HOW BLOCKCHAIN TECHNOLOGY CAN BE USED TO REDUCE INTERNET CENSORSHIP IN CHINA

by

JOSHUA WEINROBE

A THESIS

Presented to the Department of Business Administration
and the Robert D. Clark Honors College
in partial fulfillment of the requirements for the degree of
Bachelor of Science

May 2025

An Abstract of the Thesis of

Joshua Weinrobe for the degree of Bachelor of Science
in the Department of Business Administration to be taken May 2025

Title: How Blockchain Technology Can Be Used to Reduce Internet Censorship in China

Approved: *Alex Murray Ph.D.*
Primary Thesis Advisor

This Thesis examines the history of censorship in China and how current Internet censorship affects Chinese citizens. Through extensive literary review, this thesis provides information on the Chinese Communist Party's desire to improve censorship methods. A general overview of blockchain technology is provided and in-depth examinations of certain technological components are provided. Limitations of blockchain technology are also examined to help determine any issues that could potentially be faced during the implementation of a blockchain network in China. Ultimately, the question of whether blockchain technology could be used to reduce Chinese Internet censorship is addressed.

Acknowledgements

Firstly, I would like to thank my advisors, my primary advisor Professor Alex Murray, and my Clark Honors Advisor Kristen Rahilly. Your feedback and advice to me throughout this entire process has been extremely helpful and I would not have been able to do any of this without your guidance.

Secondly, I would like to thank my parents for all of their support throughout this entire process, my four years at the University of Oregon, and my entire life. I could not have done anything without your love and support and I am extremely grateful.

Finally, I would like to thank my friends for all of their support throughout my time in college. I wouldn't be the person that I am today without all of you and the ways you have shaped me.

Table of Contents

List of Figures

List of Tables

Chapter 1: Introduction

Introduction to Chinese Censorship

China has continuously evolved its censorship efforts into one of the most sophisticated in the world. Chinese censorship aims to shape public opinion by hiding information that contradicts the Chinese Communist Party's (CCP) opinions from citizens. The government uses technical controls and social frameworks to discourage anti-government thinking. The CCP promotes its own ideas to its citizens, which ultimately helps it silence opposing viewpoints and create a population that believes in its government. This leads to many consequences for citizens. Many citizens self-censor due to fear of the punishments they would receive. Some citizens agree with censorship and see it as a way to protect their national unity. However, others recognize it as a threat to free speech. There are also no clear boundaries around what is allowed, which creates more problems as citizens are uncertain of their actions. Ultimately, censorship allows the CCP to reduce free speech and promote pro-government ideologies.

Introduction to Blockchain Technology

Blockchain technology is a decentralized system for recording transactions across many different users' computers. Records are secure, transparent, and immutable due to this technology. Unlike traditional databases, blockchain enables interactions without the need for intermediaries. The technology uses cryptographic techniques to validate transactions and ensure that other users aren't able to see the involved parties. The technology's design ensures that data is authentic and can't be changed. Blockchain technology was originally conceived to power cryptocurrencies, but has since increased in applications. Blockchain's ability to create trust allows it to be useful for users. However, the technology also faces many challenges. Despite

these challenges, blockchain technology has the potential to be used to reduce Internet censorship in China.

Objectives of The Thesis And Expected Outcomes

- Gain an understanding of the history of Chinese censorship
- Gain an understanding of Internet censorship in China and its effect on citizens
- Gain a basic understanding of blockchain technology
- Gain an understanding of how blockchain technology could be used to reduce Chinese Internet censorship
- Discover limitations to the possible implementation of blockchain technology in China
- Conclude whether the introduction of blockchain technology in China could help reduce Internet censorship

Chapter 2: Internet Censorship In China

Introduction to The Framework of Chinese Censorship

The current Chinese government under Xi Jinping uses censorship to shape the public opinion of the country's citizens, ultimately allowing for more control. With control over the free spread of information in the country, the government is able to ensure that information opposing its viewpoints is not shared among the population. With this lack of information spread, citizens are often only exposed to pro-government propaganda, shaping their opinions on many important subjects. The lack of available information opposing the current ruling party can influence the general views of the citizen base of the country. This ultimately can create a loop where these popular opinions are continuously shared, increasing the percentage of people who believe in them. The continued occurrence of this loop can create a country where the majority of the public believes in a few set ideologies, and ultimately, there is little dissent among the citizens against the government-promoted views.

The censorship loop described above continues to prevent the spread of free information and allows for the suppression and ostracization of opposing viewpoints. When the majority's beliefs of a population shift, this is often due to multiple different factors. One of these factors is unrelated to the power that is trying to change public opinion, but to the population among which the belief is being spread. Those who have views that go against the common opinions in a country are often criticized and sometimes excluded by those who hold the beliefs that are popular in that population. This becomes more prominent when popular beliefs are held by the majority of the population and when the government attacks and discriminates against those who hold the minority view. This ultimately continues to reduce the spread of free information among

a population, as those holding the minority viewpoint are often silenced due to the threat of exclusion.

The current Chinese censorship methods are used as a tool to maintain political control over the population. When the majority of the population favors the current ruling party, the party is able to maintain its control. While Chinese elections are not fully free due to the authoritarian nature of the ruling party and the requirement that all candidates be approved by it, censorship and the suppression of free speech also improve the party's ability to maintain political control. By ensuring that few opposing viewpoints reach the population, the ruling party is able to ensure that there is not a mass uprising against their rule. This allows them to continue to increase the constraints put on citizens without enough opposition to decrease the effectiveness of their implementation, ultimately increasing their power and control over the population.

The Modern Historical Evolution of Censorship in China

This thesis will examine the history of censorship dating back to Mao Zedong's controls information relating to censorship before then would be outside of the scope of this thesis. While the CCP has consistently used censorship methods to try to ensure "political hegemony" (Green et al., 2024), the methods they have used have changed over time. Under Mao Zedong's rule, the party ensured that all forms of communication were subject to censorship as they "enforced centralized management over media such as film, news, and radio" (Green et al., 2024). By controlling the popular methods of communication and information spread at the time, the CCP under Mao was able to ensure the spread of the views they deemed correct. The CCP also regulated interpersonal speech between private citizens through omnipresent state surveillance", ultimately leaving few avenues for public dissent (Marie Brady 2010). The CCP's further

regulation of communication through citizens increased their control over the spread of information within the country, ultimately reducing the possibility of dissenting opinions.

After Mao's death, censorship was reduced and free speech became more prominent, ultimately becoming a prime contributing factor in the 1989 Tiananmen protest movement (Gewirtz, 2022). However, this protest, which "nearly led to the collapse of the CCP regime" (Green et al., 2024), led to strict oversight and increased censorship as the CCP looked to correct the errors it had made. Two of the methods implemented after the protests were "stricter oversight over media content" and the creation of a "National Program for Patriotic Education" (Green et al., 2024). The increased control over the media can be explained by the success of the same regulations during Mao Zedong's rule. The implementation of education programs was likely aimed at instilling ideologies in the youth of the country to ensure that the country's growing population would have the opinions promoted by the CCP.

Another important event that threatened the CCP's control over the spread of information in China was the invention and popularization of the Internet. China officially connected to the Internet through Sprint on April 20th, 1994, however, CHINANET, China's Internet backbone that allowed the public to access the Internet, was not finished until 1996. The Chinese government saw the Internet as necessary due to its ability to promote "informatization" (Marie Brady 2010) and increase economic growth. However, the decentralized nature of the Internet created an array of sources of potential dissent (Xinzhou and Yaoying, 2020). The implementation of the Internet in China had the potential to allow citizens with viewpoints that opposed the CCP to share them with other citizens, potentially leading to a snowball effect with the outcome of an anti-government majority opinion. To reduce the likelihood of these results, the government implemented both technological and legal barriers to the Internet's use for free

information spread (the technological barriers will be discussed in a later section). The government imposed policies criminalizing the use of computer networks to undermine state power or social stability (Xinzhou and Jialun, 2019). This criminalization was likely aimed at ensuring that the implementation of Internet technology in China would not become a catalyst for the spread of free information among the population. These legal and technological barriers were the first iterations of Internet control by the government of China, leading to the vast number of methods currently used by the CCP.

Modern Censorship Practices Under Xi Jinping

The current president of China, Xi Jinping, has made it clear that his censorship efforts will focus primarily on censoring the Internet. In a 2013 speech, he stated that he would make Internet public opinion work the top priority of propaganda and ideological work (Xianfu, 2013), a sentiment that he has frequently shared in later speeches. It can be assumed that President Xi sees the Internet as important in the CCP's fight to retain control over public opinion and the general population. In one of his later speeches, he stated that the success of the CCP in the ideological battle present on the Internet is "directly related to the political security of the country" (Jinping, 2023). This statement from President Xi highlights the government's desire to retain political control over the population and how the Internet could potentially harm or help the CCP in this fight. To accomplish the goal of maintaining control over public opinion on the Internet, Xi directed the party to establish a comprehensive network governance system (Ronghua 2022) which would involve technical, legal, and economic means of managing information content on the Internet This system would likely allow the party to use the Internet to suppress dissenting voices and increase the prevalence of propaganda on the Internet in China, ultimately promoting their opinions to the masses.

The CCP's efforts to reform the reform laws relating to Internet usage have focused on the creation and spread of laws that aim to create standard allowed behaviors on Internet platforms for Chinese citizens. The main way that this was done was through the "2017 Cybersecurity Law" (Descamps, 2020), which consolidated all prior laws on the usage of the Internet and gave party authorities more control over the content on Chinese networks. The original legislation came along with many other supplementary laws aimed at describing the proper use of censorship by Chinese citizens. These laws cover a variety of topics and are expanded regularly as new technologies are developed that could be used to spread anti-CCP sentiment. These laws aim to provide clearer enforcement mechanisms for ensuring compliance by Chinese citizens, improve the ability of the CCP to "identify and trace sources of online information" while monitoring public sentiment, and implement better controls over "internal and outbound flows of information" (Green et al., 2024). All three of these desires align with the overall goal of regulating the spread of information on the Internet. Identifying and tracing sources on online information would allow the CCP to ensure that the regulations are followed by providing consequences if they aren't. The other two desires allow the CCP to monitor any information that is spread through the use of the Chinese network.

While many of the CCP's efforts have focused on regulating the use of the Internet to prevent its possible use in the spread of free information, President Xi has also highlighted a proactive approach to shaping public opinion. In 2018, President Xi highlighted an engagement-based approach that emphasizes persuasion (Yang, 2020) of citizens instead of regulation. Promoting information in line with the views of the CCP may be more believable to citizens in China, as they may not be aware that it is coming from a government source. Accounts that appear to be run by individuals could be used by the CCP to appeal to citizens who may not trust

the government but may be open to pro-party ideologies. One proactive method that President Xi highlighted was the use of "social media and mobile applications to educate Chinese citizens" and reduce the prominence of "incorrect thought trends'" (Green et al., 2024). This use of mobile technology could potentially be seen as the CCP's desire to spread their ideologies to the younger generations, as social media is used most prominently by them. President Xi's acknowledgment of the presence of "incorrect thought trends'" highlights the party's awareness that information contradicting the CCP's ideologies is present on the Internet and that the Internet could potentially be used to influence citizens to disbelieve ideas that are harmful to the political control of the party.

