



# simplyBrand

Making digital commerce trustworthy through  
blockchain, AI and you

**Whitepaper**

# Table of Contents

<b>Abstract</b>	<b>4</b>
<b>Problem</b>	<b>6</b>
2.1 Global E-commerce Market	7
2.2 The Cost of Counterfeiting	8
2.3 Increasing difficulties of anti-counterfeiting	9
2.3.1 Less barriers for counterfeiters due to the proliferation of E-commerce	9
2.3.2 Increased cost for brands to prove authenticity	10
2.4 Ineffectiveness in Anti-Counterfeiting	11
2.4.1 Measures taken by countries	11
2.4.2 Measures taken by brands	13
2.5 Conclusion	14
<b>Vision</b>	<b>15</b>
<b>Solution</b>	<b>17</b>
4.1 Solution Framework	18
4.2 Roles within the ecosystem	19
4.2.1 Brands	20
4.2.2 Crowdsourced Participants	20
4.2.3 Enforcement agencies	20
4.2.4 Third parties	21
4.3 Mechanism Design	21
4.3.1 Staking Mechanism	21
4.3.2 Crowd Counterfeit Verification Mechanism	22
4.3.3 Crowd Reporting Mechanism	22
4.3.4 Rating Mechanism	23
4.3.5 Blacklist Update Mechanism	24
4.4 Development Phases	24

4.4.1 Introductory Phase	25
4.4.2 Upward Phase	25
4.4.3 Mature Phase	26
4.4.4 Future Phases	27

## **Technology** **29**

5.1 Distributed Data Acquisition System	31
5.2 Product Info Database	31
5.3 AI Classification System	31
5.4 Blockchain	33

## **Token Design** **34**

6.1 Rewarding Mechanism	35
6.1.1 Verification Rewards	35
6.1.2 Rewards from reporting URLs	35
6.1.3 Rewards of reporting fake goods received from online stores	36
6.1.4 Rewards for taking down an URL	36
6.2. Mining Mechanism	36
6.3 Balancing Mechanism	37
6.4 Total Token Reward	38
6.5 Token Flow	38

## **Roadmap** **40**

## **Team** **42**

Kaufman Chang	43
Ronnie Ng	43
Frank Shi	43
Aleen Zhang	43
Ada Yao	44
Rita Yang	44
Hsin-Chi Tsao	44
Oleksandra Zavertailo	44

Thibault Laville	45
<b>Token Sale Plan</b>	<b>46</b>
9.1 Token Design	47
9.2 Token Allocation	47
9.3 Fund allocation	48
<b>Disclaimer</b>	49

# 1 Abstract

Research has shown that counterfeits pose a great threat to individuals, companies, industries and even world governments. With the technological advancement of the internet, the negative effects of counterfeiting have now been magnified and are causing a larger scale of damage. Most brands choose to invest a large amount of money into implementing NFC or RFID technologies into their products, but the results are still limited and the costs are still high.

We will create a solution to this problem by establishing a platform with a built-in AI model and machine learning technology to identify counterfeits. Crowd-sourced participants will be incentivized to assist in verifying the unidentifiable items, while the information of the counterfeiters will be published on the blockchain, which is immutable and public for everybody to read. In addition, two major functions will be released along the way which will result in more parties joining the platform to complete the goal of the platform evolving into a self-governed ecosystem. By combining these cutting-edge technologies with new mechanisms to govern the platform by itself, our solution is able to solve this problem effectively on a large scale.

# 2 Problem

## 2.1

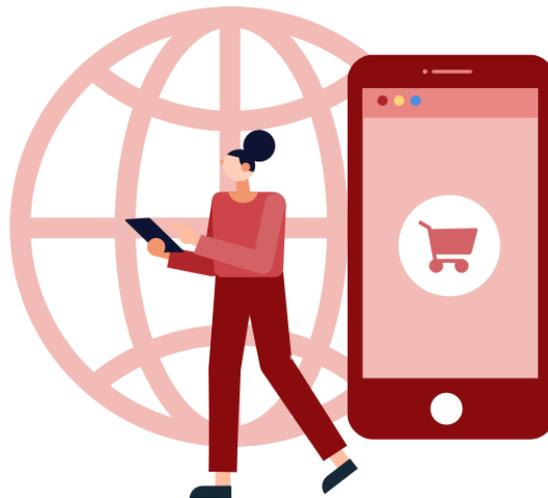
# Global E-commerce Market

Increasingly, consumer purchasing habits are shifting towards making purchases on E-commerce platforms, with eMarketer estimating such purchases will double over the next several years and reach 12% of all global trade by 2019. Compare this to Connected Commerce report which has revealed that in 2016, 57% of consumers worldwide purchased a product online from outside of their country of origin and it begins to paint a picture of an ever-growing global E-commerce landscape.

