FORESTING

Brand new social media based on blockchain technology

WHITEPAPER

“

Work four hours a day,
share every moment,
and manage your life.

with FORESTING

”

August , 2018 | VERSION 0.92

NOTICE

This material was prepared by FORESTING HQ Pte. Ltd. This document is intended solely for your information you and is subject to change without notice. This information does not provide any clarification or implied assurance or warranty, and we do not warrant the accuracy, fairness or completeness of this information. The Company, its affiliates, consultants, or representatives shall not be liable for any damages incurred by the information contained herein. This content, or any parts herein may not be reproduced, distributed or transmitted directly or indirectly, in any form or purpose.

FORESTING

FORESTING

Table of Contents

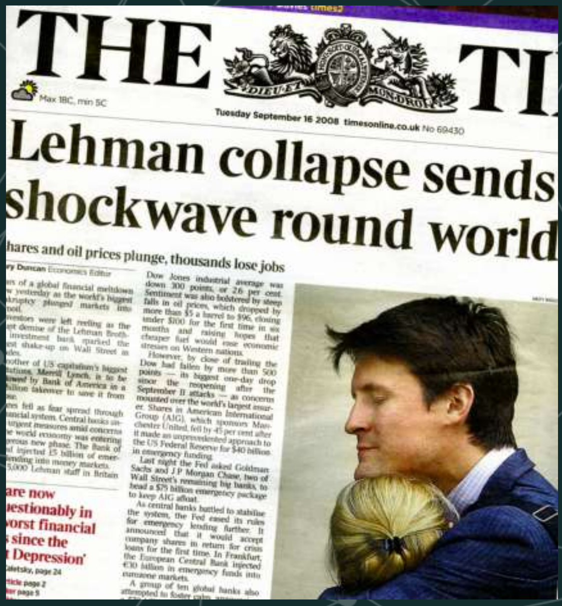
INTRO

"Among the essential features of this situation is that no one knows his place in society, his class position or social status, nor does any one know his fortune in the distribution of natural assets and abilities, his intelligence, strength, and the like."

- John Rawls, A Theory of Justice -

INTRO

In the beginning of the 20th century, national crises like the dot-com bubble, 9/11, and the War in Afghanistan, lead the American government to enforce a low interest rate policy as part of a strong economic stimulus package. While the main purpose of this initiative was to create corporate investments and private consumptions, it caused tremendous household loans. In 2004, it led to the termination of the low interest rate policies, leaving financial institutions unable to collect loans. Major financial security companies in the United States, such as New Century Financials, went bankrupt. The scandal has caused a worldwide credit crisis and hurt the real economy. One of the most widely known examples of the global financial crisis is the collapse of the investment bank 'Lehman Brothers' in 2008.


THE TI

Max 18C, min 5C

Tuesday September 16 2008 timesonline.co.uk No 69430

Lehman collapse sends shockwave round world

hares and oil prices plunge, thousands lose jobs

ry Duncan Economics Editor

rs of a global financial meltdown w yesterday as the world's biggest kruptcy plunged markets into moil.

vestors were left reeling as the pt demise of the Lehman Broth- investment bank sparked the est shake-up on Wall Street as ades.

nother of US capitalism's biggest itutions, Merrill Lynch, is to be owed by Bank of America in a billion takeover to save it from se.

res fell as fear spread through ancial system. Central banks un- urgent measures amid concerns e world economy was entering erous new phase. The Bank of al injected £5 billion of emer- ending into money markets. 5,000 Lehman staff in Britain

are now estionably in orst financial s since the t Depression'
aletsky, page 24
ticle page 2
er page 5

Dow Jones industrial average was down 300 points, or 2.6 per cent. Sentiment was also bolstered by steep falls in oil prices, which dropped by more than $5 a barrel to $96, closing under $100 for the first time in six months and raising hopes that cheaper fuel would ease economic stresses on Western nations.

However, by close of trading the Dow had fallen by more than 500 points — its biggest one-day drop since the reopening after the September 11 attacks — as concerns mounted over the world's largest insurer. Shares in American International Group (AIG), which sponsors Manchester United, fell by 45 per cent after it made an unprecedented approach to the US Federal Reserve for $40 billion in emergency funding.

Last night the Fed asked Goldman Sachs and J P Morgan Chase, two of Wall Street's remaining big banks, to head a $75 billion emergency package to keep AIG afloat.

As central banks battled to stabilise the system, the Fed eased its rules for emergency lending further. It announced that it would accept company shares in return for crisis loans for the first time. In Frankfurt, the European Central Bank injected €30 billion in emergency funds into eurozone markets.

A group of ten global banks also attempted to foster calm

One of the most interesting events is the birth of the post-revolution system and cryptocurrency, called 'Bitcoin' which was first ideated by Satoshi Nakamoto after the collapse of Lehman Brothers. Speculation has been rampant about who SatoshI Nakamoto is, since his identity remains completely veiled. The clear message he is trying to convey in his thesis, which consists of about nine pages, is the lack of trust in the banking system, especially toward the Federal Reserve Bank (FRB) which is central publisher and trustful third party and manages all information and policies after going through the financial crisis in 2008. He suggested a currency system that cannot be fabricated and can be perfectly transparent without requiring personal information with the purpose of "substitution" for existing systems.

His message raised social discourse on the system that everyone decides the system participants transparently. His will has spread not only in the banking system but also throughout media, culture and society. Rather it is not determined by the sharing and distribution of information in a fairer society, centralized control and management, with the meaning of 'Decentralization'.

Satoshi Nakamoto derives the definition of distribution from the ancient days of Platon. In particular, his discussion shows analogies to John Rawls' book "A Theory of Justice" where the moral and political philosopher emphasizes the importance of justice. Rawls argues that fairness can only exist when the procedures of distribution are fair.

Taking a closer look at how these comments relate to the blockchain, John Rawls uses the the term 'fair procedure' to account for the 'veil of ignorance' and to assert that the information solves asymmetry. The blockchain is a chain of blocks that are distributed through public trading principals, who can't modify the contents. More importantly, all of the relevant records will be disclosed. In this process, no asymmetry exists between the two parties during the transaction, making it possible to implement a fair contract. The same is true for distribution procedure. For instance, maintaining a blockchain network requires voluntary participation from the miner (e.g. PoW) who is rewarded with a donation of cryptocurrency tokens in return for their mining activities. This is in line with Rawls claim for distribution of capabilities based on procedural definitions.

A Solution for Asymmetry of Information & Realization of Fair Contract = Blockchain Technology

Fair distribution = token distribution based on system contribution

The FORESTING Network, which will be introduced in this whitepaper, is based on the creation of bitcoin and a philosophy shared by Satoshi Nakamoto and John Rawls on a more fair society. Accordingly, the FORESTING Network solves the asymmetry of the information that is prevalent in our society, pursues fair contracts, distributes them according to their ability, and shares active contributions with one another. The first chapter of this paper will be about the social media field, which has transformed people's values and lifestyles since the release of the iPhone in 2007

DEFINE

FORESTING NETWORK

The FORESTING Network consists of the blockchain based 1) social media 'FORESTING', 2) digital banking services for FORESTING participants 'FORESTING Bank' and 3) 'FORESTING Lab' to support the FORESTING community and content creators. Each of the three departments is separated into their respective functions and roles to fulfill the core values of the FORESTING Network.

FORESTING

'FORESTING' or 'FORESTING Platform' is a blockchain based social media platform that deviates from the distribution system of traditional social media platforms. It provides a fair value distribution system for users who are the true owners of the platform. They deliver content through blockchain technologies and contribute to platforms in a variety of forms.

FORESTING BANK

'FORESTING Bank' is a digital bank for content creators and curators alike. At the core of the FORESTING Network is the platform users who will be provided and supported by these financial services to create content.

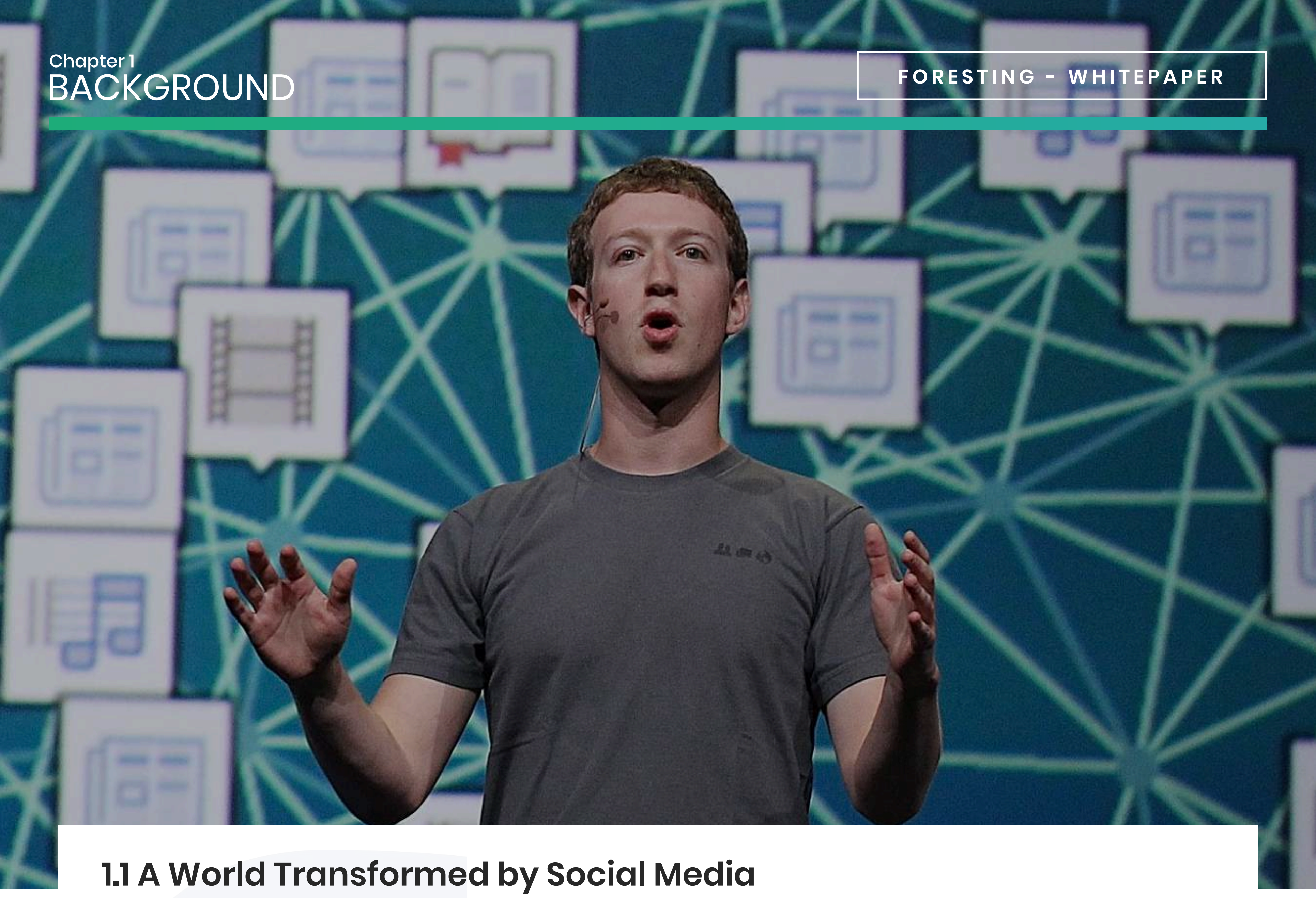
FORESTING LAB

'FORESTING Lab' supports communities and marketing activities besides the platform to activate the FORESTING Network, especially the content creators who are the owners of the FORESTING Network.

Chapter 1

BACKGROUND

Taking a glance at what it was, what it is, and what it will be



1.1 A World Transformed by Social Media

"Make the world more open and connected."

– Mark Zuckerberg –

On February 4, 2004, a 19-year-old Harvard student started Facebook with a slightly unusual goal.

facebook

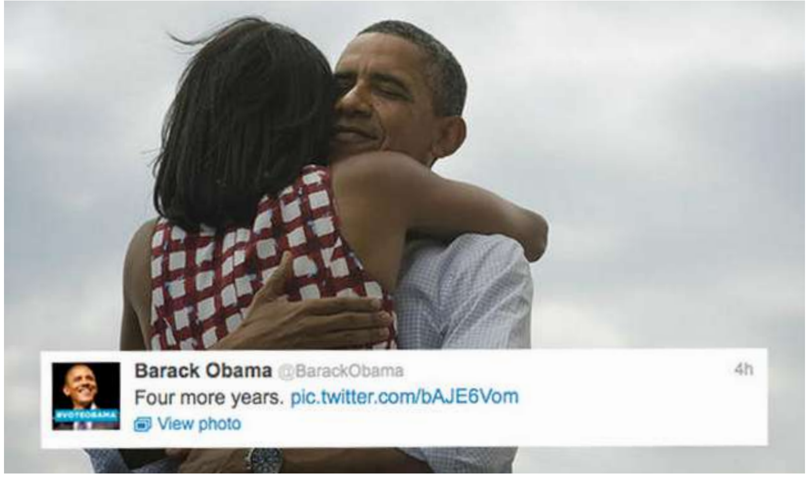
As of 2018, an average of 1.47 billion people out of approximately 2 billion are accessing and interacting with Facebook daily. From trivial daily live updates to sensitive political issues, Facebook users read and write three million articles a minute. They share their thoughts and opinions by posting pictures and videos and giving 'Likes' 2 million times a minute.

Looking back at the past decade of social media that has been represented by Facebook, there has always been social media connecting the people at the center of our lives. It has brought social changes, such as political, cultural and economic, and its influence is gradually expanding in each area.

Social media changes the election culture

'Four more years!' was U.S. President Barack Obama's Twitter post after his re-election on November 6, 2012. which came with a happy picture of him embracing his wife Michelle. This tweet was instantly shared by 680,000 individuals. On Facebook it received 400,000 shares and 3.3 million 'Likes'. The tweet had only three words and one photo but it was more effective than any multimillion dollar advertisement. The post won the hearts of Americans.

In fact, the Obama campaign hired Chris Hughes, a Facebook co-founder since 2008. He created a dedicated site for the presidential election, MyBO(My.BarackObama.com) which binded supporters together and raised campaign funds. Supporters, who formed the online version of MyBO, played a crucial role in creating the "Obama Movement" on Facebook and Twitter. In fact, the 2008 and 2012 presidential elections are considered to be the 'Textbook of Social Networking Elections' and social media has played a crucial role on the activities of politicians since.



Barack Obama @BarackObama 4h
Four more years. pic.twitter.com/bAJE6Vom
View photo

Serves as a channel for horizontal social change

Social media has become the main tool of the Jasmine revolution called the "Arab Spring". An unnamed Tunisian young man's improper death became a symbol of the democratic revolution on social networking sites around the world. In the Egyptian revolution the first group of tens of thousands of people staged a protest on Facebook.

99 percent of the young people that started the strike were also capable of taking over Wall Street and Europe through their Facebook accounts. The reason why social media has changed this rapidly is because the public is free to express their opinions. It has served as a tool to bring opinions to the public for the countries where the press has been controlled by a dictatorial government or the opinions of the minority has not been voiced. Social media has also served as an alternative medium for breaking the controlled and limited media environment and spreading hidden truths and suppressed opinions.

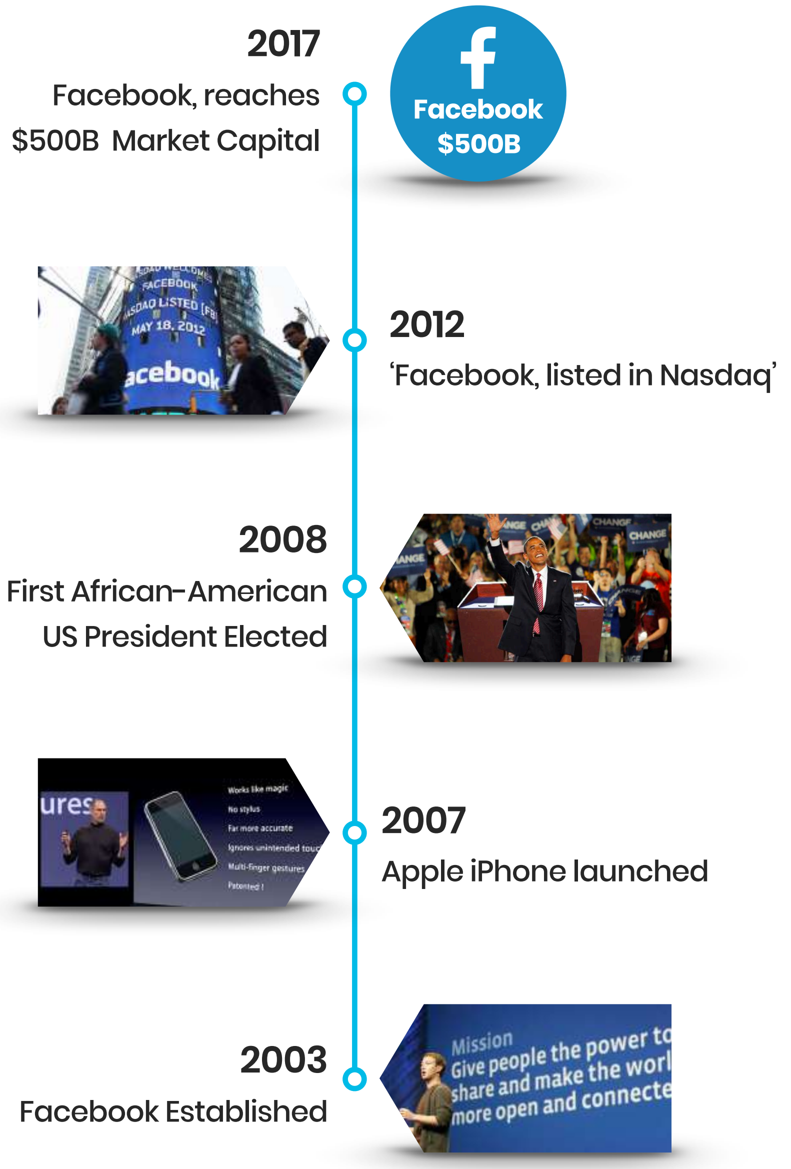
As social media became the keyword that changed the world, the position of the press grew votile. Today we can get faster news on Twitter than on any major news network. Even Syria which is known as a country where foreign media activity is under full control and journalists are not allowed to enter the country, the Syrian protest news are being widely spread through Twitter and YouTube by citizen journalists.
In the 21st century, it has become difficult for people to leave social networking sites. Apparently, Social media has caused a shift from vertical communication to "horizontal opinion spreading" in the society where it was the main subject.

1.2 Centralized Social Media

As of 2018, there are about 3 billion active users on social media, and the number keeps growing day by day. Social media has changed the world and sparked the start of a new digital economy.

Popular social media app services, such as Facebook, Instagram, Pinterest, SnapChat, Twitter, and LinkedIn have some common features that are drawing attention from many people. With the user experience and behavior in mind, this type of contents has been one of the most successful concepts for social media and has promoted the growth of mobile app services and smartphone use.

Within the social media platform, user-generated content created billions of dollars and was naturally distributed among the platform's operators and their shareholders. They would not be where they are today if it weren't for the actual interaction of the users who contributed to the platform's growth through engagements and shared contents. The companies that are running the platforms have a basic goal to bring more users onto the platform. Traffic and content generated through user interaction are the most valuable assets in platform-based services. The company provides a space where users can share their interests and interact with their friends for free. By doing so, users will be able to offer their ideas, messages and ownership of content free of charge to the network owner (corporate). Most users are not aware of the rewards associated with this and think rewards are only for certain influencers.



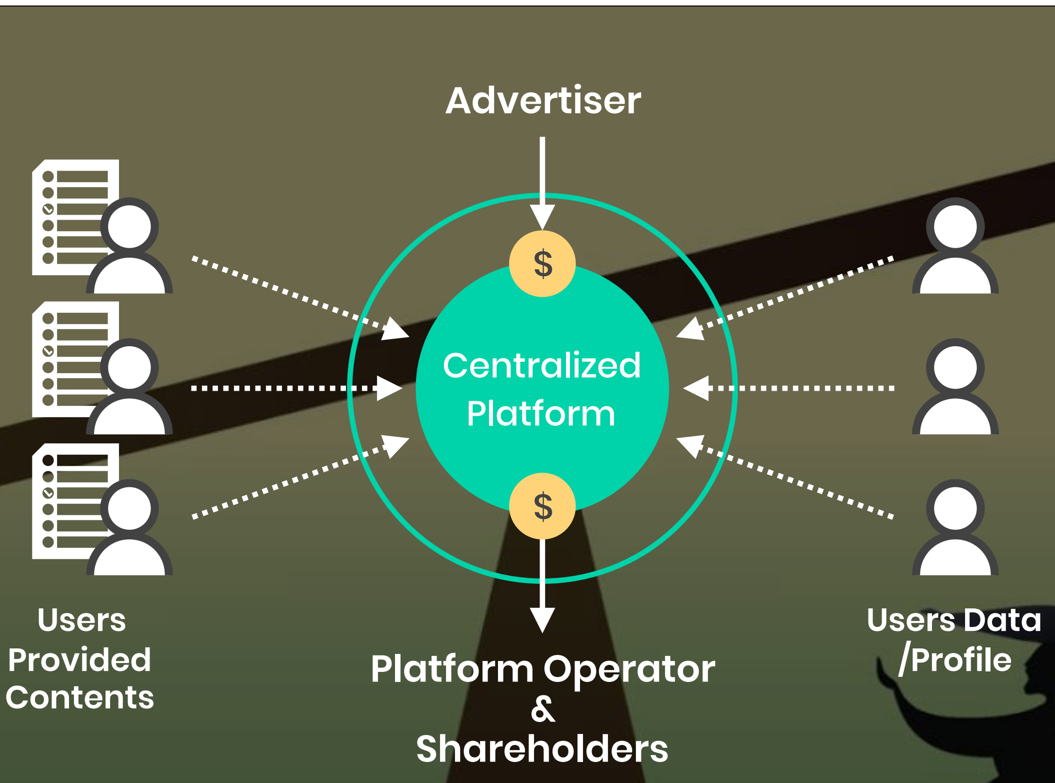
2017
Facebook, reaches
$500B Market Capital

2012
'Facebook, listed in Nasdaq'

2008
First African-American
US President Elected

2007
Apple iPhone launched

2003
Facebook Established



In the meantime, user data is becoming a commodity sold for advertising which is a major source of revenue for the company. Through the content and database that users contribute for free, the company acquires major revenue sources, making it a targeted advertising provider that encourages users' desire to own and consume.

1.3 Excessive Reliance on Ad Revenue

I. Personal Information Leakage and Theft

Almost every form of media that exists today is centralized, and social media that emphasizes a free lifestyle is no exception. Rather, they are not free from security issues, such as censorship, hacking, or personal information leakage.

The recent major disruption on Facebook's privacy has given us a strong picture of this. It revealed that about 87 million personal information records were leaked from Facebook and used for certain candidates during the last U.S. presidential election.

Making a profit is the goal of every company, so there is no reason why Facebook's business model should be criticized. However, users are complaining about the betrayal and withdrawing their trust because Facebook's business philosophy does not match the way the company operates. In particular, this is evident that Facebook has turned creative content made by its users of the horizontal network into revenue streams, creating a large, centralized conglomerate. What is especially unfortunate is that most personal information can never be recovered after it was leaked. This can cause secondary damage and criminal acts such as spam mail, identity theft, privacy breaches, and voice phishing.

Looking back on this case, the biggest problem is that most content platform providers use customer database to earn advertising revenue.

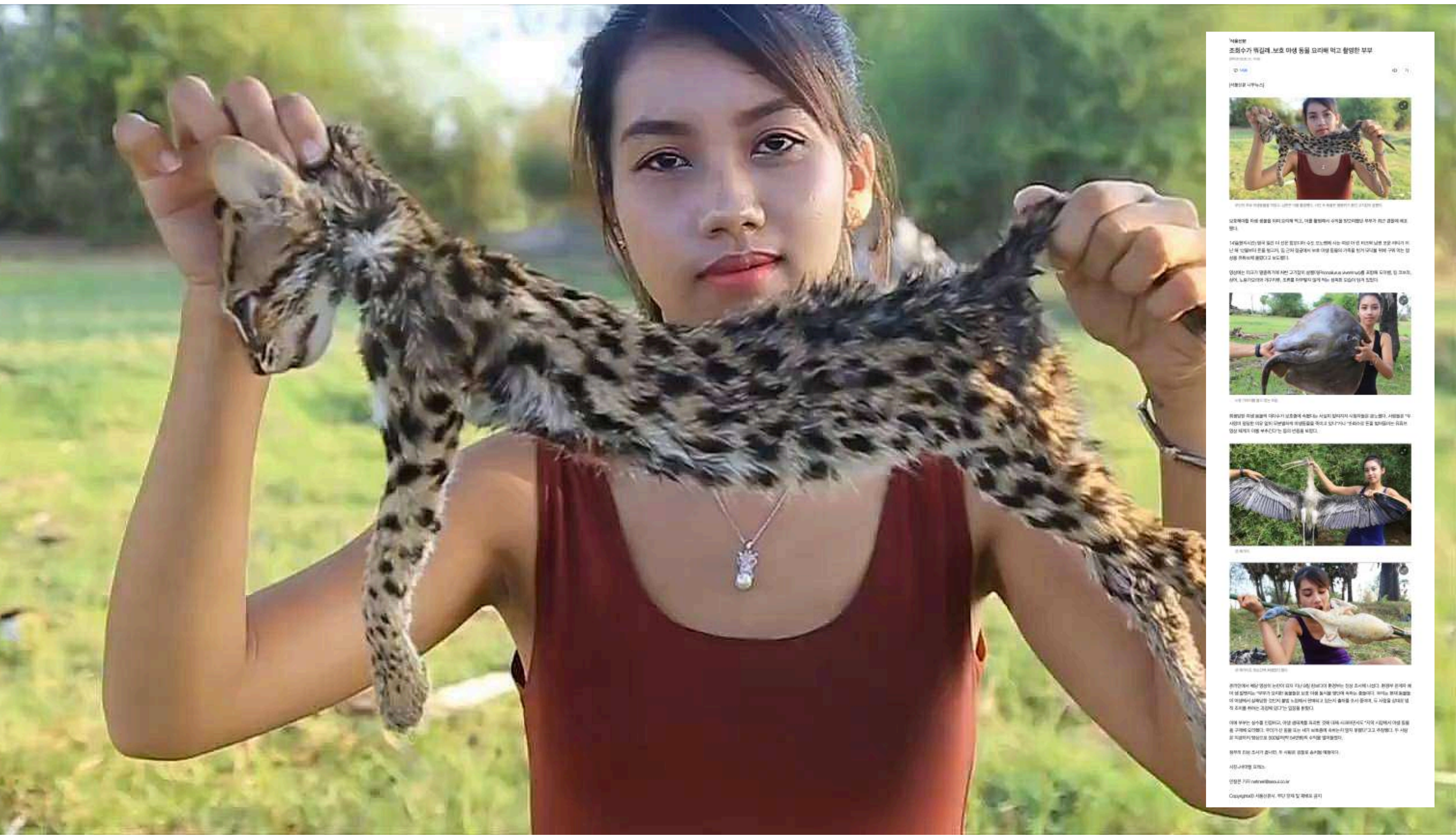
Rather than the content itself generating the primary revenue, the platform acts as an intermediary for advertisers, and advertisers are eager to collect the user database to increase the efficiency and effectiveness of targeted advertising by advertisers and advertising agencies. Facebook is already known to be a highly advertising-effective platform. This means that everything we do on Facebook used by every company using Facebook advertising.

Rather than pursuing a profit-focused platform, FORESTING will create a content-centered platform that generates direct content revenue.

Facebook says data leak hits 87 million users, widening privacy scandal

II. Advertisement Abuse

Personal information leakage is not the only problem with traditional social media that relies on ad revenue. If you rely solely on ad revenue, it also creates a big problem for the quality of content. Most social media platforms see traffic as a value measure for content rewards to expose advertising to more users. However, this may encourage provocative, content-oriented postings to attract collectors.



서울신문

조회수가 뭐길래..보호 야생 동물 요리해 먹고 촬영한 부부

[서울신문 나우뉴스]

FORESTING encourages better content creation and is focused on user voting rather than actual traffic-oriented content valuation. We will create a better content culture through evaluation.

1.4 Value Distribution

I. Unfairness of Value Distribution: Content Providers & Participants < Service Provider

The distribution of values in traditional social media is clearly disadvantageous to the user. Although users perform a whole series of procedures to create, post and share content on their own, they are not rewarded. Despite the fact that this is so well known, people don't feel it is unjustified. Even if people feel it is unfair, they don't know what to do.

II. 1 Irrationality of Value Distribution: Revenue of Content Providers

Some social media platforms share the operating revenue of content creators. We tend to think only of the higher-earning annual revenue streams exposed to the media, such as YouTubers, BJs (Broadcasting Jockeys), and Bloggers and see the platform's value and revenue between content providers separately. However, these 'Influencers' account for only a small fraction of all content creators, and they are still assigned an unreasonable share of the revenue distribution between the content provider and the service provider.

[Daniel Middleton who raised $18M in 2017 / 출처 : http://thegear.co.kr/15517]

II. 2 Irrationality of Value Distribution: Participants

The main asset of the social media platform is user traffic. User activity indicators such as daily active users (DAU), monthly active users (MAU), and average revenue per users (ARPU) are always used as performance indicators for the platform operator. In particular, content and its surrounding relationships are the source of social media platform value. All platforms are maintained by users who invest their time creating content and curating it. However, their value is not revenue-generated across most social media platforms, unlike the content providers described above, but rather through targeted advertising campaigns within the platform that makes users subject to identity theft.

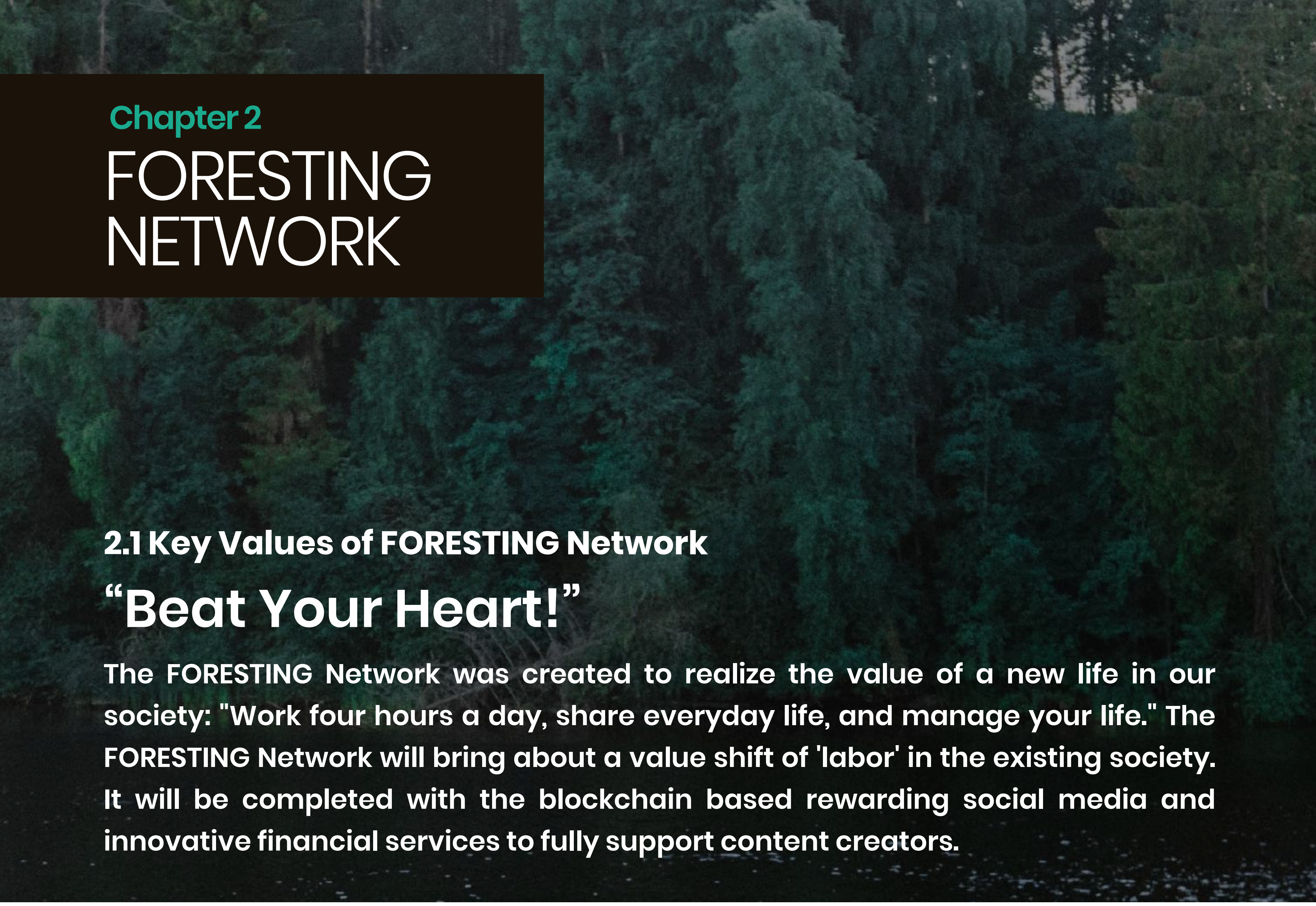
II. 3 Irrationality of Value Distribution: Operator

Through creating, publishing, sharing, and writing content within the platform, the social media platforms have generated billions of dollars in value, when most of the revenue returns to the operators and the shareholders.

Chapter 2

FORESTING NETWORK

“Beat Your Heart!”



Chapter 2

FORESTING NETWORK

2.1 Key Values of FORESTING Network

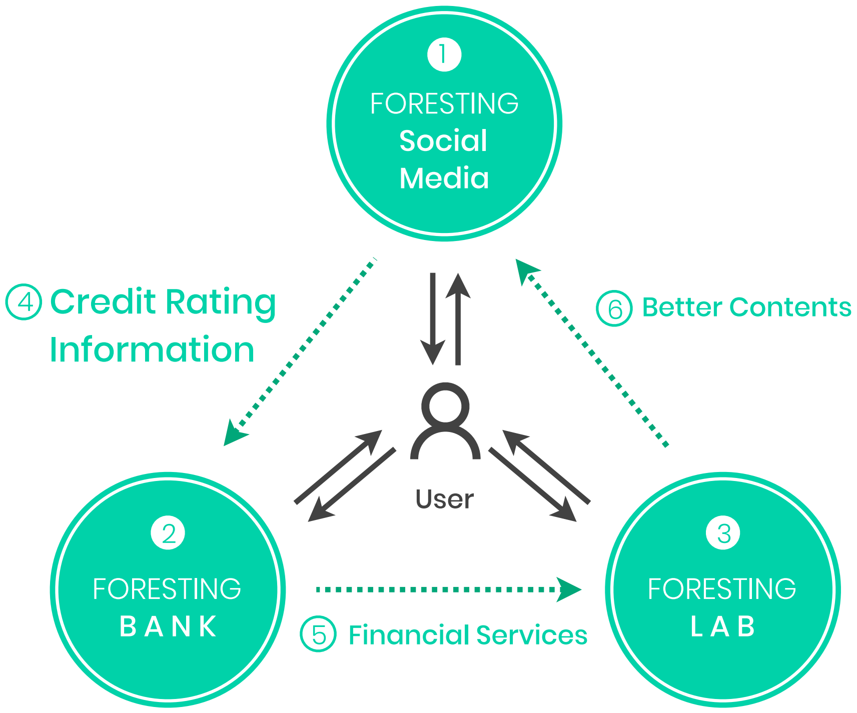
“Beat Your Heart!”

The FORESTING Network was created to realize the value of a new life in our society: "Work four hours a day, share everyday life, and manage your life." The FORESTING Network will bring about a value shift of 'labor' in the existing society. It will be completed with the blockchain based rewarding social media and innovative financial services to fully support content creators.

2.2 FORESTING Network Value Chain

The FORESTING Network is set up with three departments. 1) blockchain rewarding Social media 'FORESTING', 2) digital banking services for FORESTING participants are transformed into a direct payment from the ‘FORESTING Bank’ and 3) the ‘FORESTING Lab’, providing infrastructures and supporting content creators. While each department’s respective functions and roles are separated, the core values of the FORESTING Network remain the same. They were designed in a structure in which they interact systematically and create synergies.

1) 'FORESTING': Blockchain based rewarding Social media
2) 'FORESTING Bank': Financial services for FORESTING Network participants
3) ‘FORESTING Lab’: Providing infrastructure and supporting content creators
4) Providing credit rating information
5) Financial services
6) Using infrastructure and creating better contents

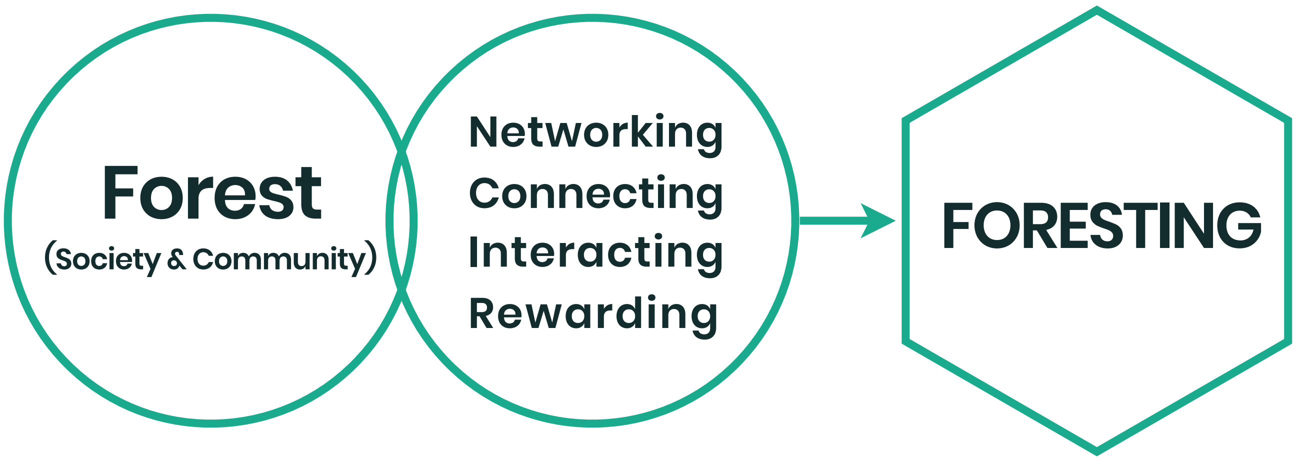


At the heart of FORESTING Network's three departments are the FORESTING users. The level of content delivery and platform involvement by the FORESTING user defines the scalability and impact of the FORESTING Network. The starting point for the FORESTING Network mechanism comes from the content providers and participants. It is also associated with the core value of the FORESTING Network, a fair world created by participants.

2.3 Blockchain Based Rewarding Social media 'FORESTING'

"Connecting the world and making lives more valuable"

FORESTING is the platform's revenue chain that allows users to quantify the content provider's contribution to offer rewards using a distributed consensus method.



FORESTING, which will open a new world, is a combination of 'Forest' and 'Networking', 'Connecting', and 'Interacting'. FORESTING is the primary social media, a blockchain with economic freedom for content providers. The platform will be able to increase the efficiency and impact of content providers by enabling them to generate new, faster content than traditional social networks. The platform will create a new ecosystem for social media through blockchain technology and a new concept of social media token operation.

FORESTING is designed to build a network by distributing income though reasonable content generation and on the assessment of the users' content. It supports all types of content, whether it is text, images, videos, audio, or live broadcasting, and provides a social network based on a content-oriented rewarding service.

2.4 FORESTING Bank

“Creating a unique credit rating system”

The purpose of FORESTING Bank is to support financial services that are required by users so that they can fully focus on creating the content at the center of the FORESTING Network.

Users can contribute to the FORESTING platform through a variety of activities, including creating and providing content, writing comments, liking, and sharing. The contribution of users is evaluated using a new contribution assessment model presented by FORESTING Bank. Users will be provided with a variety of financial services depending on the contribution level on the platform which is based on the level of their connections, the quality of their content, coin acquisition, and transactions. Users can improve their credit ratings just by working on social networking sites, and have an amazing experience with broader economic potential.

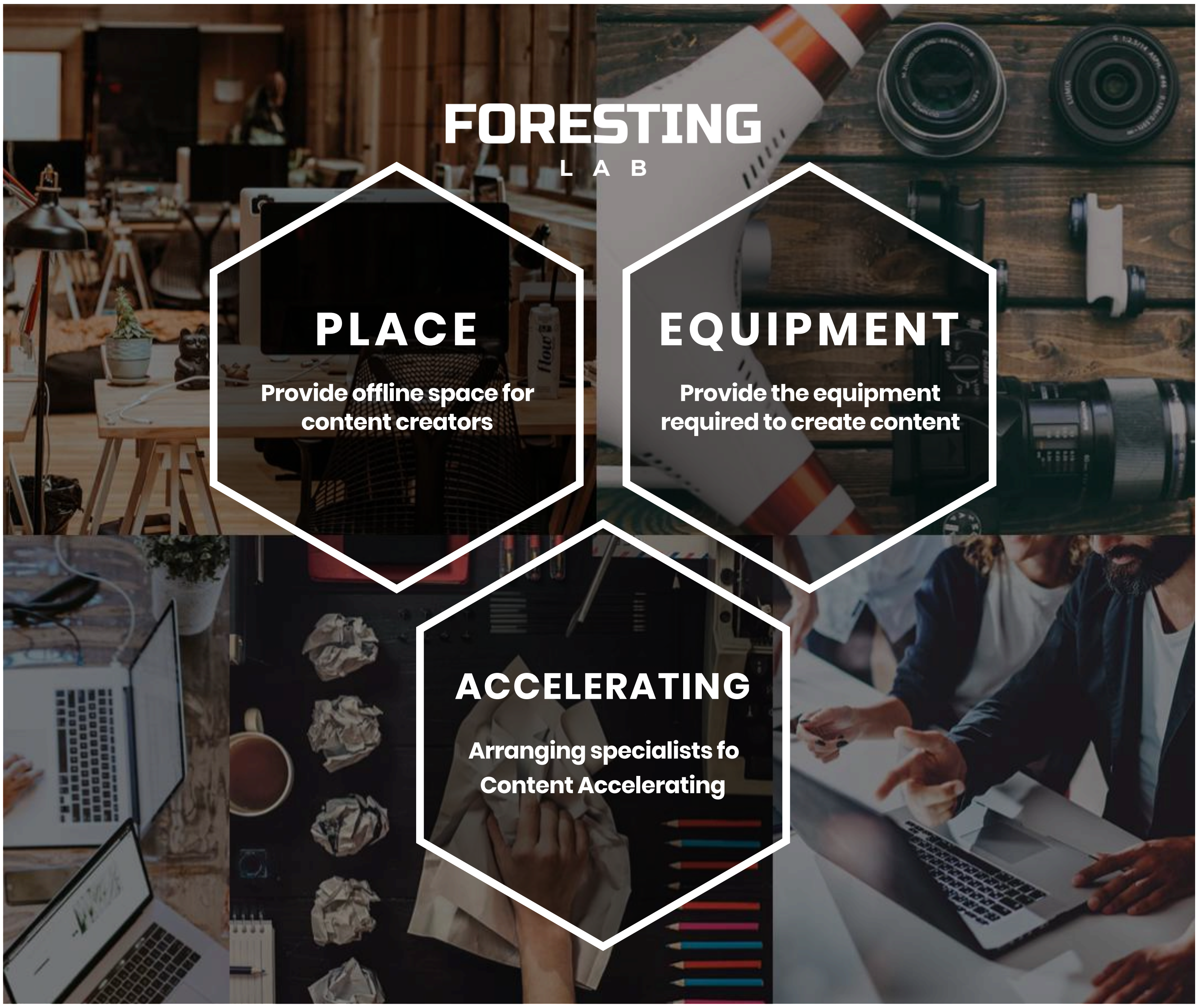
Users could not fully focus on content creation before. Some were categorized as self-employed or had to suffer economic difficulties such as low income. Financial services from existing banks are based on income, money transactions and credit ratings. Therefore this platform will lead to better content creation, enhance the quality of the content across the FORESTING platform, and ultimately lead to a virtuous circle structure that extends the rapid expansion and impact of the FORESTING platform.

2.5 FORESTING Lab

“Innovating your dreams”

The purpose of FORESTING Lab is to provide infrastructures for communities who participate in the FORESTING Network and support content creators who want to make content and post on the FORESTING platform.

The FORESTING Lab runs an offline collaborative space for FORESTING users. FORESTING's collaborative space is accessible to any participant in the FORESTING Network and is used fully to expand the FORESTING Network and develop the community. This space provides a place for the users at the core of the FORESTING Network to create higher quality content, along with the equipment needed such as cameras, microphones, lights, speakers, and instruments. Users no longer have to give up being a content creator because they cannot afford the space or equipment to create the content. By doing this, FORESTING will be able to offer high-quality content and build a stronger post-staging ecosystem.


