Digital Society (2022) 1: 4
https://doi.org/10.1007/s44206-022-00007-1

ORIGINAL PAPER

Leveraging Blockchain-Based Archival Solutions for Sensitive Documentation: a Xinjiang Case Study

Remy Hellstern[1] · Daniel C. Park[1] · Victoria Lemieux[1] · Guldana Salimjan[1]

Received: 3 January 2022 / Accepted: 26 June 2022 / Published online: 18 July 2022

Abstract

This exploratory research surveys scholarly literature on decentralized storage solutions, including theories and works of archival science, and similar applications in humanitarian contexts, to illustrate the necessity of these systems in Xinjiang Uyghur Autonomous Region in China. Xinjiang has recently shifted into the spotlight of the international press for allegations of abuse and forced labor, coercive cultural assimilation, and the creation of a police state. The leadership of the People's Republic of China (PRC) justifies the existence of these training facilities and expansive surveillance networks as part of the PRC-backed efforts to de-radicalize ethnic groups in the region. However, many governments and scholars rebuke these justifications, arguing that these centers are state-run facilities that house extrajudicially detained individuals based on their ethnic identity and religious belief. This paper aims at limiting the plausible deniability of violations conducive to cultural genocide, thus improving the prospects for deterrence and accountability through decentralized evidence management. The technological sophistication of the regime in Xinjiang is outpacing centralized systems and rendering storage solutions hosting evidence of these violations obsolete. This jeopardizes the prospect of truth and reconciliation in the future and allows the party to craft and disseminate their narrative globally with little resistance. Major findings focus on how decentralized systems can improve the streamlining and hosting of evidence regarding human rights violations occurring as well as advancing the study of cryptographic management of evidence regarding the treatment of vulnerable communities in low-rights regions.

Keywords Xinjiang · Decentralized ledger technologies · Blockchain · Human rights

✉ Remy Hellstern
remyhellstern@gmail.com

Daniel C. Park
025dpark@gmail.com

Victoria Lemieux
v.lemieux@ubc.ca

Guldana Salimjan
salimjan_guldana@sfu.ca

[1] The University of British Columbia, Vancouver, Canada

1 Introduction

Xinjiang is home to an amalgamation of cultures due to its strategically important location as well as a rich history of Turkic-speaking indigenous populations like Uyghurs, Kazakhs, Uzbeks, and Kyrgyz. From the establishment of the People's Republic of China (PRC) in 1949 to the official formation of the Xinjiang Uyghur Autonomous Region in 1955, the Chinese government tightened its control to secure Xinjiang as a resource reserve for developing the national economy. This has exacerbated tension between Han settlers and native groups who were given the "minority" status. The region shares borders with an array of countries including Mongolia, Russia, Kazakhstan, Kyrgyzstan, Tajikistan, Afghanistan, Pakistan, and India, as well as the Tibet Autonomous Region in China. Many of the indigenous groups in Xinjiang have a strong diaspora in these neighboring countries and regions which has been a cause for concern for China which fears the dissonance of national identity in the border regions.

1.1 Xinjiang as a Settler Colony

While deemed an ethnic minority group in Xinjiang by the PRC, many Uyghurs view themselves as the indigenous people of the region. Historically Xinjiang is home to over 15 million people of various ethnic lineages. This misalignment of thought creates an inherent tension between the Uyghurs and Han settler populations as they struggle for self-determination and assimilation (Unrepresented Nations & Peoples Organization, 2015). Organizations, like the Uyghur Human Rights Group, argue that while China is a signatory of the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP), they continually violate that agreement in their treatment of Uyghurs and other non-Han groups (UN Department of Economic and Social Affairs, 2007). In The *Hanification of Xinjiang, China: The Economic Effects of the Great Leap West*, Amy Liu examines the relationship between PRC leadership in Beijing and the Uyghur people in Xinjiang during the Great Leap West. This project began in the late 1990s as an economic initiative to open up the Northwestern region of China and better integrate Uyghurs into the economy (Liu & Peters, 2017). Liu points out the disconnect between the two groups as the PRC deemed the Great Leap West as a success in land and economic development, whereas the native population experienced negative consequences and economic dispossession due to these state-led projects.

These developments have attracted much scrutiny from the international community with the ongoing and active measures to displace and dispossess indigenous populations from their traditional homelands (Byler, 2021; Cliff, 2016; Guerif, 2010; Salimjan, 2021a, b; Millward & Peterson, 2020; Roberts, 2021; Ruser et al., 2020). To fulfill the newly created and numerous economic projects and job opportunities in this region, the PRC incentivized Han citizens to move to the Northwest region of China (Yi, 2019). Over time this began to rearrange and change the demographics of Xinjiang, making the region more ethnically fragmented and divided.

Due to the rich natural resources and geographic location of Xinjiang, exercising total control over the region carries enormous strategic and economic importance. Xinjiang is seen as the economic gateway to Central Asia because of its proximity to other nations. Michael Clarke contextualizes this conflict through the lens of colonialism in his article, *China's Internal Security Dilemma and the 'Great Western Development.'* He argues that the Great Leap West changed how the state interacted with and approached non-Han groups. Clark notes how the Great Leap West borrows from nation-building perspectives and emphasizes "the themes of 'manifest destiny'; the civilizing imperative; [and] the rich resources lying untapped… [for] the Chinese nation's exploitation" (Clarke, 2007:329). Through this perspective China is reclaiming land that was destined for them, mirroring similar strategies of other colonial powers, like that of the American manifest destiny, which was used to dispossess indigenous populations from their traditional homelands. This claim to land traditionally inhabited by indigenous populations unpins the theory of settler colonialism. In *Settler Colonialism and Elimination of the Native*, Patrick Wolfe argues that access to territory is a "specific, irreducible element" of modern-day colonialism (Wolfe, 2006:388).

Development projects and aid within this region are often viewed as inherently colonial and will lead to the expropriation of indigenous land. With the migration of Han settlers into the region and the removal of cultural heritage sites for the sake of development, relations are tense. Researchers at the Xinjiang Data Project argue that development in the region is being used as a facade for cultural erasure and desecration of religious sites. The group found that one in every three mosques in Xinjiang has been demolished since 2017 (Ruser et al., 2020). For local populations, these development projects uproot their traditional homeland and disrupt their cultural and social reproductions.

2 Technological Components of State Surveillance

The non-Han people in Xinjiang face the prevailing threat of intense technological surveillance daily. As one of the most technologically sophisticated countries in the world, China has strategically positioned itself to be able to monitor and surveil all citizens living within its territory. The PRC has continually invested in the development and deployment of its surveillance infrastructure, funding tech companies like Hikvision and Dahua with million-dollar contracts (Rollet, 2018). This is manifested on the ground in towns like Sanmenxia in Henan province, which used facial recognition over 500,000 times in 1 month on its residents to determine who was Uyghur (Mozur, 2019). As of May, 2021, out of the 770 million CCTV cameras in the world, 54% of those cameras are located in China (Bischoff, 2021). This situates non-Han citizens in a massive surveillance network that tracks their actions and movements. This surveillance permeates China's digital sphere as well, and with the help of communication firms in the West, China's Internet has been carefully curated since the 1990s.

2.1 The Great Firewall

The "Great Firewall of China" was not established overnight, first coined in 1997, Chinese leadership had steep concerns about exposing Chinese citizens to uncensored and vast amounts of information available through this new system of technology (Barme & Ye, 1997). The Internet first arrived in China in 1994 as an extension of the country's 1979 "Open Door Policy," connecting the world's most populous nation with the West and their conglomerates for new economic partnerships (*The Great Firewall of China* Tofox A Stanford Project, 2011). Under the presidency of Jiang Zemin, several institutions were erected to intervene in balancing citizens' exposure to the West while preserving its party ideology against the backdrop of the rapidly globalizing Internet (Sechenova, 2014). Subsequently, in 1997, the Chinese government enacted the legislation "Interim Regulation of the People's Republic of China on the Management of International Networking of Computer Information," affirming its intent to censor the world wide web through regulatory means (ibid.). In 2000, the legislation evolved into what is known as the "Golden Shield Project," establishing a web censorship regime within the Ministry of Public Security to control the cyber activity of Chinese citizens by imposing various controls over Internet Service Providers (ISPs).

Since then, the Ministry has adjusted its censorship methodologies, tailoring the Great Firewall to new domestic and international technological developments (ibid.). In retrospect, the incredible feat of creating cyberspace tailored for a domestic clientele and insulated from the rest of the world can be attributed to US telecommunication conglomerates, particularly Cisco and Sprint. In the early 1990s, Cisco had begun supplying word filtering and surveillance equipment to the Chinese censorship regime that had once been marketed to private companies for monitoring office employees' internet activities. Sprint also was contracted by China Telecom to build the country's first commercial internet, creating what would become ChinaNet (Griffiths, 2021a).