Purchases on E-commerce platform will reach

# 12%

of all global trade by 2019



Within this new globalized online sales platform are increasing amount of opportunities for counterfeit retailers to reach new, unsuspecting markets, and they are seizing these opportunities faster than anyone can imagine. In 2017 it is estimated that the losses due to online counterfeiting have reached 323 billion USD<sup>1</sup>, making counterfeiting the most profitable illegal industry on the planet. A major source of this counterfeiting problem is China, as EUROPOL and EUIPO estimate that approximately 72% of counterfeits circulating in the top three world economies (EU, USA, and Japan) originated from China. This unrestricted level of Chinese counterfeiting is costing foreign firms to lose over 20 billion USD a year.

---

<sup>1</sup> <https://www.apnews.com/ef15478fa38649b5ba29b434c8e87c94>



Counterfeiting is costing brands over  
**20B USD / year**  
for brands like Nike and Apple

## 2.2

# The Cost of Counterfeiting

The victims of counterfeiting aren't limited to developing countries and markets, but span every corner of the globe. The US Government Accountability Office estimates that in 2018, 79% of US consumers purchased products online, while the New York Times states that over a third of such consumers had unknowingly purchased counterfeit goods from major platforms, such as Amazon and eBay. The product category of counterfeit goods isn't just limited to clothing or electronics, it includes everything imaginable such as cosmetics, pharmaceuticals and even food.

Such counterfeits that we are directly ingesting or applying to our bodies can cause serious harm and even death. In 2015, The City of London Police issued a warning to citizens against buying suspiciously priced cosmetics, especially from China. In 2016 Interpol took down over 3,500 websites selling counterfeit and illicit pharmaceuticals; these counterfeit pharmaceuticals are estimated by the UN to account for 700,000 deaths worldwide per year.

## 2.3

# Increasing difficulties of anti-counterfeiting

Fighting counterfeit goods is becoming increasingly difficult due to the rise of E-commerce platforms, as sellers are often unregulated and able to use deceitful practices to disguise their products. This is complicated by the ease of buying products globally as retailers in developing nations may be subject too little to no regulations or repercussions for selling counterfeit goods. Counterfeiters are also becoming smarter and moving away from traditional E-commerce websites to other platforms, such as social networking sites and messaging apps, where it is easier to disguise oneself and where regulations on individual users are very scarce.

### 2.3.1 Less barriers for counterfeiters due to the proliferation of E-commerce

According to figures from ITU, the number of internet users reached 3.3 billion in 2016, wherein at least half use E-commerce platforms.<sup>2</sup> This is giving counterfeiters previously unparalleled access to consumers around the globe; new markets are becoming increasingly easier to find and to sell too as consumers are constantly looking for lower prices and are thus easier targets to counterfeiters.

The global E-commerce market has been growing at an average annual rate of 25% for the past few years, and the scale of transactions is estimated to surpass 4.8 trillion USD in 2021.<sup>3</sup> At the same time, the users of E-commerce platforms will exceed 2.3 billion, and 29.3% of the global retail industry revenue will be contributed from online stores.<sup>4</sup> This growth in the digital market will benefit counterfeiters as new opportunities arise for them to distribute counterfeit products globally.

---

<sup>2</sup> <https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx>

<sup>3</sup> <https://www.statista.com/statistics/288487/forecast-of-global-b2c-e-commerce-growth/>

<sup>4</sup> <https://www.statista.com/statistics/379046/worldwide-retail-e-commerce-sales/>

## 2.3.2 Increased cost for brands to prove authenticity

According to a report published by Netnames, the global anti-counterfeit track and trace market was worth 57 billion USD in 2013 and will grow to 143 billion USD by 2020. Marking systems, such as barcodes, holograms, and special inks, are poised to become a 35.3 billion USD market by 2018.<sup>5</sup> These industries are very lucrative because they are expensive to implement, and many brands cannot afford to do so for fear of losing their market segment due to increased product prices. Such measures may also damage the consumer image of the brand as they are left wondering if they should purchase certain products if the chance of receiving a counterfeit is so high.

“

The global anti-counterfeit track and trace market was worth 57 billion USD in 2013 and will grow to 143 billion USD by 2020.

- Netnames

”

---

<sup>5</sup> <https://www.netnames.com/assets/shared/whitepaper/pdf/NetNames-Counterfeiting-Report-A4-2015.pdf>

## 2.4

# Ineffectiveness in Anti-Counterfeiting

The damage caused by counterfeits is affecting every aspect of society – from the welfare of individuals like you and me, to companies. The negative impact could even expand to the level of a whole industry, or even a country. Although companies and countries are trying to take measures to prevent this major issue from worsening, results are still very limited.

