Variation: Digital Identity**	Identity is "an attribute or set of attributes that uniquely describe a subject within a given context." "Digital identity is the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service, but does not necessarily need to uniquely identify the subject in all contexts." **National Institute of Standards and Technology**[38]
Identity (and Access) Management	"Identity and access management (IAM) is the security discipline that enables the right individuals to access the right resources at the right times for the right reasons." **Gartner**[39]
Functional ID	Identities that "evolve out of a single usecase, such as voter ID, health records, or bank cards, and have potential for use across sectors." **World Bank**[40]
Foundational ID	"Foundational systems...are intended primarily to provide identity as a public good, not to supply a specific service. Foundational systems are typically owned and operated by government institutions, aim for national coverage of their population, and provide credentials that function as an official ID. Foundational ID systems can also underlie multiple functional purposes." **United States Agency for International Development**[41]

38 Paul A. Grassi, Michael E. Garcia, and James L. Fenton. "Digital Identity Guidelines." National Institute of Standards and Technology, June 2017. https://pages.nist.gov/800-63-3/sp800-63-3.html#def-and-acr

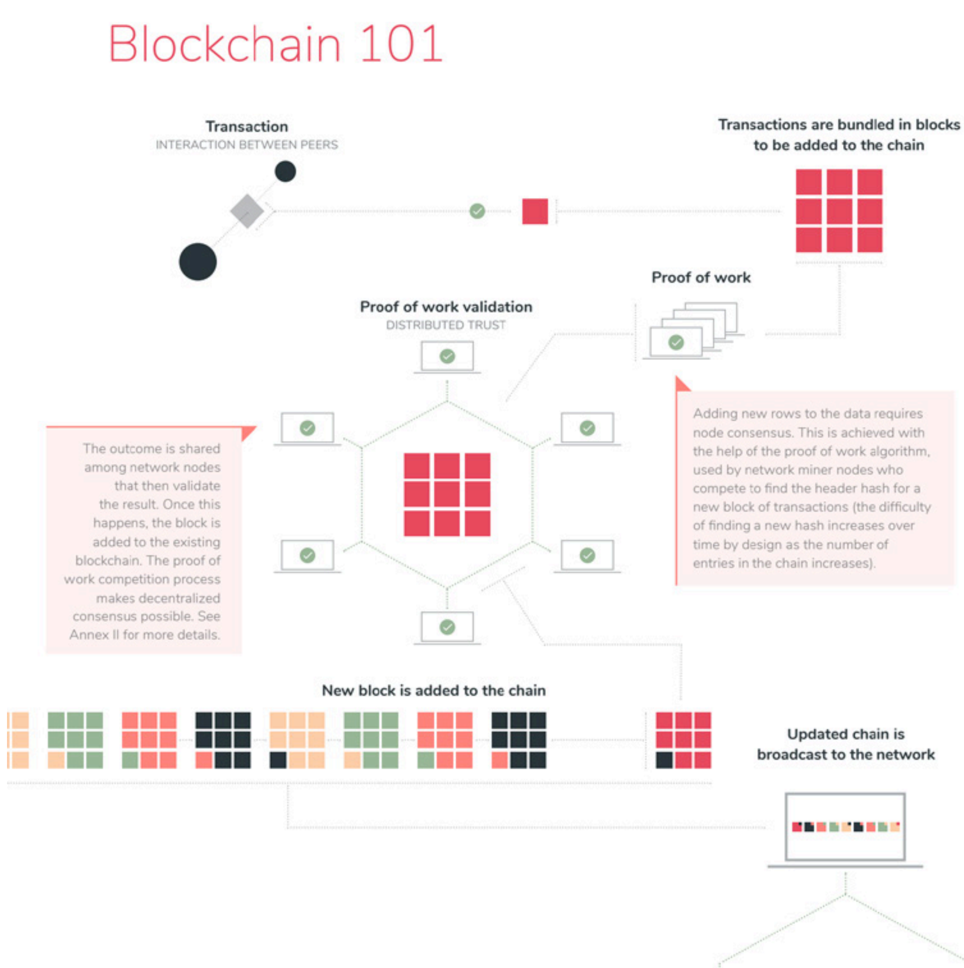
39 "Identity and Access Management (IAM)." Gartner IT Glossary. https://www.gartner.com/it-glossary/identity-and-access-management-iam/

40 Joseph J. Atick and Zaid Safdar. "Digital Identity Toolkit: A Guide for Stakeholders in Africa." World Bank Group, June 2014. http://documents.worldbank.org/curated/en/147961468203357928/pdf/912490WP0Digit00Box385330B00PUBLIC0.pdf

41 "Identity in a Digital age: Infrastructure for Inclusive Development." United States Agency for International Development. https://www.usaid.gov/sites/default/files/documents/15396/IDENTITY_IN_A_DIGITAL_AGE.pdf

Blockchain Guides

A blockchain is a distributed database that seeks to solve problems of trust, transparency, and accountability during a transaction or interaction between two parties. Using advanced cryptography, each block of data is sequentially added to the chain across a network of computers, or nodes. Thus, the information is not only decentralized but also distributed, which means no single person or entity controls the system, yet everyone (at least in a permissionless, public blockchain) can use and help run it. Distributed ledger technology frameworks intend to eliminate the need for and reliance on central authorities such as banks, large enterprises and governments as intermediaries in a wide array of transactions.



Blockchain 101 from the International Development Research Centre.[42]

42 Raúl Zambrano. "Blockchain." International Development Research Centre, August 2017. https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf

Although the preceding short introduction provides essentially all of the technical and operational information needed to understand this field report, the following curated list of blockchain guides includes a number of deeper explorations of blockchain; blockchain protocols; current applications, especially in the business world; technical guidance; and other DLTs.

Blockchain Basics

What is Blockchain Technology? A Step-by-Step Guide for Beginners Ameer Rosic *BlockGeeks*	BlockGeeks' Guide provides an overview of the central characteristics and defining principles of blockchain technology.
What is Blockchain Technology? Nolan Bauerle *CoinDesk*	CoinDesk's introduction to blockchain technology; includes an index of FAQs related to Bitcoin, Ethereum, and other cryptocurrencies.
CIO Explainer: What Is Blockchain? Steven Norton *The Wall Street Journal*	This Wall Street Journal article gives a holistic overview of blockchain – how it works, how it started, how it can be used, challenges it faces, and the current ecosystem (as of 2016).
A Complete Beginner's Guide To Blockchain Bernard Marr *Forbes*	This short article from Forbes explains the basics of what blockchain is, how it works, and why it is important.
Blockchain 101: An introduction Jedidiah Bracy *IAPP*	An introduction to blockchain that includes videos on the history of double-spending in finance and how hashing works within cryptocurrencies.
HBR Whiteboard Session: How Does Blockchain Work? Karim Lakhani *Harvard Business School Digital Initiative*	In this brief video, Professor Lakhani explains the fundamentals of blockchain and why they are important, across industries.

Bitcoin, Ethereum and Smart Contracts

A simple guide to Bitcoin Olivia Solon *Wired*	This piece from Wired focuses especially on key bitcoin fundamentals such as mining, how to buy bitcoin, exchange security, volatility, and 51 percent attacks.
What is Ethereum? A Step-by-Step Beginners Guide Ameer Rosic *BlockGeeks*	BlockGeeks' Guide explains what Ethereum is, how it works and what it can be used for.
A Beginner's Guide to Smart Contracts Ameer Rosic *BlockGeeks*	BlockGeeks' Guide explains what a smart contract is, how it can be created using blockchain, and examples of how smart contracts could benefit various industries.

Blockchain for Business & Real-World Applications

Are you ready for blockchain? *Thomson Reuters*	This Thomson Reuters report details a number of blockchain projects, provides insights from blockchain applications across different industries, and considers which blockchain use cases will become mainstream.
Blockchain basics Sloane Brakeville & Bhargav Perepa *IBM*	IBM's guide focuses on distributed ledgers and blockchain, particularly those using Hyperledger. Hyperledger is an open-source project to support the development of blockchain-based distributed ledgers for business use.
How blockchain will radically transform the economy Bettina Warburg *TEDSummit*	A TED talk on how blockchain technology can be applied in the real world and create changes in the economy
How the blockchain is changing money and business Don Tapscott *TEDSummit*	A TED talk that demystifies blockchain and explains how it holds the potential to transform money, business, government, and societ

Technical

Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto *www.bitcoin.org*	The original bitcoin whitepaper from Satoshi Nakamoto describes the digital currency as a solution to the double-spending problem by creating a peer-to-peer network. Interestingly, there is no specific mention of "blockchain" throughout the entire paper.
Learn Blockchains by Building One Daniel van Flymen *Hacker Noon*	This article from Hacker Noon takes readers step-by-step through the process of building a blockchain.
An Introduction to Ethereum and Smart Contracts: Bitcoin and the Blockchain Sebastián Peyrott *DZone*	This piece from DZone explains with code how Bitcoin, Ethereum, and smart contracts mitigate the problem of double-spending.

Beyond Blockchain: Other DLTs

Hedera Hashgraph Thinks It Can One-Up Bitcoin And Ethereum With Faster Transactions Jeff Kauflin *Forbes*	This Forbes article examines Hedera and IOTA – two DLTs that do not use a traditional blockchain; both the IOTA Tangle and Hedera Hashgraph are based on the mathematical approach called a directed acyclic graph (DAG).
Comparison of Ethereum, Hyperledger Fabric and Corda Martin Valenta & Philipp Sandner *Frankfurt School Blockchain Center*	This working paper compares the most notable differences between Hyperledger Fabric, R3 Corda, and Ethereum, toward providing decision-makers with insight on what use cases are most suitable for each DLT.

BLOCKCHANGE ATTRIBUTES AND USE CASES – A MORE NUANCED VIEW

Matrix of Blockchain Technologies

As a result of ongoing experimentation, development and investment in blockchain and distributed ledger technologies for a variety of purposes and by a variety of stakeholders, there is no single blockchain technology, but rather a variety of approaches (and hybrids of those approaches). Decisions from implementers regarding which flavor of blockchain to leverage can have important business and governance implications.

Broadly, the following matrix of blockchain implementation options has emerged:

- **Public vs. Private**
  Public blockchains (e.g., Bitcoin, Ethereum) are designed so that anyone can view, browse or audit transactions. On the other hand, on private blockchains (e.g., Hyperledger and various business applications), the data is not publicly accessible.

- **Permissionless vs. Permissioned**
  The permissionless vs. permissioned dichotomy hinges on who has the rights to add or validate[43] block transactions on the chain.[44] For permissionless ledgers (e.g., the Bitcoin blockchain) anyone has the ability to write to the blockchain, whereas permissioned ledgers provide for a restricted set of users to write and authenticate transactions. In the latter case, the application is not truly decentralized, and might not be well-suited for addressing certain types of information asymmetry.