Systematically, the Great Firewall is curated in a top-down fashion. The censorship regime rigorously scans cyberspace, with automated systems, for keywords and expressions that are considered seditious or inflammatory to the party's values, blocking content on blogs or messages on chat applications containing flagged terms (Feng & Guo, 2013). Specific pages and entire websites are also blocked, including Wikipedia, Facebook, and Google. At the consumer level, when a user in China tries to load a webpage, its respective ISP pings a list of forbidden URLs and types of content. If the page is not banned, the request is forwarded to an internet access point (IAP), which is responsible for routing traffic to servers across China and around the world (Griffiths, 2021a). Connection to the global Internet in China is channeled through a government-controlled gateway, which is strictly and exclusively controlled by six state-owned Internet operators. Whereas, in most democracies, many individual ISPs sustain separate IAPs to the global Internet (Feng & Guo, 2013).

Even if the page is not banned, a packet inspection takes place nonetheless, scouting for keywords and suspicious flags. When the destination server forwards the webpage data back to the user, it is inspected once more. A web page must undergo such checkpoints to successfully load for consumers. Notably, in 1999, the assembly of 10,000 Falun Gong practitioners in Beijing protested for the release of their peers arrested in Tianjin. This in turn catalyzed the early censorship regime to scrub all positive references to Falun Gong off the web (Griffiths, 2021b). Studies of the Great Firewall suggest terms and websites associated with Falun Gong were among the most filtered, so much so that the group had become a baseline measure of censorship for academics in the West. The anti-Falun Gong campaign has captured success globally, with foreign media repeating party lines, and Falun Gong practitioners dismissed as cultish and credulous (ibid.).

Using proxies and other sophisticated means like virtual private networks (VPNs), individuals can bypass such checkpoints. While there are successful commercialized examples, it is far from avoiding the censors entirely. Even in instances where the Firewall fails to block a user from visiting a flagged website, their access could be throttled to the point of unusability and they could even invite a face-to-face follow-up by security agents, particularly at times of heightened political sensitivity (ibid.). In addition to in-person follow-ups, dataveillance tools can now detect the use of VPNs and other encrypted applications like WhatsApp and Signal (Kuo, 2021). While these services are options for some, for those living in Xinjiang, using a VPN or WhatsApp on their phone can be grounds for re-education. Often, these tools used to circumvent the Great Firewall can have larger societal and legal implications, especially in politically sensitive regions.

2.2 Securitization of Xinjiang

While at a national level the Great Firewall blocks and restrains access to a free web, restrictions on individual citizens go even further. Unable to openly speak about living conditions and the state of surveillance at a regional level, individuals are left with few options to fight back against increasing security. Central to the rise of the police state in Xinjiang is the extensive surveillance network that relies on the collection of biometric data. Through the establishment of CCTV cameras and police convenience stops, moving through Xinjiang undetected is nearly impossible (Chin & Bürge, 2017; Leibold, 2019). According to researchers at the Human Rights Watch, QR codes on the doors of households have become commonplace, allowing local police to know the number of residents in each establishment as well as the demographic information of the home through population collection forms (Wang, 2018).

In 2016, after the ushering in of Chen Quanguo as Communist Party Secretary of Xinjiang, surveillance in the region escalated. After 5 years of working in Tibet to ensure stability and government control within the region, Quanguo was transferred to Xinjiang to erect a similar surveillance system. In this 2017 critique of the PRC's securitization of Xinjiang, Adrian Zenz describes their strategy as borrowed directly (Zenz, 2017: paragraph 3):

> *"from the imperial playbook, with past colonial powers like England and Japan enlisting 'native' populations to watch over their own people. Ethnic minorities have long served the CCP in China. However, the numbers of*

> *Uyghurs and Tibetans that have been recruited into China's security… [is] potentially setting a historic record."*

This strategy of indigenous populations policing their community members perpetuates mistrust among communities and aids in creating an "us versus them" mentality (Qu, 2021). One side is that of the PRC and the other is the remaining underrepresented populations, a key facet in the surveillance system established within Xinjiang. This point is also emphasized in Darren Byler's article, *The Xinjiang Data Police*. Byler follows the story of Baimurat, a Kazakh man living in Xinjiang who was recruited to work as an assistant police officer by the local Public Secretary Bureau. At his new job, Bairmurat was assigned to monitor Uyghur and Kazakh community members from behind a computer screen. Positions like these are what Byler refers to as data police, young low-wage workers that maintain and program systems such as the "counterterrorism swords" to monitor the targeted populations of Xinjiang (Byler, 2020). These are specific devices that are used to scan phones. The data police determine who should have their phones scanned, effectively sorting the population at face-scan and ID checkpoints. By strategically focusing on indigenous populations for data collection, the settler population is not inconvenienced by such systems (ibid.). Systems like these encourage young people to take up jobs within the surveillance economy while not being aware of what they are working on.

Against this backdrop, surveillance technology is becoming more sophisticated. During the 2017 International Conference on Machine Vision and Information Technology in Singapore, researchers from Xinjiang University introduced a new facial recognition database they had been developing. *XJU1: A Chinese Ethnic Minorities Face Database.* Researchers Zuo, Wang, and Qin outline the process used to create a facial recognition database and the ability to differentiate between different ethnic groups in the Xinjiang region. The researchers throughout the paper highlight that the database was created with the expressed interest to identify Uyghur and Kazakh faces. The most effective algorithm was able to identify ethnic minority faces 93% of the time (Zuo et al., 2017). Technological development like this demonstrates the strategic importance of Xinjiang and highlights increasing efforts to monitor the local population. In a 2019 article in *Nature*, Yves Moreau focuses on the insidious nature of these programs and how with the help of facial recognition software, governments are more effective than ever at identifying minority groups. His focus is on the collection of biometric information including but not limited to genetic testing, DNA collection, retina scanning, and more. According to his research, Moreau notes that "Uyghurs and Tibetans are 30–40 times more frequently studied than are people from Han communities, relative to the size of their populations" (Moreau, 2019:38). However, the observation and study of these communities extend overseas as well, subjecting people of Turkic communities originally from Xinjiang to a similar surveillance regime.

2.3 Pressures on the Turkic Community Abroad

In 2017, Xinjiang came into focus from an array of media outlets for the creation and proliferation of the re-education system. In these vocational training and re-education centers, non-Han populations were moved en masse to what some have described as prison-like systems (Killing et al., 2020). To subvert access and narratives condemning the extrajudicial detentions in Xinjiang on the international stage, Chinese authorities have been active overseas using their economic and diplomatic leverage to detain and extradite foreign nationals of Uyghur descent. This pressure mounted as Chinese authorities began confiscating passports and requiring all residents to submit DNA samples and other biological data when applying for travel visas. Permission, thus, must be granted to residents of Xinjiang if they plan on leaving the country (BBC, 2016).

Individuals who left Xinjiang before the crackdown still live in fear of retaliation against themselves or their families. In 2020, when speaking to Middle East Eye, Hemdullah Abduweli, an Uyghur Muslim religious scholar who had arrived in Saudi Arabia to perform a religious pilgrimage, feared that Chinese authorities had sent a request to government officials to detain and deport him (Ullah, 2020). He, along with his friend Nurmemet Rozi, was arrested at Mecca subsequently and were held in Jeddah's Bureiman prison. Later Abduweli shared that he "feared for his life" and worried that he would be deported. The two men are Chinese nationals, but residents of Turkey (Human Rights Watch, 2020). In the same year, Beijing ratified an extradition deal signed with officials in Ankara, in rhetoric, to bolster counterterrorism efforts abroad. Animating the development, Beijing had allegedly marked the deal as a precondition for the shipment of COVID-19 vaccines to Turkey (Ayasun, 2021). Turkey is home to some 50,000 Uyghurs, many of whom are still PRC citizens and are yet to hold Turkish citizenship. These individuals are most vulnerable under the new treaty; and while very few have been deported, Turkish police have held around 50 Uyghurs at deportation centers (Kang & Fraser, 2021).

Coercion against Uyghurs is not limited to China and Muslim countries with an Uyghur diaspora. In 2017, Dokun Isa, a German citizen and a leader of the World Uyghur Congress, was arrested in Italy for an "identity check." His name had appeared on Interpol's list of "red notices," exhibiting suspects wanted by police bodies of other Interpol members (Reuters, 2018). According to a 2020 Amnesty Canada report, intimidation against Canadians of Tibetan and Uyghur descent and activists affiliated with political movements in Hong Kong and Taiwan are on the rise in the country. This intimidation often manifests in the forms of cyberbullying, death threats, and racist insults as a response to content deemed to be against China's status quo. Many cases of this harassment can be traced, either directly or indirectly, to Chinese state actors (Amnesty International Canada, 2020).