Methods and Technologies of Censorship

The Chinese government uses multiple technological methods, including keyword filtering, deep packet inspection, and Artificial Intelligence, to ensure the continued Internet censorship for its citizens. Keyword filtering allowed the government to more efficiently find violations of its goals for information dissemination. The Chinese government uses keyword filtering to inspect web traffic at multiple levels, including international data transit gateways (Xu et al., 2011). Chinese methods of keyword filtering allow the CCP to discover when certain words that are often used when spreading anti-government information where present on the Chinese Internet, even if they came from outside sources. The CCP could then take action to remediate the source, ultimately maintaining its control over information spread to its citizens. Deep packet inspection was used with keyword filtering to "look for triggering words or phrases in the destination URL or HTML" (Green et al., 2024). If words or phrases were detected that were not allowed, the CCP could block access to the site for its citizens, reducing potential harm to censorship efforts. Since the increase in popularity of Artificial Intelligence, the CCP has

taken efforts to implement it in its goal of Internet control. In 2020, researchers from the Chinese National Radio and Television Administration "filed two patents" for AI tools that "used computer vision technology to analyze and extract data from audiovisual media" (Ziyu, 2020). By using AI, the CCP can continue to improve its technological ability to control information on the Internet that is viewable by Chinese citizens by expanding its ability to detect information that may be harmful to its efforts.

While the Federal government is responsible for many of the policies relating to censorship and some of the work to help maintain its control, local governments and private organizations also play a large part in the CCP's censorship efforts. A lot of the "day-to-day censorship and public opinion work is overseen by lower-level Party-state bureaucracies" (Green et al., 2024). By delegating the majority of the work to local authorities, the CCP can improve its capacity for Internet censorship while also ensuring that resources can be efficiently used by dispersing them based on necessity in individual regions. The CCP has also contracted private companies and news organizations to engage directly (Yanping, 2019) with Chinese citizens on the Internet. The companies help the CCP conduct public opinion work on the Internet to ensure that the government is aware of the success of their efforts. The CCP has also used regulations to co-opt private Internet companies into enacting censorship on their commercial platforms under threat of fines or closure (Knockel, 2020). The CCP's power over companies operating within its borders is used to improve its censorship efforts by removing possibilities for dissent at the source. This leads companies to examine the effects of operating in the opportunistic Chinese market while facing regulations that could affect their usage and benefits provided to customers.

The CCP expands on the use of private organizations in monitoring public opinion to ensure it gauges real-time threats and opportunities for increased propaganda. The Cyberspace

Administration of China (CAC) is one of the key players in monitoring real-time public opinion on the Internet. Their main tasks include "tracking, analyzing, and sharing information on public online sentiment" (Green et al., 2024). By collecting and analyzing this data, the CCP can make informed decisions about the use of resources in countering any sentiment that is against their messaging. Party Committees at the provincial level in China maintain their own Cyber Security and Informatization Committees (Hunan Provincial Department of Finance, 2020) that oversee a corresponding CAC department in this information analysis within their jurisdiction. By dividing the country into provinces, the CCP is again able to determine which regions need more resources to ensure control over information and sentiment on the Internet. The CAC is also tasked with coordinating incident responses to online public sentiment emergencies (Shuqiong, 2018). Having a division of the CCP that is dedicated to both analyzing public opinion and responding to it ensures efficiency by reducing the need for communication between divisions. However, information gathered by the CAC relating to public opinion is still shared with other divisions of the CCP to ensure the best possible response to negative sentiment.

Challenges of The Chinese Internet Censorship System

While the localization of censorship efforts could help ensure that resources can be allocated efficiently, the reality is one of disparities between regions. The structure of the CCP's censorship bureaucracy is "unevenly developed, with major disparities among various local censorship organs in terms of resourcing and capabilities" (Green et al., 2024). The unequal amount of resources contributed to individual regions allows for harsher information suppression in some regions than others. However, "all regional propaganda departments are required by the Party to perform the same information control functions" (Green et al., 2024) regardless of the resources they possess. Regions with fewer resources are often spread thin and are not able to

perform the necessary information control functions. This ultimately leads to overworked staff in regions with fewer resources and disparities in censorship and propaganda efforts throughout the country. The overall hierarchy of Chinese censorship is also poorly created due to its localized structure. The local institutions in the country that govern Internet censorship are "organized haphazardly, with many local authorities having redundant or overlapping areas of responsibility" (Green et al., 2024), and there are many problems with the bureaucratic coordination. While the CCP's overall structure of managing Internet Censorship may look complete and highly functional through a bird's eye view, many problems appear when the interworking of the system is scrutinized. Having overlapping areas of responsibility could lead to censorship of certain regions that are either more or less stringent. Ultimately, localization provides challenges for the CCP's censorship efforts, which could lead to inefficiency.

The lack of resources often leads to unqualified workers, which, combined with human errors, can reduce censorship effectiveness. The CCP is often forced to "rely upon parttime or volunteer workers" in its censorship efforts. The workers could be less qualified than those who are fully trained and employed by the CCP, and have the sole purpose of increasing censorship in the country. This can ultimately lead to information on the Internet that the CCP would be against. Even in larger metropolitan areas such as Beijing, censorship functions such as Internet commentary work are undertaken by volunteers or by government employees who are contractually obligated to fulfill those tasks in their spare time (Yunmei and Juan, 2016). The volunteers would likely be ill-equipped to handle the tasks necessary to ensure full Internet control by the CCP. The government employees who are doing the tasks in their spare time may not be as efficient as they would likely be overworked and may not be putting in their best efforts. The efforts by the CCP to censor information are often undermined by human error and

mismanagement (Ning et al., 2022), which could ultimately reduce the efficiency of the Party's censorship efforts. While many tasks are automated and the CCP has many technologies that improve its control over the Internet, decisions are often still required to be made by government officials and lower-level employees. Government officials often default to deleting posts that raise sensitive criticisms (Ning et al., 2022). The deletion of all anti-government information could lead to exacerbated public opinion crises and ultimately to protests. These concerns have been a prime contributing factor to mass incidents such as the 2011 anticorruption protests (Mattingly, 2022). Ultimately, the need for human actions in the CCP's censorship efforts can lead to inefficiency and increased anti-Party opinions.

The lack of clear boundaries on permissible speech often leads citizens to self-censor and not discuss important topics. While the CCP does make "allowances for civil discourse within China" when it seems strategic, "the boundaries that constitute what is and is not acceptable are not fixed" (Green et al., 2024). The lack of fixed rules on what is considered allowed by the CCP can lead to an unawareness by Chinese citizens of what they can say on the Internet. What is considered permissible discourse and the severity of punishments given to those whose speech is seen as unacceptable are ever-shifting (Freedom House, 2021). The uncertainty of allowed speech and punishment can again lead to an unaware citizenry. Ultimately, "many citizens self-sensor to avoid running afoul of ill-defined redlines" (Green et al., 2024). While this self-censorship may be seen as beneficial by the CCP because it can reduce the risk of information being spread that is against their ideals, citizens being afraid to spread any information can reduce social progress and awareness. Citizens may also shy away from spreading any information, even if their opinions align with the CCP, ultimately reducing the amount of pro-

government propaganda. This lack of information spread due to the fear of punishment and a lack of awareness can lead to an unknowledgeable citizenry and reduced social connections.

Chinese citizens have also discovered ways to circumvent censorship efforts by using technological methods such as Virtual Private Networks (VPNs) and encrypted messaging. While Chinese law "restricts VPN usage to authorized users", however, "unauthorized VPN usage remains prevalent" (Green et al., 2024). The prevalence of VPN's among Chinese citizens reduces the efficiency of the CCP's censorship efforts. VPN usage is particularly high among China's youth, who often use the technology for the purpose of accessing Western entertainment platforms (Economist, 2022). Allowing younger citizens, who often have larger social networks than adults, to have access to Western entertainment could allow for the spread of Western ideologies within China at an increased rate. The spread of Western ideologies is something that the CCP aims to prevent, and VPNs are an immediate threat to the Party's censorship goals. Encrypted messaging is another technology that has been used in China to evade censorship efforts. By posting photographs of text, using encrypted platforms (Claburn 2013), Chinese citizens have been able to evade the many technologies that the CCP uses to try and censor them. This method allows for the improved spread of free information among Chinese citizens, ultimately reducing the efficiency of CCP censorship efforts. However, this method does not come without risk, as several of those posting such content disappeared or were detained (Kuo, 2020). The CCP has clearly made efforts to reduce the spread of information using encrypted messaging and has harshly punished those guilty of it. However, the method still serves as a potential way around censorship for citizens, and combines with VPNs to harm the CCP's attempt to have full control over the Internet within the country.

Case Studies

During the early stages of the COVID-19 pandemic, the Chinese government suppressed information about the outbreak. The CCP implemented laws aimed at punishing those who spread information that painted China in a negative light relating to the beginning and spread of the COVID-19 virus. On February 6, 2020, the CCP issued legal guidance for severely punishing those who maliciously fabricate false epidemic information, create social panic, stir up emotions, and disrupt public order (Yongpeng, 2020). The CCP likely aimed to punish those who posted any anti-government information relating to the pandemic by defining many different terms for anti-government information spread. The statement also likely aimed to ensure that citizens didn't put information on the Internet that could cause citizens to be angry with the CCP or the methods in place for maintaining citizen complacency. However, unauthorized information about the pandemic did appear on Chinese social media, and "local authorities" exerted pressure on the "individual responsible "(Green et al., 2024). The CCP's response was likely aimed at deterring others from posting similar unauthorized information by punishing the individual. This example also highlights the CCP's aim to prevent information relating to the pandemic from being put on the Internet, ultimately reducing the citizens' awareness of narratives harmful to the Party's reputation. The same individual who had spread the information, Dr. Li Wenliang, later died, and public outcry resulted. In response, the CAC "ordered news websites not to issue push notifications alerting readers to his death, and to remove his name from trending topics pages" (Zhong et al., 2020). The CAC's probable aim to ensure that Dr. Li's death did not become a contributing factor to another public crisis was managed through censoring information relating to the event and his statements prior to it. The CCP also aimed to dispute any information relating to the potential Chinese origin of the virus. The Ministry of Education stated that any

“papers tracing the origin of the virus should be strictly managed’” and the “State Council” (Green et al., 2024) would perform the final review over them. This review process by the Ministry of Education was likely in line with the CCP’s goal of preventing any anti-Party information about the origins of the virus. Ultimately, this example, along with the others listed, shows the CCP’s aim to prevent information regarding the COVID-19 pandemic from highlighting government flaws.