The ineffectiveness of anti-counterfeiting is a manifold as it spans a variety of industries and government institutions. International customs agencies, especially in less developed nations, do not have the training, want or incentive to deal with the flow of counterfeit products. Monitoring and reporting online channels that sell counterfeits is tough to deal with when such channels exist in places with little regulation and often requires the cooperation of ISP's that may be unwilling or unable to comply with such demands. Brands also often find it troublesome to conduct on the ground investigations into retail channels, especially when local authorities do not wish to cooperate with foreign corporate entities. For MNC's policing the supply chain of their products is not cost effective, just as it is even less profitable to directly monitor individual distribution channels. Anti-counterfeiting initiatives are also greatly stifled by cross-industry information sharing as many companies and agencies are unwilling to admit the extent to which counterfeiting has permeated their industries.

### 2.4.1 Measures taken by countries

According to a report released by the OECD, governments have been actively engaged in expanding efforts to combat counterfeiting in international and national contexts. Governments have been working with each other through trade agreements and multilateral organizations to strengthen IP protection. However, while the efforts have had positive results, counterfeiting and piracy levels still remain high.<sup>6</sup>

---

<sup>6</sup> <https://www.oecd.org/sti/38707619.pdf>

An example of the ineffectiveness of anti-counterfeiting measures can be found in China. Acting as a further example, China is a major source of this problem, as a counterfeiter will only face legal consequences when the sales revenue generated from selling fake products exceeds 50,000 RMB (approx. 7300 USD), and will only be sentenced with a 15-year imprisonment or life-sentence when the revenue exceeded 2 million RMB (approx. 293.200 USD). However, the online shopping complaint analysis shows that over 60% of the complaints are from purchases under 500 RMB, and only 6.64% of the complaints are from purchases over 5000 RMB. As a result, the scope of penalties for over 99% of the infringing acts is highly limited.<sup>7</sup>



According to a report released by the OECD, governments have been actively engaged in expanding efforts to combat counterfeiting in international and national contexts by working together through trade agreements and multilateral efforts to strengthen IP protection. However, as many world governments, from smaller nations to powerhouse economies, see this area as less of a problem, results remain limited.

A major problem within the realm of governmental anti-counterfeiting measures lies within any nations' culture, as authorities in many areas wish to protect counterfeiters within their nation from the legal consequences doled out by a foreign nation or company. Simply, they wish to protect their own and allow such people to continue prospering economically.

---

<sup>7</sup> <https://zhidao.baidu.com/question/416600012.html>

## 2.4.2 Measures taken by brands

In a research conducted by NetNames, a renowned firm in the brand protection field, shows that up to 80% of the products sold on Taobao, one of the biggest E-commerce platform in China, are counterfeit products. In addition, until before June 1, 2015, Weidian, an associate company of Tencent in China, cleared almost 10 million counterfeit products from their platform, but that only amounted to 0.9% of the total products sold on their platform.

Moncler, a luxury brand from Italy, incorporated one of the latest technologies, RFID, into their products. However, efforts to fight counterfeiters like this require companies to invest millions of dollars. Companies may subsequently have no choice but to raise the price of their products to compensate for their losses, which is undesirable for both the companies and their customers. In addition, since this type of technology might involve acquiring personal information from the buyer of the product, it has been rejected in some countries or regions. For example, Burberry has been prohibited from selling in some of the areas of the United States because some of their products are produced with this kind of technology.

While brands and E-commerce platforms have been taking distinct measure to protect themselves from counterfeit products, many of their efforts have fallen short. Not even major platforms with an immense amount of capital are immune from the problem of counterfeiting as is evidenced from Apple's filing suit against Amazon after discovering that up to 90% of listed Apple charging devices were counterfeit.

To combat such expansive counterfeiting brands are turning to methods such as RFID tagging, which is quite expensive and can possibly involve acquiring sensitive personal information from the buyer, which if the product is lost or stolen can lead to such information being revealed to unscrupulous 3<sup>rd</sup> parties. Because of the potential threat to consumers, RFID technology has been banned in certain areas resulting in Burberry being prohibited from selling in certain areas of the United States because of the incorporation of such technologies.