3 Storing Evidence of Human Rights Violations

As the ongoing human rights crisis against indigenous populations in China is becoming more technologically sophisticated and ever present, traditional ways of holding the government accountable are vulnerable to attacks. Whether living in Xinjiang or abroad, non-Han groups live in fear of extrajudicial detention of either themselves or their family. Due to the innovation and massive investment in surveillance technologies within Xinjiang, conventional ways of storing documentation used by activist groups and others to capture evidence of human rights violations, reliant upon centralized storage and authority, are under threat. However, with the rise of new ways of storing and securing data, there is room for creativity in the new technological solutions being used to fight injustices.

Many activist groups, think tanks, and academic organizations are trying to gather counter-evidence that shows the human rights abuses that are happening. Groups like the Xinjiang Victim's Database and Atajurt Human Rights Group, for example, organize, store, and maintain records of extrajudicial detentions, court records, testimonial videos, and personal records of individuals detained by the state. This is vital because, without the work of their documentation project, many of these records would be lost, destroyed, and/or manipulated. However, it is often the case that these groups do not have the infrastructure in place to capture, organize, and store this material for the long term as authentic evidence of abuses. This evidence is often vital to countering the state-sanctioned narratives that dominate media and legal systems. However, maintaining all of these valuable records on one computer or server can leave them vulnerable to attacks because of the centralized nature of this information (see for example, Gutnikov et al., 2022). Further, these attacks can lead to data leakage that allows for the continuation of abuses of individuals from targeted populations.

3.1 Importance of Information Storage

These challenges are not unique to Xinjiang alone. Many groups struggle to securely amass and store information related to government abuses and human rights violations (Lyngaas, 2022). This is especially difficult when those in power are seeking to prevent any related documentation of such violations from coming to light. When human rights violations happen, it is vital for all voices of the conflict to be heard. By proposing the exploration of decentralized solutions for documentation of such human rights crises, it is possible to diffuse the power of information over a democratized system. This need for democratized access to information is also key to combating misinformation around conflicts.

Disinformation campaigns are incredibly common, as governments committing human rights violations desperately seek to control the framing and narrative surrounding the conflict. In *Master Narratives of Disinformation Campaigns*, Matthew Levinger outlines how the Russian government and state actors purposely fabricated news stories about the White Helmets, a humanitarian group working in Syria, and their alleged connections between terrorist attacks and organizations. Levinger argues that because the Russian government was able to control the master narrative surrounding the Syrian conflict and effectively dominate the online conversation through gaming social media algorithms, bots, and agitators, they effectively overwhelmed readers, leaving them confused about the "truth" (Levinger, 2007). However, no credible links have been found between the White Helmets and any terrorist activity (Hadjimatheou, 2021). This creates a dangerous precedent in which the groups with the most computing power are able to dictate what the truth is and how history unfolds. Campaigns of silence and eradication are dangerous, but common, leaving communities in dire conditions.

The following section will outline the key differences between traditional centralized systems and decentralized distributed ledgers. Highlighting the structural differences between both systems will provide a deeper understanding of how decentralized systems can empower users. Such systems enable information that is added to be viewed and agreed upon by peers before being uploaded and stored. As technology advances, means of storing and securing data in the long term are also changing. This is made increasingly difficult in areas where those in power are suppressing information. Emerging systems, like decentralized ledgers, provide an opportunity to pilot solutions working to tackle problems around government censorship and information control.

4 Centralized Systems vs. Decentralized and Distributed Ledgers

Centralized systems are the most common type of system used by activist groups to store evidence and are often what most people think of when discussing traditional archival systems. Centralized systems, albeit easier to develop and implement due to being the responsibility of a sole authority, have a single point of failure making them vulnerable to attack while also having low scalability. Further, when all of the original data is only stored in one location, it becomes more vulnerable to bad actors. Having a single point of failure makes it easier for attacks to corrupt or shut down the system because attackers only need to target one point in the system to access all of the files or bring a system down completely. Low scalability also is challenging for long-run preservation of evidence because, as projects grow and start to accrue more information, they need the flexibility to easily scale upward. Centralization therefore presents challenges to long term high-volume storage of authoritative evidence (Truong et al., 2016).

Centralized systems work well for the dominant narrative; however, it becomes the ubiquitous, default voice. This disadvantages dissenting voices, offering evidence of oppression. The ability to safely store and archive evidence of injustice is vital to movements. Gathering and securely storing evidence is the only way to hold the perpetrators accountable and move toward future efforts of truth and reconciliation. However, it is becoming clearer that traditional systems are failing to support minority groups because of the political and technological sophistication of state actors.

Attacks on centralized systems are not new. In 2020, the European Medicine Agency faced a cyber attack in which the perpetrators tried to undermine community trust in vaccines (European Medicines Agency, 2021). Recently, the International Committee of the Red Cross (ICRC) suffered a data breach of over 500,000 individual records from its global Red Cross and Red Crescent Movement's Restoring Family Links services (Greig, 2022). This breach resulted in an extreme violation of the privacy, safety, and right to receive humanitarian protection and assistance for vulnerable people.

The Xinjiang Victim's Database has struggled to maintain secure records on its online platform (Rickleton, 2021). When it comes to organizations and groups sharing information online about the ongoing crisis in Xinjiang, it is not uncommon for them to face backlash from the PRC government. Activist organization Uyghur Human Rights Group has faced a variety of attacks on its platform (Meaker, 2019). Attacks like these emphasize the need for more secure systems, especially while storing sensitive material like testimonies, court records, video footage, and other personally identifiable and sensitive information.

With the advent of innovations like blockchain and distributed ledger technology, groups are discovering they no longer need to rely on these systems that are failing them. These new forms of record-keeping offer decentralized, distributed systems that use cryptography and decentralization to hold records as immutable and protect them from attack. These innovations provide individuals with the ability to defend the documentation they hold regarding human rights abuses against manipulation and deletion. Figure 1 shows the structural differences among centralized, decentralized, and distributed systems. It is often the case that blockchain and distributed ledger technology use both a decentralized and distributed network control to safely store information.

Decentralized and distributed systems offer a fundamental shift from centralized systems in many ways but most notably the lack of a single central authority controlling the information. Instead of one data controller, these networks allow all nodes on the system equal access to a publicly available ledger. However, when referencing Fig. 1, there is a difference in the connection between nodes. In decentralized

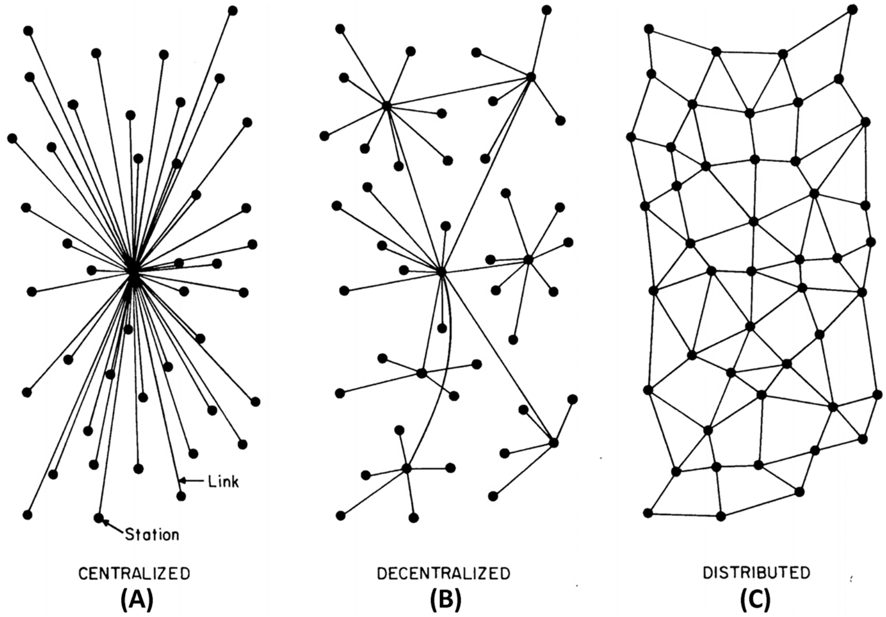

Fig. 1 This illustration shows three different types of networks. Source: *On Distributed Communications Networks* by (Baran, 1962)

systems, not all of the nodes are connected, whereas in a distributed system they are. Every node has the autonomy to make its own decisions, and the aggregation of their votes is a means to reach consensus, resulting in "democratized" system behavior (Truong et al., 2016). These systems can provide similar benefits to one another which is why they are often used together when creating storage systems.