The Chinese government has heavily censored anti-Russian and pro-Ukrainian sentiment relating to the ongoing war. At the beginning of the war, five historians in China wrote an open letter denouncing Russia’s actions, which was removed by Chinese censors (Ni, 2022) from the Internet. The CCP’s response to the denunciation of Russian aggression was likely aimed at maintaining the positive relationship between the two countries. Prowar Chinese commentators called the authors traitorous (Ni, 2022), showing the desire to side with the Russians as allies in the conflict. While CCP propaganda has often been pro-Russian since the beginning of the war, the Party has also “noticeably sought to minimize the war’s overall coverage” (Green et al., 2024). This lack of publication likely aims to maintain positive opinions of the general population regarding the relationship between the two countries. Any perception of Russian weakness by the general public would likely dampen their desire to maintain an alliance with them. Patriotic citizens could see Russia as below them and undeserving of help if they are painted as weak or a country that has not been able to win the war. Information comparing the war between Russia and Ukraine to the situation occurring in Taiwan has also appeared on the Internet and has quickly been censored. Any commentary on social media comparing Taiwan and Ukraine is rapidly censored (Zhuang, 2023). The situation in Taiwan is often a highly contested topic by the CCP, and any information trying to paint Taiwan as a victim by

comparing Chinese aggression against it to Russian aggression against Ukraine would likely be seen as extremely anti-Party. Ultimately, the CCP's desire to censor information relating to the ongoing war between Russia and Ukraine highlights their desire to maintain favorable opinions among their citizens, even relating to international relations.

The 1989 Tiananmen Square Incident is one of the most censored topics by the CCP. The CCP "allows almost no permissible public discourse on the subject", and it is "rarely discussed in internal documents or official media" (Green et al., 2024). With such a charged event, it is not surprising that the CCP aims to limit any information spread regarding it, nearly eliminating it from the public record. The Party likely does not believe that it can sufficiently shape public opinion about the event and therefore tries to remove it entirely. The event is also heavily censored digitally. The CCP ensures certain "keywords [are] censored from chats" (Green et al., 2024), referring to the massacre, to ensure that information relating to it is not posted or viewed by Chinese citizens. The CCP aimed to limit all posting capabilities relating to the massacre by restricting official and popular accounts and ensuring that user-posted content undergoes inspection before publication (Wade, 2022). It is clear that the CCP treats the Tiananmen Square Incident differently from other topics in relation to Internet censorship. The Party takes extreme measures to ensure that any information relating to the event is not available to the general population, to continue to shape public opinion.

Examples highlighting the punishments given to those who go against the CCP's opinions help explore the impact of censorship in China. One example is that of Journalist Li Yuanlong, who was sentenced to two years in prison for publishing articles critical of the CCP online. While Li was imprisoned, "Alex, his son'" (China's Censorship Of The Internet And Social Media: The Human Toll And Trade Impact, 2011, p. 5) testified to Congress in the United

States during a hearing on the impact of China's censorship on the Internet. Alex described that his dad had published "four articles online'" (China's Censorship Of The Internet And Social Media: The Human Toll And Trade Impact, 2011, p. 6), which led to his arrest by the CCP, as the statements in the article were against state ideologies. The arrest due to four articles aligns with what was stated previously about the CCP using the tactic to deter others from taking similar actions. However, information about where Li Yuanlong was taken during his prison sentence could provide more details about the punishments given to those who oppose the CCP. Li Yuanlong also "committed [the] articles for a foreign website'" (China's Censorship Of The Internet And Social Media: The Human Toll And Trade Impact, 2011, p. 6) instead of a domestic one. This shows the extent of Chinese Internet censorship, as one of their citizens was arrested for spreading information that was not released through Chinese media. The CCP also tried to arrest Alex because they believed that his "dad published the articles through [his] email address'" (China's Censorship Of The Internet And Social Media: The Human Toll And Trade Impact, 2011, p. 6). This arrest attempt never came to fruition as they determined that Li Yuanlong had not used his son's email address to publish the information. However, the arrest attempt may have been another scare tactic from the CCP, aiming to dissuade both Alex and anyone else from posting similar information online. Ultimately, Li Yuanlong's case provides an example of the tactics that the CCP uses to suppress and discourage anti-Party information on the Internet.

Another similar arrest that highlights the punishments given to those who oppose the CCP was that of Pastor John Zhang. Zhang was "a student at the Beijing Language Institute'" and "participated in the 1989 Patriotic Democratic Movement in Beijing'" (China's Censorship Of The Internet And Social Media: The Human Toll And Trade Impact, 2011, p. 7) after the

Tiananmen Square Incident by organizing memorials. As mentioned previously, the Tiananmen Square Incident is one of the most heavily censored things on the Chinese Internet. It could be assumed that due to this desire to remove the incident from the minds of Chinese citizens that those who the CCP deemed to be responsible for the incident and any following incidents would be punished. It is therefore not surprising that Zhang "was arrested on June 15'" and sent to "Qincheng prison in Beijing for two years'" (China's Censorship Of The Internet And Social Media: The Human Toll And Trade Impact, 2011, p. 7). While Zhang's arrest does not relate to anti-Party information posted on the Internet, it does show the CCP's desire to punish those with opposing viewpoints. By organizing a memorial, Zhang showed that he was on the opposing side of the Tiananmen Square Incident from the CCP, ultimately leading to his arrest. Zhang also described another one of the CCP's methods for determining which citizens needed to be punished. Zhang stated that the "Ministry of Public Security construct[ed] the Golden Shield Project'" a "national surveillance network system'" (China's Censorship Of The Internet And Social Media: The Human Toll And Trade Impact, 2011, p. 8) which could track the IPs of dissidents to allow for harassment and arrests. Zhang also stated that this system was made in cooperation with the Company Cisco. This shows that the CCP is partially relying on Private companies in its censorship efforts. The system that Cisco helped create would also allow the CCP to find the location of anyone who posted anti-Party information, further allowing the government to crack down on it. Zhang's story of arrest shows another example of the CCP's punishments towards those who have opposing viewpoints, and his description of Cisco's efforts describes the importance of private entities in China's censorship desires.

Arguments For Chinese Censorship

While arguments against Chinese Internet censorship have been made above, it is important to examine potential arguments for it to understand it and its impacts in their entirety. Chinese citizens pose many arguments for censorship due to the multiple ways they believe it helps them and their country. The first reason is that they believe that Chinese censorship improves nationalism which is desired by the country's population. Many citizens of Western countries see that the "Western media has credited the Chinese government as a powerful monster" (Jiang, 2012) due to their censorship efforts. Many Western citizens do not look for sources with opposing viewpoints to their own, and it can therefore be assumed that they would not see sources painting the Chinese government in a positive light. Western citizens only view the negative aspects of Chinese censorship and are not able to witness personally any of the consequences or benefits due to the lack of effect it has on them. The way that the CCP maintains nationalism throughout the population of China is by maintaining the ability to be an authority in removing any content they deem to be unnecessary or harmful to the country's goals. This describes how "the state encourages nationalism through manipulating online populations" (Jiang, 2012). While the ideas pushed by the CCP may not be viewed in a positive light by Western audiences, the same ideas being pushed onto all citizens of a country will ensure that the majority of the population has similar viewpoints. When the majority of the citizens view the actions of the government positively, it can ensure that they are patriotic and loyal to their nation. This ultimately can prove as a unifying force by fostering a collective identity among the citizens of China. While the ideals pushed by the CCP may not be viewed positively by Westerners, the nationalism provided by censorship and the promotion of pro-Party ideals can be seen as a benefit of their actions.

Another critique of Western media comes from Chinese bloggers who see anti-censorship information as a critique of China's national sovereignty. Chinese bloggers often "describe the Western media as arrogant towards China" (Jiang, 2012). The blogger's description of Western media as arrogant can lead one to believe that they believe Western countries see themselves as better than China. This would likely lead the bloggers to distrust and feel anger towards Western media, as they would believe that they are not painting an accurate picture of their home country. The original complaints about Western media portrayal of censorship came from Wang Jianshou. In an interview with the BBC in 2005, he stated that "there are too many pre-defined questions'" and that the "BBC is trying to find a piece of information, filter it and create an exciting picture for people in the 'civilized' world'" (Jiang, 2012). The anger at Western media likely stemmed from Jianshou's opinion that the censorship situation in China was not being reported fairly to an outside audience. It is also likely that Jianshou believes that the Western audience, who is reacting to this media, will believe what they see, as it is entertaining even if it is not accurate to the real circumstances in the country. Therefore, his anger at Western media aligns with the situation occurring, and his vocalization of it would lead others to harbor the same feelings. The criticisms of Chinese censorship by Western media also led to "heightened national loyalty" (Jiang, 2012) by Chinese bloggers. It can be assumed that due to the criticism of Western media, Chinese citizens would feel a sense of loyalty to each other and their nation in opposition to the West. While this is not a direct result of the censorship practices of the CCP, it is an unintended result and can help improve the country due to the unity it creates.

Another example of Chinese citizens using digital platforms for nationalist expression was the 2008 anti-CNN movement. The movement "was inflamed by the CNN news commentator Jack Cafferty, who described Chinese products as junk, and Chinese people as

goons and thugs" (Jiang, 2012). It would be understandable how these statements would anger Chinese citizens and would turn them away from Western media outlets. Generalizing an entire population can lead to anger and distrust between the two parties. Around the same time, CNN also "manipulated [a] photo of Tibetan rioters" (Jiang, 2012) to tell an anti-China story. This example would continue to increase the anger of Chinese citizens towards CNN and Western media as a whole. These harms from CNN ultimately led to the creation of a Chinese site by bloggers that is anti-CNN. On this site, there were statements that "We are not against the Western media, but against the lies and fabricated stories in the media. We are not against the Western people, but against the prejudice from the Western society'" (Jiang, 2012). The site shows that Chinese citizens did not believe the fault to be on all Western media or people, but on those who specifically aim to portray the country negatively. The Chinese bloggers who made the site believe that the picture of China sometimes portrayed in Western media is not accurate and harms the country's reputation. They would likely want the country to be portrayed in what they see as an accurate light. Ultimately, this example of Chinese anger at Western media portrayal shows the patriotic nature of Chinese bloggers and their desire to have the country seen in a positive light.