FORESTING
LAB
PLACE
Provide offline space for content creators
EQUIPMENT
Provide the equipment required to create content
ACCELERATING
Arranging specialists fo Content Accelerating

Chapter 3

FORESTING

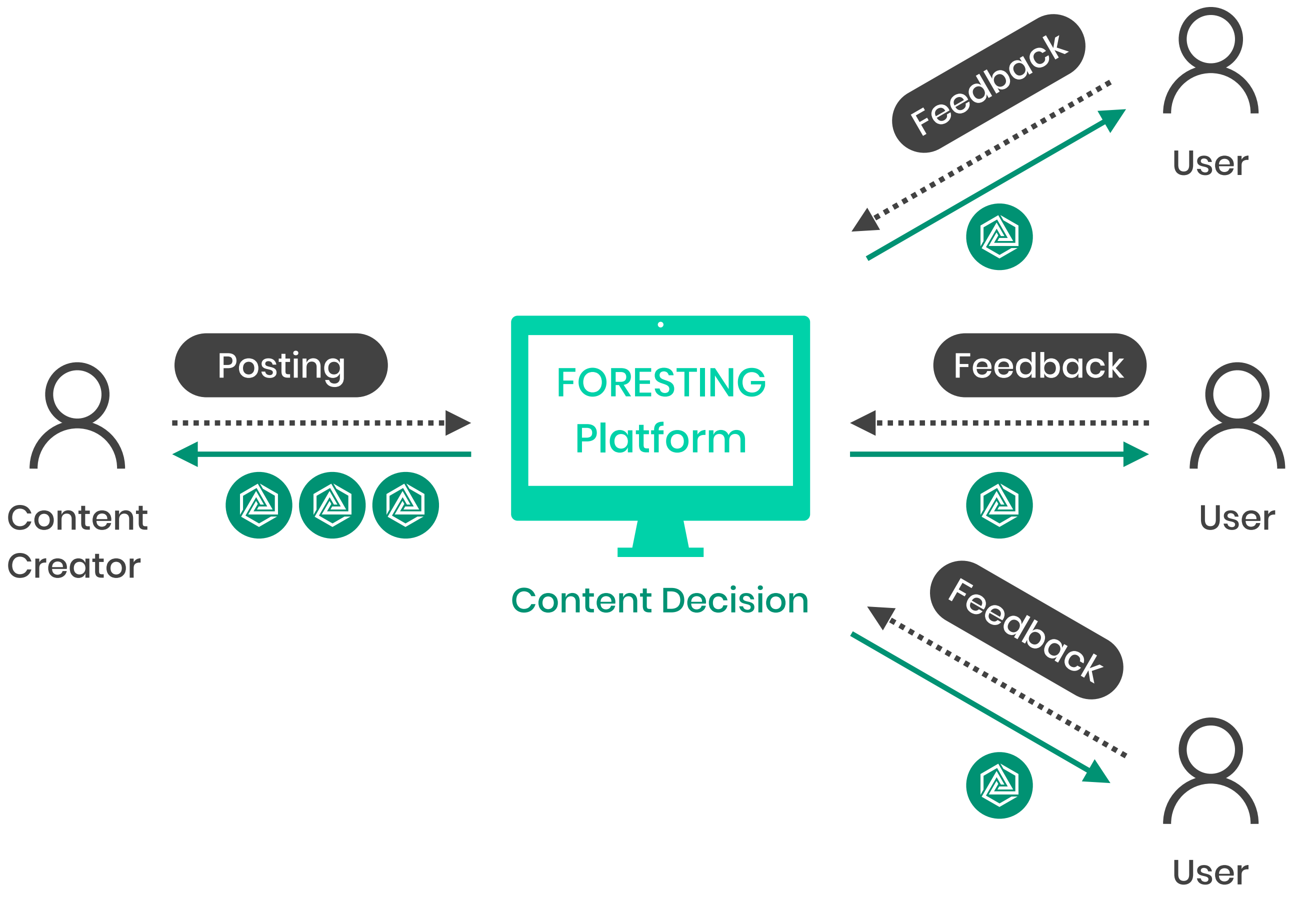
“Connecting the world and making lives more valuable”

3.1 Roles and Structures of FORESTING

FORESTING is available to anyone without prior knowledge of blockchain and cryptocurrency. Anyone in the world can easily profit from FORESTING, and just being active within the platform is rewarded with PTON.

FORESTING, a new concept of social media, distributes the revenue generated by the content to all users who contribute to it. In FORESTING, content creators no longer have to rely on the funds from followers and advertisers. Instead, users can benefit economically just by getting 'Likes' through the use of blockchain technologies and cryptocurrency. Blockchain technologies enable users to support content creators without losing anything, and users can also tap on incentives to post comments to other content creators or to 'Like' them.

[FORESTING Contents Reward Mechanism]



3.2 Core Features

Similar projects have been appearing in the market since the first blockchain-based social media platform, Steemit's successful debut. FORESTING uses the best services to implement the perfect blockchain for social networks.

I. User-Friendly UX/UI

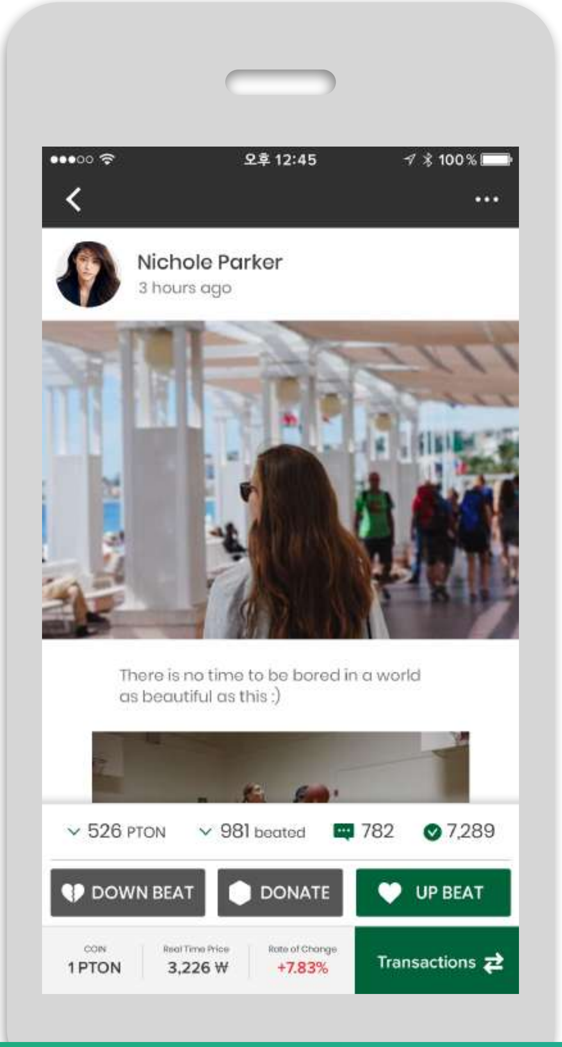
II. Device Optimization

III. Categories for Social Media

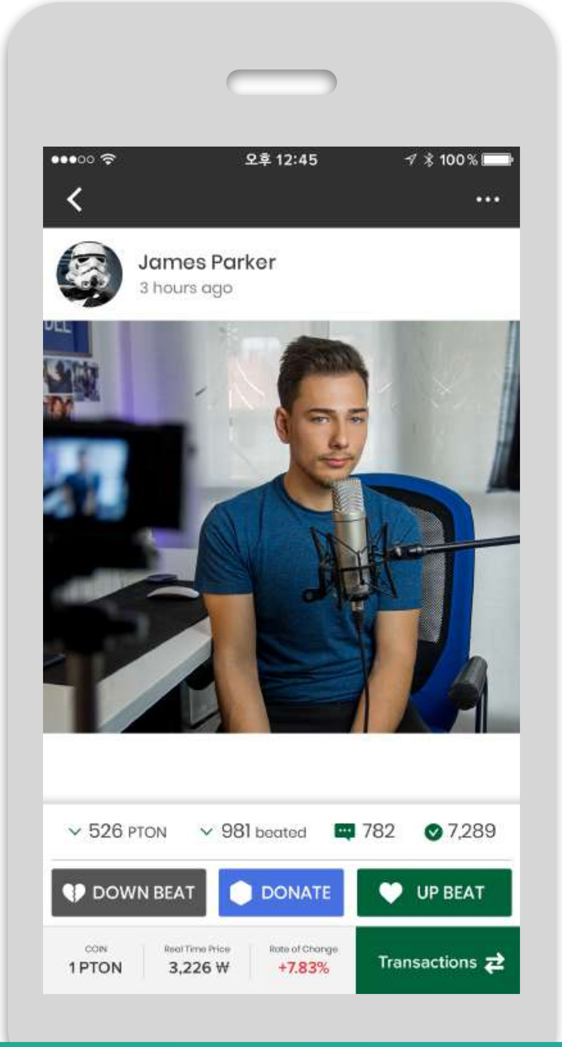
IV. Supports All Forms of Content

I. User-Friendly UX/UI

As a blockchain based social media service, FORESTING's goal is to provide users with an easy and convenient service, like on traditional social media platforms, while also providing real-time measurements and transactions of their content values. The platform also aims to provide a service that is intuitive to users, rather than a service that requires them to be aware of difficult concepts, like blockchain technology and cryptocurrency. For this purpose, we will provide a service equipped with the best UX/UI. In addition, the platform supports voluntary activities such as registering, withdrawing, and deleting posts. For content providers, 'Protection of Deletion and Personalization' and hiding options are available for posts that users don't want to be publicly viewable.



There is no time to be bored in a world as beautiful as this :)



II. Device Optimization

FORESTING is offering a new ecosystem that integrates people's lifestyles and income into a single mobile app. This makes it easy for FORESTING users to share and influence their content anytime, anywhere.

FORESTING will be designed for the users to share text, images, and videos easily. People can comfortably write comments, send messages, and navigate chronological feeds.

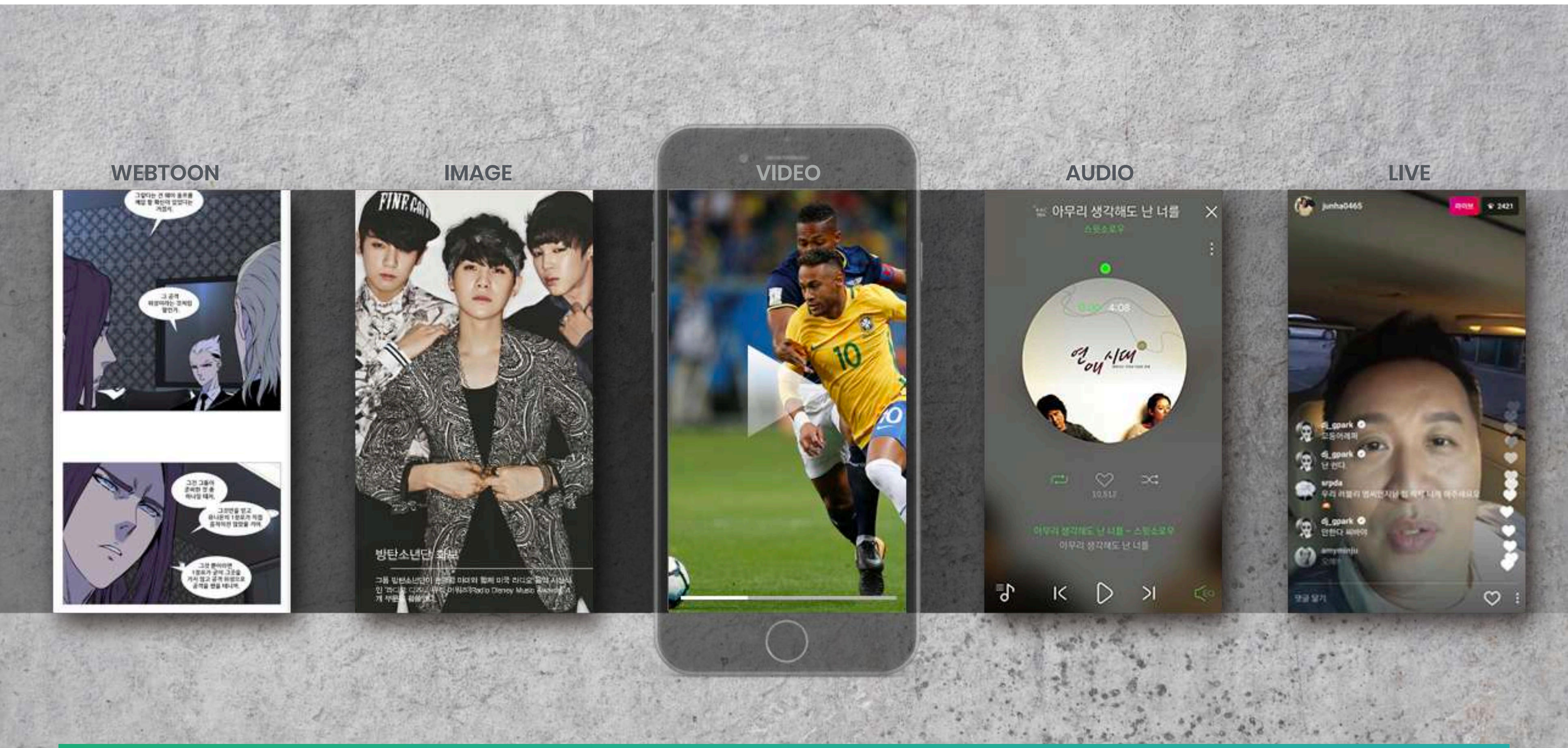
The content of FORESTING can spread rapidly across the public.
It is uploaded and shared live, and will be a unique source of social media like Facebook and Instagram, which have seen hundreds of millions of viral downloads over the years.

III. Major Categories for Social Media

Most of the social media related to the blockchain, including Steemit, is focused on specific categories such as ‘blockchain’, ‘ICO’, and ‘Cryptocurrency’.

Given the concentration of specific categories, and only having about 1 million users, Steemit is more like a community service, rather than a real social media platform like Facebook, YouTube, and Instagram, that all have more than a billion users.

In order to be a real social media platform, rather than a community platform, FORESTING is focused on major categories, ranging from lifestyle to beauty, entertainment, and so on.



IV. Supports all forms of content

FORESTING provides users with the best security and privacy system possible, using blockchain technologies. One of the key components of blockchain technology is that it does not have a broker. The block is processed into a block after the encryption process, including the transaction details, transaction summary, and block information from the previous transaction. The encrypted block contains a full list of transactions and blocks until the last minute, making it look like a chain.

3.3 Strengths

The FORESTING Network also boasts the following strengths:

I. Synchronizing Preferred Exchanges

II. Masternode based P2P Transactions

III. Coin Shooting(Donation for Content Creators)

IV. Open Market for Advertisement

I. Synchronizing Preferred Exchanges

While targeting global services, FORESTING also wants to make it easier for its users to monetize to their content. For this purpose, we will display the current coin market in real time in the app. In conjunction with main exchange offices around the world, we will make it easy to exchange coins from anywhere.

For this purpose, a link button for the country you are referring to will be installed at the bottom of the page, and decentralized voting and messaging will be implemented for community-based developments and projects. As a result, it allows for experiences such as DAO in managing community projects while maintaining simplicity from a technical standpoint.

FORESTING will allow network transaction fees to be paid with custom tokens. Orders must be sent to the next decentralized exchange where these transactions are exchanged with the main network tokens.

II. Masternode Based P2P Transactions

By default, the platform opens at least 10 coins per user. After opening, you can update them. Each blockchain can have independent settings. Coin-specific blockchain node compiles and the installations are automated. An RPC module is provided to access each coin. It provides basic operations and master nodes for node operation. Some coins may be presented with lightweight wallets. These master nodes, or wallets, can be connected to FORESTING by payment channels, state channels and so on.

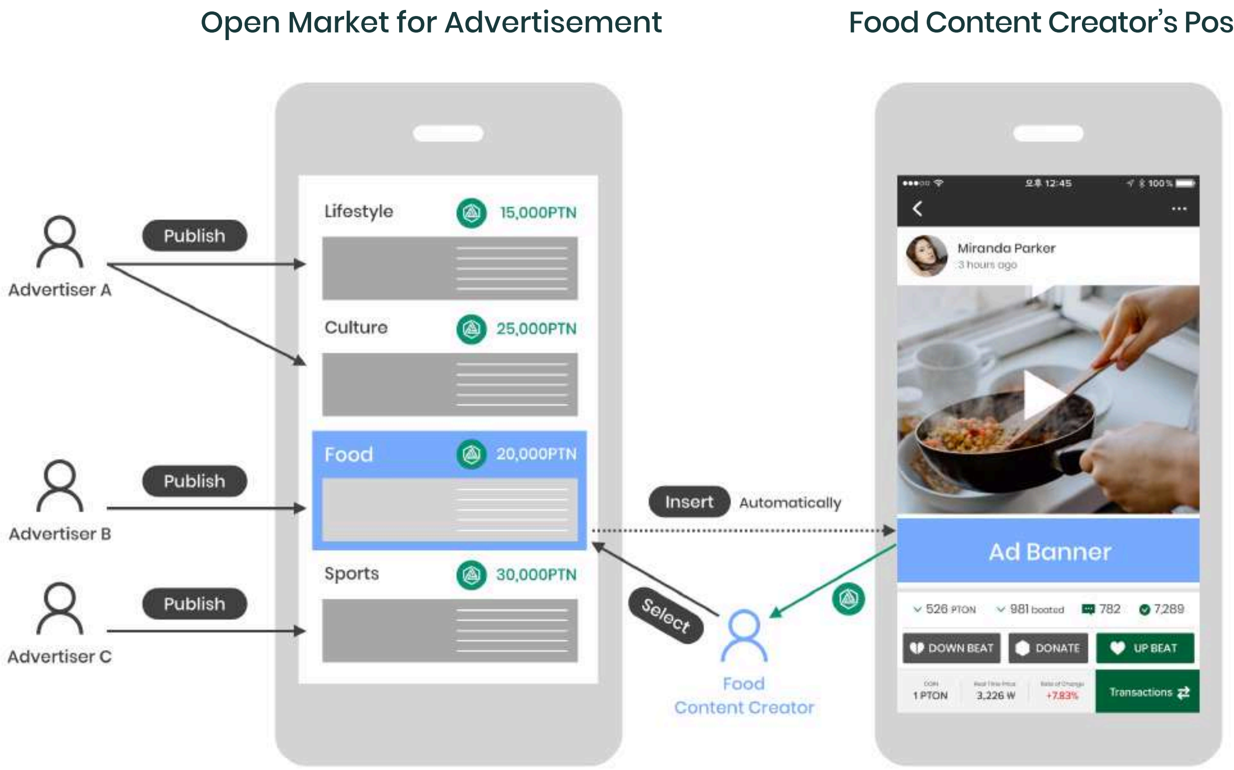
FORESTING Dex enables the sale of PTON tokens and creates a system for collecting current market information. This enables the sale of general, split, tender, and split bids without polling. For this purpose, we will use the tools to close deals, push notices, and push notifications, social networking services, email, etc., and can use different types of transaction history and statistical queries. It also enables the use of group chat rooms using zn-SNARKs libraries and provides messenger services for user transaction-related inquiries and discussions.

III. Coin Shooting(Donation for Content Creators)

In addition to supporting other users through the 'Like' button, users can also donate the PTON token by pressing the 'Donation' button under the post. This feature can also be seen as one of the ways to send a FORESTING token directly to other users, but it is difference in that donation behavior is shown openly in the posts. The donator could use PTON he or she already owns or buy PTON from preferred exchange platform in which PTON is already listed for the donation.

IV. Open Market for Advertisement

In traditional social media, a company operating advertisements and campaigns accesses and uses the users' databases through certain marketing tools. However, in FORESTING, advertisers and advertising agencies can upload their advertisements and advertising proposals to the advertising pool category or communicate with content providers that meet their respective articles and concepts. Content creators will be rewarded through the interaction of other users with their content such as comments and 'Like'. They can also select the advertisements they want and post it on their content pages for rewards. That is, a content creator can make profit over a period of time. This creates a virtuous circle in which content creators try to create better content, while FORESTING users come across better content.



A Virtuous Circle

Content creators try to create better content, while FORESTING users discover better content.

Chapter 4

FORESTING BANK

“Creating a unique credit rating system”

4.1 Purpose of FORESTING Bank Establishment

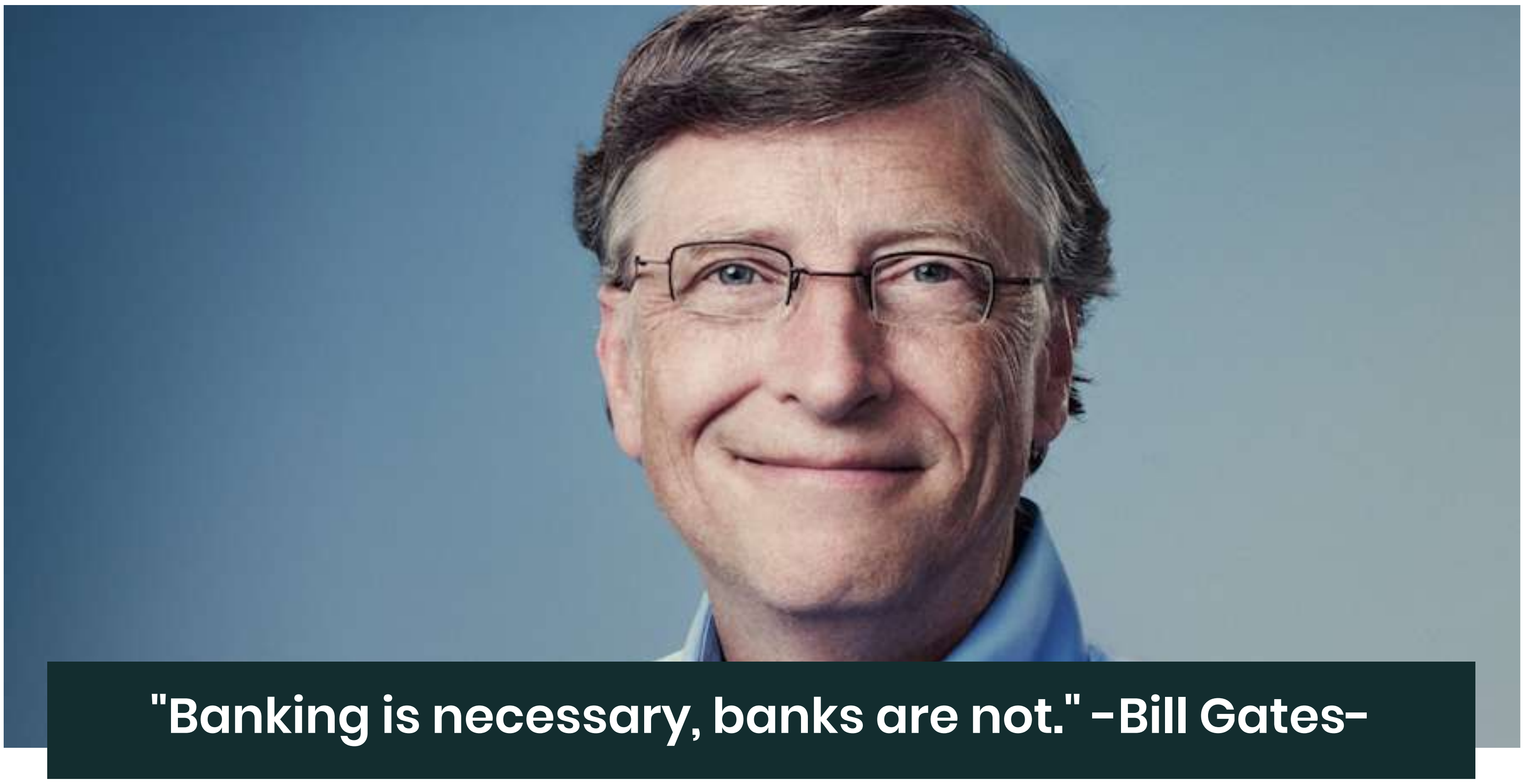
At the center of the FORESTING Network is the user. In addition to providing content, users also contribute to the platform's growth with a variety of types of content. In particular, users may no longer rely on advertising companies and centralized platforms to directly exchange their content for real value. And as the influence of the FORESTING platform continues to grow in society, 'Influencers' will start to appear just like they did on YouTube and other platforms. It will emerge as another profession that children dream of.

However, the primary income from the content does not directly influence the social ratings of users. While major social media influencers on YouTube, Instagram, Twitch, and Afreeca TV, have been known to raise millions of dollars a year, it is only applicable to a few popular influencers. Most of the people who work with professional influencers are self-employed, except for celebrities who work with large business and entertainment companies on their backs. Their income is not fixed, and some of them have a hard time dealing with their daily lives.

Furthermore, they are not classified as common jobs by traditional banking systems, in which they cannot not receive a positive credit ratings. This is because they are subject to an independent credit rating regardless of their economic activities which can result in a negative credit rating score. This means that they cannot perform common financial activities, such as getting loans. Talented creators face a lot of pressure to buy expensive equipment. In addition to spending time creating content they should also make these investments to keep up with their competitors. To solve these problems, FORESTING Bank will provide a digital banking service that is available to anyone who uses FORESTING. It provides personalized financial services for content creators that contribute to the growing platform and community. By doing so, the content provider will be able to focus on creating his/her own content, and the distribution of good content will make the FORESTING network more influential.

4.2 Digicrypto Bank "Digital Bank + Crypto Bank"

I. Challenges to Traditional Banks



"Banking is necessary, banks are not." -Bill Gates-

It is already well known that traditional banks are conservative. Recent changes have also been made to these banking institutions. There has been the establishment of new overseas transfer services and security systems based on blockchain technology with traditional financial institutions and FinTech companies, document notarization, and mobile optimization activities, including consideration of the user's UX & UI. Financial innovation has been happening throughout the industry, such as finding ways to make improvements on the SWIFT system with blockchain technology, which has been slow and expensive for overseas transfers for about since 1973.

In addition, there are compelling examples of global bank startups offering most of the financial services traditional banks provide through non face-to-face services, rather than simple financial services.

[Global Bank Startups initiating financial innovation]

FORESTING Bank makes use of its innovative digital banking model which deviates from the traditional banking system, and is based on the needs of its clients and of the digital bank's middle code, which is a blockchain based financial service.

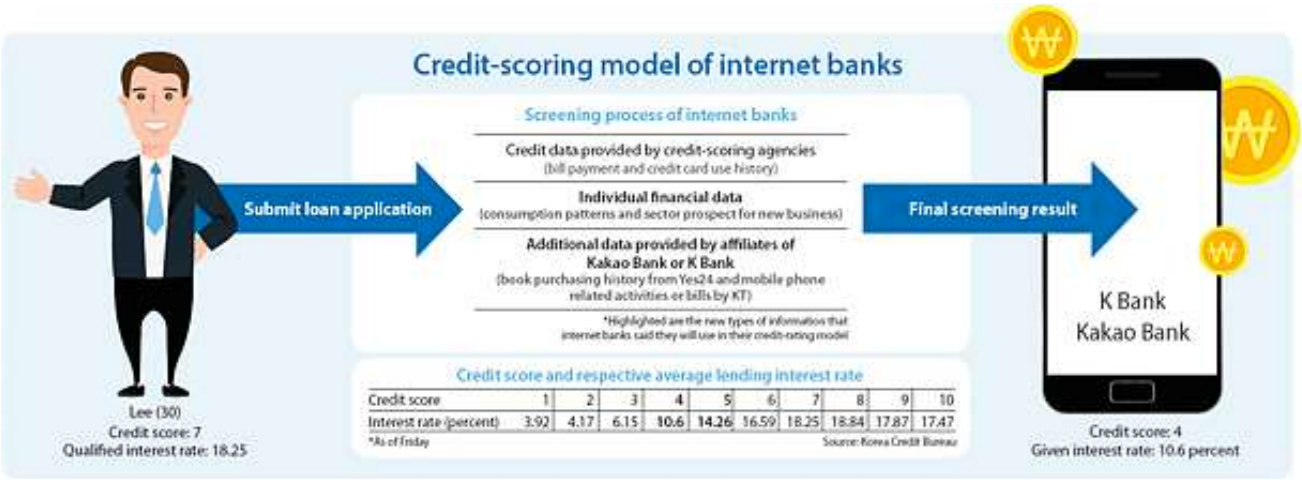
FORESTING Bank = Digital Bank + Crypto Bank = Digicrypto Bank

FORESTING Bank will provide a non face-to-face financial service that extends directly to the Internet, PCs, and even smartphones, which would be applicable with existing digital banking services. To achieve this, the FORESTING Bank has come up with a new credit rating model.

II. Traditional Credit Rating Method

The existing CSS Credit Evaluation Method predicts the customer's ability to repay their financial statements by viewing and grading the customer's financial history to provide information to financial institutions. Therefore, if CB does not have financial information data, financial activities such as loans and credit card issuance are restricted as new users cannot be assessed, even among customers with good repayment ability.

While the Financial Supervisory Service and the Financial Services Commission present various methods of supply such as warranty insurance related products, the actual situation is not well modelled as it lacks the most important credit assessment information.


Credit-scoring model of internet banks
Screening process of internet banks
Credit data provided by credit-scoring agencies
(bill payment and credit card use history)
Individual financial data
(consumption patterns and sector prospect for new business)
Additional data provided by affiliates of Kakao Bank or K Bank
(book purchasing history from Yes24 and mobile phone related activities or bills by KT)
*Highlighted are the new types of information that internet banks said they will use in their credit-rating model
Submit loan application
Final screening result
K Bank
Kakao Bank
Lee (30)
Credit score: 7
Qualified interest rate: 18.25
Credit score: 4
Given interest rate: 10.6 percent
Credit score and respective average lending interest rate

Credit score	1	2	3	4	5	6	7	8	9	10
Interest rate (percent)	3.92	4.17	6.15	10.6	14.26	16.59	18.25	18.84	17.87	17.47

*As of Friday
Source: Korea Credit Bureau

[Source : http://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3029761]

Of course, there are moves in the market to replace traditional credit rating methods, and some companies are becoming passionate about using online data and social network activity data.

From Saving Money to Saving Value > Open Digital Assets

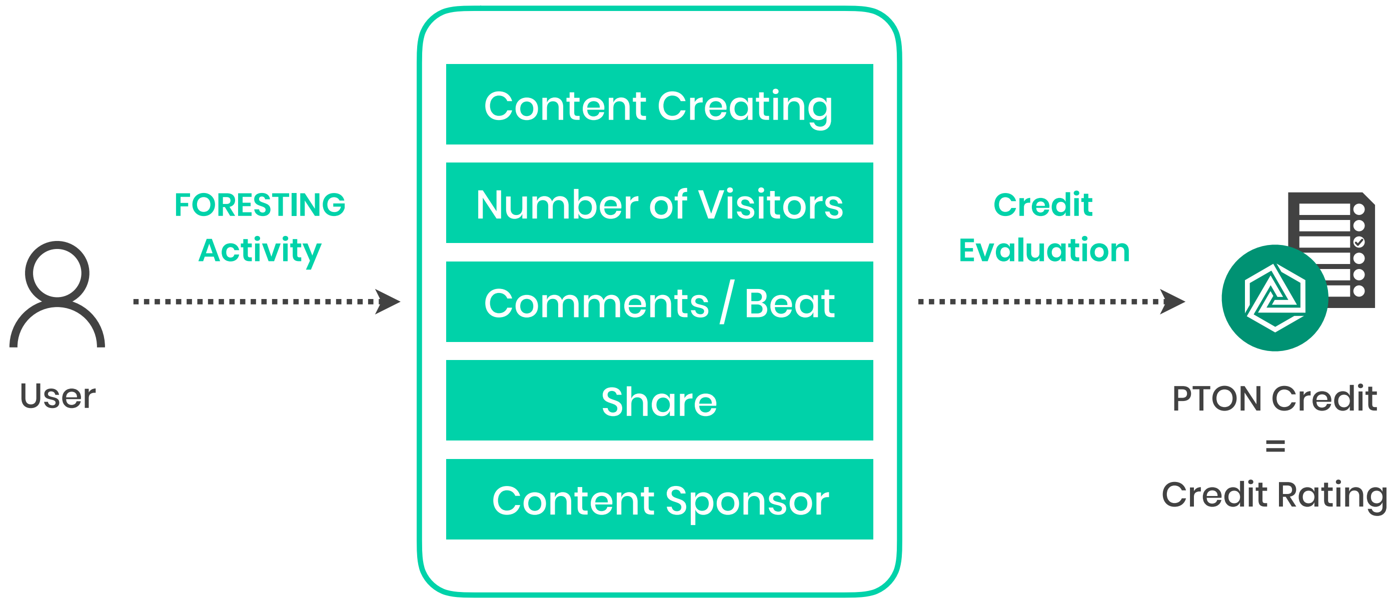
ex) World of Warcraft Gold (game item) deposit to the current checking account for digital assets

III. FORESTING Bank Credit Assessment Method

In addition to promoting credit rating through social activities, FORESTING Bank will introduce a credit rating structure according to its contribution assessment model, which only evaluates FORESTING platform contributions from FORESTING users. Every FORESTING user contributes to the growth of the FORESTING platform in a variety of ways, ranging from creating and sharing, as well as writing comments and viewing. Since the FORESTING platform's blockchain technology offers the benefit of complete transparency through a highly integrated structure, all submissions and transactions appear on the blockchain through timestamps.

The FORESTING Bank collects the data shown on the FORESTING blockchain to measure the degree of connection, content creation, coin security, and the contribution to FORESTING's growth. By doing so, the users who have opened accounts through FORESTING Bank can check their platform contributions at any time, and can raise funds required to create content. In fact, FORESTING will transform this into a credit rating assessment based on the creation of values for users rather than on a traditional credit rating assessment based on the financial histories provided by the traditional banks. Users can improve their credit ratings just by using social media, and can have an amazing experience with greater economic potential. Based on this, FORESTING Network will provide financial services that all users will be able to get access to, anytime, anywhere.

Evaluation of platform Contribution



[FORESTING Bank Credit Rating Method]

In particular, the financial services offered by existing banks are based on income, money transactions, and credit ratings. Users will be able to fully focus on creating content through FORESTING by becoming 'Influencers' which had been difficult before due to economic difficulties such as self-employment or low income. This will lead to better content creation, enhance the quality of the content across the FORESTING platform, and ultimately lead to a virtuous circling structure that extends the rapid expansion and impact of the FORESTING platform.

4.3 The Financial Innovation is the Innovation of Society.

FORESTING believes that the core of financial innovation is not technology rather the attention to society, but should be focused on problems faced by society and the actions we must take to address them. With the role of FORESTING Bank for the FORESTING Network, FORESTING Bank's vision of our society is clear. FORESTING Bank will contribute to society through constant challenges and innovation to enhance economic freedom and the value of life for more people in our society.

Citizens of Bangladesh had to pay back the interest they borrowed from loan sharks with what they earned working all day. Because of that, the large part of the population was unable to get out of poverty, and the economist Muhammad Yunus, who observed this, went to a bank in Bangladesh saying, " Why not lend money to the poor?". The bank responded, “We can not lend it to them because they do not have collateral.” Yunus established his own bank in 1976 with the condition that only less than 150 dollars could be checked out and only by the bottom 25 percent, without collateral or proof of identity. It was a micro-processing credit loan bank that lent money at low interest to be paid back over a long period of time.

[Muhammad Yunus, Nobel Peace Prize Winner in 2006]

Now it is one of the largest banks in Bangladesh, having lended 160 billion Dhaka (approx. 3.6 trillion won) across 1,117 branches throughout the country. Surprisingly, the annual repayment rate has been higher than 90 percent on average since its establishment. If there is a bad credit rating at one branch, other borrowers can also offer credit to each other’s loan limits. With the money borrowed, people can invest in carts, sewing machines, calves, and other necessities for their economic activities. Unexpectedly, the rate of recovery has reached 98 percent and citizens are now able to get out of poverty. For his work, Muhammad Yunus received the Nobel Peace Prize in 2006.

Financial innovation is never about capital and technology alone. It comes from the interest and love we have in society. FORESTING Bank will work to develop innovative financial services for small business owners, low-income workers, and vulnerable social groups, so that more people can continue to enjoy economic freedom and increase their value in life.

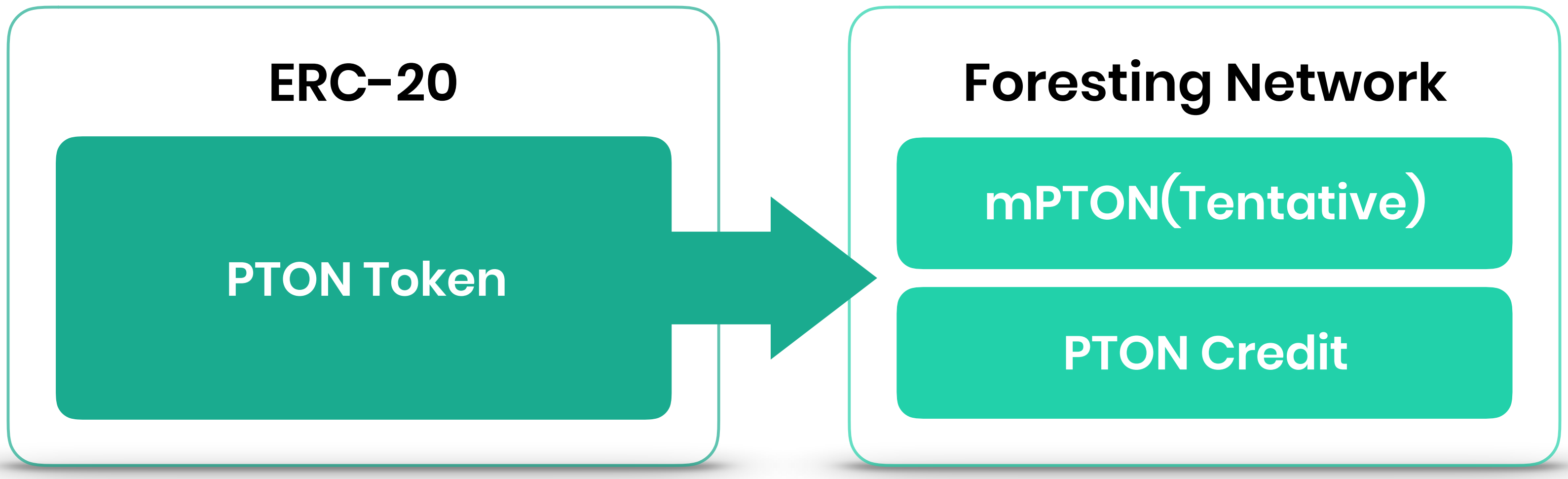
Chapter 5

PTON ECOSYSTEM

Leading the coin ecosystem to the next level

5.1 Value Model

The initial FORESTING system is built on the Ethereum network. As the project progresses, 24 billion PTON Tokens are swapped with the mPTON (tentative name) coins at a 1:1 rate after the mainnet launch. FORESTING Bank and PTON credit, which is a credit evaluation standard based on platform contributions that are connected with content creation and curation, will operate Token Economy.



Prior to the FORESTING mainnet launch, the rewards for content delivery until beta testing and operation of the super node are managed through the PTON Token payment assigned to the Reward Pool in Token Distribution. In addition, FORESTING conducts projects faster, more efficiently and more fairly through the board program that encourages participation by third parties.

In this regard, the value model to be covered in this sector is an evaluation model for the FORESTING network mainnet launch, the factors for the development of the PTON value model is as follows.

Total Number of Coin = (a)
Annual Return = Inflation = 6% = (b)
Content Reward = 75% of (b) = (c)
Supernode Reward = 25% of (b) = (d)
Daily Issued Coin = (b)/365 = (e)
Users (optimistic) = (f)
Users (conservative) = (f1)
Users (pessimistic) = (f2)
DAU (20% of (f)) = (g)
Like = Voting ((g)*5) = (h)
Daily Issued Coin for Content Reward ((c)/365) = (i)
1Like = (x)Coin = (i)/(h) = (j)
Daily Posted Contents = 20% of (g) = (k)
Like per a Content ((h)/(k)) = (l)
Daily Content Reward per a Content = (j)(l) = (m)

Factor (a) in the table above is mPTON (tentative name), which is exchanged at a 1:1 ratio with 24 billion existing PTON tokens while launching the mainnet. Afterwards, about 6 % of coins are to be issued each year. As a result, (c) 4 % of annual return (b) 6 % is paid to the content creator and the voting participant, and (d) 2 % is paid to the FORESTING network.

(a) = Number of Issued Coins at the Beginning = X = 24,000,000,000

(b) = Annual Return = Inflation Rate = Approximately 6% = (c) + (d)

(c) = Content Rewards = 4%

(d) = Supernode Rewards = 2%

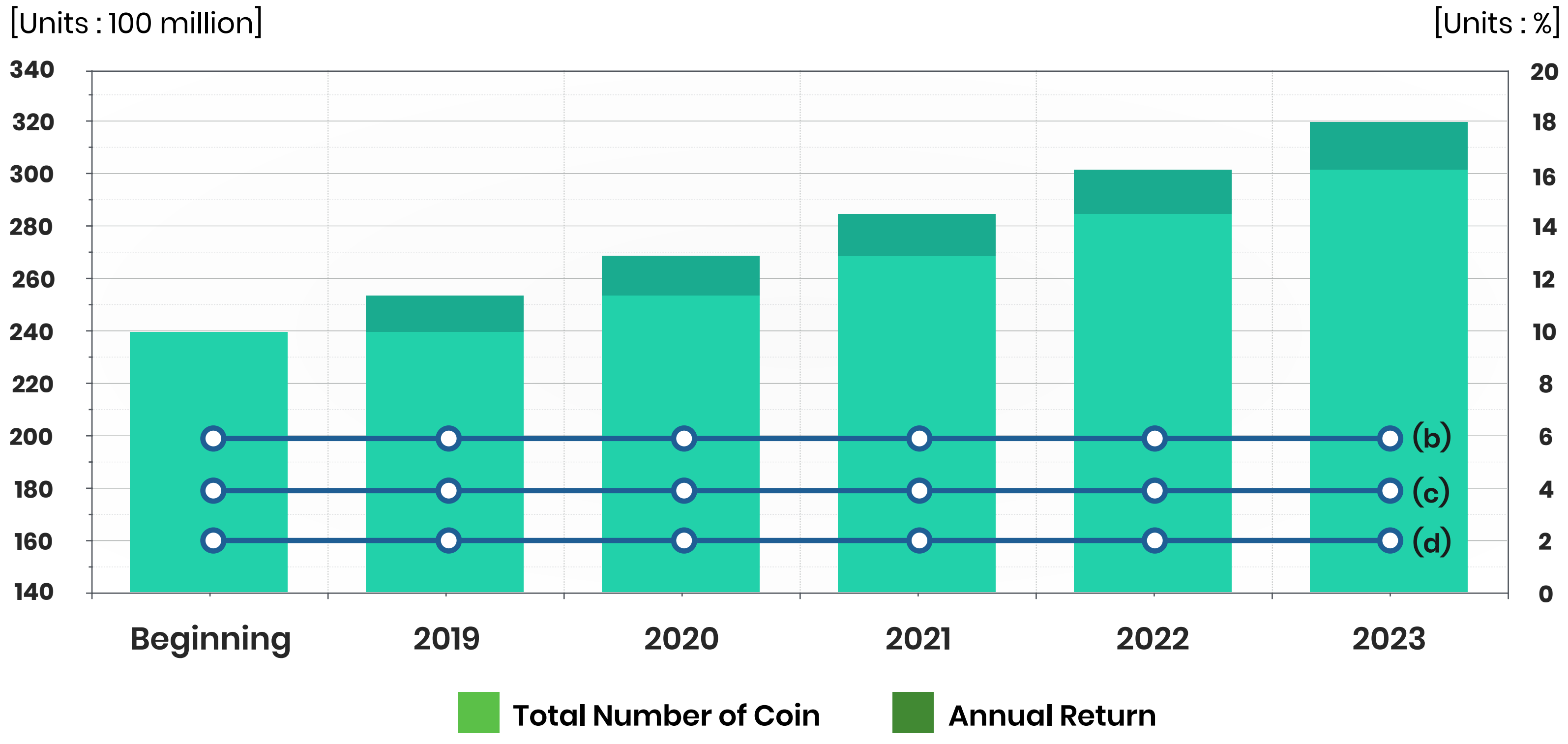
Many blockchain projects are currently underway with PoS methods. In most projects, annual return is set to between 0.5 % and 8 %. In addition, the total amount of coin flow gradually increases over time. But the amount of tokens issued on a regular basis would be similar or equal in each time period, so the compensation paid to the Supernode operator is gradually reduced.

However, to maintain the annual return 6 % rate, the FORESTING network will increase the absolute publication amount in the same rate. For this reason, in a year after the mainnet launch, the total volume of PTON will increase by 6 %. However, in 5 years the total PTON value would not increase by 30 %, but by 34%, from the initial point of entry.

After 1 Year = X + 0.06X = 1.06X = 25,440,000,000

After 5 Years = X(1.06)^5 = 1.34X = 32,117,413,862

Furthermore, although the compensation paid to the Supernode is 2 %, the limited supernode(32-128 to be confirmed by further testing) will possess 25 % of the total PTON revenue per annum. This allows it to earn higher rewards compared to other PoS projects.



The following table shows the key indicators of five-year estimation regarding content creator compensation and platform expansion.