Decentralized and distributed systems have redundancy with cryptographic chaining of transactions to provide transaction integrity. For both of these systems, there is no single point of failure that will take down an entire network or system because there is not a central data controller. Essentially, a myriad of stakeholders and data inputs engage in a transparent dialogue and transactional scheme with one another following pre-figurative algorithmic protocols wherein the objective is to build a consensus and verify that none of the information transacted has been tampered with. One example of such consensus mechanisms is proof of replication (PoRep), built into the system to determine if a node has been corrupted or altered in any manner. A successful validation entails blocks being broadcast through a peer-to-peer mesh network of nodes (see Fig. 1). Each node retains a complete or partial copy of the ledger, and theoretically, the copies of each node are an exact match. If the network encounters a mismatch, that node is singled out and communicated as invalid.

Scalability for such systems is also essentially infinite as any number of nodes can be added. Moreover, the more nodes that you add to a system, the stronger, more reliable, and secure it is against an attack. In the long-run, decentralized systems can be challenging to develop and implement due to the newness of the technology, the coordination of many distributed actors that is necessary, and the computational power needed to maintain these systems. However, this has not stopped groups from creating their own decentralized, distributed archival solutions to record injustices around the world as will be discussed in the following sections.

4.1 How Transactions Are Handled in Distributed Ledgers

A transactional exchange of ownership or control of an asset on a blockchain network means a transfer of the blockchain representation of that particular asset, otherwise referred to as a token or update of a distributed database containing a record of the ownership and control of the asset. A token, for example, can be transferred from one individual's address to another. Addresses on blockchains are denoted by the hash of a public key and resemble a zip code of the destination of the asset being exchanged (see Fig. 2). It can be thought of as similar to an electronic fingerprint, constructed solely from the file's contents or structures. Because of this, some data confidentiality is retained, since the hash is what is being stored and transacted on the network, not the actual piece of data. Lastly, for every public key, there is a matched private key and the private key is essentially used to sign and execute the transaction, completing the transfer of ownership.

Blockchains can also be dichotomously distinguished as public, permissionless, or private, permissioned. Public blockchains permit any user to access and participate in the consensus building of a network and do not require any special

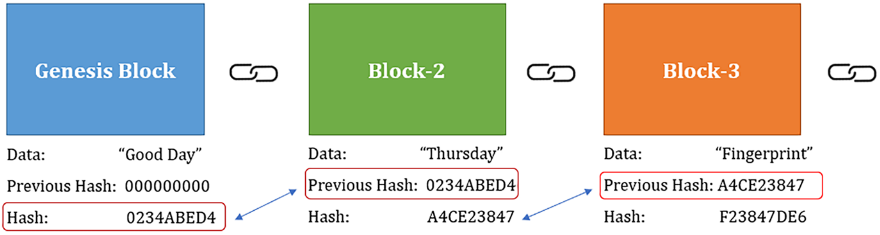

Fig. 2 Blocks in a blockchain are linked cryptographically through the hash. Source: *Blockchain key characteristics and the conditions to use it as a solution* by (Kasthala, 2019)

authorization to see the transactions being made. They are typically permissionless. In contrast, a private blockchain inherently requires each node to demonstrate some identity and prerequisites for authorization to access transacted materials. They are typically permissioned.

The decentralized space is incredibly vast, with new cryptocurrencies, decentralized finance (DeFi), and non-fungible tokens (NFTs) dominating much of the public debate. However, this paper focuses on how these blockchain-based applications can be used in real-world scenarios to protect evidence and promote transparency and accountability in times of conflict. The following section explores an array of examples including how groups are using decentralized solutions to archive and preserve news stories of the pro-democracy movement in Hong Kong, how NGOs are using blockchain for cash transfer programs, university groups preserving testimonies from genocide survivors for future truth and reconciliation work. Utilizing these types of systems for humanitarian work is a growing field with unique international pilot projects. As more work is being done to develop this area of research, adequate consideration of the local community and their immediate needs must be accessed first for the longevity and success of any project.

5 Use of Distributed Ledgers in Human Rights Work

There are an array of use cases implementing distributed ledgers as a means to document international human rights violations. However, as this is an emerging technology, special attention must be paid to the system design and implementation of such solutions. There is a race to produce the newest, most innovative solution to address some of the largest challenges society is facing. While these efforts open up great opportunities, there is a need to critically examine solutions before they are deployed in real-world settings.

Given the centralized nature of traditional institutions, information is not being distributed equally, leaving some less informed. This gatekeeping of information influences individuals to behave unilaterally and often not in the collective interest of the community. Decentralization promises to democratize the sharing of information and increase accountability within institutions when appropriately applied.

From proposed blockchain-based voting to leveraging this technology (Husain et al., 2019) to fight government corruption (Aarvik, 2020; Aggarwal & Floridi, 2019), decentralized systems offer a new way to approach legacy issues that have long seemed insurmountable. The core strength of blockchain-based applications is their immutability and transparency, which are vital to the utility and credibility of documentation in institutional and government settings.

This section explores how private groups, NGOs, and academic institutions are leveraging distributed ledger technology to document and archive societal challenges and issues. The following outlines three major use cases of such technology: Likecoin, Building Blocks, and Starling Lab.

5.1 LikeCoin

LikeCoin is a public blockchain used to publish and archive stories in areas with high censorship of content (LikeCoin, 2021). LikeCoin uses a decentralized registry called the International Standard Content Number (ISCN), which was borrowed from the concept of ISBN used in the traditional publishing industry (ISCN, 2021). An ISCN is a unique identifier that is attached to all records uploaded onto the system together with all relevant metadata related to the file, such as author, content address, publisher information, and more. This makes the documentation easily searchable, identifiable, and necessary to establishing its authenticity. The content itself is stored on InterPlanetary File System (IPFS), a decentralized web platform and Filecoin (Protocol Labs, 2017). Unlike the traditional internet that uses location-based addressing, IPFS uses content-based addressing (Forti, 2017). This means that instead of having to know exactly where a file is located, the user only needs to be aware of the name of the file for which they are searching. The name of the file is a unique, permanent identifier that is generated once the data has been uploaded onto the system. LikeCoin and IPFS both leverage decentralized storage solutions which limit the likelihood of tampering with documents and protects them from deletion via hosting them on a peer-to-peer network.

Likecoin became a natural use case for individuals publishing pro-democracy content in Hong Kong. In 2014, the city of Hong Kong was experiencing a period of unrest, as pro-democratic protesters faced intense police violence on the streets of the city. Individuals in the Umbrella Movement were fighting for universal suffrage for Hong Kong. The conflict lasted for months and left many injured and even incarcerated. While some activists fought on the streets, others took to outlets online and shared and broadcasted on-ground reporting. However, this did not come without consequence, as publishers and journalists were detained for producing and reporting on the movement (Ramzy & May, 2021). Some of those covering the Umbrella Movement turned to LikeCoin as a means to save documentation and material produced by Hong Kongers. They used this platform as a means to limit the erasure of material documenting civic protests (Hui, 2021).

In China, archives are constantly at risk of erasure due to the pervasive nature of the surveillance apparatus. Activists used LikeCoin as a means to preserve evidence of government abuses and showcase the cultural destruction happening in their home. Platforms such as LikeCoin are a powerful way to fight back against governments with strong censorship and propaganda mechanisms because there is no central authority over the data. These documents live on every computer or server on the decentralized and distributed system which drastically reduces their likelihood of erasure. This example showcases the implementability of such decentralized systems, offering insight into the challenges and successes of maintaining such a system within China.

5.2 WFP—Building Blocks

Likecoin provides a community-driven case study, where individuals from Hong Kong and its diaspora come together to address the challenges facing their society. This next example provides an overview of how larger institutions and NGOs are addressing food insecurity, autonomy, and forced migration on a larger scale. As part of the World Food Programme's (WFP) Innovation Accelerator's program, "Building Blocks" was created on the Ethereum network as a means to improve WFP's cash transfer programs (World Food Programme, 2016). The focus of this project was to enhance the experience of issuing and receiving cash transfers for Syrian and Rohingya refugees in Jordan, Bangladesh, and Pakistan. This cash transfer program works essentially as a debit card with a blockchain-based backend application (World Food Programme, 2022). This enabled individuals to freely select the purchases they were making for their household as opposed to a predetermined allotment of food and supplies. Once the cash was transferred, a blockchain-based ledger recorded each transaction. As part of the WFP's cash transfer program, each refugee had their unique biometric information saved and stored with the WFP. When individuals went to purchase with the transferred cash, their identification was confirmed via retinal scanning to guarantee a secure transfer (World Food Programme, 2016).

