NEW AMERICA

January 2019

The Blueprint for Blockchain and Social Innovation

Tomicah Tillemann, Allison Price, Glorianna Tillemann-Dick, & Alex Knight

Last edited on January 22, 2019 at 10:35 a.m. EST

Acknowledgments

Throughout the process of conceptualizing, researching and crafting the blueprint, our team has been extremely fortunate to partner with the Tata Trusts. Tata Trusts funded the blueprint to ensure that the benefits of blockchain technology transcend high-finance and reach individuals with the greatest needs. The Tata Trusts—India's oldest philanthropy—operates at the leading edge of efforts to improve lives and livelihoods across India. Their team, including Karthik Ramesh, R Venkataramanan (Venkat), and Shloka Nath, was quick to recognize the potential for blockchain to enhance the effectiveness of civil society and government organizations as they work to solve public problems. We have been honored to work together in this effort, and look forward to the Tata Trusts' expanding thought leadership and efforts to develop digital public goods to meet the needs of society in the 21st century.

We would like to thank Dahna Goldstein, Chris Doten, Veronica Garcia, Nakshidil Sadien, Asvatha Babu, Qiuyun Shang, Colleen Wong, and Julia Rhodes. We are also grateful to Nakul Saran and the participants of the Bellagio Blockchain Summit; Brian Behlendorf, E. David Burt, John Paul Farmer, Vanessa Grellet, Fuzz Hogan, Zia Khan, Cara LaPointe, Jens Molbak, Robert Opp, Laura Shin, and Sheila Warren, as well as our many colleagues with New America. Thank you for taking the time to share your perspective, time, and support. Critically, this Blueprint would not have been possible without the research contributions and diligence of our intrepid intern, Ben Gregori.

If the research herein amounts to anything, it is because of the openness of the blockchain community. Thank you: Abhay Gupta, Ad Kroft, Adithya Kumar, Alex Tong, Andrew Bakst, Ankur Kapadia, Ari Juels, Aymard Dudok de Wit, Baloko Makala, Ben Burke, Ben Joakim, Bob Visnov, Brian Waterhouse, Charlie Knoll, Chris Wood, Christopher Verceles, Cole Riccardi, Cooper Schorr, Daniel Yim, David Huysman, Elliott Hedman, Emily Mitchell, Ethan Schmertzler, Felipe Daguila, Fennie Wang, Frank Yiannas, Ish Goel, Jaka Jaksic, Jamie Green, Jess Houlgrave, Jörgen Modin, Joseph Bonneau, Ken Marke, Kevin Hu, Megan Cojocar, Mert Ozdag, Mike Kalomeni, Nick Martitsch, Pablo Tutino, Philip Gradwell, Priyanka Dekhar, Pulkhit Agarwal, Raphael Mazet, Richard Li, Riley Hughes, Russell Yanofsky, Sam Ng, Shailee Adinolfi, Stephanie Seale, Stephany Zoo, Stephen Hadeed Jr., Sterling Johnson, Tejas Bhatt, Titus Capilnean, and Zhuzeng Lu, as well as Valery Vavilov, George Kikvadze, John Mercurio, and Kathleen Collins of Bitfury.

We would also like to thank the following blockchain for social innovation pioneers for reviewing our case studies: William Collins, Brooklyn Microgrid; Nick Miller and Angus Keck, AgUnity; Jonathan Simms and Gustav Stromfelt, World Food Programme; Drew Sadler, Walmart; Eva Arevou and Kiran Jain, Neighborly; Shaun Frankson, Plastic Bank; Rachel Pipan, Bitfury; Deak Kersey, West Virginia Secretary of State's Office; Nimit Sawhney, Voatz; and Jennifer Brody, NDI.

About the Author(s)

Dr. Tomicah Tillemann is co-founder and Director of the Blockchain Trust Accelerator at New America, which works with organizations including the Rockefeller Foundation, State Department, Coca-Cola, Harvard and Levi Strauss to deploy blockchain solutions in governance and social impact applications worldwide. He chairs the Global Blockchain Business Council and advises Bitfury and other leading technology companies. He previously served at the State Department and Senate Foreign Relations Committee as a speechwriter and advisor to Hillary Clinton, John Kerry, and Joe Biden. He was educated at Yale and Johns Hopkins and is a co-holder of four patents.

Allison Price is the executive director of the Blockchain Trust Accelerator, a project of New America. The BTA is committed to advancing blockchain technology through research and innovative pilot projects designed to address some of the world's most persistent challenges like transparency, identity and corruption. Prior to diving into the global blockchain community she served in senior public affairs positions with the Department of Justice and the Peace Corps. Price worked at the intersection of public policy and communications for Obama for America, the Center for American Progress, Gillibrand for Congress, and Stonebridge International. She earned degrees from the University of Pennsylvania and the London School of Economics.

Glorianna Tillemann-Dick is a Blockchain Trust Accelerator Fellow at the New America. Prior to her time at New America, Tillemann-Dick volunteered as an instructor at the Mongolian National University of Medical Sciences in Ulaanbaatar, where she learned to enjoy horse meat shish-kebabs. During her matriculation, Tillemann-Dick founded A Curated Dialogue, LLC. The consultancy worked with industry leaders in pharma, tech, finance, academia, and entertainment to relate big ideas to broad audiences. She has her degree from Yale University.

Alex Knight was a Blockchain Trust Accelerator (BTA) Fellow at New America while researching the Blueprint for Blockchain for Social Innovation. He matriculated at the Stanford Graduate School of Business in the fall of 2018. Before becoming a fellow, Knight was a financial analyst at Blue Ridge Capital and Tiger Management, where he invested in public and private companies mostly in the media, software, internet, and cable industries. He became intrigued by blockchain technology while doing investment research and was struck by its potential to change the public, non-profit, and private sectors. Alex graduated from Yale University.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Bretton Woods II

Bretton Woods II is engaging sovereign wealth funds, pension funds, endowments and family offices to build a new business model for social finance. The initiative is harnessing analytics, advocacy, and financial tools to channel part of the $25 trillion controlled by long-term asset holders into strategic investments in social impact that address the root causes of volatility. The effort aims to help close the gap in financing for the Sustainable Development Goals while increasing investors risk-adjusted returns.

Contents

Contents Cont'd

Contents Cont'd

Preface

Law. Scientific discovery. Civilization itself. Trust rests at the core of our greatest human endeavors. It is the mechanism by which we collaborate and progress. It sustains communities and builds successful societies. When trust erodes, human progress goes with it.

Historically, institutions have served as custodians of trust. They safeguard the facts and systems that allow human beings to cooperate effectively at scales. But global confidence in institutions has dropped precipitously in recent years.[1] As the vulnerabilities and inefficiencies of existing institutional structures have emerged, these pillars of modern civilization have started to falter under the weight of antiquated systems, human error, and heightened public scrutiny.

Blockchain technology has been called a ‘trustless’ system. In fact, the opposite is true. Blockchain isn’t a replacement for or a shortcut to building trust. Rather, it is a trust accelerator, giving individuals and organizations a head start in cultivating solid relationships, built on a foundation of security, accountability, and transparency. Blockchain is an opportunity to establish previously untenable channels for collaboration and reinforce existing partnership, lengthening and strengthening the ties that bind us to each other.

To date, blockchain has been deployed most often in for-profit sectors such as finance. However, many of the technology’s most promising applications lie in the fields of social and civic innovation. Realizing this potential will only be possible as organizations push forward the frontiers of trust. As blockchain solutions are more widely applied to address global inefficiencies, their potential to fortify institutions and improve lives will become more powerful and could usher in the next chapter in the story of human cooperation.

Overview

The Blueprint for Blockchain and Social Innovation leads with a basic technical overview of blockchain technology and explores applications to increase security, accountability, and efficiency at every level of social infrastructure. After this exploration of blockchain's processes and potential uses, the Blueprint provides recommendations for those weighing the potential costs and benefits of a blockchain solution within their organizations. The Blueprint explores some real-world case studies, with examples in industry, foreign assistance, government, and media. Finally, it offers some insights on the future of blockchain. A synopsis of each section is included in this overview; read the sections which strike you as relevant.

Published alongside the blueprint is a ***Checklist for Deploying a Blockchain-Powered Solution***, as well as a glossary of ***100 Key Terms for Harnessing Blockchain in Social Impact*** (an important resource in a landscape where universally accepted definitions are hard to find).

Understanding the Technology

How do blockchain users deal directly with strangers with a high degree of trust? What types of data can be exchanged on a blockchain? How does blockchain maintain both transparency and security? How does blockchain interact with other technology? This technical review helps readers to understand the answers to these foundational questions.

Key Attributes of Blockchain

Blockchain boasts three game-changing attributes that can address the erosion of trust in public institutions: security, accountability, and efficiency. The lines between each of these traits are not rigid—features of blockchain contribute to more than one of these attributes; conversely, a blockchain solution may involve trade-offs. The origins and potential applications of each of these attributes are discussed at length within this report, along with possible challenges that may accompany them.

Solution Design

Blockchain platforms are not ready-made. Organizations wondering whether to implement blockchain-based solutions must first consider some basic prerequisites and anticipate potential inefficiencies. Established alternatives will often serve organizations better than an untested blockchain fix. However, if blockchain remains a promising option after initial evaluations, this blueprint offers guiding questions to direct design processes and identify an optimal solution—whether it relies on blockchain or related technologies. If, after a thorough investigation, blockchain does emerge as the best solution, this blueprint offers design recommendations to help organizations tailor a blockchain platforms to their particular needs and users.

Case Studies

- *Aid Provision—Building Blocks: UN World Food Programme*
- *Land Records—Republic of Georgia*
- *Supply Chain Management—Walmart*
- *Energy Management—LO3 Energy and Brooklyn Microgrid*
- *Financial Inclusion—AgUnity*
- *Mobile Voting—West Virginia*
- *Social Investment—Neighborly and City of Berkeley Blockchain Initiative*
- *Environmental Sustainability—Plastic Bank*
- *Combating Fake News—Democracy Notary*

The Future of Blockchain for Social Impact

Those considering blockchain systems as well as those who have already adopted them should remain abreast of ongoing developments in the blockchain ecosystem. Emerging topics of significance are discussed in this section of the blueprint.

Understanding the Technology

Blockchain. Everyone is talking about it. Hardly anyone understands it. Lauded as transformational technology in fields ranging from financial services to agricultural supply chains, blockchain promises to create and secure value across industries. But what if you care about more than financial return on investment? Can blockchain technology also solve problems for society?

Yes. Blockchain technology has the potential to recontour civic landscapes. It can safeguard data, simplify service delivery, clarify outcomes, and ensure accountability. Simply put, blockchains help build and sustain trust. Harnessed strategically, blockchain-based solutions can do much more than widen profit margins; they can also improve lives and society.

Spoiler alert: A blockchain may not be the answer to all (or any) of your problems. Blockchain is a powerful tool, but it's not a substitute for decent leaders or well-designed processes. This report endeavors to equip readers with a working knowledge of the technology so you can perform an informed assessment of the technology's potential relevance in your field. Education and collaboration offer the best foundation for successful blockchain solutions that create real value. This paper provides a framework for realizing that goal.

Blockchain 101: How it Works

In a sentence, blockchain is a record keeping system with two important attributes: it is distributed (with copies of the record stored on multiple computers) and permanent (easy to update, but exceptionally difficult to modify). You likely have a spare house key or backup photo storage; at its core, blockchain functions on a similar principle. It's a single cache of important information, typically digital records or financial transactions, stored securely by multiple sources. The idea of a decentralized or ***distributed ledger***[2] isn't new, but blockchain architecture applies the concept in innovative ways.

Blockchain is a frontier technology, but it's built on a foundation of proven innovations that have existed for decades. Blockchain combines established technologies to create accountable, secure, efficient platforms for exchanging data.

→ WHAT IS BLOCKCHAIN?

blockchain: (*blok-chayn*) (noun) A distributed ledger technology that empowers anyone with an internet connection to transfer data and assets frictionlessly—anywhere, anytime, with unmatched security and integrity and without relying on a third party intermediary. The first blockchain was conceived in 2008, in the wake of the global financial crisis. It has never been hacked.

Foundations

Identity and Trust

Identity is the essential ingredient of an effective, secure blockchain. Each blockchain solution will have its own identity requirements for first-time users; these may include verification through government identification, personal information, or biometric data such as fingerprints or iris scans. However, once a user's identity has been successfully established on a blockchain, the need to re-share personal data is eliminated. The system takes over, affording participants unprecedented convenience and security via a process called "public key cryptography" (PKC).

PKC uses a series of digital keys to simultaneously verify identity and protect privacy on blockchains. Traditionally, institutions like banks act as trust-brokers, allowing strangers to transact with a high degree of confidence. These third-party intermediaries often work well, but they can come with high barriers to entry, substantial costs, and inconvenient procedures that limit their utility for much of the world's population. Blockchains remove the need for third party intermediaries and enable trusted, ***peer-to-peer***[3] transactions through PKC.

Public key cryptography identifies parties to each other via ***public keys***.[4] This key functions like a P.O. Box—publicly visible, alterable, and ***pseudonymous***,[5] with the primary goal of facilitating ***transactions***.[6] PKC then validates their identities via ***private keys***[7] before executing any exchange. A private key unlocks the proverbial P.O. Box, providing its owner exclusive access to any materials stored inside. Public key cryptography facilitates accountability for blockchain users while protecting individual data.

Blockchain combines established technologies to create accountable, secure, efficient platforms for exchanging data.

Data

A person at a grocery store can exchange money for a loaf of bread. But what if you're operating in an entirely virtual space? Blockchain transactions can include a wide variety of sensitive data transfers: financial transfers, identity confirmations, inspection certifications, land receipts, and more. Data can represent tangible assets, like currency, records, identity details, or ownership titles. Information can be unencrypted (plain), encrypted (hidden), or a representative ***digital signature***[8] (a hash) for goods stored ***off-chain***.[9]

No matter the type of data being exchanged, it's imperative that it is accurate and high-quality. Blockchain's stringent protocols make logged information exceptionally difficult to alter or expunge, so if you start off with poor data, you may be stuck with it forever.

