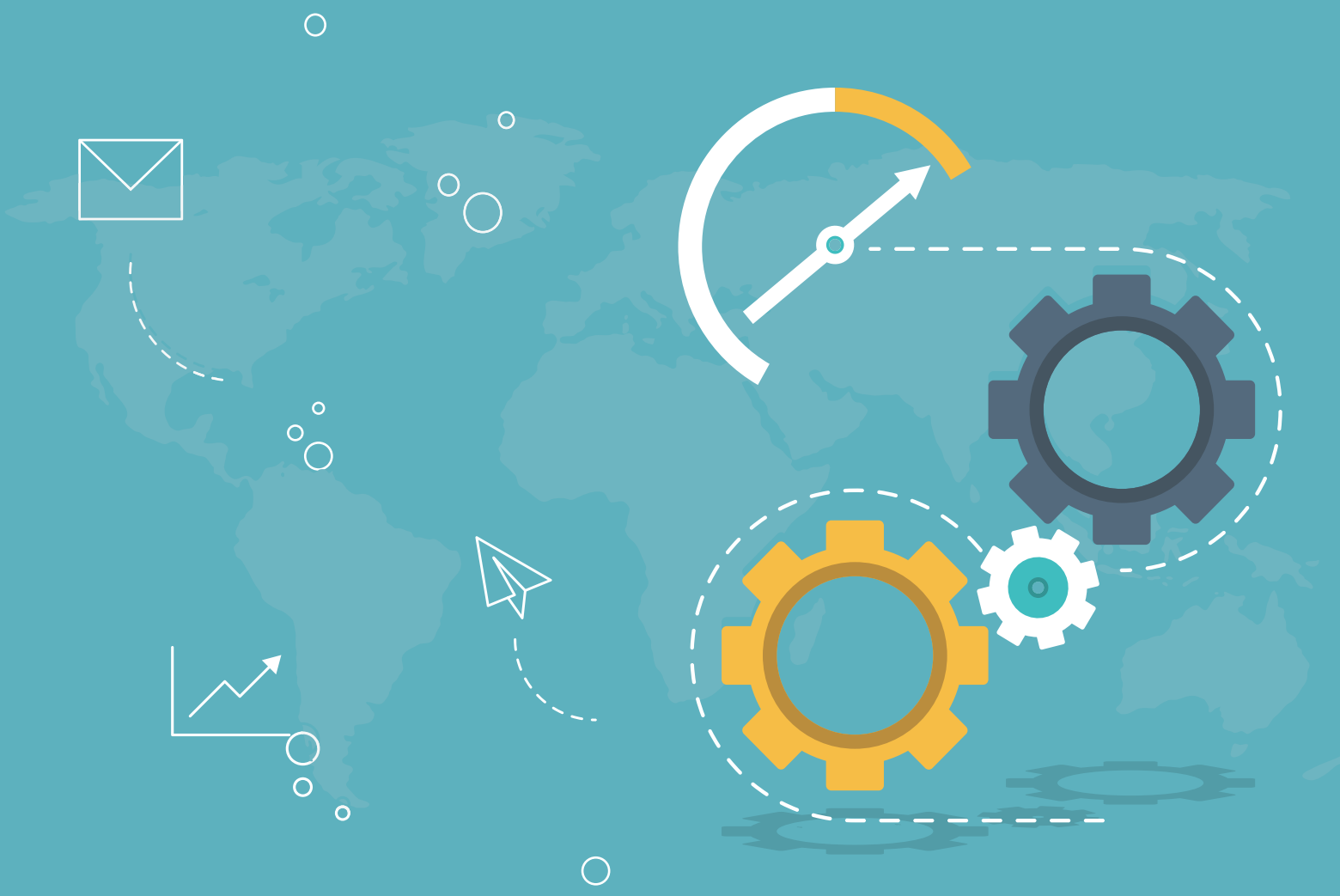
DATA PROTECTION IN THE HUMANITARIAN SECTOR

A Blockchain Approach



DH Network
Digital Humanitarian Network

MARCH 2019

Licensing Information

“Data Protection in the Humanitarian Sector: A Blockchain Approach ”
by Irene Solaiman and Andrej Verity, is licensed under
Creative Commons Attribution-NonCommercial 3.0 Unported.

DATA PROTECTION IN THE HUMANITARIAN SECTOR: A BLOCKCHAIN APPROACH

by

Irene Solaiman (irs623@student.hks.harvard.edu)
Master in Public Policy
Harvard University

Andrej Verity (verity@un.org | @andrejverity)
Office for the Coordination of Humanitarian Affairs (OCHA)
United Nations

Design

Jiahui Du (jd3399@tc.columbia.edu)
MA in Instructional Technology and Media
Teachers College, Columbia University

This document was made possible
with the support of UN-OCHA

KEY MESSAGES

- Responsible data collection spans multiple parties and organizations, who must coordinate for responsible data protection.
- In the humanitarian sector, data is increasingly digitized and sensitive information is vulnerable to cyber attack.
- Blockchain is an emerging but viable technology that enforces trust and transparency in data security and protection.
- Blockchain enables data privacy and immutability through its structure and cryptography to protect against cyber attack.
- Considerations for blockchain implementation range from resources to personal and professional perceptions to handling the technology.

