

WHITEPAPER

Version 1.06 – May 1, 2021

Connecting everyone personally, financially,
privately and securely – powered by the Blockchain

Contents

- Intoduction 01
- Our solution 13
- Benchmark analysis 16
- Sappchat's application and platform 23
- Sappchat's Token Sale 29
- Roadmap 34
- Tokenomics of the APP reward model 38
- Disclaimer 41

Chapter I:

INTRODUCTION

- Market Analysis of Mobile Messengers, Payment and Financial Applications
- Data Privacy Concerns
- Global use = Global concerns



1.1 Market Analysis of Mobile Messengers, Payment and Financial Applications

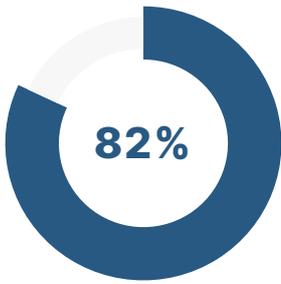
Mobile applications have become an integral part of today's phones that contain multimedia features such as text/audio/video chats, group chats, message notifications, status updates, and media sharing. The average smartphone user spends **82 percent** of his/her time on email communication, social interaction, and entertainment. Smartphones are an integral part of lives in the 21st century, with **more than 3.5 billion** mobile phone users worldwide.

Due to its characteristics, the use of mobile applications exceeds the use of social networking websites, with the most prominent applications being **WhatsApp** (with over a billion users), **WeChat** (with more than 900 million Chinese users), **Facebook Messenger** (over 1.3 billion users) and **Viber** (with 800 million registered users and 260 million active users) (Quintas de Arcanjo, 2019).



Figure 1 – Most popular mobile instant messenger apps, based on number of active users.
Source: Quintas de Arcanjo, 2019.

The development of **Mobile Instant Messaging (MIM)** applications addressed the problems of former generations of mobile phones, in which text and media communications were based on SMS and MMS messages, expensive and limited in size and content. These applications had similar features as those of desktop-based instant messengers, but the portability of mobiles signified a new renaissance for them – as mobiles make virtually any user of the MIMs accessible anytime and anywhere.



This path of development and innovation led to the exchange of vast amounts of textual, visual, audio and video information, as well as files, via MIMs. To illustrate the central role of MIMs and similar mobile forms of communication in our lives, research shows that the average smartphone user **spends 82 percent of their time** on email communication, social interaction, and entertainment (Matemba and Li, 2018).

With the technological and user-oriented progress of MIMs, new features were gradually introduced into them: users of MIMs can see if messages are received and read, different groups of users can be contacted with ease and group voice and video calls are available in addition to text messages. Therefore, it is not surprising that the use of MIMs exceeds the use of social networking websites due to their engaging characteristics, popularity, accessibility and ease of use.

Among the hundreds of different solutions available to MIM users on Android and iOS mobile phones, the most popular MIMs in the market are Facebook's WhatsApp and Facebook Messenger, Tencent's WeChat and QQ, Telegram, Snapchat and Viber (see Fig. 2 for the leading platforms).

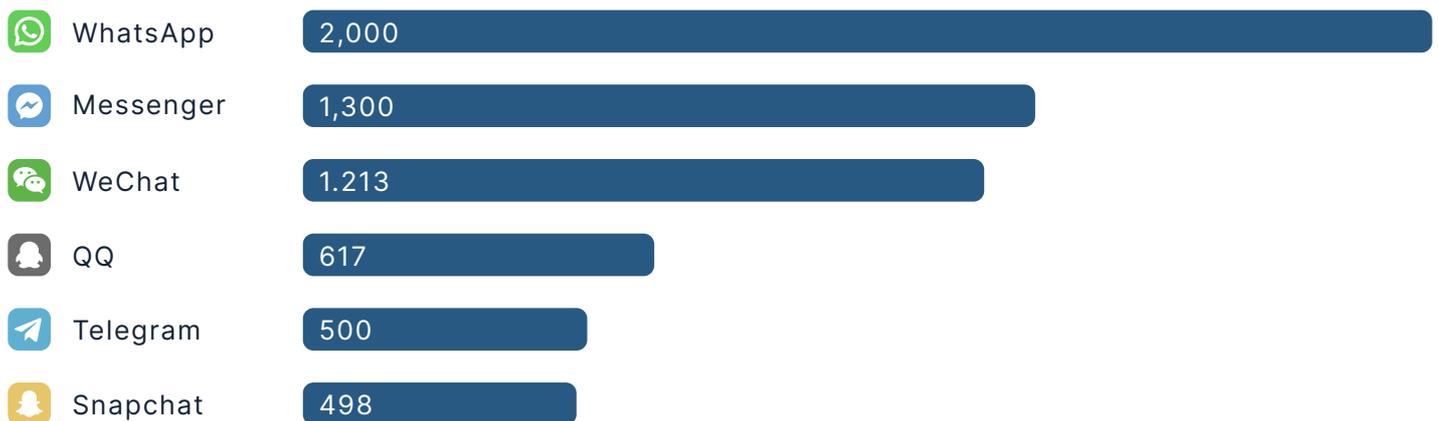


Figure 2 – The number of users (in millions) of the most popular MIMs in January 2021.
 Source: <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>

Beyond its dominance in the MIM market, **WhatsApp** is probably the most used application on mobiles. Over two billion people worldwide use it for free messaging, calls, and media use and the application is widely adopted in the Middle East and in South-East Asia (Rastogi and Hendler, 2017; Dev, Das, Rashidi, & Camp, 2019; Fig. 1.2). In particular, **WeChat**'s main market consists of Chinese mobile users with substantial growth of its user base from 900 million active users in April 2017 to over 1.2 billion users in January 2021 (Tsai and Men, 2018; Fig. 1.2). Applications with a smaller user base, such as **Viber**, are popular in particular regions. Viber is especially used by mobile users in Eastern Europe, Russia, the Middle East and in some Asian markets.

In addition to their use as communication platforms, MIMs were expanded into mobile payments and financial services (or at least examined this option). With payment services becoming more accessible to all users, as banks are willing to provide mobile solutions to their customers and to attract new and younger customers, mobile users become more comfortable using their applications for payments and money transfers. While the majority of uses are via e-banking applications, MIMs began to integrate financial services to their chat features. **WeChat** combined RMB transfers and payments into its ecosystem. Facebook was looking into issuing the Blockchain-based **Diem (formerly Libra)** token for its WhatsApp and Messenger applications (but so far has failed to do so, due to lack of support from its partners). Telegram's **TON** cryptocurrency token was prohibited by the U.S. Court from use on its MIM, causing the company to abandon further development of the project.



Diem



WeChat Pay



TON

These technological advances were facilitated in part by the decline in the number of MIM downloads, due to the propensity of users to have fewer apps on their devices. Hence, incorporation of money transactions and payment systems into existing messaging apps could help users reduce the variety of applications on their mobiles, to save storage space and encourage users to keep a MIM of their choice on their devices for longer periods.

To illustrate the success of MIMs as platforms for payments and money transfers in China in addition to their online communication features, the volume of money transactions via mobile applications in 2016 exceeded 9 trillion USD in China, while in the U.S. it was only 112 billion USD (Liu, 2019). The use of Chinese mobile payment systems, such as **Alipay** and **WeChat Pay**, is so widespread such that their users range from beggars to lenders and even criminals.

In many respects, MIMs are solid candidates for integration of payment and money transfer systems. The reasons for this form of integration are as follows:

1 MIMs provide multiple channels for transferring messages, files and data and payments and money transfers can accompany these existing feeds.

2 Usually, payments and money transfers are not carried out in void. Sending money from one person to another (or paying for services and goods) is accompanied by text, audio and video messages and files, such as payment requests, specifications, confirmation of payment, etc. By integrating payments or money transfers with the communications surrounding it, users can establish searchable references to money transfers and refer to them in future discussions.

3 In many cases, payments and money transfers are made to existing contacts (such as family, friends, contractors, employees, etc.) after discussing them the transfer. The payments and money transfers are thereby extensions of prior communication and can be completed from the same platform with ease.

4 MIMs are mature media platforms for engagement with new and existing customers, audience acquisition and partnerships for public relation purposes. Additionally, workplace MIMs (such as Slack) allow companies to get in touch with their employees anytime and anywhere. Though the use of professional MIMs within companies or corporations it is not yet fully established, employees communicate between themselves via personal MIMs, such as WhatsApp and WeChat. Although these platforms are targeted at interpersonal communications, through exchange of text, voice and multimedia messages between individuals, they do not directly involve the company or its guidelines in terms of knowledge sharing, data distribution and often cyber-security (Tsai, & Men, 2018).