Building a Blockchain

Several types of blockchain exist, but generally they involve a basic three-step process:

- Encryption-facilitated data exchanges occur between blockchain participants.
- A series of these transactions are grouped together to produce a locked data "block."
- New blocks are linked to previous ones via a cooperative ***validation***[10] protocol, thus forming a "blockchain."

Blockchains are like trees, becoming stronger as they grow larger. Like a new ring in a tree trunk, a new block on a blockchain records a specific moment in the entire chain's history; the block does not exist independently, but is a development of the entire chain, inseparably grafted onto the blocks preceding it by complex algorithms, ensuring validity and accuracy over time.

The addition of each new data block makes it increasingly difficult for unauthorized changes to occur. Just as you can't remove a single tree ring without compromising the entire trunk, the information recorded on a single block cannot be isolated or altered without affecting the entire blockchain. Each new block grows from the blocks preceding it, and in turn helps to secure and inform all subsequent blocks added to the chain.

Creating Blocks

Individual ***blocks***[11] are made up of groupings of unique transactions, or record updates. These occur constantly over a distributed network, and a blockchain system usually has multiple computers, or ***nodes***,[12] that constantly process new updates.

Record updates are added to a pool as they occur, and nodes within the network sequence them according to a timestamp. These "miner" nodes create a new block of record updates, which then awaits verification and addition to the chain. When enough data is added to the block, a checksum or "hash" is added that is unique to the records it contains. This hash functions like a fingerprint for each block of data in the chain. If a single character of a single record update is altered, the final hash will change dramatically. A block can only be added to the chain once a majority of nodes in the blockchain agree that its record update data is valid. If over half of a blockchain's nodes cannot verify a block's data, the block is rejected.

Reaching Consensus

The rules that determine how to validate new entries on the chain are known as ***consensus mechanisms***.[13] They allow all nodes in a blockchain system to collectively agree on new additions to the chain, ensuring network integrity. An effective consensus mechanism will incentivize validators to confirm legitimate blocks quickly and reliably.

Consider just one of the myriad consensus mechanisms currently in use to illustrate the concept: In a ***Proof of Stake***[14] protocol, validators (certain nodes of the blockchain) place stakes. These stakes act as part bet, part security deposit. If a validator is chosen and confirms a legitimate block, she receives compensation and the block is added to the chain. However, if the validator confirms a fraudulent block, her stake is forfeited and a new validator is selected. The protocol's forced buy-in offers both a carrot and a stick to validators, promising rewards for correctly validated blocks and while penalizing specious validations with the loss of a stake.

Each breed of consensus mechanism has its own challenges and strengths and can be adopted dependent on a particular blockchain's goals, security considerations, and network type. Other examples include ***Proof of Work***,[15] Proof of Burn, ***Proof of Authority***,[16] Practical Byzantine Fault Tolerance, Proof of Importance.

The information recorded on a single block cannot be isolated or altered without affecting the entire blockchain.

Lengthening a Chain

Once a block of data has been validated by consensus, it's ready to be connected to the rest of the chain. The new block not only incorporates data from the transactions it represents, but also a digital fingerprint of every block preceding it —firmly securing it to the entire chain. Now the block is largely tamper-proof; retroactive edits to any part of the chain will produce code divergent from that stored on every block previously appended to the chain, invalidating any new block and assuring that the record remains secure.

Choosing Your Own Blockchain

A blockchain ***protocol***[17] connects different computers in the network. Programmers can alter frameworks around this protocol to suit specific use-cases. There are two basic questions at the foundation of most blockchain protocols:

Public vs. Private: This refers to the ***openness***[18] of a blockchain to outside users. Public blockchains, like ***Bitcoin***[19] and ***Ethereum***,[20] are completely open, allowing anyone to interact with the network. A private blockchain like ***IBM's Hyperledger***[21] has a governing group that determines which and to what degree users can access a blockchain.

Private and public blockchains can assign different privileges, or "***permissions***,"[22] to users. A permissionless blockchain gives every computer an equal amount of authority to operate on a blockchain. Permissioned blockchains assign different capabilities to each computer on the blockchain, such as reading data, writing data, or verifying data and storing copies of a blockchain. A consortium of banks may appoint an administrator to control who can access their private blockchain, even though, once accepted, all computers on a blockchain can interact with it. Conversely, governments seeking to be transparent with their citizens may use a public permissioned blockchain to provide full visibility of certain records, but only allow government administrators to create entries on a blockchain.

Open Source[23] **vs. Proprietary:** This distinction refers to the level of transparency and accessibility in a blockchain. To qualify as open source, a platform must be distributed for free and function with transparent and modifiable source code.[24] Open source blockchains spur innovation, fortify security, and facilitate accountability and transparency in data infrastructures. They're ideal for refreshing antiquated infrastructure like voting systems or healthcare services. Alternatively, proprietary systems are typically leveraged for monetization or to protect market share in competitive landscapes; they can unintentionally lead to vendor lock-in.

Blockchain 102: Token Economics, Smart Contracts, AI

Token Economics

For a blockchain to function effectively, there must be incentives for users, programmers, and other actors in the system. Developers accomplish this with ***tokens***.[25] Digital tokens exchange real value by a method unique to their particular blockchain ecosystem. The most popular use of tokens is as currency, such as Bitcoin or ***Ether***,[26] but they can fill a number of roles. They may signify ownership over assets like land titles or carbon credits, be exchanged for services, earned by curating digital content or spent by consuming that content. Tokens could even represent a vote in a municipal election or board meeting. The possibilities are expansive.

Blockchain-based token economies are new and the rules that govern them are as adaptable as the code that dictates their behavior. This flexibility has the potential to enable innovative forms of value distribution and creation, potentially uprooting assumptions about traditional market behavior and providing fertile ground for business models that were previously impractical due to, for example, high transaction costs.

Smart Contracts

"***Smart contracts***,"[27] can be programmed to facilitate binding exchanges with specific conditions executed from a blockchain. Once rules and penalties are agreed to by parties, a smart contract becomes a self-executing and self-enforcing contract—all without ***intermediaries***[28] like banks, brokers, or lawyers.

For example, say a farmer needs to collect insurance after losing crops to drought. A smart contract could cross-reference the farmer's land records with local weather reports. If the report showed that the farmer lived in a drought-affected region, the smart contract would automatically execute and provide him or her with aid. This is just one example of the many ways in which smart contracts could increase efficiency, reduce misallocation, and eliminate bureaucratic friction.

Artificial Intelligence

Blockchain and ***artificial intelligence***[29] (AI) could prove to be a powerful pairing in a twenty-first century economy, providing security and accountability to the machines that will increasingly guide human decision-making. Each week brings new stories of the promises and perils of AI. One day it's forecasting outbreaks of infectious disease, the next it's going on Twitter rants. Blockchain technology offers stable data infrastructure that may not only help manage potential challenges of AI, but also distribute the gains possible through AI more equitably across the future digital economy. Blockchain-based data wallets could decentralize and democratize ownership of the data that powers AI systems. As AI steers cars and predicts weather, a blockchain could clarify and fortify the link between machines and the algorithms determining their choices, reducing vulnerability to exogenous threats like hackers.

Blockchain and AI could be a powerful pairing, providing security and accountability to the machines that will increasingly guide human decision-making.

Conclusion

There are many different flavors of blockchain. Some facilitate greater openness and flexibility, while others prioritize privacy and proprietary access. Some blockchain solutions may utilize complimentary technologies. Others won't require it. While determining which features to include in a potential blockchain solution, an organization must carefully consider the context within which that blockchain will function. The "best" blockchain does not exist, only the best blockchain for your organization and the goals you're aiming to achieve.

Key Attributes of Blockchain

"Why Blockchain is a Game Changer for Supply Chain Management Transparency"[30] "How Blockchain Can Disrupt the Future of Education"[31] "Is Blockchain the Answer to a Better Healthcare Industry?"[32] Why does an esoteric data infrastructure framework provoke such exuberant headlines? The following section discusses the defining characteristics of blockchain, especially those with implications for organizations working to deliver social impact and better governance.

Blockchain boasts three game-changing attributes:

- **Security**
- **Accountability**
- **Efficiency**

These benefits enable blockchain to address many of the failings that have contributed to the erosion of public trust in institutions in recent years. The lines between each of these traits are blurred. Many features of blockchain contribute to more than one of these attributes; conversely, blockchain-based solutions may involve certain trade-offs, such as efficiency versus security, accountability versus privacy. Exploring each trait can identify meaningful blockchain-enabled impact opportunities and anticipate challenges facing successful deployment.

Security

Opportunities	- Public Key Cryptography - Censorship-Resistant[33] - Fault-Tolerant
Challenges	- Sustainability - Latency - Privacy

Our social and economic lives are becoming increasingly digital. Today, the most important items on life's to-do list can often be checked off without ever leaving our homes. Both individuals and businesses have become dependent on the internet for commerce, product delivery, data storage, and processing. These innovations have yielded monumental efficiencies, enabling people to reinvest money, time, and energy into new ventures. They have also created the need for secure transactions and recordkeeping.

Data security is the Achilles' heel of online innovation.[34] Unitary actors and large organizations wield disproportionate control and influence in the digital age, yet even these behemoths aren't protected from bad actors. So how can individuals trust that their information is safe in an ever-more fraught digital world?

Security is at the foundation of blockchain technology. The combined power of its high standards of data verification, ***multi-layer encryption***,[35] and distributed architecture could help re-establish public confidence in digital infrastructure. Three features of blockchain combine to provide these security benefits:

- **Secure data access and exchange**: Public key cryptography identifies transacting parties to each other via public keys, then validates their identity via private keys before executing any exchange. Public key encryption demands accountability from legitimate blockchain users and protects individuals' data against hackers.

- **No unauthorized changes**: Each new block on a blockchain must be cycled through the network's various computers, a piece of an algorithmic puzzle which will only fit if no previous information within the blockchain has been altered. If any data is missing or compromised, the addition is rejected. Once information has made it onto a blockchain, it stays there. No censorship. No hacks.

- **The network won't go offline**: Traditional databases are centralized, with single points of failure that can be compromised by malicious actors. But each node of a blockchain functions with autonomy. Redundant copies of a blockchain are stored on each of these independent nodes, providing insurance for the entire system if any single one is attacked, goes offline, or otherwise becomes inaccessible. Thus blockchains are considered extremely ***fault tolerant***.[36]

The Social Impact

- **Own your data**: Once you've entered personal information online, there are no guarantees; you lose control over whether and how it's bought, sold, viewed, or used. But blockchain-enabled ***self-sovereign identity***[37] empowers people to share sensitive personal data on their own terms, allowing entities to verify identity while accessing nothing more than an alterable public key. By applying blockchain tech to digital identity, individuals can finally control of their own data.

- **Make citizens' voices heard**: Repressive governments often deprive citizens of their right to information and communication by blocking access to specific websites. But blockchain technology facilitates access to content hosted on any node within the network by any of its users, making its content exceptionally difficult to censor. If countries hope to reap the benefits of blockchain, they must also commit to a high standard of access and transparency. This information equity can help shape more representative societies.

Challenges

- **Sustainability**: Executing the consensus mechanisms which verify blocks and secure a blockchain against hackers can require tremendous processing power from blockchain computers. Multiply that by every node in the network, and you're looking at a pretty massive energy bill. This can even cause nodes to cluster in low-cost energy markets, reducing the resilience of blockchain's dispersed architecture. New types of consensus mechanisms and widespread investment in sustainable energy sources like wind and solar will reduce blockchain's environmental footprint while increasing its security.

- ***Latency:***[38] Bigger blockchains typically enjoy higher fault tolerance, but all that information takes time to travel. Blockchain users have to wait until their transaction has been added to a fully populated block and successfully verified by a majority of nodes before it's completed and securely recorded on a blockchain. This means that the more secure a blockchain (the more nodes it has verifying blocks), the higher its lag time. This latency may pose scalability and usability challenges for larger blockchains.

Headlines about cyberattacks, online fraud, and data manipulation have deterred many from participating fully in the digital economy. Blockchain offers a solution. It can provide communities the confidence necessary to apply the benefits of digital innovation while mitigating some key risks. Policymakers must still make privacy, data quality, and sustainability considerations in designing blockchains, but as they do so, it should become easier to instill security into digital interactions that will encourage wider participation in an evolving economy.

Accountability

Opportunities	- Party Authentication - Append-only Entries - Transparency
Challenges	- Privacy - Safeguarding Identity

Global trends indicate a decline in institutional accountability. According to two 2017 reports, most countries "made little or no progress in ending corruption" and global confidence in both public and private institutions dropped precipitously.[39] As ethics abuses go unaddressed, a vicious cycle forms—those in power see peers act with impunity and become opportunistic themselves. This decay of integrity causes socio-economic disparities to widen and embeds dysfunction into systems, inspiring disruptive and, too often, violent uprisings. Blockchain technology can help foster cooperation with and accountability of global institutions via mechanisms which reintroduce transparency and traceability into human governance.

- **Transparency**: Anyone with a computer can view the full record of a public blockchain, making it nearly impossible to hide transactions and relatively easy for third parties to track data entries and keep blockchain honest. Even private blockchains, while less transparent, create secure, ***auditable***[40] paper trails.

- **No catfishing**: Public key encryption lets you know who you're doing business with on a blockchain. As long as private keys remain private, blockchain identity can't be faked.

- **Secure sequence and permanence**: Transactions can only be added to the end of a blockchain, and once they're there, they can't be deleted or edited. Timestamped, ***immutable***[41] entries reduce the likelihood of inaccurate or outdated data and preserve the integrity of a blockchain.

The Social Impact

From ensuring ethical, sustainable supply chains to tracking public financing, blockchain holds staggering potential to close loopholes and increase accountability of people in power.

- **IDing abusers**: Despite visual evidence of human rights violations and criminal behavior posted to social media, it can often be the good guys who have their hands tied by a dearth of reliable verification. By capturing the indisputable Who, Where, and When behind troubling digital content, the blockchain records hard data, thereby facilitating real-life action against abuses documented online. Data traceability gives local and international enforcement bodies the tools they need to hold wrongdoers accountable.