Another potential benefit of Chinese censorship is that it ensures that the present rampant consumerism doesn't threaten the political stability of the country. Consumerism in China has spread throughout due to increases in "disposable incomes of families and individuals in urban and some rural areas" (Jiang, 2012). Increases in disposable income allow for more unnecessary purchases, which increases consumerism. While this would likely be more prominent in urban cities such as Beijing and Shanghai, increases in disposable income in rural areas would ensure that it is partially widespread throughout China. However, the CCP has decided that "promoting

consumerism also fosters nationalism in ways that benefit the central government" (Jiang, 2012). Promoting consumerism improves the economic health of a country and therefore helps the CCP, as they are able to perform better on the world stage. Buying more goods in China also helps stimulate the economy and can help improve both the individual's and the nation's well-being. The CCP's efforts to promote consumerism also help ensure that citizens can buy "consumer products made in China" (Jiang, 2012). This would again help improve China's economy as buying Chinese-made products would ensure that the money made in the country stays in the country and recirculates. This would also help improve China's standing on the global stage and improve its status as one of the biggest economies in the world. However, the rampant consumerism in China can also pose threats, and the country has operated on principles opposed to consumerism for much of its history. Therefore, the CCP "constructs sophisticated managing structures" (Jiang, 2012) to ensure that consumerism does not become an issue in the country. The CCP imposes regulations and ensures that the citizens are self-regulated, similar to their other censorship methods. The government still regulates citizens to ensure that products bought benefit the country and the CCP. Ultimately, the CCP's promotion of consumerism allows for more freedom as citizens are able to express themselves by buying products they like. However, regulations are still imposed to ensure that the rampant consumerism doesn't draw away from the CCP's interests.

Chapter 2 Summary

This chapter has outlined the historical and modern technologies that the CCP uses to enforce censorship. Their methods are highly adaptive illustrating the evolving technology of the party. From Mao Zedong's centralized oversight of traditional media to Xi Jinping's campaigns that use keyword filtering, AI, and real time sentiment tracking, the CCP has continuously

evolved its methods of suppressing dissent. While effective in many ways, the systems still has points of failure such as inefficiencies, human errors, and growing resistance through technologies such as VPNs and encrypted messaging. As China's censorship model continues to develop, the tools for countering it also have. The next chapter will introduce the potential for blockchain technology to serve as a method of reducing Chinese internet censorship. By examining the core concepts of Blockchain technology including decentralization, immutability, and pseudo anonymity, the next chapter will examine how the technology can facilitate the free exchange of information in the country.

Chapter 3: Blockchain Technology's Ability To Reduce Chinese Internet Censorship

General Overview of Blockchain Technology

The first potential benefit of blockchain technology is that its decentralized nature enables trusted transactions among participants in a network who are unknown to each other. It accomplishes this decentralization by ensuring that "no single user controls the information or data on the blockchain" (Schrepel 2021). This is directly in opposition to Web 2 or the traditional form of the Internet, where individual companies control the flow and storage of information and data. Ensuring that no particular party can control the flow and storage allows blockchain technology to provide security and trust to its users. Blockchain technology is inherently distributed among its users, "thanks to [a] code", where "transactions are put into blocks" (Schrepel 2021) that are put onto a chain and become unchangeable. The distribution being guaranteed by code provides increased trust and security to users as they understand that the distribution will be ensured independent of human intervention. The unchangeable nature of the blocks ensures that any historical transactions can't be changed again, providing trust and security to users by ensuring that all records of transactions are accurate. While the users of the network may not trust each other as individuals, the blockchain's structure ensures that trusted transactions can still occur.

To examine the potential uses of blockchain technology in China, a brief history will be provided. The early history of blockchain technology starts in the 1970s when cryptographic methods first became available to civilians. An example of this is the people "Rivest, Shamir, and Adleman" who showed how "two persons could use public–private key encryption and

digital signatures to ensure communication integrity" (Schrepel 2021), forming the early foundations of cryptographic technology that would later turn into the blockchain technologies commonly found today. However, most histories of the technology start in 1982 when "David Chaum, an American computer scientist, published his thesis" which " introduced a new protocol that harnessed cryptographic tools to protect private information" (Schrepel 2021). Chaum's work, building on the work done earlier by Rivest, Shamir, and Adleman, continued to push the technology forward and provided the roots of current technologies. Chaum's continued writings on the subject helped him become a pioneer in the cryptography sector, and he is widely considered one of the founders of digital cash. However, while Chaum's work provided important insights, many recognize 2008 as the year that blockchain technology was officially created and introduced to the public. In 2008, "Satoshi Nakamoto laid the cornerstone for blockchain technology" with "the publication of 'Bitcoin: A Peer-to-Peer Electronic Cash System'" (Gayvoronskaya and Meinel, 2021). This paper laid out the idea of a peer-to-peer network for transactions, ultimately revolutionizing the financial sector by offering a third-party, independent digital payment system. While the idea of a secure decentralized payment system had already existed, the proposal of Bitcoin provided the potential to enable "a robust and secure decentralized system, without any preconditions placed on the number of system users or their identification" (Gayvoronskaya and Meinel, 2021). Nakamoto's paper ultimately provided a larger foundation for potentially efficient and beneficial blockchain networks, which had not been seen before. Ultimately, the figures mentioned in this paragraph and those that came after paved the way for the potential uses of blockchain technology proposed in this thesis.

One of the main technologies that ensures the validity of transactions on a blockchain network is mining. Mining in the context of Bitcoin is the "process of appending new blocks to

the blockchain data structure" (Xu et al., 2019). This appending of new blocks helps in the validation process and ensures that all transactions recorded on the chain are considered and accurate reflection of all of the transactions that have occurred. Blockchain networks rely "on miners to aggregate valid transactions into blocks and append them to the blockchain" (Xu et al., 2019). This again helps in the process of validation. As mentioned previously, blocks composed of all of the recent transactions that have occurred are placed onto an unchangeable chain. However, the transactions need to be aggregated by miners and validated to ensure that all transactions in the blocks going onto the chain are accurate. Once a block is mined, the blocks "are broadcast across the whole network, so that each full node holds a replica of the whole ledger" (Xu et al., 2019). This is a crucial part of the mining process. Once a block is broadcast across the entire network, every member of the network has a record of the complete ledger and is able to ensure that it is accurate. While the chain was described as "unchangeable" previously in this thesis, rare conditions can allow for the chain to be changed by ill-acting members of the network. However, the ability of every member of the network to have access to the whole ledger reduces the likelihood of this occurring, as members of the network would be aware of any malpractice.

General Overview of Blockchain's Benefits

The decentralized nature of blockchain technology removes single points of failure, reducing risks associated with data tampering. In a centralized network, one party can have near-complete control over the flow and storage of information. This would allow that individual party to tamper with all data on the network and would ensure that other members of the network would be powerless to stop it. The problem arises as "centralized storage and management" may "lead to data tampering, manipulation, or privacy leakage due to the single source of failure

problem" (Choo et al., 2020). In a network dominated by a single party, potential malpractice or issues could lead to increased risks of failure. As mentioned, all data being held in one place leads to the potential problem of all of that data being stolen through hacking or similar practices. In networks dominated by a single party "there is [also] no guarantee regarding the provenance of the data and authenticity of the data sources" (Choo et al., 2020). With no guarantee about the origin or authenticity, of data sources, trust is less prevalent than in a network not dominated by individual power. Reliance on information is also potentially decreased as members of the network could be unsure about the reliability of transactions or information. Centralized networks ultimately pose the risk of data tampering or other malfeasances, which is greatly reduced due to the decentralized nature of blockchain technology.

Another potential benefit that blockchain technology provides is its immutability, which ensures that once recorded, transactions cannot be altered or deleted. To achieve this immutability "of the ledger data" the "blocks are linked linearly in chronological order" (Shen et al., 2020). By linking the blocks in a chronological order, the technology ensures that this order is recorded and any alterations would be noticed. This allows the entire network to collectively ensure that this order remains unchanged by any potential party. Another part of the immutability is due to the decentralized and distributed nature of blockchain technology. Because the blockchain is decentralized, no single user has the power to alter the information on the chain. Instead, the "power to alter the blockchain is equally shared among all of its users" (Schrepel 2021). If a user were to change "one copy of the ledger", it would have "no impact on the rest of the blockchain" (Schrepel 2021). The distributed nature of the blockchain prevents possible data tampering, ultimately ensuring trust among its users. The individual user's alteration of any

records likely has no effect on any other user's records, ensuring that the history of transactions is fairly represented. The immutability of blockchain data is "key to the traceability of assets recorded on blockchains" (Xu et al., 2019). If communally recognized data isn't able to be changed by an individual party, then assets recorded on a blockchain would continue to belong to the individual who purchased it on the majority of ledgers, even if it was potentially changed by an individual on the network. Ultimately, the immutable nature of blockchain technology continues to ensure trust among the users of the network.

The pseudo-anonymity of users on the network provided by blockchain technology stands as another potential benefit. Anonymity of users in transactions ultimately provides privacy that isn't available from traditional web services. The technology uses "encryption techniques that anonymize not only the identity of participants, but also that of transactions" (Schrepel, 2021). By anonymizing both the identity and the transactions, the technology is able to provide improved security and privacy to its users. If the content or purpose of transactions between users in a network remains unknown to another individual, then it allows those users to trust that their data remains private. Another technology that blockchain networks use to improve anonymity is "public key cryptography" which helps "in forming the identity and pseudo-anonymity of all participants" (Choo et al., 2020). While the use of pseudo-anonymity instead of full anonymity could prove threatening to users, it ultimately provides benefits. As described previously, transactions are listed on a blockchain and are available in a ledger to all users of the network. However, these transactions are often attached to unique addresses that are not the same as the person's actual identity. Instead, through the use of encryption techniques and public key infrastructure, transactions are linked to addresses that are often represented by a long string of numbers and letters. However, the actual identity of the users who make transactions on the

network is not readily available, ultimately providing security and partial anonymity to them. The public key provides an address for others to send digital assets to without readily providing any identifiers. Cryptographic technology's ability to provide pseudo-anonymity to users provides potential benefits in the possible implementation of the technology in China.

Public vs Private Blockchains for Use in China

There are multiple different types of blockchains with different restrictions to access, two of which are called public and private blockchains. In a public blockchain, "the ledger is open to the public," and anyone can be a "maintainer of the ledger" (Shen et al., 2020). Anyone can join a public blockchain and participate in the network's main activities. Because the ledger is public, any users of the network can also see a list of all transactions and which users they involved. A public blockchain mostly falls into the concept of a fully decentralized network, with every potential user having the ability to participate in all aspects of the blockchain. A private blockchain, on the contrary, is one where "authorization is needed to access" (Schrepel, 2021) it. Only specific users are authorized to use and participate in the network in a private blockchain. A private blockchain is likely "fully controlled by a standalone organization" (Shen et al., 2020). While private blockchain networks can provide benefits, which will be examined later in this thesis, their ability to be controlled by a single entity goes against the concept of full decentralization. Reducing power by individual entities is one of the main goals of blockchain networks, and private networks don't fully accomplish it. By examining the differences between public and private blockchain networks, their potential uses in China can be examined.