In line with the development of mobile applications, MIMs represent broad ecosystem that connects users with brands, customer relationships and brand-related contents. However, MIMs lack integrated solutions for online shopping and payments to capture the complete purchase cycle from customer engagement through product/service selection, shopping cart management and, finally, paying for the selected goods. WeChat is the exception, as it provides rich multimedia capabilities, business tools for customers and businesses, payment and e-banking features, so that users can not only interact with companies but also make payments to businesses and carry out bank operations along with instant messaging. WeChat has a range of features beyond traditional text messaging: asynchronous chat, photo sharing, video sharing, synchronous voice, video chat, and location sharing. This application also allows multiple payment options, from sending money to friends to

paying bills. In this respect, WeChat can be viewed as the "missing link" between e-commerce and social media communications. Yet, its complete set of WeChat's features is available only for Chinese users (Yang, Chen and Li, 2016).

To compare, WhatsApp supports only interpersonal communications (either on a small scale or to broad groups of up to 250 users). WhatsApp provides options for person-to-person conversations, ad-hoc discussions, and larger structured groups. However, WhatsApp does not provide any payment, money transfer, online shopping or banking features. The application is very popular in several non-western countries, primarily Saudi Arabia and India, where it is also the dominant social networking platform, beyond being the leading MIM. Interestingly, the use of WhatsApp is so widespread and intensive in Saudi Arabia and in India that it is frequently in the topics of national debates whether the platform spreads misinformation, encourages violence or is used to coordinate organized crime activities. On the other hand, WhatsApp is broadly used in both countries in information exchanges in telemedicine and it is considered a major communication tool in supporting patient-to-doctor and doctor-to-doctor communications (Calleja-Castillo and Gonzalez-Calderon, 2018).

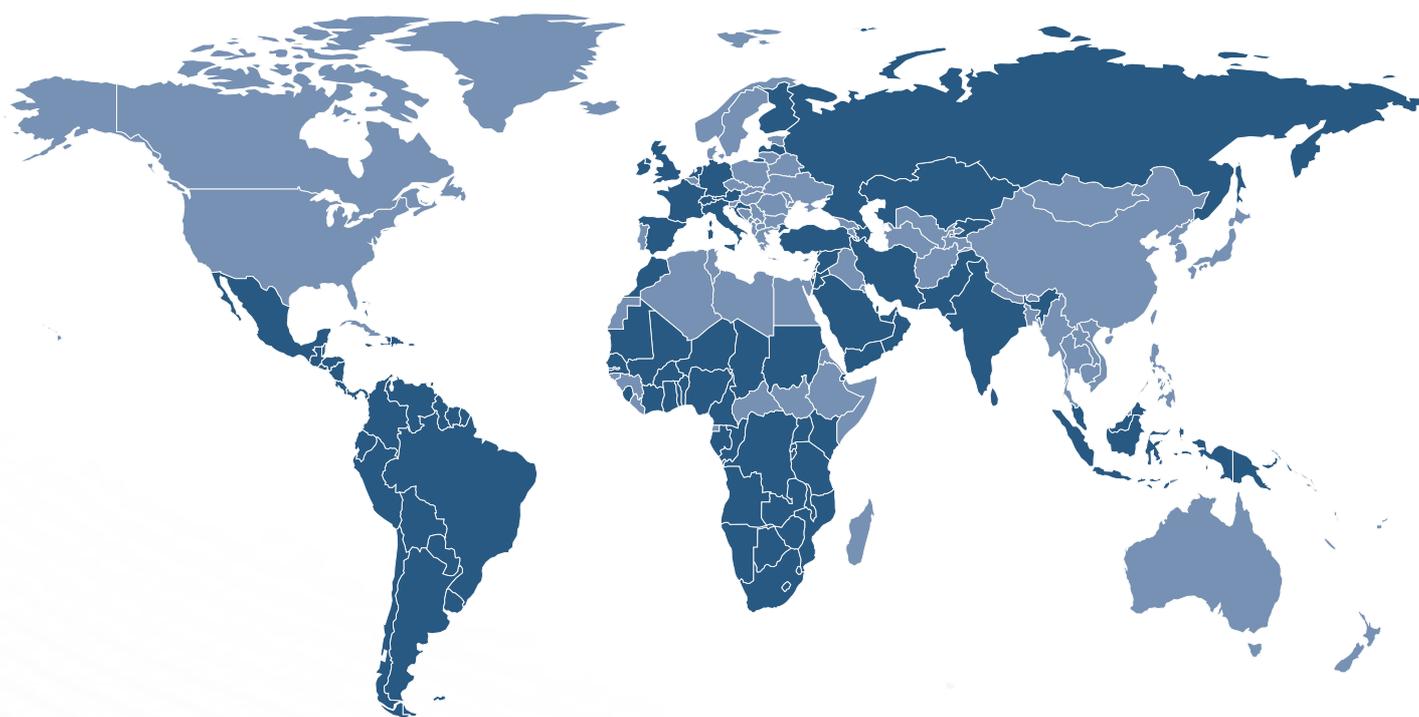


Figure 3 – • Countries or territories with the most WhatsApp users in December 2019.

Source: <https://www.businessofapps.com/data/whatsapp-statistics/>

WhatsApp expanded the capabilities of its messaging app to a business-oriented application called WhatsAppBusiness. This app allows companies to develop closer interaction with their customers by sending messages via a chatbot-like app. Similar features were implemented in Facebook Messenger for company-to-customer interactions. On average, over 20 billion messages are exchanged each month between customers and companies through it (Quintas de Arcanjo, 2019).

1.2 Data Privacy Concerns

Information privacy is defined as the ability to control information about oneself and determine when and for what purpose such information can be accessed by others (Jozani, Ayaburi, Ko, and Choo, 2020). However, today it seems that no communications and financial operations are private and safe anymore. Technological developments in recent years have significantly changed the concept of privacy, increased the value of collected data, intensified data collection efforts and raised burning issues regarding the role of third parties, the degree of user involvement in privacy settings and the commercialization of user data. For example, the Cambridge Analytica scandal in which Facebook users' data was utilized for political purposes demonstrates the threats of massive collection of publicly shared and private data. Given the large scale of data exchanges in communications, the contents shared on these platforms can attract a wide range of individuals, third organizations and especially government agencies. However, when deciding to disclose data or to chat online, users are often unaware of the threats and potential misuse of private data, either by online marketers or by oppressive regimes. Moreover, in the context of mobile applications, the disclosure of user data is supplemented by rich data that is generated on the device - device ID, user location and contact list and other data that constantly monitor the activities of their users. This variety of data can further affect the privacy of users (Jozani, Ayaburi, & Choo, 2020). Without being aware or allowing it, health records, social security numbers or financial data on purchases or eating habits is still exchanged and discussed by the doctors, the bankers or the restaurants that serve users via MIMs (Sheehan and Hoy, 2000; Smith et al., 2011).



Practically any mobile messaging application transfers our most private messages to the servers of the companies that operate them, where our text messages, photographs, audio and video recordings and feeds are processed, mined and analyzed by advanced algorithms that have only one aim – profiting the company at the expense of our most private moments and more generally – our lives.

Once we click the "record" or the "send" buttons, the contents are not within our control. Company employees can view and read them. AI can process them to offer us advertisements literally in every online channel, and data about us can be sold to other parties. Further, governments worldwide eavesdrop on our most private conversations as a part of the terms that allow mobile messaging companies to operate within their borders, and messaging in oppressive regimes can cost a person's freedom.

The ecosystem of mobile banking applications that currently provide the main solution for payments and money transfers is significantly different from that of MIMs, as the security of payments and transfers, as well as secure authorization to the bank account for these operations, are the major concerns of the financial institutes that offer them to customers. Yet, mobile payments, money transfers, and shopping applications are not excluded from these types of privacy violations in most countries worldwide. Financial institutes are successfully hacked and data are distributed online or sold through the Darknet. Uploading lists of credit card details and other payment methods to the Internet has become the norm. Banks are required to disclose any data on customers and transactions to/from their accounts should any government agency desire to receive them. Both banking applications and payment applications do not enable anonymous transactions (such as bank transfers or payments to product or service providers that can embarrass the users – such as doctors, psychologists, etc.). In banking applications, user data are transmitted to the bank to carry out the operations provided by the application. In mobile payment applications, it is necessary to provide communication technologies to and from the buyer's and the seller's devices and to transmit the user's data to approve the transaction. Both types of applications require a secure communication channel through which data reaches the Internet from the device or transmitted to it (i.e. a mobile signal or through a wireless connection).

Indeed, operating systems designed for smart mobile devices have introduced a number of different security measures and mechanisms to reduce the risk and to eliminate vulnerabilities and official app stores implement measures to prevent malicious applications that do not meet the required security standards to be offered to end-users. Nonetheless, data thefts, hacking into mobiles and personal photo thefts take place on a large and growing scale. Additionally, some of the currently most popular applications, including social networks, use a range of sensitive data collection tools and methods, such as identity profiling and location collection and analysis, as part of their strategies and business models. Therefore, it is important that applications take all measures to protect data privacy of users that entrust their personal details and broad aspects of their lives to them.