		Y1	Y2	Y3	Y4	Y5
Optimistic	User	10,000,000	36,000,000	60,800,000	84,500,000	105,600,000
	DAU	2,000,000	7,200,000	12,160,000	16,900,000	21,120,000
	Like	10,000,000	36,000,000	60,800,000	84,500,000	105,600,000
	Daily Issued Coin for Content Reward	2,958,904	3,136,438	3,324,625	3,524,102	3,735,548
	Daily Content Reward per a Content	7.4	2.18	1.37	1.04	0.88
Conservative	User	8,000,000	28,800,000	48,640,000	67,600,000	84,480,000
	DAU	1,600,000	5,760,000	9,728,000	13,520,000	16,896,000
	Like	8,000,000	28,800,000	48,640,000	67,600,000	84,480,000
	Daily Issued Coin for Content Reward	2,958,904	3,136,438	3,324,625	3,524,102	3,735,548
	Daily Content Reward per a Content	9.25	2.72	1.71	1.30	1.11
Pessimistic	User	5,000,000	18,000,000	30,400,000	42,250,000	52,800,000
	DAU	1,000,000	3,600,000	6,080,000	8,450,000	10,560,000
	Like	5,000,000	18,000,000	30,400,000	42,250,000	52,800,000
	Daily Issued Coin for Content Reward	2,958,904	3,136,438	3,324,625	3,524,102	3,735,548
	Daily Content Reward per a Content	14.79	4.36	2.73	2.09	1.77

For the number of users (f), there are three expected indicators were entered : optimistic, conservative, and pessimistic. First of all, for optimistic forecasting, we apply Facebook's user growth indicator from 2008 to 2012, since it has been the most popular social network since iPhone was introduced in 2007. The public impact of traditional social media cannot be directly compared with that of blockchain-based social network services since the former have been growing proportionally with smartphones. Therefore, the market size of FORESTING has been reduced by one-tenth. In addition, conservative (f1) and pessimistic (f2) user totals, will be discounted by 20 % and 30 % respectively from optimistic (f) user totals. As a result, sub-index such as DAU(g) based on user counts are all changed for optimistic, conservative, and pessimistic according to their circumstances.

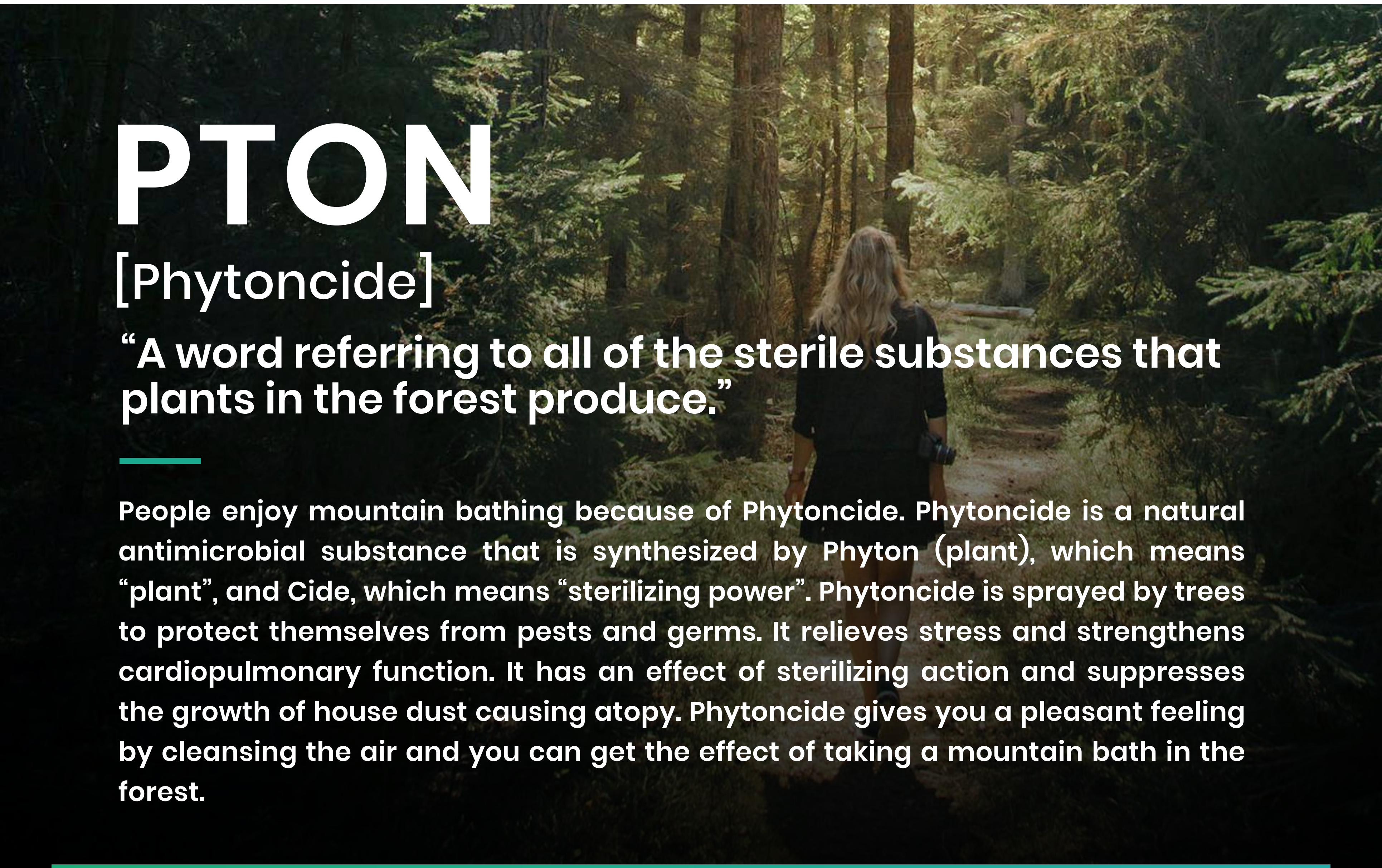
In particular, there are 7.4 coins (f) that will be compensated per package in 2019. This structure reduces the number of coins that can be paid over time. However, this section should be considered in conjunction with the increase in the value of PTON coins which are not included in the factor above. For most content platforms, the value of the platform increases as multiple activity indicators, such the MAU, DAU, PV and ARPU increase. Despite the decrease in compensated coins per transaction, the value to be compensated can increase as the platform expands rapidly.

Based on the factors above, since the number of daily votes is limited to 5, (h) is 5 times (g). Assuming the fact that all visitors participate only in the voting, DAU is satisfactory by making up 20% of the total number of users.

We will also continue to disclose the weight of the content voting power, depending on the PTON credit holdings, during the alpha and beta tests.

5.2. PTON Usage

PTON is a coin used in FORESTING. PTON's market value determines the value of the reward pool for the participants that contribute to FORESTING. Unlike traditional mining methods, PTON is created by the contribution of participants to FORESTING. PTON guarantees that people who contribute to FORESTING benefit from the app.



PTON

[Phytoncide]

"A word referring to all of the sterile substances that plants in the forest produce."

People enjoy mountain bathing because of Phytoncide. Phytoncide is a natural antimicrobial substance that is synthesized by Phyton (plant), which means "plant", and Cide, which means "sterilizing power". Phytoncide is sprayed by trees to protect themselves from pests and germs. It relieves stress and strengthens cardiopulmonary function. It has an effect of sterilizing action and suppresses the growth of house dust causing atopy. Phytoncide gives you a pleasant feeling by cleansing the air and you can get the effect of taking a mountain bath in the forest.

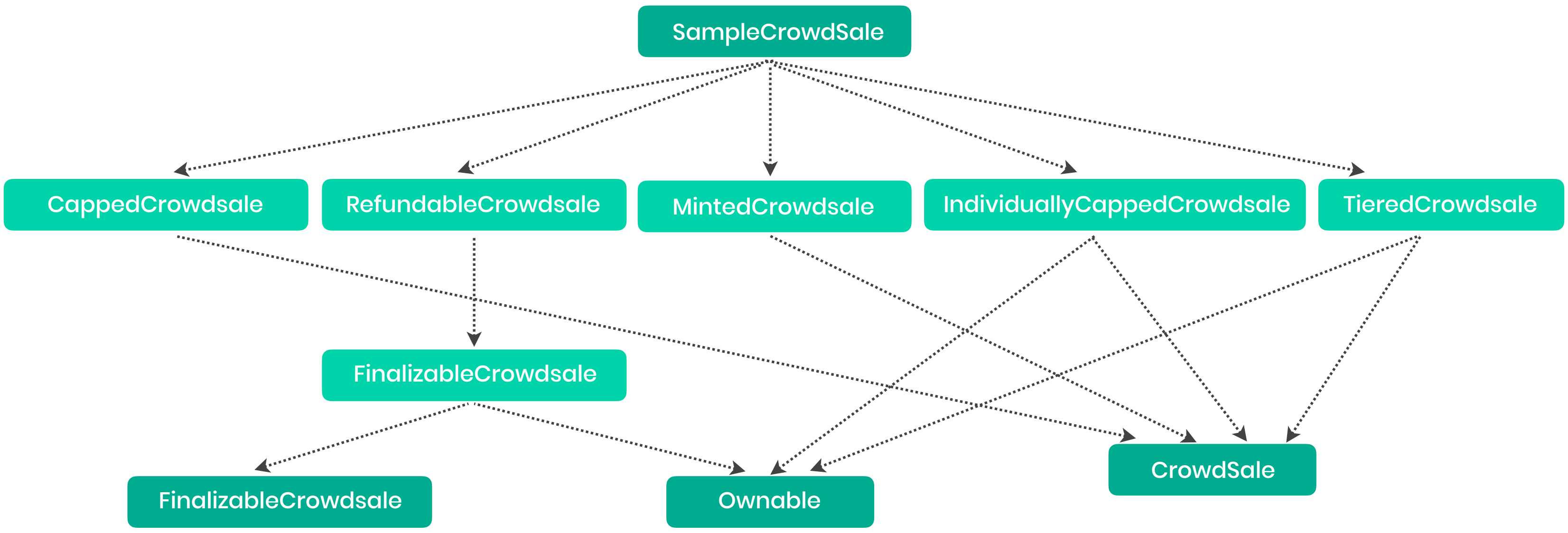
5.3. PTON ECONOMY

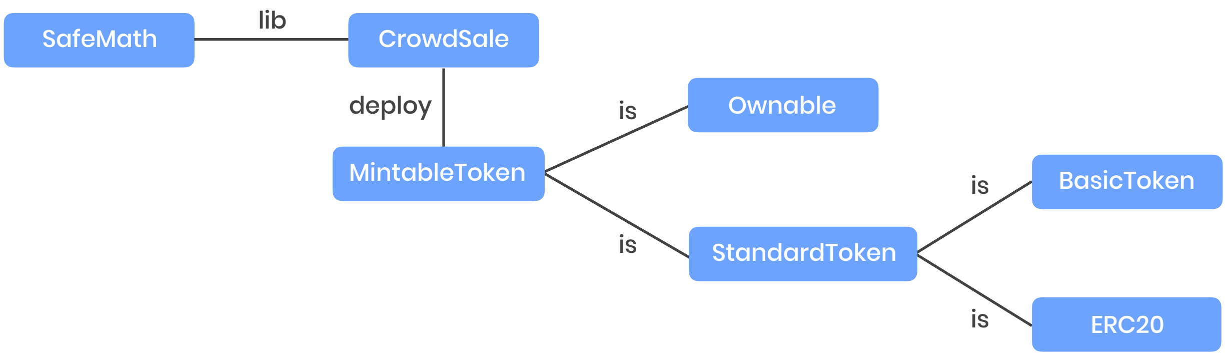
There are many examples of the idea of decentralized digital money before the fame of Bitcoin, but Digicash (1992), Cybercach (1994), e-Gold (1996) are a few examples.
But Bitcoin is the first subject to have no power, and at the same time create a system that all participants can trust.
Bitcoin is different from the previous technology because the system has incorporated, not only computer engineering and cryptographic factors, but also economic factors that drive participants' behavior. Until then, whatever technology was applied to the system, eventually someone had to maintain rules and order within the network with responsibility and authority. However, Bitcoin has created an 'incentive structure' to replace these rules and orders with protocols and at the same time to follow protocol rules. Bitcoin networks must be well-structured to allow participants to benefit. A large number of people around the world are devising new services that use blockchain, such as Bitcoins, which have to be equipped with internal services and an economic system tailored to their needs. In the PTON Economy, you can easily design an economic system that runs on top of any DApp you create.

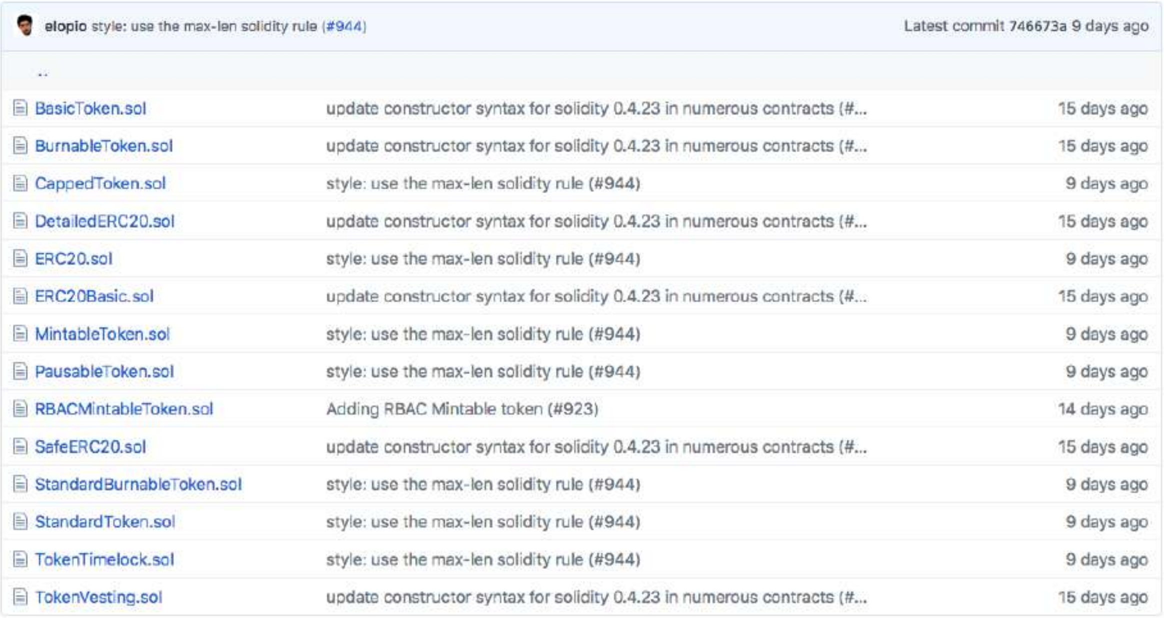
On what criteria will rewards (tokens) be given, and to whom?
How will the tokens be valued?
What are the incentives for people to hold tokens?
How will the growth of the network and the increase in the value of tokens work?
How will the price change of tokens be resolved?
The token Economy for FORESTING will have the infrastructure of the economic structure already built and will be designed and implemented in conjunction with the growth of FORESTING. It is designed according to the nature of foresters, and it is possible to design an economy suitable for all content creators and curators.

5.3.1 Truffle Framework

The development framework for issuing tokens uses the Truffle Framework, and the Open Zeppelin Contract Library, which conforms to standard interfaces such as ERC20, is available and can automatically handle a series of processes for developing smart contracts from test to deployment.







elopio style: use the max-len solidity rule (#944) Latest commit 746673a 9 days ago

..

BasicToken.sol	update constructor syntax for solidity 0.4.23 in numerous contracts (#...	15 days ago
BurnableToken.sol	update constructor syntax for solidity 0.4.23 in numerous contracts (#...	15 days ago
CappedToken.sol	style: use the max-len solidity rule (#944)	9 days ago
DetailedERC20.sol	update constructor syntax for solidity 0.4.23 in numerous contracts (#...	15 days ago
ERC20.sol	style: use the max-len solidity rule (#944)	9 days ago
ERC20Basic.sol	update constructor syntax for solidity 0.4.23 in numerous contracts (#...	15 days ago
MintableToken.sol	style: use the max-len solidity rule (#944)	9 days ago
PausableToken.sol	style: use the max-len solidity rule (#944)	9 days ago
RBACMintableToken.sol	Adding RBAC Mintable token (#923)	14 days ago
SafeERC20.sol	update constructor syntax for solidity 0.4.23 in numerous contracts (#...	15 days ago
StandardBurnableToken.sol	style: use the max-len solidity rule (#944)	9 days ago
StandardToken.sol	style: use the max-len solidity rule (#944)	9 days ago
TokenTimelock.sol	style: use the max-len solidity rule (#944)	9 days ago
TokenVesting.sol	update constructor syntax for solidity 0.4.23 in numerous contracts (#...	15 days ago

The following sections will be implemented within the Open Zeppelin ERC20 smart contract library and truffle framework that have already been proven in accordance with Token Design Patterns that conform to PTON Economy.

5.4. VOTING SYSTEM

In social media services, service users try to express their opinions about a particular issue in the decision-making process. The network can give users the right to vote and collect opinions efficiently. The Forrester voting system combines voting rights and tokens into a pattern for collecting opinions.

In Voting Token, the voting rights can be either the token itself or a number on the network. FORESTING is gives a PTON CREDIT as a number on the network that is proportional to the PTON token.

The decision target through PTON CREDIT reflects the opinions of the users of the network from the symbol marking of all content, such as community posts. For the results to reflect the opinions of the network, it is important to limit the malicious behavior and to engage many users in voting. In order to encourage users to participate in the vote, in addition to participating in the decision-making process, the compensation reward proportional to the PTON CREDIT is distributed. It also connects directly and indirectly with PTON CREDIT and PTON, which is also linked to the increase in the value of tokens in the network.

The following paragraphs will describe the important elements of PTON credit.

5.4.1 PTON CREDIT acquisition path and decision making – UpBeat

FORESTING is a social media service that uses blockchain and allows user who write articles and create content to like other users' posts. Users who receive likes are rewarded with tokens in the network, and viewers who vote will receive curation rewards.

There are two ways to stack PTON CREDIT in FORESTING. The first is 'activity,' which receives both PTON CREDIT and PTON as a reward for uploading content on the network or voting on other posts. By linking activity in the network with PTON CREDIT, it strengthens the character of the community in which users are required to participate. If you want to get additional PTON CREDIT, you can deposit PTON on the service and accumulate PTON CREDIT.

5.4.2 CONSTRAINTS OF MALICIOUS BEHAVIOR -DownBeat

FORESTING social media services are less critical. However, this decision can be exploited because it is directly related to monetary rewards. For example, for the sake of monetary gain, there is a risk that you will be indiscreetly voting or posting indiscriminate articles that are subject to compensation.

5.4.2.1 LIMITATION ACTIVITY

Activities in posting such as posting, commenting, and voting are all recorded on the blockchain. If the malicious user posts too much, or goes beyond the limits of the activity that the blockchain can accommodate, the service may become paralyzed. To prevent this, we limit the number of posts that an individual can act on, which is the nature of PTON CREDIT

5.4.2.2 INTRODUCTION OF DOWNBEAT

In FORESTING, PTON CREDIT allows you to downbeat inappropriate articles (plagiarism, fraudulent posts, spam, sexually explicit images, abominable videos, racist content, etc.), as well as upbeat, which rewards valuable content. Downbeat gives users to have a negative rating on their posts (reduction in the number of upbeats, reduction in compensation, etc.) so that users can self-operate the network.

5.4.2.3 INTRODUCTION OF CREDIT

FORESTING users can earn PTON CREDIT. This CREDIT increases as the number of upbeats received from other users. Conversely, when you receive a downbeat, that number decreases. This number affects the exposure priority of the content and serves as an important tool for users to make up for previous downbeats.

5.4.3 ADDITIONAL BENEFITS

PTON CREDIT can be secured by depositing the PTON used in the FORESTING service on the network. The PTON used in the network and the PTON CREDIT are connected indirectly, and the demand of PTON CREDIT can lead to the demand of PTON.

5.4.3.1 INTERESTS

The higher the PTON CREDIT period in foresight, the higher the interest rate. PTON will distribute interest according to CREDIT holdings.

5.4.3.2 CURATION COMPENSATION

Curation compensation is a reward given to one person who is voting. One of the factors that determine the size of this compensation is the voter's PTON CREDIT. A voter with high PTON credit will receive more curation compensation.

5.4.4 Commit-reveal voting

The first difficulty we encounter is that on the blockchain we have no notion of “an individual”. The blockchain does not know about individual people. it only knows about individual addresses. It is impractical to call for one-address-one-vote: I alone may generate thousands of blockchain addresses and send messages signed by each of them in turn. This is indistinguishable from thousands of people sending one message each. This is known as a ‘Sybil attack’.

Therefore, in order to mitigate Sybil attacks, we must have either a closed assembly which actively manages its membership, or a Voting method that does not count addresses. we consider uport identity as membership.

Another undesirable feature of the voting presented so far is not technical, but social. During the voting period, running tallies are public.

Voting mechanisms are generally intended to harness the 'wisdom of crowds'. To do so effectively, there are three main conditions which must be met:
Diversity of opinion: Each person should have private information even if it's just an eccentric interpretation of the known facts.
Independence: People's opinions aren't determined by the opinions of those around them.
Decentralization: People are able to specialize and draw on local knowledge.
Where these conditions are not met, many cognitive biases negatively impact its efficacy, and lead to undesirable consequences such as bandwagoning and groupthink. (See also: here, here, and here.)
It is important therefore that a successful voting mechanism should defend these conditions by hiding the outcome of the vote, until the vote has concluded.

Commit / Reveal
Step 1: Put your ballot in a sealed envelope.
During the voting period masked votes are submitted. Instead of submitting a vote directly, voters generate a signed voting transaction and only submit its hash. This is the 'commit' phase. The vote has been submitted to the blockchain, but the vote is private and sealed by this "hash-lock".
Step 2: Unseal your own envelope and count your own vote.
After the polls close, voters send a second transaction: the 'reveal'. The voter submits the original signed vote to which they had previously committed. The vote is only accepted as valid if its hash matches the commit. A valid reveal transaction adds its vote to the total tally.
This procedure obviates bandwagoning and allows votes to be tallied without hitting the gas limit. The downside is every voter must submit two transactions for every vote. (Note also this is not a secret ballot — after the reveal step everyone's votes are public knowledge.)

Partial-lock voting in detail
When a user submits a hash-locked vote, the time the vote closes is recorded. The account is locked from that time onward and all transfers withheld until the user submits the reveal transaction to have their vote counted and their account unlocked.

Submitting a new vote:
In order to submit a vote, the user must submit a voting transaction consisting of the following data:
1. Vote ID: what are we voting on
2. Secret: the commitment
3. Position in the list where it is to be inserted
The contract can check if the data supplied in 3. is correct (i.e. if the list remains sorted after the insertion) by comparing the corresponding previous and next timestamps. Either a new timestamp is added to the list, or if it already existed, the vote is added to the corresponding list of secrets.

Revealing a vote:
To reveal a vote, a user must submit a reveal transaction consisting of:
1. The vote ID: what vote we are revealing
2. The vote itself — the one whose hash is the commit.
From the vote ID, the contract determines the closing time of the vote and calls up the corresponding entry in the list and retrieves the committed secret. It compares the hash of the submitted vote to the committed secret. If they match, it updates the vote tally and deletes the secret. If there are no more secrets at this timestamp, it removes the timestamp's entry from the list entirely, modifying the neighbouring next/previous links accordingly.

5.5 PTON CREDIT

PTON credits represent a credit rating that is based on the user's credit rating for the use of the financial services of the FORESTING Bank, while at the same time the function of the token proportional to the 'Smart Contract' and indicates the level of influence.

Details of this are described in sections 5.3, 5.4 and 5.6.

5.6 COMMERCIAL REVENUE SHARE

Nearly all forms of media that exist today are centralized, and social media that emphasizes a free lifestyle are no exception. Rather, it is true that it is not free from various security issues such as censorship and hacking of surveillance institutions, or leaks of personal information. Recently, Facebook's personal information leak, which caused a massive worldwide impact, has confirmed this reality. It turned out that about 87 million sources personal information were leaked on Facebook and used for the last US presidential election campaigns.
There is no reason for Facebook's business model to be criticized, as profits have already been the goal of every company. However, users are complaining about betrayal and withdrawing trust because the business philosophy of Facebook is inconsistent with the business operation method.

In particular, this incident is a result of the fact that Facebook has created a centralized giant by transforming creative content created by users connected through horizontal networks into revenue. Once a personal information is leaked, it is impossible to recover the original information, and can lead to secondary fraud such as spam, impersonation, privacy violation, (voice) phishing and other commonly known scams. The biggest problem is that most content platform operators use customer databases to earn advertising revenue. The content itself does not generate primary revenue, but the platform serves as an intermediary for advertisers, and users are focused on collecting user databases to improve the efficiency and effectiveness of targeting and retargeting for advertisers and ad agencies. Facebook is already known to be highly effective. This means that our daily activity on Facebook will be used by companies that use Facebook.

Instead of focusing on these advertising revenue-driven platforms, FORESTING will create a content-centric platform that generates revenue directly from content.

This is not a problem with existing social media, where only personal information is dependent on advertising revenue. Relying solely on ad revenue is a big problem for the quality of your content. Most social media platforms judge traffic as a measure of the value of content rewards in order to reach more users. However, this can encourage content-based posting that is stimulating to attract recruiters. FORESTING encourages better content creation and will create a better content culture with valuation based on value rather than actual traffic-based content valuation.

5.6.1 PROBLEMS WITH CURATION SERVICES

The existing curation service that gives a specific result of a certain company or organization such as the top songs in the charts, the real-time keyword ranking, the restaurant list, etc. to the consumers gives the consumer a lot of information.

Is this curation service reliable, as curation service providers pay for our exploration costs? Music charts on a music site are not subject judgment, but are determined by objective numbers such as sales volume of the songs and the number of streaming plays. Therefore, the ranking of the music chart is determined by fairly objective numbers. However, since this objective data is recorded on the central server of the music site, it can be operated at any time, even if there is no operation, it is impossible to confirm that the data is actually reflected in the ranking.

In this situation, if the effect of curation directly affects revenue growth, the chances of curation being exploited are greater. In fact, when you look at the Nilo case, where the suspicion of manipulating the music charts has been raised, the curation service is not giving credit.

* Nilo suspicious incident on sound stack up
http://www.ytn.co.kr/_sn/0117_201805230924258578

5.6.1.1 THE EMERGENCE OF CURATION TOKENS

It is decentralized curation token that appear to solve problems of existing curation service. Curation tokens provide curation services through a multitude of collective intelligence rather than decimals. Many participants will be compensated if they have curated quality content through curation token. These rewards lead to voluntary participation of usrers. In addition, as the participation of a large number of users results in curation, the likelihood of negative intervention is even lower.

Currently, the decentralization curation service is a Token Curation Registry (TCR) model. The TCR is a way to vote on a specific target to include in the list.

* Token Curation Registry (TCR): A method to create a list that is suitable for a specific purpose and apply to those who want to enter the list.

In addition to the TCR method, there is also a way to implement a model that provides curation in a ranking or scoring method, but since the voting method is complicated, only the TCR method is used.

5.6.2 Curation Token Details

FORESTING solves the problems of the existing digital advertising market through TCR. The biggest problem in the digital advertising market today is the few platforms such as Google, Facebook and YouTube monopolizing the market.. Because platform companies are responsible for most of the advertising brokers, advertisers are inevitably making contracting with platform companies. However, advertisers are unable to determine which websites (or pages) are showing their ads and cannot determine if impressions are being manipulated by bots, or by actual users. We cannot trust the advertising effectiveness because of this. To solve these problems, TCR provides a list of high quality content pages that are not manipulated by bots and have high advertising effectiveness, so advertisers can publish their ads more effectively.

FORESTING decided that it would be more effective to test the functions of the TCR independently and ultimately add it to the PTON CREDIT

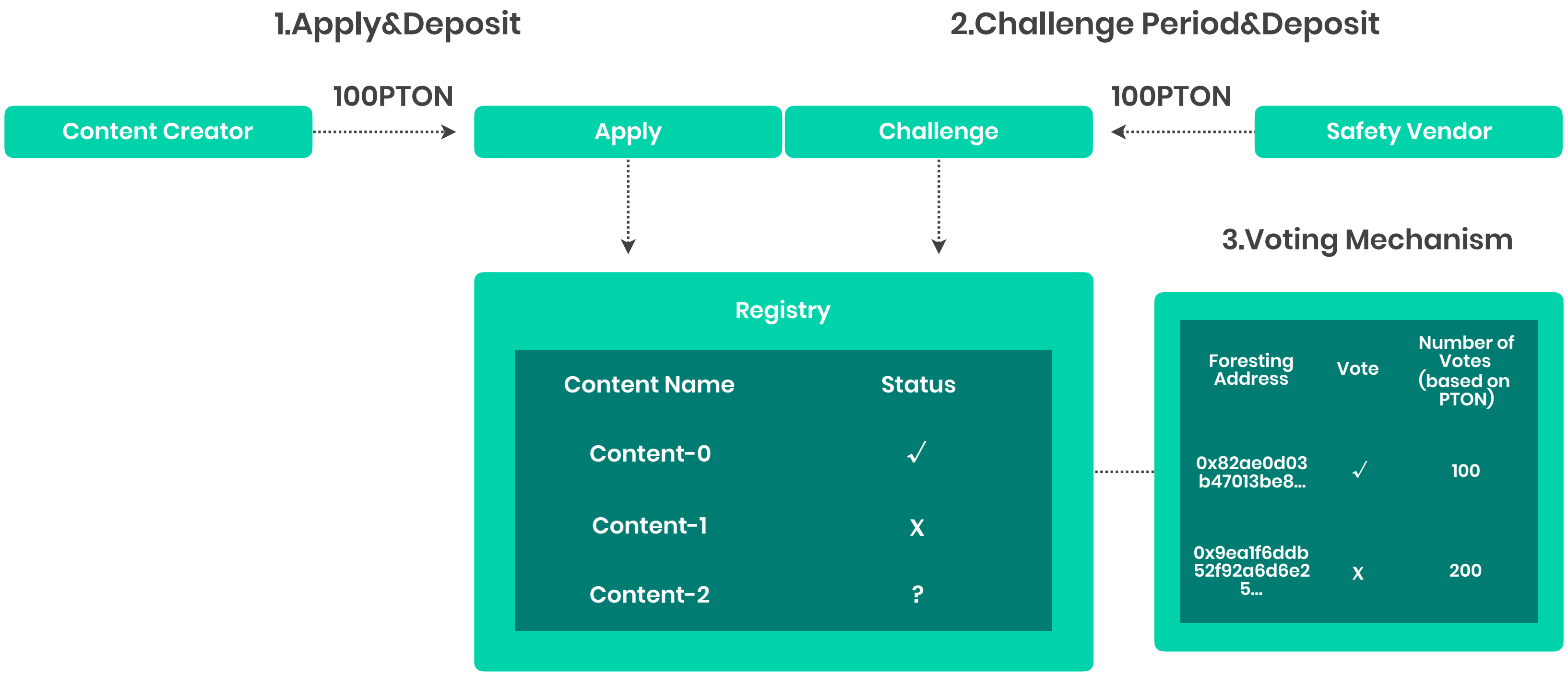
5.6.2.1 TCR Stakeholders

Customers: People who use list information and advertisers for the content on FORESTING's social media platform

Candidates: Those who want to enter the list, and each content publishing page (for public announcement)

Challengers: Anyone who is a PTON holder can apply for a challenge.

PTON holders: People who hold the PTON of the corresponding TCR, and can vote by PTON CREDIT.

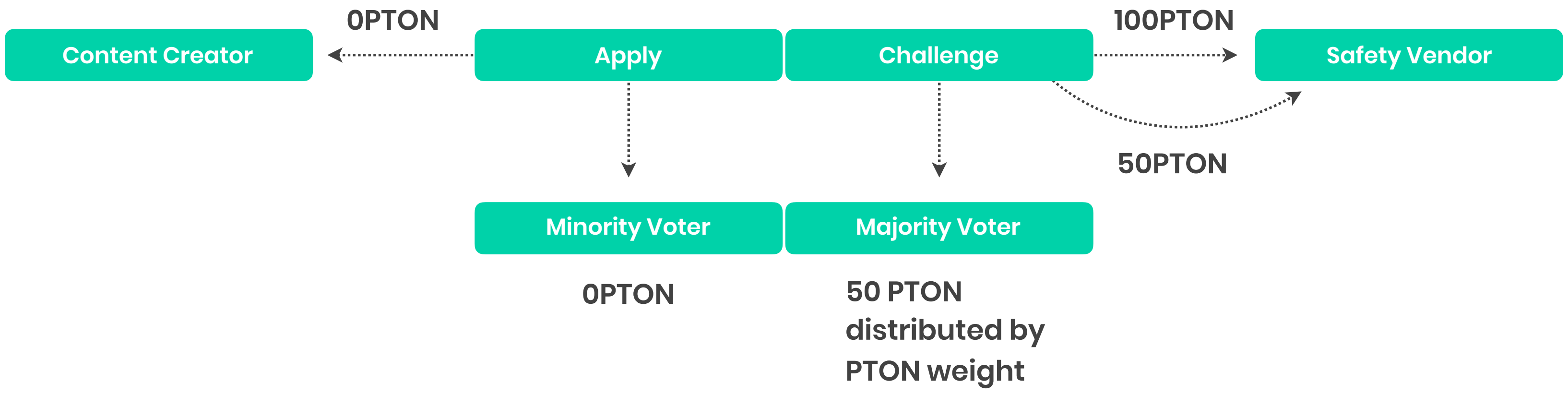


Content Name	Status
Content-0	✓
Content-1	X
Content-2	?

Foresting Address	Vote	Number of Votes (based on PTON)
0x82ae0d03 b47013be8...	✓	100
0x9ea1f6ddb 52f92a6d6e2 5...	X	200

The TCR list is a collection of quality content, and the applicant deposits 100PTON as a deposit first to add their content to this list. After the application, a challenge period is held for a certain period of time and PTON holders review whether to include the content in the list. At this time, if a certain PTON Holder thinks there is a problem, they can bet the same amount as the applicant's deposit as a challenger and conduct a challenge vote. All PTON holders are allowed to vote, and the amount of stake will determine the PTON CREDIT rewarded.

PTON distribution following challenger victory, 100 PTON deposit, 50% special dispensation



If the vote results in a successful challenge, PTON holders who voted against entry will take half the applicant's deposit as stake percentage. The inspectors will also receive half of the applicant's deposit and get their bet back.

On the other hand, if the challenge fails, half of the wagered amount will be distributed to the PTON holders who voted for the prospective entry, and half will be returned to the applicant.

This way, FORESTING can include a list of high-quality content in the list and make this content and the curation results available to everyone on the network.

5.6.2.2 HOW THE GROWTH OF FORESTING AND THE VALUE OF PTON ARE LINKED

In a curation token, the growth of the network raises the value of the list. On FORESTING, the more popular the list becomes, the more people enter the list, and its reputation and authority grows. If the value of the list increases, new applicants will have to purchase PTON to enter the list, so the demand will increase and the price will go up. Content creators can continue to enter the list as long as its authority does not decline, as it can provide advertisers with the publicity effect of the content.

Voting systems, which already consist of PTON and PTON CREDIT, are TCR functions, but in addition to this there is a need to segment the decentralized curation services on how to sort the list of various contents.

5.6.3 Voting Protocols

It is necessary to use voting protocol such as commit-reveal voting, and to add a partial lock to the third step. First, it should be implemented as a separate TCR Smart Contract and be included in PTON Economy after the test is verified.

5.7 Consensus Algorithm

I. Various Consensus Algorithms

After the invention of Bitcoin in 2009, the blockchain's Proof of Work (PoW) consensus algorithm was introduced to the world for the first time, and a variety of algorithms have been developed since. PoW, which uses hash power of nodes, is being widely being used. Recently, consensus algorithms, such as PoS, dPoW, dPoS and others have been developed.

II. PoW(Proof of Work)

PoW is a consensus algorithm used by Bitcoin. Being the simplest algorithm, it finds header hash as a result of SHA256 by using nonce value of the current block and difficulty of the previous block. This method prevents malicious blocks from withholding attacks because it requires a lot of computing power to generate header hash of the results specified in previous blocks. The advantage is that PoW ensures that the blockchain is protected clearly when the difficulty is high with a sufficient hash rate of blockchain nodes. The downside is that it costs a lot to maintain a stable blockchain. Newly-generated blockchains that do not have sufficient computing power are exposed to external pass-the-hash attacks. With the advent of a better sell and buy hash rate process with digital nomads, who generate high hash rates around the world, attacks on low hash rate blockchains have become easier.

III. PoS(Proof of Stake)

PoS is an consensus algorithm used by Dash. It is created to reduce the waste of equipment and electricity caused by the high hash rate of PoW. This is a cryptocurrency ownership method used to maintain the blockchain stability by a cryptocurrency proof process. The proof process assures to reward the real owner of cryptocurrency by screening fake blocks. PoS has an advantage in managing the blockchain with lower equipment and maintenance fees. The disadvantage is that the compensation rate on cryptocurrency used for staking in public blockchains is high, which increased inflation. As a result, The ownership percentage of a specific cryptocurrency holder increases.

IV. dPoW(delayed Proof of Work)

dPow an consensus algorithm used by KOMODO. Since it is easy to attack newly-generated blockchains with a common PoW consensus algorithm, dPoW is used to prevent attacks by inserting the hash results of Bitcoins into the algorithm. 64 blocks are generated by PoW in a single group which is monitored by nodes. The 65th block is then inserted as the Bitcoin block header to demonstrate the stability of the previous 64 results. In this case, no pass-the-hash attack is higher than the Bitcoin itself. Therefore, only the last 64 blocks that belong to the group can be damaged with a pass-the-hash attack without affecting the other blockchains. Thus, stability for the entire blockchain can be established by applying an algorithm to the previous block.

V. dPoS(Delegated Proof of Stake)

dPos is used in the EOS operating system. It solves problems of traditional PoW or PoS. Traditional PoW has a disadvantage of consuming too much resources and not being able to prevent attacks on new blockchains. PoS was originally designed to work on this issue. But the downside of PoS is that block generators are spread around the world which means that the throughput rate per second decreases. To resolve this, dPoS allows only verified nodes, not any miner, to create a new block. Then the verified nodes are grouped into a faster cloud network. Consequently, the throughput rate rises up. However, hackers can easily attack the nodes rather than attacking the blockchain itself as the number of nodes is small and the targets are clear. A disadvantage is dPos miners will dominate a higher number of tokens over time.

VI. FORESTING's consensus Algorithm

FORESTING is developing a mainnet with the advantages of multiple algorithms to minimize the weaknesses of the algorithms specified above and to highlight FORESTING’s advantage. In order to provide the FORESTING service and platform, FORESTING is improving the performance of the PoS consensus algorithm which is advantageous for mainnet management and development. Meanwhile, the algorithm of FORESTING minimizes the discarded blocks that appear while creating blocks via stake. It also boosts the synchronization speed and throughput rate among nodes.

The throughput per second will be increased by minimizing the generated blocks by delayed nodes and the rate can be maximized by processing the stored data in the mempool or txpool separately, that has not yet been up on the block. In addition to the traditional dPoS, the new system develops algorithms that can easily delegate unverified nodes even in mobile devices to fairly distribute tokens among the miners. This helps lessen the concentrated token retention on a small number of people and creates a wider user population.

FORESTING decided to use the DPoS + PBFT scheme used in the consensus algorithm to generate high-speed blocks and large-capacity transactions attempted in EOS, COSMOS, ZEN, ORBS protocol, etc. Following this it verifies and updates the supernet protocol through the testnet.
Blockchains that act as proof of work, such as Bitcoins, define agreements according to the "longest chain" rule. If you use this rule, you can not verify that none of the blocks have reached the irreversible state. At any point, anyone can create longer chains based on old blocks, and nodes can also switch. From this point of view, we can conclude that Bitcoin provides only a high probability of irreversibility based on the economic cost of trying to change the fork.

When a delegated equity certificate is introduced, stakeholders elect a block producer. Block producers are pseudo-randomly intermixed and assigned absolute time slots that may or may not produce blocks. The blockchain that most producers will write will be much longer in terms of length than a blockchain with few producers. Assuming that there are two chains lengthening at different speeds, the faster chain will eventually become the longest chain. Therefore, the original delegated equity-denomination algorithm provided a bitcoin-like guarantee. In other words, as blocks are added to a chain, there is less chance of another chain being able to flip one block.

The essence of the DPOS scheduling algorithm is to convey a lot of information to the observers watching. For example, based on the frequency of missed blocks, you can detect the possibility that the chain to which the observer belongs becomes a decimal chain. With 21 producers, a node can detect exactly when it has just missed two consecutive blocks (one second) that it may be part of the source fork. This notifies the user when the network is unreliable and allows the user to wait a little longer for the confirmation to complete. Likewise, if all the producers have not missed a block in the 21 blocks that accept the transaction, you can be sure that the generated block will not be returned.

When introducing the last-irreversible-block concept into the DPOS algorithm, the dynamical block is the most recently created block produced by the producer plus two-thirds of the number of block producers. If a producer approves a chain that approves one block plus 2/3 of the total producers plus one, then no other forks are possible.

However, given a hypothetical scenario in which a network of two chains occurs, usually one or both chains will be able to communicate until either network is reconnected to the number of producers 2/3 to 1 plus the number of producers End - Irreversible - Aborts the task of confirming the block as the next block. Once this is done, all the work goes smoothly, and when the connection is normalized, all the nodes will converge into one real chain. There is, however, a race condition in which two sub-sets switch forks at the same time, with both forks reaching the same number of votes as two or three more producers in a different block. If this happens, the nodes on either side of the fork will not be able to synchronize both nodes, since both end-irreversible blocks will not be back to the set point. Now they must be adjusted manually.

In this situation, one or both forks will stop acting on the other side of the fork to determine the irreversible point, depending on the number of producers 2/3 plus one. Decimal chains may be written at half speed, but nodes waiting for irreversible status will no longer recognize that any transaction accepted in the decimal chain is in a final state.

This type of failure may result in a single block reversing, and some services may be harmed. The probability of this happening is much lower than the probability that one of the six approved bitcoin blocks is reversed

The key idea of dPoS is that each block created is a vote for every previous block. With this model, if more than two-thirds of the producers have created blocks based on a particular block, then that block has more than two-thirds votes. This situation sounds fair in theory, except that non-Byzantine block producers are likely to create blocks in different forks at different points in time. If non-Byzantine block producers produce blocks on different forks, you end up with a situation in which one indirectly contradicts the same block numbers that appear in each forked chain.

Let's consider a network in which block producers A, B, and C participate. Suppose that two block producers have lost communication for a short period of time because of a network problem, and block producer A creates block N at time T and block producer B creates block N at time T + 1 . Suppose now that block producer C broke a tie by generating block N + 1 at time T + 2 following block N, which was produced by block producer B at time T + 1. If this happens and Producer A finds the presence of Block N + 1 in Producer C, Producer A will switch over to the longer fork. When Producer A is about to generate a block, Producer A will indirectly approve Block N of Producer B, which conflicts with Block N that he previously created.

Block N, produced by Producer B, never reaches a direct irreversible state. Because producer A must vote 2/3 + 1 from producers A, B, and C in order to reach the irreversible state, and producer A votes in the alternative block N. Instead, when producer A creates block N + 2 and producer B creates block N + 2, block N + 1 becomes irreversible. Thus, block N + 1 gets 3 votes needed to reach 2/3 + 1. When block N + 1 produced by producer C reaches the irreversible state, block N created by producer B is also regarded as irreversible.

To implement this algorithm, each block producer inserts the highest block number (H) previously approved in any fork into the block header. When block N is applied, one can only vote for irreversibility for blocks in the range [H + 1, N].
Any producer who signs a block in the overlapping range will be considered a Byzantine and will generate a credential that reveals the problem.

With this information, it can be said that at least one third of the block producers have signed a conflicting range of blocks in order to get 2/3 + 1 votes for two different blocks with the same block height of any block height. One can generate simple evidence that they prove right. This situation has resulted in an honest network partition where two groups of good producers each of 1/3 size are creating two different blocks and a bad 1/3 group signs both. To create two different blocks that are considered irreversible in a network environment that is actually well connected, there should be as many as 2/3 +1 malicious producers.

Under these rules, there are now two cases when a producer signs a Byzantine manifestation.

Signing directly or indirectly two blocks with the same block number is signing two blocks created at the same block time. Honest nodes running basic software will never do this. It is therefore easy to punish all the bad parties until the unsuccessful attempt.

Chapter 6

FORESTING SUPERNODE SUPERNET ARCHITECTURE

6.1 Nodes

Node: Any computer or server connected to blockchain.
Supernode: central point of node on Blockchain P2P System for data transfer and decentralize. normally, Supernodes do communication using high-speed broadband networks. With high-performance CPU and storage, they can process a large quantity of data at a high speed. Supernodes of FORESTING, will also generate blocks. The supernodes will have to load tests on the FORESTING test network for verification and it will become a certified Supernode after this. For faster block generation and transfer the number of supernodes will be managed by an identity number.(16EA~128EA)

This system will reward those who maintain the nodes that use the DPOS system. So, a supernode delegated by its own supernode and FORESTING may exist. depending on their share, proportion with coin age.