The advantages and disadvantages of both public and private blockchain networks will be examined to examine their potential uses in China. The first benefit of a public network would be the reduced barriers to entry. To ensure the effectiveness of a potential blockchain network in

China, increased users would be required. A public blockchain network that would allow any citizen to join would allow for this. More users would provide the best possible opportunities for citizens to participate and improve the overall free speech offered to Chinese citizens. Another advantage of a public blockchain network is that "the vast number of network participants that can join a secured public blockchain keeps it safe from data breaches, hacking attempts, or other cybersecurity issues" (Seth, 2021). Increased numbers of users of a network often lead to better security for it. Therefore, a public network would allow for these increased numbers of users and ultimately improve its security.

A public blockchain network would also have disadvantages associated with it. One such disadvantage is that a public blockchain can't ensure "complete privacy and anonymity" (Seth, 2021). As mentioned previously, blockchains aren't able to provide complete anonymity as the user's address is made available to everyone when a transaction is completed. While the ultimate identity of the user is not readily available, if it is discovered and associated with an address, then they could lose their anonymity. Because public blockchains allow anyone to view a history of transactions, this becomes a greater risk. If a blockchain were to be implemented in China, then anonymity would be an extremely important focus, as the revealing of a user's identity could lead to the punishments described earlier that have been given to those who oppose the CCP online. Therefore, a public blockchain poses the risk of not being able to efficiently allow Chinese citizens to spread anti-government information. Another potential disadvantage public blockchains allow anyone to join, which could lead to "participants who may not be honest with their intentions" (Seth, 2021). Malicious users, such as government agents or pro-CCP citizens, could join the blockchain network and potentially cause harm. The government agents could potentially discover users' identities or harm the network in other ways. Ultimately, the ability of

anyone to join a public blockchain network would harm the goal of allowing free communication for Chinese citizens.

Private blockchain networks also have advantages and disadvantages that would both help and harm their potential to be used in China. The first potential advantage is that "only those with permission" (Seth, 2021) can be full participants in the blockchain network. This means that only those who have access to the blockchain can be a node, a user who helps maintain the networks functionality. This would also mean that only those who have access can make transactions or validate the blockchain. This would help solve the problem posed by public blockchains, where anyone could access it. This would help reduce the risks of users joining the network with malicious intent and could also help keep the identities of users more secure. Another potential benefit to private blockchains is the increased focus on efficiency. Because private blockchains are able to reduce "the focus on protecting user identities and promoting transparency", private blockchain networks can "prioritize efficiency and immutability" (Seth, 2021). Private blockchain networks don't have to focus on protecting user identities because they are able to have a lot more control over who is able to see any user addresses. Therefore, they are able to focus more of their resources on ensuring that the network is as efficient as possible and that any information can't be changed. This also ensures that fewer resources are used overall, which could be potentially advantageous as it would be easier to create and maintain. These advantages would provide the potential Chinese blockchain network efficiency and would ensure that potential users with malicious intent wouldn't be allowed to join.

A private blockchain network would also have disadvantages that would reduce its appeal in China. One potential disadvantage of a private blockchain is that it would likely not allow all potential users to join. Because private blockchain networks only permit certain users to join

when they have permission, some potential users who would not use the network maliciously would likely be prevented from joining. If the overall goal of the network were to ensure that every citizen in China would have the ability to spread information without government censorship, then the permissions needed for a citizen to join would greatly hinder this goal. This would ultimately reduce the impact of the potential blockchain network in China. Another potential disadvantage to the implementation of a private blockchain network is its possible susceptibility to "data breaches and other security threats" (Seth, 2021). Private networks generally have limited validators due to the small nature of the network and this means that transactions could be validated inappropriately. This could ultimately harm the security of the network and reduce its effectiveness. A data breach of the information within the network could greatly harm its users, as it would likely be information that would lead to punishment by the government. Because of this potential for data leaks, the implementation of a private blockchain network in China would require extra resources to ensure that information shared is secure and users trust that they will not be punished for any information they share. The potential implementation would also require resources to ensure that all citizens who would contribute positively to the network could join, while also ensuring that malicious users could not. Differentiating between malicious and non-malicious users would likely prove difficult, and a potential solution to this issue would likely need to be created.

How Cryptography Could Be Used in a Potential Network

One of the main technologies that has led to the development of blockchain technology is cryptography. Generally, cryptography is used to "make a message incomprehensible for outsiders" (Bauer, 2000). While cryptography was not specifically invented for use in blockchain technology due to it having a long history dating back to "ancient [Greece]" (Gayvoronskaya and

Meinel, 2021), it is useful for providing security. The ability to make a message unreadable for anyone who is not a participant in the message is useful in blockchain technology as it can ensure the privacy that is desired. This would be extremely useful in a potential Chinese blockchain network as it would allow citizens to send messages to each other while reducing the threat of anyone else seeing the message. This would allow Chinese citizens to trust that any message sent on the potential blockchain would not lead to punishments for them. One of the most important developments in cryptographic technology "is Kerckhoffs's principle" (Gayvoronskaya and Meinel, 2021). This principle allowed "an encryption procedure [to] be made public and examined for weaknesses by experts worldwide and improved" (Gayvoronskaya and Meinel, 2021). This principle proves useful as it ensures that the messages sent on a blockchain network remain unseen. However, it allows for the cryptographic measures present in a blockchain to be improved. This would prove useful in a potential Chinese blockchain network, as the cryptographic procedures would likely not be fully efficient in their initial implementation. However, with help from experts, the procedures would be updated and the security of the network would be improved, allowing for increased trust by the citizens using it.

If a public blockchain network were to be implemented, cryptographic technology would prove extremely useful. In a public network, anyone would be able to join the network, which could reduce the security of information. However, increased focus on cryptography in the network would ensure that it is harder for any malicious users to read the messages being sent. A private blockchain would also suffer from the potential for data leaks and information from messages being seen by government officials. This would also increase the need for resources going towards cryptographic measures to reduce the likelihood of messages being seen and users

being punished. While cryptography proves important in all blockchain networks, it would be even more crucial in a potential network in China. The extreme nature of punishments given to those who speak out against the CCP often turns away potential dissenters. However, a blockchain network with efficient cryptography measures would allow citizens to trust that government officials would not have access to any messages they share. This would allow for information to be shared freely among willing citizens, which would be the ultimate goal of a potential blockchain network in China.

While cryptography would likely prove useful in a potential implementation in China, the technology is still prone to failure. Potential failures could prove catastrophic as they would potentially allow the CCP to gain information on individuals sharing sentiment with others, ultimately punishing them. Encryption is sometimes seen as "not acceptable" because of "technological developments in decryption" (Xu et al., 2019). Improvements in decryption technology would give those with malicious intent the ability to view the identities of those participating in a blockchain network. This ability could potentially be used by the CCP to punish any individuals sharing information on a potential blockchain network. These punishments would also likely serve as a way for the government to discourage any other citizens from potentially participating in a Chinese blockchain network. Other potential sources of encryption failure would be broken algorithms and weak encryption methods. While blockchain technology is not "a new encryption algorithm", it is an "innovative combination of existing technological approaches from cryptography" (Gayvoronskaya and Meinel, 2021). It can therefore be reasoned that with this new and complicated technology, problems could arise regarding the code implemented that ensures the success of encryption on any given blockchain network. Code made at the creation of a specific blockchain network may also not remain

efficient for the network's entire life. It would be necessary to continuously update the building blocks of a potential blockchain network in China to ensure the continued success of its encryption methods. Ultimately, a lack of resources put into this upkeep could lead to the reveal of the identities of those using the network and punishments for them.

How Public Key Infrastructure Could Be Used in a Potential Network

Cryptographic technology in blockchain networks is often used in conjunction with public key infrastructure to ensure privacy and security. Participants in a blockchain network have two different types of keys. Each participant has a "secret key, also called a private key, and a public key" (Gayvoronskaya and Meinel, 2021). The public key "is freely available to all communication partners" (Gayvoronskaya and Meinel, 2021) and is used as an address so that other participants of the network can send cryptocurrency to the user. In order for transactions to occur between users, this key is known. The public key functions similarly to an account number in a traditional bank in that it allows others to send funds to an individual. However, the private key "remain[s] secret and is used to decrypt and sign messages" (Gayvoronskaya and Meinel, 2021). The private key is used to ensure that the information being sent by other users can only be read by the individual associated with the public key. The private key also ensures that messages or funds can't be sent from an account, as entering the private key is necessary to ensure the completion of a transaction. It is therefore crucial that a user keep their private key unknown by others, as knowledge of both a user's public and private key would give them near complete access to their funds. While the implementation of a blockchain network in China may not include the transfer of funds between individuals, the encryption and security provided by public and private keys would prove useful. A citizen in China who had a public key would be able to receive messages from other citizens on the network. The private key would allow the

user receiving the message to decrypt it without any other parties being aware of its contents. Ultimately, the combination of public and private keys would allow for citizens to share messages without giving the government or any individuals with malicious intent the ability to see the contents.

Public keys on a blockchain network provide increased security compared to traditional public key infrastructures. For potentially malicious users, "converting a public key into a private key is impossible for practical reasons, because of the computational power this requires" (Schrepel 2021). The large amounts of computational power required provide increased security to users of a blockchain network as it ensures that their private key remains private, guaranteeing messages sent to the user remain encrypted. However, the user would have to ensure that they don't share their private key with anyone else, as this could greatly reduce their privacy. The increased security of private keys provided by blockchain technology would greatly increase the efficiency and security of a potential Chinese blockchain network, as it would ensure that the government could not discover the private keys of users on the network. While improvements in data analytics and computing could reduce these effects, current technology wouldn't allow for the discovery of messages sent on the blockchain network. Current technology also makes it "difficult to link public keys to the physical entities that control them" (Schrepel 2021). This would prove extremely important in a potential Chinese blockchain network as it would ensure the improved anonymity of users. The ability to conceal the identities of users would allow them to feel more confident sending messages in a country where dissent against the government is punished. Ultimately, the computational difficulty of discovering a private key or the identity of a user would allow the blockchain network to provide security to users.

How Smart Contracts Could Be Used in the Potential Network

Another blockchain enabled application in blockchain networks and potentially useful is smart contracts. Smart contracts ensure the continued success and efficiency of certain aspects of blockchain networks. Once "smart contracts are deployed," they will "always run as programmed" (Shen et al., 2020). This aspect of smart contracts would benefit a potential Chinese blockchain network. If the implementation required a program within the blockchain to continuously run without the need for human intervention, smart contracts would be a beneficial technology. Smart contracts would also ensure that intervention from potential malicious users wouldn't affect the continued functions of the network. This aspect of smart contracts can be further examined as smart contracts "cannot be further modified" (Shen et al., 2020). This again would ensure that potential malicious users, such as government officials, wouldn't be able to change the workings of the network. Ultimately, this would provide extended security to the network. Even though the smart contracts that are in place can't be modified, their functions can still be changed by developers of the blockchain network. If a developer would like to make changes, they should deploy "a new smart contract" to "upgrade or patch the original one" (Shen et al., 2020). New smart contracts being implemented would allow the potential Chinese blockchain network to be improved over time. This would prove beneficial as technologies would improve over time, ensuring the necessity of changes to the underlying smart contract technology. Ultimately, the almost unchangeable nature of smart contracts, along with their ability to ensure the completion of tasks independent of human intervention, provides benefits that would help improve a potential Chinese blockchain network.