- **Countering counterfeiters**: Blockchain creates transparent, tamper-proof, timestamped records of supply chain processes. Sound a bit dry? Profits from fake drugs can surpass those of opioid trafficking, and their trade endangers some of the globe's most vulnerable populations. Blockchain solutions would allow pharmacies and consumers to verify a therapy's original source, so communities can trust that their medicines will combat illness, not cause it.

Challenges

- **Privacy**: The flip side of accountability is exposure. Blockchain's public key addresses tie records to individuals, creating a pseudonymous blockchain ID. While this is far more secure than using personal information like names or emails, third parties may still be able to analyze ***metadata***[42] trends to reveal the real world identity of transactors. That could put vulnerable populations—human trafficking victims, minority groups, political dissidents—at risk.

- **Hold onto your keys**: The authenticity of an identity on blockchain depends on private keys remaining private. If people were to gain access to another party's private keys, they could effectively steal the attached identity and perform fraudulent transactions.

By creating a record that's difficult to manipulate and easy to audit, blockchain takes aim at the global trust deficit. Blockchain has the capacity to provide clear evidence of wrongdoing and hold those in power accountable. Still, while transparency and third party verification can reduce corruption, verify content authenticity, and keep supply chains sustainable and ethical, considerations must be taken to protect sensitive information both on and off of a blockchain.

Efficiency

Opportunities	- Native Data Verification - Data Efficiency - Data Openness
Challenges	- Data Quality - Energy Consumption - Latency

Efficient systems are better for wallets, the environment, and long-term development. Yet government effectiveness in OECD countries has either remained consistent or declined over the past decade. The private sector isn't doing much better. One estimate placed U.S. losses at over $3 trillion in a single year due to poor data quality alone.[43] Institutions must catch up to growing demands by more fully optimizing shrinking resources. Blockchain boasts tantalizing system efficiencies, thanks to its error-resistant data architecture and decentralized structure.

- **Native data verification**: Autonomous verification could be very useful to organizations tired of record updates that conflict with previous versions. Requiring agreement among network nodes renders data errors unsustainable, preserving the ledger's accuracy.

- **Low-risk infrastructure**: Decentralization removes intermediaries from transactions, preventing bottlenecks or indirect pathways that slow down information transfers. Furthermore, requests for updating the blockchain only have to travel to the nearest node rather than to a central database, increasing efficiency in data movement. As demand on data infrastructure increases, evenly distributed data flows will maximize network bandwidth and serve users faster.

The Social Impact

- **Fewer data errors**: Digitization improved operational efficiency compared to traditional pen and paper records, but it also created silos necessitating seemingly endless data duplication and the human error which accompanies that process. Blockchain technology lets us apply lessons learned by creating interoperable systems which can independently store and process data, leading to data with greater integrity.

- **Maximal data efficiency**: Currently, several disparate systems support government functions: healthcare, education, tax, social benefit, and property registries are all typically run on distinct platforms. Blockchain could transform this hydra into a single, agile digital ecosystem, securely breaking down silos and encouraging interaction and relevant data sharing between systems. Perhaps most compelling, it would reduce the need for manual data entry in each separate system, reducing human error and, doubtless, increasing human happiness (especially among government interns).

- **Faster, cheaper data sharing**: Middleman-free marketplaces also promise dramatic increases in efficiency. Financial service providers charge costly fees for workers seeking to send remittances to family and friends abroad. Moreover, many of these costs are not transparent and transactions can take weeks to complete. The reliability and efficiency of remittances sent on a blockchain will enable both workers and their families to more effectively apply resources, spur development, and raise living standards.

Challenges

- **Garbage in, garbage forever:** Blockchains are only as good as the data which builds them. There's a risk that poor quality data added to a blockchain will be difficult to correct, and future additions that are validated based on faulty blocks will only further embed those errors into that blockchain's architecture.

- **High energy consumption:** Blockchain's high efficiency cuts out when it comes to its own energy consumption. While solutions that process transactions without reconciling with other nodes as often, such as ***sharding***,[44] alleviate some strains on power sources, they will also be less secure than regular transaction processing on a blockchain.

- **Latency or speed:** Discussed in the section on security, but important to note when considering efficiency, blockchain users have to wait until their transaction has been added to a fully populated block and successfully verified by a majority of nodes before it's completed and securely recorded on a blockchain. This latency may pose scalability and usability challenges for larger blockchains.

Blockchain promises to upgrade the global data infrastructure by building error-resistant data chains and empowering peer-to-peer exchange. While the integrity of their data relies on human inputs and may be susceptible to mistakes, blockchain solutions will profoundly outperform legacy systems in efficiency, particularly with sensitive data. With blockchain, institutions can confront twenty-first century challenges and get the most out of diminishing resources.

Blockchain in Action

So how does strengthening security, accountability, and efficiency translate into improved social impact and governance? Take a look at how these ongoing pilots and programs are taking on real-life problems with carefully tailored blockchain solutions.

This is a representative, not comprehensive, list.

Global Challenge	Blockchain Solutions	Real World Examples
Identity Management	- Fraud reduction - Encrypted digital identity - Self-sovereign identity	- Civic streamlines secure authentication. - Sovrin is developing a government independent identity network.
Sustainability	- Energy efficiency - Supply chain integrity - Carbon credit trading - Clean energy marketplaces - Clean water accountability	- Brooklyn Microgrid is an all-local solar power marketplace, while the BitLumens powergrid promises electricity to 1.2 billion. - The World Food Programme is taking on illegal fishing and human rights abuses in the tuna trade.
Land management and property rights	- Efficient land titling - Reduced administrative burdens - Corruption-resistant records	- Land title projects are underway in Georgia, Sweden, Ukraine, and Vermont. - ChromaWay is building a secure system for land registration in Andhra Pradesh.
Legal system	- Effective documentation - Clarified chain of custody - Secure evidence processing	- Smart Dubai will use smart contracts to verify court judgements and share documents in real-time.

Global Challenge	Blockchain Solutions	Real World Examples
Emergency Response	- Accountable recordkeeping - Accurate aid distribution - Digital identities for refugees	- The World Food Programme avoids banking fees by conducting payment reconciliation to aid vendors over the blockchain.
Public Health	- Secure, shareable records - Resource management - Secure credentialing - Treatment accountability - Taming rogue drugs	- MedRec gives patients control over their medical record distribution. - Walmart tracks their supply chain to quickly locate sources of foodborne illness. - The FDA is piloting systems to securely share information among health care providers and hospitals.
E-Governance	- Secure voting and registration - Notarizing sensitive documents - Decentralized public investment	- HorizonState, MiVote, Followmyvote, VoteWatcher, Netvote, and Voatz will make voting more convenient and secure. - Neighborly rethinks municipal bonds.
Education and Training	- Secure student records - Legitimate credentials - Standardized credentialing	- At Blockcerts.org, tamper-proof digital documentation can be shared with ease. - The University of Nicosia built a blockchain library for student records.
Economic Opportunity	- Cross-border payments/ remittances - Accurate trade - Quick transactions and reduced fees - Digital identity for the unbanked	- BitPesa makes it quick and cost-effective to transact with frontier markets. - Moyee Coffee and FairChain Foundation remove the middlemen from supply chains.
Human Rights and Labor Abuses	- Supply chain accountability - Stable digital identities - Proof-of-living wage in supply chains	- Provenance builds transparent supply chains. - Everledger tracks and validates valuable assets like diamonds.

Developing Blockchain Solutions for Impact

Prerequisites for Development

Blockchain isn't one-size-fits-most technology. Each solution has to be specifically tailored to the complexities of the problem it's meant to solve. Don't decide what you want before you understand what you need; try to remain tech agnostic while researching potential solutions. This section explores questions and considerations for organizations researching and deploying blockchain-based solutions.

There are, bare minimum, two universal prerequisites to blockchain deployment:

- **Internet connectivity**: Internet infrastructure of some kind is necessary for a blockchain to function. The connection necessary depends on what it's being used for: full nodes in large public networks will require high speed connections that can handle large amounts of data, whereas "light nodes" or "internet of things" devices may not need as reliable of a connection.

- **Clean digital data**: Blockchain technology does not improve data quality, it only guarantees that the information entered onto a blockchain will stay there unaltered. So if a blockchain's source data is inaccurate, it will secure and propagate poor data. Early adopters need to ensure high quality data or they'll suffer from the "garbage in; garbage forever" problem, a perennial risk of distributed ledger technology. If you don't have comprehensive, valid data, you probably don't want a blockchain.

Once you've established that you can use a blockchain, ensure that it's the best solution for the problem you're looking to fix. Answer these questions before exploring further:

- **Is there an issue with the existing solution?** Blockchain isn't a hammer in search of a nail. The tech's potential can inspire some to look for opportunities to deploy it, however blockchain solutions aren't always feasible, nor the best answer to a given issue. Skip the hype; know why you need to use blockchain, specifically.

- **Are there no alternative technologies to effectively solve the problem?** Even if a challenge can utilize a blockchain solution, it doesn't mean it should, especially if there are established software solutions already available. Many existing tech solutions offer a well-tested product, thoroughly documented strategies, and support centers that can minimize risk, cost, and implementation time when compared to blockchain.

If you don't have comprehensive, valid data, you probably don't want a blockchain.

Solution Design

There are 10 must-answer questions to consider when designing a blockchain-powered solution.

Question 1: Who's accessing this data?

The most compelling use cases for blockchain adoption involve multiple uncoordinated parties seeking to interact with a specific set of data. If leaders trust those accessing a database, there's no need for blockchain's data verification and consensus mechanisms.

Some organizations purposefully keep data siloed to protect its integrity or differentiate access levels. In these cases, blockchain offers added value, facilitating more accessible data entry while ensuring records remain accurate; organizations can remain confident in their information regardless of who's accessing or amending it.

However, if mutually trusted parties are adding correct information to a database, then blockchain's main utility is rendered moot. Distributed ledger technology (DLT) allows multiple parties to read, write, and store identical ledgers, creating a single record automatically reconciled in real time—all without blockchain. Consider whether DLT may be a better solution to your challenge.

Question 2: Is this an uncoordinated system?

Does reconciling data remind you of herding cats? If so, you may benefit from blockchain. Complex marketplaces, where many actors transact simultaneously without full trust in each other, can increase costs and inhibit certain interactions. In these cases, blockchain creates previously unfeasible social and economic capital.

Blockchain is a clear solution when parties have misaligned incentives or are actively competing or attempting to sabotage one another. But even good-faith actors can incorrectly input data, thus undermining a system's integrity. If you need to preserve data accuracy in a chaotic environment, deploying blockchain will help. If you're operating in a trusted and well-coordinated organizational structure, consider deploying DLT instead.

Question 3: What's the existing intermediary?

Intermediaries like banks, brokers, or governments can help coordinate and facilitate trust between unacquainted actors. Before disrupting an established system, weigh the cost and efficacy of blockchain against that of your current intermediaries.

Some questions for evaluating intermediaries:

- Are they neutral?
- Do users trust them?
- Are they functioning in a system suffering from chronic corruption or ineffectiveness? In these cases, blockchain can cut out intermediaries to maintain or improve the integrity of your system.

Sometimes, appropriate intermediaries simply cannot be found. Perhaps they're impractical or economically prohibitive. Blockchain should be considered in these cases. For example, if an organization wants to promote financial inclusion, a blockchain allows individual borrowers to connect directly to lenders without the added burden of bank fees.

Question 4: Do the benefits justify the cost?

Even if a data challenge does have an existing solution, switching to blockchain may still meaningfully reduce costs and inefficiencies. Equally thorough cost appraisals should be done when comparing blockchain to legacy systems and confronting a problem for which there is no present solution. Some considerations:

- **What are the projected savings?** Savings can include not only direct costs like licensing, legal or consulting fees, and insurance premiums, but also the reduction of indirect costs such as those resulting from lower asset turnover.
- **How much would it cost to design and deploy blockchain versus upgrading existing systems? How do the projected savings compare to upfront costs?** Consider maintenance costs and investment repayment periods as you answer this question.
- **Would the maintenance costs of blockchain be lower than that of the traditional solution?** Some costs to consider: IT staffers, computing resources, server space, rent, blockchain transaction costs, etc.

Blockchain is new technology; costs of design, deployment, and maintenance today will be more expensive now than in the future. But that doesn't necessarily mean it isn't worth it. A thorough cost-benefit analysis will help you weigh all relevant considerations.

A blockchain allows individual borrowers to connect directly to lenders without the added burden of bank fees.

Question 5: Who needs a seat at the table?

Like most infrastructure projects, implementing blockchain is a complex process. Building a coalition of experts to assist with planning and deployment will lower costs, improve results, and distribute risk among stakeholders. By planning cooperatively, you'll preempt pain points and avoid impasses, leading to a smoother roll-out and a higher probability of success.

Consider the following roles when building your coalition:

- **Technical partner***:* A good technical partner will have a deep understanding of blockchain mechanisms and capabilities combined with clear communication skills so other coalition members can understand the technical boundaries of the project.

- **Regulatory or legal compliance expert***:* Blockchain is a new technology disrupting traditional industries. This leads to legal gray areas. By engaging legal counsel, you minimize your risk of noncompliance and gain insight into future regulation of the space.

- **Users and stakeholders***:* You can't code people. What will motivate participants to use the blockchain as intended? Make sure you're meeting the needs of network members by engaging potential users, whether Fortune 500 supply chain partners or smallholder farmers.

- **Third-party auditors or validators***:* The more transparent your development process, the more likely you are to find and fix glitches before they become ingrained to the platform. Consider adopting open-source standards and including code or security auditors in your pilot. Doing so will protect your organization from liability and your users from unforeseen bugs.

- **Independent guide***:* Members of any large coalition will invariably inject individual objectives into the planning process. But the priorities of one coalition partner may not fully align with the project objectives. It's important to identify coalition members who can balance those priorities and course correct towards deployment goals.

By planning cooperatively, you'll preempt pain points and avoid impasses, leading to a smoother roll-out and a higher probability of success.

Question 6: How can existing impact metrics inform project goals?

Almost as important as establishing overall objectives for a project is demarcating the metrics by which you'll measure those objectives. By identifying short-term progress identifiers, you can begin to understand how meaningful long-term outcomes will be achieved. For example, targeting foodborne illnesses by tracing and quickly removing contaminated food sources will diminish overall deaths over time. An organization should consult impact frameworks to determine useful metrics. These include:

- The Impact Reporting and Investment Standards (IRIS) for impact investing goals

- The United Nations Sustainable Development Goals (SDGs) for international goals

- The United Nations Environment Programme (UNEP) for sustainability goals

The metrics you use depend on the impact you want to make. By picking the right ones, you can achieve not just your narrowest objectives, but the well-being of the broader community.