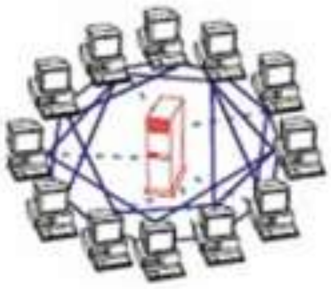
Fullnode: A node that receives, validates, stores, and transfers the blockchains generated by the supernodes and creates a database for various services. In many cases, to provide services by mobile apps as a path, permission will be denied from the main network.
Lightnode: A node that is not stored on Blockchain. It is a lightweight node for mobile that can send transactions to the block-chain network by maintaining only the part depth (6) of the chain and the blockchain, and can inquire the blockchain ledger by communicating with a fullnode.

6.2 Creation Supernode

There are three category of p2p networks.

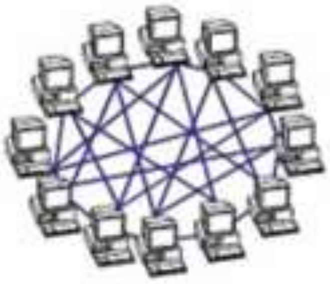
Centralized P2P

- has a centralized server
- static centralization
- high search fee
- more nodes increase its complexity



Pure P2P

- no centralized server
- all decentralized
- high search fee
- more nodes increase its complexity



Bitcoin and Ethereum Centralized P2P Network Model.

The Ethereum operation is as follows.

- Run Ethereum program (daemon)
- Daemon will connect the central server operated by Ethereum Foundation.
- Download information about another node (A,B,C) from the central server
- Attempt a handshake with A on daemon
- If this fails, attempt a handshake with B
- If the handshake succeeds, download information about the counterpart node
- Daemon type and version exchange.
- Genesis block hash change.
- Block height exchange.
- If the information matches, start sync

Start the transfer of blocks using the follow process. By using this random method with a long physical distance between the nodes, a low network speed and a slow block generation speed between the nodes, the block generation rate and the block transfer speed in the whole network will be affected, and the transaction processing speed per second (tps) will slow down.

Cryptography using the super node of the Hybrid P2P network is gradually increasing in order to solve the Bitcoin or Ethereum slow block generation rate.

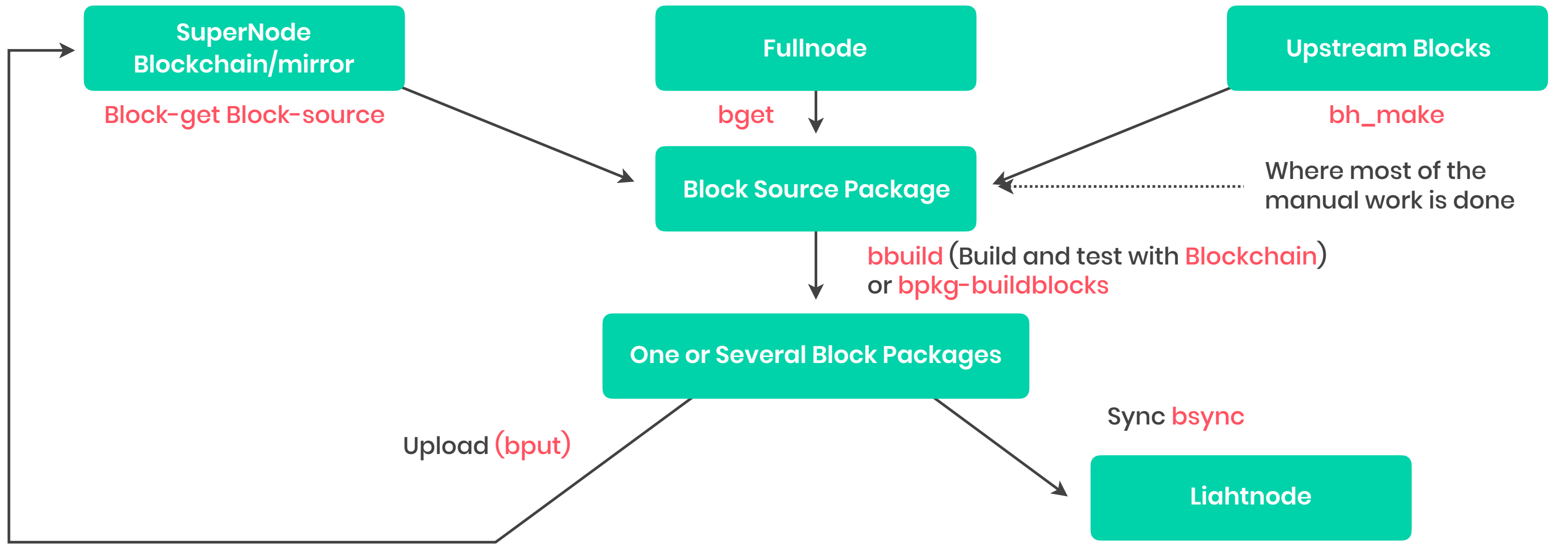
In the case of EOS, trying to solve the speed / capacity problem of the blockchain by an intensive operation of nodes through development history such as Nxt → Waves, Bitshares → Steemit → EOS, COSMOS. In this blockchain, the supernode has high-speed processing of high-volume transactions and block generation performance, and a small number of special (21 to 64) special nodes.

FORESTING has a hybrid P2P network structure to handle transaction processing at a high speed and plans to build 16 ~ 128 intensive supernode.

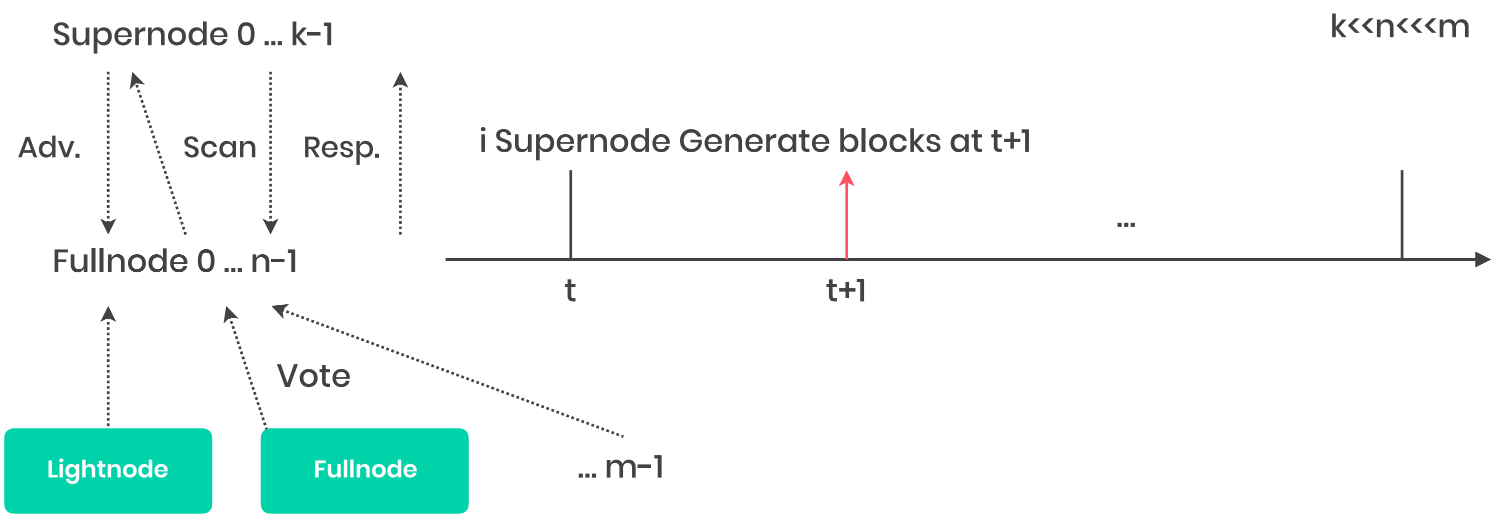
6.3 Supernet

With the advent of the supernode, the blockchain network is separated into two layers. For the purpose of high-capacity transaction processing and high-speed block generation, Supernet is required to connect supernodes. The supernet must have a protocol and a physical layer to carry out secrecy and authentication.

6.3.1 Supernode Block Workflow

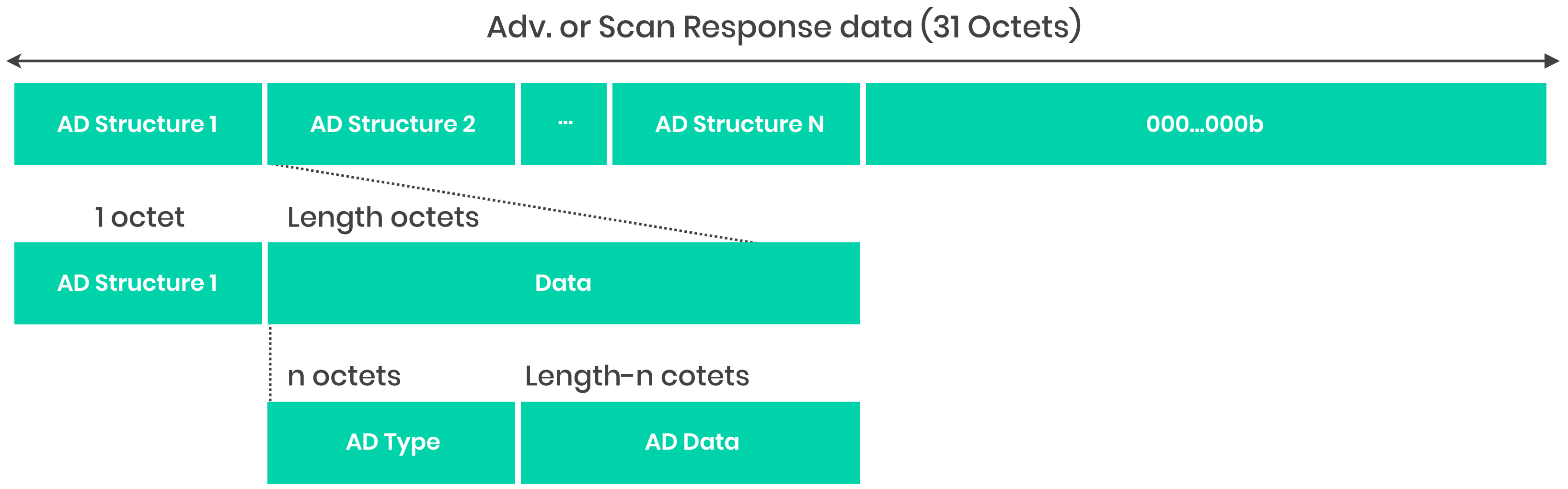

SuperNode Blockchain/mirror
Block-get Block-source
Fullnode
bget
Upstream Blocks
bh_make
Block Source Package
Where most of the manual work is done
bbuild (Build and test with Blockchain) or bpkg-buildblocks
One or Several Block Packages
Upload (bput)
Sync bsync
Liahtnode

6.4 Supernode Block Generating Process

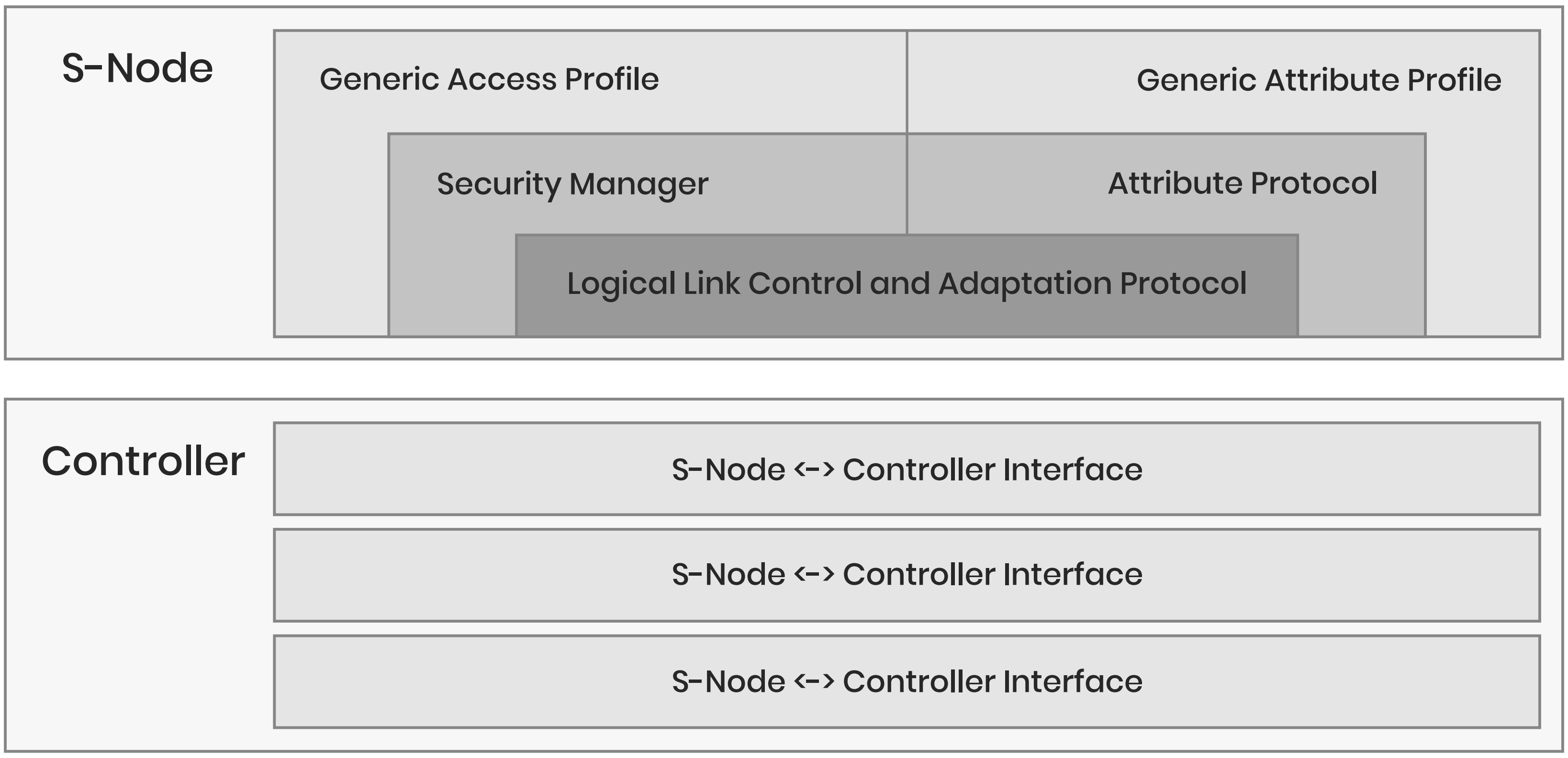


FORESTING uses the PoS agreement algorithm, which is used by the Ethereum Casper project. In order to increase the speed of slow block generation by the general PoS algorithm, nodes that satisfy the specification of FORESTING and the network criterion are added to the supernode to speed up the block generation. To maximize tps, the network will experiment with accepting the Plasma Cash used in the Loom network. Supernet protocols connecting super nodes will be verified and updated through test net.

6.5 Supernode discovery packet



6.6 Supernode protocol stack


S-Node
Generic Access Profile
Generic Attribute Profile
Security Manager
Attribute Protocol
Logical Link Control and Adaptation Protocol
Controller
S-Node <-> Controller Interface
S-Node <-> Controller Interface
S-Node <-> Controller Interface

6.7 Supernode dimension estimation

1,000 TPS	1,200 TPS
AWS EC2 m5.2xlarge	AWS EC2 m5.2xlarge
CPU: Intel Xeon Platinum 8175M 2.5Ghz*8 Core MEM: 32G DISK: EBS 120GB SSD(3000 IOPS Fix)	CPU: Intel Xeon Platinum 8124M 3.0Ghz*8 Core MEM: 16G DISK: EBS 120GB SSD(3000 IOPS Fix)
20x20	20x24

*interval(ms) x count per interval
*20x20: Generate 20 transaction per 20ms
*60x60: Generate 60 transaction per 50ms

[ref] https://steemit.com/kr/@eoseoul/bmt-eosio-tps-2-by-eoseoul-jit

6.8 Supernode testnode for Tech-Roadmap-1

Tech-Roadmap 1: Stage 1	Tech-Roadmap 1: Stage 2	Tech-Roadmap 1: Stage 3
AWS EC2 m4.2xlarge	AWS EC2 m5.12xlarge	AWS EC2 m5.12xlarge
CPU: vCPU 8 Cores MEM: 32GB DISK: SSD 300GB NETWORK: 1Gbps Monthly Bill: USD $457 Type: Cloud(AWS)	CPU: vCPU 48 Cores MEM: 192GB DISK: SSD 2TB*2EA(NVME)+EBS 16TB NETWORK: 10Gbps Monthly Bill: USD $2,800 Type: Cloud(AWS)	CPU: vCPU 128 Cores MEM: 2TB DISK: SSD 2TB*2EA(NVME)+EBS 16TB (Provisioned IOS 20000) NETWORK: 25Gbps Monthly Bill: USD $19,361 Type: Cloud(AWS)

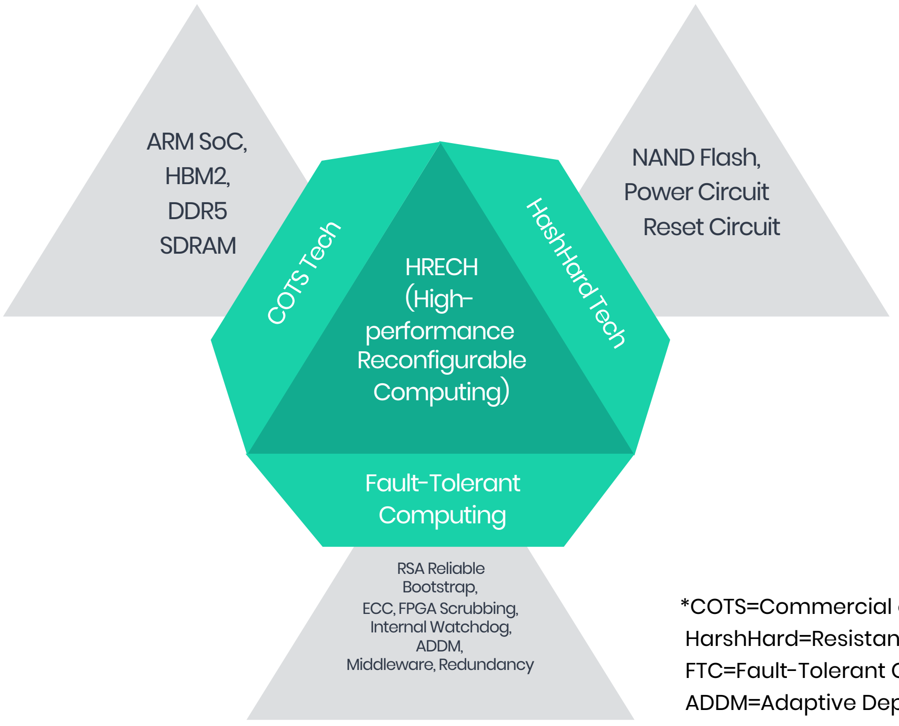
[ref] http://koreos.io/29589

6.9 HREC Supernode

- If you create a block generation using a specific manufacturer's ASIC or GPU Miner, its important feature can be affected by the manufacturer's state. The first phase of the TechRoadmap uses Amazon EC2 VPS, which can result in a situation where cloud service is not available.
- Due to the reason mentioned above, designing and building supernodes to participate in SuperNet should be provided to Opensource.
- Like in step 1 of the Tech Roadmap, using AWS will be against decentralization.
- FORESTING will lead current POW miners to participate in supernet and in the Mining Factory environment. Guides should be provided to operate the AWS reliable supernode.

*HREC=High-Performance Reconfigurable Computing

6.10 Supernode HREC for Tech-Roadmap 2,3



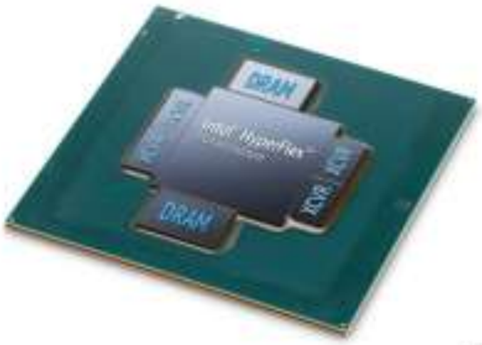
*COTS=Commercial off the Shelf
HarshHard=Resistant to Harsh Environment
FTC=Fault-Tolerant Computing
ADDM=Adaptive Dependable Distributed Middleware

6.11 Supernode platform decentralization

Anyone can develop an automated protocol and election mechanism to become a SuperNode, and qualified (w / certificate) nodes are given the opportunity to participate in competitions through SuperNet.
** The supernode certificate, it can be acquired and used only when the specification is defined in testnet and the specifications for the block generation processing capability and interoperatability are satisfied.

6.12 Supernode platform customization recommendation

Xilinx Zynq UltraScale+ MPSoC ZCU106
• Intel, HBM2 Memory Integrated Stratix 10 MX FPGA



Chapter 7

TECHNICAL CONSIDERATIONS

Solving technical difficulties for future aspects

Chapter 7

TECHNICAL CONSIDERATIONS

7.1 Technical Architecture

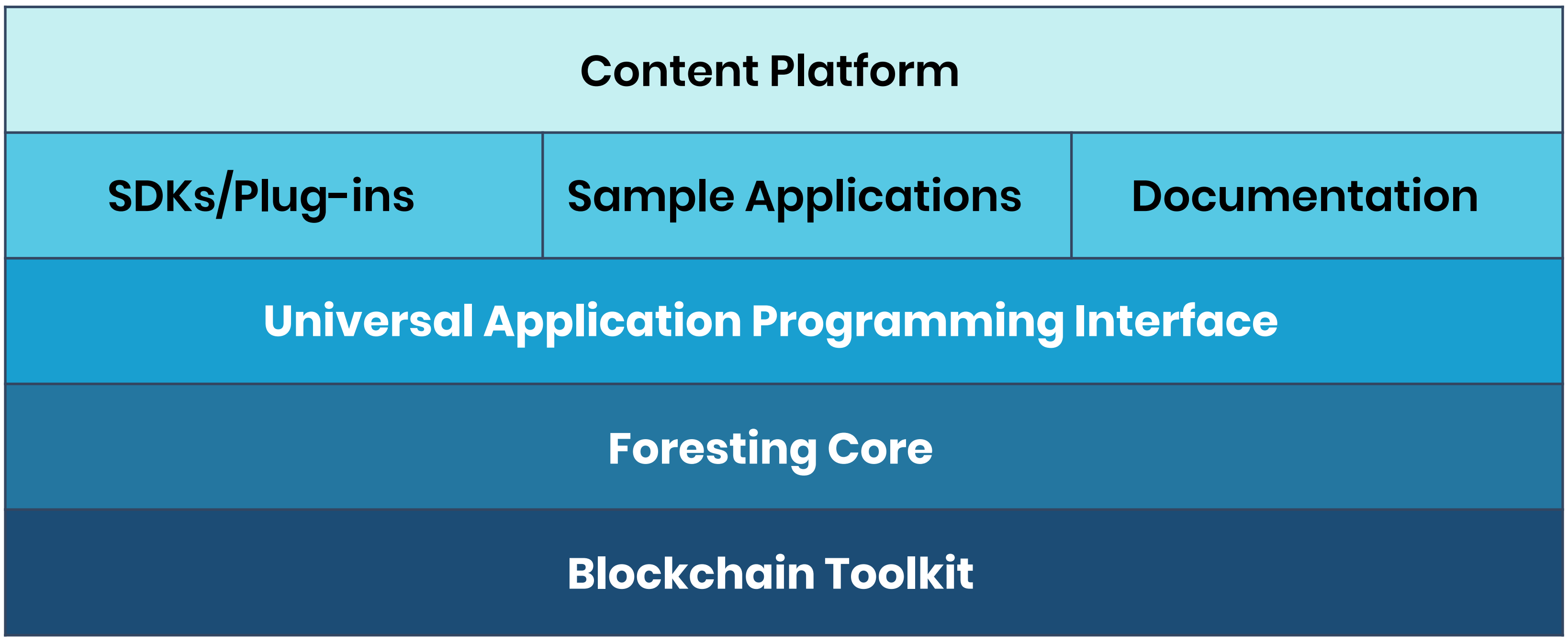
FORESTING consists of five main layers. The bottom layer consists of the Blockchain Toolkit for providing basic blockchain services such as block formats, algorithms, networks, databases, users, and permission management services. The Blockchain Toolkit enables fast, efficient multi-transaction processing, allowing users to expect high availability and low latency.

FORESTING Core is the layer responsible for key business logic implementations, account rights management, reward distribution algorithms, community platforms, and advertising systems.

The Universal Application Programming Interface (UAPI) provides third-party developers with APIs for content creation, evaluation, and user management so that they can create their own layers of development on any platform with development capabilities.

Software Development Kit (SDK), Plug-ins, Sample Applications, and Development Documents support developers and users that desire to build their own content platform. In particular, users can integrate the FORESTING Network directly onto forums, blogs, and CMS using a set of plug-in devices.

The content platform that is based on the FORESTING Network is at the top. All types of content formats, such as text, images, audio, video, and live broadcasting, can be provided with a content-oriented incentive platform supported by the FORESTING Network.



Content Platform

SDKs/Plug-ins | Sample Applications | Documentation

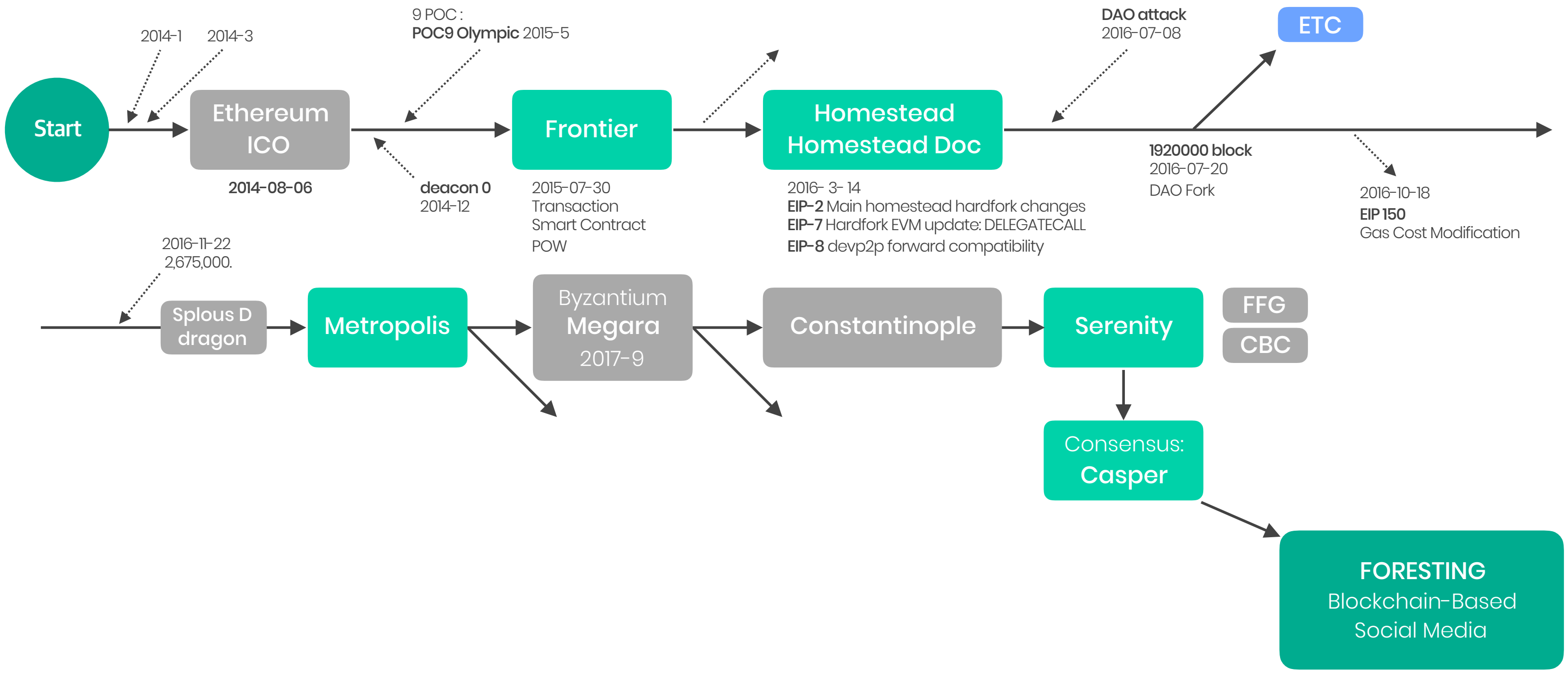
Universal Application Programming Interface

Foresting Core

Blockchain Toolkit

The first version of FORESTING will be launched on The Ethereum network, which is the largest blockchain platform. Ethereum facilitates the development of a decentralized app (DApp) driven on blockchain by using its own Ethereum Virtual Machine (EVM). DApps are mobile-responsive and fully compatible with existing major blockchain ecosystems. Ethereum combines a modified Bitcoin infrastructure with the Ethereum Virtual Machine to provide an ecosystem that can leverage smart contracts and private contracts over a transparent blockchain.

The second version of FORESTING will have its own mainnet using EVM. By using its own mainnet and EVM, as an alternative to social media, we will build our own blockchain ecosystem that complies with EVM and solidity standards.



FORESTING chooses Casper, one of several projects of the Ethereum Foundation, to launch the first large-scale social media service based on blockchain (for 0.6Billion users).

* Instead of energy-consuming PoW, Casper adopts a PoS consensus algorithm, which is an optimized blockchain for social media services and crypto games. Through the connection with expansion solutions such as Plasma, Sharding and State Channel, the scalability problems are solved by using the Loom Network, including Mainchain and Sidechain which uses DPoS.

FORESTING uses authentication methods in mobile communication environment based on Subscribe to protect users' information.

7.2 Ecosystem to Create DApp

Decentralized applications (DApps) are executable programs that are written on a blockchain. They are programs that are executed automatically when certain conditions are met, while a conditional statement is recorded on the blockchain. For example, it is possible for a blockchain to meet the following requests:

"Send a token to my address. I will give what I have to the person who sent the most tokens by 12 o'clock today. Those who send less tokens will be automatically refunded.”

Putting a conditional statement like this on the blockchain automatically selects the senders who sent most tokens and the other senders will be fully refunded. An application which works using this pattern is a DApp. It is called decentralized application, shortly DApp, because it puts the statements that anyone can see without a central control in the blockchain, and works automatically. This contract is called ‘Smart Contract’.

By using smart contracts, contracts can be executed and terminated by recording transactions, paying for logistics, etc. in detail and recording them on the blockchain with the agreement between the parties, then assigning the PTON of the promised value to the contractor.

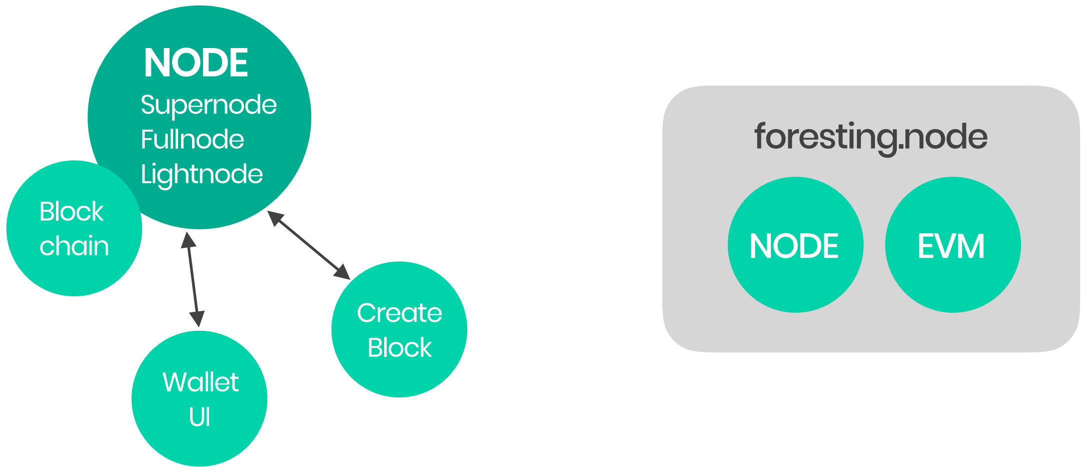
FORESTING can use EVM to implement smart contracts that automate contract execution without third party involvement. Anyone can use DApps in FORESTING without restrictions by the FORESTING nodes spread around the world.

In FORESTING, DApps are available through PTON's compatible browsers, compatible Metamask, and My PTON wallet.

7.2.1 DApp Execution

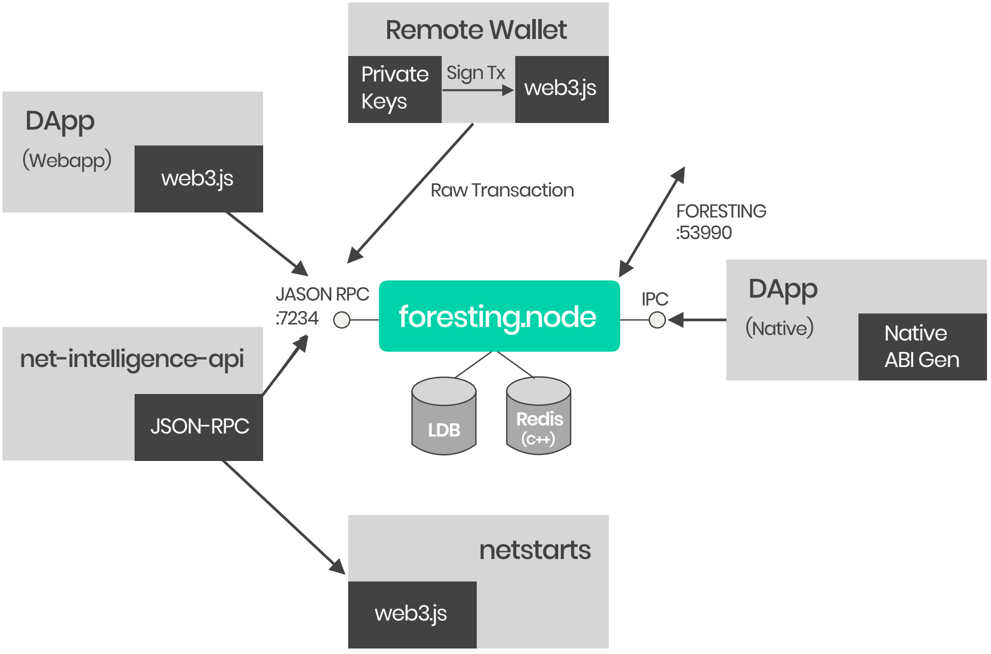
- Metamask is a desktop Lightnode that allows you to run a DApp on a Chrome browser.
- Lightnode is a Lightnode for smartphones that allows a DApp to run on smartphones.

7.2.2 Foresting node Basic Configuration



Node: Any computer or server connected to FORESTING.
Supernode: A node connected to a broadband network for rapid block generation and propagation.
Fullnode: A node that holds all blockchains. It serves as block validation, synchronization, propagation, and service provisioning. It does not participate in block generation.
Lightnode: A node that does not have a blockchain but only has the header information of the block header and the Depth (6). In general, lightnode plays the role of a home page, hardware wallet, and mobile wallet.
Supernode and fullnode run the FORESTING node daemon, which runs EVM over it. Lightnode does not have daemons or EVMs running.

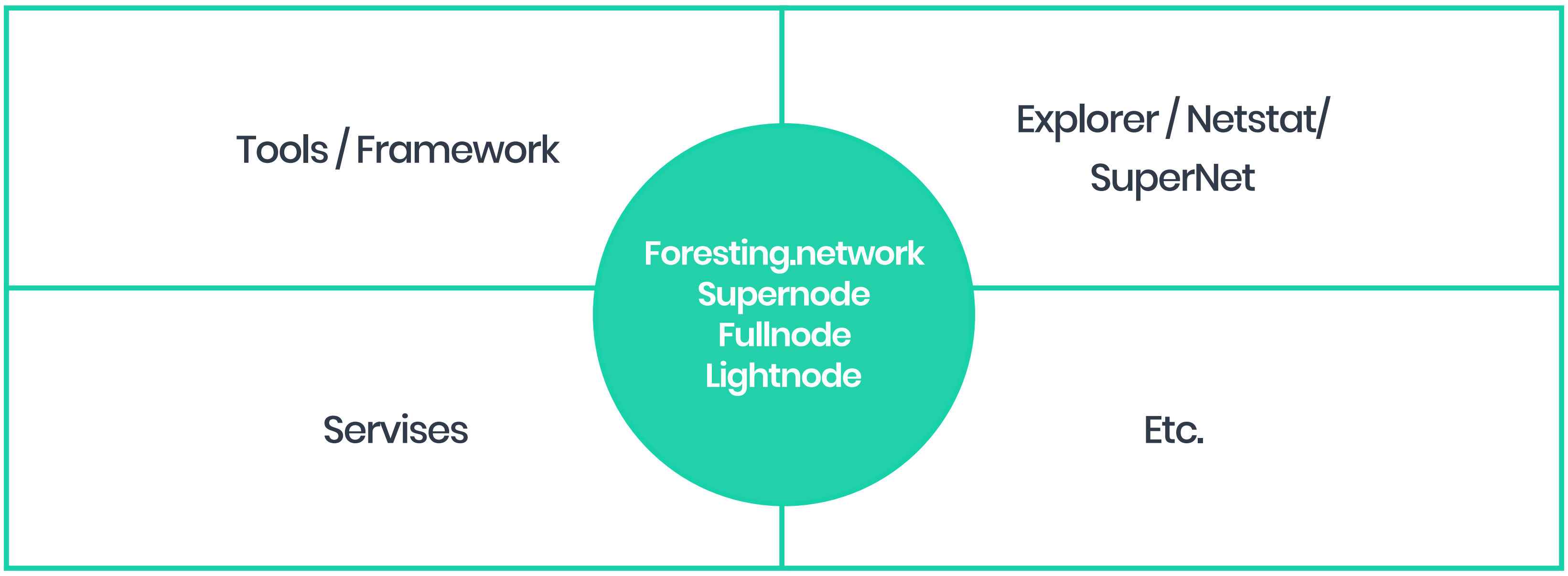
7.2.3 DApp Architecture



7.2.4 Key Technologies

Smart Contract	**Distributes turing complete code to blockchain** **When a contract is executed through a transaction, all nodes execute it** **Blockchain technology significantly impacts application area expansion**
JavaScript API/JSON RPC	**Standardizes the JSON RPC API Specification** **eth, miner, personal, db, admin, etc.** **Providing JavaScript API via web3.js**
enode ID	**A combination of Public Key and IP.Port** **Used for public key exchange for trust between peers**
Account/State	**Externally Owned Account(EOA)** **Contract Account**
RLP(Recursive Length Prefix)	**Data structure for representing variable data** **Complex multidimensional arrays are represented in one dimension** **Authenticated / encrypted communication via RPLx** **Protocol for serializing objects**
Whisper/Swarm	**Whisper - Peer-to-Peer filtered quick messaging (shh)** **Swarm - Identify and exchange distributed binary resources (bzz)**

7.2.5 Echo Systems



7.3 Systems that can create and publish tokens

The concept of colored coin access first appeared around the year 2013 when several protocols using Bitcoin blockchain protocols were implemented.

* Colored Coin Access: A type of asset issue layer that digitally represents in-kind assets through bitcoin blockchain protocols.
References: https://brunch.co.kr/@jeffpaik/13

Several other attempts have been made to develop a custom blockchain token platform from scratch, the most notable of which is the NXT token.

The method developed by NXT implements token creation and transmission with the contents recorded in the attachment by adding them to the transaction. This method is applied in a similar way to Qtum and Zencash. This method has the advantage of transferring information without breaking down the existing Bitcoin transaction structure. However, if a transaction of a new structure needs to be added, all blockchain programs must be updated at the same time. If a program that does not follow the new transaction continues to be maintained, a fork is created that separates the existing blockchain from the new blockchain

FORESTING supports plug-ins that are installed with extensions, and through these, new-style transaction structures are proposed, and solutions can be made to solve the problems caused by fixed structures. Clients that do not have the relevant plug-ins installed can also pass these custom transactions, which allows third party developers to introduce new transactions and create ecosystems, such as the DAPP store.

FORESTING's basic core level supports the following basic transaction types:

- Create, delete and transfer custom tokens
- Bid and Ask decentralized token transaction implemented as an order matching engine that matches network transactions
- Anonymity Function

FORESTING supports an advanced transaction method of trading from assets to assets by providing transactions between custom tokens through a decentralized blockchain-based transaction.

FORESTING supports token issuing systems that comply with the ERC20 and ERC721 standards. The ERC20 token is a de facto standard with a standard interface for tokens issued on an Ethereum blockchain network. The standard is cryptocurrency, which is created using smart contracts running on EVM, and DApps. Many blockchain networks are embracing this standard.

7.3.1 ERC20 - Code

```
contract ERC20 {
function totalSupply() constant returns (uint totalSupply);  // Check issue volume
function balanceOf(address _owner) constant returns (uint balance); // Check balance
function transfer(address _to, uint _value) returns (bool success); // Send
function transferFrom(address _from, address _to, uint _value) returns (bool success); //Transmission by smart contract
function approve(address _spender, uint _value) returns (bool success); // Transaction confirmation
function allowance(address _owner, address _spender) constant returns (uint remaining); // Check usage

event Transfer(address indexed _from, address indexed _to, uint _value);
event Approval(address indexed _owner, address indexed _spender, uint _value);
}
```

7.3.2 ERC20 - condition

```
// Account balance
 mapping(address => uint256) balances;
//Approve the amount that an account owner can send to another account
 mapping(address => mapping (address => uint256)) allowed;
```

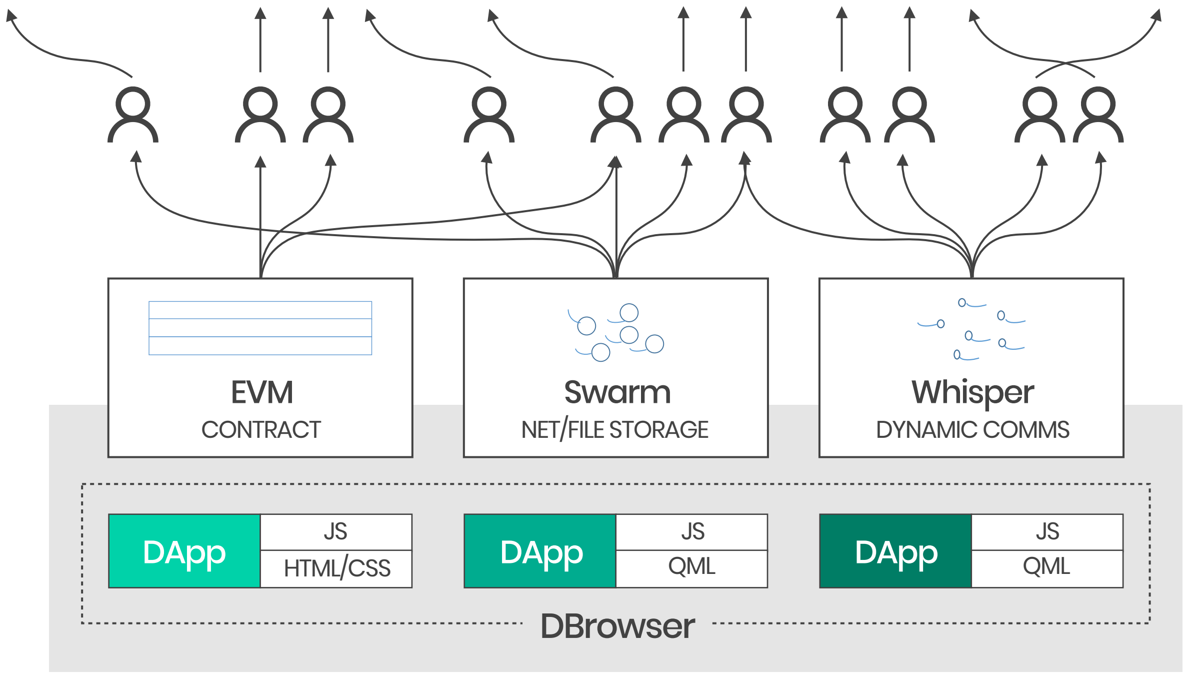
7.3.3 ERC20 - function

```
// View your account balance
function balanceOf(address _owner)
    constant returns (uint256 balance) {
      return balances[_owner];
}
// Transfer balance to another account (previous)
function transfer(address _to, uint256 _amount) returns (bool success) {
    if (balances[msg.sender] >= _amount && _amount> 0&& balances[_to]+_amount> balances[_to]) {
      balances[msg.sender]-= _amount;   balances[_to] += _amount;return true;
   } else {return false;} }
// _Tokens equivalent to value _from an address _to an address
// The TransferFrom function is used by contracts to transfer coins on behalf of an account.
 // For example, it can be used to send a coin to a contract address or charge a transaction fee for a sub-token.
 // fees in sub-currencies; the command should fail unless the _from account has
// deliberately authorized the sender of the message via some mechanism; we propose
// these standardized APIs for approval:
function transferFrom(    address _from,    address _to,    uint256 _amount ) returns (bool success) {
    if (balances[_from] >= _amount && allowed[_from][msg.sender] >= _amount&& _amount > 0 && balances[_to] + _amount > balances[_to]  {
        balances[_from] -= _amount; allowed[_from][msg.sender] -= _amount;  balances[_to] += _amount;return true;
   } else {return false; }
```

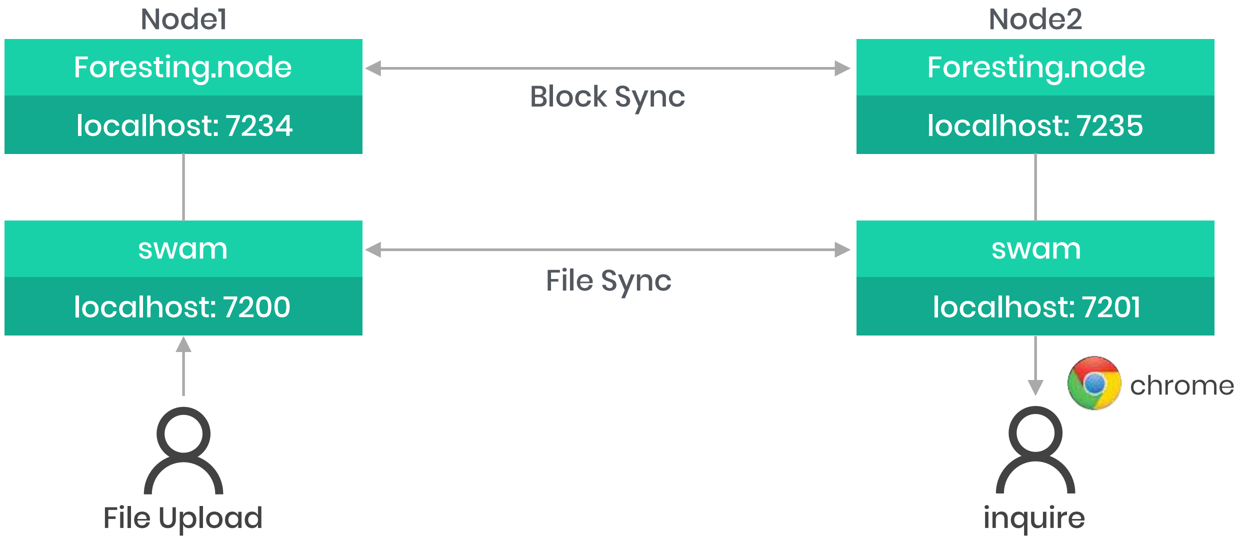
https://theethereum.wiki/w/index.php/
ERC20_Token_Standard#Sample_Fixed_Supply_Token_Contract
https://github.com/Giveth/minime/blob/master/contracts/MiniMeToken.sol

7.4 Distributed FORESTING Storage DApp

FORESTING Storage PoC (Proof of Concept) uses Swarm and NS (Name Service) on the blockchain to search contents such as DNS of serverless WWW, and will provide application extensions, such as transactions with smart contracts in conjunction with tokens.