This new way of transferring cash did not use cryptocurrency. Instead, the scheme merely served as a ledger for each transfer offering a more efficient and secure backend technology while not adding further complexity to the refugee experience (World Food Programme, 2017). In the Azraq Camp in Jordan, the Building Blocks program was able to distribute $1 million to over 10,500 beneficiaries (ibid.). WFP was able to provide over $325 million with over 15 million completed transactions (World Food Programme, 2022).

5.3 Starling Lab for Data Integrity

This last example focuses on how academic institutions are partnering together to create decentralized archives for video testimony and photographic evidence of human rights violations. The Starling Lab for Data Integrity is jointly run between the Department of Electrical Engineering (EE) at Stanford and The Institute for Visual History and Education at the USC Shoah Foundation. The overriding objective of their joint partnership is to create a reliable visual archive that documents all metadata and content of a multimedia clip or picture to a blockchain-based ecosystem. This project has three main principles "to capture, store, and verify digital content" (Takahashi, 2021). Using Textile's developer tools and Application Program Interfaces (APIs), Starling Labs uses the InterPlanetary File System (IPFS) protocol to stamp each file with a universal and survivable ID that allows sources to upload a file to its decentralized web storage. To prove the integrity of community-based storage, the Lab leverages the FileCoin protocol (Protocol Labs, 2017).

FileCoin first initializes secure storage by sealing the data with stacked depth-robust graphs to create a proof of replication. Moving forward, the protocol uses advanced proofs of space–time (Moran & Orlov, 2019) to randomly select leaf nodes of the encoded replicas, and run Merkle proofs (Pomerantz, 2021) on them to demonstrate that a file has been stored continuously and has not been tampered with or degraded. Without having to rely on a centralized node, Starling's tools conduct audits on every sector of storage with verifiable zero-knowledge proofs to ensure each server's commitment is kept. This framework allows Starling users to securely capture photographs. These digital pictures are safely secured and verified as each pixel of a photograph is hashed and stored, along with its metadata, on the blockchain infrastructure. Applications like Starling are working to combat misinformation online and establish multimedia content that can be trusted.

6 Envisioned Components for Private Blockchains

System design and components play a major role in the success of blockchain-based projects. While leveraging a public blockchain architecture is more common, like in the aforementioned examples, the following section will explore a private, permissioned system design. Private systems offer more control over who is allowed to enter the system while still enabling the distribution of network nodes. This can be beneficial, as in the Xinjiang use case, because any new node that enters the system would have to be verified. This can provide a level of protection over the identities of individual users participating in the network, as all nodes on the system would be validated as trusted parties. Combined with the use of decentralized identifiers, which allows users to generate and control their own digital identity without depending on a specific service provider, it is possible to provide even greater privacy protection for those interacting with such a system (Decentralized Identity Foundation, 2022). The following section outlines five major components, as identified through literature, that warrant consideration when designing a private blockchain system for human rights work.

6.1 Anonymization

Through blockchain, users can upload sensitive documentation and verify that their partners in their scholarly or press networks have received the complete version of data they had submitted. Transactions can be made without the concern of malicious actors tampering with their data or of their partners later claiming they had received wrong information. This can be achieved when underlying metadata, including timestamp, device ID, Bluetooth signature, and WiFi MAC address, etc., are hashed, creating forensic markers that can be validated to thwart manipulation attempts. Significantly, blockchain can also enable users to oversee in a transparent manner which stakeholders are accessing their data without calling for intervention from a central authority, and deny certain or all partners from accessing specific metadata, such as geotags and user information, to retain anonymity of personnel involved.

The erasure of data as a means of anonymization, however, cannot easily be practiced in blockchain technology. "Right to be forgotten" provisions appearing in data privacy laws, for example, are difficult to comply with when using distributed ledgers because blockchain records are most commonly intended to be immutable and not editable. However, this depends on the system design and architecture as some blockchain-based systems use techniques to render the blockchain editable, for example, l chameleon chains which allow for an editable, redactable structure (Tatar et al., 2020). Depending on the purpose of the system, leveraging such techniques allows for more flexibility in the information added to the network but would call into question the immutability of the record and its security properties. In the context of Xinjiang documentation, it is unclear what the long-term consequences would be of not being able to erase any and every inscribed record that a user uploads.

Absolutism, particularly in technology, however, has held little credence and there are many examples of blockchain systems having been compromised as a result of weaknesses in the security architecture of such systems or insecure implementation of system components. Because of this, activists and scholars working on Xinjiang-related topics must consider the risks attached to the data they upload on the blockchain. Another option commonly used to address privacy concerns associated with storing records on-ledger is to store only the hash "fingerprints" of the records on-ledger, with the actual records themselves being stored off-ledger in a distributed network of cloud object stores or other types of decentralized storage solution such as the aforementioned IPFS. Even with this approach, however, system design and implementation must be complemented by securing system components from hacking, human error, and social engineering attempts.

6.2 Accuracy of Original Source

Accuracy, in archival science, refers to "the degree to which data, information, documents or records are precise, correct, truthful, free of error or distortion, or pertinent to the matter" (InterPARES 2, 2018). The accuracy of uploaded information, in the context of Xinjiang documentation, consequently depends on the competence of users to accurately record and submit their documentation. First-hand evidence of human rights abuses, however, is presently being collected and leaked through untrained citizen activists and government officials. Professional journalists and academics have yet to gain proper access to Xinjiang since the creation and proliferation of the re-education camp system. That means, considering the lack of physical, procedural, and technical controls on-ground, the accuracy of evidence captured and uploaded onto the blockchain may simultaneously present significant gaps (Flores et al., 2017). Individuals currently working on this topic lack mechanisms to assure that accurate material (i.e., material that is correct, sufficiently precise, pertinent, and truthful) is stored and can be shared over the long term. This causes an inherent tension between meeting the need of scholars and community members seeking a platform to host their materials and ensuring that the materials being shared are accurate in the first place. The struggle is not unique to blockchain-based archives, but it does pose a challenge to the long-term success of such platforms.

However, it is possible to increase the accuracy of data transferred from such systems through audits. For example, where a document is manually transferred from an original paper registry to a computerized blockchain-based system, multi-signatures can be used to help maintain the integrity of data transferred to the blockchain by issuing one key that would be used to record the entry and one or more keys to validate the correctness of the documentation uploaded onto the blockchain (ibid.).

In instances where documentation is transferred from a digital registry onto a blockchain-based platform, an original record in the registry can be hashed and compared with the hash of its mirror entry. A comparison of the hashes would ensure that the records match perfectly before anyone can make a final commitment to migrating and onboarding their entire archive onto a blockchain system. However, this approach would only ensure that the transaction records have been accurately transcribed from an original registry into a blockchain-based system—not that the original records were accurate in the first place (Sarin & Kim, 2018). Accuracy depends upon the degree to which data from originating sources are correct, precise, pertinent, and truthful. Because of this, the only quality control users can exert to raise the chances that the documentation is accurate is by establishing data entry input controls and constraints, and linking them to transaction records that corroborate the truthfulness of the documentation present on the blockchain (Lemieux, 2017a).

6.3 Reliability

In archival science, reliability refers to the trustworthiness of a document and its ability to mirror and memorialize a real-world observation. Achieving reliability depends upon the competency of the creator to create the record, the degree of control over the record creation process, the demonstration that the systems used to create or capture records were operating reliably and without inference, and whether the records were made in the usual and ordinary course of business. With so many platforms and third-party apps being used to capture and store evidence of human rights abuses, which are often not transparent about their data processing practices and strip away crucial metadata needed to establish the authenticity of records, reliable record creation remains a challenge. Establishing a reliable chain of preservation is crucial to creating reliable records.

Once created, the issue becomes one of preserving the authenticity of records and sustaining archival reliability from the point of creation of the record until it is distributed and seen by stakeholders. Various blockchain protocols orchestrate the diffusing and trusted distribution of data as a means of storage and historical preservation. Hashes of the data are replicated across multiple storage nodes.

Problematically, one small change to the format of the data, such as citizen-generated videos, can result in a completely different hash for the footage if there is a single change in the pixels of the photograph (Dotan, 2021), ultimately causing the system to indicate that the record lacks evidentiary integrity when, in fact, its bit structure has only been changed to allow for preservation. At the same time, the fact that mathematical proofs are used to establish that data is being stored and duplicated successfully across the nodes, while alerting and repairing data corruption and errors, is a key blockchain strength. Essentially, detecting alterations is the core strength of blockchain technology, ensuring the integrity of records through the transaction processes (ibid.). Critically, users uploading evidence gathered in Xinjiang can be assured that their stakeholders will only be seeing the exact evidence they have uploaded for them to see.