Another potential benefit of smart contract technology is the reduction in costs that it can provide. Smart contracts "always execute a certain part of their source code if they are

‘triggered’” (Gayvoronskaya and Meinel, 2021). The automated nature of smart contracts would help reduce the costs necessary to maintain the potential blockchain network. Without the need for any human intervention or non-automated tasks, the network would be able to reduce operating costs compared to traditional computer programs. This cost reduction would be beneficial as the implementation of the network would already be a costly endeavor, and reducing costs would help increase the efficiency while also making the project more appealing. The autonomous parts of a smart contract are “executed at the computer of every” (Gayvoronskaya and Meinel, 2021) user of the network. This would help improve the efficiency of the network as the smart contract would ensure that every user is able to retain the same information while also having the same access to all features of the network. No individual user would be at a disadvantage compared to others, as the autonomous agent would run on all users' computers simultaneously. Ultimately, the congruent nature of smart contracts as well as the reduction in costs that they can provide allow them to provide benefits to a potential Chinese blockchain network.

Smart contracts have shown many potential use cases that could potentially be implemented in the Chinese blockchain network based on the history of their use. The first use case of smart contracts is their ability to “automate or monitor the execution of parts of legal contracts” (Xu et al., 2019). One potential use of this ability of smart contracts would be the licensing of content shared throughout the potential network. Legal contracts would be necessary to determine who would be able to replicate or share the content that users of the network create. Therefore smart contract would be able to automate the process of licensing this content and determining which other users would be able to have access to it. The potential network could also be used to connect content creators with other users of the network to help share anti-party

content beyond its confines. Such connections between users would require contracts to ensure that the creators are paid by the other users. Smart contracts would be able to seamlessly ensure payments without removing the ability of the user to scam the creator. This would ultimately provide more trust to all users of the network, especially those looking to find opportunities for potential employment. Another use of smart contracts that has been previously shown is their ability to "define a protocol of interaction between different parties" (Xu et al., 2019). This ability would again prove to be useful, as there would likely be many different parties interacting on the network, and regulations would be necessary to ensure that problems don't arise. Smart contracts would be able to automate potential regulations for communications between users, ultimately improving the culture and efficiency of the network.

How Decentralized Autonomous Organizations (DAOs) Could Be Used in the Potential Network

Decentralized Autonomous Organizations (DAOs) are another blockchain-enabled application that could be used in the proposed Chinese blockchain network. DAOs have "neither a business manager, nor any other central leadership instance or company headquarters, but instead [have] a decentralized structure with automated decision-making according to defined rules" (Gayvoronskaya and Meinel, 2021). This lack of central leadership present in a DAO would allow it to ensure that no individual in the potential Chinese blockchain network had power over others. This would ensure that a user with malicious intent wouldn't be able to set up a structure that harmed other users. The automated decision-making present in DAOs is possible because of the smart contract technology described previously. The ability to create rules and have the DAO continuously ensure that they are followed would allow the network to create a good environment for sharing anti-CCP messages. Ultimately, rules would likely need to be set

by users to ensure the fair treatment of all. These rules "are determined by the majority decisions of the involved participants and continuously developed" (Gayvoronskaya and Meinel, 2021). By allowing the users of the network to set the rules employed, the network would be the best representation of their opinions. Majority decisions would ensure that the rules implemented are beneficial for the largest number of users. This would prove useful in the potential network as it would ensure that citizens who are concerned with their privacy or with other issues get a say in the operations of the network. The continuous nature of updating and developing rules would also ensure that the network would be able to conform to updates in technology from the government. Users would be able to propose rules that would aim to ensure the security of their messages and identities. Ultimately, a DAO would allow the potential Chinese blockchain network to provide decision-making and decentralization to users.

DAOs have the potential to lead to exploitation and can have security issues, which would pose a threat to the potential Chinese blockchain network. One historical example of this is known as the "Dao Incident" (Schrepel 2021). During this incident, a malicious user " discovered a vulnerability in the smart contract governing" (Schrepel 2021) a DAO. The error was discovered "by one user who seized" (Schrepel 2021) cryptocurrency from the DAO in what became known as a famous incident of blockchain technological failure. This example ultimately shows the failures of not only DAOs but of blockchain technology as a whole. A malicious user was able to find a vulnerability in the technology and exploit it. A failure such as this could prove catastrophic in the Chinese blockchain network. Malicious attacks by other users could lead to punishments for the citizens using the network. If users don't have trust that the network will protect their identities, then they will likely not use the network, and it will result in a waste

of resources and an unsuccessful implementation. Ultimately, historical examples of the failings of DAOs force the need for improved security of the network.

Another potential weakness of DAOs is their ability to be manipulated. DAOs "generally rely on a decentralized architecture for governance" (Schrepel 2021). As stated earlier, decisions about smart contracts are made based on votes by the majority of users. However, this could also potentially lead to these votes being manipulated by users with malicious intent. If a user or group of users were to gain the majority vote, then they would be able to create smart contracts that could potentially harm others. For example, if the CCP were to create a majority in the network, then they could potentially create a smart contract that automates the execution of transactions or agreements that would harm citizens using the network. This potential harm could reduce the efficiency and usefulness of the network, as it would allow the government to gain partial or full control. To reduce the likelihood of this happening, there would need to be a way to ensure that one party can't gain majority control over votes. A private blockchain network would be a simple solution to this problem, as it would make it more difficult for users with harmful intentions to join. However, programs limiting the number of votes that any individual user could have would also prove useful. While this would still allow for the government to potentially accumulate votes by creating more users, it would increase the difficulty. Ultimately, potential voting problems may arise in a DAO, and solutions regarding them would have to be created before the implementation of the network to ensure its continued success.

How Oracles Could Be Used in the Potential Network

The final technology that could potentially prove useful in the Chinese blockchain network is Oracles. Oracles are "a connection to information outside the blockchain" (Gayvoronskaya and Meinel, 2021). Having connections to media outside the information being

shared on the network would increase the amount of information being shared between users. Connections could be set up between the network and other data or media sources to allow users to see the most much information. This would allow the network to accomplish its ultimate goal of being a way for citizens to see information that they would not otherwise see. Oracles have the ability to "function as a bridge to the real world" (Gayvoronskaya and Meinel, 2021). While the blockchain network may be seen as siphoned off from the rest of the Internet, Oracles provide a connection between the two without sacrificing the decentralization that makes blockchain networks appealing. Oracles are "enabled for smart contracts" (Gayvoronskaya and Meinel, 2021), which ensures that any functions the oracles are performing are automatically performed independently of human actions. This ensures that any potential uses of oracles cannot be able to be tampered with by malicious users. One example of an oracle being used was one that ensured that currency could automatically be converted "From US Dollar to BTC" (Gayvoronskaya and Meinel, 2021), which is better known as Bitcoin. While this example of an oracle may not prove extremely useful in a potential Chinese blockchain network, it proves the ability of oracles to perform automated tasks using real-world outside information. Conversions could be made between languages using an outside translator instead of a currency converter in the potential network. Ultimately, the ability of oracles to connect blockchain networks with the greater Internet would improve the efficiency and potential uses of the Chinese blockchain network.

Oracles provide other technological advantages that could prove useful in a potential Chinese blockchain network. Smart contracts "and oracles can replace numerous middlemen" (Gayvoronskaya and Meinel, 2021). As mentioned previously, the automation of tasks performed by smart contracts increases efficiency by removing the need for many middlemen. Oracles continue to increase this efficiency by working in collaboration with smart contracts to connect

the blockchain network to the greater Internet. While traditional Internet networks would likely need programs and possibly even human intervention to ensure the completion of tasks, blockchain networks are able to fully automate them. This would prove useful in a potential Chinese blockchain network, as increased efficiency would be desired by potential users and the groups setting it up. Automating necessary tasks would reduce the resources needed to create the blockchain network, which would make it more appealing. The automation of tasks, especially those relying on connections to the Internet, would allow the network to be continuously updated and new features to be added. Users would be able to define features that they would like added, and instead of searching for middlemen or a way to complete these tasks, the infrastructure would already be in place to ensure their completion. Ultimately, the improved efficiency provided by oracles due to their ability to remove the need for intermediaries would make a potential Chinese blockchain network more desirable to the country's citizens.

While the efficiency and information provided by oracles would likely prove useful in the potential Chinese blockchain network, disadvantages would still arise and need to be considered during implementation. Oracles are able to supply information “about the external world to the blockchain” by “adding that information to the blockchain as data in a transaction” (Xu et al., 2019). However, this requires a connection to the outside Internet as the data has to be taken from somewhere else. This could potentially become problematic in the potential Chinese blockchain network due to restrictions on the Internet in the country. As mentioned previously, the CCP has strict controls set on the use of the Internet by Chinese citizens. It could therefore be reasoned that the implementation of an oracle connecting the Chinese Internet to the Chinese blockchain network would be threatened. If the CCP discovered that the connection was made, they would likely try and stop the connection from occurring. They may also discover the

blockchain network due to their discovery of the connection, which could put the network and its users in jeopardy. Connections between the blockchain network and traditional Internet networks outside of the country of China could potentially mitigate these risks. This would likely affect the data supplied to the network through this connection. However, it may be necessary to ensure the safety of the users of the network as well as the security of the greater network. Ultimately, it could prove difficult to create connections between the potential blockchain network and traditional Internet networks. However, the benefits provided by Oracles would likely outweigh the threats associated with their use.

Potential Layer 1s to Be Used in the Implementation

There are multiple different layers of blockchain networks that serve different functions and provide different benefits to users. Layer 1s are extremely important as they "allow an unlimited number of applications to be added on top" (Schrepel 2021). The ability to build "decentralized applications, or dApps for short" (Gayvoronskaya and Meinel, 2021) proves extremely useful as it provides the ability to create endless use cases for blockchain technology. These decentralized apps have historically provided the bulk of uses as they create real-world applications and execute the necessary tasks. Layer 1s serve as the base layer of the blockchain network, providing the foundational technology and framework for any dApps built on top of it. It can therefore be reasoned that the implementation of a potential Chinese blockchain network would not require the creation of a layer 1. Layer 1 blockchain networks are expensive to create, and there are already many good options that the potential blockchain network could be built on top of. Therefore, an examination of potential layer 1s for the network to be built on top of will be used to provide information on the differences between them. This would ultimately help uncover potential weaknesses and show which layer 1 could provide a good base for the

potential network. The three layer 1s that will be examined are Solana, Ethereum, and BNB Smart Chain, as they are all layer 1s that have a history of providing use for dApps. All three layer 1s are well-known within the blockchain community and would provide benefits to the potential network.