Make sure you're meeting the needs of network members by engaging potential users, whether Fortune 500 supply chain partners or smallholder farmers.

Question 7: How sensitive is this data?

Ensuring the security of all data stored on a blockchain is paramount. But blockchain's transparency can raise privacy questions for certain types of information, including sensitive personal data, trackable metadata, and data impacted by legal privacy requirements

For some organizations, data privacy can be maintained by limiting access through a private blockchain. However, if your data is most valuable when shared on a public blockchain, ensure that no combination of data searching can reconnect a piece of anonymized data back to an individual through a ***differential privacy***[45] test.

Question 8: Does this project involve off-chain data?

Blockchain is a digital infrastructure, so goods which can be digitally expressed (e.g. ownership records, energy stores, credentials), as well as actions taken with them, integrate naturally. However real-world goods and commerce can be harder to accurately log on a blockchain.

The easiest hard assets to manage on blockchain are either completely interchangeable (like mass-produced consumer goods) or very difficult to alter or imitate (like diamonds). The easier it is to forge an item, the more difficult it will be to secure it using blockchain tech. In these cases, effective validation relies on off-chain infrastructures like trusted attestations, unique serial numbers, QR codes, and RFID tags.

A blockchain solution can de-paper supply chains and make source-to-consumer records accessible within minutes as opposed to days. However, its implementation across a supply chain would require the buy-in of every participant along the way and additional enforcement structures to ensure off-chain asset integrity. Consider running pilots of this kind in parallel with legacy systems to test objectives without jeopardizing critical functionalities.

Question 9: Who will engage with this solution?

Sympathy is a critical feature of well-made blockchain solution. If designers fail to understand the human problems they're trying to address, their end-product will be just that: a product, not a real solution. A human-centered, multidisciplinary approach to protocol design reduces the risk of creator biases which could limit project performance and scalability.

For example, a critical technical consideration is whether or not network members care about who is validating transactions or participating in a network. If so, a public blockchain may not be the right choice. If an organization operates in a heavily regulated industry, requires accountability for actions in off-chain settings (such as courts), or needs to verify validator identity in certain cases, it should choose between a private blockchain and a DLT.

To keep objectives aligned, it's important to consistently engage with those affected by your blockchain solution. If that solution is successfully scaled, revisit its initial goals and expectations to ensure they're still being met.

Question 10: How can likely challenges be mitigated?

As with any innovation, there are risks with blockchain which should be thoughtfully considered by project managers and solution designers. Take aspects such as vendor and platform lock-in, data interoperability, data quality, open-source solutions, scaling, regulatory landscapes, and backup systems into careful account as you build.

Without a strategy to identify and mitigate risk, many promising proofs of concept will fail to realize their full potential. Conversely, asking questions and anticipating pressures will help to unearth and resolve previously unidentified challenges.

Design Considerations

After a you've figured out the type of blockchain solution you need, *or whether a blockchain is even right for you*, it's time to move onto design considerations. To ensure that your goals are met, don't be afraid to work alongside your technical team and take an active role in the design process. Even if you aren't a tech expert, you'll contribute valuable big-picture insights. Keep the following recommendations in mind as you build.

Treat software like hardware: Though blockchains are technically a type of software, blockchain governance is decentralized, making any changes subject to the agreement amongst a majority of blockchain stakeholders. This means the tech is poorly suited to the traditional, more unilateral software design process.

Blockchain design and implementation should more closely resemble the development of hardware components, which undergo extensive testing before being produced at scale. Because blockchain technology is still evolving, widely accepted design standards are not yet in place and the sustainability of today's major protocols and platforms is uncertain. Utilize pilots to experiment and spot problems before scaling operations, and maintain flexibility by ensuring interoperability and avoiding vendor or platform lock-in.

Plan to scale: Given the complexity and cost of designing, implementing, and scaling a blockchain, all organizations should seriously consider conducting a pilot before any more extensive rollout. A controlled environment allows for effective measurement and evaluation of social impacts, facilitates experimentation, and simplifies protocol modification in the event of issues.

Avoid premature expansion—even if early results are promising—and acquire third party support to consistently audit your system. Growing pains are common with blockchain, and they won't necessarily stem from the protocol itself. Everything from relationships with constituent parties to ecosystem growth can have an impact. These can take time to resolve.

Further, success in a small-scale pilot is insufficient evidence of the sustainability of a particular protocol. If you're operating a legacy solution, keep it running. You can gradually transition to the blockchain as you work out bugs and gain confidence in it.

Consider user experience: It doesn't matter how cutting-edge your backend tech is if users can't figure out how to operate it. A quality user experience (UX) is key to the overall project viability; work with programmers and designers that are committed to providing one. A few tips to start off:

- Humanize the process by seeking the support of your coalition.
- Use existing UX patterns and keep visual distractions to a minimum.
- Be consistent, steer clear of jargon, provide guidance, and welcome user feedback.

Innovate ethically: The Beeck Center at Georgetown University has devised a framework to facilitate intentional blockchain design and deployment strategies.[46] Ask these questions:

- What will the governance structure be? How is it created and maintained?
- How is identity established?

- How is access to this blockchain network defined, granted, and executed?

- How are data inputs verified and transactions authenticated?

- How is ownership of data defined, granted, and executed?

- How is security set up and ensured?

It’s important to have a thorough qualitative understanding of answers to these questions, regardless of the degree to which an organization is outsourcing the design and development of its blockchain solution.

It doesn’t matter how cutting-edge your backend tech is if users can’t figure out how to operate it.

Case Studies

How to Harness Blockchain: Exploring Case Studies

The following eight case studies represent not only what blockchain can do today, but what it promises to accomplish in the future. Each example demonstrates how blockchain has helped to overcome challenges of accountability, security, or efficiency within a specific social sector.

Aid Provision: Building Blocks (UN World Food Programme)

PROBLEM: How do individuals without bank accounts or government identity documents participate in financial systems? Currently, organizations like the UN World Food Programme (WFP) coordinate with more than 30 other relief organizations and international financial institutions to deliver aid. Traditional systems not only incur significant banking fees, but also delay transaction resolution between cooperating partners, banks, and the WFP. As numbers of displaced persons increase and cash transfers become a predominant form of aid disbursement, intermediary banking services create inefficiencies and absorb resources.

SOLUTION: The Building Blocks program is built on the Ethereum blockchain, due to its need for high scalability. Money transfers are represented with digital tokens, which are exchanged for food and supplies. WFP reconciles payments with vendors monthly, bypassing escrow and bank charges while preserving payment security. The initial pilot in Jordanian refugee camps serves over 100,000 people, while significantly reducing bank transfer fees and increasing responsiveness and time-efficiency when acting on beneficiary needs.[47]

HOW IT WORKS: Refugee families receive tokens in their digital wallet every month, which can be credited to participating markets in exchange for goods and services. Each family's identity is verified by the existing UNHCR case number via iris scanners (biometric identity) at each vendor. WFP transfers payment directly to the vendor. In this system, cash never enters the blockchain, but represents wealth transfers that are reconciled each week.

WHY BLOCKCHAIN: By creating a transparent, tamper-proof record of provisions purchased by refugees, blockchain allows relief agencies to directly reconcile payments to each other and to suppliers, reducing redundant activity in auditing payments. Furthermore, the security of blockchain technology removes the need for banks to facilitate transactions and for refugees to carry cash or bank cards, lowering associated costs and potential theft.

CHALLENGES: The initial pilot underutilized the blockchain's capacity to integrate data from multiple sources, since WFP was the sole party processing information. Once additional parties—such as markets, banks, and other UN agencies—are added, Building Blocks will encounter new governance challenges as more entities access and write to the blockchain.

BROADER IMPACT: The potential to secure human rights and improve access to resources extends beyond refugee populations. UNICEF is exploring blockchain applications to crowdsource aid funding, reduce operational expenses, and make field staff more effective. Other examples of organizations working to leverage blockchain to safeguard human rights include a partnership between BTA, Coca-Cola, and the U.S. State Department to combat forced labor in global supply chains which utilize migrant workers. The De Beers Group has announced a project to weed out blood diamonds from supply chains. Everledger is a start-up company building blockchain-based solutions in markets where provenance matters, such as diamonds, art, and wine—proving a consumer appetite for transparency and ethical trade.

Land Records: Republic of Georgia

PROBLEM: Land is a principle source of wealth and economic mobility, and land registries grant owners legal authority to leverage property. Ambiguous ownership, corruption, and cumbersome transaction processes increase instances of fraud, erode trust in institutions, and stifle economic mobility. In Georgia, years of corruption enabled by a fragmented registry system crippled trust in a new digital public registry system implemented as a result of government reforms following the 2003 Rose Revolution.

SOLUTION: The Republic of Georgia's National Agency of Public Registry (NAPR) partnered with Bitfury in April of 2016 to create a blockchain solution that allows NAPR to verify proof of ownership, while enabling citizens to verify the legitimacy of their documents without exposing confidential information. Citizens now have a transparent and auditable method of ensuring that land registry records remain legitimate.

HOW IT WORKS: Citizens register their property through a digital interface, which creates a timestamped hash of the property certificate and uploads the hash to the public Bitcoin blockchain. Timestamping the hash on the Bitcoin blockchain tamper-proofs the documentation and enables its owner to prove that the certificate was authorized by NAPR and any subsequent records disputing their ownership are invalid. A fraudulent record results in a different hash than that registered on the public blockchain, proving the edited record invalid.

WHY BLOCKCHAIN: By creating transparent and verifiable registry systems, governments can restore confidence in property titling and foster investment and economic growth. The decentralized blockchain network reduces the risk of fraud by constantly verifying and reconciling transactions against unique land ownership records. The transparency and resiliency of a publicly accessible blockchain reduces the risk of corruption and restores public confidence in the system.

CHALLENGES: The Republic of Georgia land management bureaus underwent significant institutional reform beginning in 2004, and already held land registries in a digital format. Nascent bureaucracies like in Honduras, on the other hand, may have incomplete or analog records that are not ready for blockchain implementation. Additionally, encoding records onto a blockchain assumes confidence in the existing registry. Countries must ensure that land registries have not been manipulated before adding them to the blockchain, or else risk codifying injustice into a new registry.

BROADER IMPACT: Other countries are pursuing land registries to reduce transaction costs and secure land capital for economic growth. The Swedish Lantmariet is piloting a solution to accelerate real estate transaction speeds from 3-6 months to 10 days. The Dubai Land Department has begun recording property transactions via blockchain, enabling global investors to verify property data and ensure the accuracy, credibility, and transparency of investment transactions. The University of British Columbia partnered with blockchain land registry company Ubitquity to pilot a solution for the Real Estate Registry Office of Brazil to reduce fraud and human error in the recording of land ownership. Land registry solutions are projected to benefit developing countries with lower levels of institutional trust, where a projected interest rate reduction of 0.1 percent "would create USD $14B per year in added value worldwide," opening up new sources of capital for millions of landowners.[48]

Supply Chains: Walmart

PROBLEM: While retail food stores safely provide fresh produce to their consumers the vast majority of the time, food contamination poses severe dangers to consumers, retailers, and farmers. Tracking the sources of food products through the supply chain is notoriously difficult and time consuming. Paper-based systems are susceptible to human error, and digital data systems are often siloed and unable to trace the full journey of a product from farm to store. When food contamination is discovered, stores must implement sweeping recalls despite only a small fraction of products being affected, costing millions of dollars in wasted food and labor, and posing significant danger to the public.

SOLUTION: Walmart leveraged IBM's Food Trust technology, a private blockchain built on Hyperledger that can traces food production in retailer supply chains. Food Trust stores data on a traditional database and exports a record of changes to the blockchain, which ensures data privacy of supply chain partners, maintains high scalability, and aligns with existing industry standards. Initial pilots in Spring 2017 reduced trace time from days or weeks to seconds, encouraging Walmart to implement Food Trust as a requirement for all suppliers of fresh produce by September 2019.

HOW IT WORKS: Workers within the supply chain upload food processing data to the blockchain via a standard naming convention so goods can be consistently tracked across suppliers. Between each exchange of ownership, the blockchain confirms the origin, path, destination, and entry date of the product. Authorized users can then verify food provenance to determine the scope of the problem, determine contamination origins, and conduct more precise recall measures from affected retailers, creating transparency and accountability that doesn't exist in the original system.

WHY BLOCKCHAIN: Blockchain provides a tamper-resistant and decentralized way to trace a food item from its origin to its point of sale at a store. By requiring food producers and logistics workers to input transportation data onto the blockchain as a product travels through the system, retailers can transparently and accurately trace dangerous food items directly to their source, reducing the risk of foodborne illness and passing on savings to consumers.

CHALLENGES: IBM Food Trust is a private and permissioned blockchain that restricts visibility of data to authorized users. While this enables transparency within the distributor's network, it excludes other important entities such as regulatory agencies and research institutions from accessing data, limiting accountability to the public and depriving public-interest organizations from capitalizing on data. Inclusive permissions can enable third party read-access to the food supply chain while restricting write-access to authorized distributors, which would more fully employed the benefits of blockchain openness and provide impactful data to organizations operating in the public interest. Additionally, tracking non-digital assets increases the probability of errors and requires external structures to encourage correct data entry into a blockchain.

BROADER IMPACT: Despite its reliance on human input, Walmart leveraged a blockchain system that considered the needs of users, scaled carefully after early pilot success, and worked alongside redundant system for added security. Blockchain has diverse applications beyond food supply chains. The World Wildlife Fund launched a pilot to improve traceability of fishing practices in the Pacific Islands and help mitigate illegal and unregulated fishing. Maersk built a blockchain to more efficiently fulfill shipping orders, reducing wasted cargo space and diminishing marine shipping traffic in the long-run. These are a few examples of how blockchain can securely track assets and increase efficiencies within supply chains.

