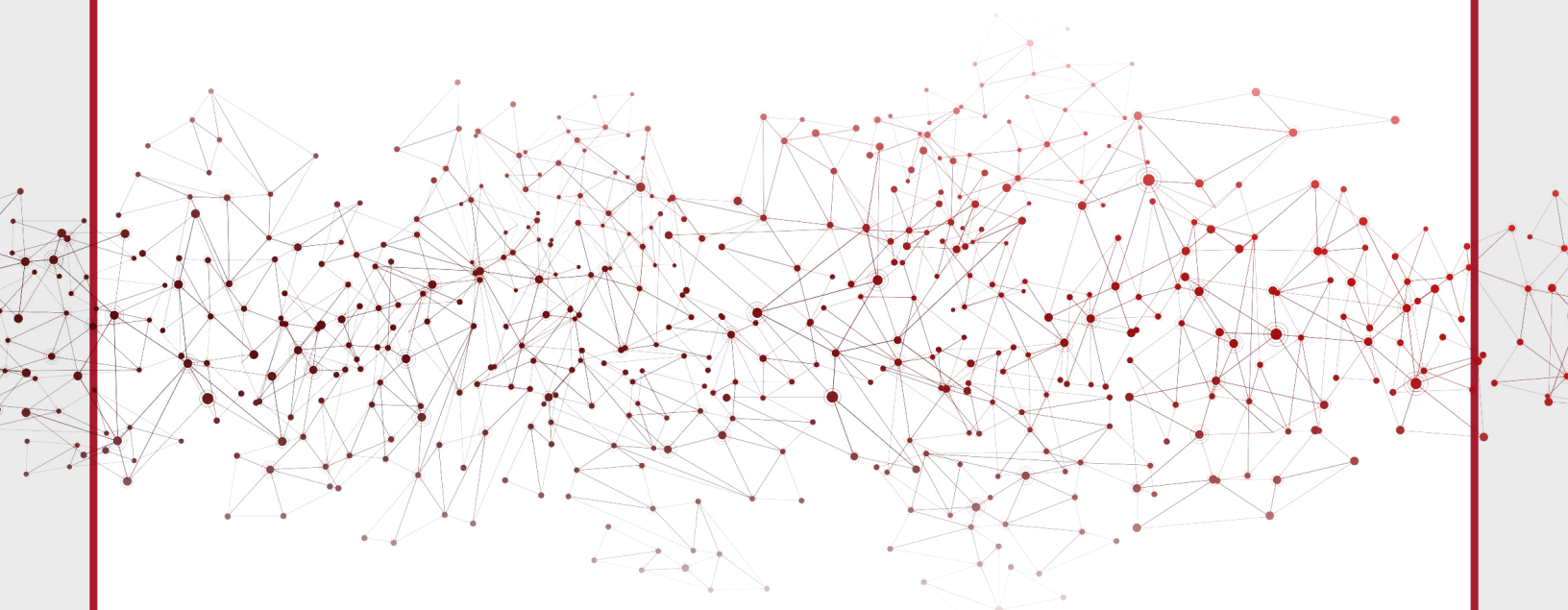


TECHNOLOGY FACTSHEET SERIES

Blockchain



CONTRIBUTORS:

Buck Endemann, KL Gates
Irving Wladawsky-Berger, MIT
Cara LaPointe, Georgetown
Hugo Yen, Harvard

EDITORS:

Amritha Jayanti
Bogdan Belei

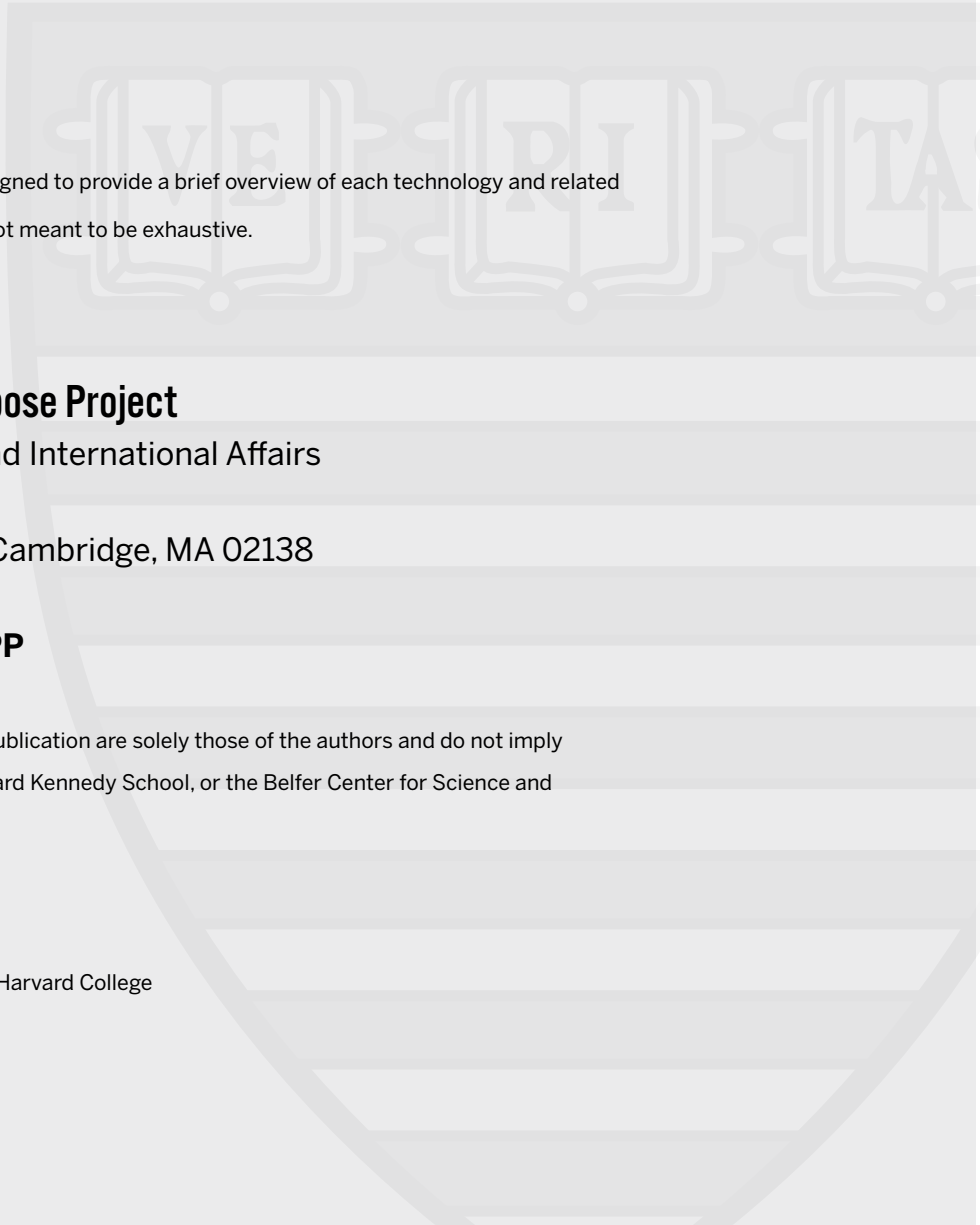


HARVARD Kennedy School

BELFER CENTER

for Science and International Affairs

Technology & Public Purpose Project



The Technology Factsheet Series was designed to provide a brief overview of each technology and related policy considerations. These papers are not meant to be exhaustive.

Technology and Public Purpose Project

Belfer Center for Science and International Affairs

Harvard Kennedy School

79 John F. Kennedy Street, Cambridge, MA 02138

www.belfercenter.org/TAPP

Statements and views expressed in this publication are solely those of the authors and do not imply endorsement by Harvard University, Harvard Kennedy School, or the Belfer Center for Science and International Affairs.