## 2.5

# Conclusion

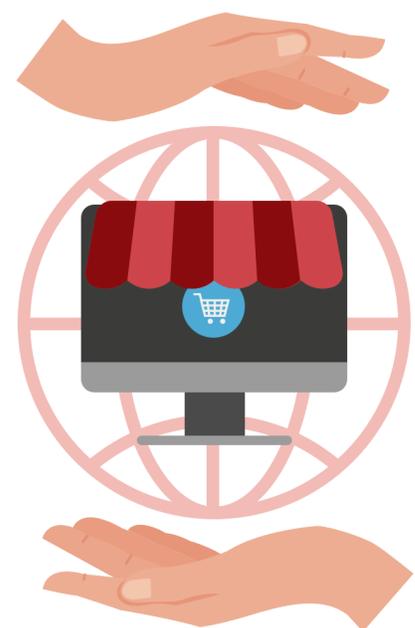
The counterfeit products market has grown rapidly in recent years with the expansion of E-commerce and compounded with the increased use in mobile devices resulting in 7% of world trade being counterfeit products; purchasing goods online is becoming easier than ever, so counterfeiters are able to penetrate multiple global markets. Despite the fact that counterfeiting poses significant threats to individuals, brands, insurers and governments, effective methods have not been undertaken to tackle this issue. As consumers and brands have continued to suffer from counterfeiters, simplyBrand has developed the perfect solution to stop counterfeiting in global E-commerce for good.

# 3 Vision

The world today is rapidly becoming a global stage where people are connected in ways that even several decades previously would have seemed impossible. But with these new modes of life come new threats to our safety and well-being. Counterfeiting, especially within digital commerce, is becoming increasingly common and hard to stop. As digital commerce expands, especially alongside the use of mobile devices, consumer purchasing habits are shifting more and more towards the internet. Brick and mortar stores are no longer the only option for purchasing goods and as globalization continues, so too does the ease of purchasing less expensive products from overseas location. This new form of commerce has allowed for counterfeiters to exploit global digital commerce by expanding their operations and selling inferior products globally, damaging consumers and brands alike around the planet. This threat has moved beyond the bounds of developing nations and is beginning to infect markets around the globe. Even the largest online retailers in America and Europe are not immune to the threat of counterfeit products on their platforms. There is no reason for such a scourge to exist in this day and age; people and their purchases matter, as do brands and their products, which is the core belief of simplyBrand.

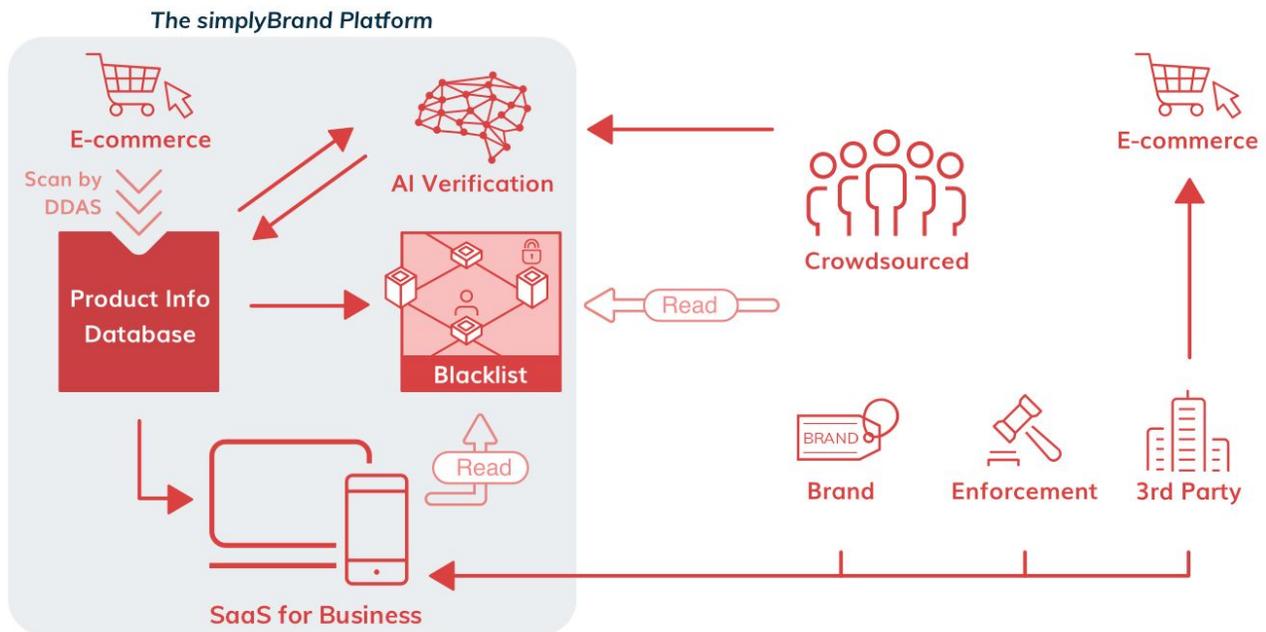
simplyBrand was built to create a new world for digital commerce wherein brands and consumers are protected from the damaging and lethal effects of counterfeit goods. A world where consumers can purchase goods globally without fear of receiving a low quality or harmful product; where brands are able to regain their rightful market shares and no longer have to worry about being tarnished by counterfeit products which have made their way into the hands of loyal consumers. simplyBrand is creating a world of safe and trustworthy digital commerce free from the harm caused by the counterfeiting industry.