Examination of Layer 1 Blockchain Networks

Examination of Networks	Solana	Ethereum	BNB Smart Chain
Maximum Transactions per second (TPS)	2,909	62.34	1,731
Average time it takes to create a new block (Block Time)	0.39 Seconds	12 Seconds	1.5 Seconds
Time it takes for transactions to be considered final (Time to Finality)	12.8 Seconds	16 Minutes	7.5 Seconds
Number of nodes participating in the network (Node Volume)	5,680	13,900	240
Nakamoto Coefficient (a coefficient that measures the decentralization of the network based on how many nodes it would take to control the network)	21	2	7

Layer 1 Comparative Table

Table comparing different statistics of Layer 1 blockchains

While these measures help begin to describe the efficiency and decentralization, they are not able to paint a full picture of the benefits offered by each layer 1. Ethereum has a “rich ecosystem of tools, frameworks, and protocols, driving innovation and growth” due to its “extensive developer community” (KuCoin, 2025). There are many other factors that would need to go into the decision on which layer 1 to use. Therefore, extensive research would need to be conducted during the implementation to decide on one.

Potential for a Chinese-run Blockchain Network

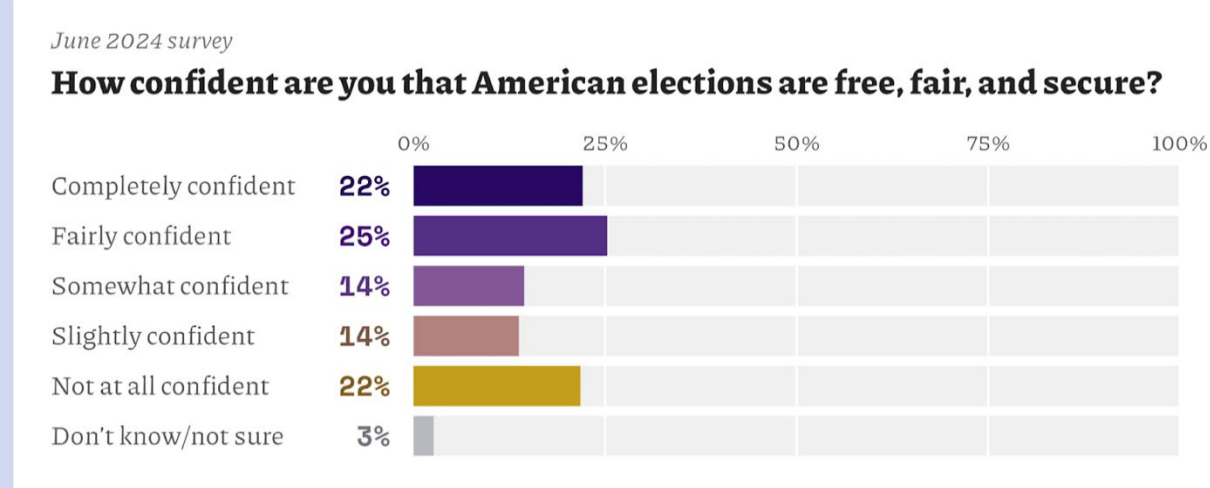
As described previously, the current Chinese government is not one under which a blockchain network to improve freedom of communication on the Internet could be run. It is important to recognize " the importance of legal certainty and a clear regulatory regime in areas pertaining to blockchain-based applications" (Legal And Regulatory Framework For Blockchain, 2024). However, this regulation can sometimes be for the benefit of the users, as increased regulation can ensure that everyone on the network is being treated fairly. If a blockchain network were to be created in China, it would likely not be run by the CCP. If the CCP were to run the network, then it would have the ability to create rules that go against its main goal of allowing free communication. Therefore, it can be assumed that the network would be run by some other organization or country. This would likely be necessary to ensure the success of the implementation. However, having another group create the network would require that group to have the resources necessary to create a blockchain network. It would also require a group to have the desire to create the network, even without receiving the benefits from it. There would be potential for a network run by the CCP in the future. If the goals of the CCP were to be changed, then there would be the potential for them to be a part of a blockchain network in China. However, this would ultimately reduce the need for a blockchain network, as under these circumstances, free speech would be allowed.

Case Studies of Similar Uses of Blockchain Technology

There have been many examples of blockchain technology being used for situations similar to the one described in China. One such example is Securevote, which is a "blockchain [based] voting platform" (Securevote, 2025). A blockchain-based voting system would likely prove useful in a potential Chinese blockchain network, as it would allow users to make

decisions on features to be added, similar to the DAO technology described earlier. Secure vote, through blockchain technology, was able to create a platform “that can mathematically prove the validity of election results without compromising individuals' privacy” (Securevote, 2025). Election validity is extremely important, especially in a time when public sentiment is that elections aren’t fair.

Figure 1 - American Election Confidence



American opinions on election security

June 2024 Survey on American confidence in free, fair, and secure elections

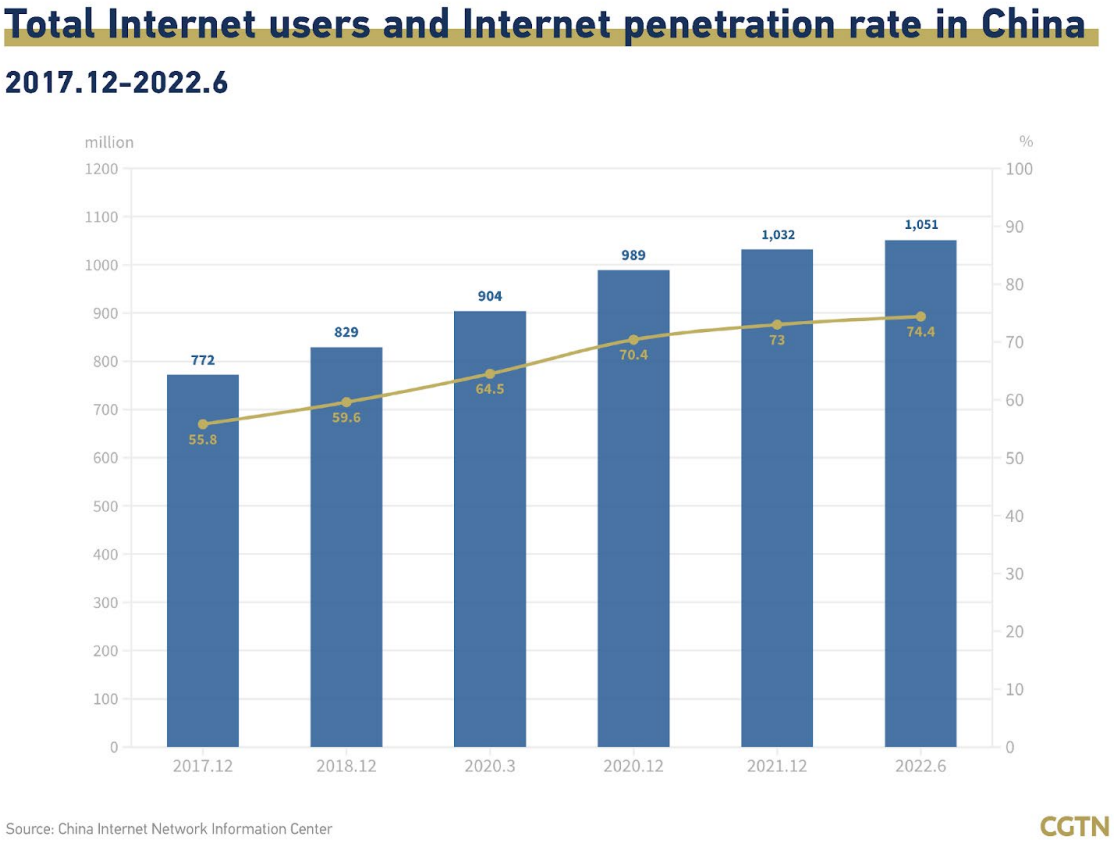
It is clear from this sample that American sentiment towards election security and fairness is relatively negative. While this is a sample of Americans and not Chinese citizens, it can be reasoned that election sentiment traverses international borders. The decentralized nature of Securevote increases the security of elections and the trust users have in them. Securevote’s “immutable” (Securevote, 2025) nature ensures that election results are unchangeable, which would increase user trust. Securevote also uses many of the technologies described earlier, such as “encryption” (Securevote, 2025), to ensure the most secure voting experience for its users.

Ultimately, platforms such as Securevote show a proof of concept and help build the case that blockchain technology can be used to reduce Internet censorship in China.

Potential Limitations of Implementation in China

There are many potential limitations that could inhibit the implementation of a Chinese blockchain network. Practical limitations would reduce the effectiveness of the implementation of the network. The first practical challenge that would be faced would be the inability to use the technology. As described throughout this thesis, blockchain technology is complex and requires a high degree of understanding. While individual citizens would not need to have knowledge of the technology being used, they would still need to understand how to use the network. It would be extremely important for the platform to have an easily understandable user interface, as this would make the technology available to the many citizens as possible. It would also be beneficial to have a network that is culturally made for Chinese citizens. Having potential users help make decisions on the design and many aspects of the network would allow for the best possible implementation and likely increase the user base. Voting systems described earlier would be usable in this scenario, along with surveys given to potential users before their implementation. Another practical issue that could potentially be faced during implementation is a lack of access to the Internet. Most blockchains "can be accessed by anyone on the Internet" (Xu et al., 2019). While Internet access is not always required to access a blockchain network, most networks do require Internet access for users.

Figure 2 - Internet use and penetrations rate in China



Internet use in China

Total Internet users and Internet penetration rate in China from 2017-2022

While Internet penetration is high at 74.4% in 2022, there are still many citizens who wouldn't have access to the network. Therefore, it would be important to ensure that all potential citizens who desire access also have Internet access. This endeavor would likely be independent of the implementation of the blockchain network, but important nonetheless. Ultimately, practical challenges would provide possible limitations to the implementation of the network.

Another potential challenge that the implementation would face would be the probable CCP efforts to reduce the effects of the blockchain network. As described, the CCP has

historically taken efforts to reduce the effects of freedom of speech through its methods of Internet censorship. It can therefore be reasoned that the implementation of a blockchain network would be compromised by government actions. With the technological capabilities of the CCP, the government would likely have the resources to discover methods for reducing the effects of blockchain technology. While some aspects of the technology would remain, it is currently unknown if a network would be able to survive long-term attacks by the CCP. Citizens who would potentially use the network may be turned away due to the punishments historically given to those who speak out against the CCP. It can be reasoned that any citizen found using the potential network to spread anti-government information would be punished similarly. The government would likely try and use any potential punishments to make an example out of citizens who go against them. While this may turn users away, citizens with a desire to spread anti-government information in a secure way would likely still use the network. Ultimately, the ability of the CCP to improve technology and punish dissidents could reduce the impact of the potential Chinese blockchain network.

