Study Proposal

Team Member：

BIYING YAO   YINING LI   JINGRU HU   RUIYUAN YANG

Abstract
An artistic attempt to create a more democratic cyberspace, based on cryptography, by encrypting user information and data.

Keywords
Decentralization, Crypto-anarchism, Cryptography, Semeiology

Research questions
The key issue that needs to be addressed is the disappearance of the boundaries of power over personal data brought about by centralisation. In a centralised system, the system platform operator, has access to all your data in the background. In order to gain commercial benefits, platform parties without self-control will take this data out and apply it commercially, they sell it and sell it to the corresponding service providers.

We need to guarantee the anonymity and equality of users and strengthen the technical protection of individual privacy. For example, addresses cannot correspond to real identities, address generation is done locally and does not contain any information about the real identity of individuals. The IP address of the sender is protected from disclosure by the fact that the IP of the source of the new message cannot be determined by other nodes through the network's radial distribution.

Inspiration
There is main two things that inspired us of Crypto-anarchism. One is for IP dependencies, on Weibo as well as WeChat which were China's two most-used social media platforms, were introduced in the first half of 2022 to display users' IP dependencies in accordance with state policy.

As users use theses internet platform, this IP locality is like a giant label on every user's face. Though this tag can be circumvented and misleading by turning on a VPN. But over the course of the experience, IP dependencies become an abomination. For example, when a user

comments on a specific news event, his or her IP address can easily be targeted by people who disagree with him or her. IP users overseas, for example, are often referred to as 50W (defined in China's online environment as those who seek to undermine national sovereignty and endanger national security). In addition, users often feel that their power becomes a commodity of digital capitalism, and that all their data becomes a bargaining chip for the platform. Like, our search history on shopping platforms will eventually return to us as part of our social media advertising. That's why we interested in this topic.

Analysis of Literature and theories

We combine semiotics and cryptography to research and guide our way of creating output. During our research, we selected the two works of two artists for a detailed interpretation: Nestor Siré - Virtual/Reality: Digital Media Goes Offline[1]


1-1

In Cuba, led by a highly centralized government, the Internet is a near-luxury for two main reasons:1. Strict censorship 2. The fee to Internet is incredibly expensive. So that in Cuba, the internet is not the first choice for information dissemination. In Siré's practice, he chose to use physical communication to circumvent Cuba's strict system of monitoring the flow of information on the Internet. In the "Communications Network" he created, a group of people download information from the Internet and also the TV, international channels and then

---

[1] Proximamente – Néstor Siré (nestorsire.com)

share them. It is shared by hand. A very physical way of distributing digital material offline. But in this context, another thought arises: when we don't have other forms of consuming media, is it necessary to pay for copyright?

Erik Bordeleau - The Sphere As Speculative Gesture[2]
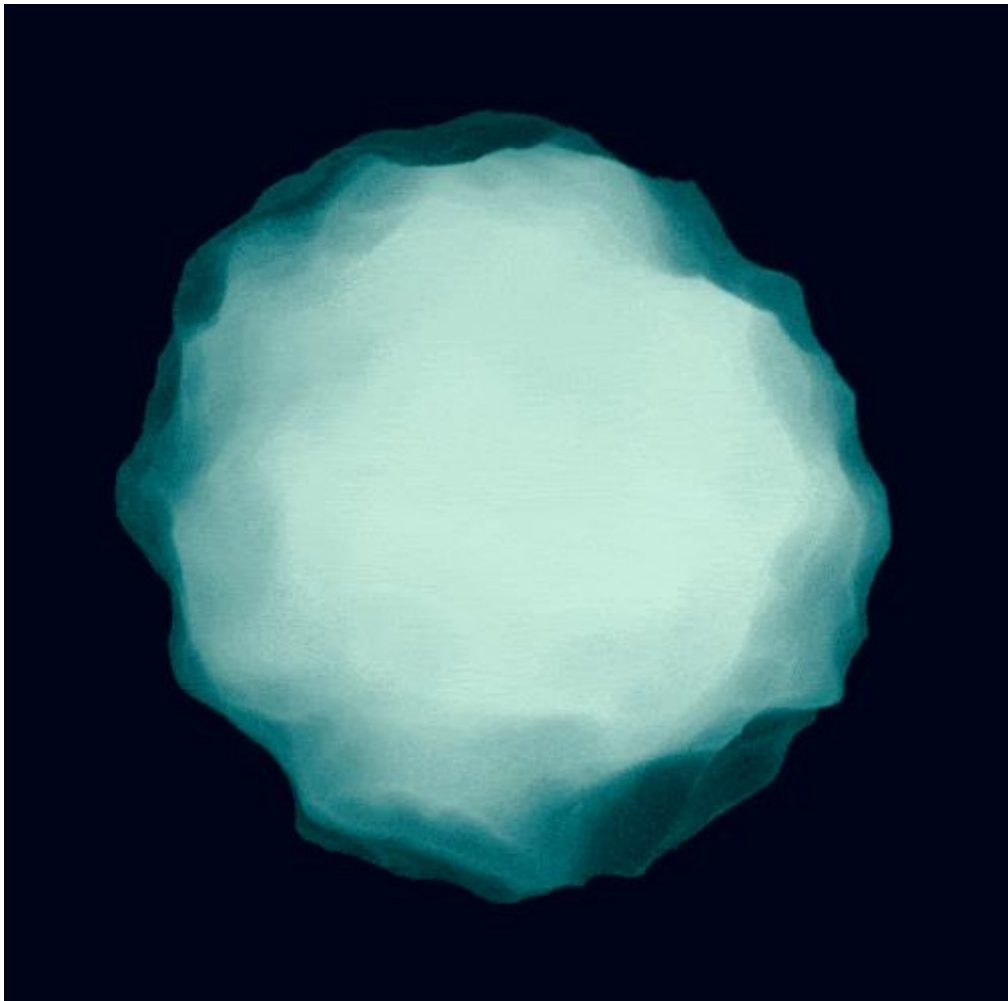
2-1