In addition to the vulnerabilities of personal data in mobile phone communications, corporate and business data and communications are vulnerable as well. Devices issued by companies or private devices used for business purposes may serve as targets for industrial espionage, eavesdropping and unauthorized data retrieval for profit. End-to-end encryption (E2EE) that converts the original message into encrypted formats that can only be decrypted via private keys on the phones of recipients (so data cannot be retrieved from proxy servers) was introduced as a solution to this problem, but was implemented only by a fraction of the MIMs (Calleja-Castillo and Gonzalez-Calderon, 2018).

Data misuse is of particular concern when it comes to applications used for payments. For example, Venmo is a social payment app where a P2P payment feature allows mobile phone users to easily share accounts and transfer money to friends and to vendors. Its social features allow users to share notes, emojis, comments, likes and reactions to other transactions on the platform, encouraging social engagement. However, all transactions are public by default, unless users intentionally change their settings to private or accessible only to friends. To use the app, users must grant Venmo access to their contact list, media files, camera and device ID and must provide a valid phone number, complete personal information (e.g., Social Security number, date of birth and driver license) and their credit or debit card information. The application stores data on user transactions and their social activities with time-marked geolocation data. Personal and financial data collected by Venmo and social feed applications can therefore reveal the lifestyle and habits of their users either to Venmo itself, to third parties or to the government (Zhang et al., 2017).

1.3 Global use = Global concerns

Much research and the discussion on data privacy and the use of MIMs have focused on "WEIRD" - Western, Educated, Industrialized, Rich and Democratic populations. However, similar concerns were found in different parts of the world, including Middle Eastern and developing economies (Dev, Moriano and Camp, 2020). For example, studies conducted in Saudi Arabia and in India found that both Saudis and Indians were concerned about adding them to WhatsApp groups without their consent, with Saudis mostly being more concerned about the private life aspects of it and Indians concerned over work related aspects. Gender has proven to be a significant variable in the perception of privacy risks and concerns. Although both sexes are equally prone to invasion of privacy, women tend to have greater privacy concerns and enforced privacy-preserving behavior, mostly in patriarchal societies (Dev, Moriano and Camp, 2020).

The growth in the use of MIMs, payment, money transfer and banking applications has caught the attention of attackers, who take advantage of online store flaws for apps, uploading malicious program codes or their own app clones that endangered the privacy and security of users and their financial assets.

Some of the reasons why the volume of attacks on mobile devices increases are the relative ease of obtaining personal and use data from the device and the exponential growth in carrying out banking transactions, payments and money transfers via apps. The aim of the attacks is to gather access data and to gain control over these applications to steal funds from their users.

Nowadays, payment services are more accessible to all users. Banks to offer mobile payment, money transfer and banking solutions and attract new and younger customers while maintaining the existing ones. However, some of the cybersecurity risks emerge from lack of adequate integration of traditional banking systems and less secure and reliable third-party mobile solutions.

Payment exchange services are relatively slow, as information about the outcome of the transaction is sent and approved by both the sender and the recipient, due to the need for verification of transactions by a centralized body – the bank - which is primarily responsible for validating the incoming transactions. This delay in processing the transactions may cause ambiguity and mistrust whether the sender has not executed the transaction as promised, whether the transaction has successfully been completed or has failed, which harm the experience of users and may financially harm companies that depend on incoming money to start processing purchased services and goods in exchange.



To overcome this problem, the Chinese messaging app WeChat has developed a feature that allows users to add their credit card information to their account and make a payment via a QR code to transfer money from the app. However, there were certain restrictions in applying this service - until 2018 WeChat users could associate only credit and debit cards from Chinese banks. Currently, the use of foreign bank cards is allowed only if the application is downloaded within the borders of Mainland China, probably for security reasons.

The use of Big Data technologies in China allows collection of detailed personal data without informing users and collected data can be used for security or for political purposes. The research work of journalists revealed that in China the private and personal data can be obtained without restrictions.

The data collected in China via the use of applications (including MIMs and payment and banking apps) serve a social credit system that monitors and indicates which individuals violate social norms or rules. The government can blacklist them and put restrictions on their daily activities and freedom. If users have good social credit records, they show no opposition to rules and political goals and parties and if they have good social responsibility measures, they receive rewards and incentives from the government (Liang, Das, Kostyuk and Hussain, 2018).

The government has access to billions of user and communication data records collected through mobile apps, giving it insights into the behaviour of individual Chinese citizens, as well as trends in different groups of the population, at any time. The government uses it for various purposes: First, sensitive and compromising data of political opponents is accessible via MIMs and payment applications. Second, the monitoring system that continuously collects and analyses data dictates the distribution of social loans and benefits to citizens that are loyal to the government. Third, the analysis of data leads the government to identifying criminal and corruption acts, such as bribes and violations of various laws. Overall, this ownership of data by the government allows it to capture and to retain additional political, economic and social power.

This reward and punishment strategy also allows the government to decide who can be employed in the public sector and even who can get access to public services or be prevented from receiving them. In this way, the government builds channels for confidential users to access public services, optimizing administrative services and reducing transaction costs. In contrast, citizens on the blacklist receive penalties and restrictions that affect their social, political and economic activities, as well as their well-being. The Chinese government presents its social credit policy as beneficial to citizens. Clearly, by monitoring the activities of users in MIMs, payment and banking apps, the government can enforce its intentions and eliminate potential opposition at the cost of privacy and civil right violations.

To exemplify, the WeChat application monopolizes online communications and payment in China and its operation is necessary for day-to-day life in the country, to the extent that deleting this application essentially means deleting life in China (Chen, Mao, & Qiu, 2018). However, beyond its lightness, accessibility and ease of use lies a darker side – the application, its use and the data are strictly controlled and regulated by the Chinese Communist Party, including monitoring and censoring contents. WeChat defines its role as an effort to improve life in China, but in reality the role of the application maintains the will and power of the ruling party and its privacy policy does not offer protection from government oversight. In protests that took place in Hong Kong against a law passed by the government, WeChat played a key role in blocking news and images of the protests from being distributed to other users (Kharpal, 2019). Additionally, when securing user data and their privacy was evaluated, WeChat received 0 points out of 100 (Grigg, 2018).