Energy Management: LO3 Energy and Brooklyn Microgrid

PROBLEM: Newly affordable sources of renewable energy enable households to produce and consume power locally, creating a more efficient energy grid. However, the current centralized model of energy distribution is inefficient and restrictive. Establishing a decentralized model of energy infrastructure is crucial as energy demand evolves and fossil fuels exacerbate climate concerns.

SOLUTION: LO3 Energy created a local energy marketplace which enables solar panel owners ("prosumers") to buy and sell energy locally over existing electrical infrastructure. The Brooklyn Microgrid uses its blockchain based marketplace to connect various solar sites to customers, who can buy and sell local power while preserving the utility provider maintenance of the electrical grid. This solution promotes a sustainable clean energy model, increases electrical grid efficiency and resiliency, and drives down costs for consumers.

HOW IT WORKS: Participants access the local energy marketplace through the Brooklyn Microgrid mobile app. In the app, people can choose to buy local solar energy, renewable energy produced outside of the Brooklyn, New York area, and/or grid energy. Prosumers sell their excess solar energy onto the marketplace for consumers to bid on. Local solar energy is "won" by consumers via an auction. Prosumers can sell their excess energy on the marketplace once they have installed a Brooklyn Microgrid smart meter system, which gathers and records energy data for use within the energy markets.

The marketplace is scalable to communities all over the world via Exergy, an open-source platform and token system for managing and permissioning access to energy data. As a foundational protocol, Exergy enables digital applications, such as the Brooklyn Microgrid marketplace, to be deployed almost anywhere.

WHY BLOCKCHAIN: Blockchain provides a decentralized infrastructure, a secure method of recording transactions, and a transparent interface. Smart contracts built into the blockchain enable the marketplace auction mechanism. The distributed functionality will allow for millions of users and devices—with different incentives—to participate in the market over time.

CHALLENGES: Brooklyn Microgrid is aiming to change the way electricity is bought and sold. Although this innovative approach is in alignment with New York's energy policy "Reforming the Energy Vision," it requires a revision of the existing regulatory framework.

Currently, this model functions on a small scale, but may receive industry pushback as it scales. Additionally, the pace of expansion will be limited by the installation speed of and excess supply from local solar panels. Therefore, owners may not feel the network effect benefits until a critical mass of additional participants are established.

BROADER IMPACT: LO3 Energy and other organizations continue to test how blockchain technology can democratize access to sustainable energy. LO3 Energy also partners with Centrica to test a similar peer-to-peer energy exchange market in Cornwall, England. The energy needs of the twenty-first century require innovative ways of producing and effectively allocating power to the world's population. Blockchain technology offers a secure and decentralized structure to ensure that new infrastructure is equipped to handle this need.

Financial Inclusion: AgUnity

PROBLEM: Smallholder farmers in developing countries greatly benefit from cooperatives in which they can collectively bargain for better prices for their goods, share equipment, and circulate best practices. However, restricted access to information and corruption within cooperatives erode trust in the system, disrupt transactions, and create financial losses.

SOLUTION: AgUnity provides smartphones to farmers that are pre-loaded with the app, ensuring that farmers use compatible hardware for the program and utilize secure devices when accessing the AgUnity blockchain. Built on the Multichain blockchain platform, the app can operate offline in rural areas until an internet connection is reestablished. The pictographic interface is customizable, enabling different crop types and cultural nuances to integrate into the platform. Initial pilots in Kenya and Papua New Guinea demonstrated a 300 percent increase in income for farmers equipped with AgUnity devices.

HOW IT WORKS: Farmers log on to record crop-processing transactions and sales. The transactions are visible to all other members, ensuring transacting parties follow through on agreements. Each farmer is assigned a digital wallet which stores receipts, which are then converted to cash upon arrival at the cooperative. AgUnity also provides encrypted messaging services for farmers to collaborate on harvest planning and equipment sharing.[49]

WHY BLOCKCHAIN: Blockchain creates a permanent record of transactions, enabling farmers to be confident that agreements with cooperative representatives will not be changed without their consent. Furthermore, the record is auditable by other members of the cooperative, providing transparency and accountability to farmers who are concerned that crop brokers might renege on their commitments.

CHALLENGES: Despite the efforts to instill trust in the cooperative system, AgUnity centrally controls transaction records, identity data, and programming on participating devices. This requires farmers to trust AgUnity as a mediator and limits expansion. Additionally, farmers are not paid independently of financial institutions and must exchange digital credits for cash (although integration with digital cash platforms like M-Pesa are forthcoming). Lastly, there is no independent validator of transactions and farmers still rely on off-chain enforcement if a cooperative defaults on an agreement.

BROADER IMPACT: AgUnity continues to expand its financial inclusion offerings, including digital wallet capabilities and securitized loans. Other blockchain companies are addressing gaps in financial services in developing countries. BitPesa is a mobile payment system that lowers transaction costs and manages risk, bringing stability to communities and fostering economic mobility. WorldRemit provides blockchain-driven remittance services that are near-instant, secure, and direct, encouraging financial exchange and providing stability to beneficiaries. Building financial tools for marginalized populations is a critical component of achieving global development goals, and blockchain will be central to successful financial inclusion.

Voting: West Virginia

PROBLEM: Overseas military members and their families have few choices when it comes to voting in U.S. elections. Currently they must either mail in their ballot, fax or email it to a county clerk's office, all of which have proven to be cumbersome (and often impossible) for uniformed service members in remote areas of the world. But military members have no guarantee that their vote will reach their clerks in time, be counted, or remain private and secure throughout the process. These factors reduce the ability, willingness, and motivation of service members and overseas voters to participate in the democratic process.

SOLUTION: The Office of the Secretary of State of West Virginia, in partnership with Voatz, Tusk Montgomery Philanthropies, and the Blockchain Trust Accelerator piloted a mobile voting application powered by blockchain in the 2018 Primary and General elections in accordance with state and federal regulations for absentee ballots. The initial pilot was limited to West Virginia UOCAVA (the Uniformed and Overseas Citizens Absentee Voting Act) eligible voters registered in Harrison and Monongalia Counties for the Primary election, then scaled up to 24 counties in the General election. The first vote in a U.S. federal election cast through a blockchain-based solution was cast on March 24, 2018—the day absentee voting opened in the 2018 West Virginia primaries. The first vote cast in a general election was hashed to blockchain on September 21, 2018. In the Primary election, 13 votes were cast through the solution. In the General election, 144 votes from voters in 31 different countries were cast out of 160 voters who applied to use the technology.

HOW IT WORKS: Eligible voters complete and submit the Federal Post Card Application (FPCA) to their county clerk. Once the FPCA is received and the voter's information is confirmed, voters are prompted to download the Voatz app, verify their identity and eligibility using biometric security measures, and then complete the voting process securely and privately through their smartphones or tablets.

WHY BLOCKCHAIN: Blockchain enables voters to submit their election ballots through a distributed, cryptographic ledger that has no single point of failure and cannot be edited. Furthermore, votes remain auditable by election committee officials without providing personally identifiable information about a voter, providing the same anonymity that poll voters are guaranteed.

CHALLENGES: While the blockchain mobile voting process is a significant improvement to existing systems for overseas voters, a number of concerns remain. Mobile voting requires voters to have smartphones or tablets, and despite the security measures that blockchain offers once data is recorded, unsafe internet connections and/or unsupported devices may impact the ability of a voter to submit a ballot successfully. The application utilizes sophisticated malware detection software, which will disable the application and prevent a ballot from being accessed if the device is deemed insecure. In that case, alternative methods of absentee voting remain available to those whose devices are insecure, and to those who do not own or cannot operate a smartphone. However, like all technology, security must be constantly monitored and updated as nefarious actors adapt and look for ways around the current protections.

BROADER IMPACT: Blockchain has the potential to transform the way citizens interact with their government and restore trust in the institution of voting. The city of Zug, Switzerland recently leveraged a blockchain-powered mobile voting platform by Luxoft for its municipal elections. The Republican Party of Utah partnered with Smartmatic to offer its party members the ability to vote from anywhere in the world for the 2016 Republican Presidential Caucus. As the technology matures and more election officials and the general public increase their understanding of the system, blockchain-powered voting will provide citizens with a responsive, effective, and trusted method by which to engage with their government.

Social Investment: Neighborly and City of Berkeley Blockchain Initiative

PROBLEM: Municipal bonds have long been a key source of funding for public projects. By connecting investors with local governments issuing bonds, they fund civic investments like schools, libraries, and parks. However, complex regulations and a scattered bond landscape create barriers for willing investors, preventing communities from accessing capital when needed. Furthermore, investors encounter challenges when tracking the impact of their investment, leading to accountability issues that dissuade investment within communities.

SOLUTION: Elected officials with the City of Berkeley partnered with Neighborly and the UC Berkeley Blockchain Lab to explore building a platform that would facilitate investment opportunities between residents and the city for as low as $10. By broadening the range of investors and investment opportunities, City of Berkeley officials seek to empower residents to invest in projects that are significant to them, expanding the types of projects that could be funded with municipal bond financing given current federal, state and local regulations.

HOW IT WORKS: Investors will buy tokenized municipal bonds, denominated in U.S. dollars, that will enable the city to allocate resources more broadly and quickly, but also to create new initiatives such as food vouchers for the homeless. Since local investors will have better access via the blockchain enabled financial tools, it could be increasingly easy for investors to indicate a project they would like to fund, discover how their funds will contribute to the project, and review investment characteristics.

WHY BLOCKCHAIN: Blockchain technology can bypass middlemen and decrease transaction costs, enabling small investors and municipalities to easily form mutually beneficial partnerships. Decentralization enables companies like Neighborly to store financial information accurately and cheaply, while an auditable trail provides "Know Your Customer" audit compliance. Finally, blockchain tracks all financial movements to prove that investments have been spent as intended.

CHALLENGES: This pilot is in its infancy and few details have been published about the mechanics of the blockchain solution. However, blockchain would enable varying degrees of data viewability, instilling transparency and accountability for regulators and investors. While blockchain makes the transaction process between issuers and investors easier, more accessible, more efficient, and more transparent, project selection will be contingent on the local governments issuing the bonds.

BROADER IMPACT: The efficiency and transparency challenges in procurement, fundraising, and social investment are well-suited for blockchain intervention. AidCoin built a fundraising platform that tracks contributions through blockchain to lower fees and offer clarity into how funds are being allocated. St. Mungo's, a charity based in London that provides services to the homeless population, uses a blockchain transparency tool called Alice to track contributions in real-time and reallocate funds as new priorities arise, giving more power to donors to choose how their contributions are utilized. Blockchain offers the security and accountability that communities and charities seek to revitalize trust and galvanize social good investments.

Environmental Sustainability: Plastic Bank

PROBLEM: Every year, approximately 8 million tons of plastic enter the oceans, adding to the over 4 trillion pounds of plastic currently destroying marine ecosystems, endangering food supplies, and degrading living conditions for millions of coastal communities. Over 80 percent of waste is generated by populations with insufficient waste management systems. Garbage can provide income for millions of marginalized people living in polluted areas through recycling redemption programs. However, cash transfers invite crime in underdeveloped societies and currency localization inhibits organizations from growing to meaningfully impact the enormous accumulation of plastic on the planet.

SOLUTION: Plastic Bank partnered with Cognition Foundry and IBM to create a mobile app to track the amount of recyclables submitted to local drop off depots in participating areas.

HOW IT WORKS: Local populations download the app onto their smartphone and collect plastic in their neighborhoods. Collectors earn digital tokens by weight that they can either redeem for currency or spend at participating stores, Wi-Fi hotspots, and phone charging stations. The plastic is then exported to factories processing sustainably-sourced plastics.

WHY BLOCKCHAIN: The growing ubiquity of internet-enabled smartphones allows blockchain to provide financial services to previously inaccessible populations. Failure-resilient, secure transactions offer a reliable and safe method of earning and spending income. Rather than constructing a centralized network, blockchain enables decentralized ecosystems in which local plastic collectors can directly connect with manufacturers without any intermediaries managing the relationship.

CHALLENGES: Despite the wide adoption of smartphones and significant gains in internet connectivity, Social Plastic still relies on internet connectivity to provide financial services to its clients. While they do not need connectivity while collecting plastic, transactions that occur outside of covered areas will not benefit from immediate transaction resolution. Also, income for collectors is contingent upon companies paying above-market prices for recycled plastic. The success of this model relies on sustained demand for ecologically responsible products.

BROADER IMPACT: Other organizations are leveraging the power of blockchain technology to repair and protect the environment. Sustainability International's Clean Up Niger Delta project pays community members via digital currency for completing clean up assignments, then documents it on the blockchain. In another project, IBM partnered with Chinese Energy-Blockchain Labs to build a carbon asset management system on Hyperledger, reducing the cost of participating in carbon credit exchanges and helping businesses emit less carbon into the environment. Blockchain technology enables small groups to create economically viable environmental cleanups around the globe by storing verifiable information about pollution trends and repairing the environment through decentralized collaboration.

Combating Fake News: Democracy Notary

PROBLEM: Factual proof forms the foundation of all evaluation and decision-making, from journalism to policymaking and voter choice. Forgeries undermine the public's ability to make sound judgements or to trust facts when they are presented. Increasing sophistication of photo-editing software, lower barriers to access, and larger networks to proliferate forgeries have eased the circulation of misinformation. Convincing forgeries of photos, videos, documents and voice recordings post severe threats to privacy, national security, and democracy.

SOLUTION: Identifying disinformation is only one piece of the puzzle. In partnership with the Design 4 Democracy Coalition, Emercoin, and the Blockchain Trust Accelerator piloted the **Democracy Notary** platform, which secures official copies of public statements to prove that content is original and legitimate. Its first use case was in relation to the 2018 Macedonian referendum. Built on Emercoin's permissioned blockchain, it permits trusted civil society organizations to upload content and provides the public with read access to compare disseminated reports with verified blockchain entries.

HOW IT WORKS: Democracy Notary immutably encodes key documents into a blockchain that can serve as a "truth-check" when manipulated or falsified documents are used as a weapon of disinformation during high-stakes events such as elections. The Design 4 Democracy Coalition aims to eventually give permissions to trusted civil society organizations to post to the Democracy Notary, which converts documents, reports, and other original media of public interest into unique hashes and posts them on the blockchain where it becomes mathematically impossible for data placed in the system to be altered or destroyed. Blockchain, therefore, can demonstrate the integrity of information and make it possible to debunk forgeries and manipulation.