INTRODUCTION

Data collection and storage are becoming increasingly digital. In the humanitarian sector, data motivates action, informing organizations who then determine priorities and resource allocation in crises.

"Humanitarians are dependent on technology and on the Internet. When life-saving aid isn't delivered on time and to the right beneficiaries, people can die."

-Brookings[1]

In the age of information and cyber warfare, humanitarian organizations must take measures to protect civilians, especially those in critical and vulnerable positions.

"Data privacy and ensuring protection from harm, including the provision of data security, are therefore fundamentally linked—and neither can be realized without the other."

-The Signal Code[2]

Information in the wrong hands can risk lives or even force aid organizations to shut down. For example, in 2009, Sudan expelled over a dozen international non-governmental organizations (NGOs) that were deemed key to maintaining a lifeline to 4.7 million people in western Darfur[3]. The expulsion occurred after the Sudanese Government collected Internet-accessible information that made leadership fear international criminal charges[4] . Responsible data protection is a crucial component of cybersecurity.

As technology develops, so do threats and data vulnerabilities. Emerging technologies such as blockchain provide further security to sensitive information and overall data storage. Still, with new technologies come considerations for implementation.

---

1. Why Humanitarians Should Pay Attention to Cybersecurity. Brookings, 2014. https://www.brookings.edu/blog/up-front/2014/06/02/why-humanitarians-should-pay-attention-to-cybersecurity/
2. The Signal Code: A Human Rights Approach to Information During Crisis. Harvard Humanitarian Initiative, 2017. https://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf
3. More aid agencies under "investigation". IRIN, 2009. http://www.irinnews.org/report/83330/sudan-more-aid-agencies-under-investigation
4. Why Humanitarians Should Pay Attention to Cybersecurity. Brookings, 2014. https://www.brookings.edu/blog/up-front/2014/06/02/why-humanitarians-should-pay-attention-to-cybersecurity/

DIGITAL DATA IN THE HUMANITARIAN SECTOR

Overview: What is data in the humanitarian sector?

The humanitarian sector is information-driven. Responding to crises requires various type of information to be shared - from assessments, to logistics, to delivered assistance, to organizational response[5]. Collection is increasingly digital and provided through new, modern means such as KoBoToolbox. And, modern devices are extending data sources even further. For example, civil society members on personal devices, such as mobile phones, are part of the Internet of Things[6] contributing to data collection.

Data collection and actors involved

Data collected in four phases

Data collection changes depending on the type and stage of an emergency. In general, data collection can be seen in four chronological phases: preparedness, acute, chronic, and post-crisis[7]. The data collected may overlap and differ per incident.

1. **Preparedness**: The preparedness phase provides baseline data for humanitarian actors to gauge the population and environment pre-crisis. This includes demographics, infrastructure, and regional geography[8].

2. **Acute:** During the acute phase, the crisis has recently hit and affected a certain population. Data includes the severity of damage on people and environment. Data may evolve over the course of the crisis, meaning data must be continuously collected and managed[9].

3. **Chronic**: If a crisis situation is long-lasting, chronic data collection refers to iterative collection processes.

---

5. The Signal Code: A Human Rights Approach to Information During Crisis. Harvard Humanitarian Initiative, 2017. https://hhi.harvard.edu/sites/default/files/publications/signalcode_final.pdf
6. Humanitarianism in the Network Age. OCHA, 2013. https://www.unocha.org/sites/unocha/files/HINA_0.pdf
7. Guidelines on Data Issues in Humanitarian Crisis Situations. UNFP, 2010. https://www.unfpa.org/publications/guidelines-data-issues-humanitarian-crisis-situations#
8. Data preparedness: connecting data, decision making, and humanitarian response. Harvard Humanitarian Initiative, 2016. https://hhi.harvard.edu/sites/default/files/publications/data_preparedness_update.pdf
9. Data preparedness: connecting data, decision making, and humanitarian response. Harvard Humanitarian Initiative, 2016. https://hhi.harvard.edu/sites/default/files/publications/data_preparedness_update.pdf

4. **Post-crisis**: Once the crisis has ended, meaning hostilities have ceased or a natural disaster has ended, post-crisis data is collected for transition, recovery, and reconstruction[10].

Actors

Humanitarian sector actors change based on the situation and environment. These actors may work independently, but are most likely to collaborate and share information during crises.

Humanitarian agencies

Humanitarian agencies may include international and national NGOs as well as UN agencies such as the Office for the Coordination of Humanitarian Affairs (OCHA), the International Organization for Migration (IOM), and the UN High Commission for Refugees (UNHCR).

Using the Humanitarian Programme Cycle, organizations collect data in a cycle for effective coordination and information management. Ideally, organizations first conduct a needs assessment and analysis then begin strategic response planning. Using this strategy and data, they are able mobilize resources in order to undertake their response and related monitoring. Post response, organizations conduct an operational review and evaluation[11].