For the past several years, simplyBrand has united technology with business to help brands protect themselves and their images. Based in Shanghai and assisting a variety of multinational brands, we have witnessed firsthand the damage that counterfeit products causes to consumers and businesses. This damage extends far beyond simple, low quality goods, but widely effects industries as diverse as aircraft manufacturing and even pharmaceuticals. This is why our experienced tech savvy team of like-minded professionals decided to unite under the shared belief of ridding the threat of dangerous counterfeit goods from digital commerce by using the resources at our disposal, while also combining the latest technologies to develop the best solution possible.



# 4 Solution

simplyBrand is presenting a solution to the problem of rampant counterfeit products which that have flooded global E-commerce by establishing an organic platform which will combine blockchain, AI and crowdsourced participants working together. The ecosystems is detailed in the following:



Brands will use the simplyBrand platform to request brand-protection services, Crowdsourced Participants will directly report counterfeit products, or work with the AI to verify the authenticity of E-commerce products and the Enforcement Agencies will use the platform to access lists of verified counterfeit products.

## 4.1

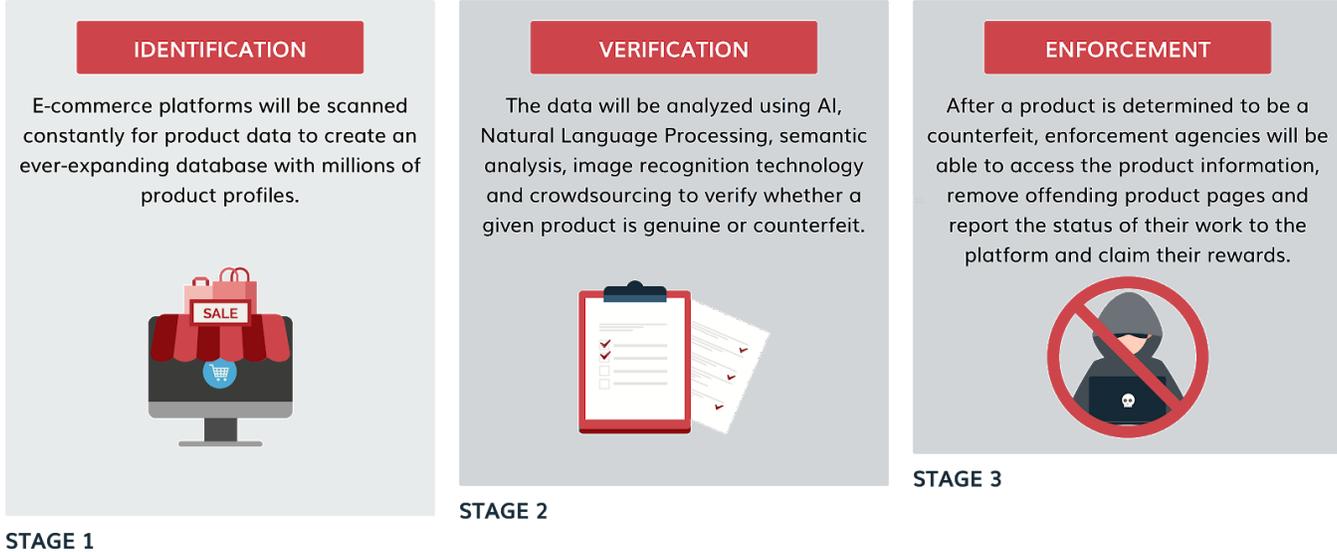
# Solution Framework

In today's increasingly technological world, E-commerce is becoming more influential to people's lives, which is also creating new and expanding avenues for counterfeiters to

exploit. These counterfeiters exist everywhere and have permeated E-commerce channels all over the world, creating an unprecedented flow of counterfeit products. Counterfeits are low quality and dangerous, which is why simplyBrand is presenting a new way to improve global E-commerce that will benefit everyone from major brands to individual consumers.

The simplyBrand platform will combine AI, human ingenuity and blockchain technology which will be used to create an immutable “blacklist” of counterfeit product vendors available for the world to see, while the tokens within the blockchain will incentivize crowdsourced participants to utilize the simplyBrand platform.

The simplyBrand platform for cleaning up E-commerce will follow 3 stages:



## 4.2 Roles within the ecosystem

Below are the various roles and the benefits they will gain from being a part of the simplyBrand platform.

## 4.2.1 Brands



Brands will directly benefit from the simplyBrand platform by having counterfeit versions of their products quickly identified, verified and removed, helping them to maintain a positive brand image and regain their market share. Counterfeit retailers will also be exposed, giving brands the chance to learn more about the source of counterfeit products. Brands will join the ecosystem by paying a service fee, and by offering products and services as rewards to crowdsourced participants. Brands will give back to the ecosystem by helping to

improve the accuracy of the verification process and contribute to whitelisting legitimate retailers.