43 "Every computer in the network checks (validate) the transaction against some validation rules that are set by the creators of the specific blockchain network. Validated transactions are stored into a block and are sealt with a lock (hash). This block becomes part of the blockchain when other computers in the network validate if the lock on the block is correct". https://medium.com/ignation/pulling-the-blockchain-apart-the-transaction-life-cycle-7a1465d75fa3

44 Further complicating matters is the concept of hybrid or sidechains: "An additional area is the emerging concept of sidechain, which allows for different blockchains (public or private) to communicate with each other, enabling transactions between participants across blockchain networks." Blockchain: How this technology could impact the CFO role. Ernst & Young, 2017. https://www.ey.com/gl/en/industries/technology/ey-how-blockchain-technology-could-impact-the-cfo

PUBLIC PERMISSIONLESS

Who can see the result?
Everyone

Who can write to the blockchain/transact?
Anyone

Example: Bitcoin, Ethereum

PRIVATE PERMISSIONLESS

Who can see the result?
Select / Verified Participants

Who can write to the blockchain/transact?
Anyone

Example: Monax, Multichain, Federal Byzantine Agreement

PUBLIC PERMISSIONED

Who can see the result?
Everyone

Who can write to the blockchain/transact?
Select / Verified Participants

Example: Land titles, university degrees

PRIVATE PERMISSIONED

Who can see the result?
Select / Verified Participants

Who can write to the blockchain/transact?
Select / Verified Participants

Example: Medical records, KYC, AML

Blockchain Core Attributes: Immutability, Integrity, and Resilience

Although we often hear references to blockchain as a monolithic entity, it has become increasingly clear, especially as the field has evolved, that there is in fact no single blockchain technology. Rather, there are several variations of attributes that provide for different technological scenarios – for example, restrictions on the ability to view and/or contribute to the blockchain. So while blockchain technologies, and DLTs more broadly, are often treated as a single, homogenous innovation, in fact, the attributes of different blockchain implementations can vary widely, just as the resulting outcomes of those implementations will necessarily vary.

Despite these variations, some core attributes do remain foundational and (more or less) consistent across blockchain applications. In the following sections, we distinguish between those core attributes and those optional attributes that could exist in some, but not all, implementations.

IMMUTABILITY

Blockchain ledgers exhibit a level of immutability not present in other similar management systems.[45] While questions are increasingly arising on how immutable blockchains truly are,[46] in general terms, "it is nearly impossible to alter or falsify information on the blockchain."[47] Of course, this immutability helps to ensure that nearly all entries of information (including information that is corrected later in the chain) remain as "permanent legacies."[48]

(GUARANTEED) INTEGRITY

The distributed validation mechanisms that confirm additions to the blockchain cannot easily be manipulated to intentionally add low quality or inaccurate information to the blockchain. This integrity of user information and activity is also the result of automated capturing of transaction metadata for all activity undertaken on the chain.[49]

DISTRIBUTED RESILIENCE

The information security offered by blockchain arises from the distribution of information and agency across nodes in the blockchain. Data breaches can strike centralized databases, such as the infamous Equifax breach of 2017, but given the distributed nature of blockchain, a similarly effective attack would require "an attack on every copy of the ledger simultaneously."[50]

45 Some private permissioned blockchains and DLTs allow selected users and nodes to edit or delete records.

46 Christina Comben. "Are Blockchains Actually Immutable?" The Merkle, April 7, 2018. https://themerkle.com/are-blockchains-actually-immutable/

47 Raúl Zambrano. "Blockchain." International Development Research Centre, August 2017. https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf

48 Michael Mainelli. "Blockchain Will Help Us Prove Our Identities in a Digital World." Harvard Business Review, March 16, 2017. https://hbr.org/2017/03/blockchain-will-help-us-prove-our-identities-in-a-digital-world

49 Raúl Zambrano. "Blockchain." International Development Research Centre, August 2017. https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf

50 Philip Boucher, Susana Nascimento, and Mihalis Kritikos. "How blockchain technology could change our lives." European Parliamentary Research Service, February 2017. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf. However, note that so-called 51% attacks on blockchains have recently increased thus challenging its resilience. See http://newsaltcoins.com/51-percent-attacks-increase.

Blockchain Optional Attributes: Disintermediation, Transparency and Accessibility

While essentially all blockchain implementations exhibit some level of immutability, integrity, and resilience, many of the benefits most commonly cited by blockchain optimists and vendors are in fact largely optional—they depend on deliberate technical and design choices. Questions about what types of implementation yield what types of benefits will likely be central going forward for those seeking to use blockchain, whether in a business or social good setting. Here, we outline three of the most important – and potentially transformative – attributes of certain blockchain varieties.

DISINTERMEDIATION

Bitcoin, the original blockchain use case, was developed in order to create a disintermediated monetary system, allowing users to transact peer-to-peer without involving central banks. Blockchains, especially public ones, can enable such disintermediation, but not every implementation will necessarily cut out the middlemen – nor is the destruction of intermediaries always straightforward or desirable, as discussed in more detail below. A private, permissioned blockchain, for example, implemented with hand-selected nodes would exhibit vastly different levels of disintermediation compared to something like the Bitcoin blockchain. Blockchains can also generate a new set of intermediaries such as miners, exchanges and programmers specializing in smart contracts, for example.

TRANSPARENCY

In public blockchains, the entirety of information and metadata held on-chain is available to all users.[51] Only cryptographic hashes containing user information are publicly visible and information on all transactions is time stamped and available to all.[52] While all blockchain implementations make visible such information, different implementations can restrict access to a small set of pre-approved users to such an extent that transparency can not be reasonably attributed.

ACCESSIBILITY

Just as blockchain is often framed as a technology for disintermediation, narratives commonly describe how blockchain can create new levels of service accessibility, allowing previously disconnected individuals (e.g., the so-called "unbanked") to transact and access services without relying on traditional gatekeepers and third parties.[53] Again, while such accessibility improvements can be enabled through some blockchain implementations, others place limits on who can view or contribute to the chain. Some blockchain implementations are entirely on the "backend," meaning that individuals whose activity is represented on the blockchain do not necessarily need to be aware that they are contributing to the blockchain. This is the case, for instance, with the World Food Programme's Building Blocks project discussed more below and in Appendix 1.

51 Raúl Zambrano. "Blockchain." International Development Research Centre, August 2017. https://idl-bnc-idrc.dspacedirect.org/bitstream/handle/10625/56662/IDL-56662.pdf

52 Garrick Hileman and Michael Rauchs. "2017 Global Blockchain Benchmarking Study." September 22, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224

53 Philip Boucher, Susana Nascimento, and Mihalis Kritikos. "How blockchain technology could change our lives." European Parliamentary Research Service, February 2017. http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

Three Types of Blockchange Applications: Track and Trace, Smart Contracts, Identity

Blockchain is increasingly viewed as a transformative technology for creating social change. The meteoric rise of Bitcoin in many ways acted as a proof of concept for disrupting centralized legacy systems, particularly those that require high levels of trust between parties that otherwise lack clear incentives to trust one another. Blockchain is now seen as providing a potential solution to everything from homelessness in New York City[54] to the Rohingya crisis in Myanmar[55] to government corruption around the world.[56] Demonstrating the breadth of current experimentation, Stanford's Center for Social Innovation recently analyzed and mapped nearly 200 organizations and projects aimed at creating positive social change with blockchain.[57] Complementing this work, the GovLab is developing a mapping of Blockchange implementations[58] across regions and topic areas.

Informed by our analysis of the current field of practice, we identified three key types of Blockchange applications or use cases: Track and Trace, Identity, and Smart Contracts. In the following table, we desribe each of these use cases, provide examples of projects implemented across them, and identify the commonly cited social change objectives for such projects.

54 Ben Schiller. "This New Blockchain Project Gives Homeless New Yorkers A Digital Identity." Fast Company, December 6, 2017. https://www.fastcompany.com/40500978/this-new-blockchain-project-gives-homeless-new-yorkers-a-digital-identity

55 Beh Lih Yi. "Stateless Rohingya to get digital IDs with blockchain." Reuters, December 20, 2017. https://www.reuters.com/article/us-myanmar-rohingya-tech/stateless-rohingya-to-get-digital-ids-with-blockchain-idUSKBN1EE1VA

56 Laura Shin. "New Initiative Aims To Eliminate Corruption With Blockchain Technology." Forbes, June 20, 2017. https://www.forbes.com/sites/laurashin/2016/06/20/new-initiative-aims-to-eliminate-corruption-with-blockchain-technology/#542415641309

57 Doug Galen, Nikki Brand, et. al. "Blockchain for Social Impact Moving Beyond the Hype." Stanford Graduate School of Business Center for Social Innovation. https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype_0.pdf

58 Blockchange Repository. The Governance Lab, 2018. https://docs.google.com/spreadsheets/d/1AmzM2aDT-F03lSZs3QQYHlPw-vYdP4up-pR50TPO0X91Y/edit#gid=0

TRACK AND TRACE

Description

Improving the traceability of tangible and intangible objects as they, for example, are shared between parties or travel across supply chains.

Capacity for Addressing Information Asymmetries

The impact of blockchain is already starting to be felt in global supply chains, including in the pharmaceuticals and food industries. By immutably recording various steps in supply chains and other logistics chains, blockchain has the potential to reduce waste and fraud, crack down on duplicates and illicit products, and increase consumer safety. Blockchain in effect allows transparency watchdogs, as well as average consumers, to track the provenance of goods they purchase and consume, in the process leveraging the power of information so that consumers and citizens can make better choices.

Illustrative Examples

- Verisart[59] creates verifiable, digital certificates for art and collectibles which helps buyers ensure each piece's provenance.
- Grass Roots Cooperative[60] along with Heifer USA created a blockchain-powered app that allows every package of chicken marketed and sold by Grassroots to be traced on the Ethereum blockchain.
- Everledger[61] works with stakeholders across the diamond supply chain to track diamonds from mine to store.
- Ripe[62] is working with Sweetgreen[63] to use blockchain and IoT sensors to track crop growth, yielding higher-quality produce and providing better information for farmers, food distributors, restaurants, and consumers.

59 Verisart, 2018. https://www.verisart.com/

60 Grass Roots Farmers' Cooperative, 2017. https://grassrootscoop.com/

61 Everledger, 2018. https://diamonds.everledger.io/

62 Annie Massa. "Someone Figured Out How to Put Tomatoes on a Blockchain." Bloomberg, November 9, 2017. https://www.bloomberg.com/news/articles/2017-11-09/the-internet-of-tomatoes-is-coming-starting-with-boston-salads

63 Sweetgreen, 2016. https://www.sweetgreen.com/

IDENTITY

Description

A distributed system of trusted identifiers with some level of immutability that can allow for the confirmed and authenticated identification of people and objects.

Capacity for Addressing Information Asymmetries

The lack of verifiable, self-sovereign identities is emerging as one of the major problems of the information age, enabling everything from identity theft to privacy violations, new and existing forms of surveillance, and other forms of fraud. Today, citizens do not control their online presences, and this not only leads to immediate problems but erodes long-term trust in the entire data ecosystem. Several projects are underway to use blockchain to remedy this situation.

Illustrative Examples

- The State of Illinois is working with Evernym[64] to pilot digitization for birth certificates, to test the feasibility of giving individuals a digital identity from birth.
- BanQu[65] creates an economic passport for previously unbanked populations by using blockchain to record economic and financial transactions, purchase goods, and prove their existence in global supply chains.
- In 2015, AID:Tech[66] piloted a project working with Syrian refugees in Lebanon to distribute over 500 donor aid cards that were tied to non-forgeable identities.
- uPort[67] provides digital identities for residents of Zug, Switzerland to use for accessing governmental services.
- Identity Foundation[68] is a community-driven group of developers and organizations working toward an interoperable, decentralized identity ecosystem.[69]
- Bitnation[70] is the world's first Decentralised Borderless Voluntary Nation (DBVN). The website proof-of-concept, including the blockchain ID and Public Notary, is used by tens of thousands of Bitnation Citizens and Embassies around the world.