Metrics for Measuring the Success of the Implementation

To measure the success of the implementation of the blockchain network, metrics would be used. The number of users would be the first metric used, as it would be able to show if the network were actually being used to reduce Internet censorship. If the number of users is below the desired amount, then the implementation will have failed. Another metric will be the number of transactions occurring on the network. This will show how much the network is actually being used, more than just the number of users. If the network is not being used to its full extent, then this will provide more opportunities for improvement and learning. The usage of the network

will also provide an idea of the success of the actual implementation of the network. Along with numerical metrics measuring the success of the implementation, surveys about the sentiment of users could be used. Gaining actual user feedback would give a better understanding of the success of the implementation. The final way of gaining feedback on implementation success would be to interview users to gain qualitative data about the success of the implementation. This qualitative data would provide feedback on room for improvement and whether or not the overall implementation is a success. However, votes through the DAO would also be a good way to see room for improvement.

Chapter 4: Conclusion

The CCP has put in extensive resources towards its censorship efforts throughout the country's and the Internet's evolution. From Mao Zedong's era of total media control to Xi Jinping's Internet governance, it is clear that censorship by the Chinese government is important to their control over their citizens. The CCP manipulates information on the Internet through technologies such as deep packet inspection, keyword filtering, and AI-driven moderation. These are all used to suppress dissenting voices and ensure that all opinions in the country are those of the government. Blockchain technology is a potential solution due to its decentralized nature. Blockchain has core attributes such as immutability, decentralization, pseudonymity, and transparency that make it a possible solution. Technologies such as smart contracts, public key infrastructure, oracles, and DAOs improve their ability to be a potential solution. However, there would also be significant challenges to implementing a blockchain network in China, including the CCP's ability to improve technologies to adapt to threats, limitations of blockchain technologies, and practical challenges. Ultimately, the flaws of the technology and potential implementation do not combat the benefits it would provide to Chinese citizens. Therefore, it can be reasoned that blockchain technology is a potential solution to Chinese Internet censorship.

Chapter 5: Areas for Further Research

This thesis focused entirely on the potential implementation of a blockchain network in China. However, other dictatorships such as Turkmenistan and North Korea face similar challenges to free speech and therefore could also potentially benefit from the implementation of blockchain networks. While the necessary research is outside the scope of this thesis, similar analyses of the history of Internet censorship in those countries could be conducted, and conclusions could be drawn.

Other potential research would require the implementation of the network. If a network were to be implemented, research into its success using the metrics discussed would be crucial. It is likely that the network would need to be improved as well as its security due to threats of government interference. Therefore, field research into the success of the implementation as well as steps for upkeep and improvement would prove to be vital.

Bibliography

Bauer, F. L. Entzifferte Geheimnisse: Methoden und Maximen der Kryptologie. Springer, 2000.

Brady, Anne-Marie. Marketing Dictatorship: Propaganda and Thought Work in Contemporary China. Rowman & Littlefield, 2010.

Cai, Ning, et al. "Research on the Analysis and Governance of Internet Public Opinions under the Environment of SelfMedia." Office Informatization, 2022. Translation.

Chainspect. "Solana vs BNB Chain [TPS, Max TPS, Block Time] | Chainspect." Chainspect, 2020, chainspect.app/compare/solana-vs-bnb-chain. Accessed 17 May 2025.

Chainspect. "Solana vs Ethereum [TPS, Max TPS, Block Time] | Chainspect." Chainspect, 2020, chainspect.app/compare/solana-vs-ethereum.

China's Censorship of the Internet and Social Media: The Human Toll and Trade Impact: Hearing before the Congressional-Executive Commission on China, One Hundred Twelfth Congress, First Session, November 17, 2011. U.S. G.P.O., 2012.

Choo, Kim-Kwang Raymond, et al. Blockchain Cybersecurity, Trust and Privacy. Springer, 2020, https://doi.org/10.1007/978-3-030-38181-3.

Claburn, Thomas. "China's GitHub Censorship Dilemma." Information Week, 30 Jan. 2013.

Descamps, Maud. "China's Cybersecurity Legislation: A Paper Tiger or an Institutionalized Theft?" Institute for Security and Development Policy, Focus Asia: Perspective and Analysis, May 2020.

Economist. "As Censorship in China Increases, VPNs Are Becoming More Important." 30 June 2022.

Freedom House. "Freedom on the Net 2021." Freedom House, 2021.

Gayvoronskaya, Tatiana, and Christoph Meinel. Blockchain: Hype or Innovation. Springer, 2021, https://doi.org/10.1007/978-3-030-61559-8.

Gewirtz, Julian. Never Turn Back. Harvard UP, 18 Oct. 2022.

Gov.cn. A Great History of the People's Republic of China (1989), 9 Oct. 2009.

Green, Kieran, et al. Censorship Practices of the People's Republic of China. Exovera, CIRA, 2024.

Huang, Yongpeng. "Expelling Rumors amid the Epidemic According to Law." Xinhua, 18 Feb. 2020. Translation.

Hunan Provincial Department of Finance. 2023 Budget Explanation for the Chinese Communist Party Committee of Hunan Province Cyberspace Affairs Commission General Office. Translation: Chinese Communist Party Liuyang Municipal Committee Cyberspace Administration, 2020.

James, Adam. "Ethereum's 13,900 Nodes Are Running 1 Million Validators, with 26% of the Supply Staked." The Block, 28 Mar. 2024, www.theblock.co/post/285262/ethereum-one-million-validators.

Jiang, Ying. Cyber-Nationalism in China: Challenging Western Media Portrayals of Internet Censorship in China. The University of Adelaide Press, 2012.

Knockel, Jeffrey, et al. "We Chat, They Watch: How International Users Unwittingly Build Up WeChat's Chinese Censorship Apparatus." Citizen Lab Research Report No. 127, May 2020.

Kuo, Lily. "'They're Chasing Me': The Journalist Who Wouldn't Stay Quiet on Covid-19." The Guardian, 1 Mar. 2020.

Mattingly, Daniel C. The Art of Political Control in China. Cambridge UP, 2020, pp. 184–90.

Mao, Yunmei, and Wang Juan. "Establish a Team of University Online Commentators Who Are Politically Firm and Professionally Skilled." China Higher Education Magazine, 18 Apr. 2016. Translation.

Mozur, Paul, Muyi Xiao, and John Liu. "'Breach of the Big Silence': Protests Stretch China's Censorship to Its Limits." New York Times, 1 Dec. 2022.

Ni, Vincent. "'They Were Fooled by Putin': Chinese Historians Speak Out against Russian Invasion." The Guardian, 28 Feb. 2022.

Pan, Shuqiong. "Establishing a Three-Level Internet Information System to Lay a Solid Foundation for Ideological and Theoretical Work—Tianjin Actively Explores Internet Information Work Methods." Cyberspace Administration of China, 12 Nov. 2018.

Reynolds, Sam. "S&P Global Just Made Ethereum's Centralization Risk a TradFi Concern." CoinDesk, 22 Feb. 2024, www.coindesk.com/markets/2024/02/22/sp-global-just-made-ethereums-centralization-risk-a-tradfi-concern. Accessed 17 May 2025.

Schrepel, Thibault. Blockchain + Antitrust: The Decentralization Formula. Edward Elgar Publishing, 2021.

Secure.vote. "SecureVote | Secure, Reliable Blockchain Voting." Secure.vote, 2018, secure.vote/business-and-government/. Accessed 19 May 2025.

Seth, Shobhit. "Public, Private, Permissioned Blockchains Compared." Investopedia, 29 June 2021, www.investopedia.com/news/public-private-permissioned-blockchains-compared/.

Shen, Meng, et al. Blockchain: Empowering Secure Data Sharing. Springer, 2020, https://doi.org/10.1007/978-981-15-5939-6.

Solanacompass.com. “Solana Decentralization Dashboard: Just How Decentralized Is Solana, Really?” Solanacompass.com, 2023, solanacompass.com/statistics/decentralization. Accessed 17 May 2025.

States United Democracy Center. “Tracking Attitudes about Elections and Political Violence over Time.” States United Democracy Center, 16 Aug. 2024, statesunited.org/resources/over-time-survey/.

“Top 15 Layer-1 (L1) Crypto Projects to Watch in 2025.” KuCoin Learn, 6 Jan. 2025, www.kucoin.com/learn/crypto/top-layer-1-blockchains-to-watch.

Trautman, James. “BNB Chain: The Evolving Juggernaut.” Messari.io, 30 June 2022, messari.io/report/bnb-chain-the-evolving-juggernaut.

Wade, Samuel. “Minitrue: No Tanks or Candles during Special ‘Network Control Period.’” China Digital Times, 3 June 2022.

Wang, Xianfu. “Make Online Public Opinion Work the Top Priority of Propaganda and Ideological Work.” People's Daily Online via CPC News, 31 Oct. 2013. Translation.

Xi, Jinping. “Improve the Comprehensive Internet Governance System and Create a Good Network Ecology.” Red Flag Manuscript, 15 Jan. 2023.

Xie, Xinzhou, and Li Jialun. “A Brief History of Macro Policy and Basic System Development of Internet Content Management in China.” Journal of Information Resources Management, 2019.

Xie, Xinzhou, and Zhu Yaoying. “Research on the Development Trends and Response Strategies of Online Content Governance.” Journalism and Writing, 2020. Translation.

Xu, Xiwei, et al. Architecture for Blockchain Applications. Springer, 2019, https://doi.org/10.1007/978-3-030-03035-3.

Xu, Xueyang, Z. Morley Mao, and J. Alex Halderman. “Internet Censorship in China: Where Does the Filtering Occur?” International Conference on Passive and Active Network Measurement PAM 2011, 2011.

Xue, Ziyu, et al. “Public Opinion Guidance Methods, Devices, Equipment and Computer-Readable Storage Media.” People’s Republic of China Patent No. CN202011147501, 8 May 2020.

Yang, Fengning. “Analysis of the Difficulties and Countermeasures of Government Network Public Opinion Management in the New Media Era.” Advances in Social Sciences 11:9 (2022). Translation.

Zhang, Yanping. “Hebei Completes ‘Six Major Events’ and Creates ‘Three First-Class.’” New Media, 2019:2 (2019).

Zhong, Raymond, et al. “No ‘Negative’ News: How China Censored the Coronavirus.” New York Times and ProPublica, 19 Dec. 2020.

Zhuang, Sylvie. “How Online Searches for ‘Ukraine’ and ‘Taiwan’ Are Censored in China: Study.” South China Morning Post, 28 Apr. 2023.