The Sphere, an interdisciplinary sphere as a speculative gesture, is a Creative Europe-funded 'Network 3.0 Infrastructure' project developed for the self-organisation of the performing arts. the Sphere focuses on how to integrate creators, producers and the public into an emerging ecosystem that promotes, in a speculative spirit alignment of interests and purposes.

---

[2] The Sphere As Speculative Gesture | Weird Economies

How to change traditional models of value capture and reopen them for the benefit of communities, and how to translate economic cycles into social and artistic flows are all questions to be considered. Under anarchist leadership, the old, bad ways of organising in the past should be discarded and the way we create new models of techno-social coordination becomes truly crucial in a world moving towards social fragmentation.

In essence, the whole human social organism -- in which social policy, the laws of economic operation, and order are all interlinked and restrained, like a distorted, circular system, the post-digitization phase would give the system more meaning than that. In our traditional way of thinking, numbers are unconscious, mindless matter, but in this case, numbers, or the economy, are given a soul by the creator.

Research Methodology

The methodology we use is cryptography, which is a tool that can put all the infromation together and combine them with specific scenarios to solve problems. Memorise cryptographic tools in a coherent way, then analyse them in relation to specific scenarios, corresponding to which security analysis is committed, model security, balance performance and security, design protocols and solve problems.

Research Plan

Artefact:

We would create a virtual environment which was based on the leading of Cryptography. Through encrypting and transforming user data with the encryption system we design, we ensure the perfection of users' privacy right, and we will ensure its open source to enable everyone participate equally in the management and maintenance of the data, reducing the information gap, data information will no longer be centralised, thus preventing the platform party from selling user data to others, strengthening the technical protection of individual privacy rights, while increasing the rights of users and avoiding the traditional centralised model where platforms can delete and control the exposure of user content at will.

Document:

Recording thinking process:

By collecting research and reading materials in the corresponding field, organising them in writing. And gathering visual materials for previous artists' ideas.

Recording design process:

We would take video to record our design process. Make sure all the experimental attempts would be recorded.

Recording debug and iteration process:

We would create a repository in GitHub to make sure every iteration of the code would be saved. Meanwhile, each of our team members can participate in group activities fairly and guarantee everyone's initiative of propose - modifications.
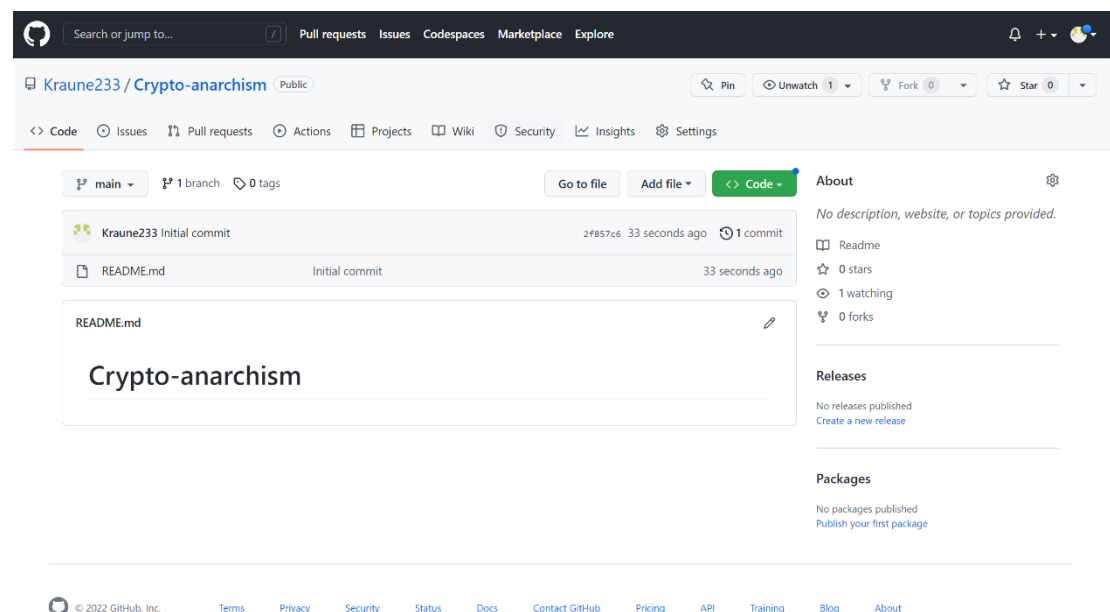
3-1

Timeline:

11.01-11.07

Identify the concept of the theme, Gathering possible used materials.

Brainstorm

11.07-11.13

Secondhand Research: brainstorming based on the work of other artists in similar fields.

Study proposal Finished.

11.14-11.20

Determine the specific direction and form of implementation of the concept, make sketches, simulate the prototype of the installation or graphic representation, search for relevant code examples, try to combine them and document the process.

11.21-12.11

Enter into a concrete experimentation session to determine the concrete output through continuous experimentation.

Iterate through design-code versions, identifying possible gaps in the research process and refining them. Complete the final product. Complete the final output.

Bibliography

[1] Craig Jarvis. 1992–1998. "Cypherpunk ideology: objectives, profiles, and influences in the Internet Histories", no.6:3, 315-342, DOI: 10.1080/24701475.2021.1935547

[2] Huckle, Steve, and Martin White. 2016. "Socialism and the Blockchain" *Future Internet* 8, no. 4: 49. https://doi.org/10.3390/fi8040049

[3] Nofer, Michael, Peter Gomber, Oliver Hinz, and Dirk Schiereck. 2017. "Blockchain." Business & Information Systems Engineering 59, no. 3: 183-87.

[4] Huckle, Steve, and Martin White. 2016."Socialism and the Blockchain." Future Internet 8, no.4: 49.

[5]乔诚, 张岩, and 耿文涛. 2015. "大数据时代读者隐私保护研究." Nongye Tushu Qingbao Xuekan 27, no. 8: 77-79.

[6]Desmedt, Y. 1988. "Society and Group Oriented Cryptography: a New Concept. " Lecture Notes in Computer Science, vol 293. Springer, Berlin, Heidelberg. https://doi.org/10.1007/3-540-48184-2_8

[7]Benny Applebaum, Yuval Ishai, and Eyal Kushilevitz. 2006. "Cryptography in NC0" SIAM Journal on Computing 36:4, 845-888

[8]Nissenbaum, Helen Fay. 2010. "Privacy in Context : Technology, Policy, and the Integrity of Social Life. " Stanford, Calif.: Stanford Law Books.

[9]Ferguson, Niels., Tadayoshi. Kohno, and Bruce Schneier. 2010. "Cryptography Engineering Design Principles and Practical Applications. " Indianapolis, Ind.: Wiley.

[10]Welsh, Dominic. 1989."Welsh, Dominic. Codes And Cryptography // Review." Scientific American 260, no. 5: 145.

[11]Schneier, Bruce. 2015. "Applied Cryptography : Protocols, Algorithms, and Source Code in C. " Second Edition, 20th Anniversary ed. Indianapolis, IN: John Wiley & Sons.