64 Evernym, 2013-2018. https://www.evernym.com/

65 BanQu, 2018. http://www.banquapp.com/

66 AID:Tec, 2017. https://aid.technology/

67 uPort, 2018. https://www.uport.me/

68 Identity Foundation. http://identity.foundation/

69 ID2020. https://id2020.org/

70 Bitnation, 2018. https://tse.bitnation.co/

SMART CONTRACTS

Description

Automated processes that take a particular, predefined action, triggered when another predefined action is executed and confirmed by blockchain nodes.

Capacity for Addressing Information Asymmetries

Much has been made of blockchain's potential for automated contracting. Smart contracting has the potential to reduce fraud and transaction costs for businesses, governments and citizens.[71] More generally, it has the potential to drastically simplify processes (by, for example, automating compliance and enforcement), thus opening up new business models and permitting average citizens to enter into complex and hitherto expensive arrangements with businesses, governments and each other. Smart contracting is an example of how existing information asymmetries can potentially be leveled and flattened, putting more power into the hands of citizens and consumers.[72]

At the same time, security concerns related to smart contract technologies (following several high profile hacks) suggests the need for a more cautious use.[73]

Illustrative Examples

- In Indonesia, Carbon Conservation[74] and Dappbase have created smart contracts that will distribute rewards to villages that can prove the successful reduction of incidences of forest fires.
- Alice[75] has built Ethereum-based smart contracts for a pilot donation project that supports 15 homeless people in London. The smart contracts ensure donations are released only when pre-determined project goals are met and aims to test a new and more transparent approach for donation platforms.
- Bext360[76] uses smart contracts to pay coffee farmers fairly and immediately based on a price determined through weighing and analyzing beans by the Bext360 machine at the source.
- BitLumens[77] uses smart contracts and solar panels to provide energy to areas lacking an operational power grid where costs would otherwise be prohibitive.

71 Blockgeeks, 2018. https://blockgeeks.com/guides/smart-contracts/

72 Lin William Cong and Zhiguo He. "Blockchain Disruption and Smart Contracts." May 22, 2018. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2985764

73 Sherman Lee, Blockchain Smart Contracts: More Trouble Than They Are Worth? July 10, 2018 Forbes. https://www.forbes.com/sites/shermanlee/2018/07/10/blockchain-smart-contracts-more-trouble-than-they-are-worth/#590c82e223a6

74 Carbon Conservation. http://www.carbonconservation.com/index.html

75 Alice, 2017. https://alice.si/

76 Bext360, 2018. https://www.bext360.com/

77 Bitlumens, 2018. https://bitlumens.com/

BLOCKCHANGE AND IDENTITY – THE FOUNDATIONAL USE CASE

The right to identity is a fundamental human right as defined by the United Nations Human Rights' 1989 Convention on the Rights of the Child.[78] While the initial definition of identity as a human right was focused particularly on children, the adoption of the Sustainable Development Goals (SDGs) further supported the concept, with SDG 16.9 setting the objective of "legal identity for all, including birth registration."[79]

The central importance of identity to human development and participation in society is now broadly recognized. Modern identity and access management (IAM) came into focus during the late 1930s, when a group of European countries began issuing national ID cards. During this time, creating a more systematic approach for establishing and authenticating the official use of trusted identities emerged. More recently, IAM has benefited from biometrics and the emergence of digital platforms and solutions. Digital identity is indeed becoming the default standard for most if not all forms of ID. Recent estimates suggest that over one hundred countries currently issue national ID cards of various sorts.

Of course, the universe of identity stretches far beyond government-issued, general purpose IDs assigned to individuals. Different institutions (colleges, companies, libraries, workplaces) issue their own identities, and most individuals also possess a wide array of different online identities for different services. In addition, and particularly with the proliferation of sensors and the IoT economy, objects and "things" (e.g., parts in a supply or shipping chain) now have their own identities. One of the central challenges of modern identity is its fragmentation and variation across platform and individuals. There are also issues related to interoperability between different forms of identity, and the fact that different identities confer very different privileges, rights, services or forms of access. The universe of identities is vast and manifold. Every identity in effect poses its own set of challenges and difficulties—and, of course, opportunities.

78 United Nations: Office of the High Commissioner for Human Rights. 1996-2018. http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx

79 Eric Burger and Clare Sullivan. "E-residency and blockchain." Computer Law & Security Review. Vol. 33(4) August 2017: 470-481. https://ac-els-cdn-com.proxy.library.nyu.edu/S0267364917300845/1-s2.0-S0267364917300845-main.pdf?_tid=489c84fc-cfa9-11e7-af64-00000aacb362&acdnat=1511371343_f774582ce0e99f042302ed53cd077d32

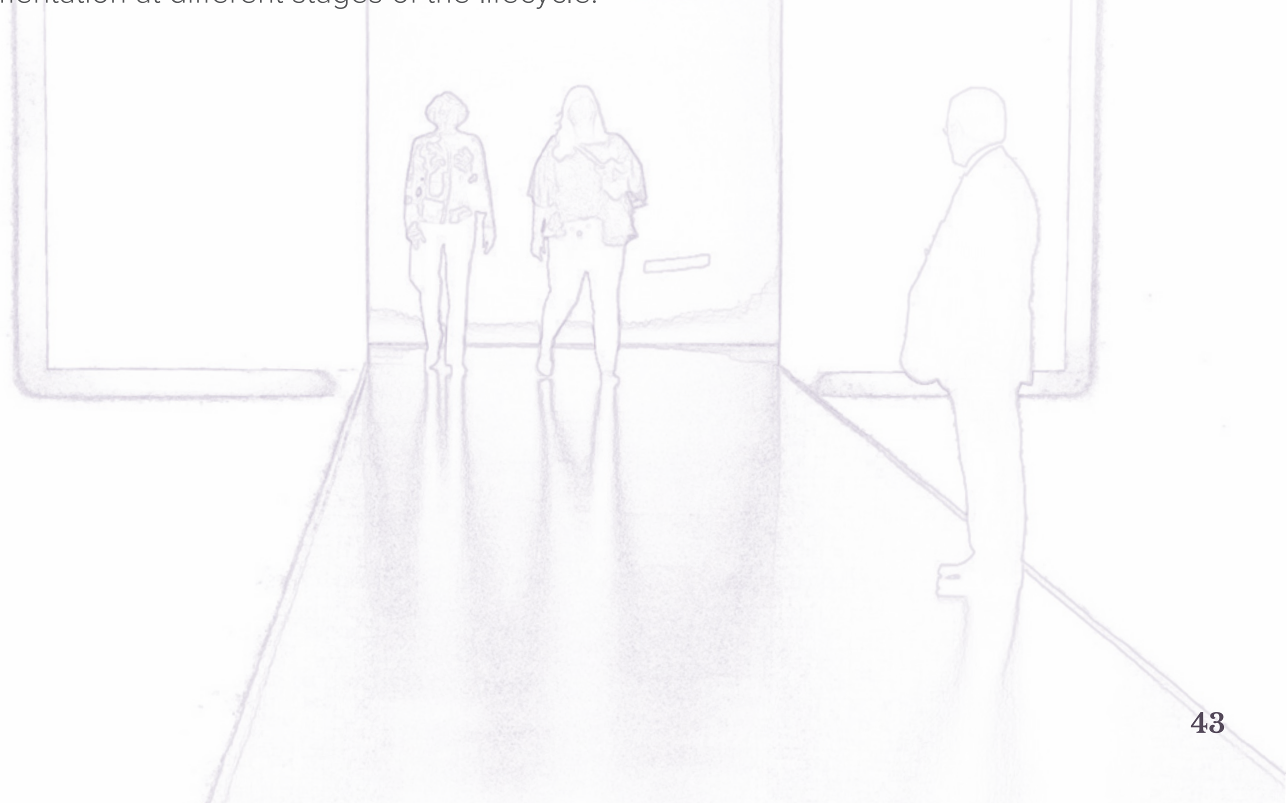
The contemporary IAM literature focuses on two central types of identity.[80] The first is foundational identity, which is usually equated with legal identity. Here, after collecting attributes, individuals are issued a unique ID that is legally recognized at the national level and can be used to access different services.[81] Legal IDs are almost always issued by the state in a centralized fashion. National ID cards are perhaps the best example of a foundational identity.

The second type is called functional or transactional ID. In this case, a particular entity, public or private, issues individuals or customers a unique ID that is only valid for the specific purposes previously established by the issuing entity. Electoral identities, health or car insurance cards, and ecommerce login credentials are good examples.

As the potential of blockchain to enable social change has grown, identity – and the need for more and better trusted identifiers across contexts – has regularly been flagged as an area of particular potential impact. Blockchain, it is felt, can help address many of the challenges related to identity, in issues related to identity fragmentation and interoperability. This report examines if, when, and how blockchain's attributes can unlock new value and address stubborn challenges at different stages of the identity lifecycle. In this section, we discuss in more detail why identity matters for creating social change, consider why identity is a foundational Blockchange use case, and examine the potential for blockchain to address problems at different stages of the lifecycle. In addition, we use our case study research to reflect on the maturity of experimentation at different stages of the lifecycle.

80 "Identification for Development: Strategic Framework" World Bank Group, January 25, 2016. http://pubdocs.worldbank.org/en/179901454620206363/Jan-2016-ID4D-Strategic-Roadmap.pdf

81 Passports are issued nationally but recognized internationally. In countries where no national ID card exist, passports can be used as such.



Why Identity Matters for Social Change

Identity is a key component for a wide array of social concerns. To broadly understand the importance of identity at the individual level, consider the many challenges arising from a lack of identity. In its Identity for Development (ID4D)[82] initiative, the World Bank has explored a number of these challenges,[83] including those related to accessing:

- Financial services – a lack of identity creates barriers to opening a bank account and accessing credit, among other issues.
- Basic public services and social protection – including social security, food support, pensions, as well as more general rights and services provided by governments.
- Healthcare – including access to health insurance, and health services like vaccinations and maternal care.
- Education – including enrollment at all levels of education and the ability to access scholarships for higher education.
- Political and legal rights – including fundamental civic concerns, like voting, filing petitions, and the ability to own property.

These challenges – as well as less immediately obvious development-related issues such as the inability to buy a mobile SIM card – can affect all those lacking legal identities but hit already vulnerable and marginalized populations hardest. Without legal identity, girls can face even more difficulty avoiding early or child marriage; refugees and asylum seekers can face greater threats when crossing borders, leading to more unsafe migration practices, such as patronizing people-smuggling networks; and the poor and unbanked can face challenges receiving salaries or welfare payments.[84]

82 Identification for Development (ID4D). World Bank. http://id4d.worldbank.org/

83 "Principles on Identification for Sustainable Development: Toward the Digital Age." World Bank Group. February 2017. http://pubdocs.worldbank.org/en/200361509656712342/web-English-ID4D-IdentificationPrinciples.pdf

84 Identification for Development, World Bank Group. 2018. http://www.worldbank.org/en/programs/id4d

Identity challenges are persistent and deeply entrenched. They are not likely to dissipate without some type of concerted intervention. As it stands, half of all low-to-middle-income countries do not have systems in place to register births. This problem is notably present in South Asia and Sub-Saharan Africa, where just 39 percent and 44 percent of children are officially registered at birth.[85] Identity problems are often deeply intertwined with existing social, political and governmental problems.