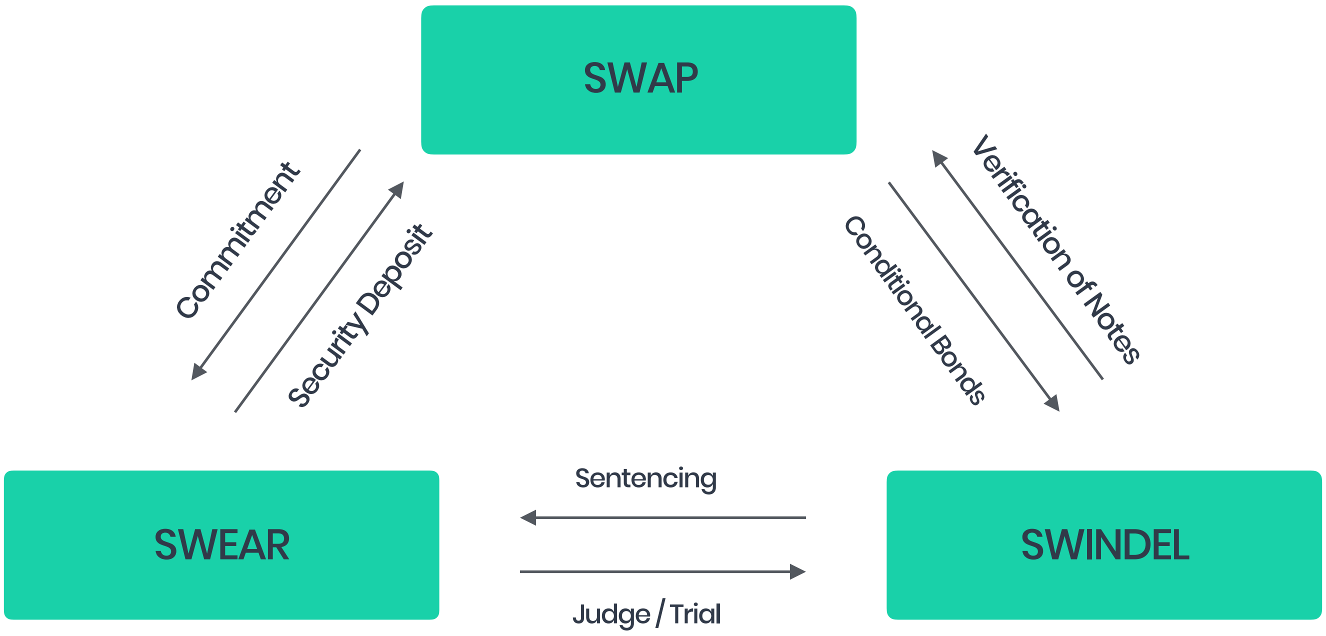


7.4.1 FORESTING Storage Synchronizing and Using Swarm Between Multi-Nodes



7.4.2 Swap, Swear and Swindle for FORESTING Storage

The basic components of the incentive system to maintain the FORESTING.Storage network	
SWAP(Swarm Accounting Protocol, Secured With Automated Payments)	Smart contracts with delinquent payments, payment channels, escrow management, and debt management
SWEAR(Secure Ways of Ensuring ARchival or SWarm Enforcement And Registration)	Membership registration, Membership conditions, Deposit processing
SWINDLE(Secured With INsurance Deposit Litigation and Escrow)	Audits, transfer of lawsuits



The storage ecosystem's gadgets will be the first implementation devices to fully support SWAP, SWEAR and SPINDLE, and will provide FORESTING's users with a more decentralized, distributed storage experience.

7.5 QRNG(Quantum Random Number Generator)

The creation of a True Random Number in the cryptography is really important. However, due to the constraints of the actual economic transaction time, FORESTING uses Pseudo Random Numbers.

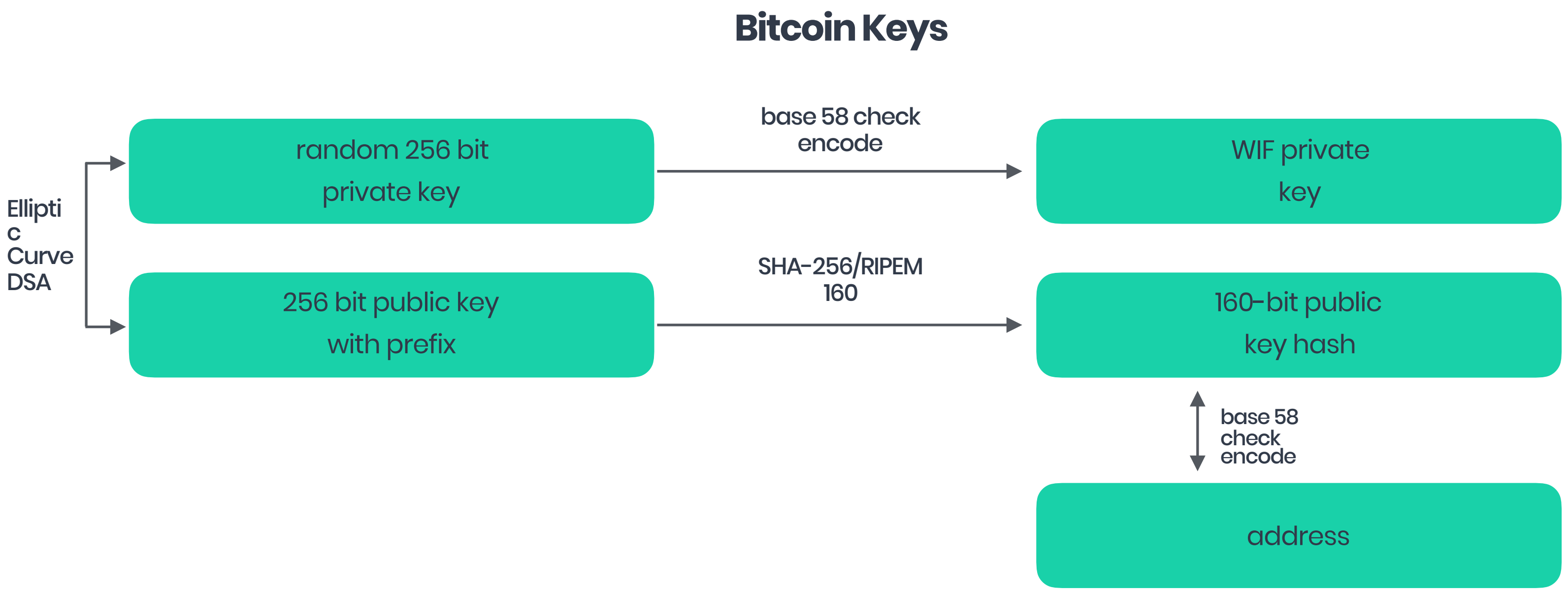
After Wang Xiaoyun, a female cryptographer at the Chinese Academy of Commerce University Information, released the study of "Collision for Hash" finding a single way password vulnerability in the current cryptology. On August 17, 2014, True Random Number became more significant.

The FORESTING network recognized the challenge of building a decentralized and distributed community. The FORESTING Network proposes a new method, QRNG, to add fundamental safety to the creation of a cryptocurrency address and to the transactions of Bitcoins or tokens. Since Bitcoin created the signature algorithm by using digital signatures, it has been widely known and applied to all altcoins in transferring cryptocurrency.

Bitcoin uses a secp256k1 standard elliptical curve function (function) in the ECDSA (Elliptic Curve Digital Signature Algorithm) family, which is an unsynchronized key algorithm. The public key is expressed as the coordinates (x, y) of the elliptical curve function, and since the (x, y) was used in the Bitcoin client in the past, it can be expressed only with the value of x. This is called a compressed public key, and the latest version uses it to create addresses. If we call it PubKey, the formula for finding the cryptocurrency address hash is as follows.

PubKey hash<20bytes/160bits> = RIPEMD160(SHA256(PubKey))
bitcoin address = Base58CheckEncode(PubKey hash)
** RIPEMD160 and SHA256 are hash functions*

Therefore, the Bitcoin address is based on the public key.



The storage ecosystem's gadgets will be the first implementation devices to fully support SWAP, SWEAR and SPINDLE, and will provide FORESTING's users with a more decentralized, distributed storage experience.

Therefore, generating addresses for all blockchains of Bitcoin follows the procedure as below:

256-bit random number private key is generated. The private key is required to sign the transaction and send Bitcoin. If the private key is not kept securely, there is a risk of Bitcoin being stolen.

The Elliptic Curve DSA algorithm generates a 256-bit public key from the private key (elliptical password will be explained later), which is used to verify the signature of the transaction. The bitcoin protocol adds 04 to the public key. The public key is not released until the transaction is signed, which is different from what most other systems do.

The next step is to create a bitcoin address and share it with others. Because the 256-bit public key is large, the SHA-256 and RIPEMD hash algorithms are used to downgrade it to 160 bits. The key is encoded in ASCII using Bitcoin Custom Base58Check Encoding. The final result will be the same value as 1KKKK6N21XKo48zWKuQKXdvSsCf95ibHFa and will be the address to which people can send/ receive Bitcoin. The public and private keys can not be obtained from the address. If one loses their private key, they won't be able to access their bitcoin.

Finally, the Wallet Import Format (WIF) is used for adding to the bitcoin core program. This is a base58Check encoding of the private key in ASCII and makes it easy to extract a 256-bit private key.

In summary, there are four types of keys: 1) private keys, 2) public keys, 3) hash of public keys, and 4) external keys with Base58check encoding. This is because the private key is a very important key, and is necessary to generate Bitcoin and other keys. The open key hash is a Bitcoin address.

The following code manipulations are used to generate WIF formats and addresses. The private key is only a 256-bit random number. The ECDSA password library generates a public key from a private key. The Bitcoin address is created by a SHA-256 hash generator, RIPEMD-160 hash calculator, and by adding Base58 and Checksum. Finally, it encodes the private key to Base58Check and inserts it into the Bitcoin Core program.

We know the technology of the world of atoms and photons that go against intuition. We know that at each particle level, there is a whole new potential for quantum chance. Quantum Nonlocality presents a new possibility for secure, non-national distribution, which is based on non-national correlation. This is a technology using entanglement and quantum incontrativity, and the principle is based on the principle of uncertainty that was discovered in the early 20th century.

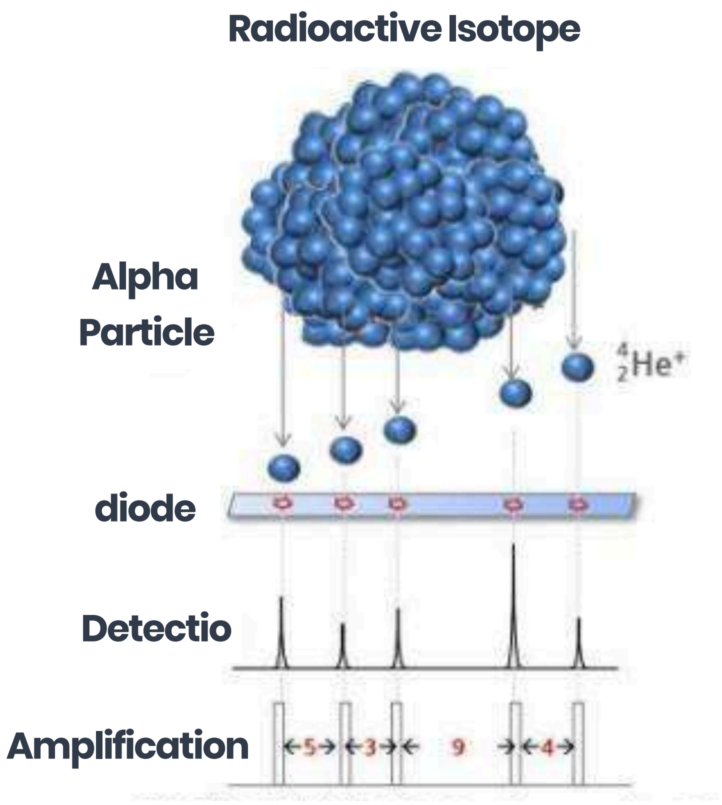
$$\Delta x \Delta p \geq \hbar/2$$

We have the opportunity to use this technology in the core of the FORESTING chain, and it is the H/W HD Walls of " FORESTING for Phone " and the super nodes that support the Port.

Available Products

QRNG – EYL [Suitable for Super Node]

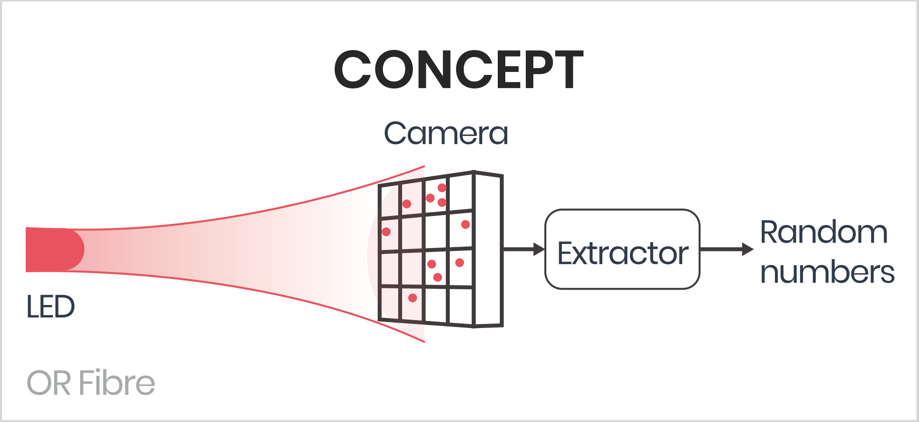
Principle of Micro QRNG



- Use alpha particles emitted by radioactive isotopes for a half-life.
- It follows uncertainty in terms of quantum mechanics and thus has full uncertainty.
- Produce random numbers that humans can not predict.
- Alpha particle → Diode collision → pulse generation
- Measure the time interval between pulses to generate random numbers.

[Measurement of the time interval between pulses:]

QRNG - SKT [Suitable for Mobile]



QRNG - SWISS IDQ [Suitable for Super Node]

Quantis QRNG: USB

- 4Mbps of true quantum randomness
- Certified by Swiss National Laboratory
- USB 2.0 interface
- OS Support: Windows, Linux, Solaris, FreeBSD, MAC OS X
- Demo application

Quantis QRNG: PCIe 4Mb

- 4Mbps of true quantum randomness
- PCI Express interface
- Certified by Swiss National Laboratory
- OS Support: Windows, Linux, Solaris, FreeBSD
- Demo application

Quantis QRNG: PCIe 16Mb

- 16Mbps of true quantum randomness
- PCI Express interface
- Certified by Swiss National Laboratory
- OS Support: Windows, Linux, Solaris, FreeBSD
- Demo application

7.5.1 Using in game Dapp

QRNG is a method for use in a random games with a quantum random number generator. It provides an API that can be linked in game apps or other sites.

However, although it is possible to link game apps, handing over the random number needed for the game directly to other sites should not be allowed.

It is possible to receive and process game result values through the linked game app.

7.5.2 Using Blockchain OTP

Allow the EVM smart contract code to read the QRNG from the view to provide OTP.
The secret key for the OTP registration should be stored in the mapping variable of the smart contract (storage in the blockchain).

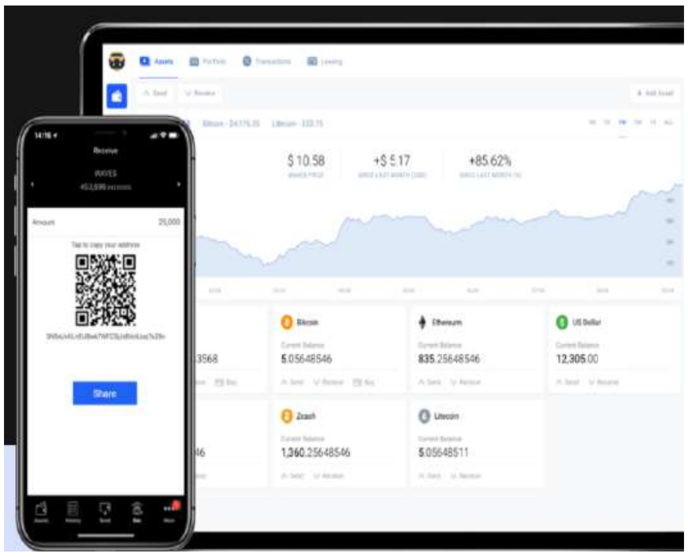
When OTP smart contract code is imported into library code and smart contract is created, OTP code is input to withdrawal, deposit, and other function calls that are important for security, and allow withdrawals and deposits only when the corresponding OTP code is verified.

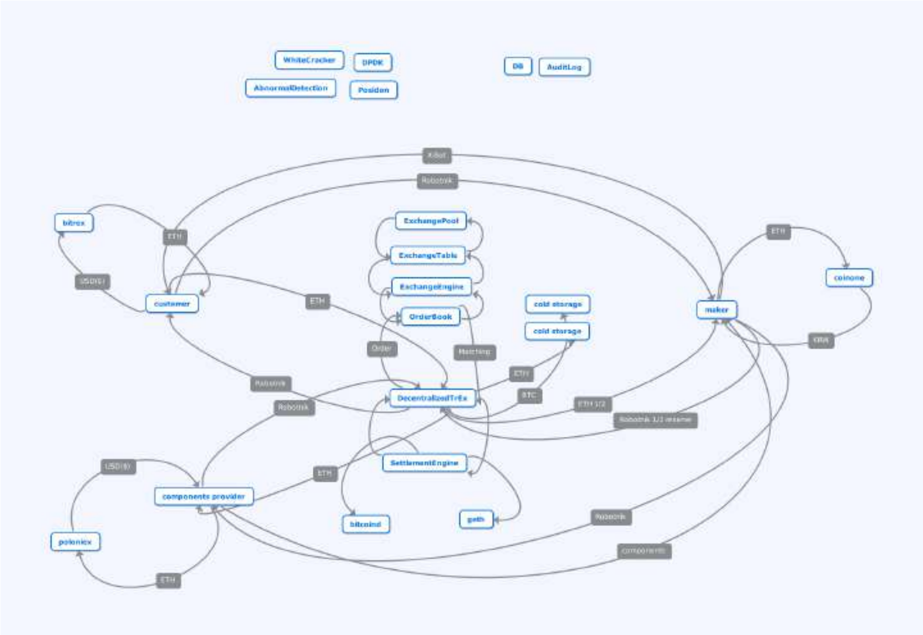
7.5.3 Randomness Beacon

In order to efficiently use True Random Number extracted from QRNG, it would be more efficient to broadcast a random number in a separate beacon chain using JSON-RPC API and Schema, and it will be implemented through sufficient experiment and verification.

7.6 Exchange Protocol

FORESTING aims toward global services, while making content more comfortable for all users using FORESTING and easily exchanging the value granted into fiat. To do this, the app shows the current coin price in real time through connection with the main exchanges worldwide. It also provides value-secured token transactions through links with StableCoin and Dex.





FORESTING is primarily aimed at community-based development and projects. Decentralized voting and messaging are implemented to achieve that goal. This allows the same experience as DAO in managing community projects while being simple from a technical standpoint.
FORESTING allows users to pay network transaction fees with custom tokens. Along with such transactions, orders to exchange assets with a primary network token are sent to a different decentralized exchange. The transaction can be added to the next block only after the order has been processed.

7.7.1 P2P Exchange Based on Fullnode Optimized for Social Media

In general, P2P Exchange Based on Fullnode Optimized for Social Media opens at least 10 coins per user and can be updated after opening. Setting by blockchain is possible, and compilation and installation of blockchain nodes for each coin is automated. The RPC Module is provided for coin-specific access. Basic work and master node are provided for the operation of nodes, and some coins may be provided at lighter wallet level. These master nodes or wallets can be connected to FORESTING's Payment channel, and State Channel.

The Dex of FORESTING allows selling and buying FORESTING tokens enabling general, split, bidding, split bids, and establishing a polling pricing information collecting system. Use the notification service such as closing of a transaction or announcement, push alarms, social media, e-mail etc. Transaction details and statistical inquiry are made available in a variety of ways.

This allows group chat to be used through the zn-SNARKs library. It also provides instant messaging services for consultation and inquiry about transactions between users.

7.7.2 Ring Signature

A ring signature is a type of digital signature in which a group of possible signers are merged together to produce a distinctive signature that can authorize a transaction.

Messages signed with ring signature are warranted by users of certain groups.

One of the security properties for ring signature is that it is not possible by calculation to determine which key of group members was used to generate the signature.

The actual signer is a one-time spend key that corresponds with an output being sent from the sender's wallet.

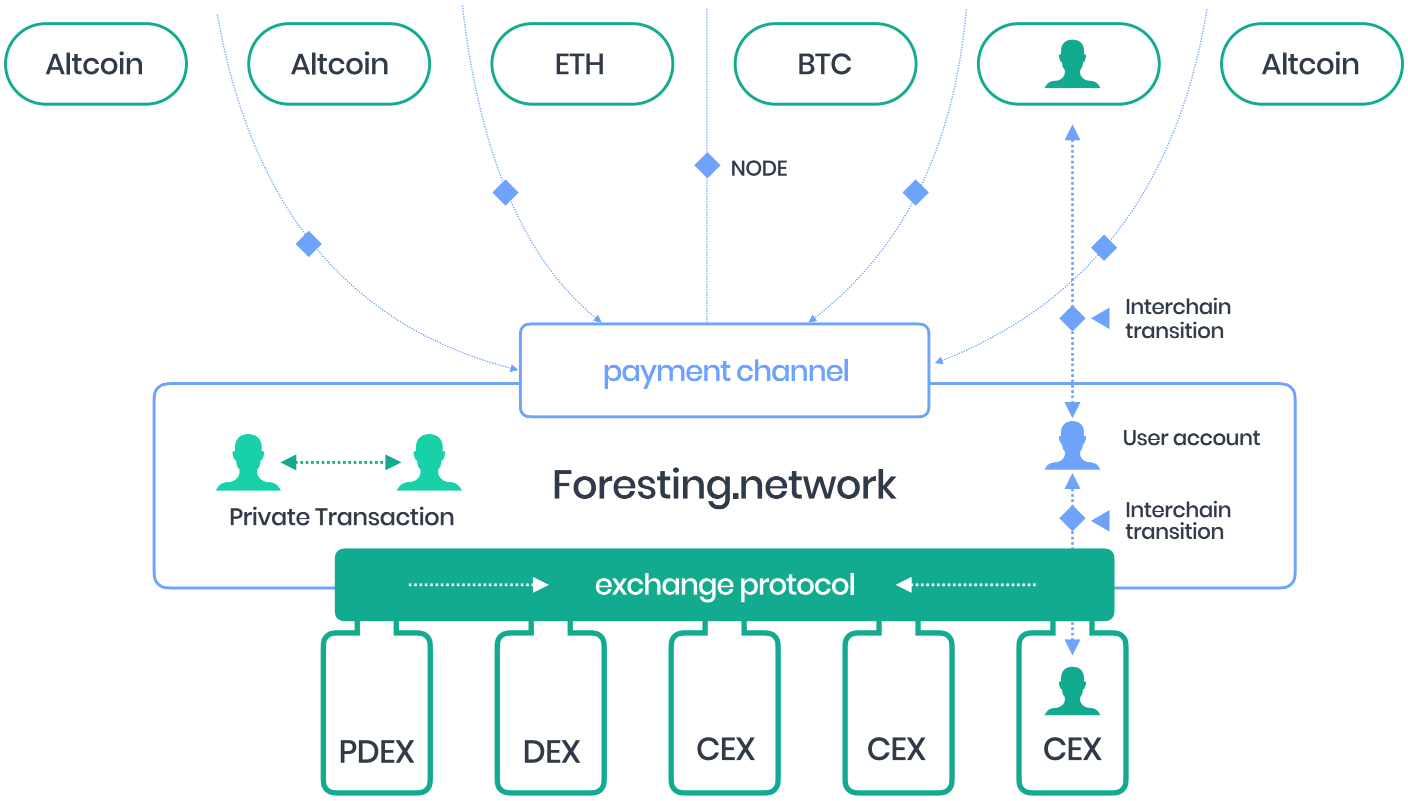
Ring Size: The more signatures allocated to the ring signature, the stronger the security will be. There will be 3 foreign outputs and 1 "real" output if there are 4 ring sizes to disguise where the transaction is being sent.

Since Monero uses ring signature techniques, it must include the ability to determine the output consumed by ring signature transactions to solve double spending problems.

Resolve with key image of Monero

If Bob tries to send a Monero to Alice, she has a ring size of 5 and one of the five inputs is taken from Bob's wallet and added to the ring signature transaction.

- Other four are past transactions from the Monero blockchain
- Four inputs are called decoys and are fused with Bob's transactions to form a group of five signers
- The third party cannot determine which Tx was actually signed by Bob's one-time spend key.
- Key image allows you to ensure that the Monero sent to Alice's account has not previously been spent



7.7.3 Stealth address

One of the keys to Monero's security is to allow and require the sender to generate a random one-time address on behalf of the recipient for all transactions.

When you create a Monero account, you'll have a private view key, a private spend key, and a Public Address.

View Key- The key to view transactions that have been entered into corresponding account ; the transactions sent by that account cannot be viewed

Spend Key - The key that can generate transactions of the corresponding account for which other keys can be derived.

Monero allows optional semi-transparent transactions through the view key.

7.7.4 One-Time Account System

Account Generation Algorithm

1. Main account generation

The private key of Alice's main account is (A, a), and (B, b) from the one - time account system. If the original account of Alice in blockchain was named (A, a), the main account in the one time account system would be (B, b). The private key of Alice's main account is (a, b), and the public key is (A, B).

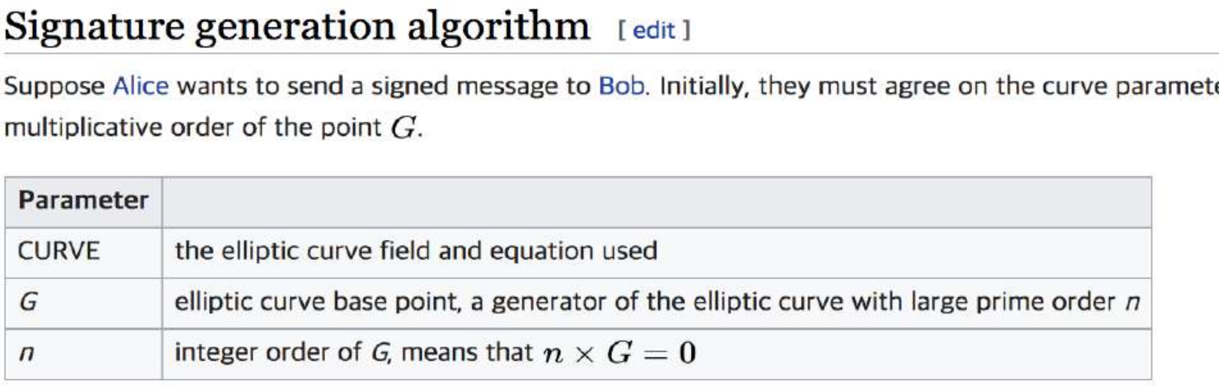
Alice will now have a private key (a, b), a scan key (A, b), and a public key (A, B) as the addresses of the main account

2. Sub-Account Generation

Bob tries to send a transaction to Alice, and her main account (A, B) creates a sub-account (A1, S1), which is a one time account.

Bob generates the random number 's' and calculates S1 = [s] G와 A1 = A + [Hash_p([s]B)] G, (A1, S1) as the one time account.

7.7.5 ECDSA G



Signature generation algorithm [edit]

Suppose Alice wants to send a signed message to Bob. Initially, they must agree on the curve paramet multiplicative order of the point G.

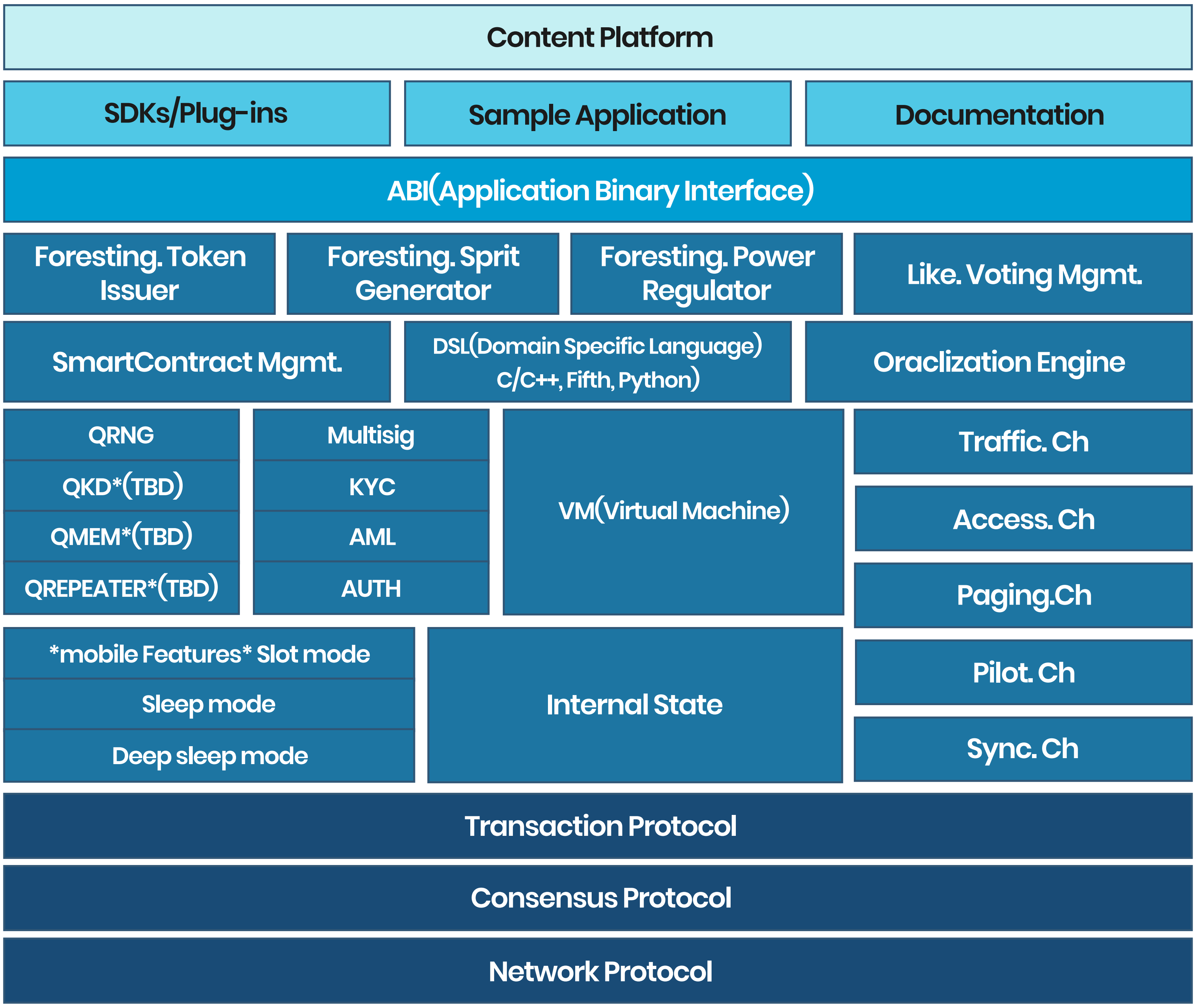
Parameter	
CURVE	the elliptic curve field and equation used
G	elliptic curve base point, a generator of the elliptic curve with large prime order *n*
n	integer order of *G*, means that $n \times G = 0$

7.7.6 Stamp System

A system that determines which accounts pay for transactions. Since transactions cannot be tracked in a one-time account system, there is no way of knowing which transactions to pay. In technical terms, a one-time account and one-time stamp is the same.

User purchases stamps before performing transactions. Stamp is replicated into a transaction and used only once.

7.8 Technical Roadmap



Content Platform

SDKs/Plug-ins

Sample Application

Documentation

ABI(Application Binary Interface)

Foresting. Token Issuer

Foresting. Sprit Generator

Foresting. Power Regulator

Like. Voting Mgmt.

SmartContract Mgmt.

DSL(Domain Specific Language) C/C++, Fifth, Python)

Oraclization Engine

QRNG

QKD*(TBD)

QMEM*(TBD)

QREPEATER*(TBD)

Multisig

KYC

AML

AUTH

VM(Virtual Machine)

Traffic. Ch

Access. Ch

Paging.Ch

Pilot. Ch

Sync. Ch

mobile Features Slot mode

Sleep mode

Deep sleep mode

Internal State

Transaction Protocol

Consensus Protocol

Network Protocol

Tech-Roadmap 1

Stage 1
Foresting.network Alpha Test Net
Supernode make
Wallet Sample

Stage 2
Foresting.network Beta Test Net
Fullnode make
Foresting.Block explorer
Web Wallet
Community Site First Edition
Test issue of PTON token
Test operation of PTON CREDIT and CASH

Stage 3
Forseting.network Mainnet Launching
Android, iOS Mobile Wallet(Lightnode)
Foresting for phone make and distribution
BLE nano ledger make
Foresting.scan info site
Foresting.dashboard site
Community Site Second Edition
Proof Mechanism of Concept(PMC) for Like Voting
PMC for Reward and echo system
PMC Credit Evaluation

Tech-Roadmap 2

Foresting.Bank launching
Ensuring the confidentiality of orders and transactions (porting znSNARKs)
StableCoin issue or Pegging w/ DAI for value stability
Acquire Liquidity and interoperate w/ Gateway(such as OpenANX)
Make Foresting.Storage.node and distribute gadget
Make first Foresting.Storage DApp and IDE SDK Release
Community Site Third Edition release
Make KYC,AML,Oraclization utility-chains
Make Foresting.QRNG and release

Tech-Roadmap 3

Make Forsting WASM Plug-ins for high transaction speed
Use dPoS+modifiedPBFT Core Consensus Mechanism and Make Advanced for 1,000 transaction per second
Use modifiedFBA and Make improvements for 250,000 transaction per second
Use modifiedSharding and Make improvements for 1,000,000 transaction per second
Community Site Forth Edition
Make Foresting.Messenger.node and distribute gadget
Make lightweight DApp repository
Make IBC(Inter-Blockchain-Communication) Interface hub and convertor
DApp Project to Side-chain,Child-chain,utility chains
Research HashLimit protocol and delayedPoW and make low-power miner
Community Site Fifith Edition release

Chapter 8

SECURITY & PROTECT THE PERSONAL INFORMATION

8 Security & Protect the personal Information

For various services, storing and appropriating personal information is essential. However, there are many incidents related to personal information extraction from personal information and big data. In order to provide services related to the blockchain, a certain amount of personal information can be obtained. However, since the blockchain is a public ledger, personal information can not be stored in the blockchain in any way.

Although the encryption of the block chain itself is excellent, it's impossible to store personal or sensitive personal information that can identify an individual.

the following table shows the protection of existing Internet services and the common blockchain, and Foresting

Category	Internet	block chain network	Foresting
Confidentiality	X	X	○
verification	X	X	△
Purity	X	○	○
ban negative	X	△	△

FORESTING will combine new perspectives of technology solve security and personal information problem which depend on loadmap. FORESTING is a totally new technology implementation that, for the first time in a blockchain ecosystem, will provide fundamental security and information protection technologies using the principles of physical phenomena.

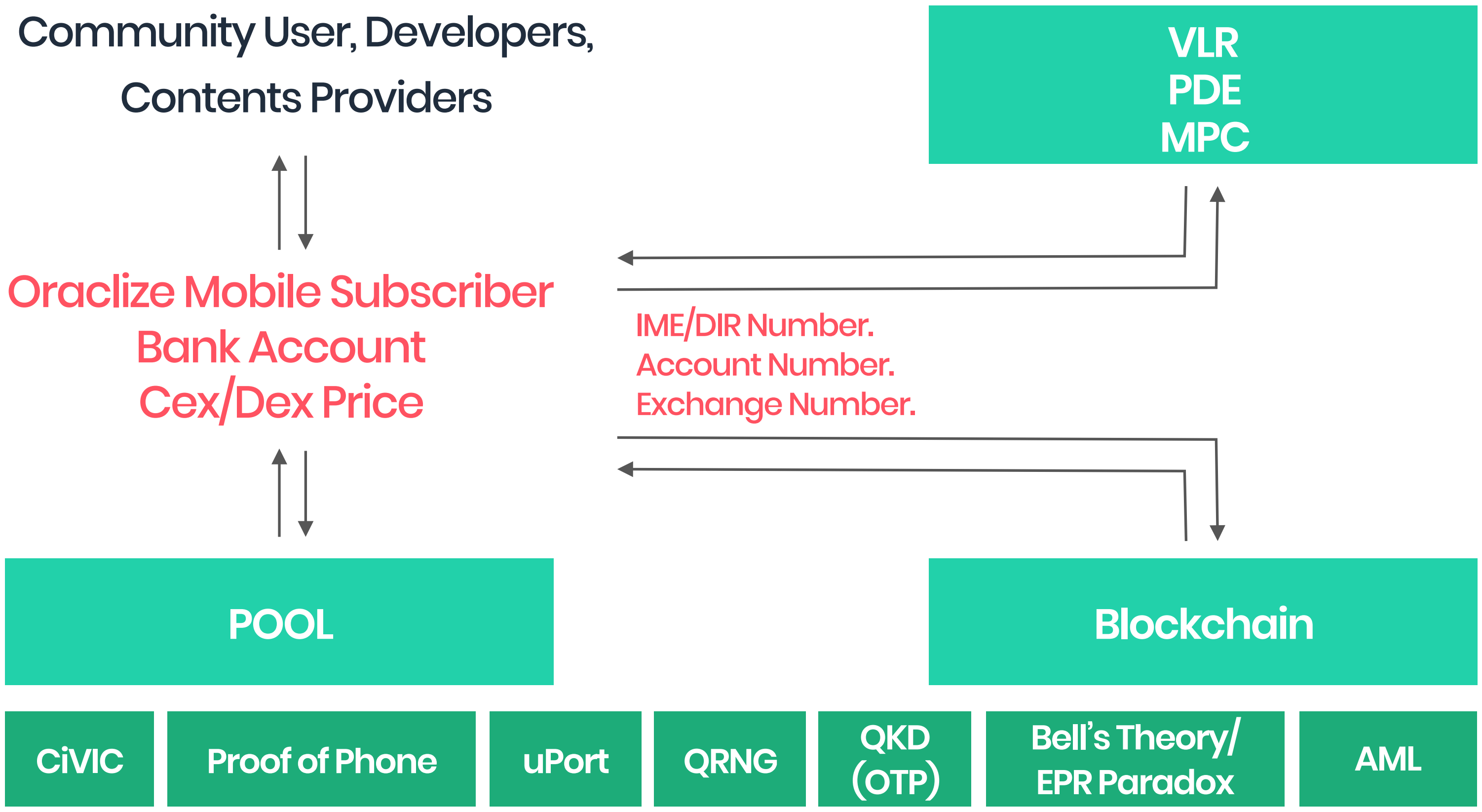
8.1 Oraclization

The content creator has copyright for the uploaded contents on social media.

The content creator can prove ownership of the content by writing evidence in the blockchain that it has created this content. The user can then prove that the data has not been tampered with.

All subsequent revision records can be validated through a blockchain. However, it is not possible to put all of this data in a blockchain. If one attempts this, the amount of data in the node increases very quickly, making it difficult for the node to survive. Therefore, information that gets uploaded to the social media platform is stored in a blockchain by compressing and encrypting only specific information.

In this process, we need a system that accurately links content to content creators, ensuring that important data is not tampered with.This system is called a 'FORESTING Implementation', and is a system that exchanges interactive data between the content producer and user operating smart contracts on a blockchain. This ensures that important data is not tampered with since there is a sufficient and completely trusted system to protect the data.



By examining existing implementations in depth, we apply this feature to mobile-optimized FORESTING, to ensure that the rights and interests of participating content contributors are met.

8.2 uPort Identity

When you use various social media, you will use various accounts and passwords. If you use the same username or password, and an account hacking occurs at one site, the damage will spread to all sites and have a severe impact. However, if you have different account information for each site, you could easily lose your account information. This can lead to the centralized management of account information for specific account management services. If this service suffers a hacking attack, all related sites will be hacked at the same time.

To solve this problem, it is possible to apply a private key / public key encryption technique using a blockchain instead of the existing account information method. However, it is not easy for a typical social media user to manage a private key / public key system in a blockchain. Therefore, FORESTING supports a solution that makes it easy to manage login information at the consumer level of the mobile environment. This solution supports EVM and ERC20 to create a foundation for accepting uPort identity services on social media platforms. By adding relevant logic to the smart contract, it reduces the burden of key cancellation, recovery, and user's key management.

8.2.1 Introduction to uPort

uPort is a user personal identification DApp based on EVM. It is similar to OpenID on Facebook and Naver. With its highly secure system, uPort's core technologies are smart contracts, development libraries, and mobile apps. Smart contracts include informational encrypted hash values such as url associated with person identification, and algorithms that can be recovered when personally identifiable information is changed or lost. The Developer Library contains information that manages url, dropbox, google, etc. that are associated with personally identifiable information. The mobile app contains the user's key, so users can verify their identity.

uPort identities can be issued by individuals or institutions. The creator of the identity is called the self-sovereign identity. Identity creation and verification is not centralized. This identity can be used for electronic signatures, transaction checks, and so on.

Identity is stored as an encrypted hash of attribute information such as IPFS, Azure, AWS, Dropbox, etc., in which related personal identification information is stored. Therefore, when private information is required to be destroyed, the original personal information can be easily destroyed without touching the blockchain. By using hash information, it is easy to check authenticity of the first identification information.