WHY BLOCKCHAIN: Blockchain technology uses algorithms to assign hashes to uniquely identify data files. Any changes to an original file will result in an obviously different hash, and therefore be easily recognizable as a different file than the original. Blockchains are accessible globally, enabling individuals around the world to easily record hashes of original content and enable others to verify copies of information by comparing their hashes to the catalogued hash of the original.

CHALLENGES: While the Democracy Notary platform was designed to help citizens find accurate sources of information for elections, challenges remained in driving user adoption. The team sought to embed the technical complexities of the platform behind the user interface to simplify the user experience. Despite its difficulty, creating user-centric interfaces is critical to creating value for end users and for broader adoption of a new technology. Moreover, Democracy Notary experienced challenges in educating the public about its service in the weeks leading up to the election. Platforms that combat fake news should be coupled with sustained public education campaigns to inform concerned citizens of secure, reliable news alternatives.

BROADER IMPACT: Blockchain enables immutable timestamping of content, creating a niche for content verification and notary services to make forging information more difficult. Blocksign enables users to sign legal documents and timestamp digital signatures on the blockchain to prove that a document was validated at a certain time without trusted intermediaries. Blocknotary extends these services to any type of media, and offers a video interview process for remote verification of identity. While questions of originating ownership and court eligibility demonstrate off-chain challenges to digital notary services, they offer a significant tool to combat fraud and forgery in public documentation.

The Future of Blockchain for Social Impact

Where Do We Go From Here?

In today's world, widespread uncertainty cultivates fear and suspicion; disillusionment prevails between communities, their governments, and the institutions that uphold societal values. The cooperation which builds successful human enterprise is founded upon trust, but that trust is eroding at an alarming rate.

Leaders must analyze the problems they face and their potential solutions. Blockchain technology will not always prove an optimal approach. However, the degree of accountability, security, and efficiency that blockchain lends to recordkeeping systems merits serious consideration by government agencies, nonprofits and businesses attempting to rebuild trust between themselves and the communities they serve.

Blockchain is still in its infancy, and technologists, policymakers, and academics will continue to discover new dynamics of the technology. These will affect both potential and established blockchain deployments. Those considering blockchain systems as well as those who have already adopted them should remain abreast of ongoing developments in the space.

Additional Areas of Research

The Blockchain Trust Accelerator has identified the following areas of research to be pursued as this technology matures:

Digitizing off-chain assets and analog data: Blockchain requires integration with digital data sources, posing challenges to groups limited to analog data. If high-bandwidth connectivity and accurate digitized records remain largely restricted to developed countries, the potential impact of blockchain tech will be significantly limited. As blockchain technology gains traction, limited internet connectivity in certain regions of the world will exacerbate the existing digital divide and may lead to greater global inequality. Accurately converting physical data to digital form will be expensive and time consuming, both in terms of input processes and data accuracy. The latter is especially important considering the difficulty of altering data on the chain. Regardless of potential difficulty, these hurdles must be addressed for blockchain to achieve its full potential as an open, democratic technology.

Refining effective identity solutions: Blockchain solutions require an integrated identity management platform to authenticate users and maintain accountability. The lack of an effective blockchain identity solution creates gaps of anonymity which can be exploited to threaten the integrity of blockchain tech. The development of a secure proof-of-identity on blockchain will facilitate the effective linkage of on- and off-chain activity, potentially transforming the lives of 1.1 billion people worldwide without recorded identity. By providing a verifiable identity, many of the services governments and nonprofits are currently unable to provide, such as aid distribution, land titling, and financial services, will become manageable.

Simplifying blockchain governance: Blockchains are rigid by design. The creation of an effective and secure identity solution may also help to simplify protocol changes while minimally impacting the technology's tamper-resistance and security. Despite the technology's inherent inflexibility, the blockchain ecosystem is evolving rapidly. Anticipating bugs and errors within governance models and developing methodologies to improve existing protocols and course-correct as mistakes arise is vital to system sustainability.

Instituting blockchain-specific laws and regulations: Regulators must balance the entrepreneurial opportunities of blockchain tech with the imperative to protect human participants. To date, most regulation has centered on cryptocurrencies themselves—not their underpinning infrastructure. While tokens and the blockchains on which they're traded merit consideration, regulation of the base technology can be applied to far more use cases. Particularly important will be to manage how on-chain data impacts the off-chain world; information sharing information, digital signatures, and smart contracts all require a framework upon which to interact with existing legal systems. Doing so will provide much-needed clarity for developers and improve interactions between blockchains and legacy processes.

Developing blockchain ethics: Blockchain technology may involve certain trade-offs, such as efficiency versus security, accountability versus privacy, or permanence versus flexibility. Though many may be tempted to address these questions exclusively through the lens of code and mathematics, these problems —and their potential solutions—stem from cultural norms in future contexts we cannot anticipate. As traditional ethicists construct a code of moral standards and considerations for technologists and policymakers, social values can be better upheld within interactive blockchain ecosystems.

Combatting disinformation through blockchain: Today it seems more vital than ever to re-instill trust in the digital information which comprises and informs current events. Blockchain-verified timestamps and geolocation can combat disinformation in the news and on the web. Blockchain can serve as a supply-chain record for facts, helping citizens to distinguish genuine content from fake news. As these capabilities are further developed and disseminated, they will help to return integrity, clarity, and trust to public information landscapes.

Exploring the intersection of frontier technologies: To address social impact and governance challenges, innovators must consider potential synergies between blockchain and other emerging technologies (such as **Artificial Intelligence**,[50] **Internet of Things**,[51] and quantum computing). Tech companies are already considering how these technologies will interact. Social sector innovators should do the same.

Incorporating differential privacy into blockchain solutions: Despite the significant value that collecting and synthesizing large amounts of public data can contribute to effective policy making and service provisions, privacy concerns have become a primary consideration as more personal data is captured by companies and governments.[52] Even though many groups anonymize datasets in an attempt to protect individuals, identities remain vulnerable to discovery through certain coding tricks. Blockchain could exacerbate this problem by offering increased opportunities for data synthesis and access to accurate public data. Coalitions of data scientists, game theorists, privacy experts, and policymakers should consider using methods which prevent the isolation of specific individuals from datasets while maintaining those datasets' openness and completeness.

Cultivating future talent for blockchain solutions: Like computer science a generation ago, blockchain technology is only thoroughly understood by a few programmers and tech firms. There is consensus in the blockchain community that there's a need for more programmers proficient in building blockchain solutions. As the field grows, emerging programming talent should ideally reflect the diversity of a global user base. Blockchain resides at the nexus of several disciplines: cryptography, game theory, tokenomics, network theory. Cross-sector blockchain projects, startup-in-residence programs, academia, hackathons, and traditional accelerators will continue to attract new leaders to the discipline as the tech matures.

Conclusion

Humanity's greatest accomplishments are also humanity's greatest collaborations. Humans are not the only species capable of teamwork, but we are particularly good at it. Unfortunately, some of the same traits that help us help each other also make us particularly adept at duplicity. The achievement of universally beneficial ends can be obscured or inhibited by self-interest and deception. By facilitating transparency and verity, blockchain technology can create opportunities for collaboration that were previously rendered impossible by boundaries, both digital and physical, and mistrust.

The technology's benefits promise to be vast. It will provide the opportunity to facilitate the inclusion of billions left behind by economic progress. Blockchains may also allow for greater coordination among impact organizations, reducing redundant and ineffective spending and increasing the visibility of those having the biggest impact. Greater efficiency and transparency in governance will increase institutional trust and accountability while empowering individuals to make informed, independent decisions about their own data. Digitized records and interoperable government services will equip governments for the twenty-first century.

Blockchains are not a panacea. As such, the decision to implement them should not be a foregone conclusion. But, in one capacity or another, blockchain will likely play a meaningful role in restoring trust in global civil, governmental, and charitable institutions. More importantly, it will facilitate innovations which improve people's lives. Someday, this technology's benefits will be taken for granted; it will become as mundane and indispensable as scanners and spreadsheets. Only when reports like this have become irrelevant will blockchain technology have begun to reach its potential. The contributors to this blueprint hope to move the world a little closer to that eventuality.

Checklist for Deploying a Blockchain-Powered Solution

- **Define your challenge, define your solution:** Blockchain is powerful technology, but it can't solve every problem. You wouldn't use a scalpel to crack an egg, right? Before adopting a blockchain-based solution, know your goal and know how blockchain technology will help to achieve it.

- **Prep your data:** Any digital system that runs on shoddy data runs the risk of garbage in, garbage out. With blockchain's immutable data structure, if you start with bad data you could be stuck with it forever. So ensure accurate, high quality data before moving to blockchain.

- **Make friends:** Collaborating with partners can lower costs, improve outcomes, and deliver more powerful solutions for everyone. Identify potential stakeholders—entities with shared interests who may benefit from the fixes you're introducing—and consider inviting them to the party. Innovation is an opportunity to make new alliances and engage old ones as you work together to build a secure common platform.

- **Think ahead:** You don't want today's solution to turn into tomorrow's headache. During the design process, consider your solution's compatibility with both existing legacy systems and other frontier technologies, as well as other blockchain platforms; in the future, your project could create unwanted silos if it's not interoperable. Think of both the financial and human resources required to maintain it—how much will troubleshooting cost and who will do it? Design today for a world three to five years in the future.

- **Innovate ethically:** Technology can have unintended consequences. Given the difficulty of altering data on a blockchain, consider how your solution will affect the people represented by the sensitive data contained therein—both now and into the future. Their privacy is your responsibility.

- **Consider accessibility**: What level of tech literacy or access is required to participate in your solution? Is the language accessible? How will particular communities respond to implementation? If you aim to serve marginalized populations, keep their needs in mind as you design.

- **Solve for identity:** Who are your users? More importantly, how do you know it's actually them? Identity is at the root of blockchain solutions. Scrutinize how best to confirm user identity in your project; biometrics, passwords, government issued IDs, and knowledge based authentication are all potential options.

- **Assess risks:** Every new technology has its risks; blockchain is no different. Try to anticipate potential pain points between collaborators and carefully weigh the pros and cons of design features like vendor and platform lock-in as you build. Factor in cybersecurity as well—just because blockchain is cryptographically secure doesn't mean that software built on it will be. Independent security audits can help fortify systems.

- **Expect to grow:** Starting small with a pilot or proof-of-concept makes sense, but you don't want to stay there. As you perform controlled tests of your blockchain-based system, remember that your ultimate goal is to reach full-scale operation. As you begin to scale up, consider running your blockchain solution in parallel with its predecessor until you're confident in the new system's results.

- **Comply and codify:** Blockchain solutions for governance and social impact rarely encounter major regulatory hurdles, but platforms that transfer financial assets or issue tokens with monetary value face more stringent requirements. Engaging legal counsel at the outset of your project can save a lot of trouble (and money) later on.

- **Assume unknown unknowns:** Blockchain is a new technology. Since unexplored territory is, well, unexplored, it's best to anticipate some uncertainty. Incorporate flexibility into your project timelines to accommodate surprises along the way. Ask questions about the tech and the specific solution on which you're working to clarify problems and inspire innovations.

100 Key Terms for Understanding Blockchain for Social Impact

To alleviate some of the confusion surrounding blockchain technology, it's vital to build a common lexicon of terms. Doing so will support understanding and innovation. In this spirit, New America created a list of key terms to serve as a resource and reference for the governance and social impact leaders working with this new technology. These terms have been written to be accessible and concise. A deeper explanation of many of these terms is included in other sections of the ***Blueprint for Blockchain and Social Innovation****. As the technology continues to evolve so will this list. We welcome your feedback at bta@newamerica.org and will try to incorporate additional views from the community.*

51% Attack: An attack on a network blockchain which allows the attacker to create fraudulent transactions. This is possible by means of controlling more than 50 percent of the network's mining or consensus-making power.

Accountability: The condition of an outcome being attributable to an individual's decisions or actions. By attaching record updates to individual identities, blockchain enables users to analyze who made a specific change, and hold them responsible for those changes.

Anchoring: An auditing mechanism used by some private blockchains that involves periodically storing a cryptographic fingerprint (called a hash) of all of the data on a private chain on a public platform (like Bitcoin or Ethereum). This applies the mining power that protects the public blockchain to the private blockchain, making the private blockchain more secure.

Append-Only: A quality of a database such that users can only write to, but not delete from the data. This is a key characteristic of blockchains.

Artificial Intelligence (AI): The study and development of computer systems that can perform "intelligent" tasks, such as speech recognition and decision-making. Machine learning is a type of artificial intelligence whereby computers use pattern recognition to predict answers based on a set of given examples. Blockchain technology may complement artificial intelligence by securely storing sensitive data, efficiently solving cryptography algorithms, and providing new data sources for machine learning.

Auditability: The degree of ease or difficulty that the outcome of a process can be verified by independent validators. The transparency of blockchain records enables third parties to verify the integrity of data.

Authentication: A method by which a person or machine can prove its identity, such as with a username and password or a digital signature. Authentication ensures that access to data or programs is restricted to an approved set of users.

Authorization: The process by which a person or machine determines what actions another machine or person can take. Users may have different privileges, such as reading data or writing information on the blockchain, based on their set of permissions.

Biometric Authentication: A form of authentication that uses body measurements (like fingerprints, iris scans etc.) as a means of identifying and granting access to individuals. Incorporating biometric systems into blockchain authentication processes has enabled some vulnerable communities, such as refugees and homeless populations to establish elements of their identity. Another use of biometric authentication in blockchain-based solutions is to add an additional layer of security for users.

Bitcoin (BTC): Bitcoin (BTC): The word "Bitcoin" refers to both a cryptocurrency and the blockchain that manages it. It was created in 2009, following publication of a white paper outlining the key parameters of the system. The paper was authored pseudonymously by Satoshi Nakamoto in 2008.[53]

Block: The foundational element of blockchain data structure. Transactions are grouped together into blocks and then and cryptographically linked in a chain to the preceding block. By linking blocks together into a blockchain, data becomes very difficult to change or delete.