Design and layout by Andrew Facini

Copyright 2020, President and Fellows of Harvard College

Printed in the United States of America

Executive Summary

Blockchain is a type of distributed ledger technology (DLT) that stores data (commonly immutable and sequenced transaction records) in a decentralized manner via encryption and consensus algorithms.¹ The first widely recognized implementation of blockchain was in 2009 with the Bitcoin public blockchain. Since then, other types of blockchains have been developed for a wide range of applications and features built on common principles such as decentralization, encryption, consensus, and immutability. In particular, blockchain technology has been most widely used in the banking and finance sector for transaction settlement and digital currencies, as well as in supply chain applications to help participants resolve issues quickly and efficiently.² Other use cases are continuing to develop.

As a form of information management, blockchain and related DLTs offer advantages over traditional databases and may be useful in the development of certain emerging technologies, such as the Internet of Things. Regulation of blockchain is currently limited at the international and federal levels, though state-level legislation has shown support and recognition of aspects of blockchain technology. Most current regulation is in the form of self-regulation by blockchain developers and related communities, though a number of challenges and risks such as data privacy and security need to be addressed in the near future.

What is Blockchain?

Blockchains come in many forms and generally share four main features: decentralized data storage (a public ledger of transaction records), encryption, immutability, and a consensus algorithm. As a specialized type of decentralized ledger technology (DLT), blockchains store encrypted data across peer-to-peer networks, linking together sequential “blocks” of information into “chains”.³ The information available to all network participants is a shared ledger of all information transactions on the blockchain. The consensus algorithms ensure that information is consistent and immutable across this decentralized network and deter individual users from adding to ledger information without authorization from the network. Furthermore, due to blockchain’s structure, prior information on the chain cannot be edited or removed, as doing so would compromise the integrity of the decentralized ledger.⁴

1 Nakamoto, Satoshi. “Bitcoin: A Peer-to-Peer Electronic Cash System.” Bitcoin, October 31, 2008. <https://bitcoin.org/bitcoin.pdf>.

2 Tapscott, Alex, and Don Tapscott. “How Blockchain Is Changing Finance,” August 21, 2019. <https://hbr.org/2017/03/how-blockchain-is-changing-finance>.

3 Houben, Robby, and Alexander Snyers. “Cryptocurrencies and Blockchain.” European Parliament’s Special Committee on Financial Crimes, Tax Evasion and Tax Avoidance, July 2018. <http://www.europarl.europa.eu/cmsdata/150761/TAX3> Study on cryptocurrencies and blockchain.pdf.

4 Ibid.

One common classification scheme for blockchains is with respect to membership or accessibility. **Public blockchains** have a publicly viewable ledger and are fully decentralized; users may still require permission to write or add to the blockchain. Most cryptocurrencies are implemented as public blockchains. **Private blockchains** are accessible only to the specific host organization and used primarily for internal purposes, such as auditing or records management. **Consortium blockchains** (or hybrid blockchains) are semi-private and accessible to a set group of organizations, such as groups of banks, energy traders, or hospitals, and can facilitate more efficient transactions or information-sharing among the parties. The type of blockchain depends on its purpose and will also result in different design schemas. Private and consortium blockchains are less decentralized and focus on smaller groups of users; thus, they may be more sustainable and cost-efficient than public blockchains.

Among public blockchains, there is a wide variety of blockchain implementations that differ in design schemas across attributes such as consensus algorithm, data accessibility, mutability, decentralization, and design architecture focus. Additionally, some blockchain projects focus on developing the blockchain architecture itself (i.e. the platform level), while other blockchain projects build on top of blockchains to implement specific functions (i.e. the application level).