REFERENCES

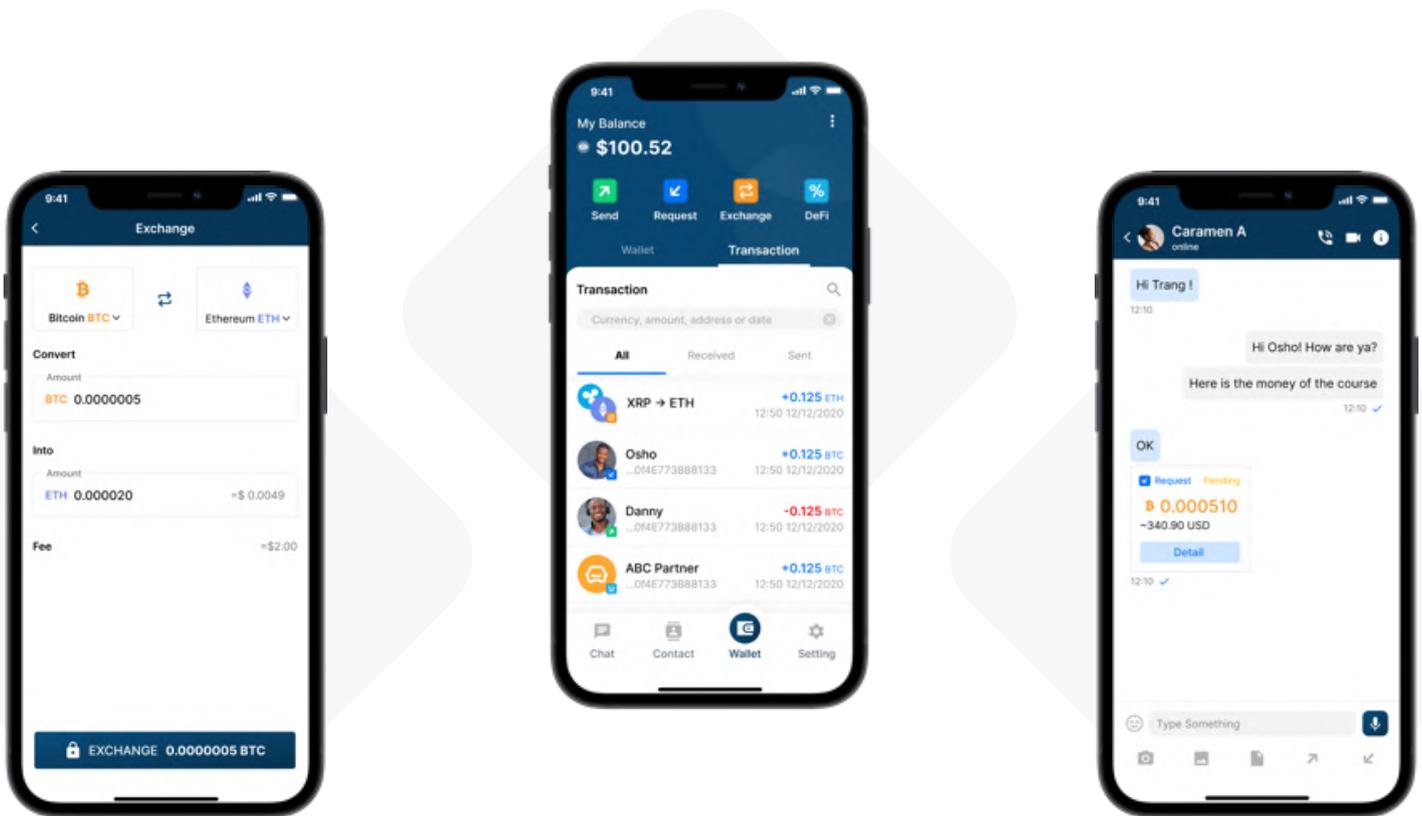
- Calleja-Castillo, J. M., & Gonzalez-Calderon, G. (2018). *WhatsApp in stroke systems: current use and regulatory concerns*. *Frontiers in neurology*, 9, 388.
- Chen, Y., Mao, Z., & Qiu, J. L. (2018). *Super-sticky WeChat and Chinese society*. Emerald Group Publishing.
- Dev, J., Das, S., Rashidi, Y., & Camp, L. J. (2019). *Personalized WhatsApp privacy: demographic and cultural influences on Indian and Saudi users*. Available at SSRN 3391021.
- Dev, J., Moriano, P., & Camp, L. J. (2020). *Lessons Learnt from Comparing WhatsApp Privacy Concerns Across Saudi and Indian Populations*. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)* (pp. 81-97).
- Grigg, A. (2018, February 21). *WeChat's privacy issues mean you should delete China's No. 1 messaging app*. *Australian Financial Review*. <https://www.afr.com/world/asia/wechats-privacy-issues-mean-you-should-delete-chinas-no1-messaging-app-20180221-h0wgct>.
- Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). *Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective*. *Computers in Human Behavior*, 107, 106260.
- Kharpal, A. (2019, June 13). *How social media is shaping what people know - and don't know - about the Hong Kong protests*. *CNBC*. <https://www.cnbc.com/2019/06/13/hong-kong-protests-role-of-technology-and-china-censorship.html>.
- Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). *Constructing a data-driven society: China's social credit system as a state surveillance infrastructure*. *Policy & Internet*, 10(4), 415-453.
- Liu, A. (2019). *An Analysis of the PBOC's New Mobile Payment Regulation*. *Cato J.*, 39, 87.
- Matemba, E. D., & Li, G. (2018). *Consumers' willingness to adopt and use WeChat wallet: An empirical study in South Africa*. *Technology in Society*, 53, 55-68.
- Quintas de Arcaño, T. (2019). *Sending cryptocurrency over mobile applications (Doctoral dissertation, Dublin City University)*.
- Rastogi, N., & Hendler, J. (2017). *WhatsApp security and role of metadata in preserving privacy*. *arXiv Prepr. arXiv1701*, 6817, 269-275.
- Tsai, W. H. S., & Men, R. L. (2018). *Social messengers as the new frontier of organization-public engagement: A WeChat study*. *Public relations review*, 44(3), 419-429.
- Zhang, X., Tang, S., Zhao, Y., Wang, G., Zheng, H., & Zhao, B. (2017, May). *Cold hard E-cash: Friends and vendors in the Venmo digital payments system*. In *Proceedings of the International AAAI Conference on Web and Social Media (Vol. 11, No. 1)*.

Chapter II:

OUR SOLUTION



2.1 Sappchat Platform



Sappchat is a Blockchain-based, distributed platform that aims at safely, privately and securely connecting users worldwide by cutting edge of encryption and mobile communication technologies. Sappchat is built upon the Sappchain – our technical partner's Blockchain, especially developed to cater to the needs of users of both cryptocurrencies and communication technologies.

Sappchat's vision and development addresses the multiple shortcomings of existing MIMs and platforms by providing solutions to the following aspects:

- 1 Sappchat is a Blockchain-based solution and it has a full security against hacking, online attacks, financial fraud and data and identity theft. By providing strong encryption infrastructure and capabilities to support transmission of text messages, video, audio and files and secure transfer of payments and funds on the Blockchain, Sappchap provides a complete solution that integrates communications and financial transactions between users.

Sappchat offers a complete mobile solution and eco-system for any type of communications between users. In addition to secure transmission of text messages, audio and video feeds and the transmission of files, Sappchat also provides the following features to its users:

- Mobile payments and money transfers that are carried out through the Sappchat application –Sappchat completes cryptocurrency payments and transfers by sending cryptocurrency funds to other users through the chat with them or at any time. This way, the payments and money transfers are global, have very low transaction costs in comparison to any national or international money transfer service and are completed within a very short time.
- Sappchat will have an online shopping platform, in which users can purchase digital goods, such as NFTs by paying with cryptocurrencies. The platform will be an integral part of the Sappchat application, user friendly and without need to navigate between different applications or website and to convert cryptocurrency to fiat or to link the user's wallet to external applications to complete the purchase of goods.
- Sappchat will include an integrated crypto-exchange through which users can swap cryptocurrencies and trade them. This module is especially important as users may receive payments and funds in cryptocurrency while operating Sappchat or wish to immediately react to changes in the conversion rates of cryptocurrencies. Hence, the crypto-exchange provides a seamless solution that streamlines the financial operations of users, supporting multiple cryptocurrencies.
- Sappchat will also integrate a DeFi platform, where users of the application can link their wallet assets (in multiple types of tokens) to liquidity pools, provide liquidity to borrowers and generate interest from their crypto assets. By operating the DeFi as a part of the application's ecosystem, Sappchat users can have another source of profit, in addition to cryptocurrency trade and offering digital goods via the online shopping platform, hence generate interest on their assets that otherwise could stay as holdings with no additional returns.

Chapter III:

BENCHMARK ANALYSIS OF COMPETITORS

- Introduction
- Results
- Sappchat DeFi Solution and its Main Competition

3.1 Introduction

Mobile applications are an integral and substantial tool of our mobile communications. With rich and broad possibilities to communicate via text, audio and video messages, to engage in one-on-one chats and group discussions, to receive notifications and to upload and watch status updates and to share media, mobile instant messengers (MIMs) are among the most important and essential applications in our smartphones.

The use of mobile applications surpasses the use of most of the social network platforms, with over a billion WhatsApp users, more than 900 million Chinese WeChat users, over 1.3 billion Facebook Messenger users and 260 million active Viber users. However, most of the MIMs (except WeChat) do not include financial features, such as a payment system, electronic wallet and saving accounts, and none of them supports financial operations with cryptocurrencies.

Sappchat developing a platform that integrates both decentralized Blockchain-based mobile communications and financial operations in cryptocurrencies, including payments, fund transfers, crypto-exchange for conversions and yield farming (DeFi). Sappchat communication are fully anonymous as the platform does not require any personal or mobile details upon registration and provides end-to-end encryption of all messages and shared files. Additionally, Sappchat's platform will support multiple solutions for online shopping and e-commerce and will utilize AI technologies to support voice-only management of its communications and financial operations.

Sappchat conducted this study to assess the functionality of other non-blockchain and blockchain based MIMs. The platforms were compared according to prominent features of mobile messaging, privacy and security and financial operations of the platforms.

Information about the projects and the platforms was collected from multiple resources published by them, including whitepapers and brochures, websites, videos, forums, blogs, technical reviews, etc.

3.2 Results

The benchmarking analysis was based on a comparative study of projects and platforms for mobile communications that are based on centralized and decentralized solutions.

The results of the comparison considering the multiple attributes of the platforms are follows:

	Sappchat	Wechat	Whatsapp	Dust	Echo	Signal	Crypviser
Content Privacy	✓	✓	✓	✓	✓	✓	✓
Metadata Privacy	✓	✓	✓	✓	✓	✓	✓
Authentication Security	✓			✓	✓	✓	✓
Decentralized Architecture	✓			✓	✓	✓	✓
Anonymity	✓			✓	✓	✓	✓
Transparency	✓	✓	✓	✓	✓	✓	✓
Blockchain+AI	✓						
Crypto payment	✓				✓		✓
Crypto transfers	✓				✓		✓
DeFi and Staking	✓						
Shopping and e-commerce	✓						

Sappchat

Sappchat is a free decentralized and rich application that provides an ecosystem for mobile users for communications, cryptocurrency payment, exchange and DeFi (yield farming) and online shopping and e-commerce. Sappchat offers end-to-end encryption and operates on its Sappchain blockchain. Sappchat also integrates voice recognition and AI technologies to operate its multiple features and financial operations and crypto asset management only by voice.