Block Reward: A prescribed number of cryptocurrency tokens awarded to the node that successfully mines a block in a blockchain. These provide economic incentive for nodes to participate in a blockchain and form part of the consensus mechanism.

Censorship Resistance: A quality of blockchains that makes it difficult for a single entity to permanently prevent another party that is part of the network from posting data to a blockchain.

Consensus: A state of agreement which nodes reach regarding the status of new data that has been proposed to the blockchain.

Consensus mechanism: A fault-tolerant mechanism that is used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network within a peer-to-peer system.

Proof of Authority (PoA): A type of consensus mechanism used in private blockchains in which predetermined nodes are delegated validating authority.

Proof of Stake (PoS): A type of consensus mechanism used in blockchains that is based on a miner's existing token/cryptocurrency holdings. It has been positioned as a potential solution to the sustainability challenges of Proof of Work, but disproportionately empowers large cryptocurrency holders.

Proof of Work (PoW): A type of consensus mechanism used in blockchains that is based on the computing power that a miner contributes to a particular blockchain. Particularly when deployed in large networks such as the Bitcoin blockchain, PoW protocols are extremely secure. However, the amount of electricity required to power PoW blockchains has raised questions about their long-term sustainability.

Consortium Blockchain: A private blockchain where the consensus process is controlled by a pre-selected set of nodes, whose ownership is distributed among multiple organizations or individuals. This provides some of the efficiency and security available through public blockchains while enabling the higher levels of control of private blockchains.

Cryptocurrency: A type of digital currency, created using cryptographic techniques, which is used within a particular blockchain ecosystem.

Cryptography: A term used to describe the creation and use of protocols, algorithms, and codes to keep information confidential and to make changes to data evident as well as to authenticate users.

Decentralized Application ("DApp"): A smart contract or series of smart contracts with an unbound number of participants that may or may not involve digital assets. They are used to accomplish a goal (like sharing files) on a peer-to-peer network and can be more resilient than applications run on centralized databases as they do not have a single point of failure.[54]

Decentralization: The transfer of administrative control away from a single authority to other centers of control, typically through some degree of autonomy. The decentralized structure of blockchain makes it more secure and efficient when compared to other types of centralized databases.

Decryption: The conversion of coded, encrypted information, usually using computer algorithms.

Differential Privacy: A term coined by Cynthia Dwork in 2005 that describes a system which reduces the privacy loss when private information is used in a statistical data set. Public blockchains may benefit from differential privacy measures by allowing open data analysis without compromising user confidentiality.

Digital Signature: The application of a private key on a blockchain transaction, which provides a unique signature that proves the identity of the transacting party. Anyone with a corresponding public key, the signature, and the document, can verify that the document was “signed” by the owner of the private key. Digital signatures encrypt data between two parties, as well as prove the identity of those two parties.

Digital Wallet: A software designed to hold credentials for processing online transactions, such as public and private keys. Digital wallet addresses are cryptographically related to public and private keys, enabling users to direct payments or validate identity using their digital wallet addresses.

Disintermediation: The process of reducing or removing intermediaries in transactions.

Distributed Ledger Technology (DLT): A distributed database that exists across multiple locations in a peer-to-peer network. DLTs require a consensus mechanism to sequence, approve and synchronize changes that are broadcast to the network. Blockchains are a type of DLT, but not all DLTs are blockchains. A few examples of DLTs include R3 Corda, Hashgraph, and Tangle.

Double Spending: The attempt to spend the same resource (like a bitcoin) twice. Bitcoin was the first form of digital currency to solve the double spending problem, making it a viable currency substitute.

Efficiency: The quality of minimizing resource waste while achieving objectives. An example is data interoperability, which helps government fulfill their obligations at lower costs. Blockchain solutions can also be scaled easily and enable organizations to leapfrog in technological progress.

Ether: The main cryptocurrency used on the Ethereum blockchain.

Ethereum (ETH): A public blockchain platform designed by the Ethereum Foundation and released in 2015.

Encryption: The conversion of information into code, usually using computer algorithms. Encryption is typically used to prevent unauthorized access to data.

ERC20: The Ethereum Request for Comments 20 is the official protocol used to build applications on the Ethereum blockchain. ERC20 defines the protocols needed in order for a token to be considered an ERC20 token.

Exchange: A digital marketplace where traders can buy or sell cryptocurrencies and other blockchain tokens for fiat currency. Due to their centralized storage of private keys and fiat currencies, they have been the target of high profile hacks, such as Mt. Gox in 2013 and Bitfinex in 2016.

Fault Tolerance: The ability of a database to continue to function despite the failure of multiple nodes in its network.

Financial Inclusion: The provision of useful and affordable financial products and services that meet the needs of individuals and businesses.

Fork: A split in a blockchain, typically involving a change to the underlying protocol. Following a fork, members of a network choose which set of protocols to follow.

Hard Fork: A fork that fundamentally changes underlying blockchain software, creating an updated blockchain and legacy blockchain that run parallel and contain diverging blocks.

Soft Fork: A fork that upgrades blockchain software so that the original blockchain will accept transactions from both legacy and updated notes, while a new blockchain accepts only upgraded nodes. The software upgrade is only adopted if the majority of nodes update, otherwise it will fail and the original blockchain continues.

Friction: The total costs, both financial and non-financial, associated with a transaction or the movement of data and resources.

Gas: A fee charged by nodes on the Ethereum network to process a transaction or smart contract. Denoted in Ether, it economizes the computing power on the Ethereum network to ensure its efficiency.

Hash: A unique string of letters and numbers of prescribed length produced by a hash function that represents any unique piece of data. Any changes to underlying data will significantly change the hash output, contributing to the append-only nature of a blockchain.

Hashing: The act of taking an arbitrary amount of information, applying an algorithm (or "hash function"), and producing an output of fixed length. It can also reproduce the original information from the hash output.

Hybrid Blockchain: A type of blockchain that combines elements of private and public chains. These typically take one of two forms: a private blockchain built on a public platform like Ethereum (sometimes called a "side chain"), or a private chain that is "anchored" to a public platform.

Hyperledger: An open source blockchain project that provides software and tools for the creation and modification of mostly private blockchains.

Immutability: The quality of permanence or the inability to change. While often used to describe data within a blockchain, many argue that blockchain data is not immutable, but rather highly tamper resistant and can be changed under rare circumstances.

Initial Coin Offering (ICO): A process by which a portion of a particular protocol's cryptocurrency or tokens are sold to early backers in exchange for either fiat currency or a more established cryptocurrency. These funds can be used for a variety of purposes. ICOs are seen as being subject to less stringent regulation than initial public offerings (IPOs), but the process is under scrutiny from regulators.

Intermediary: A third party that serves to coordinate or facilitate exchange between two or more entities. Blockchains use algorithms to instill trust within an exchange, and may remove the need for many intermediaries.

Internet of Things (IoT): The network created by the connection of everyday devices (refrigerators or cars, for example) via the use of the internet and embedded computers. Autonomous coordination between devices promises to yield large efficiency gains. Blockchain technology has been suggested as a way to secure IoT systems from cyber threats while efficiently exchanging information and autonomously executing tasks through smart contracts.

Interoperability: The ability of different protocols, databases, and software to communicate, exchange, and use information. As blockchain solutions scale across industries and geographies, ensuring that disparate systems can communicate with one another will be central to blockchain scalability.

Latency: The amount of time it takes data to propagate across and be stored by a network (used to describe the speed of a particular network). For many blockchains, there is a direct relationship between network security and latency.

Litecoin (LTC): A cryptocurrency derived from Bitcoin. Its most notable differences are the increased block creation rate, which decreases transaction time but creates more orphaned blocks, and its use of the Scrypt algorithm for its proof of work consensus mechanism, which relies more heavily on computer RAM for processing rather than processor power.

Metadata: The information that helps organize and locate data within a system, such as the timestamp of a sent message.

Miner: The process of adding transaction records to a public blockchain. Miners solve a difficult mathematical problem using a cryptographic algorithm. This results in a solution called the Proof Of Work, which ensures that a miner did in fact solve the problem. Miners are usually rewarded for finding successful solutions with digital currency.

Multichain: An open-source blockchain platform created by Coin Sciences that enables organizations to create custom blockchains using a series of modular components and setting to fulfill certain organizational needs.

MultiSignature: A technology that adds security to transactions by requiring more than one key to authorize a transaction. As such, single points of failure can be eliminated by ensuring that funds can be accessed even if a single key is compromised. It provides insurance to digital asset holders while preserving the security of public key cryptography. It is often abbreviated as "MultiSig."

Network: An interconnected system of two or more digital devices that can exchange data.

Node: An alternative term for a computer that is a member of a network, blockchain or distributed ledger.

Full Node: A node that stores a full copy of a blockchain database and can act as a validator. See also "lite node" and "validator."

Lite Node (Lite Client): A node that stores only the portion of a blockchain database that is relevant to its owner. This is in contrast to Full Nodes, which store the entire database.

Off-chain: A type of data resulting from real-world events or physical processes that take place outside of the confines of a blockchain, and is not governed by its protocol.

On-chain: A type of data resulting from digital processes that take place within of the confines of a blockchain, and is governed by its protocol.

Open Source: A classification of software for which the source code is freely available, operates independently of other software, and which can be modified and improved upon by virtually any party. Open source software can be easily audited by other experts, and provides stakeholders with transparency in how the underlying code functions.

Openness: The degree of ease or difficulty for a node to join a network.

Oracle: A source of external data to a blockchain that can be used to triggersmart contract executions when predefined conditions are met. This is because smart contracts on a blockchain cannot automatically access data outside of their network. For example, the Associated Press or Weather.com could serve as an oracle for rainfall data used to determine the payout of a smart contract for crop insurance.

Peer-to-Peer Network: A network that allows participating parties to exchange information without relying on a central node or actor as a relay.

Permission: The access required to perform a task, such as reading or writing data. Blockchains vary in how open they are to individuals using, processing and building on them. Permissionless blockchains allow anyone to create new block and contribute to the network. Private or permissioned blockchains require access privileges.

Personally Identifiable Information (PII): The information that can be used to identify, locate, or contact an individual. While some blockchain configurations provide more secure methods of storing PII than centralized databases, some argue that the transparent nature of some blockchains could jeopardize individual privacy.

Pilot: A test of a protocol in the field to determine whether it is technically and economically viable to produce, uncovers bugs with the underlying code, and ultimately determines whether it is likely to successfully scale. Frequently used interchangeably with proof of concept (PoC).

Prefix: Otherwise known as the "longest chain", the prefix is considered the consensus view of a blockchain network at any one time.

Private Blockchain: A blockchain in which a single entity, or group of entities, that is typically already part of the network, select what nodes have the ability to read, write, and validate data added to the chain. Data is typically visible only to those allowed into the network.

Private Key: A long string of randomly generated alphanumeric characters that is cryptographically linked to a public key and functions as a secret password to generate a signature that can be used to authorize transactions and authenticate data. A private key is unique to one party.

Proof of Concept (PoC): Frequently used interchangeably with pilot. However, a proof of concept (PoC) is the act of demonstrating that a design concept or plan is feasible, a pilot is focused on testing. A PoC is usually small in scale, and sometimes incomplete.

Protocol: 1) An alternative name for a particular blockchain or distributed ledger; 2) A difficult to change rule or set of rules that defines the terms by which a blockchain or other type of DLT operate.

Pseudonymity: The means of identifying a party on a blockchain using a false name. While blockchains are frequently referred to as providing anonymity, pseudonymity is more precise, since parties do have identifiers.

Public blockchain: A blockchain in which read, write, and validate permissions are theoretically open to anyone with access to the Internet and the appropriate hardware. Data is typically visible to anyone who joins the network.

Public Key: A long string of randomly generated alphanumeric characters that is cryptographically linked to a private key and functions as a form of address or alias. This is also known as an "address."

Public Key Cryptography: A cryptographic method used to securely exchange information without revealing the information itself. Also referred to as public key encryption or asymmetric encryption.

Resiliency: The capacity to maintain the capacity to function despite challenges. Blockchain's decentralization and consensus mechanism protect the network from challenges like node failure and malicious actors.

Right to be Forgotten: A digital privacy right for online personal information. According to the European Union’s General Data Protection Regulation (GDPR), any individual can file a claim for the correction or removal of their personal data (or personally identifiable information) from public sources if the information is no longer necessary for the purposes it was collected for or if the person has not given consent for data storage or processing.

Ripple (XRP): A controversial cryptocurrency that is now commonly used by the financial service sector to settle large asset transfers and pay remittances. Ripple sacrifices the "trustless" environment of typical blockchains for transaction speed and current stability, giving rise to the critique that it is not a true cryptocurrency.

Scalability: The capability of a system, organization or process to sustain or increase its performance and accommodate growth. For example, a blockchain solution can be designed as a proof-of-concept (smaller in scope), but the design can account for the potential to scale to serve larger populations in the future.

Security: The ability to ensure continued access and integrity of data despite threats. Blockchain networks safeguard data by preventing single points of failure and leverage cryptography to ensure unauthorized additions to the ledger are noticed and rejected by the network.

Self-Sovereign Identity: A new conceptualization of identity based on blockchain. It enables individuals to maintain control of individual identity information and allows institutions and organizations to authenticate access to services based on identity attributes rather than full identity information.

SHA-256: A cryptographic hash function created by the NSA which is used in the Proof of Work algorithm and in the creation of public and private keys on certain blockchains.

Sharding: A technical term used to describe the partitioning of a database into smaller parts. Sharding can be used to build a scalable database and is necessary if a dataset is too large to be stored in a single database.

Side Chain: A type of hybrid blockchain in which a private blockchain is attached to a larger, public blockchain.

Smart Contract: A program written onto a blockchain that performs a specific task once predetermined conditions are met. Once rules and penalties are agreed to by its parties, a smart contract becomes a self-executing and self-enforcing contract. For example, a smart contract can hold upfront payments for produce in escrow for farmers to ensure fair and equitable payment throughout the year. See also, **Oracle**.

Tamper Resistance: Used to describe the quality of blockchains that makes data encoded in them hard to change and makes changes, when executed, evident.

Token: A type of cryptographically secured asset used for different applications on blockchains (it may or may not have monetary value). These can either be used as an endemic currency within the platform, or represent assets in the real world such as electricity, financial credit, or physical space in a shipping container. Also referred to as a "coin".