Besides blockchain, other forms of DLT include hashgraphs, directed acyclic graphs, and tangles. Hashgraphs are DLTs that rely on computational gossip to achieve consensus and are structured like interweaving chains.^{5,6} Directed acyclic graphs use an alternative data structure—their eponymous structure—to store data, allowing for parallel transactions and branches.⁷ Tangles use portioning and inter-node transactions to implement novel network structures that make them well-suited for Internet of Things (IoT) applications.⁸

While blockchain is currently the most popular DLT, alternative DLTs such as the aforementioned ones may be more appropriate depending on the application type and data requirements. Likewise, compared to traditional databases (centralized ledgers), blockchains offer advantages such as increased security, improved information integrity, and decentralization, which may make blockchains and DLTs more effective for certain functions (such as IoT).

5 December 9, 2017. <https://cryptoslate.com/hashgraph-vs-blockchain/>.

6 “Hedera: A Public Hashgraph Network & Governing Council.” Hedera Hashgraph, 2019. <https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf>.

7 (June 20, 2018. <https://medium.com/fantomfoundation/an-introduction-to-dags-and-how-they-differ-from-blockchains-a6f703462090>.

8 Schiener, Dominik, May 21, 2017. <https://blog.iota.org/a-primer-on-iota-with-presentation-e0a6eb2cc621>.

Common Applications and Market Development

As a form of information management, blockchain can and has been applied to many industries, ranging from IT to healthcare to energy. The blockchain market has been growing rapidly in the last three years, and the main companies in this space are divided into three groups that directly reflect the three categories of blockchains: public, private, and consortium.

Most public blockchains offer platform-as-a-service (PaaS) and provide tools for users to develop blockchain-based applications, or DApps (decentralized applications). Such DApps are in various stages of market-readiness, and the most popular deployed DApps include those focused on gaming, trading, and payments. Cryptocurrencies are also implemented on public blockchains, and commonly exist as coins (akin to digital currency), utility tokens (tokens used as a fee for using the blockchain), or security tokens (tokens that represent a digital security). Of the three blockchain types, public blockchains have fueled much of the recent blockchain hype and Initial Coin Offerings (ICOs) and may pose significant legal and regulatory risks. In particular, many “users” of public blockchains utilize them as speculative investments (i.e. cryptocurrencies) rather than for the blockchain technology itself. Major groups working on public blockchains include Ripple Labs (the Ripple protocol)⁹, the Ethereum Foundation (the Ethereum public chain)¹⁰, and block.one (the EOS public chain)¹¹.

Private blockchains tend to be offered as software-as-a-service (SaaS) or infrastructure-as-a-service (IaaS) and can be general (such as blockchain network management) or adopted to industry-specific functions (such as for electronic voting and for supply chain tracking). Most enterprise solutions and applications are built on private blockchains, which may be more practical than public blockchains due to decreased energy costs, increased consensus efficiency, faster processing times, and stronger privacy. Many private blockchains are hard forks of or inspired by public blockchains. Major groups include Amazon (Amazon Managed Blockchain)¹², IBM (IBM Blockchain)¹³, Microsoft (Azure Blockchain Workbench)¹⁴, MasterCard (MasterCard Blockchain API)¹⁵, and JP Morgan (Quorum)¹⁶.

Consortium blockchains focus on specific applications for use among members of the consortia and are more commonly used in the banking and finance sector as well as in supply chain and energy applications. Advantages offered by consortium blockchains over conventional systems include reduced transaction costs

9 “Ripple,” n.d. <https://ripple.com/>

10 “Ethereum,” n.d. <https://www.ethereum.org/>

11 “Block.one,” n.d. <https://block.one/>

12 “Amazon Managed Blockchain,” n.d. <https://aws.amazon.com/managed-blockchain/>

13 “IBM Blockchain,” n.d. <https://www.ibm.com/blockchain>

14 “Azure Blockchain Workbench,” n.d. <https://azure.microsoft.com/en-us/features/blockchain-workbench/>

15 “Mastercard Blockchain to Bring Visibility to Food Systems,” (2019, October 27). Retrieved from <https://newsroom.mastercard.com/press-releases/mastercard-blockchain-to-bring-visibility-to-food-systems/>

16 “Quorum,” n.d. <https://www.jpmorgan.com/global/Quorum>

and data gaps. Major consortiums include Hyperledger Fabric (spearheaded by the Linux Foundation)¹⁷, Corda (focused on financial transactions and coordinated by R3)¹⁸, BlockApps¹⁹, and the Energy Web Foundation (focused on tracking and trading environmental compliance credits)²⁰.