While secondary to the many human costs resulting from the lack of identification, ineffective or non-existent identification systems also create significant challenges for governments. Without a clear understanding of their populations, governments face major challenges in effectively delivering services, collecting taxes, recognizing and rectifying duplicative programs, allocating resources in an efficient and evidence-based manner, efficiently responding to crises, managing borders and ensuring national security, and collecting accurate statistics.[86]

Considered broadly, identity is relevant for a number of social change topic areas; challenges arising from insufficient identity solutions exist within each domain.

85 "Identification for Development: Strategic Framework." Identification for Development, World Bank Group. January 25, 2016. http://pubdocs.worldbank.org/en/21571460567481655/April-2016-ID4D-Strategic-RoadmapID4D.pdf

86 "Principles on Identification for Sustainable Development: Toward the Digital Age." World Bank Group. February 2017. http://pubdocs.worldbank.org/en/200361509656712342/web-English-ID4D-IdentificationPrinciples.pdf

ECONOMIC

CURRENT CHALLENGES

- Financial exclusion
- High cost remittances
- Provenance not verifiable

SOCIAL

CURRENT CHALLENGES

- No universal coverage
- Social exclusion
- Marginalization/discrimination

POLITICAL / HUMAN RIGHTS

CURRENT CHALLENGES

- Privacy
- Ownership
- Security
- Dignity

GOVERNANCE

CURRENT CHALLENGES

- Agency
- Participation
- Redress mechanisms

Why Identity Matters for Blockchange

In addition to being essential for a number of social change objectives, identity is also foundational for other Blockchange use cases – i.e., track and trace and smarter contracting efforts. Recognizing this, a diversity of corporations, consortiums, and initiatives are pioneering an array of new blockchain for identity projects and protocols.[87] For each type of use case, the creation of trusted identifiers for tangible or intangible objects is essential. Without a clear and trusted understanding of how a signifier tracks to a signified person or object, it is impossible to track and trace certain objects over time and to confirm that certain actions occurred as part of a smart contract.

87 Hyperledger, Evernym, IBM, ID2020, R3, and the Sovrin Foundation are among the main actors that seek to establish the standards and early conceptual models for using blockchain for identity while, for instance, BanQu, uPort, Civic, ObjectTech, ShoCard, Tierion and Cambridge Blockchain have sought to provide identity solutions using blockchain.

TRACK AND TRACE

IDENTITY REQUIREMENT

A trusted digital identity is required for tangible or intangible objects. Once such identity is recorded in a blockchain, users can track and trace its transactional history.

Example:

Walmart and IBM's Smart Package[88] initiative aims to track package contents, conditions, location, and other details. In order for these activities to occur, a confirmed identity for each package is needed.

SMART CONTRACTING

IDENTITY REQUIREMENT

Blockchain smart contracts are automatic, algorithmically enforced and take an "if this, then that" form. They are also linked to the blockchain identities of the parties involved in the process. Contract execution is confirmed by nodes and linked to such parties only.

Example:

The Bext 360[89] project uses smart contracts to pay coffee farmers automatically based on bean analysis conducted at the source. Confirmed identities are a prerequisite for fair and accurate funds to be released to the correct farmers.

A benchmarking study conducted by researchers at the University of Cambridge makes clear the importance of identity in the emergent blockchain ecosystem.[90] The study's authors found that across-public-and private-sector DLT implementations, 73% involved tracking digital records, 70% monitor financial assets, 55% involved tracking physical items, and another 55% involved the direct creation of digital identities. The creation of a trusted identity (for individuals or objects) is essential across all four realms.

88 Helen Partz. "Walmart To Implement Blockchain-Based Delivery System." Coin Telegraph, March 2, 2018. https://cointelegraph.com/news/walmart-to-implement-blockchain-based-delivery-system

89 Bext360, 2018. https://www.bext360.com/

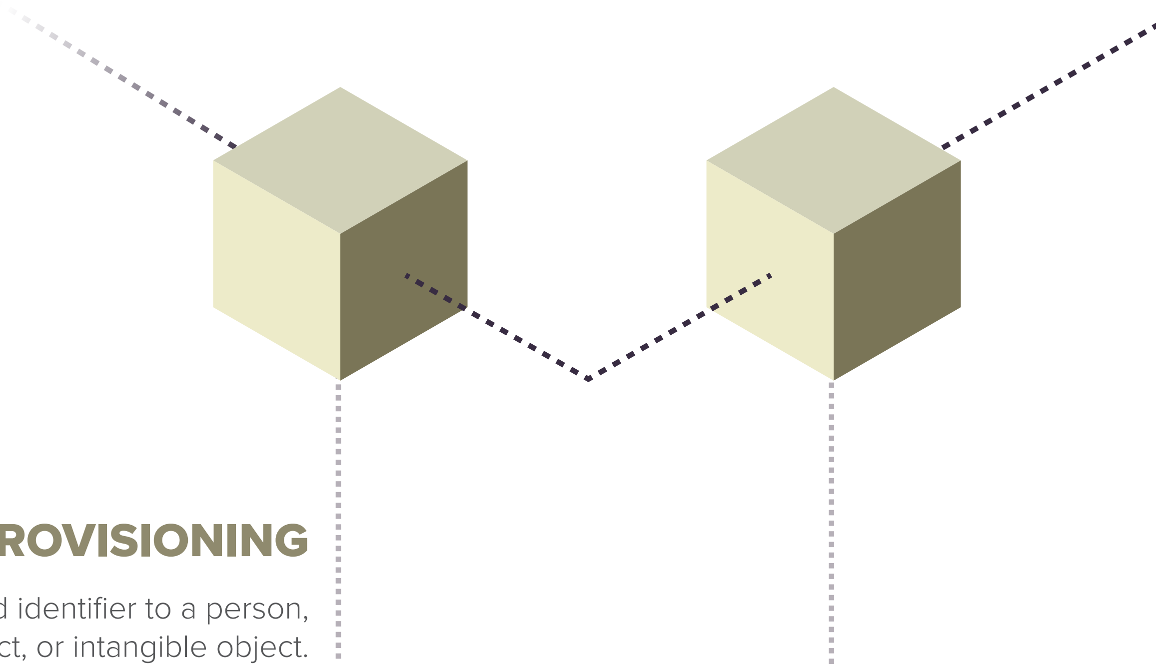
90 Garrick Hileman and Michael Rauchs. "2017 Global Blockchain Benchmarking Study." September 22, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224

Beyond Attributes – Challenges and Opportunities Across the Identity Lifecycle

91 Based on https://blogs.technet.microsoft.com/privatecloud/2013/01/28/the-four-pillars-of-identityidentity-management-in-the-age-of-hybrid-it/ and "A Blueprint for Digital Identity: The Role of Financial Institutions in Building Digital Identity." Presentation, World Economic Forum, 2016. http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf

Stages of the Identity Lifecycle[91]

Unlike the government-issued ID cards that we often associate with the concept, identity is a process, not a thing. To inform our analysis of if, when, and how blockchain can provide value in the identity space, we must first consider the stages of the identity lifecycle and the problems experienced within each stage.



1. PROVISIONING

Assigning a trusted identifier to a person, tangible object, or intangible object.

2. ADMINISTRATION

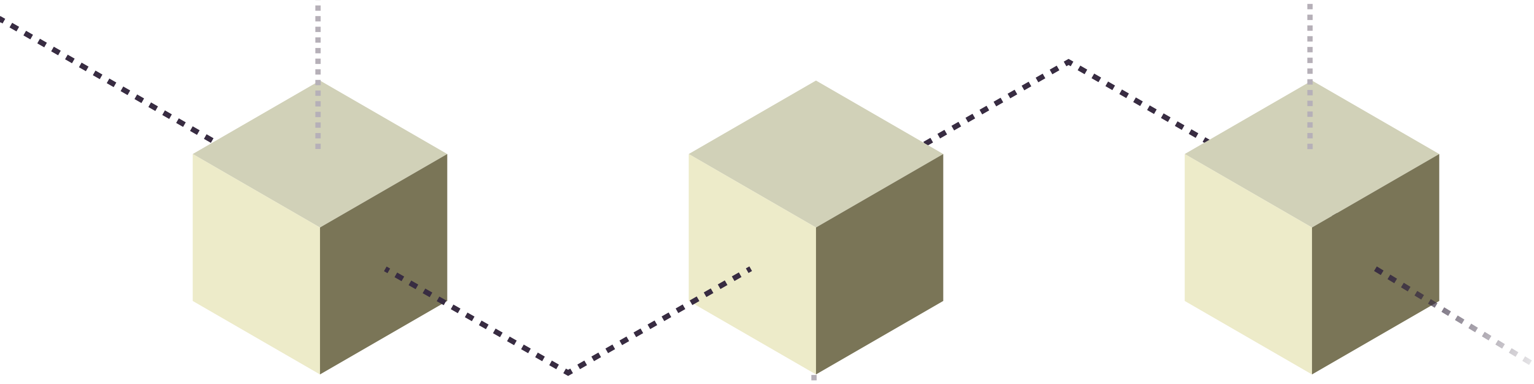
Managing identifiers – both by the provider and the user – including standards setting, attribute collection and storage, access, and service provision.

3. AUTHENTICATION

The process of linking a person or object to attributes collected. Authentication approaches generally rely on one of three factors: 1) something you know, like a password; 2) something you have, like an identity card or QR code; or 3) something you "are," most often in the form of biometric information, like a fingerprint.[92]

5. AUDITING

Monitoring user access to resources. Also entails creating governance mechanisms that address ownership, privacy, security, transparency and accountability issues, and establishes auditing policies and rules.



4. AUTHORIZATION

Confirming what actions the confirmed identity can take – in many cases, providing access to goods and services based on attributes.

92 National Institute of Standards and Technology, US Department of Commerce. https://www.nist.gov/programs-projects/identity-management

Current Challenges Throughout the Identity Lifecycle

It's clear that identity is essential for a wide array of social change objectives and for ensuring access to rights, opportunities, and equity. It's also clear that identity management is a complex process that features disparate actions undertaken by different stakeholders. To aid in our analysis of why current identity management approaches have not been uniformly successful in achieving relevant social change objectives (and to enable consideration of new and more effective approaches), we identified central identity challenges prevalent at each stage of the identity lifecycle. We also include an illustrative sampling of manifestations of those various challenges.