This is beneficial when working to combat ubiquitous state narratives that often domain news media outlets. Being able to ensure that individuals can upload documentation with the assurance it will not be tampered with, destroyed, and/or degraded is incredibly valuable. As mentioned earlier, platforms like Xinjiang Victim's Database and Atajurt Human Rights Group, struggle with cybersecurity attacks and deplatforming over their content. Both of these groups hold important primary source material regarding on the ground implementation of the re-education camp system that can come under threat. For example in June 2021, Atajurt Human Rights Group was temporarily suspended from Youtube resulting in what could have meant "the loss of an invaluable grassroots archive of more than 3,000 interviews" and testimonies of those in Xinjiang (Wood, 2021). Relying on centralized platforms, such as Youtube, leaves groups vulnerable to the whims of platform terms and conditions, community reporting, and a general lack of oversight of such valuable documentation. Private decentralized systems offer the opportunity to return the governance of data and documentation to only trusted stakeholders in contributing to a participatory data ecosystem.

6.4 Authenticity, Preservation of Semantic and Contextual Information

There are, however, disadvantages of blockchain that may burden users with additional problems unseen in traditional centralized storage systems. Due to the newness of blockchain, applications for Xinjiang human rights documentation can be appreciated from a scholarly context. Future research on blockchain technology should be exploratory until there is a clear method to measure the efficacy of a blockchain-based archival solution against that of a centralized model.

For documentation purposes, all of the aforementioned attributes of blockchain records must be made to persist through space and time. They must satisfy archival authenticity over time, referring to the ability to determine whether or not the record has not been tampered with and is, in fact, what it claims to be. Today, it is difficult to conclusively say whether the case of cultural genocide in Xinjiang will be subject to a truth and reconciliation process. Ambiguity on when exactly transitional justice in Xinjiang will prevail is exactly why it is important to sustain archival authenticity of all human rights records of Xinjiang across decades and centuries. Toward this goal, an authentic record, for example, must exhibit a determinate relationship to the observation which it is recorded to reflect, to the actor who kept it as a record, and to other records of the same observation. This relationship is otherwise referred to as an "archival bond" and establishes the evidentiary character of the record.

Contrary to much of the literature on blockchain technology (Woodall & Ringell, 2019), solely preserving the integrity of the bit structure of data is not a sufficient form of establishing the authenticity of records (Lemieux, 2017b). Critically, the semantic and contextual loss may prevent interpretability in the future. Information on blockchains is sometimes stored in a partial form to save storage space, but the ability to understand the depth and significance of the bits depends upon the preservation of the semantic and contextual information of their origins as well, including the context of their creation and the records' original intended effect. This is essential to sustain the information in an interpretable and meaningful way (ibid.). Human verification of preserved evidence is still used as the final aspect in cementing trust between activist groups, academics, and the press, even though some attempts have been made to introduce artificial intelligence-based approaches (Bui et al., 2020). Typically, once a human expert verifies the accuracy, reliability, and authenticity of the evidence, the analysis can be cryptographically signed and sealed. Only then can the data be considered truly valid, enabling publishers to release expert notarization on a ledger that can be syndicated across permitted stakeholders on the blockchain (ibid.).

6.5 Establishing Trust Across Stakeholders, Key Management

What can also be achieved within the scope of blockchain is the establishment of procedures governing which stakeholders are legitimately allowed to access and observe evidence of human rights violations. To prevent malicious actors without access from seeing the protected dataset, access warrants tight control, relying upon identity, authentication, and authorization. In any system, such as blockchain-based evidence storage and sharing platform, whichever actor holds the key, in theory, has the complete authority to make the data accessible or not for anyone else—although in practice, this is relative to how the platform is designed procedurally (Lemieux, 2017a).

Critically, it would be undesirable if a bad actor were to hold the private key that provides control over the access to sensitive Xinjiang documentation (i.e., data that users have generated or uploaded). As such data would become vulnerable, open to theft, and subject to exploitation. This is because it may be possible for some partners to have malicious intent or to confer upon themselves the level of access that exceeds what the partner is competent to view as per the users' judgment. To prevent such an event, users and their stakeholders, such as a registration authority, have a vital and continuing role to play in ensuring that an active organization does not establish a blanket oversight over determining the level of access for other parties.

In practice, a registration authority could also be a bad actor. To address this risk, it is ideal to adhere to the “four eyes” principle in which two stakeholders involved in Xinjiang documentation must sign off on a change in the level of access of participants; and registering content or transactions on the blockchain should be treated separately from access. It might be that decisions about who can record or register transactions on the blockchain are also subject to dual or multiple signatures, as in this human rights–oriented solution (Rehman et al., 2021).

7 Conclusion

Storing and preserving evidence is crucial for communities impacted by human rights violations and the future of truth and reconciliation work. It is too easy for state actors and agencies to produce and maintain the dominant narrative surrounding current events in their jurisdiction. Human rights groups, activists, scholars, and individuals on the ground need new innovative solutions to fight back against systemic injustices. Before they can seek justice, they need to be able to build evidence and proof of what they observe to be happening. Xinjiang materials such as court records, pictures, videos, and familial and citizenship records reference human subjects; thus, they are inherently sensitive and pose a risk to the safety and security of individuals.

Currently, there is no streamlined approach for sending and retrieving such materials. This is inconvenient and unreliable for activists and scholars who are documenting this crisis and could even expose them to danger. It is unfavorable to rely on systems controlled and operated by the government that is attacking the rights of specific groups. Traditional centralized systems, even if not operated by the state, and databases for capturing and preserving evidence of human rights abuses are failing for a myriad of reasons including cybersecurity attacks, misinformation, tampering attempts, or human error.

It is advisable for groups looking into developing decentralized and distributed storage solutions to minimize the number of individuals who have control over the system and incentivize correct and secure behavior through algorithmic consensus mechanisms. It is recommended for groups interested in exploring blockchain-based archival solutions to seriously consider private, permissioned systems to increase the ability to oversee the users of the system. Utilizing a private, permissioned architecture could allow the network administrator to know the identity of each node on the system and establish prerequisites for authorization, unlike public permissionless systems. This could be beneficial for the security of the system because it is highly likely that the documentation and evidence submitted to the network could contain compromising identifiable information.

For individuals to have trust in the security of the system and be willing to share such information, knowing who is present on the system and who has access to this material is vital. In limiting the nodes on the system to those verified by the system administrator, the likelihood of the presence of malicious actors might be decreased. On the other hand, care must be taken to ensure that the authorities responsible for the governance of the system can be fully trusted. The structure of the network also must incorporate checks and balances so that no single agency can unilaterally make decisions about access and how documentation is handled and preserved. Identity, authentication, and authorization, which are features of permissioned systems, must not be solely relied upon to protect system users. Other mechanisms, such as privacy-preserving system design and techniques, must also be applied.

This exploratory paper offers insight into some of the benefits and challenges associated with establishing decentralized storage solutions for archives. Due to the political sensitivity of the human rights violations taking place in Xinjiang, researchers and activist groups need to be aware of the vulnerabilities associated with current archival storage solutions. Cybersecurity attacks and manipulation of data are becoming a massive threat to the infrastructure that currently we have in place for hosting and storing sensitive information. Exploring decentralized and distributed solutions offers the potential for increased security and integrity of records, although we still observe that such solutions alone cannot inherently guarantee the accuracy, reliability, and authenticity of records without human verification.

Future research in this field includes developing the specific requirements needed to support activist groups working on Xinjiang-related issues. For example, while in theory blockchain can be incredibly strategic for evidence curation and preservation, some technological literacy is required to properly operate and verify blockchain systems. Any interest in deploying blockchain-driven approaches in Xinjiang, for example, must consider the technological aptitude of stakeholders on-ground and consult literature on using nascent technologies in humanitarian affairs. Evaluating which competing protocol would be the most appropriate to store sensitive documentation is important. However, configuring and tailoring user experiences and user interfaces (UX/UI) of such systems to the socio-cultural considerations of activists, and identifying scenarios in which off-chain human errors can compromise blockchains in a humanitarian setting, for example, become of higher importance.

While there are limitations to this emerging technology, the literature indicates that distributed ledger systems offer an opportunity to place less reliance on centralized parties for archival purposes. This is especially important when centralized parties have a vested interest in suppressing the truth and any related documentation or may present a single point of failure and security vulnerabilities. While individuals must be cautious when applying new technological solutions to social challenges like that in Xinjiang, there is evidence from use cases to suggest that decentralized systems could be an effective way to support groups on the ground. As technology is evolving and changing, so is its ability to have a social impact.