- uPort, based on EVM, can be used for personal identification. It is a system with high security
- Three Elements: Smart contracts, development libraries, and mobile apps
- Smart contract: Core of personal identification, including logic to recover personally identifiable information when a user loses a device
- Development Library: Contains information associated with an external repository.
- Mobile app: Store User Key
- uPort identities
- Form: Person, device, object, institution
- Authority: The creator with self-sovereign identity has permission to create a new user ID without leaving the creation or verification to a third party with centralized management
- Key Features: Transaction verification, digital signature, etc.
- Identity is password-protected with off-chain data stores
- Each identity can store a hash of attribute information (such as IPFS, Azure, AWS, Dropbox, etc. where all data related to identity is securely stored)
- Identities: Ability to change profiles, automatically update friends, read and write to specific files
- Because uPort identities can interact with blockchains, they can manage digital assets (encrypted currency, token assets).

8.2.2 Proposed Use Cases

Features of the self-sovereign identity system

Own and control and individual identity, reputation, data and digital assets through a personal identifiable information creator.

Allows personal data to be accessed by the public selectively because the operator generates personal identifiable information.

Allows access to the digital service using a key without password

Allows digital transactions and digital documents to be signed for using the key

Allows data to be sent on the blockchain and enables control management

Can interact with dApps and smart contracts

Can send encrypted message and data using the key

Pros of self-sovereign identity system

Easy to sign up for as a new member since the personal information disclosure is small.

Features an enhanced KYC (Know-Your-Customer) process.

Reduces liability since the sensitive customer information is not stored

Easy for employees to comply with since it does not handle personal information

Easy to attract content providers because of the easy sign up process

Can easily allocate specific roles with specific privileges

Easy to use without any background knowledge once development is complete

8.2.3 uPort Technical Overview

- At the heart of uPort identity is a uPort identifier (20 byte hex String, globally unique)
- Identifier: Address of EVM Smart Contract, also known as Proxy contract
- Proxy contract: Forward transaction process which interacts with other smart contract identities on an EVM basis
- When a user interacts with a specific smart contract application, the controller contract sends a transaction via a proxy contract. This architecture allows the application to interact with the Proxy contract address. Proxy contracts indirectly ties users' private keys (stored on mobile devices) and application smart contracts.

The purpose of the Proxy contract with the core identifier is to allow the user to change the private key during persistent identifier management. If the uPort identifier of the user replaces the public key (corresponding to the private key), the control and management of the identifier will be lost when the device with the private key is lost.

In the event of a device loss, the Controller contract maintains a list of recovery agents (which help uPort users recover their identity). Agents may be institutions such as friends, family, banks and credit unions. To allow users to restore their identity, many of the minimum agents for decision-making are required to connect the user identity to the new device

Account Recovery

1. The recovery network will be stored in the controller contract
2. If you have a new device, you must recover your device
3. Notify a new public key to the recover network
4. If approved for new public key by ⅔ of the recovery contact, the controller contract will update the public key
5. The account identity will be successfully recovered

- uPort can be used in association with identity, even if it is not a blockchain. Bundle the external data structure with the uPort identifier using the Registry contract
- Registry contract: A mapping of uPort identifiers to IPFS hashes
- IPFS: Decentralized system for transferring, connecting and storing data
- Hash: Ensuring the integrity of the data structure, encrypting the identifier is defined only by smart contract access management (the authority to update the registry contract is only uPort proxy)
- The name of the data structure corresponding to the IPFS hash includes profile information, and so on. It

  includes data, such as public keys, to support a decentralized public key infrastructure. The data structure is JSON type and strengthens the cooperation with Blockstack. Each JSON schema is digitally signed with a private key to create a JSON Web token. This token is used as a certificate in off-chain
- The attestation is a general structure, and a sure identity makes a different identity. Proof of signature that indicates that the public key belongs to a particular identity. Attestation is connected in two ways, much like Twitter, users are allowed to use their Twitter account to access other social media platforms.
- If the uPort user owns the encrypted key, attributes and attestations (connected to the Registry) can also be encrypted. By default, profile data can be private → and can be encrypted with the public cryptographic key of another identifier. The data will share these identifiers.

8.2.4 Technical Components

Smart Contract Components

- Proxy contract is the minimum contract used to send the transaction and the proxy contract address is the core identifier of the uPort identity
- Controller contract manages access control of the proxy contract and allows additional features
- Recovery Quorum Contract is used to recover identity if the key is lost.
- Registry contract password-binds off-chain data attributes and uPort identifiers

Data Components

Attestations are signed data records containing profile attributes that are stored off-chain with provable claims

- Optional public methods to encrypt data (with added privacy to attributes or attestation)

Developer Components
The developer library considers simple integration of uPort into decentralized applications or existing digital services.

Mobile Components
The mobile application stores the private key of the identity. Used to control identity and to sign attestations in the security of the smartphone.

Server Components
- Chasqui - messaging server
- Sensui - gas fueling server
- Infura RPC
- Infura IPFS

8.2.5 FORESTING blockchain and Smart Contracts

FORESTING blockchain: Blockchain architecture with associated state databases to store smart contracts and their state
Smart Contract: Any user of FORESTING can distribute this function-based interface.
Smart contracts are referred to as addresses (encrypted identifiers). A user can call a smart contract function by sending a transaction with a transaction data history that includes a smart contract address (destination), a source signature, and an input value. One can send or receive PTON, or can call another smart contract
Function call: The block producer on the network runs the program and updates its state.

8.2.6 Smart Contract Components

Proxy Contract
Benefits of Proxy Contro
- One can insert functions such as playing a used key or key.
- If one regenerates a key, the identifier of the identity does not change
- Two basic functions of proxy contract
- One can create a transaction with a different external address
- It's possible to transfer contract ownership

Controller Contract
Purpose: To isolate the controller part so that you can change the logic of a smart contract without changing the uPort identifier.
RecoverableController.sol
- User Address: The public key which is normally used
- Recovery Address: The key used for recovery
- Recovery Quorum: See below

1. The user address can send a transaction with a proxy contract
2. The user address can transfer control of the proxy controller to the new controller connector.
3. The user address can change itself to another address (time-locked)
4. The recovery address can change the user address to another address (time-out)

Recovery Quorum Contract
Recovery Delegate: Allows the user to change the user's address to another trusted person

recovery delegate
- If more than half of the users agree, the user address changes.
- The user can change the recovery delegate.

Registry Contract
Purpose : uPort identifier - mapping of data structures outside the blockchain

8.2.7 Data Components

Attributes and Attestations

Attestations
Signed data records containing profile attributes and / or verifiable claims, stored off-chain.
uPort Registry
Cryptographically linked profile data or attributes to a uPort identifier
> plain JSON structure or signed JSON web token (JWT) (/ by blockchain-profile-js)
* JWT reference site: https://jwt.io/introduction

Example
> Attribute: {"name": "Christian Lundkvist"}
> Attestation: Configure as JWT (Header.Payload.Signature)
Signing user attributes allows for the identification of the identity and the validity of the profile data. This can be useful for KYC (*), where a bank can attest to the validity of profile data or other attributes of their customer. The bank can also be used as a cashier.

The signed user attribute (information) can be validated by a third party, which is useful as a KYC is required by the anti - money laundering system, and can be utilized by financial services through a portable KYC token.
uPort identity
> Provisioning keys for applications, devices or services and revoking
> Linked profiles: Using existing social media services to bootstrap your identity

Signing the attribute with the uPort signing key creates a claim that the uPort identity controls the twitter account with the handle, e.g ChrisLundkvist.

Selective Disclosure

A mechanism for encrypting data that adds a layer of privacy to attributes and attestations.
> Adds a layer of privacy to the uPort by allowing users to encrypt some or all attributes by default, and chooses who to share the data with.

Due to the openness of the information in the blockchain, we have an added Layer of privacy so that uPort users can encrypt and share some or all privacy attributes..

The system relies on each uPort identity to have a public encryption key. The disclosure of an attribute works by having the user encrypt an attribution with a symmetric encryption key. This key is then used to encrypt the public key of each identity.

One can use a symmetric key to determine whether the property is public, and encrypt the public key individually with the public key of the uPort ID.

Consider this situation.
Suppose we wish to share this attestation with only identities X, Y and Z. We first generate a random symmetric key k, and encrypt it symmetrically.
We denote this ciphertext sym (k, A).
Now we assume that X, Y and Z each have a public encryption key. Let asym (U, V, d) denote the asymmetric encryption between identities U and V of some data, d. Specifically, asym (U, V, d) = sym (DH (U, V), d)
Where DH (U, V) is a symmetric key generated from the public key of U and the private key of V using a Diffie-Hellman key exchange.
Asym (Z, R, k), asym (Y, R, k), asym (Z, R, k))

8.2.8 Mobile Application

Mobile applications are the means by which end users interact with their uPort. Which in principle means managing the users' private keys.
The basic idea for users' primary keys is to put them in a secure isolated space and accesses them through local biometric authentication whenever the key is used for signing.
The user's private key remains on the device and there is no way to export that private key outside of the device.
The user experience is the main consideration of this mobile app interaction model's design.
There are two main actions for interacting with the FORESTING blockchain using DApp.

1. "Connect": Provide a uPort identifier to the DApp. (Or to the Foresting address)
2. "Verify / validate / authorize" an interaction by signing a transaction with a private key. The interaction has been designed using patterns found in popular applications like WhatsApp and WeChat
The desktop version of these apps shows a QR code and if users scan this code using their mobile app, they can sign in.

This precise user flow is used by the uPort mobile app for the "connect" flow in DApp.
When the user needs to confirm the interaction with the blockchain, such as transaction signing, another QR code is shown.
The user scans these codes and is presented them with a confirmation screen (which can be verified using the user's fingerprint).
Similar to this, there is a BankID system that interacts with a bank in Sweden and verifies the transaction.

If the DApp works in a mobile browser, the interaction model is slightly different. Instead of showing the QR code, the DApp will ask the user to run the uPort app.
The user will redirected to the uPort app in which users can authenticate the distribution of their identifiers and sign transactions.
After that, they can return to the mobile browser for later DApp interaction.

FORESTING intentionally seeks to create a user experience in which the user no longer needs to know the public / private key encryption algorithm.
User's mental models will be their smartphones and uPort apps. Smartphones and uPort apps can be used for interacting with the DApp, logging in to websites, verifying transactions, signing documents, and so on. If the user loses their cell phone or mobile device, they can ask their acquaintances to help them recover their identity.

FORESTING will provide uPort-based KYC, CDD to protect content creators and contributors who issue a DApp or tokens, and will provide an infrastructure that is flexible and easy to use through DApp technology.

All of this will be the first implementation of FORESTING Improvement Proposal (FIP) 001 "FORESTING for Phone" by FORESTING.

* KYC (Know Your Customer): This system came into effect on January 18, 2006 and was introduced to prevent illegal funds transactions and money laundering, and is in accordance with international standards. If a customer (including an agent in the case of a proxy transaction) opens a new account or makes a one-off transaction, it shall additionally confirm the address and contact information in addition to their real name under the Financial Real Name Act. The anti-money laundering system (AML) also refers to CDD (**)

** Customer Due Diligence (CDD): This is when a financial institution is obliged to ensure that their services are not used for illegal activities such as money laundering, by paying diligent attention to their service user's financial transactions and activities.

8.3 Certification

FORESTING will use the authentication method in a Subscribe-based mobile communication environment. This authentication method that should be considered to be the core of user's information protection technology.
Currently, GSM is the representative mobile communication system in Europe and IS-95 in the United States that authentication parameters and global roaming service support. The following will describe the authentication requirements of the next-generation digital mobile communication system through an analysis of authentication threat factors and authentication methods in mobile communication.

The most serious information security threats in information and communications networks are illegal tampering, eavesdropping, identity theft and retransmission. With these confidentiality and integrity services, authentication services are among the most important information protection services.

In particular, authentication can protect against identity theft and retransmission threats and can provide access control, data integrity, confidentiality.
It is an important service that can be used in various forms in conjunction with non-repudiation and audit services. Certified objects are those processes that are executed either in a person, using a part of equipment, or a computer system in an information communication network. One may indicate their identity during the certification process and assert themselves as the applicant. The other party who verifies that the claim is legal is the verifier.

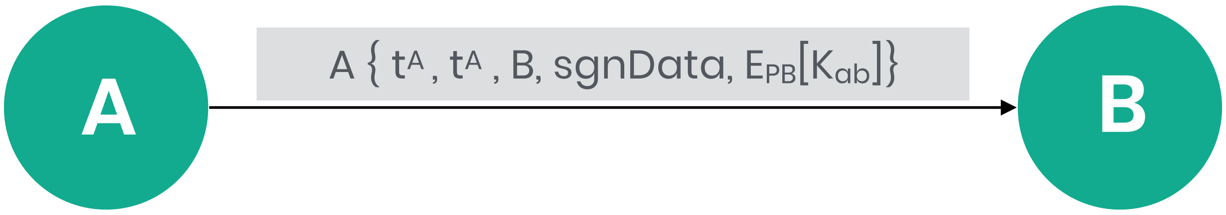
The authentication can be performed by the information exchanged between the applicant and the verifier. According to the contents of the authentication, it is classified into message content authentication, message origin authentication and general entity authentication. An attack that masquerades as an identity may be disguised as an applicant or a verifier, or it may have the form of disguising both parties in the middle. A retransmission attack may have various forms, such as simple retransmission and reverse retransmission without modification. It should be able to protect against threats of identity theft and retransmission attacks.

Particularly, digital mobile communication such as digital cellular mobile communication and personal mobile communication provides voice and data services without restriction of time and place.

The use of radio waves as a communication medium has a problem of increasing the possibility of wiretapping by tapping, radio recording, and illegal copying. In order to prevent such a situation, it is necessary to provide protection service and technology to prevent such money theft since e-mail and smartphones are currently being used for representative services. FORESTING, which is planning blockchain-based social media services, is actively embracing these benefits.

8.3.1 Authentication Mechanisms Using Cryptographic Techniques

An authentication mechanism based on cryptographic techniques is based on the principle that the subject knows certain secret keys and can ensure the verifier.
Symmetric key or public key technique: When using symmetric key technology, the simplest concept is that a subject and a verifier can share a symmetric key, then encrypt or seal a message using that key, to notify the verifier to decrypt or correctly open the message. The contents of the message include non-repetitive value. A non-repetitive value can be used to protect against a replay attack. With the public key technique, the subject signs the message with his / her private key, and the verifier checks the signature with the subject's public key In this case:
- Repetitive values are used for protection against replay attacks. However, in today's large network environments, authentication using a secret key scheme in a complex multi-carrier environment which is not practical from the viewpoint of key management.
- A basic and concrete authentication mechanism is the one published in the 1998 OSI Directory Standard
X.509, which is a collection of distributed servers that manage the database of servers or users.
- This has a directory structure that can act as a repository for public key certificate format. In addition, in a distributed or centralized structure environment, there is a certification service provided by Kerberos that is developed as part of a centralized X.509 one-way authentication.
- One-way authentication is done by adding and sending an authentication token signed with the originating secret key and is unique due to B's identity service and message. The message actually created by A is sent to B and not sent in the integrity and bulk of the message The following is a one-way authentication procedure, All.



Step 1 : A generate rA

Step 2 : A? B: As {tA, rA, B, sgnData, EPB [Kab]}

Step 3 : B:- Obtain AP and check the validity period of A's certificate

(AS is A's secret key, AP is A's public key)

Verify signatures and check the integrity of signed information

(This allows EPB to encrypt with B's public key)

Check if B is a legitimate recipient

Check whether tA is current time

Check if rA has not been retransmitted

In this case, only the identity is confirmed, not the response side. The timestamp (tA), the unique number
(RA), the identity of B, and the signature of A's public key. tA is the creation date and expiration date of the token.
This prevents the delayed delivery of messages. The unique number rA is used to prevent replay attacks.
This number should be unique to the expiration date of the message. Thus, B has to wait until the period expires.
One can store numbers and reject new messages with the same number. The authentication in the pure sense is A. B, the message, may contain information to be transmitted. All. sgnData is included within the scope of the signature, ensuring the authenticity and integrity of the message. This message can also be used to send a session key encrypted with B's public key to B.

Verification procedure for Kerberos (version 4)
Each message exchange used in the Kerberos (version 4) authentication procedure is as follows.
1) Exchange of certification services (to obtain a ticket-authorization ticket)
Step 1: C? AS: IDc // IDtgs // TS1
Step 2: AS → C: Ekc [Kctgs // IDtgs // TS2 // lifetime2 // Tickettgs], Tickettgs = Ektgs [Kctgs // IDc // ADc // IDtgs // TS2 / lifetime2]

2) Ticket → Authorization service exchange (to obtain service-authorization ticket)
Step 3: C → TGS: IDv // Tickettgs // Authenticatorc
Step 4: TGS? C: Ekctgs [Kcv // IDv // TS4 // Ticketv]
Tickettgs = Ektgs [Kctgs // IDc // ADc // IDtgs // TS2 // lifetime2],
Ticketv = Ekv [Kcv // IDc // ADc // IDv // TS4 // lifetime4],
Authenticatorc = Ekctgs [IDc // ADc // TS3]

3) Client / Server authentication exchange (to obtain service)
Step 5: C → V: Ticketv // Authenticatorc
Step 6: V → C: Ekcv [TS5 + 1] (for mutual authentication),
Ticketv = Ekv [Kcv // IDc // ADc // IDv // TS4 // Lifetime4], Authenticatorc = Ekcv [IDc // ADc // TS5]

IDv: Identifier of server V, ADc: Network address of C, Kv: Secret encryption key shared by AS and V, TGS : Ticket-Granting Server, TGStgs: C and TGS session key, IDtgs: TGS identifier for requesting use of C and TGS service, Ekv: means encrypting with TGS and the secret key known only to the server, Ktgs: shared to AS and TGS Secret key, Kcv: a secret key shared by C and V (issued by TGS), respectively.

8.3.2 Analysis and Use of Mobile Communication Systems

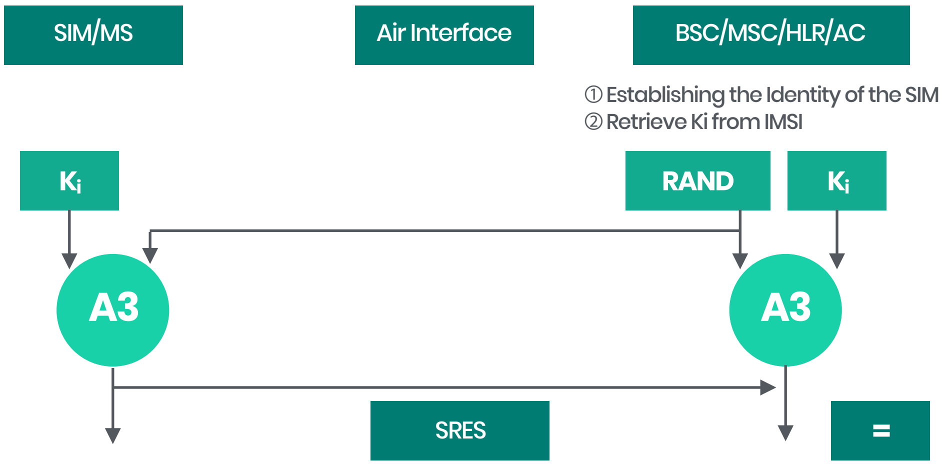
The protection service provided in the mobile communication system is subscriber authentication, subscriber anonymity (subscriber identifier protection), wireless line password service, etc. The protection service-related element includes a Subscriber Identity Module (SIM) that stores an individual subscriber authentication key Ki in the smart card and performs an authentication algorithm A3 and a cryptographic key generation algorithm A8, a mobile station (MS) A Visitor Location Register (VLR) for storing Temporary Mobile Subscriber Identity (TMSI) and determining whether the authentication is successful, as well as temporarily storing the information of the subscribers in the area, and the cryptographic key associated with the subscriber identifier. There is an HLR (Home Location Register) for storing and managing the value Kc, the random value RAND, and the authentication signature value SRES. The following are the protection services and features of GSM.

Key preparation

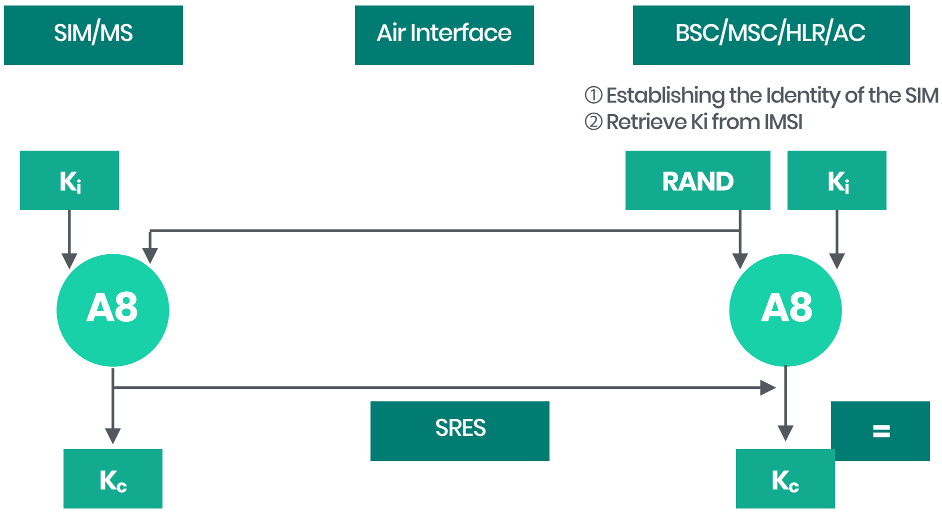
In the mobile communication system, a SIM containing various keys and algorithms is inherited in the smart card and issued to the subscribers. Therefore, it is possible to prepare basic keys and parameters, and the service provider controls the network access through this. The SIM contains a 128-bit authentication key called Ki, and the subscriber should use and manage it securely so that Ki is not exposed to the outside. If Ki is exposed, many cases of fraudulent access could occur, in which case the subscriber may be charged for unused charges and the secure communication channel may be broken. Therefore, Ki should be kept only by his / her SIM and the service provider provided at registration.

Authentication and Key Matching

In a mobile communication system, a unique challenge/ response protocol is used to generate an authentication key and an encryption key. This protocol actually occurs during call setup and is executed by the service provider or the network operator. That is, the network compares the 32-bit SRES with the internally calculated SRES for the generated mobile station using the 128-bit random value and the Ki that it has attempted to authenticate. At this time, if the authentication is successful, Ki is used to generate the encryption key Kc, and the same process is also performed in the network to prepare a session encryption key, such as a mobile station.



Password Session Key Sharing Procedure



Wireless Interval Message Password Communication Procedure

Ki is used to generate the encryption key Kc, and the same process is also performed in the network to prepare a session encryption key such as a mobile station.

Password
In mobile communication, the subscriber anonymity is maintained as TMSI / IMSI, and the message encryption communication for the wireless section is based on the secret key method. Here, the IMSI is a secret ID unique to the subscriber which is generated by the service provider based on the identity of the subscriber The network basically controls the subscriber's network access through the IMSI / TMSI which is the unique ID of the subscriber. In the above figure, it shows the process for the geocrypt communication.

Roaming
In mobile communication system, the roaming service can transmit five preliminary Triplets (consisting of RAND / SRES / Kc) from the Home Location Register (HLR) to the Visited Location Register (VLR). Thus, the user can receive communication functions and additional services by being authenticated by this triplet in their visited network. The subscriber can be authenticated without exposing his or her authentication key Ki. This value will change even if the triplet is intercepted, thus reducing the risk of permanent exposure. However, this approach does not provide complete roaming and is unable able to attack the authentication functions, depending on the safe handling and handover of the unused remaining set of triplets passed from the HLR to the VLR.

Location Registration

If the mobile station wishes to register its location in the base station, the mobile station informs the base station of its identity using the IMSI and registers the location. The location registration process of the present invention will be described as follows:

When the HLR sends the IMSI along with the authentication parameter request to AC, the AC performs the A3 and A8 algorithms by inputting Ki and RAND to calculate SRES and Kc.

If the AC sends authentication information including IMSI, Kc, RAND and SRES to the HLR, as a database, the MS transmits a Registration Update Request message, including the IMSI to the HLR, through the BSS / MSC / VLR.

The HLR sends authentication parameters such as Kc, RAND, and SRES to the VLR associated with the received IMSI. The VLR manages this information in a database.

The VLR sends an Authentication Request message to the MS that includes the RAND. The MS sends the received RAND. The secret key Ki is input, and the algorithms A3 and A8 are performed to calculate Kc and SRES. Kc. MS and the SRES are included in the authentication response message and transmitted to the VLR.

The VLR compares the received SRES with the SRES it has, and assigns the TMSI to the MS.

Call Sign Authentication

When the registered MS desires to call, the mobile station informs the base station of its identity using TMSI. The procedure of the mobile station call authentication is as follows.

The call setup indication message including the MS's TMSI is transmitted to the VLR via the BSS / MSC.

The VLR transmits to the BSS / MSC for the RAND authentication associated with the TMSI in the database it manages, and the BSS / MSC transmits RAND to the MS by including the RAND in the authentication request message.

S calculates the Kc and the SRES by performing the algorithms A3 and A8 with the received RAND and the secret key Ki as its input, stores Kc, and SREDS includes the authentication response message through the BSS / MSC to the VLR.

The VLR compares the received SRES with the SRES it has.

Call Authentication

When the registered MS attempts to respond to the call of the base station, the authentication procedure is as follows:

1) When the VLR receives an ISUP Initial Address Message (IAM), the BSC / MSC sends the MSRN to the VLR. The VLR selects TMSI, LAI, Kc, RAND and SRES and sends the SRES to the BSS / MSC together with the authentication message.

2) When the BSS / MSC sends a paging request message to the MS, the MS sends a channel request message to the BSS / MSC, the BSS / MSC sends an immediate assignment message to the MS, Lt; / RTI & gt. The message exchanged between the MS and the BSS / MSC at this time includes the TMSI. The BSS / MSC then sends an Authentication Request message to the MS that includes the RAND.
3) The MS performs the A3 / A8 algorithm with the received RAND and its own Ki as inputs,
After generating Kc, Kc is stored and the SRES is transmitted to the VLR through the BSS / MSC.

VLR compares the received SRES with its own SRES It has.

There are other procedures such as Location Area Identification (LAI) query and update related to other authentication services.

In order to use these authentication services, FORESTING will use SimToolkits and Radio Interface Layer (RIL) SDK for access and control.

Chapter 9

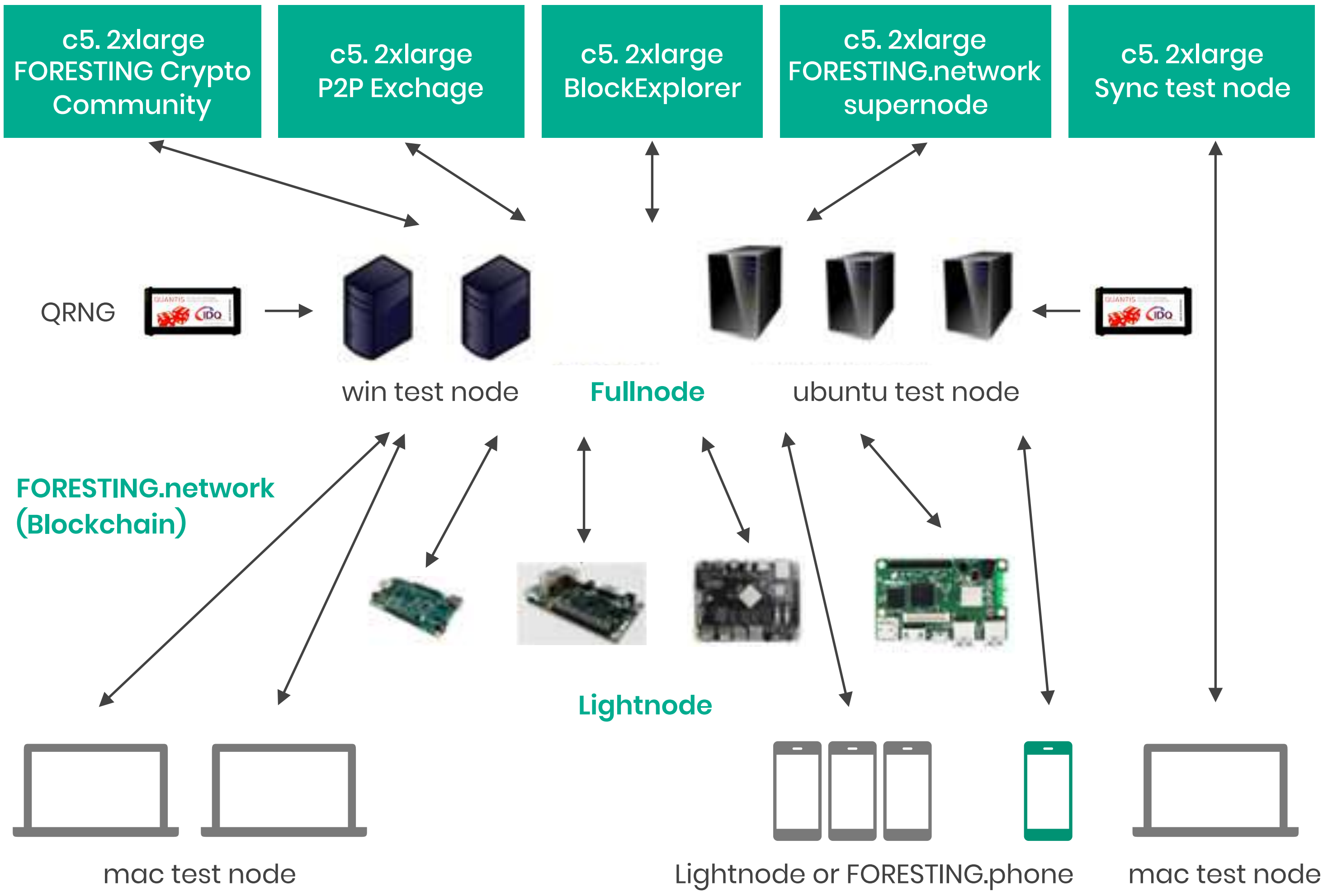
CONCLUSION

Counting down for important dates and numbers

9.1 FORESTING.testnet Diagram

Testnet Alpha

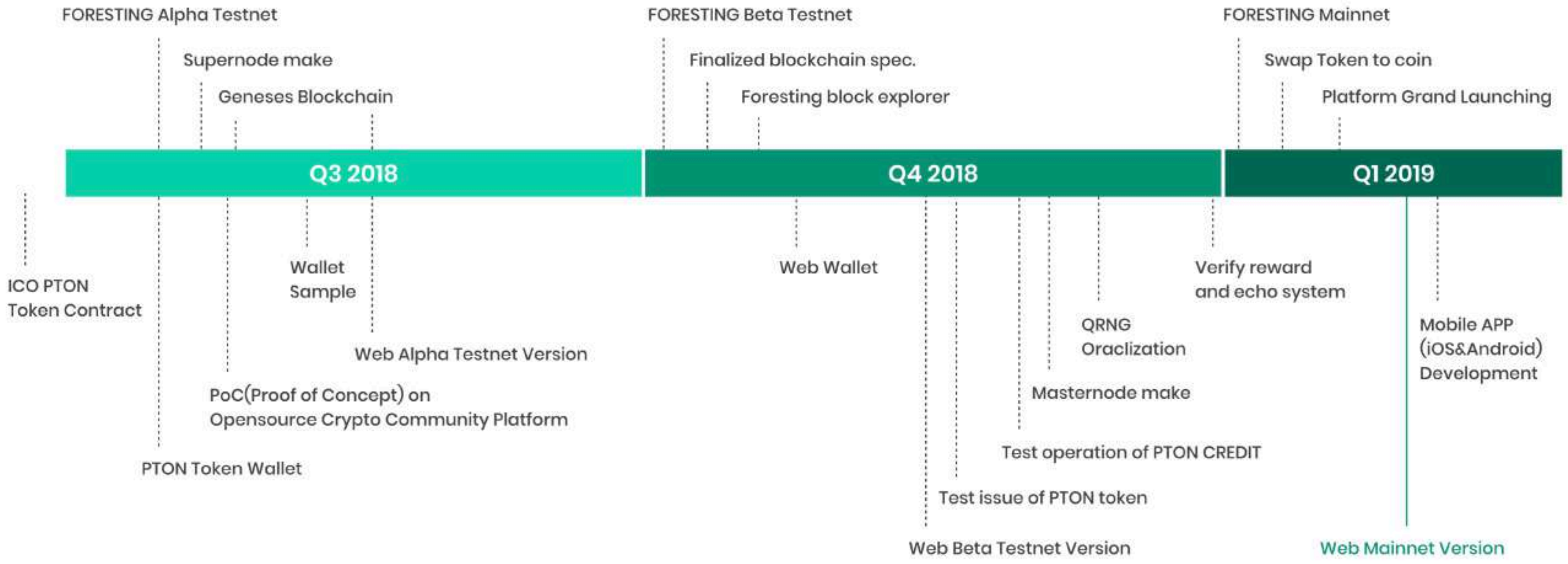
Amazon EC2 Instance (Ubuntu Server16.04 LTS)


c5. 2xlarge FORESTING Crypto Community
c5. 2xlarge P2P Exchage
c5. 2xlarge BlockExplorer
c5. 2xlarge FORESTING.network supernode
c5. 2xlarge Sync test node
QRNG
win test node
Fullnode
ubuntu test node
FORESTING.network (Blockchain)
Lightnode
mac test node
Lightnode or FORESTING.phone
mac test node

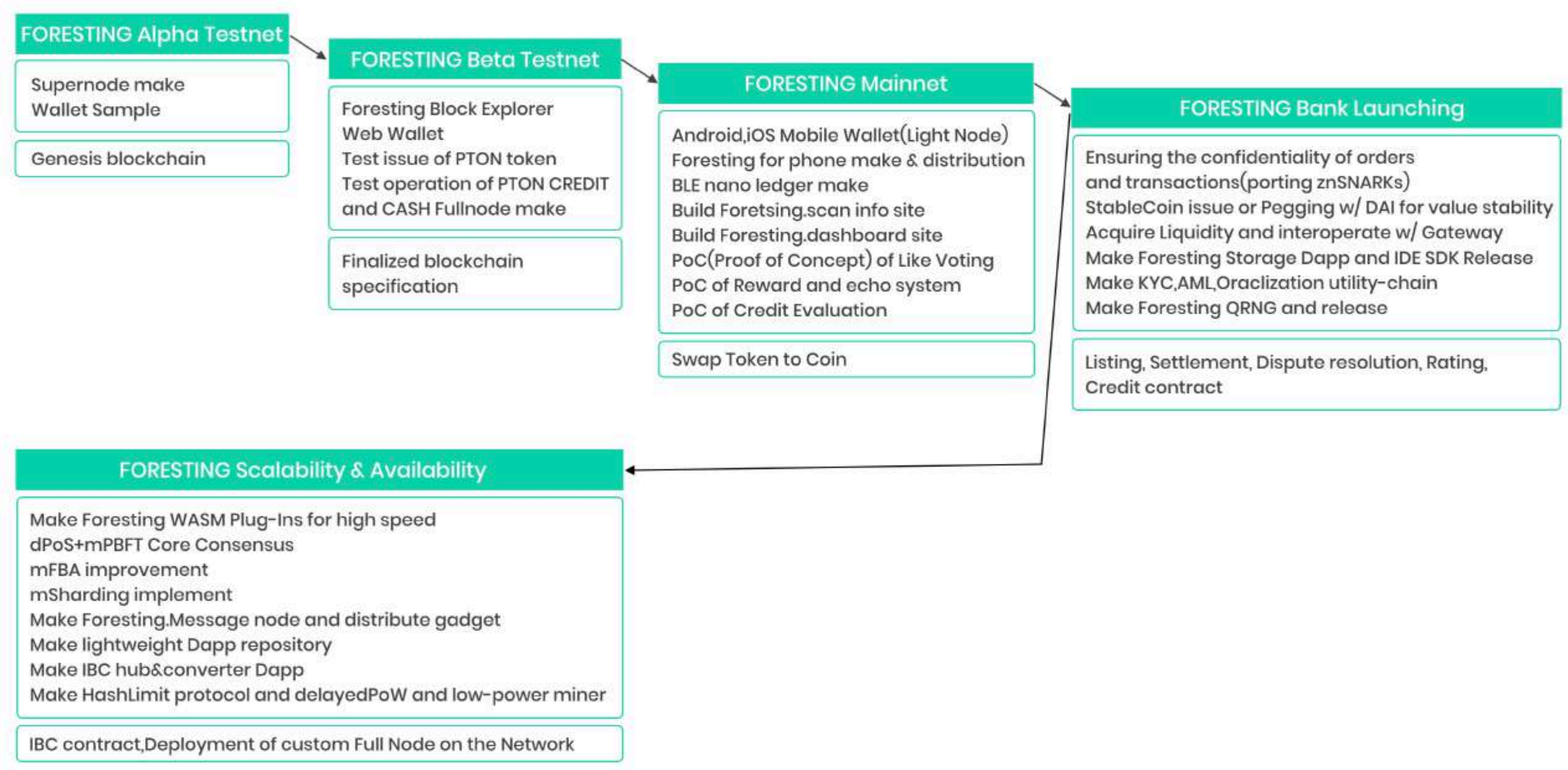
	Supernode	Fullnode	Lightnode
Testnet Beta	~5	10	100
Mainnet	21	100	1,000

10.2 Schedule

18'3Q-19'1Q Schedule



9.3 FORESTING.roadmap



FORESTING Alpha Testnet

Supernode make
Wallet Sample

Genesis blockchain

FORESTING Beta Testnet

Foresting Block Explorer
Web Wallet
Test issue of PTON token
Test operation of PTON CREDIT and CASH Fullnode make

Finalized blockchain specification

FORESTING Mainnet

Android,iOS Mobile Wallet(Light Node)
Foresting for phone make & distribution
BLE nano ledger make
Build Foretsing.scan info site
Build Foresting.dashboard site
PoC(Proof of Concept) of Like Voting
PoC of Reward and echo system
PoC of Credit Evaluation

Swap Token to Coin

FORESTING Bank Launching

Ensuring the confidentiality of orders and transactions(porting znSNARKs)
StableCoin issue or Pegging w/ DAI for value stability
Acquire Liquidity and interoperate w/ Gateway
Make Foresting Storage Dapp and IDE SDK Release
Make KYC,AML,Oraclization utility-chain
Make Foresting QRNG and release

Listing, Settlement, Dispute resolution, Rating, Credit contract

FORESTING Scalability & Availability

Make Foresting WASM Plug-Ins for high speed
dPoS+mPBFT Core Consensus
mFBA improvement
mSharding implement
Make Foresting.Message node and distribute gadget
Make lightweight Dapp repository
Make IBC hub&converter Dapp
Make HashLimit protocol and delayedPoW and low-power miner

IBC contract,Deployment of custom Full Node on the Network

9.4 Grand Mainnet Launching

FORESTING will target 0.6 Billion User when launching Grand Mainnet Net, and aims to build a network optimized for blockchain-based social media services.

The RAM usage of the account for one user on the blockchain is 4KBytes.

4Kbytes * 6 * 10 ^ 8 = 4TBytes

We already have a database of 600 million user candidates and plan to develop the optimal Supernode with a capacity of 4TB and 16TB as users increase in the future.

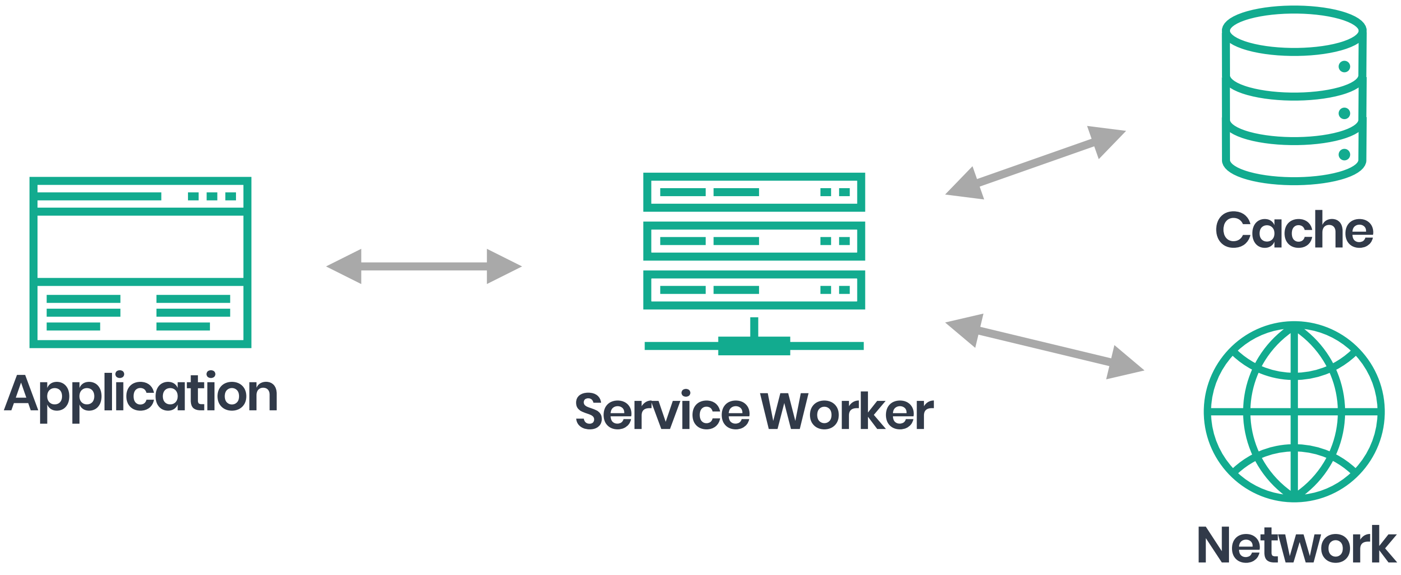
9.5 FORESTING Web App Tech Spec

FORESTING Describes key technologies and systems for building a Frontend / Backend that constitutes a major component of social media services. It will be optimized for the web and mobile, maximize user UX and provide optimized interoperability with the core blockchain technology of FORESTING.

9.5.1 Front-end Framework

9.5.1.1 PWA(Progressive Web Apps)

A new way to deliver a positive user experience on the web.



Building a high-quality Progressive Web App has incredible benefits, making it easy to enhance the user experience, promote engagement and increase conversions.

<u>Worthy of being on the home screen</u>

When the Progressive Web App criteria are met, Chrome prompts users to add the Progressive Web App to their home screen.

<u>Work reliably, no matter the network conditions</u>

Service workers enabled Konga to send 63% less data for initial page loads, and 84% less data to complete the first transaction.

<u>Increased engagement</u>

Web push notifications helped eXtra Electronics increase engagement by 400%. It's those users who spend twice as much time on the site.

<u>Improved conversions</u>

The ability to deliver an amazing user experience helped AliExpress improve conversions for new users across all browsers by 104% and by 82% on iOS.

Source: https://whatwebcando.today/

9.5.1.2 Vue.js

https://vuejs.org/

The Progressive JavaScript Framework

Vue is a progressive framework for building user interfaces. Unlike other monolithic frameworks, Vue is designed from the ground up to be incrementally adoptable. The core library is focused on the view layer only, and is easy to pick up and integrate with other libraries or existing projects. As well as this, Vue is also perfectly capable of powering sophisticated Single-Page Applications when used in combination with modern tooling and supporting libraries.

In 2017, Vue.js received 40.0k stars, making it the #1 most popular JavaScript project on GitHub.

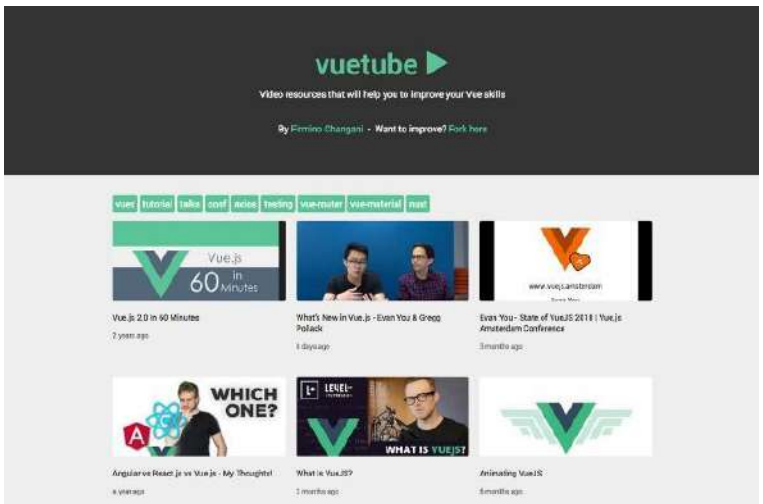
So, what makes Vue.js special?

Firstly, it is intuitive to use, with a component approach like React, but with a more familiar syntax.

The ecosystem is well defined, including a set of de-facto standards: router: vue-router, state management library: Vuex

It uses the concept of a single-file component that includes template, logic and styles in a single file. This is one of the main benefits of using a .vue file.

It's used by one of the most popular PHP frameworks, Laravel, as its default view engine.


vuetube

Video resources that will help you to improve your Vue skills

By Fermino Changani - Want to improve? Fork here

Vue.js 2.0 in 60 Minutes
2 years ago

What's New in Vue.js - Evan You & Gregg Pollack
1 days ago

Evan You - State of VueJS 2018 | Vue.js Amsterdam Conference
3 months ago

Angular vs React.js vs Vue.js - My Thoughts!
a year ago

What is Vue.JS?
1 months ago

Animating VueJS
5 months ago

9.5.2 Front-end Echosystem

9.5.2.1 Vuex

https://vuex.vuejs.org/

Vuex is a state management pattern + library for Vue.js applications. It serves as a centralized store for all the components in an application, with rules ensuring that the state can only be mutated in a predictable fashion. It also integrates with Vue's official devtools extension to provide advanced features such as zero-config time-travel debugging and state snapshot export / import.