	Central Challenge(s)	Manifestation/Evidence
1. PROVISIONING	▪ Coverage and accessibility (Lack of Identity) ▪ Lack of dignity in some solutions	▪ Unable to obtain housing, create bank account, enroll in school, etc. ▪ "Invisible" population is at risk of exploitation (trafficking, slavery, etc.). ▪ Unable to receive basic public services such as healthcare, food subsidy, etc. ▪ Unable to participate in elections.
2. ADMINISTRATION	▪ Autonomy ▪ Vender and technology lock-in	▪ Individuals store their IDs with institutions and corporations, thereby surrendering their ability to manage their own identities (e.g., manifested, for instance, in difficulties changing names, addresses, etc.).
3. AUTHENTICATION	▪ Quality of Identity – Accuracy and Fit for Purpose ▪ Trust of Identity – Privacy and Security	▪ Identity theft and fraud in financial transactions and beyond. ▪ Personal information hacking or data breach.
4. AUTHORIZATION	▪ Fragmentation of Identity – Lack of Interoperability ▪ Transaction Costs	▪ Multiple IDs for each need, ie. driver's license for driving, ATM card for banking, passport for traveling, credit card for retail, birth certificate, insurance card for healthcare, etc. ▪ High background check fee for accessing housing, employment, and other necessities.
5. AUDITING	▪ Lack of transparency, accountability, and information trail	▪ Secondary use of data – no guarantee that data possessed by third parties (such as banks, insurance companies, or social media networks) will not be used for unanticipated or inappropriate purposes. ▪ Inability to monitor instances where identity information was accessed and for what purpose.

Promise of Blockchain for Addressing Challenges Across the Identity Lifecycle

As it stands, much enthusiasm surrounding blockchain and identity is driven by aspirational use cases – e.g., providing identities for the homeless – rather than by a considered alignment between real social needs and blockchain's possibilities. In order to enable a more nuanced analysis and fit-for-purpose implementation, we seek to identify the specific blockchain attributes that are most salient at each stage of the identity lifecycle to address actual problems or challenges. We seek to identify realistic Blockchange applications that respond most effectively and efficiently to genuine needs.

	Blockchain Promises and Attributes	Social Change Implication
1. PROVISIONING	▪ Equality – Addressing inequitable treatment in identity management through disintermediation	▪ Streamline identity management systems ▪ On-ramp to various services from the public, private and civil sectors
2. ADMINISTRATION	▪ Integrity and Immutability – Improving personal information privacy and security with immutable, encrypted ledger	▪ Eliminating ID storage silos and transaction costs ▪ Securing trust in institutional identity systems, particularly in sensitive areas
3. AUTHENTICATION	▪ Agency – Addressing personal identity management challenges through disintermediated and pseudo-anonymous system	▪ Increasing users' control over who can access their personal information, how, and when ▪ Leveraging zero knowledge proof and similar mechanisms to avoid sharing information beyond what is needed for a particular task.[93]
4. AUTHORIZATION	▪ Efficiency – Addressing high transaction costs through distributed, open source system that could serve as a replacement for traditional bureaucracy[94]	▪ Distributed identity management with reduced friction and fewer bottlenecks ▪ Lowered transaction costs arising from less time- and resource-intensive means for verifying and cross-referencing information
5. AUDITING	▪ Transparency – Addressing opacity of identity system through transparent but secure hash-based system	▪ Maintaining (and confirming) the consistency of identity information over time ▪ Access to information that could benefit institutional accountability objectives

93 Juri Mattila. "The Blockchain Phenomenon: The Disruptive Potential of Distributed Consensus Architectures." Berkeley Roundtable on the International Economy, 2016. https://www.researchgate.net/profile/Juri_Mattila/publication/313477689_The_Blockchain_Phenomenon_-_The_Disruptive_Potential_of_Distributed_Consensus_Architectures/links/589c31caa6fdcc754174493a/The-Blockchain-Phenomenon-The-Disruptive-Potential-of-Distributed-Consensus-Architectures.pdf

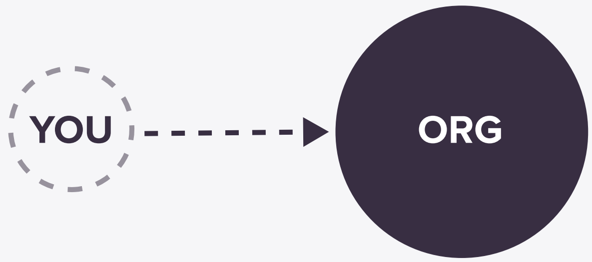
94 MyungSan Jun. "Blockchain government - a next form of infrastructure for the twenty-first century." Journal of Open Innovation: Technology, Market, and Complexity, February 13, 2018. https://link.springer.com/article/10.1186%2Fs40852-018-0086-3

THE BLOCKCHAIN IDENTITY PARADIGM CHANGE

During our analysis, some have suggested that the above (enterprise) ID lifecycle is not representative of how blockchain can transform Identity. They have subsequently called for a new paradigm.

According to Kaliya "Identity Woman" Young[95]: "The mental models of how identity is "managed" whether by an employer relative to an employee or by a government relative to a citizen or by an individual just logging into to a web service is disrupted by the new emerging standards of DIDs and Verifiable Credentials.

In the classic identity management lifecycle an individual establishes an account (enrollment) with an organization and then returns to use that account (doing authentication to prove they are the owner). The establish many different accounts all in this same manner and with a user-name and password.



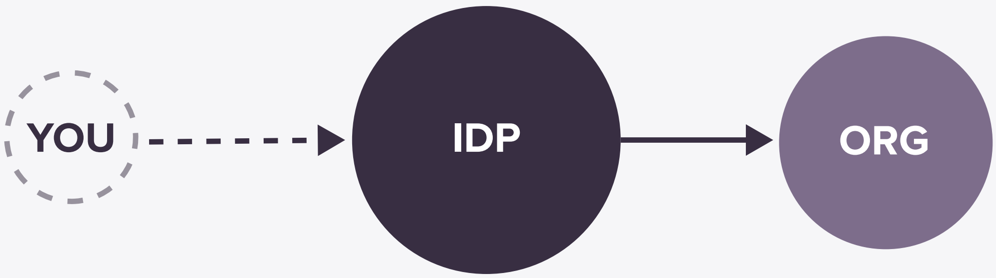
The individual gets an account with an organization. This happens dozens if not 100's of times at a variety of different services.

If they want to prove things about themselves from one service to another in a digital way they have to connect with another service an identity or attribute provider to retrieve the attributes. This means that the two services have to have a technical and also likely a business relationship. It creates a privacy challenges and technical complexity.

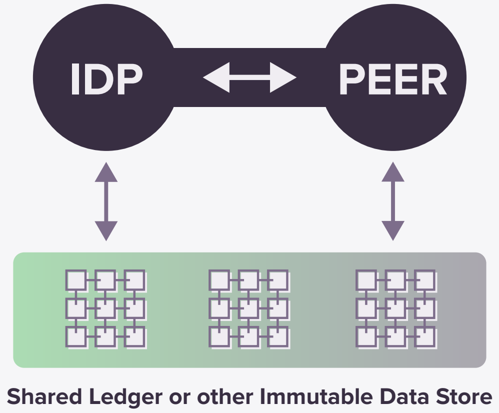
There is also the emergence in the consumer space of Mega IDPs such as Google and Facebook that sit in the middle between the individual and many of the the services and organizations they log in to. They have a account within the name space of that IDP and it can be terminated by them, individuals have almost no recourse when this happens.

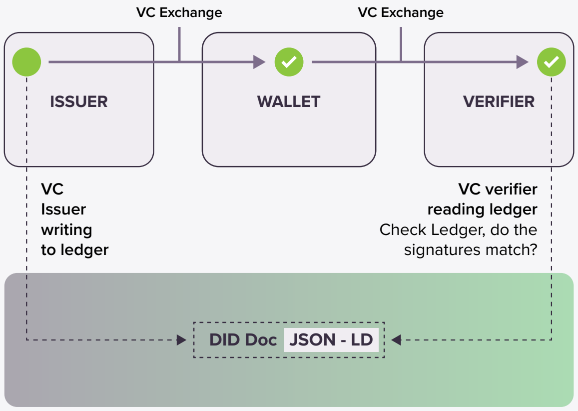
Systems like India's Aadhaar and the Estonia eID system have the government in the role of Mega Identity provider seeing all the places that one uses the digital identity issued by the government to the citizen.

95 See also Kaliya Young, Identity Woman, The Comprehensive Guide to Self Sovereign Identity. https://ssiscoop.com/



With Decentralized Identity the paradigms change completely. The individual has the capacity to stand on their own with an identifier (DID) they created and control completely.





The other thing that changes with this new technology is ability to share credentials from what used to be called an “identity provider” and this new paradigm is called the issuer with what used to be called a “relying party” and now is called the verifier. Blockchain technology provides a way issue credentials to the individual in a digital wallet under their control and present the claims to whatever verifier they choose. The Verifier and the Issuer never actually communicate electronically and they do not have to have a business or technical relationship.”

Maturity of Blockchange Experiments Across the Identity Lifecycle

For the most part, the efforts to leverage blockchain to address identity issues are still fledgling. Their lack of maturity is consistent with ongoing experimentation taking place across the Blockchange landscape. For example, Stanford's Center for Social Innovation's 2018 study found that of the nearly 200 blockchain initiatives examined, 74% were still at the pilot or idea stage, and just over half were estimated to have the potential to impact their beneficiaries by early 2019.[96]

Our research, culminating in the nine Blockchange for identity case studies contained in Appendix 1, reinforced this perception. We conclude that impact is still largely aspirational and notional. But we did find that experimentation at different stages of the identity lifecycle have reached different levels of maturity, if not yet on-the-ground impact. These variations are worth considering as they may suggest differential potential for impact in the near- and medium-term future. In the below table we describe the overarching maturity of experimentation at different stages of the identity lifecycle, and reflect on specific projects from our case studies. Our maturity assessment, to be clear, is based on a cross-cutting consideration of how well blockchain attributes map to problems present at each stage of the lifecycle, and are not entirely based on the projects referenced in our case studies – many of which have still not achieved a high level maturity.

96 Doug Galen, Nikki Brand, et. al. "Blockchain for Social Impact Moving Beyond the Hype." Stanford Graduate School of Business Center for Social Innovation. https://www.gsb.stanford.edu/sites/gsb/files/publication-pdf/study-blockchain-impact-moving-beyond-hype_0.pdf

Stage	Impact and Maturity
1. PROVISIONING **Current Examples** ■ Illinois Secure Digital Birth Certificates	**Maturity: Low** Explanation: Although the need to provide identities to 1.1 billion people is seen as a major goal for Blockchange, effectively achieving that goal still appears relatively far in the future. Compelling projects like the Illinois birth registry pilot (which was a proof-of-concept registering existing birth certificates on a blockchain) are beginning to elucidate a roadmap for continued development, but confirmed, broadly credible entities prepared to recognize newly provisioned IDs are still lacking. At an operational level, an ID is only valuable if it can be shared with and accepted by another party.
2. ADMINISTRATION **Current Examples** ■ Self-Sovereign Identity on the Blockchain in Zug, Switzerland ■ Blockchain for Early Childhood Development in South Africa	**Maturity: Medium** Explanation: The potential to move from pilot experimentation to larger scale implementations is somewhat greater at the administration stage. The potential for blockchain to meaningfully address issues around information silos, security and privacy, as well as other administrative concerns, is clearer given the guaranteed attributes of integrity and immutability. However, in many cases, questions remain about whether blockchain is uniquely—or even most effectively—capable of providing such administrative value.
3. AUTHENTICATION **Current Examples** ■ World Food Programme Building Blocks	**Maturity: Medium** Explanation: From a technological perspective, the authentication process – i.e., confirming whether an identifier is accurate and credible – is relatively straightforward given consensus mechanisms and the immutable information held on chain enabling confirmation. The question of leveraging blockchain at the authentication stage toward increasing individual agency, however, is less clear. WFP's Building Blocks represents a good example of an identity system that is operationally effective but does not grant any additional control or agency to the participating refugee user base.
4. AUTHORIZATION **Current Examples** ■ MIT Digital Diplomas ■ Blockchain-enabled Voting in University and State Party Convention Elections	**Maturity: High** Explanation: Identity authorization processes are generally more mature as the central problems at that stage in the life-cycle are primarily efficiency-related. Across sectors – including notably in industry-driven efforts[97] – efforts to increase efficiency and lower transaction costs, often by cutting out middlemen and replacing bureaucratic processes with automated ones, are yielding the clearest and most concrete benefits. The digital diploma and voting pilots we studied as part of our series of case studies are not necessarily far more mature than experiments at earlier stages in the lifecycle, but the alignment between blockchain attributes and authorization challenges is clearer.
5. AUDITING **Current Examples** ■ Swedish Blockchain Land Registry ■ Blockchain Vote Registration in Sierra Leone	**Maturity: High** Explanation: The capacity for blockchain to help deliver benefits in auditing and monitoring is high given the possibility of implementing a blockchain in such a way that the immutable information held on chain can be made transparent to the public or shared with certain target actors (such as election monitors or land use governance institutions). Of course, possessing the capacity for delivering such benefits does not necessarily mean that all implementations of blockchain will be similarly successful. A private, permissioned blockchain, for example, or a blockchain whose first block included inaccurate or low-quality information, will obviously not lead to the same types of auditing capabilities.