In considering blockchain applications, it is also important to understand blockchain's limitations and whether blockchain is appropriate for a specific application. Whereas many ICOs and public blockchain projects failed to deliver on their promised functions (due to both technological limitations and fraudulent behavior), there are instances where blockchain may be appropriate, especially in cases where blockchain can coordinate shared information or settle transactions among decentralized actors. Such cases are more prevalent among private and consortium blockchains. Blockchains may also have disadvantages for a given application, such as intensive capital costs for initial deployment, the potential to exacerbate societal or market inequalities depending on who has access to the blockchain, and potential accessibility challenges for regulators when industry-wide blockchain ecosystems are developed. Thoughtful approaches to regulation and development can help prevent or mitigate these challenges.

Current State of Governance and Regulation

Regulating blockchain is challenging due to its decentralization and rapid development. Thus far, there are two key regulations that affect blockchain development: GDPR and the SEC Act of 1934, 21(a). GDPR is a European law that establishes strict guidelines for data privacy, including the right to be forgotten; this poses a number of challenges for blockchain due to its immutability and data transparency.²¹ In particular, since GDPR requires a right to be forgotten, there are some analyses that conclude that blockchain is incompatible with GDPR because of its immutable nature. The SEC Act of 1934 is a securities law that has been applied specifically to cryptocurrencies and ICOs; this regulation has slowed the pace of ICOs in the United States, though it may be relevant to blockchain projects in other domains.²²

Other domestic legislation has been of limited effect, though on the whole supportive of blockchain technology. The Congressional Blockchain Caucus was formed in 2016 to support blockchain development with a hands-off regulatory approach, and Co-Chair Representative Tom Emmer introduced HR1102 as a statement of support for blockchain.²³ At the state-level, various state legislatures such as those of Arizona,

17 "Hyperledger," n.d. <https://www.hyperledger.org/>

18 "Corda Enterprise—a next-gen blockchain platform," n.d. <https://www.r3.com/corda-platform/>

19 "BlockApps Powers Business Ecosystems," n.d. <https://blockapps.net>

20 "The Grid's New Digital DNA," n.d. <https://www.energyweb.org/technology/energy-web-chain/>

21 Finck, Michèle. "Blockchain and the General Data Protection Regulation." European Parliamentary Research Service, July 2019. [https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU\(2019\)634445_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf).

22 Securities Exchange Act of 1934, Section 21(a) (2018).

23 Brito, Jerry. "Bipartisan Blockchain Caucus Formed in Congress," September 26, 2016. <https://coincenter.org/entry/bipartisan-blockchain-caucus-formed-in-congress>.

Wyoming, and Vermont have passed legislation recognizing the legality of blockchain smart contracts, ownership rights, and storing public records on blockchain.

On the non-governmental side, there has been limited work done by external groups on blockchain governance frameworks. Most intergovernmental groups (G20, OECD, etc.) have focused on cryptocurrency regulation, subject to the laws of each nation, while industry associations and NGOs are still exploring applications of blockchain, responding to government regulations, and focusing on high-level implementation principles with limited direct technical links to blockchain design.

Most current blockchain regulation is self-regulation via the developers and communities. Unlike many existing technologies, the core principles of blockchains are directly enforced through technological design (i.e. algorithms which ensure that all transactions comply with the rules of the blockchain). The prime blockchain example is the Bitcoin public chain. The principles pushed forward by Bitcoin (such as anonymity, decentralization of authority, transparency, etc.) are reflected in its design (a form of code as law). Disagreements over core principles may lead to “hard forks,” or splits of the public chain. These essentially split the ledger into two ledgers that share the same root but develop separately at the point of forking (ex. Ethereum).²⁴ Thus, blockchain code and design enforce best practices and principles agreed upon by the developers and community.