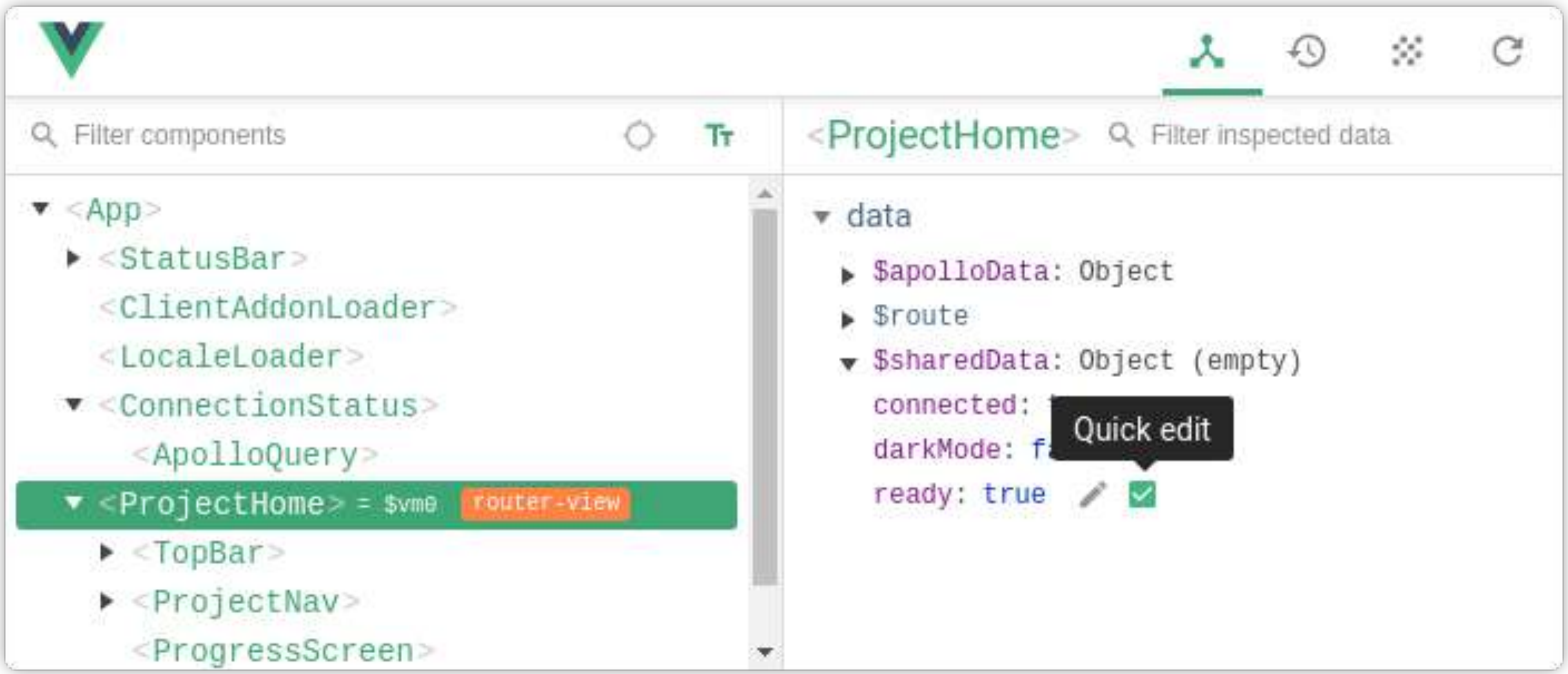
Vue.js devtools

https://github.com/vuejs/vue-devtools

Browser devtools extension for debugging Vue.js applications.

Live edit component data lets you debug faster without going back to IDE and edit the seed data.

Debug Vuex with Time Travel enables you to debug different states.



```
▾ <App>
  ▸ <StatusBar>
    <ClientAddonLoader>
    <LocaleLoader>
  ▾ <ConnectionStatus>
      <ApolloQuery>
  ▾ <ProjectHome> = $vm0  router-view
    ▸ <TopBar>
    ▸ <ProjectNav>
      <ProgressScreen>
```

```
▾ data
  ▸ $apolloData: Object
  ▸ $route
  ▾ $sharedData: Object (empty)
    connected:
    darkMode: f
    ready: true
```

9.5.2.2 Vue Router

https://router.vuejs.org/

Vue Router is the official router for Vue.js. It is deeply integrated with Vue.js core to make building Single Page Applications with Vue.js simple.

9.5.2.3 Axios

https://github.com/axios/axios

The Axios library is the most used HTTP client.

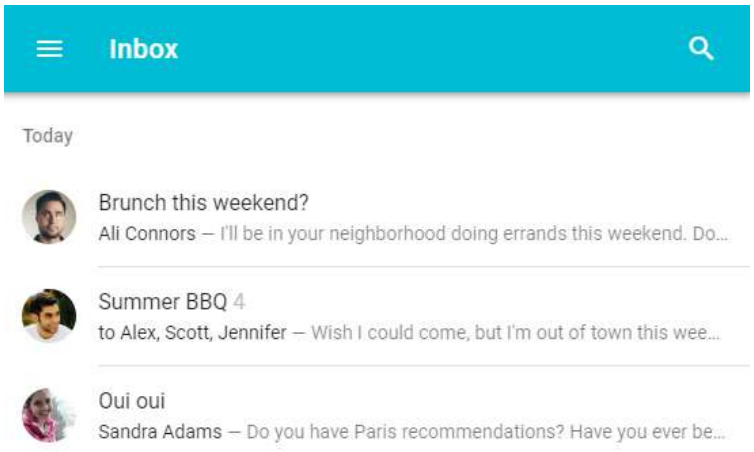
It can work on both the client side (AJAX requests from the client) or on the server-side (HTTP requests in a Node.js environment)

Its success may be related to Vue.js too, because a lot of Vue.js tutorials use it to query a distant API through HTTP.

9.5.2.4 Vuetify

https://vuetifyjs.com/en/

Vuetify is developed exactly according to Material Design spec. Every component has been designed to bring the strongest UI tools to an app.

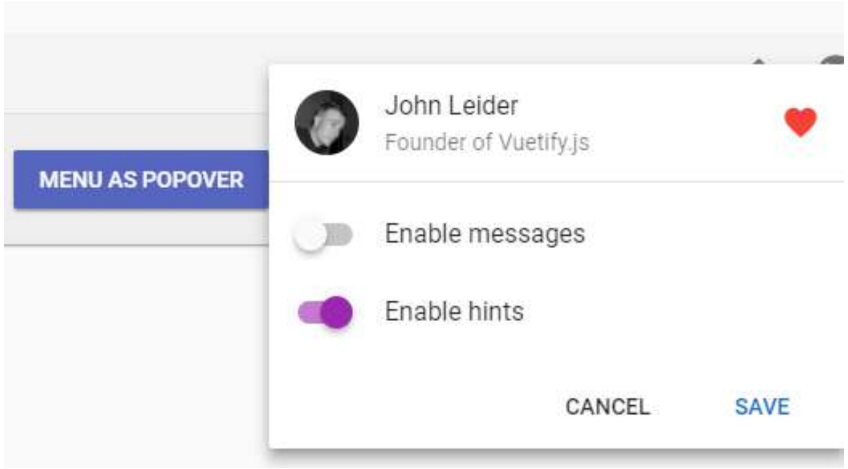


Today

Brunch this weekend?
Ali Connors – I'll be in your neighborhood doing errands this weekend. Do...

Summer BBQ 4
to Alex, Scott, Jennifer – Wish I could come, but I'm out of town this wee...

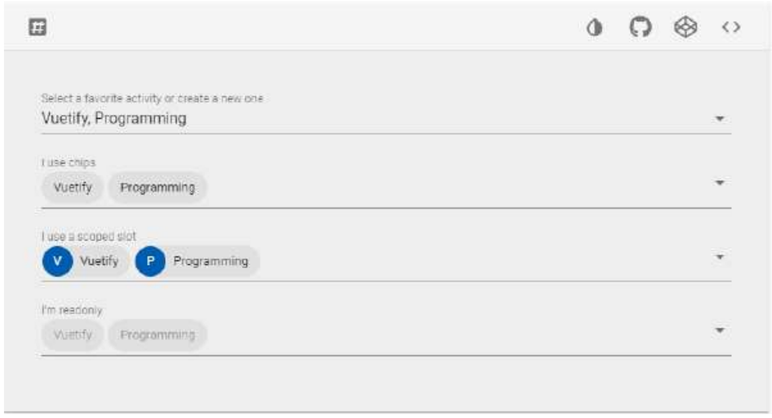
Oui oui
Sandra Adams – Do you have Paris recommendations? Have you ever be...



John Leider
Founder of Vuetify.js

Enable messages

Enable hints

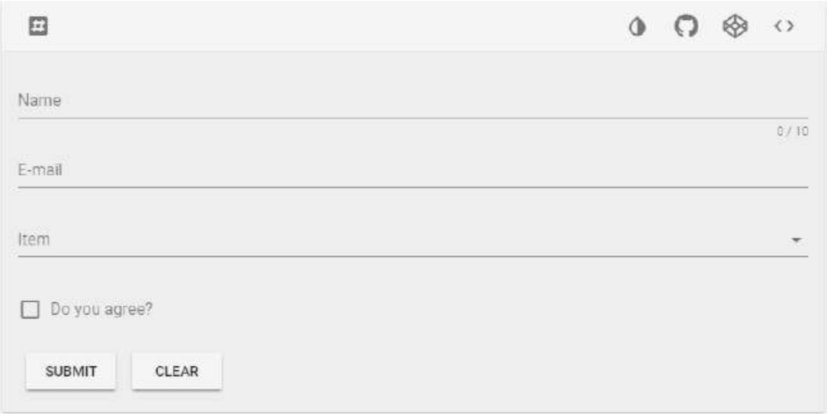


Select a favorite activity or create a new one
Vuetify, Programming

I use chips
Vuetify Programming

I use a scoped slot
V Vuetify P Programming

I'm readonly
Vuetify Programming



Name
0 / 10

E-mail

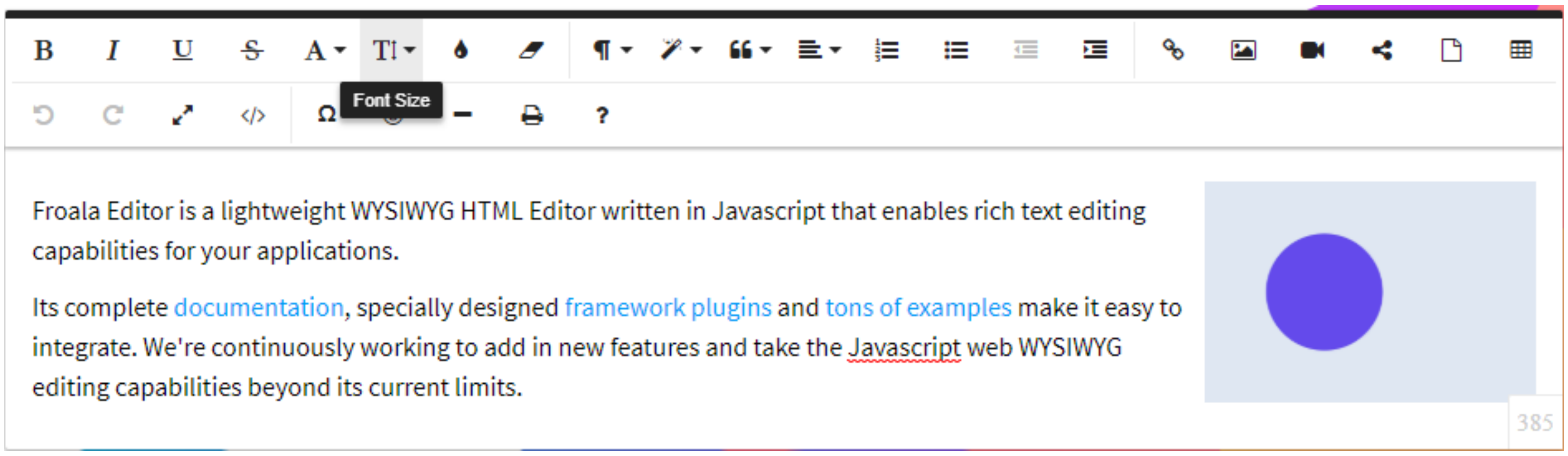
Item

□ Do you agree?

9.5.3 WYSIWYG Editor

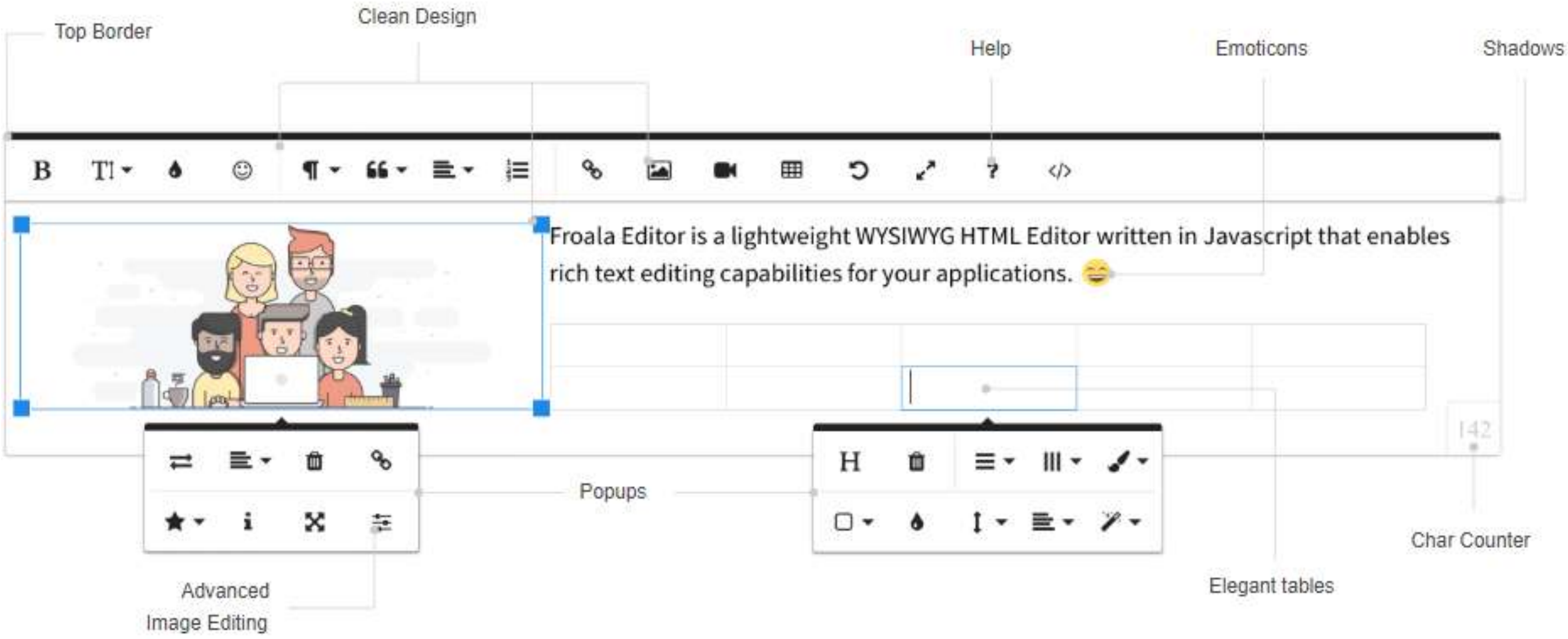
9.5.3.1 Froala

https://www.froala.com/
Javascript web editor that's easy to integrate for developers with an eye-catching and clean design.
Froala Editor will be FORESTING's main editor that will bring whole capability of posting, editing and consuming.
With Its fully customizable WYSIWYG editor, writing and consuming contents will be seamless on almost every form-factor device.



Froala Editor is a lightweight WYSIWYG HTML Editor written in Javascript that enables rich text editing capabilities for your applications.

Its complete documentation, specially designed framework plugins and tons of examples make it easy to integrate. We're continuously working to add in new features and take the Javascript web WYSIWYG editing capabilities beyond its current limits.



Froala Editor is a lightweight WYSIWYG HTML Editor written in Javascript that enables rich text editing capabilities for your applications. 😄

9.5.4 Code formatter

9.5.4.1 Prettier

https://prettier.io/

Prettier formats code to make it cleaner and easy for developers to interpret.

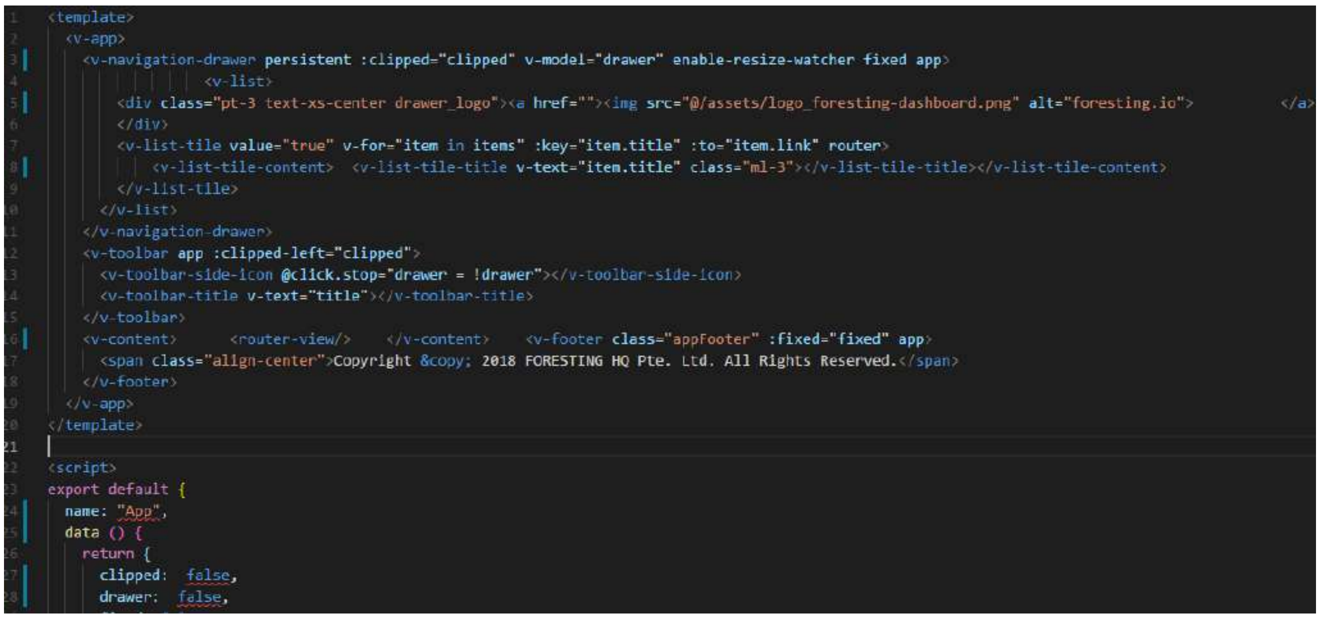
Auto formatting html, javascripts can improve the development experience and code maintenance.

Developers just need to press save to format their code.

There's no need for them to discuss style in code review.

Saves developers time and energy.

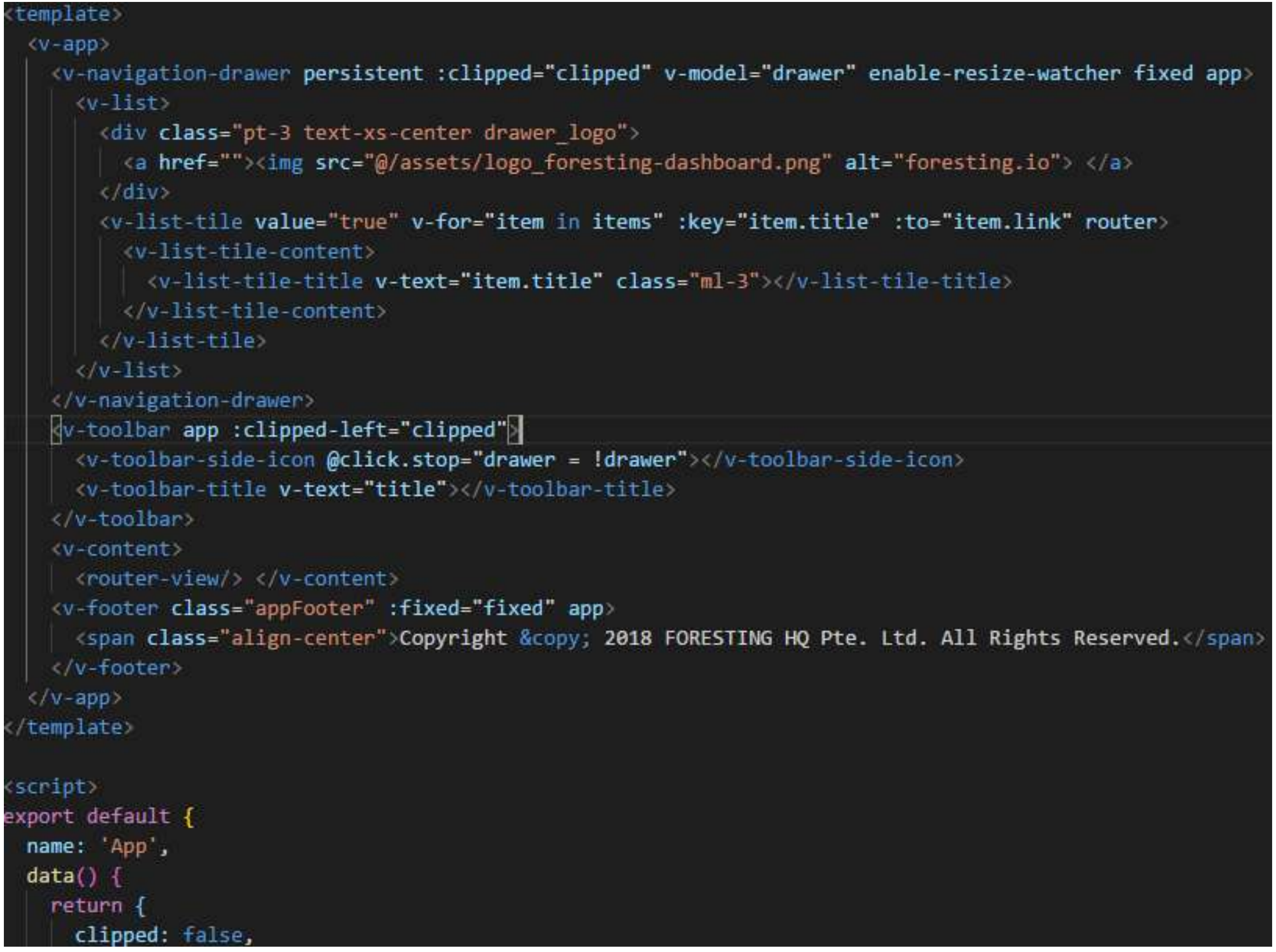
Before formatting



```
<template>
  <v-app>
    <v-navigation-drawer persistent :clipped="clipped" v-model="drawer" enable-resize-watcher fixed app>
                  <v-list>
        <div class="pt-3 text-xs-center drawer_logo"><a href=""><img src="@/assets/logo_foresting-dashboard.png" alt="foresting.io">         </a>
        </div>
        <v-list-tile value="true" v-for="item in items" :key="item.title" :to="item.link" router>
            <v-list-tile-content>  <v-list-tile-title v-text="item.title" class="ml-3"></v-list-tile-title></v-list-tile-content>
        </v-list-tile>
      </v-list>
    </v-navigation-drawer>
    <v-toolbar app :clipped-left="clipped">
      <v-toolbar-side-icon @click.stop="drawer = !drawer"></v-toolbar-side-icon>
      <v-toolbar-title v-text="title"></v-toolbar-title>
    </v-toolbar>
    <v-content>      <router-view/>    </v-content>    <v-footer class="appFooter" :fixed="fixed" app>
      <span class="align-center">Copyright &copy; 2018 FORESTING HQ Pte. Ltd. All Rights Reserved.</span>
    </v-footer>
  </v-app>
</template>

<script>
export default {
  name: "App",
  data () {
    return {
      clipped:  false,
      drawer:  false,
```

After formatting (auto format on save)



```
<template>
  <v-app>
    <v-navigation-drawer persistent :clipped="clipped" v-model="drawer" enable-resize-watcher fixed app>
      <v-list>
        <div class="pt-3 text-xs-center drawer_logo">
          <a href=""><img src="@/assets/logo_foresting-dashboard.png" alt="foresting.io"> </a>
        </div>
        <v-list-tile value="true" v-for="item in items" :key="item.title" :to="item.link" router>
          <v-list-tile-content>
            <v-list-tile-title v-text="item.title" class="ml-3"></v-list-tile-title>
          </v-list-tile-content>
        </v-list-tile>
      </v-list>
    </v-navigation-drawer>
    <v-toolbar app :clipped-left="clipped">
      <v-toolbar-side-icon @click.stop="drawer = !drawer"></v-toolbar-side-icon>
      <v-toolbar-title v-text="title"></v-toolbar-title>
    </v-toolbar>
    <v-content>
      <router-view/> </v-content>
    <v-footer class="appFooter" :fixed="fixed" app>
      <span class="align-center">Copyright &copy; 2018 FORESTING HQ Pte. Ltd. All Rights Reserved.</span>
    </v-footer>
  </v-app>
</template>

<script>
export default {
  name: 'App',
  data() {
    return {
      clipped: false,
```

9.5.5 Compiler

9.5.5.1 Babel

https://babeljs.io/
Babel is a toolchain that is mainly used to convert ECMAScript 2015+ code into a backwards compatible version of JavaScript in old browsers or environments.

9.5.6 Build Tool

9.5.6.1 Webpack

https://webpack.js.org/
At its core, webpack is a static module bundler for modern JavaScript applications. When webpack processes your application, it internally builds a dependency graph which maps every module your project needs and generates one or more bundles.

9.5.7 Testing Frameworks

9.5.7.1 Chai

http://www.chaijs.com/
Chai is a BDD / TDD assertion library for node and the browser that can be delightfully paired with any javascript testing framework.

9.5.7.2 Mocha

https://mochajs.org/
Mocha is a feature-rich JavaScript test framework running on Node.js and in the browser, making asynchronous testing simple and fun. Mocha tests run serially, allowing for flexible and accurate reporting, while mapping uncaught exceptions to the correct test cases. Hosted on GitHub.

9.5.8 Backend Framework

9.5.8.1 ASP.Net Core

https://docs.microsoft.com/en-us/aspnet/core
ASP.NET Core is a cross-platform, high-performance, open-source framework for building modern, cloud-based, Internet-connected applications.
With ASP.NET Core, you can:
- Build web apps and services, IoT apps, and mobile backends.
- Use any development tools on Windows, macOS, and Linux.
Deploy to the cloud or on-premises.
Run on .NET Core or .NET Framework.

9.5.8.2 ASP.Net Web API

Application Programming Interface resembles the online web services that are used by the apps at the client side to retrieve and update information.

9.5.8.3 Data access with EF Core

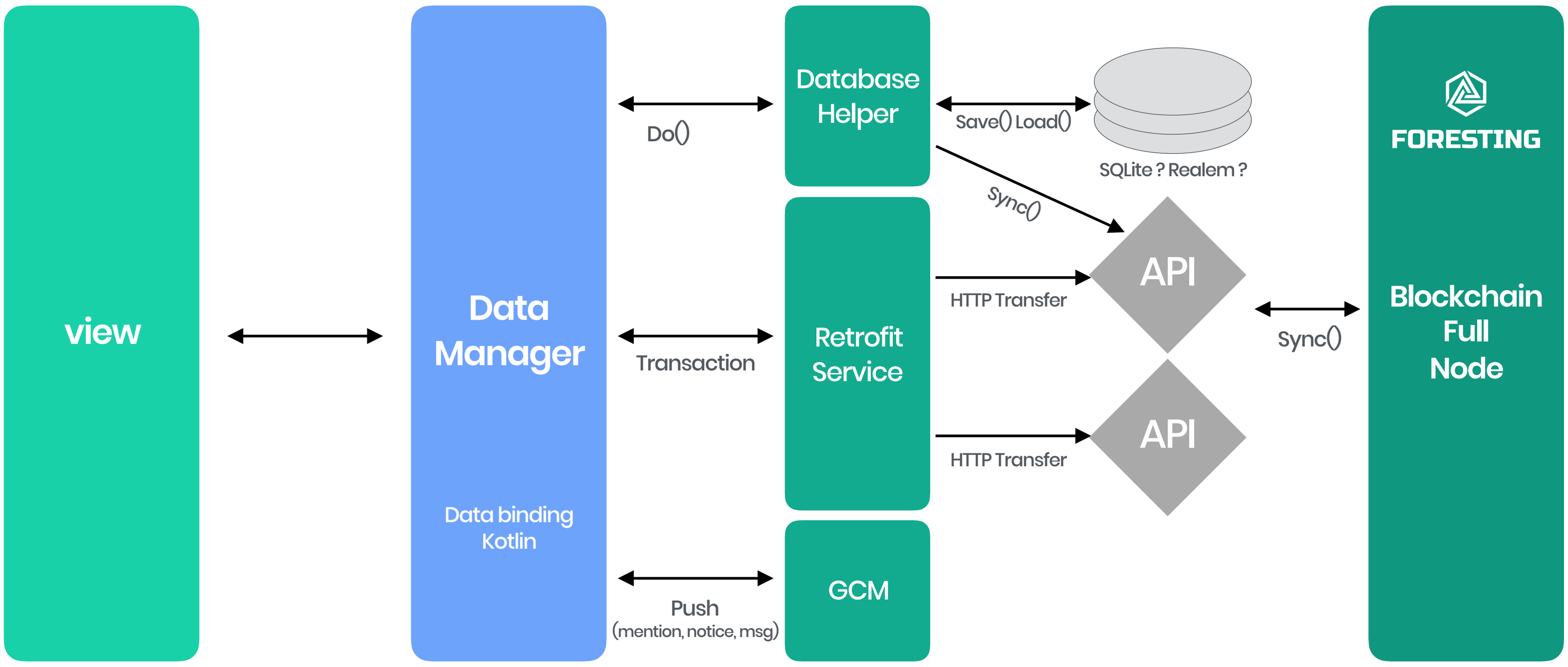
Entity Framework (EF) Core is a lightweight, extensible, and cross-platform version of the popular Entity Framework data access technology.
EF Core can serve as an object-relational mapper (O/RM), enabling .NET developers to work with a database using .NET objects, and eliminating the need for most of the data-access code they usually need to write.
EF Core supports many database engines, see Database Providers for details.

9.6 FORESTING Mobile App Tech Spec

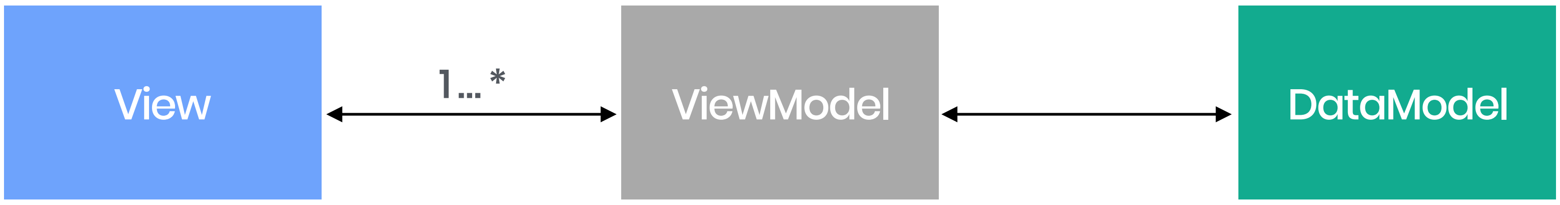
FORESTING for android software is a mobile platform for using the PTON which is used in a FORESTING blockchain network.

NOTICE: The use referred to in this document refers to all situations in which the PTON is utilized (including earning, using, trading, selling, etc.) on the FORESTING system.

9.6.1 MVVM Architecture



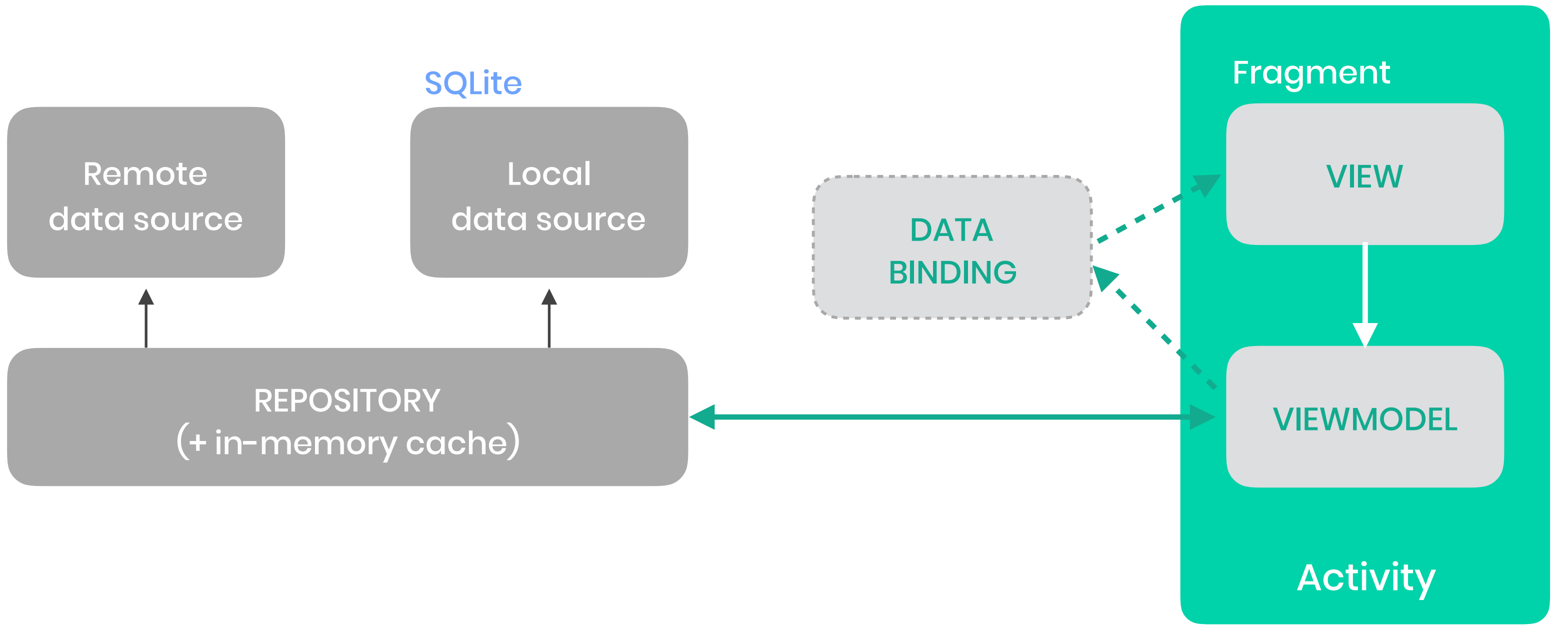
It is based on MVVM (Model - View - ViewModel) architecture. The MVVM architecture is designed to minimize the dependence on views and help make unit testing and modularization easier.



In MVVM, the ViewModel exposes a stream of events so that the view can bind to that stream. The ViewModel does not need to have a View's reference, unlike the Presenter in the MVP architecture. This means that all the interfaces that MVP usually needs will be no longer needed.

Views also tell ViewModel that other actions have occurred. So, the MVVM pattern supports bidirectional data binding between View and ViewModel. The View and ViewModel have a many-to-one relationship. The View will have a reference to the ViewModel, but the ViewModel will have no information about the View. The data consumer needs to know about the data provider, but the data provider (in this case, the ViewModel) does not know or care about who the data consumer is.

Data binding
You can bind events that occur in each view of Android using data binding. This improves code productivity and eliminates the need to manage data separately, allowing you to design applications that can focus on a more robust business logic.
http://gun0912.tistory.com/71
https://developer.android.com/topic/libraries/data-binding/



Kotlin

Developed by IntelliJ IDEA and Android Studio developer JetBrains, Google.io has been designated as Android's official language. It has a concise syntax, can operate in a JVM-based environment, and is 100% interoperable with Java. JVM bytecode is the default, but final compilation is possible using machine language or LLVM using the Kotlin / Native compiler. It can be used to develop Android, Tomcat, JavaScript, Java EE, HTML5, iOS, Raspberry pie and more.

The following link shows Google's example project using Kotlin and Data binding.
https://github.com/googlesamples/android-architecture/tree/todo-mvvm-databinding/

9.6.2 Data Model

All Data used for HTTP transport borrows the JSON-RPC model. All objects are transferred in json format using the Gson library below. Gson (Google + JSON)
https://github.com/google/gson

Gson is a Java library that can be used to convert Java Objects into their JSON representation. It can also be used to convert a JSON string to an equivalent Java object. Gson can work with arbitrary Java objects including pre-existing objects that one does not have the source-code of. There are a few open-source projects that can convert Java objects to JSON. However, most of them require that one place Java annotations in their classes; something that cannot be done by someone who doesn't have access to the source-code. Most also do not fully support the use of Java Generics. Gson considers both of these as very important design goals.

9.6.3 Network Transfer

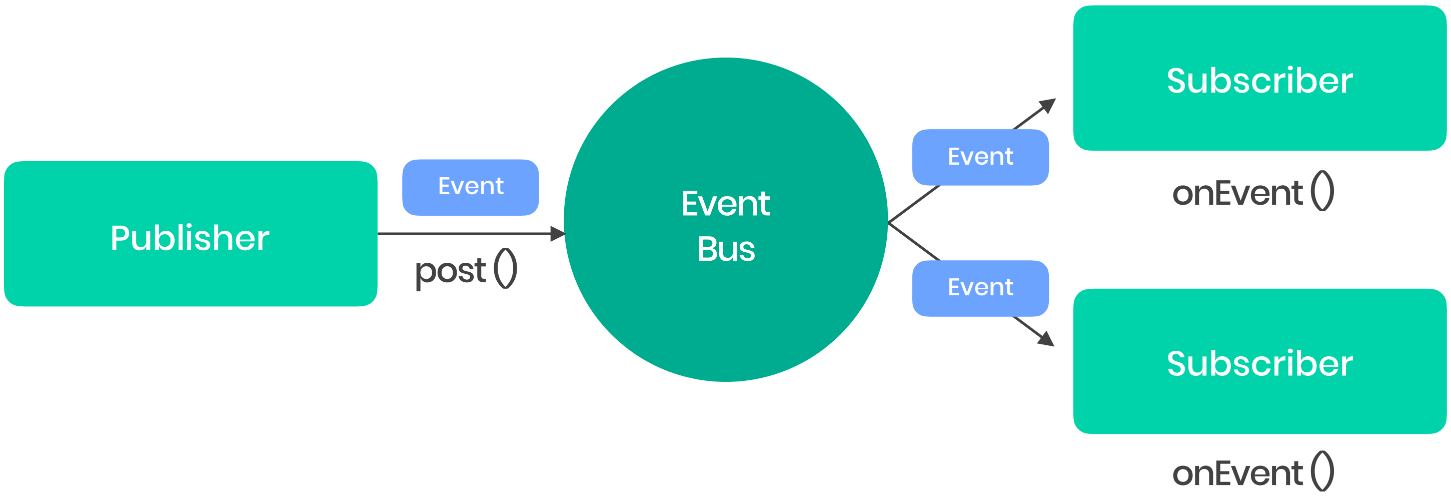
Network transfer communicates HTTP communication using Square Retrofit Library and communicates with API server which is linked with Blockchain Main network. Retrofit Library provides all CURD functions used in Rest API. (POST (create), PUT (update), GET (read), DELETE (delete)

Retrofit is much faster than other HTTP libraries. It provides concise network logic and increases reusability, allowing you to write fast, good quality code.

	One Discussion	Dashboard (7 requests)	25 Discussions
AsyncTask	941ms	4,539ms	13,957ms
Volley	560ms	2,202ms	4,275ms
Retrofit	312ms	889ms	1,059ms

Square Retrofit
A type-safe HTTP client for Android and Java
http://square.github.io/retrofit/

It utilizes a Java library called EventBus to receive events about the subscription / publishing model of the content creator and to notify the user. You can improve the interconnection between the reader and the creator



Event Bus
EventBus is a publish/subscribe event bus for Android and Java.
https://github.com/greenrobot/EventBus

Chapter 10

PTON ISSUANCE

Counting down for important dates and numbers

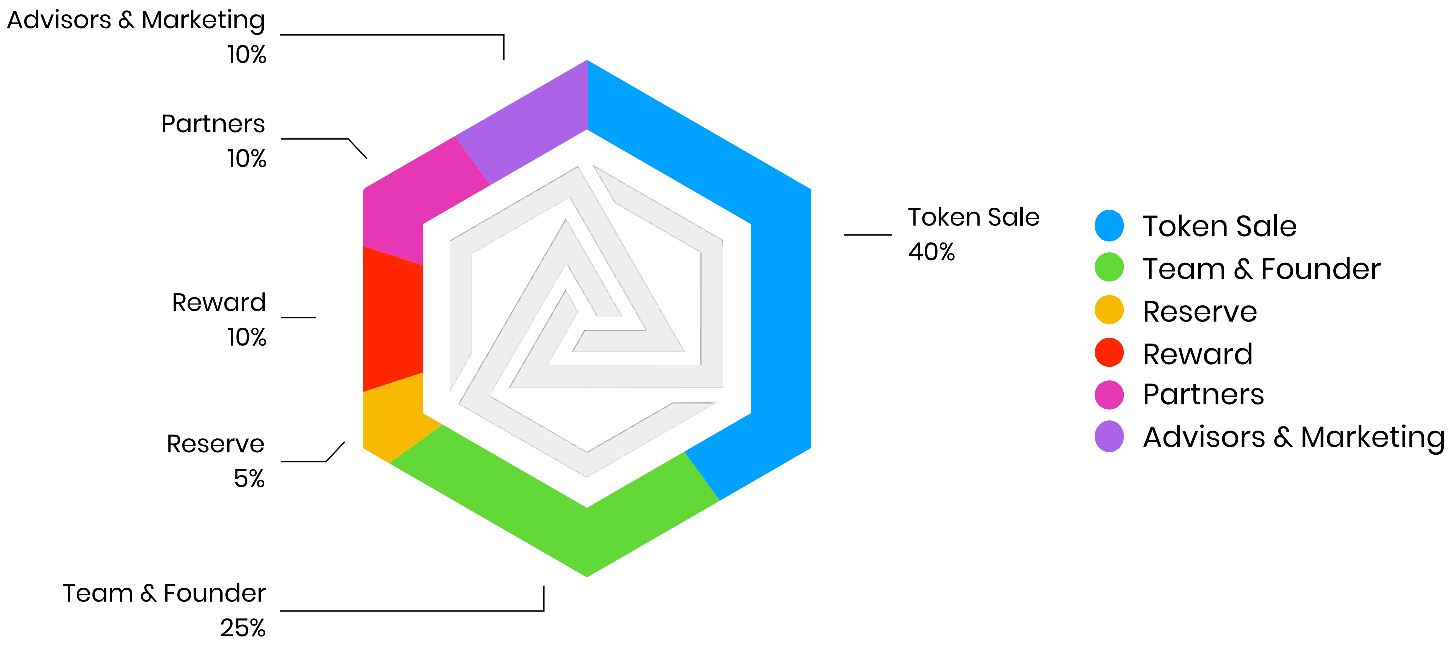
10.1 ICO Planning

The PTON token will be issued as a total of 24,000,000,000 (24 billion) tokens with ERC-20, with 40 % of the total token set for sale. ICO participants may receive the swap through the listed exchange wallet or the FORESTING wallet after the launch of the FORESTING mainnet.

General Information

Total Issuance	**24billion PTON**		
Token name	**PTON**	**Purchase**	**Ether (ETH)**
Base	**Ethereum**	**Pre-initial PTON Token Sale**	**1ETH = 49,999.5 PTON**
Standard	**ERC-20**	**Initial PTON Token Sale**	**1ETH = 33,333 PTON**

Token Distribution



FORESTING

DISCLAIMER

IMPORTANT: YOU MUST READ THE FOLLOWING DISCLAIMER IN FULL BEFORE CONTINUING

The FORESTING Protocol is intended to be maintained by FORESTING HQ Pte. Ltd. and/or its affiliate(s). References in this Whitepaper to FORESTING HQ Pte. Ltd. shall be deemed to include a reference to such affiliate(s).

The sale ("Token Sale") of FORESTING tokens ("Tokens") is only intended for, made for and directed towards, and to be acted upon by only the person(s) (a) who is not a citizen, domiciled, or resident of the United States of America or the People's Republic of China (which for the purpose of these Terms, shall exclude the Hong Kong Special Administrative Region of the People's Republic of China, the Macau Special Administrative Region of the People's Republic of China, and the Republic of China) ("PRC"); and (b) outside the United States of America or PRC.