97 Such as the growing use blockchain among industry-led consortia seeking to increase efficiency in commodity trading. https://www.ft.com/content/e088e0b6-131c-11e7-b0c1-37e417ee6c76

LESSONS LEARNED — CROSS-CUTTING CHALLENGES AND OPERATIONAL CONDITIONS

The preceding discussion has tried to present a balanced, evidence-based portrait of blockchain at this particular moment in its evolution and as a social and economic phenomenon. In its short history—Bitcoin emerged only in early 2009—substantial myth and distortion have attached to blockchain. This had clouded our ability to understand what it really is, and its true potential impact. The purpose of this report has been to unpack some of the myths, and to try to understand blockchain's possibilities as an agent for social change, particularly as it is applied to the identity lifecycle.

If there is one overarching conclusion that flows from our research, it is this: despite the limitations of blockchain, despite the hype surrounding the technology—and despite the backlash to that hype—blockchain's potential to create positive social transformation is real. However, it is important to emphasize that this potential can only be realized for certain types of use cases and under specific conditions.[98] This more granular understanding is critical to understanding blockchain's potential, and to harnessing that potential.

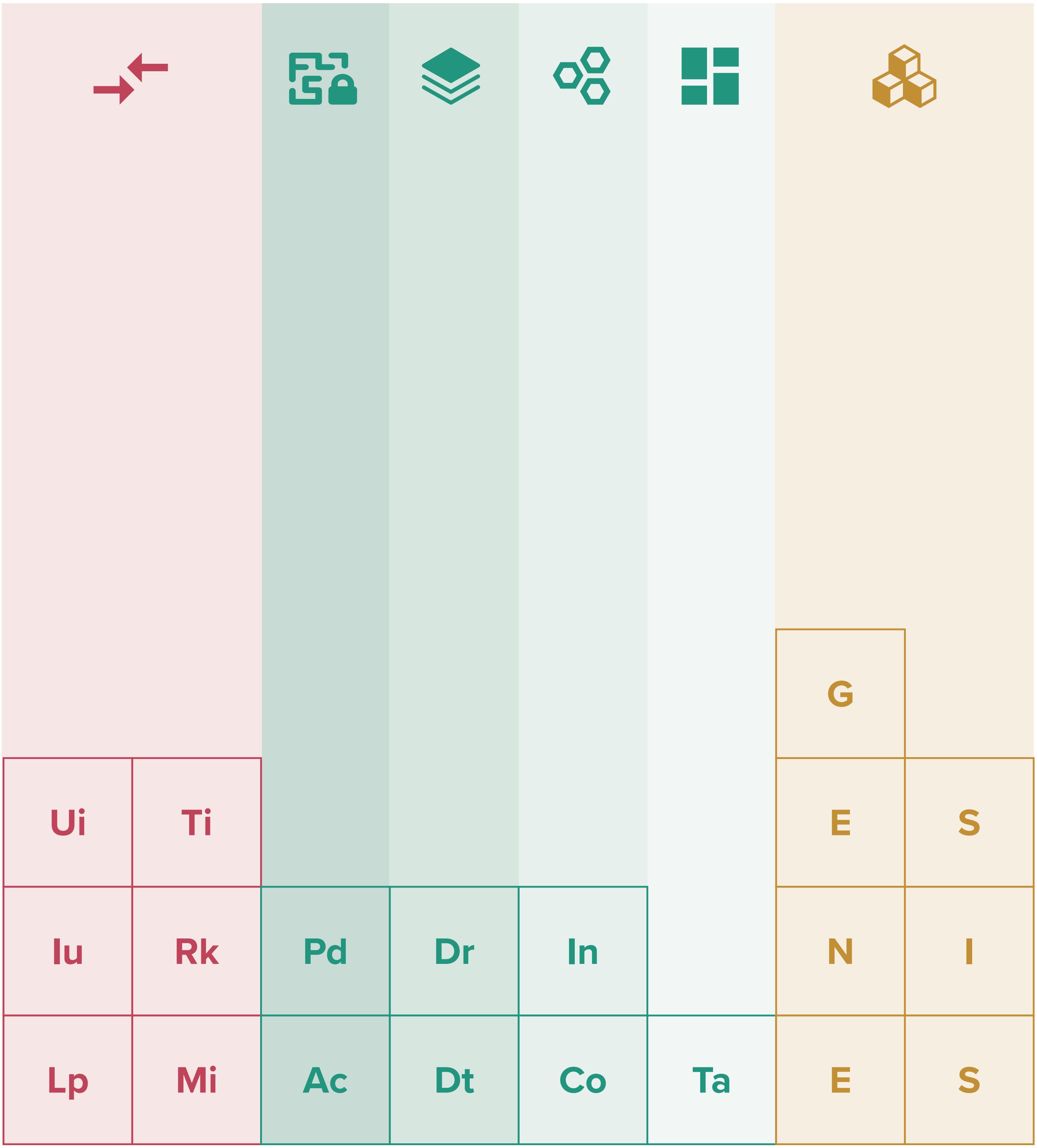
In this section and the next, we present some of the challenges of using blockchain, as well as necessary conditions and specific design principles to overcome those challenges and enable Blockchange. Although only a preliminary discussion (our research is ongoing), these operational conditions and design principles can serve as a toolkit for individuals and organizations seeking to deploy DLTs and blockchain-based applications or platforms within a social change context.

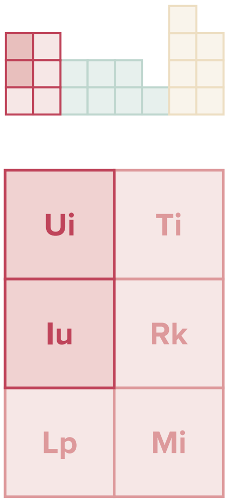
98 Nouriel Roubini and Preston Byrne. "The Blockchain Pipe Dream." Project Syndicate, March 5, 2018. https://www.project-syndicate.org/commentary/blockchain-technology-limited-applications-by-nouriel-roubini-and-preston-byrne-2018-03

CROSS-CUTTING CHALLENGES

ENABLING OPERATIONAL CONDITIONS

DESIGN PRINCIPLES





Cross-Cutting Challenges: User Interfaces, Incentives, Legal and Policy Uncertainty, Technical Inefficiencies, Risk and Impact Measurement

During the design, implementation, and scaling processes of different Blockchange projects, a number of persistent challenges tend to surface again and again. In this section we examine six of the most commonly occurring and potentially disruptive challenges facing actors seeking to create positive social change with blockchain.

USER INTERFACES

User interfaces of blockchain for identity solutions are often neither clear nor compelling. As a result, incentivizing individual users is difficult.

Blockchain brings together a number of complex technologies – "P2P networking, distributed timestamping, cryptographic hashing functions, digital signatures, and Merkle trees, among others."[99] To date, the user-friendliness of many implementations of these complex technologies is lacking, creating challenges to broad, mainstream adoption.[100]

INCENTIVIZING USE

Incentivizing use at the institutional/legacy level will be required for many blockchains in order to identify initiatives that provide true value.

Similar challenges—concerning user interfaces, incentives, and others--confront institutional users as individual ones. Incentives questions are particularly pressing when institutions must replace existing legacy systems. Many Blockchange initiatives seek to circumvent and disrupt legacy systems with the goal of establishing a fully self-sovereign and decentralized replacement; given the long time horizon for such solutions to reach critical mass, partnership with relevant domain area institutions will likely remain essential for use and impact.

99 Garrick Hileman and Michael Rauchs. "2017 Global Blockchain Benchmarking Study." September 22, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3040224

100 Iyke Aru. "User Interface - The Missing Link to Mainstream Adoption of Blockchain." Coin Telegraph, June 11, 2017. https://cointelegraph.com/news/user-interface-the-missing-link-to-mainstream-adoption-of-blockchain

LEGAL AND POLICY UNCERTAINTY

Legal and policy questions can introduce further challenges to the governance of blockchain for social change.

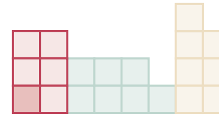
At its current stage of experimentation – within the identity space and beyond – blockchain is raising a number of challenging legal and policy questions, including but not limited to those listed below.

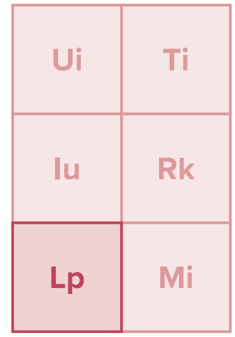
Legal Questions:

- How can Blockchange experimentations ensure ongoing regulatory compliance, including sector-specific identity concerns and regulations (e.g., HIPPA issues for health, KYC concerns for finance)?
- How can questions of liability and redress – for example arising from a privacy breach – be answered in a distributed and, at least in some cases, disintermediated system?
- Especially given new and emergent legal mandates, such as the General Data Protection Regulation (GDPR) in Europe,[101] how can Blockchange for identity initiatives navigate diverse legal frameworks and ensure regulatory compliance and interoperability across regions?
- How can Blockchange achieve its social change potential when vendor lock-in and a race to patent blockchain applications and protocols[102] threaten to limit use and experimentation?

Policy Questions:

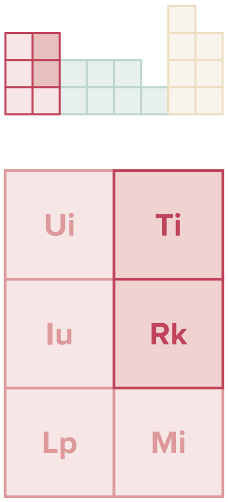
- Is the policy landscape ready for disruptive new identity approaches at a time when identity requirements differ widely across, for example, government service providers?
- Will the types of digital signatures used in Blockchange for identity initiatives be considered valid by existing legacy systems, intermediaries, and gatekeepers?
- Can Blockchange projects adhere to data protection policies (e.g., GDPR) that increasingly guarantee a right to be forgotten and other principles regarding personal information collection, storage, and use that run counter to certain DLT attributes like immutability?
- What types of policies can and should be put into place regarding information handling, privacy, and security considerations in a distributed system?