## 4.2.2 Crowdsourced Participants



The participants in this system will be the people supporting the verification process; people who are likely fans of specific brands and products, or those who simply wish to make some pocket money. Within the ecosystem, participants will be shown product pages and verify if they are counterfeit or not, helping to improve AI accuracy. They will also be shown two product pictures and will verify the real version, helping to improve image recognition. Finally, they will directly report counterfeit products on E-commerce platforms, helping

the AI to collect real samples for further improvement.

## 4.2.3 Enforcement agencies



Enforcement agencies refers to the organizations that specialize in working with E-commerce platforms to remove counterfeit products from the E-commerce platforms. By joining the ecosystem and working within the platform, they will have access to a large amount of counterfeit product info instead of having to find it manually, allowing them to increase their earning potential and prove their effectiveness to brands and potential new clients.

## 4.2.4 Third parties



The platform will also be available to a variety of third party organizations, including legal firms and other organizations that wish to do business with brands and/or participate in the ecosystem. These organizations will participate because it improves their access, and subsequent offerings, to a variety of global brands. Many third parties already working with brands will benefit by having access to a system wherein they can find data to help evaluate the risk factors which counterfeiting poses to a brand.

# 4.3 Mechanism Design

This section is dedicated to introducing the mechanisms throughout the whole solution.

## 4.3.1 Staking Mechanism

Staking mechanism is a vital part of the platform operation. One of the purposes of staking is to obtain “the right of use” of the platform, and the other is to prevent any abusive action against the platform.

1. The Right of Use: It is required for all parties (except users accessing the blacklist) on the platform to stake in order to participate in the activities on the platform or to gain information from the platform.
2. Abuse-prevention: With the crowds accessing the platform and joining the anti-counterfeiting activities, abuse-prevention mechanisms are crucial to keep the platform stable. When users perform an abusive act against the platform, their stake will be deducted as a warning. If their stake is insufficient, their right to use will be suspended until the staking requirement is met again.

### **4.3.2 Crowd Counterfeit Verification Mechanism**

Every time a user participates in an anti-counterfeiting activity, they will receive a set of products information. The sets of products will be randomly distributed between different users, meaning that it is impossible for two different users to keep receiving the same sets of products. This design avoids the situation where two less-accurate individuals verify the same product sets, resulting in a not-so-accurate result. Regardless of the random distribution of product information, each product will still receive the required number of verifications from crowdsourced individuals.

The required number of verifications will also evolve according to different phases of the platform. At the introductory phase of the platform, we still need more input from the masses to train the neural network of our AI model. Therefore, each possible counterfeit product will be verified by 20 participants, with the result regarded as the correct answer only when over 75% of the participants reach a consensus on the result.

The abuse-prevention mechanism embedded in this section is that if a participant's valid verification submission reached 10 sets, and the accuracy level is lower than 70%, the received token will not be confiscated, but their work will be counted as "failed work". This mechanism is described in more detail in Section 4.3.4 Rating Mechanism.

### **4.3.3 Crowd Reporting Mechanism**

There will be two types of reporting. The user can report to the platform when they receive a fake product after placing an order on an online store. Another way of reporting is when the user sees an online store selling counterfeits. The users can receive tokens after the reported items have been verified with a high possibility of being a counterfeit product.

In the first type of reporting, the most common scenario is that all of the information shown by the online store is legitimate, but when the seller receives an order, they ship a counterfeit that has some kind of resemblance to the product they show on the online store. When the user receives the product, he can report to the platform with the URL of the page selling the product and also related information. The limitation of this type of report is 5 cases in 30 days. If the user reports 5 items within 30 days, they will have to wait until all 30 days has passed, and then they could report another item.

The second type of report is submitted by users that see an online store selling counterfeit products when they are browsing through E-commerce stores. The limitation of this type of report is 30 URLs per day. The platform will calculate the accuracy of the reported URLs for every 10 URLs reported. If the accuracy is lower than 60%, the user can still receive tokens for the correct ones, but their work will be counted as a “failed work”. This mechanism is described in more detail in Section 4.3.4 Rating Mechanism.

If a user reports a product page using either the first or second type of report that has already been reported before, then the reward of the token will be adjusted.

In the following equation, N represents the times that the same product page has been reported, T represents the tokens that a user can receive for completing a job, and R represents the reward that the user can get:

$$\begin{aligned} \text{if } N \leq 10, R &= \frac{T}{2^{(N-1)}} \\ \text{else, } R &= T \times 0.001 \end{aligned}$$

For example, if the reward for reporting a URL that sells counterfeit product is 10 tokens, the first participant to report this URL will receive 10 tokens once the URL is verified, the second participant will only receive 5 tokens, and the third one will receive even less with 2.5 tokens, and so on. This design is to prevent a participant from abusing the platform by reporting an URL’s info or a fake product repeatedly to receive rewards infinitely.