By accessing and/or accepting possession of any information in this Whitepaper or such part thereof (as the case may be), you represent and warrant to FORESTING Pte. Ltd. (Singapore Company Registration : 201816629Z) ("FORESTING HQ Pte. Ltd.") that:

(a) you are not an Excluded Person (as defined herein), or a citizen or resident of a country in which the token sale (as referred hereto in the Whitepaper) has been prohibited;

(b) you agree to be bound by the limitations and restrictions described herein; and

(c) you acknowledge that this Whitepaper has been prepared for delivery to you so as to assist you in making a decision as to whether to purchase Tokens.

IMPORTANT INFORMATION

PLEASE READ THIS DISCLAIMER SECTION CAREFULLY. IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

This Whitepaper in its current form is circulated by FORESTING HQ Pte. Ltd. for general information and to invite participant feedback only on the FORESTING Protocol (the "FORESTING Protocol") and the Tokens as presently conceived, and is subject to review and revision by the directors and/or advisors of FORESTING HQ Pte. Ltd. Please do not replicate or distribute any part of this Whitepaper without this section in accompaniment. The information set forth below may not be exhaustive and no part of this Whitepaper is intended to create legal relations between a recipient of this Whitepaper or to be legally binding or enforceable by such recipient against FORESTING HQ Pte. Ltd. An updated version of this Whitepaper may be published at a later date and to be announced by FORESTING HQ Pte. Ltd. in due course.

PLEASE READ THIS SECTION AND THE FOLLOWING SECTIONS ENTITLED “DISCLAIMER OF LIABILITY”, “NO REPRESENTATIONS AND WARRANTIES”, “REPRESENTATIONS AND WARRANTIES BY YOU”, “CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS”, “THIRD PARTY INFORMATION AND NO CONSENT OF OTHER PERSONS”, “TERMS USED”, “NO ADVICE”, “NO FURTHER INFORMATION OR UPDATE”, “RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION”, “NO OFFER OF INVESTMENT OR REGISTRATION” AND “RISKS AND UNCERTAINTIES” CAREFULLY.
IF YOU ARE IN ANY DOUBT AS TO THE ACTION YOU SHOULD TAKE, YOU SHOULD CONSULT YOUR LEGAL, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVISOR(S).

While we make every effort to ensure that any material in this Whitepaper is accurate and up to date, such material in no way constitutes the provision of professional advice. Foresting HQ Pte. Ltd. does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency, or completeness of any material contained in this Whitepaper . Participants and potential Token holders should seek appropriate independent professional advice prior to relying on, or entering into any commitment or transaction based on, material published in this Whitepaper , which has been is purely published for reference purposes alone.

The Tokens subject of the Pre-Initial Token Sale and Initial Token Sale are proprietary cryptographic tokens issued and sold by Foresting HQ Pte. Ltd. (“Issuer”). The Token will function as the native universal utility token used in the FORESTING Protocol as the means of value exchange and to power the FORESTING Protocol.

The Tokens are not intended to constitute securities of any form, units in a business trust, units in a collective investment scheme or any other form of regulated investment or investment product in any jurisdiction. This Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities of any form, units in a business trust, units in a collective investment scheme or any other form of regulated investment or investment product, or a solicitation for any form of regulated investment or investment product in any jurisdiction.

No regulatory authority has examined or approved of any of the information set out in this Whitepaper . No such action has been or will be taken by Foresting HQ Pte. Ltd. and/or Issuer to obtain such approval under the laws, regulatory requirements or rules of any jurisdiction. The provision of this Whitepaper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with.

This Whitepaper does not constitute or form part of any opinion on any advice to purchase, sell or otherwise transact with Tokens and the fact of presentation of this Whitepaper shall not form the basis of, or be relied upon in connection with, any contract of investment decision.

THE TOKEN SALE (AS REFERRED TO HEREIN) IS INTENDED FOR, MADE TO OR DIRECTED AT ONLY PERSONS OUTSIDE THE UNITED STATES OF AMERICA OR THE PRC AND MAY BE ACTED UPON ONLY BY PERSONS OUTSIDE THE UNITED STATES OF AMERICA OR THE PRC. ACCORDINGLY, YOU ARE NOT ELIGIBLE AND YOU ARE NOT TO PURCHASE ANY TOKENS IN THE TOKEN SALE IF YOU

ARE:
(A) A CITIZEN, DOMICILED IN, OR RESIDENT OF THE UNITED STATES OF AMERICA OR THE PRC;
(B) LOCATED IN THE UNITED STATES OF AMERICA OR THE PRC AT THE TIME OF YOUR WHITELISTING FOR AND INTENDED PURCHASE OF OR PURCHASE OF TOKENS IN THE TOKEN SALE;
(C) LOCATED IN A JURISDICTION WHERE THE TOKEN SALE IS PROHIBITED, RESTRICTED OR UNAUTHORISED IN ANY FORM OR MANNER WHETHER IN FULL OR IN PART UNDER THE LAWS, REGULATORY REQUIREMENTS OR RULES IN SUCH JURISDICTION; OR
(D) A PERSON WHO IS OTHERWISE PROHIBITED OR INELIGIBLE IN ANY WAY, WHETHER IN FULL OR IN PART, FROM PARTICIPATING IN ANY PART OF THE TRANSACTIONS CONTEMPLATED IN THE TOKEN SALE TERMS (AS DEFINED BELOW),
(COLLECTIVELY, "EXCLUDED PERSONS").

For the purpose of this Whitepaper , to be "Whitelisted" means to be identified to be eligible to participate in the Token Sale by the Issuer, subject to satisfactory know-your-client and anti-money laundering and counter financing of terrorism checks conducted in connection therewith, or such other criteria as may be imposed by the Issuer in connection therewith at its sole and absolute discretion.

No Token should be construed, interpreted, classified or treated as enabling, or according any opportunity to, purchasers to participate in or receive profits, income, or other payments or returns arising from or in connection with the FORESTING Protocol or the Tokens or the proceeds of the Token Sale, or to receive sums paid out of such profits, income, or other payments or returns.

No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of the Tokens, and no cryptocurrency or other form of payment is to be accepted on the basis of this Whitepaper .

Any agreement as between Issuer and you as a purchaser, and in relation to any sale and purchase, of Tokens is to be governed by only a separate document setting out the terms and conditions (the "Token Sale Terms") of such agreement. In the event of any inconsistencies between the Token Sale Terms and this Whitepaper , the former shall prevail.

There are risks and uncertainties associated with Foresting HQ Pte. Ltd., the Issuer and their business and operations, the Tokens, the FORESTING Protocol, and the Token Sale. Please refer to the section entitled "Risks and Disclosures" set out at the end of this Whitepaper .

This Whitepaper , any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of this Whitepaper is prohibited or restricted.

No part of this Whitepaper is to be reproduced, distributed or disseminated without including this section and the following sections entitled “Disclaimer of Liability”, “No Representations and Warranties”, “Representations and Warranties By You”, “Cautionary Note On Forward-Looking Statements”, “Third Party Information and No Consent of Other Persons”, “Terms Used”, “No Advice”, “No Further Information or Update”, “Restrictions On Distribution and Dissemination” and “Risks and Uncertainties”.

DISCLAIMER OF LIABILITY

To the maximum extent permitted by the applicable laws, regulations and rules, Foresting HQ Pte. Ltd. and Issuer shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you.

NO REPRESENTATIONS AND WARRANTIES

Foresting HQ Pte. Ltd. and Issuer does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this Whitepaper .

REPRESENTATIONS AND WARRANTIES BY YOU

By accessing and/or accepting possession of any information in this Whitepaper or such part thereof (as the case may be), you represent and warrant to Foresting HQ Pte. Ltd. as follows:

(a) you agree and acknowledge that the Tokens do not constitute securities of any form, units in a business trust, units in a collective investment scheme or any other form of regulated investment or investment product in any jurisdiction;

(b) you are not an Excluded Person, or a citizen or resident of a country the laws of which prohibit or conflict with the Token Sale or your participation in the Token Sale;

(c) you are not located in a jurisdiction where the Token Sale is prohibited, restricted or unauthorised in any form or manner whether in full or in part under the laws, regulatory requirements or rules in such jurisdiction;

(d) you are not a person who is otherwise prohibited or ineligible in any way, whether in full or in part, from participating in any part of the transactions contemplated in the Token Sale Terms;

(e) you agree and acknowledge that this Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities of any form, units in a business trust, units in a collective investment scheme or any other form of regulated investment or investment product in any jurisdiction, or a solicitation for any form of regulated investment or investment product, and you are not bound to enter into any contract or binding legal commitment
and no cryptocurrency or other form of payment is to be accepted on the basis of this Whitepaper ;

(f) you acknowledge and understand that no Token should be construed, interpreted, classified or treated as enabling, or according any opportunity to, Token holders to participate in or receive profits, income, or other payments or returns arising from or in connection with the Tokens or the proceeds of the Token Sale, or to receive sums paid out of such profits, income, or other payments or returns;

(g) you agree and acknowledge that no regulatory authority has examined or approved of the information set out in this Whitepaper , no action has been or will be taken by Foresting HQ Pte. Ltd. to obtain such approval under the laws, regulatory requirements or rules of any jurisdiction and the publication, distribution or dissemination of this Whitepaper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with;

(h) you agree and acknowledge that this Whitepaper , the undertaking and/or the completion of the Token Sale, or future trading of Tokens on any cryptocurrency exchange, shall not be construed, interpreted or deemed by you as an indication of the merits of Foresting HQ Pte. Ltd., the Tokens, the Token Sale, and the FORESTING Protocol;

(i) The distribution or dissemination of this Whitepaper , any part thereof or any copy thereof, or acceptance of the same by you, is not prohibited or restricted by the applicable laws, regulations or rules in your jurisdiction, and where any restrictions in relation to possession are applicable, you have observed and complied with all such restrictions at your own expense and without liability to Foresting HQ Pte. Ltd.;

(j) you agree and acknowledge that in the case where you wish to purchase any Tokens, Tokens are not to be construed, interpreted, classified or treated as:

(i) any kind of currency other than cryptocurrency;

(ii) debentures, stocks or shares issued by any person or entity;

(iii) rights, options or derivatives in respect of such debentures, stocks or shares;

(iv) rights under a contract for differences or under any other contract the purpose or pretended purpose of which is to secure a profit or avoid a loss;

(v) securities;

(vi) units or derivatives of units in a business trust;

(vii) units in a collective investment scheme; or

(viii) any form of regulated investment or investment product;

(k) you are fully aware of and understand that you are not eligible and you are not to purchase any Tokens if you are an Excluded Person;

(l) you are legally permitted to participate in the Token Sale and all actions contemplated or associated with such purchase, including the holding and use of Tokens;

(m) the amounts that you use to purchase Tokens were not and are not directly or indirectly derived from any activities that contravene the laws and regulations of any jurisdiction, including anti-money laundering laws and regulations;

(n) if you are a natural person, you are of sufficient age and capacity under the applicable laws of the jurisdiction in which you reside and the jurisdiction of which you are a citizen to participate in the Token Sale;

(o) you are not obtaining or using Tokens for any illegal purpose; (p) neither:

(i) yourself;

(ii) any person who is controlling or is controlled by you;

(iii) if you are a privately-held entity, any person who has a beneficial interest in you(relevant only to privately held entities); or

(iv) any person for whom you are acting as an agent or nominee in connection with this Token Sale,

is a senior foreign political figure, or any immediate family member or close associate of a senior foreign political figure.

A “senior foreign political figure” is defined as a senior official in the executive, legislative, administrative, military or judicial branch of a government (whether elected or not), a senior official of a major political party, or a senior executive of a foreign government-owned corporation, and includes any corporation, business or other entity that has been formed by, or for the benefit of, a senior foreign political figure.

“Immediate family” of a senior foreign political figure typically includes such figure’s parents, siblings, spouse, children and in-laws.

A “close associate” of a senior foreign political figure is a person who is widely and publicly known to maintain an unusually close relationship with such senior foreign political figure, and includes a person who is in a position to conduct substantial domestic and international financial transactions on behalf of such senior foreign political figure;

(p) if you are affiliated with a non-U.S. banking institution (“Foreign Bank”), or if you receive deposits from, make payments on behalf of, or handle other financial transactions related to a Foreign Bank, you represent and warrant to Foresting HQ Pte. Ltd. that:

(i) the Foreign Bank has a fixed address, and not solely an electronic address, in a country in which the Foreign Bank is authorised to conduct banking activities;

(ii) the Foreign Bank maintains operating records related to its banking activities;

(iii) the Foreign Bank is subject to inspection by the banking authority that licensed the Foreign Bank to conduct its banking activities; and

(iv) the Foreign Bank does not provide banking services to any other Foreign Bank that does not have a physical presence in any country and that is not a regulated affiliate;

(q) you have a basic degree of understanding of the operation, functionality, usage, storage, transmission mechanisms and other material characteristics of cryptocurrencies, blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology;

(r) you are fully aware and understand that in the case in which you wish to purchase any Tokens, there are risks associated with Foresting HQ Pte. Ltd. and its businesses and operations, the Tokens, the FORESTING Protocol and the Token Sale;

(t) you bear the sole responsibility to determine what tax implications purchasing Tokens may have for you and agree not to hold Foresting HQ Pte. Ltd. or any other person involved in the Token Sale liable for any tax liability associated with or arising therefrom;

(u) you agree and acknowledge that Foresting HQ Pte. Ltd. and/or any person involved in the Token Sale and/or with the creation and distribution of Tokens or the FORESTING Protocol, is not liable for any direct, indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you;

(v) you waive the right to participate in a class action lawsuit or a class wide arbitration against Foresting HQ Pte. Ltd. and/or any person involved in the Token Sale and/or with the creation and distribution of Tokens or the FORESTING Protocol; and

(w) all of the above representations and warranties are true, complete, accurate and non-misleading from the time of your access to and/or acceptance of possession of this Whitepaper or such part thereof (as the case may be).

CAUTIONARY NOTE ON FORWARD-LOOKING STATEMENTS

All statements contained in this Whitepaper , statements made in press releases or in any place accessible by the public and oral statements that may be made by Foresting HQ Pte. Ltd. or its directors, executive officers or employees acting on behalf of Foresting HQ Pte. Ltd. (as the case may be), that are not statements of historical fact, constitute “forward-looking statements”. Some of these statements can be identified by forward-looking terms such as “aim”, “target”, “anticipate”, “believe”, “could”, “estimate”, “expect”, “if”, “intend”, “may”, “plan”, “possible”, “probable”, “project”, “should”, “would”, “will” or other similar terms. However, these terms are not the exclusive means of identifying forward-looking statements. All statements regarding Foresting HQ Pte. Ltd.’s business strategies, plans and prospects and the future prospects of the industry which Foresting HQ Pte. Ltd. is in, are forward-looking statements. These forward-looking statements, which include but are not limited to statements as to Foresting HQ Pte. Ltd.’s prospects, future plans, other expected industry trends and other matters discussed in this Whitepaper regarding Foresting HQ Pte. Ltd. are matters that are not historic facts, but only predictions.

These forward-looking statements involve known and unknown risks, uncertainties and other factors that may cause the actual future results, performance or achievements of Foresting HQ Pte. Ltd. to be materially different from any future results, performance or achievements expected, expressed or implied by such forward-looking statements. These factors include, amongst others:

(a)changes in the political, social, and economic landscape, and the stock or cryptocurrency market conditions, and the regulatory environment in the countries in which Foresting HQ Pte. Ltd. conducts its business and operations;

(b) the risk that Foresting HQ Pte. Ltd. may be unable to execute or implement its business strategies and future plans;

(c) changes in interest rates and exchange rates of fiat currencies and cryptocurrencies;

(d) changes in the anticipated growth strategies and expected internal growth of Foresting HQ Pte. Ltd. and the FORESTING Protocol;

(e) changes in the availability and fees payable to Foresting HQ Pte. Ltd. in connection with its businesses and operations or on the FORESTING Protocol;

(f) changes in the availability and salaries of employees who are required by Foresting HQ Pte. Ltd. to operate their respective businesses and operations;

(g) changes in preferences of users of the FORESTING Protocol;

(h) changes in competitive conditions under which Foresting HQ Pte. Ltd. operates, and the ability of Foresting HQ Pte. Ltd. to compete under such conditions;

(i) changes in the future capital needs of Foresting HQ Pte. Ltd. and the availability of financing and capital to fund such needs;

(j) war or acts of international or domestic terrorism;

(k) occurrences of catastrophic events, natural disasters and acts of God that affect the businesses and/or operations of Foresting HQ Pte. Ltd.;

(l) other factors beyond the control of Foresting HQ Pte. Ltd.; and

(m) any risk and uncertainties associated with Foresting HQ Pte. Ltd. and its business and operations, the Tokens, the FORESTING Protocol and the Token Sale.

All forward-looking statements made by or which are attributable to Foresting HQ Pte. Ltd. or persons acting on behalf of Foresting HQ Pte. Ltd. are expressly qualified in their entirety by such factors. Given that risks and uncertainties that may cause the actual future results, performance or achievements of Foresting HQ Pte. Ltd. could be materially different from what has been expected, expressed or implied by the forward-looking statements in this Whitepaper , undue reliance must not be placed on these statements. These forward-looking statements are applicable only as of the date of this Whitepaper .

Neither Foresting HQ Pte. Ltd. nor any other person represents, warrants, and/or undertakes that the actual future results, performance or achievements of Foresting HQ Pte. Ltd. will be as discussed in those forward-looking statements. The actual results, performance or achievements of Foresting HQ Pte. Ltd. may differ materially from those anticipated in these forward-looking statements.

Nothing contained in this Whitepaper is or may be relied upon as a promise, representation or undertaking as to the future performance or policies of Foresting HQ Pte. Ltd.

Further, Foresting HQ Pte. Ltd. disclaims any responsibility to update any of those forward-looking statements or publicly announce any revisions to those forward-looking statements to reflect future developments, events or circumstances, even if new information becomes available or other events occur in the future.

THIRD PARTY INFORMATION AND NO CONSENT OF OTHER PERSONS

This Whitepaper includes information obtained from various third party sources (“Third Party Information”). None of the publishers of the Third Party Information has consented to the inclusion of the Third Party Information in this Whitepaper and is therefore not liable for the Third Party Information. While Foresting HQ Pte. Ltd. has taken reasonable action to ensure that the Third Party Information have been included in their proper form and context, neither Foresting HQ Pte. Ltd., nor its directors, executive officers and employees acting on its behalf, has independently verified the accuracy, reliability, completeness of the contents, or ascertained any applicable underlying assumption, of the relevant Third Party Information. Consequently, neither Foresting HQ Pte. Ltd. nor its directors, executive officers and employees acting on their behalf makes any representation or warranty as to the accuracy, reliability or completeness of such information and shall not be obliged to provide any updates on the same.

TERMS USED

To facilitate a better understanding of the Tokens being offered for purchase by Foresting HQ Pte. Ltd., and the businesses and operations of Foresting HQ Pte. Ltd., certain technical terms and abbreviations, as well as, in certain instances, their descriptions, have been used in this Whitepaper . These descriptions and assigned meanings should not be treated as being definitive of their meanings and may not correspond to standard industry meanings or usage.

Words importing the singular shall, where applicable, include the plural and vice versa and words importing the masculine gender shall, where applicable, include the feminine and neutral genders and vice versa. References to persons shall include corporations.

NO ADVICE

No information in this Whitepaper should be considered to be business, legal, financial or tax advice regarding Foresting HQ Pte. Ltd., the Tokens, the FORESTING Protocol, or the Token Sale. You should consult your own legal, financial, tax or other professional advisor regarding Foresting HQ Pte. Ltd. and its business and operations, the Tokens, the FORESTING Protocol, and the Token Sale. You should be aware that you may be required to bear the financial risk of any exchange of Tokens for an indefinite period of time.

None of the advisors engaged by us has made or purports to make any statement in this Whitepaper or any statement upon which a statement in this Whitepaper is based and each of them makes no representation regarding any statement in this Whitepaper and to the maximum extent permitted by law, expressly disclaims and takes no responsibility for any liability to any person which is based on, or arises out of, any statement, information or opinions in, or omission from, this Whitepaper .

NO FURTHER INFORMATION OR UPDATE

No person has been or is authorised to give any information or representation not contained in this Whitepaper in connection with Foresting HQ Pte. Ltd. and its business and operations, the Tokens, the FORESTING Protocol, or the Token Sale and, if given, such information or representation must not be relied upon as having been authorised by or on behalf of Foresting HQ Pte. Ltd.. The Token Sale shall not, under any circumstances, constitute a continuing representation or create any suggestion or implication that there has been no change, or development reasonably likely to involve a material change in the affairs, conditions and prospects of Foresting HQ Pte. Ltd. or in any statement of fact or information contained in this Whitepaper since the date hereof.

RESTRICTIONS ON DISTRIBUTION AND DISSEMINATION

The distribution or dissemination of this Whitepaper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this Whitepaper or such part thereof (as the case may be) at your own expense and without liability to Foresting HQ Pte. Ltd.

Persons to whom a copy of this Whitepaper has been distributed or disseminated, provided access to or who otherwise have the Whitepaper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this Whitepaper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur.

NO OFFER OF INVESTMENT OR REGISTRATION

This Whitepaper does not constitute a prospectus or offer document of any sort and is not intended to constitute an offer of securities of any form, units in a business trust, units in a collective investment scheme or any other form of investment, or a solicitation for any form of investment in any jurisdiction. No person is bound to enter into any contract or binding legal commitment and no cryptocurrency or other form of payment is to be accepted on the basis of this Whitepaper.

THE TOKEN SALE (AS REFERRED TO HEREIN) IS INTENDED FOR, MADE TO OR DIRECTED AT ONLY PERSONS WHO ARE NOT EXCLUDED PERSONS

No regulatory authority has examined or approved of any of the information set out in this Whitepaper . No such action has been or will be taken under the laws, regulatory requirements or rules of any jurisdiction. The publication, distribution or dissemination of this Whitepaper does not imply that the applicable laws, regulatory requirements or rules have been complied with.

RISKS AND UNCERTAINTIES

Prospective purchasers of Tokens should carefully consider and evaluate all risks and uncertainties associated with the Issuer and Foresting HQ Pte. Ltd., and their business and operations, the Tokens, the FORESTING Protocol, and the Token Sale, and all information set out in this Whitepaper and the Token Sale Terms prior to any purchase of the Tokens. If any of such risks and uncertainties develops into actual events, the business, financial condition, results of operations and prospects of the Issuer could be materially and adversely affected. In such cases, you may lose all or part of the value of the Tokens.

Please read the following risks and warnings before deciding to purchase Tokens. It should be noted the following list of risks and warnings is not exhaustive. Accordingly, prospective purchasers should not place undue reliance on these statements.

1.

RISKS RELATING TO PARTICIPATION IN THE TOKEN SALE

The Issuer may be forced to cease operations

It is possible that, due to any number of reasons, including, but not limited to, an unfavorable fluctuation in the value of cryptographic and fiat currencies, the inability of the Issuer to establish the Project or the Token's utility, the failure of commercial relationships, or intellectual property ownership challenges, the Issuer may no longer be viable to operate and the Issuer may dissolve or take actions that result in a dissolution of the Issuer.

There is no prior market for the Tokens and the Token Sale may not result in an active or liquid market for the Tokens

Prior to the Token Sale, there has been no public market for the Tokens. In the event that the Tokens are traded on a cryptocurrency exchange, there is no assurance that an active or liquid trading market for the Tokens will develop or if developed, be sustained after the Tokens have been made available for trading on such cryptocurrency exchange. There is also no assurance that the market price of the Tokens will not decline below the purchase price of the Tokens (the "Purchase Price"). The Purchase Price may not be indicative of the market price of the Tokens after they have been made available for trading on a cryptocurrency exchange.

A Token is not a currency issued by any central bank or national, supra-national or quasi-national organisation, nor is it backed by any hard assets or other credit. The Issuer is not responsible for nor does it pursue the circulation and trading of Tokens on the market. Trading of Tokens merely depends on the consensus on its value between the relevant market participants, and no one is obliged to purchase any Token from any holder of the Token, including the purchasers, nor does anyone guarantee the liquidity or market price of Tokens to any extent at any time. Accordingly, the Issuer cannot ensure that there will be any demand or market for Tokens, or that the Purchase Price is indicative of the market price of Tokens after they have been made available for trading on a cryptocurrency exchange.

Future sales of the Tokens could materially and adversely affect the market price of Tokens
Any future sale of the Tokens (which were not available for sale in the Token Sale) would increase the supply of Tokens in the market and this may result in a downward price pressure on the Token. The sale or distribution of a significant number of Tokens outside of the Token Sale, or the perception that such further sales or issuance may occur, could adversely affect the trading price of the Tokens.

Negative publicity may materially and adversely affect the price of the Tokens
Negative publicity involving the Issuer, the FORESTING Protocol, the Tokens or any of the key personnel of the Issuer may materially and adversely affect the market perception or market price of the Tokens, whether or not such negative publicity is justified.

There is no assurance of any success of the FORESTING Protocol
The value of, and demand for, the Tokens hinges heavily on the performance of the FORESTING Protocol. There is no assurance that the FORESTING Protocol will gain traction after its launch and achieve any commercial success.

The FORESTING Protocol has not been fully developed, finalised and integrated and is subject to further changes, updates and adjustments prior to its launch. Such changes may result in unexpected and unforeseen effects on its projected appeal to users, and hence impact its success.

While the Issuer has made every effort to provide a realistic estimate, there is also no assurance that the cryptocurrencies raised in the Token Sale will be sufficient for the development and integration of the FORESTING Protocol. For the foregoing or any other reason, the development and integration of the FORESTING Protocol may not be completed and there is no assurance that it will be launched at all. As such, distributed Tokens may hold little worth or value, and this would impact its trading price.

If and when the FORESTING Protocol is fully developed, there is no assurance it will be widely adopted or utilised by its target users.

The trading price of the Tokens may fluctuate following the Token Sale
The prices of cryptographic tokens in general tend to be relatively volatile, and can fluctuate significantly over short periods of time. The demand for, and correspondingly the market price of, the Tokens may fluctuate significantly and rapidly in response to, among others, the following factors, some of which are beyond the control of the Issuer:

(a)new technical innovations;

(b) analysts' speculations, recommendations, perceptions or estimates of the Token's market price or the Issuer's financial and business performance;

(c) changes in market valuations and token prices of entities with operations similar to that of the Issuer that may be made available for sale and purchase on the same cryptocurrency exchanges as the Tokens;

(d) announcements by the Issuer of significant events, for example partnerships, sponsorships, new product developments;

(e) fluctuations in market prices and trading volume of cryptocurrencies on cryptocurrency exchanges;

(f) additions or departures of key personnel of the Issuer;

(g) success or failure of the Issuer's management in implementing business and growth strategies; and

(h) changes in conditions affecting the blockchain or financial technology industry, the general economic conditions or market sentiments, or other events or factors.

The funds raised in the Token Sale are exposed to risks of theft

The Issuer will make every effort to ensure that the funds received from the Token Sale will be securely held at such address as directed by the Issuer ("Receiving Address"). Further, upon receipt of the funds, the Issuer will make every effort to ensure that the funds received will be securely held through the implementation of security measures. Notwithstanding such security measures, there is no assurance that there will be no theft of the cryptocurrencies as a result of hacks, mining attacks (including but not limited to double-spend attacks, majority mining power attacks and "selfish-mining" attacks), sophisticated cyber-attacks, distributed denials of service or errors, vulnerabilities or defects on the Receiving Address, the FORESTING blockchain, or any other blockchain, or otherwise. Such events may include, for example, flaws in programming or source code leading to exploitation or abuse thereof. In such an event, even if the Token Sale is completed, the Issuer may not be able to receive the cryptocurrencies raised and the Issuer may not be able to utilise such funds for the development of the FORESTING Protocol, and the launch of the FORESTING Protocol might be temporarily or permanently curtailed. As such, the issued Tokens may hold little worth or value, and this would impact its trading price. The Tokens are uninsured, unless you specifically obtain private insurance to insure them. In the event of any loss or loss of value, you may have no recourse.

2. RISKS RELATING TO THE RECEIVING ADDRESS AND WALLETS

The Receiving Address may be compromised and the cryptocurrencies may not be able to be disbursed

The Receiving Address is designed to be secure. However, in the event that the Receiving Address is, for any reason compromised (including but not limited to scenarios of the loss of keys to such Receiving Address), the funds held by the Receiving Address may not be able to be retrieved and disbursed, and may be permanently unrecoverable. In such an event, even if the Token Sale is successful, the Issuer will not be able to receive the funds raised and the Issuer will not be able to utilise such funds for the development of the FORESTING Protocol, and the implementation of the FORESTING Protocol might be temporarily or permanently curtailed. As such, distributed Tokens may hold little worth or value, and this would impact its trading price.

The loss or compromise of information relating to your wallet may affect your access and possession of the Tokens

Your access to the Tokens in a cryptocurrency wallet ("Wallet") depends on, among other things, the safeguards to the information to such Wallet, including but not limited to the user account information, address, private key, and password. In the event that any of the foregoing is lost or compromised, your access to the Wallet may be curtailed and thereby adversely affecting your access and possession to the Tokens, including such Tokens being unrecoverable and permanently lost.

The Wallet or Wallet service provider may not be technically compatible with the Tokens.

If Wallet or Wallet service provider may not be technically compatible with the Tokens, this may result in the delivery of Tokens being unsuccessful or affect your access to such Tokens.

3. RISKS RELATING TO Foresting HQ Pte. Ltd.

The FORESTING Protocol is intended to be operated and maintained by Foresting HQ Pte. Ltd.. Any events or circumstances which adversely affect Foresting HQ Pte. Ltd. may have a corresponding adverse effect on the FORESTING Protocol if such events or circumstances affect Foresting HQ Pte. Ltd.'s ability to maintain the FORESTING Protocol. This would correspondingly have an impact on the trading price of the Tokens.

Foresting HQ Pte. Ltd. may be materially and adversely affected if it fails to effectively manage its operations as its business develops and evolves, which would have a direct impact on its ability to maintain the FORESTING Protocol and consequently the trading price of the Tokens.

The financial technology and cryptocurrency industries, and the markets in which Foresting HQ Pte. Ltd. competes, have grown rapidly and continue to grow rapidly and evolve in response to new technological advances, changing business models and other factors. As a result of this constantly changing environment, Foresting HQ Pte. Ltd. may face operational difficulties in adjusting to the changes, and the sustainability of Foresting HQ Pte. Ltd. will depend on its ability to manage its operations, adapt to technological advances and market trends and ensure that it hires qualified and competent employees, and provide proper training for its personnel.

As its business evolves, Foresting HQ Pte. Ltd. must also expand and adapt its operational infrastructure. Foresting HQ Pte. Ltd.'s business relies on its blockchain-based software systems, cryptocurrency wallets or other related token storage mechanisms, blockchain technology and smart contract technology, and to manage technical support infrastructure for the FORESTING Protocol effectively, Foresting HQ Pte. Ltd. will need to continue to upgrade and improve its data systems and other operational systems, procedures and controls. These upgrades and improvements will require a dedication of resources, which are likely to be complex and increasingly rely on hosted computer services from third parties that Foresting HQ Pte. Ltd. does not control. If Foresting HQ Pte. Ltd. is unable to adapt its systems and organization in a timely, efficient and cost-effective manner to accommodate changing circumstances, its business, financial condition and results of operations may be adversely affected. If the third parties whom Foresting HQ Pte. Ltd. relies on are subject to a security breach or otherwise suffer disruptions that impact the services Foresting HQ Pte. Ltd. utilises, the integrity and availability of its internal information could be compromised, which may consequently cause the loss of confidential or proprietary information, and economic loss.

The loss of financial, labor or other resources, and any other adverse effect on Foresting HQ Pte. Ltd.'s business, financial condition and operations, would have a direct adverse effect on Foresting HQ Pte. Ltd.'s ability to maintain the FORESTING Protocol. As the FORESTING Protocol is the main product to which the Tokens relate, this may adversely impact the trading price of the Tokens.

There may be weaknesses, vulnerabilities or bugs in the FORESTING smart contract
Foresting HQ Pte. Ltd. will make reasonable efforts to ensure that the smart contracts underlying the Tokens are audited, tested and approved by technical experts. However, as smart contract technology is still in its early stage of development and its application of experimental nature carries significant operational, technological, financial, regulatory and reputational risks, there are inherent risks that such smart contracts could contain weaknesses, vulnerabilities or bugs.
Purchasers of Tokens should understand and accept that there are no warranties that Tokens are fit for a particular purpose or do not contain any weaknesses, vulnerabilities or bugs which would cause a loss in their worth or value. In the event that any of the aforementioned risks materialises, Foresting HQ Pte. Ltd.'s business strategies, results of operations and prospects may also be adversely affected.

Foresting HQ Pte. Ltd. may experience system failures, unplanned interruptions in its network or services, hardware or software defects, security breaches or other causes that could adversely affect Foresting HQ Pte. Ltd.'s infrastructure network, and/or the FORESTING Protocol
Foresting HQ Pte. Ltd. is unable to anticipate when there would be occurrences of hacks, cyber-attacks, mining attacks (including but not limited to double-spend attacks, majority mining power attacks and "selfish-mining" attacks), distributed denials of service or errors, vulnerabilities or defects in the FORESTING Protocol, the Tokens, the Receiving Address, the Wallet or any technology (including but not limited to smart contract technology) on which Foresting HQ Pte. Ltd., the FORESTING Protocol, the Tokens, the Receiving Address that the Wallet relies on, or on the FORESTING blockchain or any other blockchain. Such events may include, for example, flaws in programming or source code leading to exploitation or abuse thereof. Foresting HQ Pte. Ltd. may not be able to detect such hacks, mining attacks (including but not limited to double-spend attacks, majority mining power attacks and "selfish-mining" attacks), cyber-attacks, distributed denials of service errors vulnerabilities or defects in a timely manner, and may not have sufficient resources to efficiently cope with multiple service incidents happening simultaneously or in rapid succession.

Foresting HQ Pte. Ltd.'s network or services, which would include the FORESTING Protocol, could be disrupted by numerous events, including natural disasters, equipment breakdown, network connectivity downtime, power losses, or even intentional disruptions of its services, such as disruptions caused by software viruses or attacks by unauthorised users, some of which are beyond Foresting HQ Pte. Ltd.'s control. Although Foresting HQ Pte. Ltd. has taken steps against malicious attacks on its appliances and its infrastructure, which are critical for the maintenance of the FORESTING Protocol and its other services, there can be no assurance that cyber-attacks, such as distributed denials of service, will not be attempted in the future, and that any of Foresting HQ Pte. Ltd.'s enhanced security measures will be effective. Foresting HQ Pte. Ltd. may be prone to attacks on its infrastructure intended to steal information about its technology, financial data or user information or take other actions that would be damaging to Foresting HQ Pte. Ltd. and users of the FORESTING Protocol.

We are dependent in part on the location and data center facilities of third parties
Foresting HQ Pte. Ltd.'s infrastructure network is in part established through servers which it owns and houses at the location facilities of third parties, and servers that it rents at data center facilities of third parties. If Foresting HQ Pte. Ltd. is unable to renew its data facility lease on commercially reasonable terms or at all, Foresting HQ Pte. Ltd. may be required to transfer its servers to a new data center facility, and may incur significant costs and possible service interruption in connection with the relocation. These facilities are also vulnerable to damage or interruption from, among others, natural disasters, arson, terrorist attacks, power losses, and telecommunication failures. Additionally, the third party providers of such facilities may suffer a breach of security as a result of third party action, employee error, malfeasance or otherwise, and a third party may obtain unauthorised access to the data in such servers. As techniques used to obtain unauthorised access to, or to sabotage systems change frequently and generally are not recognised until launched against a target, Foresting HQ Pte. Ltd. and the providers of such facilities may be unable to anticipate these techniques or to implement adequate preventive measures. Any such security breaches or damages which occur which impact upon Foresting HQ Pte. Ltd.'s infrastructure network and/or the FORESTING Protocol may adversely impact the price of the Tokens.

General global market and economic conditions may have an adverse impact on Foresting HQ Pte. Ltd.'s operating performance, results of operations and cash flow.

Foresting HQ Pte. Ltd. has been and could continue to be affected by general global economic and market conditions. Challenging economic conditions worldwide have from time to time, contributed, and may continue to contribute, to slowdowns in the information technology industry at large. Weakness in the economy could have a negative effect on Foresting HQ Pte. Ltd.'s business, operational and financial condition, including decreases in revenue and operating cash flow. Additionally, in a down-cycle economic environment, Foresting HQ Pte. Ltd. may experience the negative effects of increased competitive pricing pressure and a slowdown in commerce and usage of the FORESTING Protocol. Suppliers on which Foresting HQ Pte. Ltd. relies for servers, bandwidth, location and other services could also be negatively impacted by economic conditions that, in turn, could have a negative impact on Foresting HQ Pte. Ltd.'s operations or expenses. There can be no assurance, therefore, that current economic conditions or worsening economic conditions or a prolonged or recurring recession will not have a significant adverse impact on Foresting HQ Pte. Ltd.'s business, financial condition and results of operations and hence the FORESTING Protocol, which would correspondingly impact the trading price of the Tokens.

Foresting HQ Pte. Ltd. or the Tokens may be affected by newly implemented regulations.
Cryptocurrency trading is generally unregulated worldwide, but numerous regulatory authorities across jurisdictions have been outspoken about considering the implementation of regulatory regimes which govern cryptocurrency or cryptocurrency markets. Foresting HQ Pte. Ltd. or the Tokens may be affected by newly implemented regulations relating to cryptocurrencies or cryptocurrency markets, including having to take measures to comply with such regulations, or having to deal with queries, notices, requests or enforcement actions by regulatory authorities, which may come at a substantial cost and may also require substantial modifications to the FORESTING Protocol. This may impact the appeal of the FORESTING Protocol for users and result in decreased usage of the FORESTING Protocol. Further, should the costs (financial or otherwise) of complying with such newly implemented regulations exceed a certain threshold, maintaining the FORESTING Protocol may no longer be commercially viable and Foresting HQ Pte. Ltd. may opt to discontinue the FORESTING Protocol and/or the Tokens. Further, it is difficult to predict how or whether governments or regulatory authorities may implement any changes to laws and regulations affecting distributed ledger technology and its applications, including the FORESTING Protocol and the Tokens. Foresting HQ Pte. Ltd. may also have to cease operations in a jurisdiction that makes it illegal to operate in such jurisdiction, or make it commercially unviable or undesirable to obtain the necessary regulatory approval(s) to operate in such jurisdiction. In scenarios such as the foregoing, the trading price of Tokens will be adversely affected or Tokens may cease to be traded.

The regulatory regime governing blockchain technologies, cryptocurrencies, tokens, and token offerings such as the Token Sale, the FORESTING Protocol, and the Tokens is uncertain, and regulations or policies may materially and adversely affect the development of the FORESTING Protocol and the utility of the Tokens
Regulation of tokens (including the Tokens) and token offerings such as the Token Sale, cryptocurrencies, blockchain technologies, and cryptocurrency exchanges currently is undeveloped and likely to rapidly evolve, vary significantly among international, federal, state and local jurisdictions, and is subject to significant uncertainty. Various legislative and executive bodies in Singapore and other countries may in the future, adopt laws, regulations, guidance, or other actions, which may severely impact the development and growth of the FORESTING Protocol and the adoption and utility of the Tokens. Failure by Foresting HQ Pte. Ltd. or users of the FORESTING Protocol to comply with any laws, rules and regulations, some of which may not exist yet or are subject to interpretation and may be subject to change, could result in a variety of adverse consequences, including civil penalties and fines.
Blockchain networks also face an uncertain regulatory landscape in many foreign jurisdictions such as the European Union, the PRC, South Korea, and Russia. Various foreign jurisdictions may, in the near future, adopt laws, regulations or directives that affect the FORESTING Protocol. Such laws, regulations or directives may directly and negatively impact Foresting HQ Pte. Ltd.'s business. The effect of any future regulatory change is impossible to predict, but such change could be substantial and materially adverse to the development and growth of FORESTING Protocol.

Protocol and the adoption and utility of the Tokens.
New or changing laws and regulations or interpretations of existing laws and regulations may materially and adversely impact the value of the currency in which the Tokens may be sold, the value of the distributions that may be made by Foresting HQ Pte. Ltd., the liquidity of the Tokens, the ability to access marketplaces or exchanges on which to trade the Tokens, and the structure, rights and transferability of Tokens.

Tokens holders will have no control on Foresting HQ Pte. Ltd.
The holders of Tokens are not and will not be entitled, to vote or receive dividends or be deemed the holder of capital stock of the issuer for any purpose, nor will anything be construed to confer on the purchaser any of the rights of a stockholder of Foresting HQ Pte. Ltd. or any right to vote for the election of directors or upon any matter submitted to stockholders at any meeting thereof, or to give or withhold consent to any corporate action or to receive notice of meetings, or to receive subscription rights or otherwise.

The purchaser may lack information for monitoring their investment
The purchaser may not be able to obtain all information it would want regarding Foresting HQ Pte. Ltd., the Tokens, or the FORESTING Protocol, on a timely basis or at all. It is possible that the purchaser may not be aware on a timely basis of material adverse changes that have occurred. Information in relation to the development of Tokens may also be highly technical by nature. As a result of these difficulties, as well as other uncertainties, the purchaser may not have accurate or accessible information about the FORESTING Protocol.

There may be risks relating to acts of God, natural disasters, wars, terrorist attacks, riots, civil commotions widespread communicable diseases and other force majeure events beyond the control of Foresting HQ Pte. Ltd.

The Token Sale and the performance of Foresting HQ Pte. Ltd.'s activities may be interrupted, suspended or delayed due to acts of God, natural disasters, wars, terrorist attacks, riots, civil commotions, widespread communicable diseases and other force majeure events beyond the control of Foresting HQ Pte. Ltd.. Such events could also lead to uncertainty in the economic outlook of global markets and there is no assurance that such markets will not be affected, or that recovery from the global financial crisis would continue. In such events, Foresting HQ Pte. Ltd.'s business strategies, results of operations and prospects may be materially and adversely affected. Further, if an outbreak of such infectious or communicable diseases occurs in any of the countries in which Foresting HQ Pte. Ltd., the developers, data providers or data consumers have operations in the future, market sentiment could be adversely affected and this may have a negative impact on the FORESTING Protocol and community.

There may be unanticipated risks arising from the Tokens
Cryptographic tokens such as the Tokens are a relatively new and dynamic technology. In addition to the risks included in this Annex, there are other risks associated with your purchasing, holding and using the Tokens, including those that Foresting HQ Pte. Ltd. cannot anticipate. Such risks may further materialize as unanticipated variations or combinations of the risks discussed hereto.

REFERENCES

[1] https://github.com/bitcoinbook/bitcoinbook Andreas M. Antonopoulos. Mastering Bitcoin. O'Reilly Media, Inc., 2010.

[2] https://forum.ethereum.org/discussion/46/total-supply-of-eth

[3] Sunny King and Scott Nadal. 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. (August 2012). http://peercoin.net/assets/paper/peercoin-paper.pdf.

[4] Jae Kwon. 2014. Tendermint: Consensus without Mining. (2014). http://tendermint.com/docs/tendermint.pdf.

[5] https://www.stellar.org/papers/stellar-consensus-protocol.pdf

[6] https://github.com/input-output-hk/Scorex

[7] https://theethereum.wiki/w/index.php/ERC20_Token_Standard#Sample_Fixed_Supply_Token_Contract

[8] https://github.com/Giveth/minime/blob/master/contracts/MiniMeToken.sol

[9] https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md EOS.IO Technical White Paper v2

[10] Nicolas Gising. Quantum Chance: Nonlocality, Teleportation and Other Quantum Marvels. Copernicus, 2014.

[11] https://ubports.com/ UbuntuTouch: A Mobile Version of the Ubuntu Operating System

[12] david J. Stang and Sylvia Moon, Network Security Secrets, IDG Books Worldwide, Inc., 1993.

[13] S. Bellovin and M. Merritt, "Limitations of the Kerberos Authentication System," Computer Communications Review, October 1997.

[14] Ray Bird et al., "Systematic Design of a Family of Attack Resistant Authentication Protocols," IEEE Journal on Selected Areas in Communications, Vol. 11, No. 5, June 1993.

[15] eric-maxwell-mvc-mvp-and-mvvm-on-android https://academy.realm.io/kr/posts/eric-maxwell-mvc-mvp-and-mvvm-on-android/

[16] gson
https://github.com/google/gson

[17] Retrofit
http://square.github.io/retrofit/

[18] Event Bus
https://github.com/greenrobot/EventBus

[19] Token Curated Registries 1.1, 2.0 TCRs, new theory, and dev updates

https://medium.com/@ilovebagels/token-curated-registries-1-1-2-0-tcrs-new-theory-and-dev-updates-34c9f079f33d

[20] adChain registry smart contracts
https://github.com/AdChain/AdChainRegistry

[21] Learning Solidity Part 2: Commit-Reveal Voting

https://karl.tech/learning-solidity-part-2-voting/

[22] Partial Lock Commit Reveal Voting System that utilizes ERC20 Tokens
https://github.com/ConsenSys/PLCRVoting