Tokenization: The conversion of the rights to a real world asset (digital or physical) into a digital token that can be transferred between parties via blockchain.[55]

Transaction: An exchange of value or data in a blockchain network. The exchanged data can be the actual unencrypted information, an encrypted version, or a digital signature that represents the data while the data itself is held off-chain.

Transaction Fees: The fees that network members pay to incentivize miners to verify transactions and include said data or transaction in their block. They are also used to explain one of the benefits of disintermediation: transaction fees garnered by intermediaries can be reduced or eliminated.

Transparency: The ability for citizens or stakeholders to monitor and understand actions taken by their government or company. Certain blockchains enable anyone to access data and information about who adds data to the ledger, providing stakeholders with information to facilitate participation in decision-making.

Two-Factor Authentication: A security measure in which an individual must demonstrate something they know, such as a password, and something they own, such as a phone, to prove their identity.

Valid: A block or transaction that is aligned with the rules established by a particular protocol.

Validation: The process by which nodes within a blockchain ensure that a transaction adheres to a set of rules previously established by a blockchain's protocol. By determining if data is valid or not, a blockchain maintains accuracy and cleanliness as more uses append information over time.

Validator: A node that stores a full copy of a blockchain ledger and is authorized to validate data from other nodes in a blockchain network.

Zero Knowledge Proof: A method of verifying that a transacting party knows a piece of information without revealing what that information is. This enables two untrusted parties to persuade each other without sacrificing secrecy. Zero proof knowledge can be used to verify a person's identity without jeopardizing confidentiality, such as verifying eligibility for social benefits without revealing personal information.

Additional Resources

Big Picture

- **Bellagio Blockchain Summit: Outcomes and Insights**, New America, Tomicah Tillemann and Allison Price
- **The Blockchain Application Stack**, Coindesk, Joel Monegro
- **Explain Blockchain at 5 Levels**, Animal Ventures, Tom Serres
- **Programmable Blockchains in Context: Ethereum's Future**, ConsenSys, Vinay Gupta
- **The Truth About Blockchain**, Harvard Business Review, Marco Iansiti and Karim Lakhani
- **Why the blockchain matters**, *Wired*, Reid Hoffman
- **WTF is The Blockchain**, Hacker Noon, Mohit Mamoria

Key Concepts

- **The Blockchain Ethical Design Framework**, the Beeck Center for Social Impact & Innovation, Cara Lapointe and Lara Fishbone
- **The Meaning of Decentralization**, Vitalik Buterin
- **What Do We Mean by "Blockchains are "Trustless"?** Preethi Kasiready

Blockchain Applications

- **Blockchain Powered Financial Inclusion**, Pani Baruri
- **How Blockchain is Enabling a Local Energy Movement**, New America, Eli Wallach
- **How to Save the World with Blockchain**, New America, Asvatha Babu
- **The Nail Finds a Hammer**, New America, Michael Graglia, Christopher Mellon, and Tim Robustelli

- **Republic of Georgia's Blockchain Land-Titling Project**, Bitfury
- **Sustainable Supply Chains**, New America, Allison Price and Sara Golden
- **USAID Primer on Blockchain**, USAID, Paul Nelson

Newsletters, Courses, Books

- **Blockchain Revolution (Book)**, Don Tapscott and Alex Tapscott
- **Chain Letter (Newsletter)**, MIT Technology Review

Quick Intros (<10 mins)

- **Not Just Bitcoin: Why The Blockchain Is A Seductive Technology To Many Industries**, NPR, Naomi Lachance

Technical Overviews (2-4 hours)

- **Bitcoin and Blockchain: Two Revolutions For The Price Of One?** Richard Gendal Brown
- **Blockchain Demo** (simple)
- **Blockchain Technology Overview**, National Institute of Standards and Technology
- **Hash, Block, and Blockchain Interactive Demo**, Anders Brownworth
- **Hashing used in blockchain**

Books (1 - 2 days)

- **Blockchain Revolution**, Don Tapscott and Alex Tapscott

Courses (4 - 5 weeks)

- **Blockchain Fundamentals**, University of California, Berkeley

Notes

[1] "2017 Edelman Trust Barometer," Edelman, January 21, 2017, https://www.edelman.com/research/2017-edelman-trust-barometer

[2] A distributed database that exists across multiple locations in a peer-to-peer network. DLTs require a consensus mechanism to sequence, approve and synchronize changes that are broadcast to the network. Blockchains are a type of DLT, but not all DLTs are blockchains. A few examples of DLTs include R3 Corda, Hashgraph, and Tangle.

[3] A network that allows participating parties to exchange information without relying on a central node or actor as a relay.

[4] A long string of randomly generated alphanumeric characters that is cryptographically linked to a private key and functions as a form of address or alias. This is also known as an "address."

[5] The means of identifying a party on a blockchain using a false name. While blockchains are frequently referred to as providing anonymity, pseudonymity is more precise, since parties do have identifiers.

[6] An exchange of value or data in a blockchain network. The exchanged data can be the actual unencrypted information, an encrypted version, or a digital signature that represents the data while the data itself is held off-chain.

[7] A long string of randomly generated alphanumeric characters that is cryptographically linked to a public key and functions as a secret password to generate a signature that can be used to authorize transactions and authenticate data. A private key is unique to one party.

[8] The application of a private key on a blockchain transaction, which provides a unique signature that proves the identity of the transacting party. Anyone with a corresponding public key, the signature, and the document, can verify that the document was "signed" by the owner of the private key. Digital signatures encrypt data between two parties, as well as prove the identity of those two parties.

[9] A type of data resulting from real-world events or physical processes that take place outside of the confines of a blockchain, and is not governed by its protocol.

[10] The process by which nodes within a blockchain ensure that a transaction adheres to a set of rules previously established by a blockchain's protocol. By determining if data is valid or not, a blockchain maintains accuracy and cleanliness as more uses append information over time.

[11] The foundational element of blockchain data structure. Transactions are grouped together into blocks and then and cryptographically linked in a chain to the preceding block. By linking blocks together into a blockchain, data becomes very difficult to change or delete.

[12] An alternative term for a computer that is a member of a network, blockchain or distributed ledger.

[13] A fault-tolerant mechanism that is used in blockchain systems to achieve the necessary agreement on a single data value or a single state of the network within a peer-to-peer system.

[14] A type of consensus mechanism used in blockchains that is based on a miner's existing token/cryptocurrency holdings. It has been positioned as a potential solution to the sustainability challenges of Proof of Work, but disproportionately empowers large cryptocurrency holders.

[15] A type of consensus mechanism used in blockchains that is based on the computing power that a miner contributes to a particular blockchain. Particularly when deployed in large networks such as the Bitcoin blockchain, PoW protocols are extremely secure. However, the amount of electricity required to

power PoW blockchains has raised questions about their long-term sustainability.

16 A type of consensus mechanism used in private blockchains in which predetermined nodes are delegated validating authority.

17 An alternative name for a particular blockchain or distributed ledger; 2) A difficult to change rule or set of rules that defines the terms by which a blockchain or other type of DLT operate.

18 The degree of ease or difficulty for a node to join a network.

19 The cryptocurrency used on the Bitcoin blockchain. The word "Bitcoin" can both refer to the cryptocurrency and the blockchain that manages the bitcoin currency.

20 A public blockchain platform designed by the Ethereum Foundation and released in 2015.

21 An open source blockchain project that provides software and tools for the creation and modification of mostly private blockchains.

22 The access required to perform a task, such as reading or writing data. Blockchains vary in how open they are to individuals using, processing and building on them. Permissionless blockchains allow anyone to create new block and contribute to the network. Private or permissioned blockchains require access privileges.

23 A classification of software for which the source code is freely available, operates independently of other software, and which can be modified and improved upon by virtually any party. Open source software can be easily audited by other experts, and provides stakeholders with transparency in how the underlying code functions.

24 "The Open Source Definition (Annotated)," Open Source Initiative, https://opensource.org/osd-annotated. Due to the prevalence of legacy platforms in the blockchain space, the independent operability requirement has been omitted.

25 A type of cryptographically secured asset used for different applications on blockchains (it may or may not have monetary value). These can either be used as an endemic currency within the platform, or represent assets in the real world such as electricity, financial credit, or physical space in a shipping container. Also referred to as a "coin".

26 The main cryptocurrency used on the Ethereum blockchain.

27 A program written onto a blockchain that performs a specific task once predetermined conditions are met. Once rules and penalties are agreed to by its parties, a smart contract becomes a self-executing and self-enforcing contract. For example, a smart contract can hold upfront payments for produce in escrow for farmers to ensure fair and equitable payment throughout the year. See also, Oracle.

28 A third party that serves to coordinate or facilitate exchange between two or more entities. Blockchains use algorithms to instill trust within an exchange, and may remove the need for many intermediaries.

29 The study and development of computer systems that can perform "intelligent" tasks, such as speech recognition and decision-making. Machine learning is a type of artificial intelligence whereby computers use pattern recognition to predict answers based on a set of given examples. Blockchain technology may complement artificial intelligence by securely storing sensitive data, efficiently solving cryptography algorithms, and providing new data sources for machine learning.

30 Jon-Amerin Vorabutra, "Why Blockchain is a Game Changer for Supply Chain Management Transparency," Supply Chain 24/7, October 3, 2016, https://www.supplychain247.com/article/why_blockchain_is_a_game_changer_for_the_supply_chain

[31] Laurel Deppen, “Infographic: How blockchain can disrupt the future of education,” TechRepublic, June 18, 2018, https://www.techrepublic.com/article/infographic-how-blockchain-can-disrupt-the-future-of-education/

[32] Andrew Arnold, “Is Blockchain The Answer To A Better Healthcare Industry?” *Forbes*, Aug 26, 2018, https://www.forbes.com/sites/andrewarnold/2018/08/26/is-blockchain-the-answer-to-a-better-healthcare-industry/#309b07ae75a8

[33] A quality of blockchains that makes it difficult for a single entity to permanently prevent another party that is part of the network from posting data to a blockchain.

[34] “Cyber Incident & Breach Trends Report,” the Online Trust Alliance, January 25, 2018, https://www.otalliance.org/system/files/files/initiative/documents/ota_cyber_incident_trends_report_jan2018.pdf In 2017, hackers gained access to more than 7 billion records from enormous data providers like Verizon, Uber, and Equifax. Since 2015, breaches in supposedly secure business email accounts have cost nearly $16 billion.

[35] The conversion of information into code, usually using computer algorithms. Encryption is typically used to prevent unauthorized access to data.

[36] The ability of a database to continue to function despite the failure of multiple nodes in its network.

[37] A new conceptualization of identity based on blockchain. It enables individuals to maintain control of individual identity information and allows institutions and organizations to authenticate access to services based on identity attributes rather than full identity information.

[38] The amount of time it takes data to propagate across and be stored by a network (used to describe the speed of a particular network). For many blockchains, there is a direct relationship between network security and latency.

[39] “Corruption Perceptions Index 2017,” Transparency International, February 21, 2017, https://www.transparency.org/news/feature/corruption_perceptions_index_2017.

[40] The degree of ease or difficulty that the outcome of a process can be verified by independent validators. The transparency of blockchain records enable third parties to verify the integrity of data.

[41] The quality of permanence or the inability to change. While often used to describe data within a blockchain, many argue that blockchain data is not immutable, but rather highly tamper resistant and can be changed under rare circumstances.

[42] The information that helps organize and locate data within a system, such as the timestamp of a sent message.

[43] Thomas C Redman, “Bad Data Costs the U.S. $3 Trillion Per Year,” *Harvard Business Review*, September 22, 2016, hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year

[44] A technical term used to describe the partitioning of a database into smaller parts. Sharding can be used to build a scalable database and is necessary if a dataset is too large to be stored in a single database.

[45] A term coined by Cynthia Dwork in 2005 that describes a system which reduces the privacy loss when private information is used in a statistical data set. Public blockchains may benefit from differential privacy measures by allowing open data analysis without compromising user confidentiality.

[46] Cara LaPointe and Lara Fishbane, "The Blockchain Ethical Design Framework," The Beeck Center for Social Impact and Innovation at Georgetown University, June 2018, http://beeckcenter.georgetown.edu/wp-content/

uploads/2018/06/The-Blockchain-Ethical-Design-Framework.pdf

[47] Russ Juskalian, "Inside the Jordan Refugee Camp That Runs on Blockchain," *MIT Technology Review*, April 12, 2018, https://www.technologyreview.com/s/610806/inside-the-jordan-refugee-camp-that-runs-on-blockchain

[48] Magnus Kempe, “The Land Registry in the Blockchain - testbed,” Kairos Future, March 2017, https://chromaway.com/papers/Blockchain_Landregistry_Report_2017.pdf

[49] "AgUnity: Blockchain for the Greater Good", AgUnity, http://www.agunity.com.

[50] The study and development of computer systems that can perform “intelligent” tasks, such as speech recognition and decision-making. Machine learning is a type of artificial intelligence whereby computers use pattern recognition to predict answers based on a set of given examples. Blockchain technology may complement artificial intelligence by securely storing sensitive data, efficiently solving cryptography algorithms, and providing new data sources for machine learning.

[51] The network created by the connection of everyday devices (refrigerators or cars, for example) via the use of the internet and embedded computers. Autonomous coordination between devices promises to yield large efficiency gains. Blockchain technology has been suggested as a way to secure IoT systems from cyber threats while efficiently exchanging information and autonomously executing tasks through smart contracts.

[52] Cynthia Dwork, *Four Facets of Differential Privacy*, Differential Privacy Symposium, Institute of Advanced Study, November 12, 2016, https://www.youtube.com/watch?v=lg-VhHlztqo.

[53] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Bitcoin. https://bitcoin.org/bitcoin.pdf

[54] Vitalik Buterin, “ DAOs, DACs, DAs and More: An Incomplete Terminology Guide,” Ethereum Blog, May 6, 2014, https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/

[55] Addison Cameron-Huff, "How Tokenization is Putting Real-World Assets on Blockchains,” Nasdaq, March 30, 2017, https://www.nasdaq.com/article/how-tokenization-is-putting-real-world-assets-on-blockchains-cm767952,

NEW
AMERICA