### 4.3.4 Rating Mechanism

At the beginning of every account creation, every account will be given an invisible rating with the initial value of 80 as their rating. With every successful job that the user has participated in, 1 point will be added to the existing value, with 100 being the maximum value of the rating. The rating will be in the system, and the user will not be able to see it. If the user has performed a “failed work” as described in the previous sections,  $2^1 = 2$  points will be removed from their rating. If, in the two following activities after the first “failed work”, a “failed work” takes place again, then another  $2^2 = 4$  points will be taken from their current rating. If the user performed a third “failed work” in the two following work after the second,

then  $2^3 = 8$  will be deducted. However, if the user didn't perform a "failed work" for 2 consecutive activities, then the next "failed work" will cost him only  $2^1 = 2$  points.

When the rating of an account drops below 75, then the account will be suspended for a week. After the suspension, the value of the rating will restore to 80. If an account receives three suspensions, then the account will become permanently inaccessible, and all the staked tokens will be confiscated.

### **4.3.5 Blacklist Update Mechanism**

On the suspicious blacklist, other than the information about the counterfeiting products, channels and sellers, there will be information about when the list is verified and added or updated to the blacklist. The list will be reviewed regularly by the platform and any updates will be added to the list and also to the blockchain.

If an online store or seller listed on the blacklist wishes to be reviewed as soon as possible, they can pay tokens to the platform for an early-review process, and the entry that contains their information will be reviewed in the next month.

## **4.4 Development Phases**

This section will describe the growth phases of the simplyBrand platform, detailing the specific occurrences in each phase and the evolution of the ecosystem itself.

### **4.4.1 Introductory Phase**

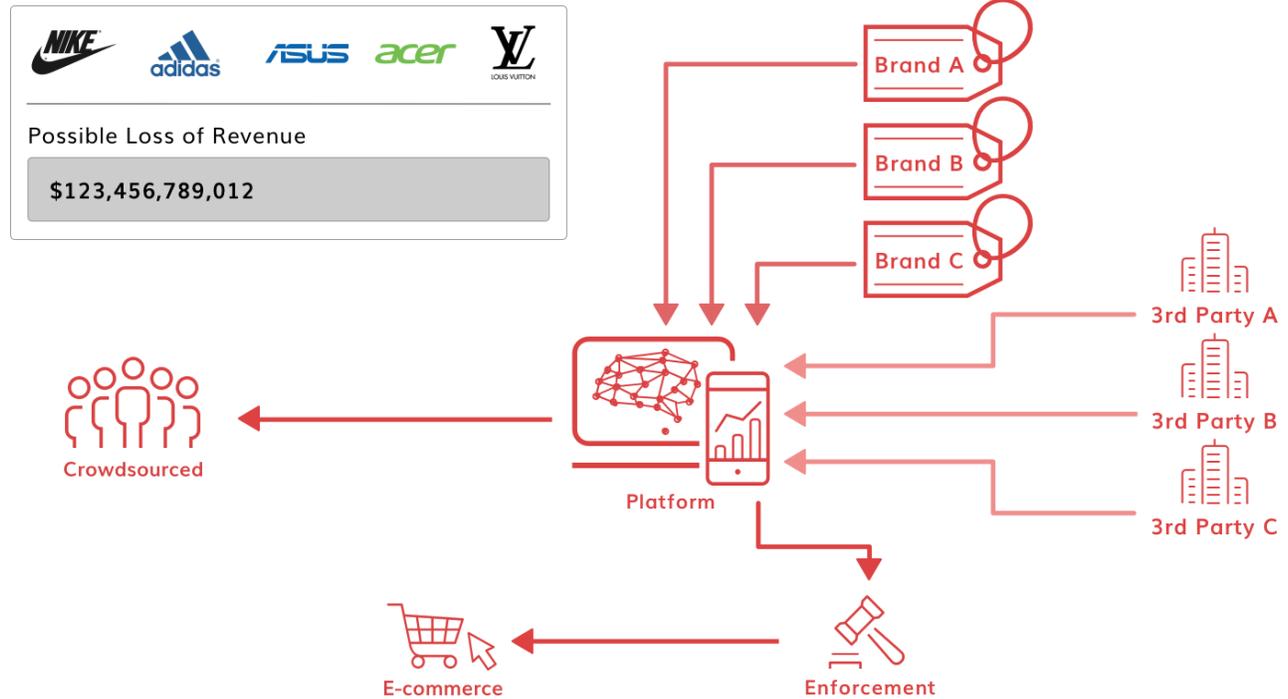
In the introductory phase, brands will join the ecosystem by paying a service fee, or by offering platform-specific products and services in lieu of payment; such products or services could be a limited-edition product or special service which can be redeemed by crowdsourced participants through the simplyBrand platform. Initially, collecting counterfeit product info will be done either via submission from crowdsourced participants, or through the AI. The latter method will be introduced more thoroughly in the technology section. Counterfeit product info will then be first verified by the AI and then by the participants. There will be systematic cross checks if the former verification method cannot properly determine the authenticity of a product. After the process is complete, the counterfeit product info will be given a score, indicating the possibility of it being a counterfeit, and enforcement parties will then report these products accordingly.