As regimes are becoming more technologically sophisticated, activists, scholars, and community leaders have to continually find new ways to hold people accountable, in the short and long terms. With the advent of distributed ledger systems, preserving and archiving materials for truth and reconciliation work at the community level is more possible than ever. In situations of identity-based conflict and cultural erasure, to be silenced is to allow the oppressor to win. Communities and people are resilient and need archives that are reflective of that. Decentralized systems create a powerful tool to combat those in power and push for truth and transparency in times of darkness and conflict.

Funding Preliminary research for this paper was funded in part by the Natural Science and Engineering Research Council of Canada.

Data Availability The authors confirm that the data supporting the findings of this study are available within the article [and/or] its supplementary materials.

Declarations

Conflict of Interest The authors declare no competing interests.

References

Aarvik, P. (2020). *Blockchain as an anti-corruption tool. Case examples and introduction to the technology*. Chr. Michelsen Institute. Retrieved from https://www.cmi.no/publications/7208-blockchain-as-an-anti-corruption-tool-case-examples-and-introduction-to-the-technology

Aggarwal, N., & Floridi, L. (2019). The ppportunities and challenges of blockchain in the fight against government corruption. *19th General Activity Report (2018) of the Council of Europe Group of States against Corruption.*

Amnesty International Canada. (2020). *Human rights defenders increasingly face threats, intimidation over China advocacy: Report*. Retrieved from https://www.amnesty.ca/news/human-rights-defenders-increasingly-face-threats-intimidation-over-china-advocacy-report

Ayasun, A. (2021). *Uyghurs wary of Turkey's pending extradition deal with China* . – The Diplomat. Retrieved from https://thediplomat.com/2021/01/uyghurs-wary-of-turkeys-pending-extradition-deal-with-china/

Baran, P. (1962). On distributed communications networks. *IEEE Transactions on the Professional Technical Group on Communications Systems*, *CS-12*(1). https://doi.org/10.7249/p2626

Barme, G. R., & Ye, S. (1997). *The Great Firewall of China*. Wired. Retrieved from https://www.wired.com/1997/06/china-3/

BBC. (2016). *China confiscates passports of Xinjiang people*. BBC News. Retrieved from https://www.bbc.com/news/world-asia-china-38093370

Bischoff, P. (2021). *Surveillance camera statistics: Which cities has the most CCTV cameras?* Comparitech. Retrieved from https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/

Bui, T., Cooper, D., Collomosse, J., Bell, M., Green, A., Sheridan, J., & Thereaux, O. (2020). Tamper-proofing video with hierarchical attention autoencoder hashing on blockchain. *IEEE Transactions on Multimedia, 22*(11), 2858–2872.

Byler, D. (2020). *The Xinjiang data police*. Retrieved from https://www.noemamag.com/the-xinjiang-data-police/

Byler, D. (2021). *Terror capitalism: Uyghur dispossession and masculinity in a Chinese city*. Duke University Press.

Chin, J., & Bürge, C. (2017). *Twelve days in Xinjiang: How China's surveillance state overwhelms daily life*. The Wall Street Journal. Retrieved from https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355

Clarke, M. (2007). China's internal security dilemma and the "Great Western Development": The dynamics of integration, ethnic nationalism and terrorism in Xinjiang. *Asian Studies Review, 31*(3), 323–342. https://doi.org/10.1080/10357820701621350

Cliff, T. (2016). *Oil and water: Being Han in Xinjiang*. University of Chicago Press.

Decentralized Identity Foundation. (2022). *Identifiers and discovery*. DIF. Retrieved from https://identity.foundation/working-groups/identifiers-discovery.html

Dotan, J. (2021). *Trustless truth: How private and public ledgers can take on misinformation - and win. Hyperledger*. Retrieved from www.youtube.com/watch?v=w1r3Fsjaw0s

European Medicines Agency. (2021). *Cyberattack on ema - update 6 European Medicines Agency*. European Medicines Agency. Retrieved from https://www.ema.europa.eu/en/news/cyberattack-ema-update-6

Feng, G. C., & Guo, S. Z. (2013). Tracing the route of China's Internet censorship: An empirical study. *Telematics and Informatics, 30*(4), 335–345. https://doi.org/10.1016/j.tele.2012.09.002

Flores, D., Lacombe, C., & Lemieux, V. (2017). (rep.). *Real estate transaction recording in the blockchain in Brazil (RCPLAC-01) – Case Study 1.*

Forti, L. (2017). *InterPlanetary File System (Ipfs) Tutorial - Building the distributed web. Fullstack Academy*. Youtube. Retrieved from https://www.youtube.com/watch?v=6kqgsGXpykM&ab_channel=FullstackAcademy

Greig, J. (2022*). Red Cross worried about misuse of stolen data by nation states and cybercriminals after hack.* ZDNet. Retrieved from https://www.zdnet.com/article/red-cross-worried-about-misuse-of-stolen-data-by-nation-states-cybercriminals/

Griffiths, J. (2021a). Over the wall - China's first email and the rise of the online censor. In *Great Firewall of China: How to build and control an alternative version of the internet*. essay, Zed Books Ltd.

Griffiths, J. (2021b). Enemy at the gates - How fear of Falun Gong boosted the Firewall. In *Great Firewall of China: How to build and control an alternative version of the internet*. essay, Zed Books Ltd.

Guerif, V. (2010). Making states, displacing peoples a comparative perspective of Xinjiang and Tibet in the People's Republic of China . *The Refugee Studies Centre Working Paper Series*, 1–46.

Gutnikov, A., Kupreev, O., & Yaroslav, S. (2022). *DDoS attacks in Q1 2022.* Securelist. Retrieved from https://securelist.com/ddos-attacks-in-q1-2022/106358/

Hadjimatheou, C. (2021). *Mayday: How the White Helmets and James Le Mesurier got pulled into a deadly battle for truth.* BBC. Retrieved from https://www.bbc.com/news/stories-56126016

Hui, M. (2021). *Hong Kongers are using Blockchain archives to fight government censorship.* Quartz. Retrieved from https://qz.com/2008673/hong-kongers-use-blockchain-to-fight-government-censorship/

Human Rights Watch. (2020). *Saudi Arabia: Clarify status of Uyghur detainees*. Retrieved from https://www.hrw.org/news/2020/11/23/saudi-arabia-clarify-status-uyghur-detainees

Husain, S., Sathik, M., & Nisha, S. (2019). Enhanced security on e-voting system using BlockChain. *SSRG International Journal of Computer Science and Engineering,* 23–25.

ISCN. (2021). *International standard content number specifications*. LikeCoin Foundation Ltd. Retrieved from https://iscn.io/

Kang, D., & Fraser, S. (2021). *Turkey Uighurs fear sellout to China in exchange for vaccine.* AP News. https://apnews.com/article/turkey-beijing-coronavirus-pandemic-ankara-china-c8b714974552c484c501a5784efc117a

Kasthala, V. (2019). Blockchain key characteristics and conditions to use it as a solution. *Medium*. Retrieved from https://medium.com/swlh/blockchain-characteristics-and-its-suitability-as-a-technical-solution-bd65fc2c1ad1

Killing, A., Rajagopalan, M., & Buschek, C. (2020). *Blanked-out spots on China's maps helped us uncover Xinjiang's camps*. BuzzFeed News. Retrieved from https://www.buzzfeednews.com/article/alison_killing/satellite-images-investigation-xinjiang-detention-camps

Kuo, L. (2021). *China appears to block Signal app, tightening internet controls*. The Washington Post. Retrieved from https://www.washingtonpost.com/world/asia_pacific/signal-app-china-blocked-firewall/2021/03/16/a7972b52-860c-11eb-be4a-24b89f616f2c_story.html

Leibold, J. (2019). Surveillance in China's Xinjiang Region: Ethnic sorting, coercion, and inducement. *Journal of Contemporary China, 29*(121), 46–60. https://doi.org/10.1080/10670564.2019.1621529

Lemieux, V. L. (2017a). (rep.). Blockchain recordkeeping: A SWOT analysis. ARMA. Retrieved from http://imm.arma.org/publication/?i=454085&article_id=2939577&view=articleBrowser&ver=html5

Lemieux, V. L. (2017b). Future Technologies Conference 2017b. In *Blockchain and distributed ledgers as trusted recordkeeping systems: An archival theoretic evaluation framework* (pp. 1–11). Vancouver.