Dust

Dust is a free private messaging app that uses end-to-end encryption for secure communication. Its main advantage is that messages cannot be kept and stored over time, but they disappear without any possibility to retrieve them or to use screen capturing of them. Dust utilizes a centralized network architecture and its own encryption protocol. It is solely for online messaging and does not have e-commerce capabilities, AI technologies and does not support cryptocurrency operations.

Echo

Echo is a free decentralized chatting app that operates on the Graphene blockchain. Echo provides end-to-end encryption of messages. Additionally, it integrated Payger – a coin agnostic payment platform for storing, transferring and trading digital assets. However, Echo did not develop its online shop and e-commerce solution, it does not implement AI technologies in its platform or supports yield farming via DeFi.

Signal

Dust is a free private messaging app that uses end-to-end encryption for secure communication. Its main advantage is that messages cannot be kept and stored over time, but they disappear without any possibility to retrieve them or to use screen capturing of them. Dust utilizes a centralized network architecture and its own encryption protocol. It is solely for online messaging and does not have e-commerce capabilities, AI technologies and does not support cryptocurrency operations.

Crypviser

Crypviser is subscription based secure messaging application. The app has blockchain-based end-to-end encryption for transmission and storage of messages. Crypviser also supports cryptocurrency payments and transfers. However, Crypviser does not include online shopping and e-commerce solutions, yield farming and DeFi and AI technologies.

WeChat

WeChat is a free centralized mobile communication platform, owned by the Chinese Tencent corporation. It provides a broad ecosystem to its users. WeChat has an integrated fiat (RMB) payment system, fiat (RMB) saving account and shopping platform. However, WeChat does not have end-to-end encryption and includes backdoors that allow other parties to read the sent and received messages of users.

WhatsApp

WhatsApp is a free centralized mobile messaging platform owned by Facebook. It provides end-to-end encryption that is based on its native protocol. However, WhatsApp does not include shopping and e-commerce solutions, does not support fiat or cryptocurrency financial operations or payments and does not implement AI technologies in its application.

3.3 Sappchat DeFi Solution and its Main Competition

BlockFi is Sappchat's major competitor in the domain of DeFi and loan provision backed by crypto assets. BlockFi is based on the provision of liquidity by crypto asset owners that are transferred to borrowers to finance their operations and needs in return to "freezing" their own cryptocurrencies as a collateral. Liquidity providers earn higher interest rates than offered by banks and financial institutes for providing cryptocurrency liquidity to borrowers.

The services of BlockFi require holders of cryptocurrencies to register through its website and to identify themselves with their full legal name. Sappchat takes a contrary approach and chooses to protect the privacy of liquidity providers and borrowers: Liquidity providers can anonymously link their wallet and their funds to the liquidity pools by approving the amounts that they wish to dedicate for liquidity provision and the terms offered to them by Sappchat. Similarly, borrowers can anonymously receive funds by providing collateral in crypto assets in their holdings to guarantee the return of the loan and approving the terms of the loan via the application. In this way, funds can be provided and interest gains can be generated in a completely secure and anonymous manner and can be carried out via Sappchat with ease, as a part of the integral financial operations that it offers to its users.

Chapter IV:

SAPPCHAT'S APPLICATION AND PLATFORM



4.1 Sappchat Application

Sappchat is a Blockchain-based, distributed mobile instant messaging application that utilizes the Sappchain to carry out financial operations in parallel to secure communications between its users.

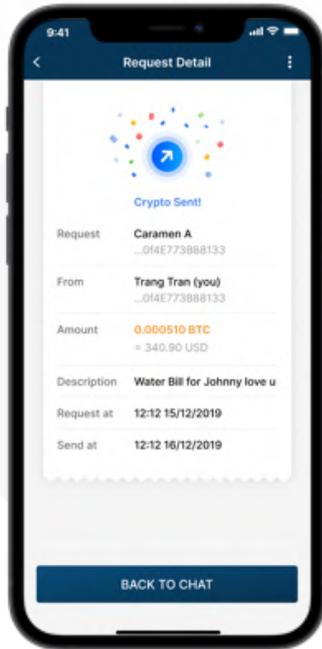
Our vision is to introduce an app that will be fully secure, will maintain the privacy of users and their anonymity, without collecting data on users and their interactions or disclosing data to companies and governments, as other MIMs do. Therefore, Sappchat prioritizes the security and the anonymity of users and therefore its user-to-user communications will be based on a distributed architecture, without going through a single and centralized server. This architecture prohibits the collection and the storage of users' data and interaction by our company or by any other party, as all the communication data are not transferred and managed by a single node, but rather by an ever-changing network of multiple nodes that dynamically inter-connect to each other during discussions and then disconnect.

An end-to-end encryption will ensure that text, video and audio messages and feeds, as well as the files transmitted between users, will be secure from eavesdropping or from intervention of any external party.

Users can remain completely anonymous, as the only requirement for signing up and operating the platform is their wallet address, as a unique and anonymous identifier. We do not request or attempt to retrieve any further details, such as the mobile ID, geolocation or phone data – We respect the security, safety and anonymity of users and do not attempt to collect any data about them, their habits of app use, their contacts or their communications.

Sappchat enables both person-to-person chats and group discussions. At any time, groups can be deleted from the app and users can be blocked, should a user feel any concern about his or her privacy and safety.

With Sappchat, cryptocurrency payments and transfers are completed immediately and with ease. Sappchat provides an electronic wallet that supports multiple tokens on the Blockchain and the transfer of funds from one user to another can be completed in one click, during chats or between them (see Fig. 4).



TRANSFER **WHILE CHATTING**

Figure 4 – Sappchat's transfer-while-chatting feature and user notifications.

In addition to cryptocurrency payments and transfers, Sappchat provides a "one-stop shop" for all the crypto-based financial operations and needs of its users. Sappchat integrates a mobile crypto-to-crypto exchange to carry out cryptocurrency exchanges and trades. The exchange supports a broad range of cryptocurrencies that are listed and traded on the main exchanges, as well as conversion to and from our APP token. With one click, users can dedicate funds to DeFi and enjoy interest gains for their crypto assets (see Figure 5).

ALL-IN-ONE **FINANCIAL ECOSYSTEM**

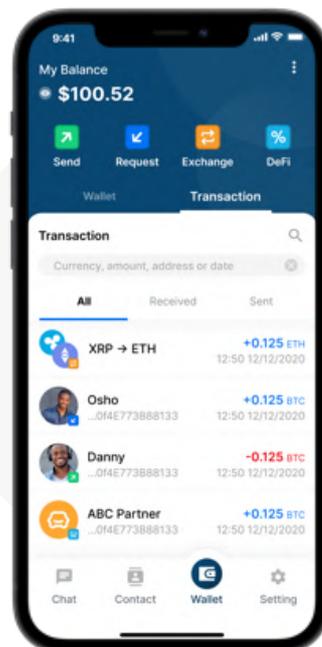


Figure 5 – Sappchat's all-in-one financial ecosystem enables users to transfer funds, to manage their transactions, to operate DeFi and trade operations at any time, as a part of their chats or independently of them.

Sappchat integrates an online shopping experience, where users can offer and purchase unique NFT artworks and stickers to enrich their communication experience. The NFTs can be browsed via the Sappchat store and purchased with one click by confirming the payment from the user's wallet. The NFT is delivered to the user's wallet and can be used in personal and group chats, benefitting Sappchat users with extensive options to personalize their communications with others (see Fig. 6).



Figure 6 – The Sappchat Store provides an integrated and seamless experience for shoppers and creators of NFTs.

Sappchat's cryptocurrency payments, transfers, trades, DeFi and online shopping are completely anonymous and are managed and completed only via the wallet addresses of senders and recipients of funds without any additional information or reference to the context of the payment (such as a chat or a purchase of NFTs). By doing so, Sappchat ensures that not only your communications and messages will be secured, but also your financial operations will remain private, anonymous and safe.

Sappchat bases its architecture on transactions of APP tokens to conduct financial operations by users. The APP token will be issued on the Binance Smart Chain that will serve as the backbone of all the financial operations of Sappchat, including cryptocurrency transfers, payments, exchanges, trade and DeFi. In latter stages of the projects, we plan to integrate additional Blockchains to be supported by Sappchat, including our Blockchain to carry out fully secure communications between users on it at the highest encryption strength.