The Centre for Humanitarian Data exemplifies data connectivity, transparency, and responsible use; systems are increasingly shared among organizations and must be properly and responsibly integrated[12].

International/National NGOs

Whether solely a humanitarian organization or a larger organization with a humanitarian-focused department, NGOs may be involved directly or "touch" processes with data collection.

UN agencies

In addition to agencies specifically dedicated to humanitarian response and coordination, UN missions and programs globally work with vulnerable peoples and crises. This includes organizations such as World Health Organization (WHO), the UN Development Programme (UNDP), UN Women, and the UN Population Fund (UNFPA).

Government ministries/departments

Government data collection reaches past constituents to visitors. The Census Bureau and other Statistics offices gather regular data and statistics on the country and regional populations.

---

10. Guidelines on Data Issues in Humanitarian Crisis Situations. UNFP, 2010. https://www.unfpa.org/publications/guidelines-data-issues-humanitarian-crisis-situations#
11. Humanitarian Programme Cycle. 2018. https://www.humanitarianresponse.info/en/programme-cycle/space
12. Centre for Humanitarian Data. 2016. https://centre.humdata.org/wp-content/uploads/centreforhumdata_handout_dec2016.pdf

Multiple ministries are involved in either data collection, humanitarian response, or both, from storing administrative records to actively conducting surveys. National Emergency Task Force, and other agencies with response capabilities, collect data for people's protection.

Civil society

Local communities and overall civil society may formally or informally collect public or sensitive data. This may range from administrative records in community-organized groups or personal information in a local religious group.

Researchers and Partners

Research institutions may data collect for public or private reports on demography or other aspects of a certain region. They may conduct research alone, or partner with government and other agencies to produce surveys and analyses. Other development partners and consultants may conduct similar research.

Private companies

Ranging from local retail shops to large, global-spanning social media sites, the private sector will collect information on the affected population. This collection is generally part of their regular daily commerce-related activities, but could provide benefit to the humanitarian actors if shared properly.

Types of information being collected

The actual data being collected can be placed into four categories: personal information, community information, environmental information, and metadata[13].

Personal information

Personal information refers to data on individuals. This often means victims of crises, but can be expanded to all individuals involved like humanitarian workers. Data collected can range from bank accounts and financial data to biometrics, like fingerprints and iris scans. Personal information is highly sensitive and subject to data privacy rights.

Community Information

Community information defines a preset population or community. It refers to the population size and spatial distribution and physical demographics like the community's age-sex structure. Socioeconomic characteristics factor in income levels and educational levels, as well as human capacity and skills by sector and occupation. More personal information, like reproductive behavior patterns, meaning family size and contraceptive practice is also collected. In addition, community culture, though more difficult to gauge, is of interest. During crisis, counts and qualitative and quantitative surveys of number of people affected and their causes for displacement, location, and health needs are critical for response. Also noted is the mortality rate in a given population and the culture in an affected zone.

13. Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies. OCHA, 2014. https://www.unocha.org/sites/unocha/files/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf

Environmental information

Environmental information refers to community facilities and regional and geographical information, like satellite imagery. This can be paired with community information through Geographic Information System mapping.

Metadata

Data that does not fit explicitly into the previous categories or is not intentionally collected for a specific purpose may include what populations are being researched, what organizations are collecting data, and time of collection. Often overlooked, collated metadata can reveal personal information or be used to access datasets.

Existing protection on this data

Existing protection on humanitarian data is covered in international guidelines and regional data protection and privacy laws. The UN General Assembly's 1990 Guidelines for the Regulation of Computerized Personal Data Files and the 2013 resolution on "the right to privacy in the digital age" exemplify international recognition of data protection in humanitarianism[14]. Regionally, the EU's General Data Protection Regulation (GDPR) applies to EU members and states in the European Economic Area. All members of the Council of Europe--over 50 states--have ratified the 1981 Convention for the Privacy of Individuals with regards to Automatic Processing of Personal Data treaty[15]. Globally, 126 countries have national data protection legal frameworks[16]. However, technology and hacking methods progress faster than guidance and legal frameworks can be created and passed.