Levinger, M. (2007). Master narratives of disinformation campaigns. *Journal of International Affairs,* 75(1.5), 125–134. https://www.jstor.org/stable/26508126?seq=1&cid=pdf-reference

LikeCoin. (2021). *Decentralized Publishing*. LikeCoin. Retrieved from https://docs.like.co/

Liu, A. H., & Peters, K. (2017). The Hanification of Xinjiang, China: The economic effects of the Great Leap West. *Studies in Ethnicity and Nationalism, 17*(2), 265–280. https://doi.org/10.1111/sena.12233

Lyngaas, S. (2022). *Aid groups helping Ukraine face both cyber and physical threats*. CNN. Retrieved from https://edition.cnn.com/2022/04/23/politics/humanitarian-aid-ukraine-war-cyberattacks/

Meaker, M. (2019). *China is trolling and hacking Uighur exiles across the world.* WIRED UK. Retrieved from https://www.wired.co.uk/article/china-uighur-hacking

Millward, J., & Peterson, D. (2020). *China's system of oppression in Xinjiang: How it developed and how to curb it*. Global China: Assessing China's Growing Role in the World. Retrieved from https://www.brookings.edu/wp-content/uploads/2020/09/FP_20200914_china_oppression_xinjiang_millward_peterson.pdf

Moran, T., & Orlov, I. (2019). Simple proofs of space-time and rational proofs of storage. *Advances in Cryptology – CRYPTO 2019*, 381–409. https://doi.org/10.1007/978-3-030-26948-7_14

Moreau, Y. (2019). Crack down on genomic surveillance. *Nature, 576*(7785), 36–38. https://doi.org/10.1038/d41586-019-03687-x

Mozur, P. (2019). *One month, 500,000 Face Scans: How China is using A.I. to profile a minority. The New York Times*. Retrieved from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Pomerantz, O. (2021). *Merkle proofs for offline data integrity* Etherum Foundation. Retrieved from https://ethereum.org/en/developers/tutorials/merkle-proofs-for-offline-data-integrity/

Protocol Labs. (2017). *Filecoin: A decentralized storage network* [White Paper]. Retrieved from https://filecoin.io/filecoin.pdf

Qu, Y. (2021). *Extending grassroots power and mobilizing the people*. Xinjiang Documentation Project. Retrieved from https://xinjiang.sppga.ubc.ca/critical-scholarship/project-reports/extending-grassroots-power-and-mobilizing-the-people/

Ramzy, A., & May, T. (2021). *"Hong Kong cracks down on a pro-democracy newspaper"*. The New York Times. Retrieved from https://www.nytimes.com/2021/06/16/world/asia/hong-kong-apple-daily.html

Rehman, E., Khan, M. A., Soomro, T. R., Taleb, N., Afifi, M. A., & Ghazal, T. M. (2021). Using Blockchain to ensure trust between donor agencies and NGOs in under-developed countries. *Computers*, *10*(8), 98. MDPI AG. Retrieved from https://doi.org/10.3390/computers10080098

Reuters. (2018). China upset as Interpol removes wanted alert for exiled Uighur leader. Retrieved from-https://www.reuters.com/article/us-china-xinjiang-idUSKCN1G80FK

Rickleton, C. (2021). *China hounds Xinjiang data collectors*. Eurasianet. Retrieved from https://eurasianet.org/china-hounds-xinjiang-data-collectors

Roberts, S. R. (2021). *The roots of cultural genocide in Xinjiang*. Foreign Affairs. Retrieved from https://www.foreignaffairs.com/articles/china/2021-02-10/roots-cultural-genocide-xinjiang

Rollet, C. (2018). *Hikvision wins Chinese government forced facial recognition project across 967 mosques*. IPVM. Retrieved from https://ipvm.com/reports/hik-mosques

Ruser, N., Leibold J., Munro K., & Hoja, T. (2020). Cultural erasure: Tracing the destruction of Uyghur and Islamic spaces in Xinjiang (Policy Brief No. 38). Australian Strategic Policy Institute. Retrieved from https://www.aspi.org.au/report/cultural-erasure.

Salimjan, G. (2021a). C*amp land: Settler ecotourism and Kazakh dispossession in contemporary Xinjiang*. Lausan. Retrieved from https://lausan.hk/2021a/camp-land/

Salimjan, G. (2021b). Naturalized violence: Affective politics of China's 'ecological civilization' in Xinjiang. *Human Ecology: An Interdisciplinary Journal, 49*(1), 59–68. https://doi.org/10.1007/s10745-020-00207-8

Sarin, A., & Kim, S. (2018). Distributed ledger and Blockchain technology: Frameworks and use cases. *Journal of Investment Management*. https://doi.org/10.2139/ssrn.3373347

Sechenova, M. (2014). Fahrenheit 451 - Burning through The Great Firewall of China. *The Indonesian Journal of International & Comparative Law*, 283–314.

Takahashi, D. (2021). *USC and Stanford launch Starling Lab to protect human rights with decentralization*. VentureBeat. Retrieved from https://venturebeat.com/2021/06/10/usc-and-stanford-launch-starling-lab-to-protect-human-rights-with-decentralization/

Tatar, U., Gokce, Y., & Nussbaum, B. (2020). Law versus technology: Blockchain, GDPR, and tough tradeoffs. *Computer Law & Security Review*. https://doi.org/10.1016/j.clsr.2020.105454

The InterPARES Project. (2018). (rep.). *Glossary - InterPARES 2 project book*. Retrieved from http://www.interpares.org/ip2/display_file.cfm?doc=ip2_glossary.pdf

Tofox A Stanford Project. (2011). *The Great Firewall of China: Background*. Retrieved from https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-chinabackground/index.html

Truong, N. B., Jayasinghe, U., Um, T.-W., & Lee, G. M. (2016). A survey on trust computation in the Internet of Things. *Information and Communication: Journal of the Korean Telecommunications Society*, *33*(2).

Ullah, A. (2020). Uighur scholar fears deportation from Saudi Arabia. *Middle East Eye*. Retrieved from https://www.middleeasteye.net/news/uighur-china-saudi-arabia-scholar-deportation

United Nations Department of Economic and Social Affairs. (2007). United Nations declaration on the rights of indigenous peoples for indigenous peoples. Retrieved from https://www.un.org/development/desa/indigenouspeoples/declaration-on-the-rights-of-indigenous-peoples.html

Unrepresented Nations & Peoples Organization. (2015). *East Turkestan*. UNPO. Retrieved from https://unpo.org/members/7872

Wang, M. (2018). *"Eradicating ideological viruses"*. Human Rights Watch. Retrieved from https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs

Wolfe, P. (2006). Settler colonialism and the elimination of the native. *Journal of Genocide Research, 8*(4), 387–409. https://doi.org/10.1080/14623520601056240

Wood, C. (2021). *"Why Atajurt's brief YouTube suspension matters"*. The Diplomat. Retrieved from https://thediplomat.com/2021/06/why-atajurts-brief-youtube-suspension-matters/

Woodall, A., & Ringel, S. (2019). Blockchain archival discourse: Trust and the imaginaries of digital preservation. *New Media & Society, 22*(12), 2200–2217. https://doi.org/10.1177/1461444819888756

World Food Programme. (2016). Building Blocks. In *Center for Innovation and Partnerships* (pp.1–2). Université de Genève. Retrieved from https://www.unige.ch/gsem/files/5815/8858/2412/Building_Blocks_website.pdf

World Food Programme. (2017). *Building Blocks- The future of cash disbursements at the World Food Programme*. Retrieved from https://unite.un.org/sites/unite.un.org/files/session_2_wfp_building_blocks_20170816_final.pdf

World Food Programme. (2022). *Building Blocks Blockchain network for humanitarian assistance- Graduated Program*. Retrieved from https://innovation.wfp.org/project/building-blocks

Yi, X. (2019). Recruiting loyal stabilisers: On the banality of carceral colonialism in Xinjiang. *Made in China Journal, 4*(3). https://madeinchinajournal.com/2019/10/25/recruiting-loyal-stabilisers-on-the-banality-of-carceral-colonialism-in-xinjiang/

Zenz. A. (2017). Chen Quanguo: The strongman behind Beijing's securitization strategy in Tibet and Xinjiang. *China Brief, 17*(12). Retrieved from https://jamestown.org/program/chen-quanguo-the-strongman-behindbeijings-securitization-strategy-in-tibet-and-xinjiang/

Zuo, H., Wang, L., & Qin, J. (2017). XJU1: A Chinese ethnic minorities face database. *International Conference on Machine Vision and Information Technology, 2017*, 7–11. https://doi.org/10.1109/CMVIT.2017.17