One of the unique and innovative features introduced in Sappchat is the integration of Artificial Intelligence (AI) technologies into the application. By using the AI engine and the advanced models and algorithms applied for data analysis on the platform, Sappchat can serve users in multiple ways: First, the anonymous data on user communications and the capacity of the Blockchain to transmit messages will constantly be analysed. The AI-based recommender system will alert Sappchat and will open new nodes or dedicate additional computing and processing power when peaks in use are predicted. This feature can optimize and better utilize the Blockchain and provides better service quality to support high capacities on communications on the Blockchain. Second, the AI technologies will track the values of cryptocurrencies and their trade and will offer Sappchat users recommendations based on financial predictive analytics, including exchange rate forecasts and expected completion of transactions (see Fig. 7).

ARTIFICIAL INTELLIGENT

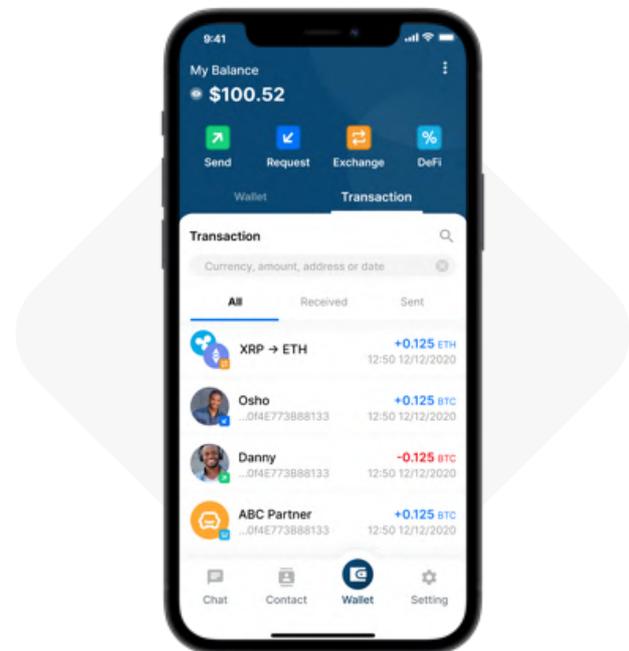


Figure 7 – Sappchat's AI embedded technologies provide users with financial predictive analytics and insights on cryptocurrency trades.

The major AI technologies embedded in Sappchat's platform will be based on neural networks for ongoing training and analysis of the performance of the Blockchain as well as for financial predictions and insights. These will be complemented by a series of Machine Learning algorithms for statistical learning, where the analysis process is presented in more detail and can be followed by users (see Fig. 6).

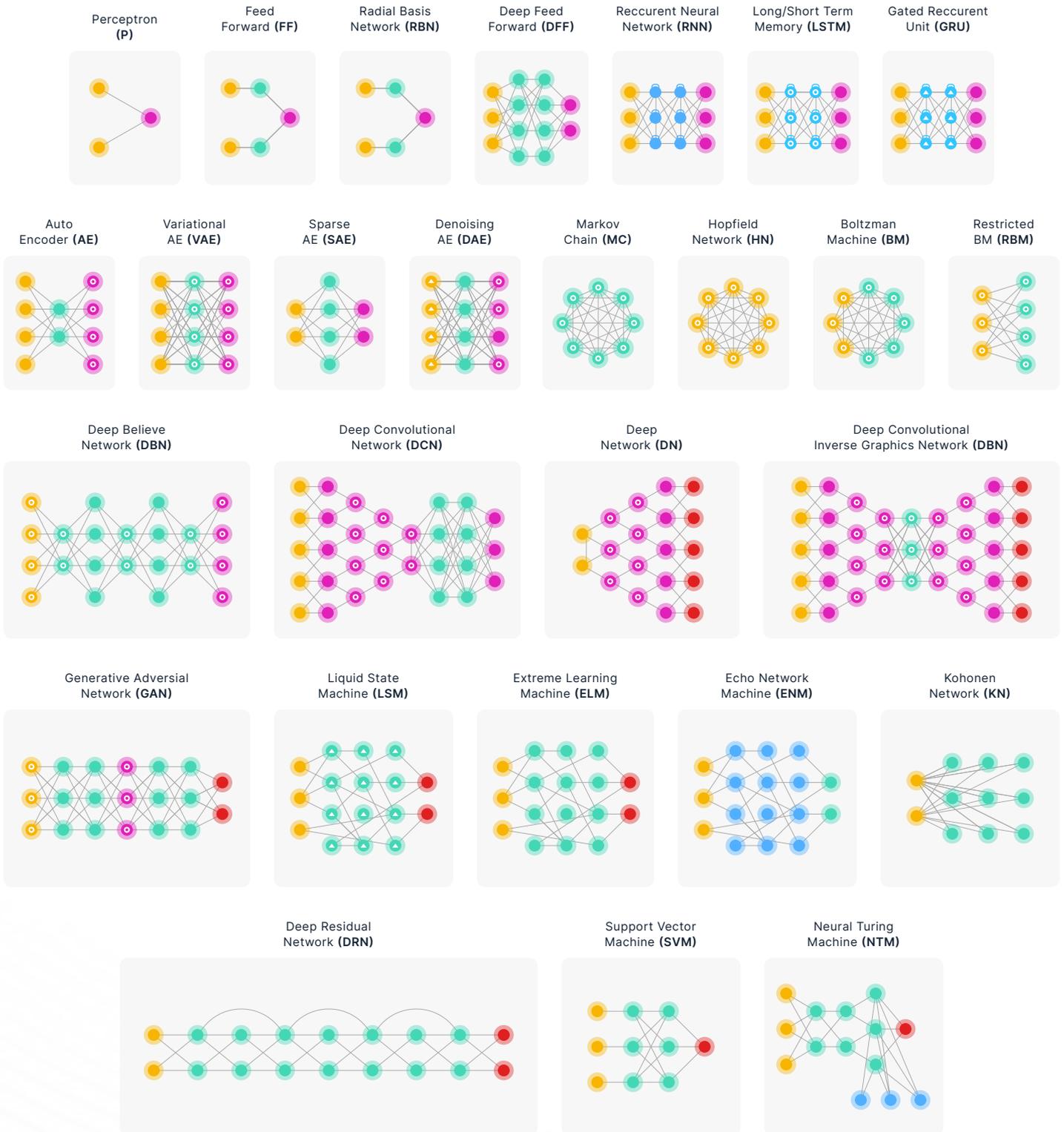


Figure 8 – Artificial Intelligence models used to analyse a broad variety of data structures and attributes. Source: <https://www.becominghuman.ai/>

Chapter V:

SAPPCHAT'S TOKEN SALE

- Structure
- Timeline

5.1 Structure

Sappchat's token sale is an opportunity for investors to fund and to participate in the development of an advanced communication and financial platform that provides an ecosystem of capabilities in the domains of secure payments and transfers and secure communications. The APP token integrated into the Sappchat will carry out all types of financial transactions, including:

- Payments
- Transfers of funds
- Cryptocurrency exchange and trade
- DeFi investments
- Online shopping and e-commerce

Prior to the token sale, Sappchat will mint 10,000,000,000 APP tokens.

After minting the APP tokens on the Blockchain, Sappchat will proceed to offering them to investors in the token sale: **4,000,000,000 APP tokens (40%)** will be offered to early investors, while the remaining **6,000,000,000 tokens (40%)** will be allocated to other purposes, such as marketing, promotion, staking rewards and to Sappchat's team, as follows:

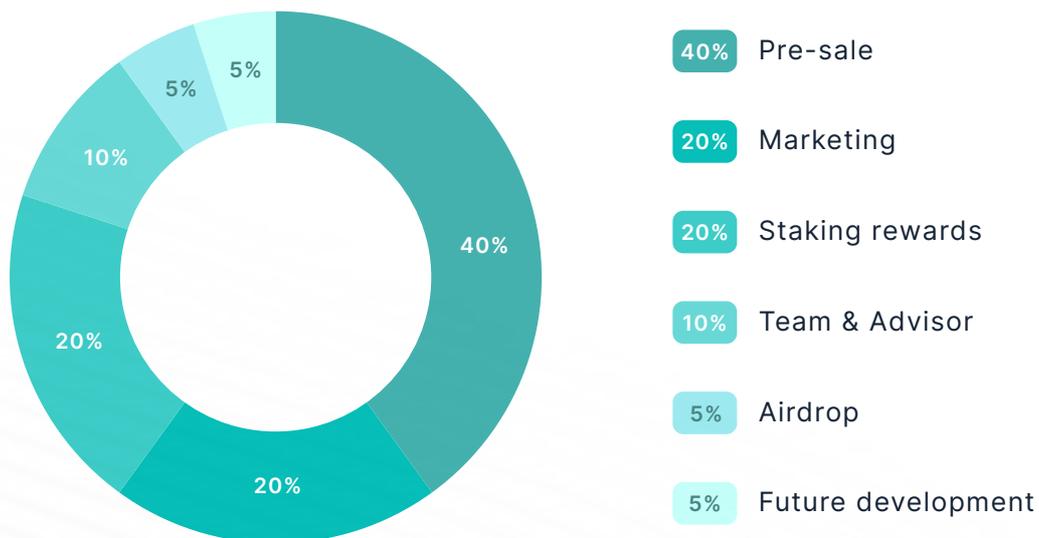


Figure 9 – The distribution of the APP token allocation.