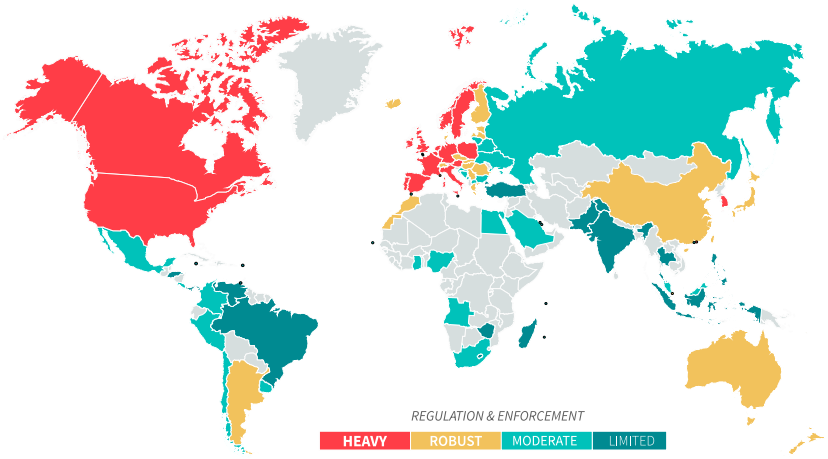


Figure 1: Data protection laws heatmap17

14. Humanitarianism in the Age of Cyber-warfare: Towards the Principled and Secure Use of Information in Humanitarian Emergencies. OCHA, 2014. https://www.unocha.org/sites/unocha/files/Humanitarianism%20in%20the%20Cyberwarfare%20Age%20-%20OCHA%20Policy%20Paper%2011.pdf

15. Details of Treaty No. 108. Council of Europe, 2018. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108

16. Data Protection Day 2018: A Global Perspective to Privacy. Privacy International, 2018. https://privacyinternational.org/blog/1080/data-protection-day-2018-global-perspective-privacy

17. Data Protection Laws of the World. DLA Piper, 2018. https://www.dlapiperdataprotection.com/index.html?t=world-map&c=AO

CYBERSECURITY 

As the humanitarian sector becomes increasingly digitized, cybersecurity becomes increasingly more important. Vulnerabilities paired with threat lead to risk, which may have disastrous consequences. Compromised data could not only affect the world's most vulnerable populations, but also undermine trust in humanitarian organizations.

Vulnerabilities

Key vulnerabilities lie in sensitive information and in data storage.

Sensitive and Personally Identifiable Information (PII): critical information ranges from data on infrastructure to the most sensitive of personal data. This includes information of people working in the humanitarian sector, who may be targeted. Sensitive information must only be accessible to appropriate personnel. If compromised and used by a malicious actor, it could foil humanitarian missions.

"If this information falls into the wrong hands, it could jeopardize personnel or leave vulnerable populations without life-saving supplies."

-Devex International Development

Data storage

How data is stored and shared affects its vulnerability to cyber attack. Most data is stored on a central system. However, once compromised, a central system can lead to large amounts of data being vulnerable. Data may be easily lost and requires frequent backups. Since only located centrally, data may not be valid or may have been altered.

Potential attacks

Potential attacks that compromise data can come from inopportune circumstances, like a physical disaster, as well as malicious actors. Attacks resulting in data loss or theft can be devastating, especially if the data is not backed up or recoverable.

Environmental/physical

Environmental or physical incidents, such as a building fires, floods, or power outages, can affect hardware systems. Physical access to a system may be temporarily lost in an environmental event where personnel physically cannot get to a hardware system. If the data is not backed up and only exists on a single hardware system, physical damage to that hardware can result in permanently lost data.

Malicious actors

Malicious actors with intent to conduct cyber-attacks may use various methods to hack and manipulate, surveil, or extract data. Attackers may attempt to shut down systems entirely, preventing access. This is often done through a Distributed Denial of Service (DDoS) attack. There are also insider threats, meaning someone with authorized access to data may intend to use or alter it for malicious purposes.

BLOCKCHAIN APPLICATIONS: STRENGTH IN CYBERSECURITY

What is blockchain technology?

A blockchain is a distributed ledger system that is structured to effectively secure data.

Current applications

Blockchain is currently and most popularly used for cryptocurrencies. Other applications include storing health records and mobile, digital voting. The cryptocurrency Bitcoin popularized blockchain technology while Ethereum introduced new applications other than currency transactions[18]. Blockchain use in electronic health records is being intensely researched and developed, with blockchain-based products already existing. A medical blockchain would store and secure personal data[19]. In the U.S. and abroad, the technology is being applied to electoral voting. For example, West Virginia introduced a blockchain-based mobile voting application for active-duty military service members[20].

18. Explainer: What is a Blockchain? MIT Technology Review, 2018. https://www.technologyreview.com/s/610833/explainer-what-is-a-blockchain/

19. The Potential for Blockchain to Transform Electronic Health Records. Harvard Business Review, 2017. https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records

20. West Virginia tests secure mobile voting app for military personnel. The Hill, March 28, 2018. http://thehill.com/policy/cybersecurity/380690-west-virginia-tests-secure-mobile-voting-app-for-military-personnel

Architecture of the technology

There are three core components that make up a blockchain: the data in the block, its "hash", and the hash of the previous block. The created blockchain is stored on a decentralized network comprised of nodes and links.

Data

The data stored in this technology is secured in a block. The block is open for data addition and alteration until validated and closed. The block's content is time stamped and the block is given a unique identification code, or hash. Neither the block, nor its contents, nor the blocks' order may be adjusted once sealed, at risk of breaking the blockchain.

Hash

The hash is a specific code that gives each block a unique identifier, like a fingerprint. "Hashing" is a method of calculating a relatively unique fixed-size output hash for an input of nearly any size or any data type. This method works one-way. It is preimage resistant; mapping to a predetermined output is infeasible[21]. It is also computationally infeasible to find two or more inputs that produce the same output, making hashing collision resistant. Hash stability can show if a block's contents has been recently changed, solidifying trust in the block's history.