An apt comparison can be made with databases: as basic tools, databases don’t have any significant principles with respect to public good. While similar to databases, blockchain differs in that it is shared, and thus the community decides on the principles that govern its usage.

24 Islam, A.k.m. Najmul, Matti Mäntymäki, and Marja Turunen. “Why Do Blockchains Split? An Actor-Network Perspective on Bitcoin Splits.” *Technological Forecasting and Social Change* 148 (2019): 119743. <https://doi.org/10.1016/j.techfore.2019.119743>.

Public Purpose Considerations

Blockchain has the potential to advance important elements of public purpose, such as:

- **Data Security:** Blockchain can enhance data security through decentralization or having exact copies of the same ledger stored and updated simultaneously on all system nodes. This prevents individual actors from taking control of or maliciously editing data ledgers and offers an advantage over centralized databases when paired with encryption.²⁵
- **Data Integrity:** Blockchains, along with their consensus algorithms and private key identifiers, help ensure data integrity and validate that all data stored has been approved via the consensus algorithm (i.e. no external unwanted data inserted). Depending on data and architecture type, blockchains may also verify the authenticity of the data as well as the validity of the transaction.
- **Transparency:** All transactions and information on blockchains are available to the network in encrypted form. This can increase the transparency of real-world processes and information, such as identities, electronic voting, and public utility costs.
- **Inclusivity/Accessibility:** Blockchain can help connect rural populations to digital infrastructure in a secure way across various domains, such as micro-financing, access to accurate market prices and information, and verification of humanitarian aid.

At the same time, blockchain faces risks and challenges in many areas, such as:

- **Data Privacy & Ownership:** Due to the distributed and immutable nature of blockchain information, data privacy and ownership are among the biggest challenges for blockchain. Some blockchain features seem at odds with existing regulations (such as the right to be forgotten and blockchain's data permanence), while other data privacy features such as identity verification are not implemented consistently across blockchains.²⁶
- **Legality:** With smart contracts being one of the popular tools on blockchain, the validity and legality of smart contracts and other blockchain-based agreements must be squared with traditional principles of contract law.²⁷ Additionally, blockchain provides a tool to transfer ownership of digital

²⁵ Lee, Jae Hyung. "Systematic Approach to Analyzing Security and Vulnerabilities of Blockchain Systems." Massachusetts Institute of Technology, February 2019. <https://web.mit.edu/smadnick/www/wp/2019-05.pdf>.

²⁶ "Blockchain and the General Data Protection Regulation."

²⁷ Levi, Stuart D., and Alexis Lipton, May 26, 2018. <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>.

assets and information, so effective rules and governance structures to regulate ownership transfers are critical.

- **Financial Risk:** Cryptocurrencies and tokens are currently one of the main uses of blockchain, and additional certainty is needed in this space (such as for trading of securities-equivalents, tokenization of assets, taxation of cryptocurrencies, etc.).
- **Digital Divide:** Current blockchain tools and smart contracts rely heavily on code, which can be risky for non-coders who cannot verify the stated function of the code. Moreover, there is not enough public education about blockchain, resulting in skewed understanding of the technology.
- **Platform Self-Regulation:** Even more so than centralized platforms, decentralized platforms such as blockchain also face self-regulation challenges with regards to stewardship, corrective actions, data responsibility, user rights, and other areas.
- **Technical Implementation:** Blockchains still face many technical challenges, including cybersecurity, reversibility of data, and loopholes in the code.
- **Scalability & Sustainability:** Depending on the type of consensus algorithm used, some blockchains are difficult or impractical to scale, due to both transaction speed limitations and energy costs/sustainability. This is primarily relevant to fully-distributed blockchains and public blockchains, and there are emerging consensus algorithms that increasingly address the problems of scalability and sustainability.
- **Enduring Security:** Encryption techniques have a finite lifespan as computing power increases and decryption techniques evolve, therefore encrypted data in an immutable blockchain may likely become vulnerable at some point in the future.
- **Codifying Negative Social Impacts:** Blockchain technologies can be used to further solidify monopolistic or other societal power inequities based on who is involved in creating and enforcing the rules of a blockchain and who is given access to participate in the blockchain.²⁸

The above risks and challenges are of immediate concern, as they directly affect the structure and implementation of blockchains and blockchain applications. Since the technology is still in the early stages, proper regulation can limit negative developments in the blockchain space.