- **2,000,000,000 tokens (20%)** will be locked for marketing and promotions, enhancing awareness of the community and forming strategic partnership.
- **2,000,000,000 tokens (20%)** will be locked for staking liquidity rewards and for providing attractive APY (annual percentage yield) to DeFi investors.
- **1,000,000,000 tokens (10%)** will be locked for team and advisors. This amount will be locked via a smart contract and only 2% of it can be withdrawn each month by the advisors and the team.
- **500,000,000 tokens (5%)** will be allocated to the Sappchat research lab for future development of the Sappchat applications and for trials of new features. This amount will be fully locked by a smart contract.
- **490,000,000 tokens (4.9%)** will be allocated for airdrops and bounties and for incentivizing the Sappchat community by distributing loyalty rewards to users of the application and to holders of the APP token for their ongoing use.
- **10,000,000 tokens (0.1%)** will be allocated to early investors.

Tokens that remain unsold will be fully dedicated to the community vault and will be fully distributed to the users of Sappchat and to holders of the APP token through a gradual release process over a long period of time.

In Sappchat we believe in complete transparency: the address of the community vault wallet will be published and can be examined and audited by everyone at any time.

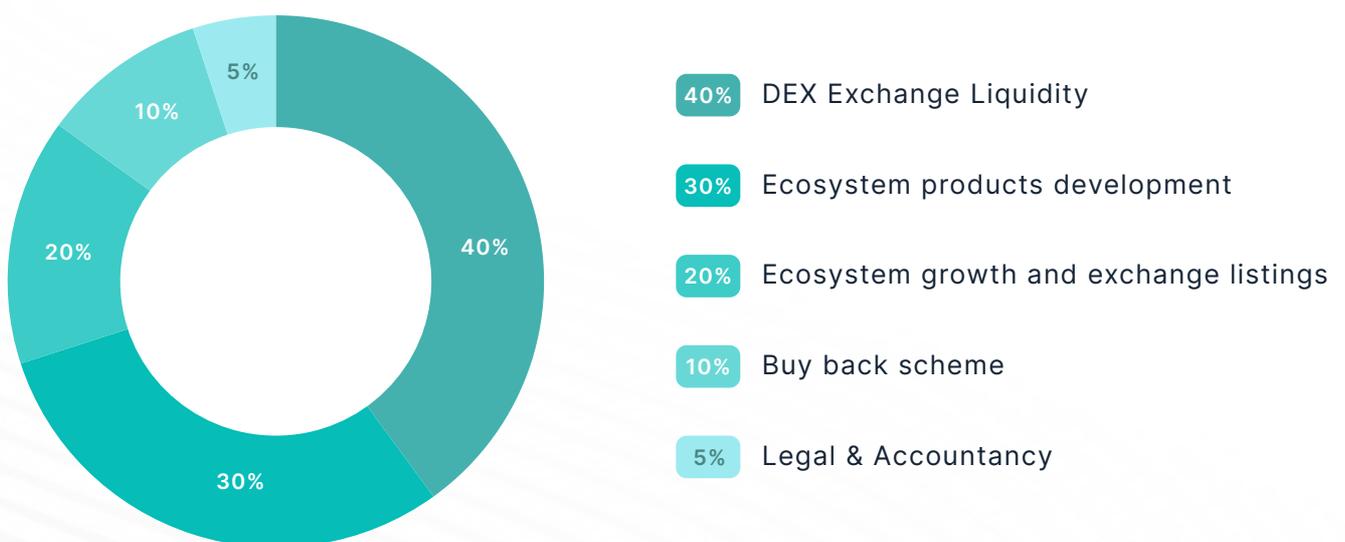


Figure 10 – The planned allocation of funds raised in the token sale.

The company will offer **4,000,000,000 tokens (40% of the tokens)** to investors in a token sale that will be allocated as follows:

- **40%** of the amount raised will be locked as liquidity on a DEX after the token sale.
- **2,000,000,000 tokens (20%)** will be locked for staking liquidity rewards and for providing attractive APY (annual percentage yield) to DeFi investors.
- **25%** of the raised funds will be allocated to Sappchat's partners and to the team to support the development and marketing of the application and the use of the APP token. Sappchat aims at promoting the application to be a market leader and a game changer in the MIM market due to its innovative and secure features for communications and financial operations. The use of the APP token and its adoption are likely to increase vis-à-vis the use of the app.
- **20%** of the raised funds will be dedicated to support the growth and the use of Sappchat and the APP token, including listing it on Centralized Crypto-Exchanges.
- **10%** of the raised funds will be allocated for token buybacks and burn after the token sale to support its value.
- **5%** of the funds will be dedicated to legal and accounting costs.

5.2 Timeline

During the token sale, purchases of APP tokens can be made in **Binance token (BNB)**. Please refer to instructions on the company's website how to convert other cryptocurrencies and fiat money into BNB in order to participate in the token sale.

Due to the U.S. Securities and Exchange Commission's regulations and to the People's Republic of China's government regulations, we cannot accept purchases and funds from U.S. and Chinese citizens or residents.

Chapter VI:

ROADMAP



6.1 Roadmap

The following roadmap describes the development of the Sappchat platform after the completion of the token sale:

Month 1 – Month 4:

- Development of the Sappchat application for both Android and iOS, including text messaging, person-to-person messaging and group messaging.
- Implementation of end-to-end encryption in text messaging.
- Development of the crypto-wallet.
- Integration of the crypto-wallet to the Sappchat platform.
- Integration of cryptocurrency payments and transfers to the chat (or outside a chat).
- Integration of Sappchat's operation into the Binance Smart Chain.
- Development of the token reward mechanism for holders of the APP token and users of the platform.

Month 5:

- Testing the Sappchat application and platform and its operations on the Binance Smart Chain.
- Testing the Sappchat platform under extreme conditions (huge volumes of messages, high volume of users registering and logging in within a short period, huge volumes of cryptocurrency payments and transfers, etc.).
- Testing for cyber-security vulnerabilities.

Month 6-10:

- Integration of swap and trade solutions via DEXs and centralized crypto-exchanges.
- Development of the DeFi and the online shopping platform (including NFTs) and their integration into the platform and the application.
- Development of person-to-person audio and video chats.

Month 10-12:

- Development of group audio and video chats.
- Development and integration of advanced graphics and UI/UX features.

Q3 – Q4 2020

- Project Planning and Research
- Consultation with Industry Experts
- Website Version 1 launch

Q1 – Q2 2021

- Smart Contract Development
- Smart Contract Audit
- WhitePaper Release
- Market Campaign launch
- SappChat App Testnet
- Sapp Wallet Testnet
- Presale launch
- Public sale launch
- DEX listing
- CEX listings
- CoinGecko & Coinmarketcap listing

Q3 – Q4 2021

- More CEX listings
- SappChat App Beta Version launch
- Sapp Wallet Beta Version launch
- Sapp-NFT Store Launch
- Sapp-Swap Product launch
- Sapp-Blockchain integration