Hash of previous block

The following block contains the hash of the previous block. This is the component that creates a chain for security; changing one block will render the following blocks invalid. Since changing a block changes its hash, altering a block will break the chain. Proof of work slows the creation of new blocks. All new and adjusted blocks must be verified by consensus. Tampering with one means recalculating proof of work for following blocks in order to keep the chain. This process is computationally less resource intensive than rehashing an entire set of data each time an edit is made[22].

Nodes and links: A "node" is any individual system within the blockchain. This may include a system used to "mine", or create, blocks, or to store and view the blockchain. Every node is linked and connected to an overall network. This peer-to-peer network allows various computers, or nodes, to connect directly with each other without a central authority[23].

21. Blockchain Technology Overview. NIST, 2018. https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

22. Beyond Bitcoin: Emerging Applications for Blockchain Technology. Congressional Research Service, 2018. https://docs.house.gov/meetings/SY/SY21/20180214/106862/HHRG-115-SY21-Wstate-JaikaranC-20180214.pdf

23. Beyond Bitcoin: Emerging Applications for Blockchain Technology. Congressional Research Service, 2018. https://docs.house.gov/meetings/SY/SY21/20180214/106862/HHRG-115-SY21-Wstate-JaikaranC-20180214.pdf

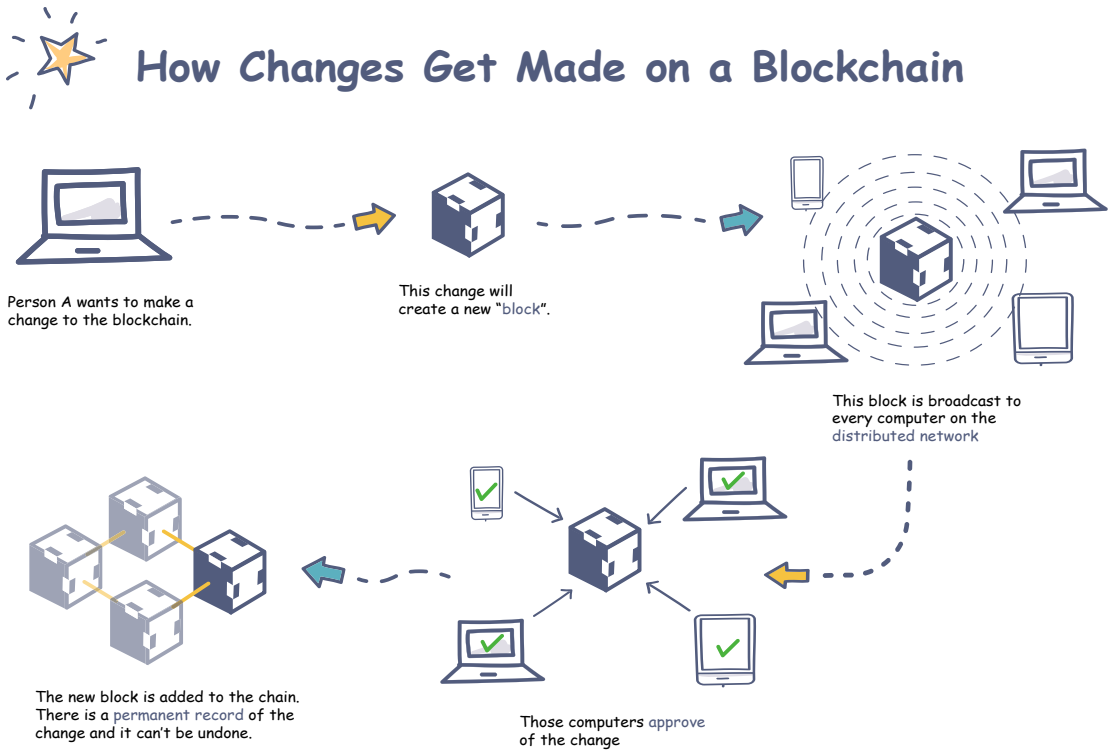


Figure 2: Changing a blockchain[24]

Centralized, Decentralized, Distributed systems

By nature of the peer-to-peer network, the overall system is distributed.

Figure 3: Centralized, Decentralized, and Distributed Networks[25]

24. Here's everything you need to know about blockchains, the ground-breaking tech that could be as disruptive as the internet. Business Insider, 2017. https://www.businessinsider.com/what-is-blockchain-how-does-it-work-explainer-2017-11
25. Decentralized? What does that really mean? Wall Street Technologist, 2015. http://www.wallstreettechnologist.com/2015/06/26/decentralized-what-does-that-really-mean/

This is different from a standard centralized system where all participatory systems are connected through a central server or operational authority. A centralized system is most vulnerable and easy to take down at its focal point: the center. This is different from a decentralized system, where there are multiple centralized systems that are connected together. Each center point in a decentralized system is vulnerable, but the overall system is difficult to take down. A distributed system links all individual systems with no central point. This makes it difficult to bring down the system (i.e. DDoS attacks) and reduces risk of permanently losing critical data.