28 Longstaff, Simon. "Blockchain: Some Ethical Considerations," March 25, 2019. <https://ethics.org.au/blockchain-some-considerations/>.

APPENDIX A:

Key Questions for Legislation and Regulation of Blockchain Technologies

Cybersecurity

- What testing process has your blockchain undergone to detect bugs and limit cybersecurity risks?
- What technical features have you implemented to prevent or deter cyberattacks (such as phishing, man-in-the-middle, etc.) targeting users' private keys?
- What precautionary measures or backdoors are in place, in case the chain is hijacked?

Privacy and Data Ownership

- Who will have access to the data stored on the chain and in the chain ecosystem (including DAPPs, wallets, etc.)? What specific data will be stored on the chain, and what data will be stored off-chain (for example, in the case of a DAPP)?
- Who owns the data stored on the chain? Do individual users own their own data, or do they have the rights to all the data stored on the chain (regardless of encryption)?
- Is it reasonably feasible for an entity to access/identify private information or data, based on publicly-shared information on the chain such as the blockchain's transaction history/ledger?
- How have you implemented your blockchain for data privacy (beyond encryption), data removal or chain modification, and the "right to be forgotten"?
- How do you prevent private or personal data from unwillingly being placed on the chain? What corrective measures are in place to remove such data if requested?

Consumer Protection and Accessibility

- Blockchains function based on users holding private digital keys that provide access and control to all of their information and assets on a blockchain, so is there a process for users to reset their access in the event of a lost private key? Who handles this process?

- How does your user registration process verify the identities of users and detect fraudulent accounts? Do you know your users?
- What process is in place to regulate and review smart contracts, so that they are safe for users and perform the functions described? Is there anything similar to the Apple AppStore in place?
- How are you protecting code illiterate users and making code-dependent or code-based blockchain functions accessible to them?
- Does your chain use transaction fees or “gas” for processes? How are transaction fees set, and how will you ensure they are affordable?
- How do you ensure the system-specific technology literacy of your users? Is there a qualification process for participants?

Product Safety and Compliance

- Who in your chain community will regulate the chain, hold stewardship, and accept responsibility for any damages? How are they selected, and what authority will they hold?
- Will your chain allow for the creation of cryptocurrencies and assets trading? If so, how are you ensuring compliance with the SEC and other relevant entities?
- What role will the original developers play in the management of the chain? How will this be balanced with the decentralized nature of blockchain technology?
- What is your token sale or distribution process? What makes it different from an ICO?
- How is verification of non-digital assets accomplished for relevant entries into your blockchain? How is the initial, or “zero,” state of your blockchain verified?

Technical Development and Challenges

- Why is blockchain—as opposed to conventional systems such as databases—needed to achieve your stated functions? What advantages does a blockchain implementation offer, and what are the potential disadvantages?
- What makes your blockchain different from other blockchains?

- What are the main challenges of your consensus algorithm with regards to scalability, control attacks/hijacks, equity/accessibility for new users, and sustainability?
- What is the current average transaction speed of your chain and number of users? How do you predict that speed will change with increased scale?
- What applications have been developed and deployed on your chain? How many users are there for these applications, and what are the comparative benefits over non-blockchain solutions?
- Do the appropriate government regulators have adequate access to your blockchain to fulfill their legal responsibilities?



HARVARD Kennedy School

BELFER CENTER

for Science and International Affairs

Technology & Public Purpose Project