Q1 – Q2 2022

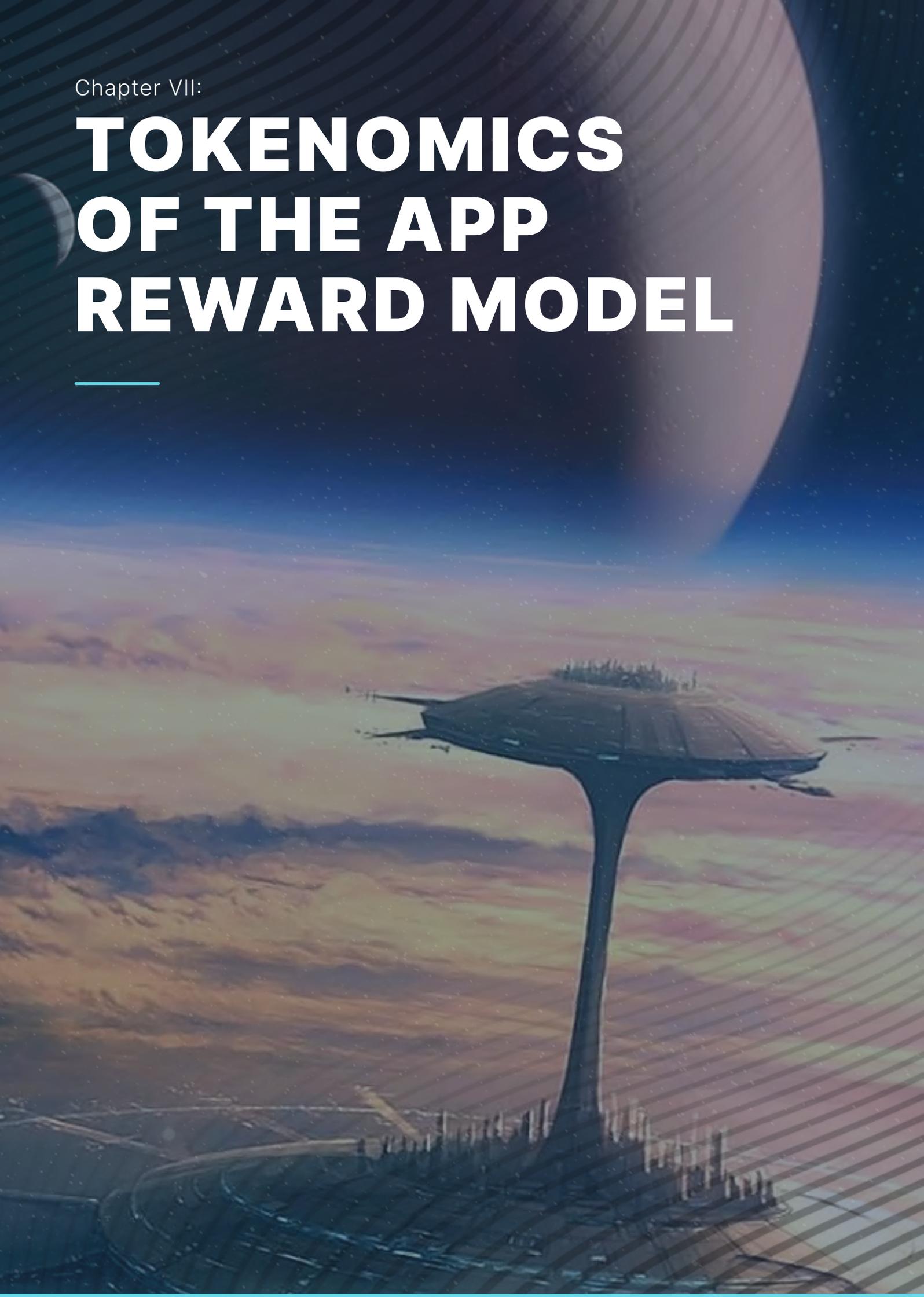
- Sapp-Pay launch
- More CEX listings
- More Crypto Coins/Tokens listing to SappChat Wallet
- Continuous Research & Development
- Continuous Improvement and marketing expansion
- More Strategic Partnerships collaboration

Q3 – Q4 2022

- More potential CEX listings
- Continuous Improvement on SappChat Platform and more Product release
- Introduction of more Unique Features to ecosystem
- Continuous Marketing expansion
- More Strategic Partnerships and Collaboration

Chapter VII:

TOKENOMICS OF THE APP REWARD MODEL



7.1 Tokenomics

In order to attract users to the Sappchat platform and to benefit from the use of the APP token, Sappchat will periodically distribute APP rewards to holders of the token.

The distribution of APP tokens will be based on the volume of APP tokens managed in their wallets, which are connected to the Sappchat platform and application (serving as the identifiers of users) and on the time APP tokens are held by their owners. The APP reward model aims at benefitting users and holders of APP tokens not only for the volume of their token holdings at a particular time (as dividends are distributed to stock owners at a given time), but rewards users for their loyalty and use over time. The calculation of the APP token distribution is as follows:

i	User's index.
AH	The amount of APP tokens held by the user.
TH	The time of holding APP tokens in the user's wallet.
AL	The amount of APP tokens used for financial operations (such as payments, cryptocurrency transfers, conversions and trade).
AD	The amount of APP tokens used to provide liquidity via Sappchat's DeFi.
TD	The time of liquidity provision in Sappchat's DeFi.
w	The weight provided to using APP tokens in financial operations (for example: $w = 0.15$)
d	The weight provided to using APP tokens as contribution to a liquidity pool in the DeFi (for example: $d = 0.25$)
$(1-w-d)$	The weight provided to holding APP tokens in the account without utilizing them for financial transactions.

The relative share that each user i will receive from the distributed proportion of the APP token reward, s_i , is as follows:

$$S_i = \frac{w \cdot AL_i + d \cdot AD_i \cdot TD_i + (1-w) \cdot AH_i \cdot TH_i}{w \cdot \sum_i AL_i + d \cdot \sum_i AD_i \cdot TD_i + (1-w) \cdot \sum_i AH_i \cdot TH_i}$$

Public Review of the Token Contract

The Token Contract and associated audits will be published on a later date on Etherscan. We invite all potential participants to review them for features and functionality.

Chapter VIII:

DISCLAIMER



8.1 Disclaimer

APP tokens and the Sappchat platform are not for speculative investment. No promises regarding value or future performance are made regarding APP tokens. No promises regarding any particular value of APP tokens are made. No other rights associated with holding APP tokens are given. Proceeds of the APP token sale may be spent as the company sees appropriate, which may change as deemed necessary in the maturation and advancement of the APP token and the Sappchat platform.

Our team is investing heavily in the safety and security of the services that Sappchat provides. However, we cannot protect against all possible sources of error and malicious deeds initiated by any party. Therefore, all risks assumed by using the Sappchat platform in any capacity, transferring, receiving and accumulating APP tokens are solely assumed by the user. APP tokens are meant to be held and used by those well experienced and knowledgeable in cryptographic tokens, their acquisition, transfer, and use only for accessing the services offered on the Sappchat platform.

Sappchat and its team must abide within the laws set forth in its operational country(ies). We intend to provide our services in as decentralized a fashion as reasonably feasible, but our legal entity must act according to the rules and bounds encoded in applicable laws. This includes but is not necessarily limited to laws governing financial operations, employment, fee charging, and sales. Due to the U.S. Securities and Exchange Commission's regulations and to the People's Republic of China's government regulations, we cannot accept contributions from U.S. and Chinese citizens or residents.

REFERENCES

- Calleja-Castillo, J. M., & Gonzalez-Calderon, G. (2018). WhatsApp in stroke systems: current use and regulatory concerns. *Frontiers in neurology*, 9, 388.
- Chen, Y., Mao, Z., & Qiu, J. L. (2018). *Super-sticky WeChat and Chinese society*. Emerald Group Publishing.
- Dev, J., Das, S., Rashidi, Y., & Camp, L. J. (2019). Personalized WhatsApp privacy: demographic and cultural influences on Indian and Saudi users. Available at SSRN 3391021.
- Dev, J., Moriano, P., & Camp, L. J. (2020). Lessons Learnt from Comparing WhatsApp Privacy Concerns Across Saudi and Indian Populations. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS) 2020* (pp. 81-97).
- Grigg, A. (2018, February 21). WeChat's privacy issues mean you should delete China's No. 1 messaging app. *Australian Financial Review*. <https://www.afr.com/world/asia/wechats-privacy-issues-mean-you-should-delete-chinas-no1-messaging-app-20180221-h0wgct>.
- Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, 107, 106260.
- Kharpal, A. (2019, June 13). How social media is shaping what people know - and don't know - about the Hong Kong protests. *CNBC*. <https://www.cnbc.com/2019/06/13/hong-kong-protests-role-of-technology-and-china-censorship.html>.
- Liang, F., Das, V., Kostyuk, N., & Hussain, M. M. (2018). Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy & Internet*, 10(4), 415-453.
- Liu, A. (2019). An Analysis of the PBOC's New Mobile Payment Regulation. *Cato J.*, 39, 87.
- Matemba, E. D., & Li, G. (2018). Consumers' willingness to adopt and use WeChat wallet: An empirical study in South Africa. *Technology in Society*, 53, 55-68.
- Quintas de Arcanjo, T. (2019). *Sending cryptocurrency over mobile applications (Doctoral dissertation, Dublin City University)*.
- Rastogi, N., & Hendler, J. (2017). WhatsApp security and role of metadata in preserving privacy. *arXiv Prepr. arXiv1701*, 6817, 269-275.
- Tsai, W. H. S., & Men, R. L. (2018). Social messengers as the new frontier of organization-public engagement: A WeChat study. *Public relations review*, 44(3), 419-429.
- Zhang, X., Tang, S., Zhao, Y., Wang, G., Zheng, H., & Zhao, B. (2017, May). Cold hard E-cash: Friends and vendors in the Venmo digital payments system. In *Proceedings of the International AAAI Conference on Web and Social Media (Vol. 11, No. 1)*.