Public and private blockchains

Data within the block may be public-access or permission-based. On a public system, all nodes may openly view each block's contents. However, it is extremely difficult to change those contents and impossible to do so without breaking the chain. This system is open to participation without users requesting access and is best used for public-facing data. On a private system, the blockchain is permissioned and user access is restricted[26].

Cryptography

Cryptography links blocks together and ensures records can't be changed or counterfeited. It confirms user identity and protects sensitive data, reinforcing trust in the technology. This takes form in hashing, data encryption, and user keys. Cryptography is a common and valuable tool in cybersecurity.

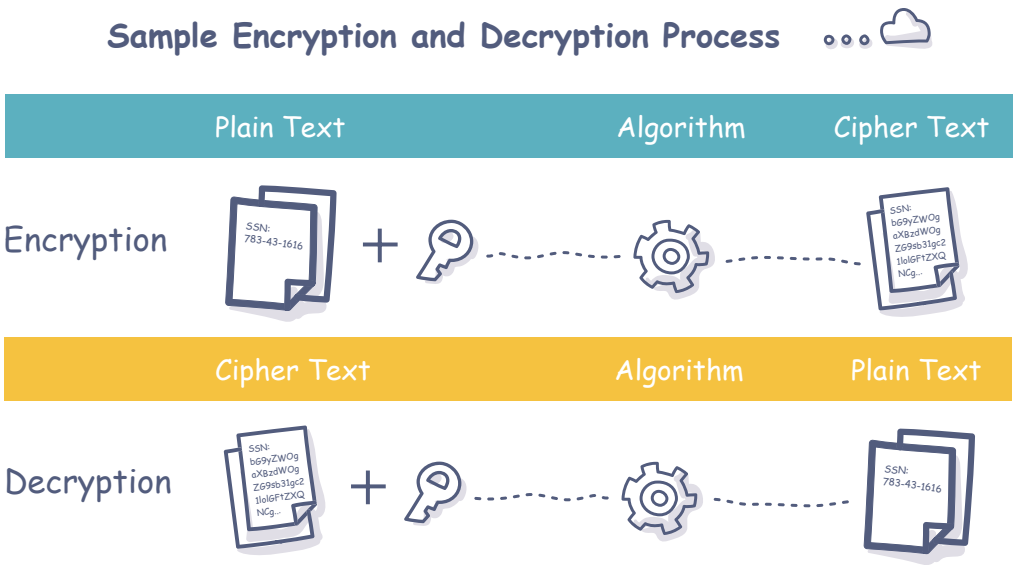


Figure 4: Encryption visualization[27]

26. Blockchain Technology Overview. NIST, 2018. https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

27. Encryption. Middlebury, 2017. https://mediawiki.middlebury.edu/wiki/LIS/Encryption

Encryption

Encryption is a tool for both public and private system to mask and protect sensitive information, especially identity systems (identity documents, biometric test results, health data, etc.)[28]. It encodes or scrambles information, making content unreadable and inaccessible unless unlocked with the proper key. As long as this key is protected, encryption is highly effective at protecting data from outside viewers[29]. It can be applied to data in a block for privacy protection.

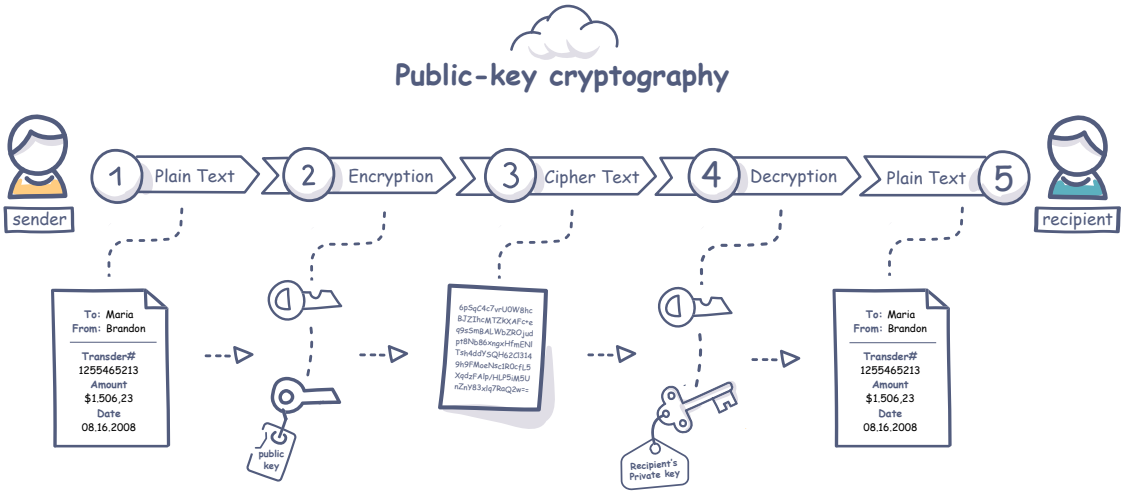


Figure 5: Public and private key cryptography[30]

Public key cryptography and asymmetric key encryption: Key encryption on the blockchain creates identities and authenticates users. The asymmetric key system requires public and private keys that must be used together and function as a signature. The public key identifies the user and verifies that user's resources. The private key locks data[31]. A compound identity guarantees that only a small fraction of the data is compromised in the event of an adversary obtaining both the signing and encryption keys. If the adversary obtains only one of the keys, then the data is still safe[32].