101 Lucas Mearian. "Will blockchain run afoul of GDPR? (Yes and no)." ComputerWorld, May 7, 2018. https://www.computerworld.com/article/3269750/blockchain/will-blockchain-run-afoul-of-gdpr-yes-and-no.html

102 Jack Filiba. "The Role of Patents in Blockchain Innovation." Coinsquare, May 2, 2018. https://discover.coinsquare.io/business/patents-blockchain-innovation/



TECHNICAL INEFFICIENCIES

Technical inefficiencies embodied especially in proof-of-work mechanisms in some (but not all) blockchains can create major environmental concerns.

- Although blockchains can help increase institutional efficiency, Nouriel Roubini argues that they are "less efficient than existing databases," with higher requirements for storage space, computational power, and with higher latency levels than in a centralized database.[103]
- In many blockchains, the inefficient-by-design proof-of-work mechanism has significant—and negative— ecological impacts. Mining on the Bitcoin blockchain, in particular, is creating an unsustainable carbon footprint.[104]

RISKS

Risks (including to intended beneficiaries from vulnerable communities, like refugees) can outweigh the potential value created by certain blockchain-for-identity initiatives.

- Blockchain's sophisticated cryptography is often viewed as a means for creating high levels of information security. Many blockchain implementations, however, rely on private keys handled by the end user. These keys can introduce otherwise non-existent information security and personal privacy concerns should they be lost or stolen.[105]
- The "coercive force" of immutability has surfaced concerns regarding the removal of human agency and decision-making in some processes. Smart contracts, in particular, can be used to create an immutable "absolute law"[106] that cannot be altered or iterated upon without significant transaction costs and distributed buy-in.
- Blockchain's immutability can also amplify issues surrounding the notion of "garbage in; garbage out."[107] If low quality information is allowed to enter the blockchain, not only will it negatively impact resulting actions, but the low-quality information will remain on the blockchain permanently (unless significant transaction costs are undertaken to rectify the issue).
- These challenges are especially salient given the use of privacy-preserving, zero knowledge proof approaches. Zero knowledge proofs leverage an automatic system for determining whether or not something is true without sharing information with the authenticating entity.[108]

103 Nouriel Roubini and Preston Byrne. "The Blockchain Pipe Dream." Project Syndicate, March 5, 2018. https://www.project-syndicate.org/commentary/blockchain-technology-limited-applications-by-nouriel-roubini-and-preston-byrne-2018-03

104 Emily Atkin. "The Environmental Case Against Bitcoin." The New Republic, December 5, 2017. https://newrepublic.com/article/146099/environmental-case-bitcoin

105 Mark Frauenfelder. " 'I Forgot My Pin: An Epic Tale of Losing $30,000 in Bitcoin." Wired, October 29, 2017. https://www.wired.com/story/i-forgot-my-pin-an-epic-tale-of-losing-dollar30000-in-bitcoin/

106 MyungSan Jun. "Blockchain government - a next form of infrastructure for the twenty-first century." Journal of Open Innovation: Technology, Market, and Complexity, February 13, 2018. https://link.springer.com/article/10.1186%2Fs40852-018-0086-3

107 Jemima Kelly. "Blockchain insiders tell us why we don't need blockchain." Financial Times. May 2, 2018. https://ftalphaville.ft.com/2018/05/02/1525253799000/Blockchain-insiders-tell-us-why-we-don-t-need-blockchain/

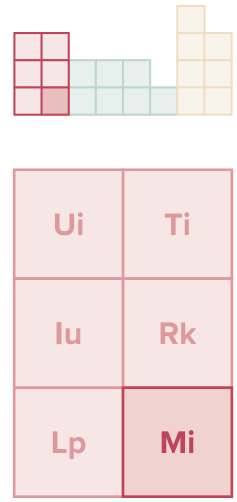
108 Lukas Schor. "On Zero-Knowledge Proofs in Blockchains." Medium, March 23, 2018. https://medium.com/@argongroup/on-zero-knowledge-proofs-in-blockchains-14c48cfd1dd1

Mi

MEASURING IMPACT

Measuring impact remains a challenge, and the lack of clear metrics of success negatively affects attempts to scale up.

With the vast majority of Blockchange applications still at the conceptual or pilot stage, impact measurement is lacking. Moreover, given that much of the field of experimentation is being driven by startups in the private sector, open and context-specific impact measurement will likely remain a challenge without leadership from the public, academic, and civil sectors.



Enabling Operational Conditions: Problem, Data & Tech, and Ecosystem

Where does one begin seeking to deploy Blockchange? This section outlines some foundational operational conditions that can play a role in the likelihood of success for blockchain implementations seeking to create positive social change. It lists some critical questions that need to be asked and includes examples to illustrate the importance of those questions. These examples are further elaborated upon in the case studies contained in Appendix 1.

Operational Condition: Problem

Pd

IS THERE A CLEAR PROBLEM DEFINITION?

Blockchain is frequently accused of being a solution in search of a problem.[109] As is the case with most innovations, Blockchange implementations are most likely to find success when they are targeted at a clear, well-defined problem, and when progress toward addressing that problem can be measured.

For example: The World Food Programme's Building Blocks authentication project is an efficiency-led initiative focused on addressing high transaction costs in the distribution of aid at the Azraq refugee camp in Jordan. While only addressing a tiny portion of the broader refugee challenge (in Jordan and beyond), the tight focus has yielded clear financial benefits, including cost-reduction and disintermediation, translating into additional resources for programming.

109 Jason Bloomberg. "Eight Reasons To Be Skeptical About Blockchain." Forbes, Mary 31, 2017. https://www.forbes.com/sites/jasonbloomberg/2017/05/31/eight-reasons-to-be-skeptical-about-blockchain/#1d7c1a7d5eb1

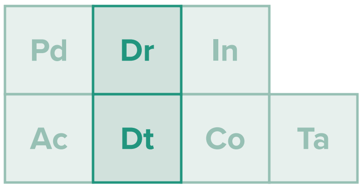
Ac

DO INFORMATION ASYMMETRIES AND HIGH TRANSACTION COSTS INCENTIVIZE CHANGE?

As demonstrated in the seminal economics paper, "The Market for Lemons," by Nobel Prize-winner George Akerlof,[110] information asymmetries can create significant transaction costs for disadvantaged parties in both commercial or social engagements. When such asymmetries exist, there is significant incentive for implementing a system—such as blockchain—that levels the information playing field and establishes transparency and trust between disparate parties.

For example: In Kenya, BanQu was launched to address information asymmetries that disadvantage the extremely poor, many of whom currently lack access to credit and banking. For the so-called 'unbanked,' building up the credit and identity profile necessary to access financial opportunities is a difficult process with high levels of transaction costs and stumbling blocks. The BanQu blockchain aims to enable the unbanked to "develop a tractable, vetted financial and personal history," while simultaneously providing financial institutions with anti-money laundering and know-your-customer tools. The result is lowered transaction costs on both sides of the equation.

110 George A. Akerlof. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism." The Quarterly Journal of Economics, August 1970. https://www.jstor.org/stable/1879431?seq=1#page_scan_tab_contents



Operational Condition: Data and Technology

Dr

ARE ACCURATE AND HIGH-QUALITY DIGITAL RECORDS AVAILABLE?

In cases where high quality digital records are already available, the move toward a blockchain-enabled system is likely to be smoother and more rapid than an attempt to move from an analog identification system to one leveraging DLTs.

For example: The canton of Zug, Switzerland is experimenting with a self-sovereign identity initiative aimed at providing blockchain-based IDs for citizens to access public services. The process for participating in the initiative makes clear both the importance of engagement with legacy systems for some Blockchange use cases, as well as the related benefits of accessing existing digital records. Upon signing up for the Zug SSI project, citizens must register in person at the Zug records office, where civil servants can cross-check existing government documentation on the individual with their new blockchain-enabled identity. Officials can also associate existing records with individuals' new digital credentials, thus avoiding the time- and resource-intensive process of recreating those records for new IDs.

Dt

IS THERE NO AVAILABILITY OF CREDIBLE AND ALTERNATIVE DISCLOSURE TECHNOLOGIES?

Much of the skepticism surrounding blockchain uses for social change is based on the belief that in many cases, technologies already exist to achieve the same objectives, and often with better user interfaces and lower ecological and financial costs.[111] Although all problems look like nails to true believers[112] wielding the blockchain hammer, the most successful Blockchange efforts will fill a true gap rather than trying to address problems already being addressed effectively with other tools.

For example: The Lantmäteriet, the Swedish Land Registry, developed a prototype in which real estate transactions would be put on the blockchain from the point an agreement to sell is reached until the land title is transferred, allowing all parties — banks, land registry, brokers, buyers, and sellers — to monitor the progress of the transaction. The impetus behind the pilot project is the belief that there exists no other trustworthy solution for creating, enacting, verifying, storing, and securing digital contracts. The project seeks to test the idea that blockchain has unprecedented capacity to rapidly and effectively create new digital entities that cannot be fraudulently copied or tampered with, and secure processes that cannot be manipulated.

111 Ben Yuan, Wendy Lin, and Colin McDonnell. "Blockchains and electronic health records." https://www.fer.unizg.hr/_download/repository/blockchain_ehr.pdf

112 Izabella Kaminska. "Why blockchain is a belief system." Financial Times. January 11, 2018. https://ftalphaville.ft.com/2018/01/11/2197546/why-blockchain-is-a-belief-system/

Operational Condition: Ecosystem

In

ARE THERE TRUSTED INTERMEDIARIES ACTIVE IN THE SPACE AND DOES THEIR EFFICIENCY OR LACK THEREOF INCENTIVIZE CHANGE?

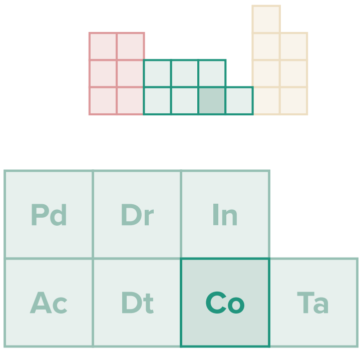
The presence or absence of intermediaries, and their effectiveness or ineffectiveness, can act as a key enabler for Blockchange. As a fully self-sovereign system of identity management is unlikely to reach critical mass for some time, effective intermediaries can enable engagement with both intended users and any legacy systems relevant to the Blockchange implementation. On the other hand, the absence of trusted intermediaries, or the presence of ineffective ones, could help to incentivize the creation and use of a more decentralized approach.

Moreover, intermediaries can play complex and varied roles, meaning that certain functions could be disintermediated without entirely removing the need for or value of a particular type of intermediary.

Indeed, it is likely going forward that new intermediaries will be established – for example, to address unforeseen circumstances or adjudicate contingencies that cannot be handled effectively through an automated and distributed system.[113] In addition, it is likely that existing intermediaries may take on new roles and responsibilities as they transition to blockchain enabled-platforms.

For example: MIT's Digital Diploma initiative is the result of a collaboration between the MIT Registrar's Office and the Learning Machine startup. While still limited, use to date is largely the result of using the existing registrar office as a distribution channel, and would not be likely if the Blockcerts application was developed and implemented in isolation toward providing a fully decentralized credentialing system.