28. Blockchain Could Help Us Reclaim Control of Our Personal Data. Harvard Business Review, 2017. https://hbr.org/2017/10/smart-ledgers-can-help-us-reclaim-control-of-our-personal-data
29. Cyber Security Planning Guide. Federal Communications Commission, 2012. https://www.fcc.gov/cyber/cyberplanner.pdf
30. Cryptography. Lisk, 2018. https://lisk.io/academy/blockchain-basics/how-does-blockchain-work/blockchain-cryptography-explained
31. Beyond Bitcoin: Emerging Applications for Blockchain Technology. Congressional Research Service, 2018. https://docs.house.gov/meetings/SY/SY21/20180214/106862/HHRG-115-SY21-Wstate-JaikaranC-20180214.pdf
32. Decentralizing Privacy: Using Blockchain to Protect Personal Data. IEEE, 2015. https://ieeexplore.ieee.org/document/7163223/

CONSIDERATIONS FOR IMPLEMENTATION IN THE HUMANITARIAN SECTOR

Resources and efficiency

In order to function at large capacities, the blockchain uses a high level of electricity and long time periods, especially for generating a new node that must download the entire blockchain[33]. The cryptocurrency Bitcoin has used as much electricity annually as Nigeria[34]. Moving data also requires adequate storage space on every node. However, smaller-scale blockchains would use significantly less energy; fewer nodes and less mining would be less taxing. Developing countries or regions where electricity is expensive or scarce should consider electricity consumption, but solutions to consume less electricity are being developed[35]. Furthermore, validating and sealing blocks can take a long time to process, due to complexity[36].

Hard to track identity of users

Although blockchain access may be traced to a node and asymmetric keys authenticate users, these access points do not necessarily trace to a specific identity. A key may be linked to a real-world identity, or to a pseudonymous identity[37]. Should there be an attacker under a pseudonymous identity, that attacker would be difficult to pinpoint.

Threat of malicious actors on the blockchain

There are few cybersecurity threats to blockchain technology, but they must also be taken into consideration. An existing node required to validate a block may ignore validation, refuse to transmit data, or create a secret alternative chain to corrupt the existing chain[38]. Another potential threat is the

33. Blockchain Technology Overview. NIST, 2018. https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf
34. Blockchains Use Massive Amounts of Energy—But There's a Plan to Fix That. MIT Technology Review, 2017. https://www.technologyreview.com/s/609480/bitcoin-uses-massive-amounts-of-energybut-theres-a-plan-to-fix-it/
35. Blockchains Use Massive Amounts of Energy—But There's a Plan to Fix That. MIT Technology Review, 2017. https://www.technologyreview.com/s/609480/bitcoin-uses-massive-amounts-of-energybut-theres-a-plan-to-fix-it/
36. The 5 Big Problems With Blockchain Everyone Should Be Aware Of. Forbes, 2018. https://www.forbes.com/sites/bernardmarr/2018/02/19/the-5-big-problems-with-blockchain-everyone-should-be-aware-of/
37. Beyond Bitcoin: Emerging Applications for Blockchain Technology. Congressional Research Service, 2018. https://docs.house.gov/meetings/SY/SY21/20180214/106862/HHRG-115-SY21-Wstate-JaikaranC-20180214.pdf
38. Blockchain Technology Overview. NIST, 2018. https://csrc.nist.gov/CSRC/media/Publications/nistir/8202/draft/documents/nistir8202-draft.pdf

"51% attack". Although run on a distributed system, on a public and permissionless network, attackers may enter a network and multiply until the majority of network participants are under the attacker's control (for permissionless networks)[39]. With the majority of the blocks, an attacker may compromise the system. However, this may be mitigated with permissions.

Individual system vulnerability

Each node, or individual system on the network that stores the blockchain and touches sensitive data, must be secure; if a device used to secure the system is vulnerable, later actions may be vulnerable. Unauthorized access to personal keys, passwords, and nodes presents risk. However, blockchain is particularly strong against unauthorized modification of past records. If hacking occurs, a "fork" can upgrade the blockchain to move in a new direction, essentially undoing mistakes while keeping records[40].