113 Nouriel Roubini and Preston Byrne. "The Blockchain Pipe Dream." Project Syndicate, March 5, 2018. https://www.project-syndicate.org/commentary/blockchain-technology-limited-applications-by-nouriel-roubini-and-preston-byrne-2018-03



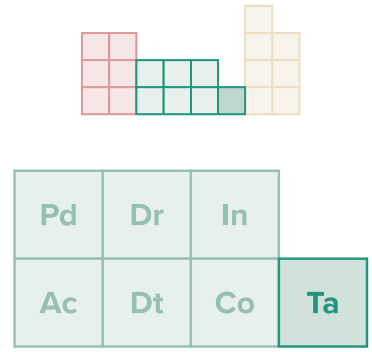
Operational Condition: Ecosystem

IS THERE A LEVEL OF COOPERATION (OR 'CO-OPETITION') AMONG PLAYERS? IS THERE AN ECOSYSTEM OF POTENTIAL USERS?

The successful implementation of any new technology, especially one as complex as blockchain, requires a level of cooperation, if not full-scale collaboration, among a diversity of stakeholders. Just as an overreliance on and an outsized empowerment of vendors can lead to lock in, so a fragmented rather than cooperative approach among stakeholders can lead to the creation of unnecessary silos and a minimization of interoperability. Similarly, if there is no ecosystem of potential users, the initiative may have limited uptake.

For example: Voatz is one of the first movers in blockchain-enabled voting (not just vote tallying and auditing). To date, pilot projects for a university student union election and a state party convention election represent its major implementations, with remote voting for one state's midterm congressional election launched just after this writing. Going forward, as more actors are likely to enter the blockchain-enabled voting space, some level of cooperation and interoperability will be key in order to ensure that voting processes across regions and levels of government are compatible.

Operational Condition: Capacity



Ta

ARE PUBLIC OFFICIALS TECHNOLOGY AWARE AND DATA LITERATE?

Like any technology being considered for governance use cases, blockchain can only be effective if it is implemented in an enabling environment by stakeholders with a firm grasp of the technology, its strengths, its weaknesses, and how it fits into the broader governance landscape. Given blockchain's nascence and complex nature, achieving this level of understanding is likely to pose an ongoing challenge to public officials. The issue of public sector technical literacy is especially important as private sector vendors continue to dominate the space.

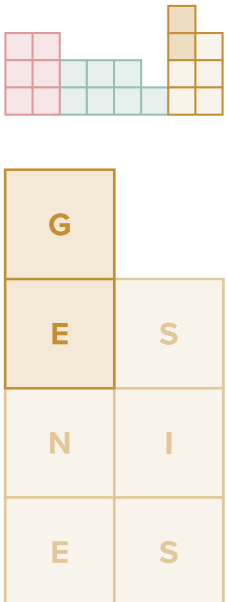
For example: In Sierra Leone, controversy erupted after the global media publicized the so-called "Blockchain Election" in the country enabled by Agora, a Swiss blockchain startup. While it remains unclear how the misunderstanding originated, it is evident that Agora and the National Electoral Commission were not aligned on the use and objectives of blockchain in the election, and the media's somewhat distorted coverage exacerbated that disconnect.

CONCLUSION: GENESIS – DESIGN PRINCIPLES FOR BLOCKCHANGE

Despite the challenges listed above, blockchain technologies can promote positive social change in the identity space. In order to be effective, organizations deploying blockchain applications need to begin with the foundational principles and conditions we have outlined above. If those conditions are adequately addressed, then the task is to design applications and platforms in a way that maximizes effectiveness while limiting risk.

In this concluding section, we present and describe seven design principles. These principles should be taken under consideration together with related efforts to steward experimentation with blockchain in the public interest – including notably the Beeck Center's Blockchain Ethical Design Framework[114] – and need to be applied from the very first block: the so-called genesis block of the blockchain. And that is why, collectively, we call these principles the GENESIS principles.

114 Cara LaPointe. "The Blockchain Ethical Design Framework for Social Impact." Georgetown University Beeck Center, March 8, 2018. http://beeckcenter.georgetown.edu/blockchain-ethical-design-framework-social-impact/



GOVERNANCE LEGITIMACY

Given the broad positive and negative potential impacts of an immutable ledger that can automatically take pre-defined actions when a condition is met, a transparent, accountable, and participatory process for decision-making should be in place.

Recommendations for Operationalizing:

- When implementing Blockchange projects, consider existing ethical frameworks for blockchain,[115] as well as data responsibility policies and principles.
- Define and make accessible a clear process showing how decisions are to be made.

ETHICALLY SOUND

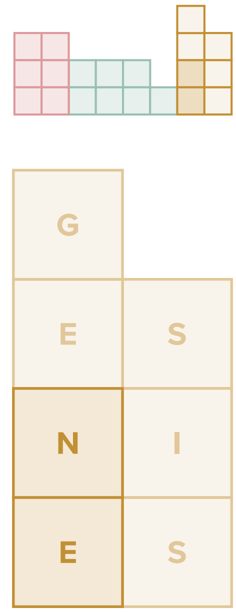
Whether foundational or functional, identity plays a major role in cementing individuals' access to diverse rights, and issues around identity could lead to rights being jeopardized. Blockchange implementations should take into consideration any potential positive or negative impact on the rights of individuals.

Moreover, many Blockchange initiatives are aimed at addressing problems experienced by the most vulnerable. In seeking to solve the world's most important and intractable problems, practitioners should ensure that they avoid reckless experimentation and undertaking risky actions that could further jeopardize already vulnerable communities.

Recommendations for Operationalizing:

- Engage potential users, domain experts, and other critical stakeholders early in the design process to ensure that identity authentication efforts in particular enable safe, secure, and dignified user interactions.
- During the design phase, identify and map individual rights that could be impacted positively or negatively by the Blockchange application.
- Provide clear guidance on how users can monitor activity related to their identity and intervene when necessary.

115 Cara LaPointe. "The Blockchain Ethical Design Framework for Social Impact." Georgetown University Beeck Center, March 8, 2018. http://beeckcenter.georgetown.edu/blockchain-ethical-design-framework-social-impact/



N

NOT TECHNOLOGIES, BUT SOLUTIONS TO REAL PROBLEMS

Like many new technologies, blockchain is often treated as the proverbial hammer in search of a nail. While the tendency toward broad experimentation is a worthy aim, a clear and actionable understanding of the problem to be solved is essential both for meaningfully addressing the problem at hand, as well as contributing to a greater understanding of if, when, and how blockchain can positively impact social change.

Recommendations for Operationalizing:

- When defining the problem to be solved, engage experts, stakeholders, and affected communities to understand better why the problem currently exists, and why previous efforts to address the problem were or were not successful.
- Capture the value proposition, relevant assumptions, and potential knock-on effects of the problem to be addressed early in the design phase in order to inform decision-making.
- Be open to the determination that the optimal solution for the problem at hand does not involve blockchain.

E

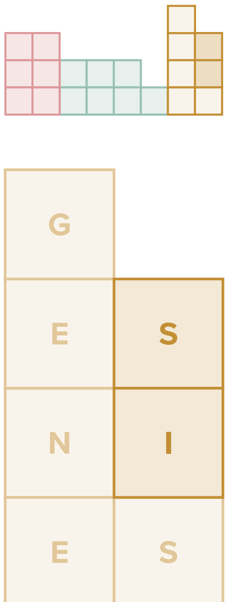
ECOLOGICAL FOOTPRINT

The Bitcoin blockchain has a massive and growing ecological footprint resulting from the high levels of energy powering proof-of-work mining activities.[116] If Blockchange is going to have a positive impact on creating social change, and allow for scaleable solutions beyond the initial prototyping, validation mechanisms that do not accelerate climate change will be essential.

Recommendations for Operationalizing:

- Consider the ideal transaction validation mechanism for the initiative and avoid highly energy-dependent proof-of-work mining approaches where possible.

116 Adam Rogers. "The Hard Math Behind Bitcoin's Global Warming Problem." Wired, December 15, 2017. https://www.wired.com/story/bitcoin-global-warming/



SYNCHONIZED WITH EXISTING INITIATIVES

Many identity challenges are neither new nor unrecognized by existing institutions. While blockchain could offer a promising option for addressing some identity challenges, new efforts should seek to be complementary with existing work.

Recommendations for Operationalizing:

- Conduct due diligence at the design phase to identify existing efforts to address the identity problem at hand and consider if and how the new Blockchange approach can be complementary.
- Engage experts on both the policy and technology sides to gain a sense of what technologies are currently in use – e.g., change-tracking databases for identity administration or open data for certain auditing processes – and assess their viability relative to a new blockchain-enabled effort.
- If a Blockchange approach is deemed viable, work with actors already present in the space to ensure that lessons learned and guiding principles developed over time are not lost when transitioning to a new identity solution.

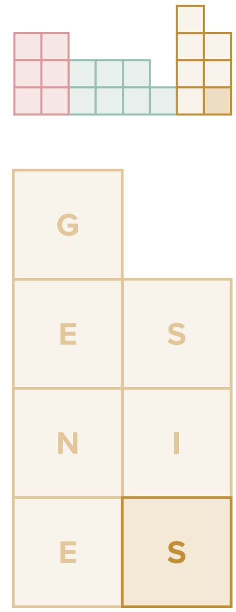
INTEROPERABILITY AND OPEN STANDARDS

Much of the current activity around blockchain's use for identity is being driven by the private sector. This is to be expected given where the vast majority of blockchain-related skills and capacity reside. But while vendors are an important part of the blockchain ecosystem, without whom experimentation would be impossible, government and civil society must work to avoid long-term vendor lock-in and the patenting of Blockchange protocols.[117] Ensuring the interoperability of different systems, and the development of open technical standards for these systems will be key to ensuring that the public sector's use of blockchain remains flexible and problem- rather than technology-driven.

Recommendations for Operationalizing:

- Consider the potential for vendor lock-in and the centralized control of identifiers when contracting with blockchain technology providers.
- Research the field of practice relevant to the particular Blockchange use case and context and seek ways to ensure interoperability with other related efforts.

117 Matt Asay. "Why big vendors could ruin Blockchain by making it a centralized service." TechRepublic, April 4, 2017. https://www.techrepublic.com/article/why-big-vendors-could-ruin-blockchain-by-making-it-a-centralized-service/



S

SECURING FIRST BLOCK ACCURACY

While blockchain's attributes of immutability and (guaranteed) integrity ensure a level of information accuracy and consistency for on-chain information, the first block in the chain remains an important single point of failure. Consistent with the aphorism "garbage in, garbage out," the quality of information held on the blockchain is only as good as what is entered in the genesis block. In fact, in a blockchain environment, the lesson is "garbage in, garbage immutably stored and broadly accessible." At the same time we are seeing several initiatives where a trusted identity or reputation is built over time, yet those initiatives tend to work best if linked with verified credentials from a trusted source.

Recommendations for Operationalizing:

- Identify any existing processes or intermediaries in use to validate information and seek out multiple sources of collaboration.
- Consider optimal upfront information vetting, user disclosure and validation, and redress and correction approaches early in the design process.
- Establish mechanisms for trusted parties to monitor new information added to the chain and flag any potentially suspect additions.

GOVLAB