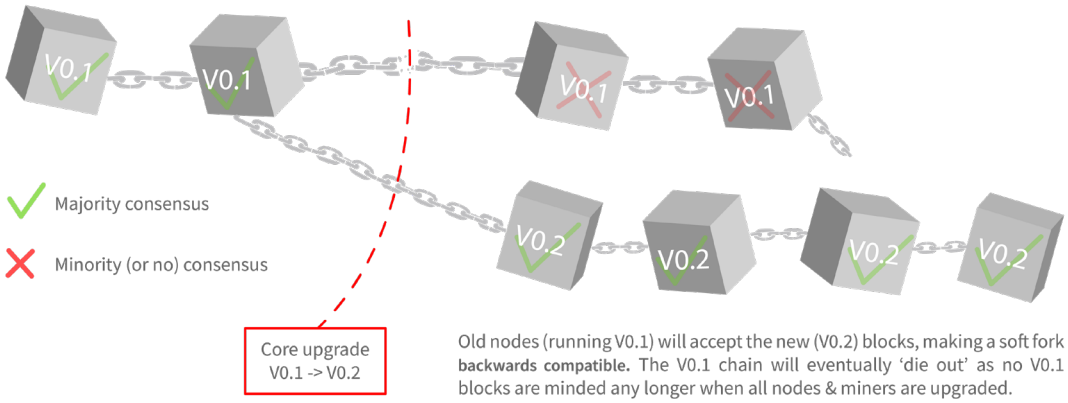


Figure 6: Forking to undo[41]

Public perception and user knowledge of the technology

The ability to mine and maintain Blockchain's large association with finance contributes to lack of awareness in other sectors. Blockchain is still a relatively new technology and its use is not yet mainstream. Worldwide, only 1% of Chief Information Officers (CIOs) from organizations across sectors reported investing in and deploying blockchain. Some may perceive it as an immature technology; 77% of CIOs surveyed reported no interest in or plan of action to implement blockchain[42]. Its popular

39. Distributed Ledger Technology (DLT) and Blockchain. World Bank, 2017. http://documents.worldbank.org/curated/en/177911513714062215/pdf/122140-WP-PUBLIC-Distributed-Ledger-Technology-and-Blockchain-Fintech-Notes.pdf
40. Hard Fork. Investopedia, 2018. https://www.investopedia.com/terms/h/hard-fork.asp
41. Hard and Soft Forks. Cryptographics, 2018. https://cryptographics.info/cryptographics/blockchain/hard-soft-forks/
42. Gartner Survey Reveals the Scarcity of Current Blockchain Deployments. Gartner, 2018. https://www.gartner.com/newsroom/id/3873790

connection to cryptocurrencies like Bitcoin may arise associations with finance, or cryptocurrencies' associations with illegal activities like money laundering or black-market trade[43]. In order for an organization to manage the system, it must have the appropriate personnel or personnel trained on the technology.

Legality

Although blockchain is tamper-proof and can be encrypted and permissioned for security, these aspects of the technologies may conflict with data protection laws, such as the 2014 European Court of Justice's ruling that EU citizens may be removed, or de-indexed, from undesirable information collected on them. Integrated in the EU's General Data Protection Regulation (GDPR) as the "right to be forgotten"[44], erasing personal data may be difficult if it is locked into a blockchain. However, it may be permanently encrypted and made inaccessible.

Financial cost to implement

Adopting blockchain technology requires specific software and may require specialized hardware. In addition, the organization implementing blockchain must ensure qualified personnel are working with the technology, who are often eligible for competitive salaries.

Political will to implement and bureaucratic considerations

Political will to implement a new technology requires the understanding of the aforementioned considerations and appropriate bureaucratic procedures. This includes training personnel or hiring personnel familiar with mining and contributing to a blockchain, identifying and transferring all relevant data, shifting all past data storage processes, and amending past cybersecurity protocol. This may mean integrating, or even overhauling an existing system. Bureaucratic considerations include the time to transfer data and entirely switch to a new technology, as well as the size of the blockchain network and how capable each relevant party is of contributing. All relevant parties must also be on the same blockchain, being careful to avoid multiple chains among different but relevant parties[45]. This means addressing existing culture within or among parties and factoring in accessibility and the potential for unequal access, due to resource or bureaucratic constraints.

---

43. Five Challenges Blockchain Must Overcome Before Mainstream Adoption. Forbes, 2018. https://www.nasdaq.com/article/five-challenges-blockchain-technology-must-overcome-before-mainstream-adoption-cm899472

44. Blockchain from a perspective of data protection law. Deloitte, 2018. https://www2.deloitte.com/dl/en/pages/legal/articles/blockchain-datenschutzrecht.html

45. Blockchain: Enigma. Paradox. Opportunity. Deloitte, 2016. https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/Innovation/deloitte-uk-blockchain-full-report.pdf

CONCLUSION

The humanitarian sector relies on information to implement a strategic and targeted response. The people, communities, and environments involved in humanitarianism expect and rely on data protection and security. Blockchain, as an emerging technology, presents solutions to existing cyber threats and could afford more security around sensitive humanitarian-related data. Although implementation considerations will vary by agency, humanitarian organizations should be dedicating resources to better understand the possibilities and be scanning for potential small or trial use cases. The affected people that we help deserve our best and if Blockchain can provide that, we should take the option seriously.