### **4.4.2 Upward Phase**

After accumulating large amounts of data in the introductory phase, the platform will be able to announce its first Proof of Concept, or PoC1. Major information exposed in PoC1 is the expected loss of revenue due to counterfeits sold on E-commerce channels for any given brand. Users will be able to enter the platform, select a brand icon, and view their expected losses. By releasing such information, other brands will be prompted to join the platform to gain the information they need to prevent more losses, while also attracting third parties and enforcement agencies that are seeking new clients and business opportunities.

## The Upward Phase

PoC1

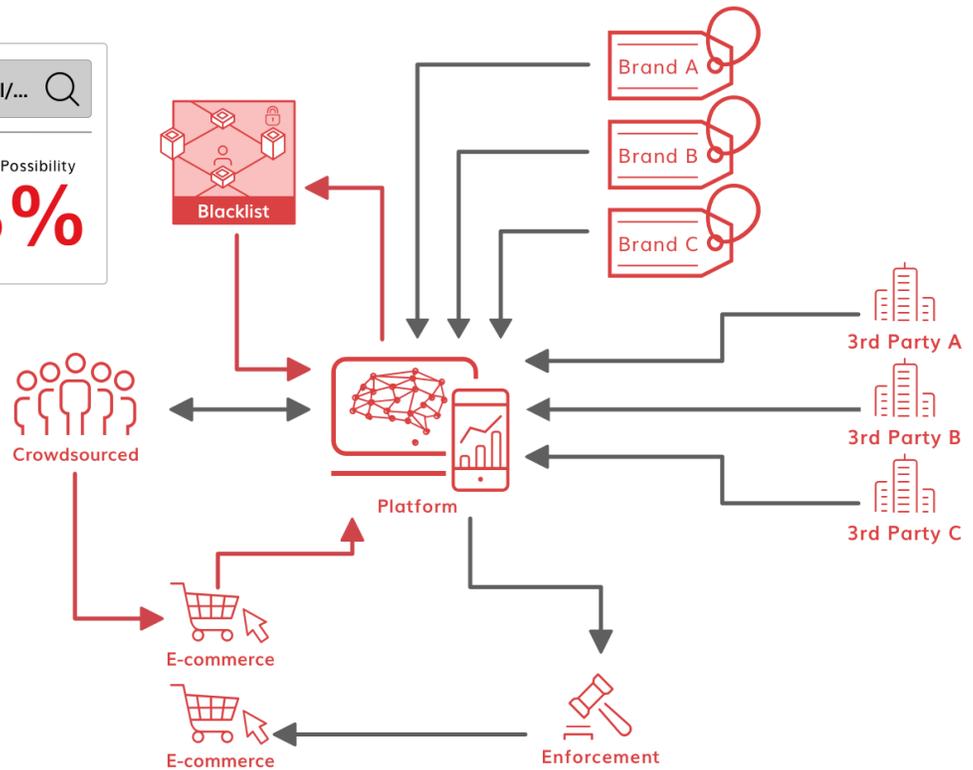


### 4.4.3 Mature Phase

The mature phase will be marked by the release of the second Proof of Concept, or PoC2. PoC2 will be defined by the release of a new area within the simplyBrand platform that allows users to enter a product URL and will be shown with corresponding information such as the product name and the price, and most importantly, the possibility of the item being a counterfeit and the percentage of possible counterfeits being sold on a specific E-commerce platform. This will allow consumers to make informed decisions when purchasing online and help reduce their chance of purchasing counterfeits.

## The Mature Phase

PoC2



The release of PoC2 will also trigger E-commerce platforms to join this ecosystem as it can help them identify counterfeit retailers within their platforms and help protect their brand image. Finally, during this phase the counterfeit retailer blacklist will be put on the blockchain for the public to gain access to the information we have accumulated. The counterfeit retailer's information and products they are selling will be included on the Blacklist, which may never be erased or edited, but only amended to reflect their current status as counterfeit or legitimate retailer's.

The culmination of the mature phase will result in a high demand token economy existing in a self-governing ecosystem without the need for external interference.

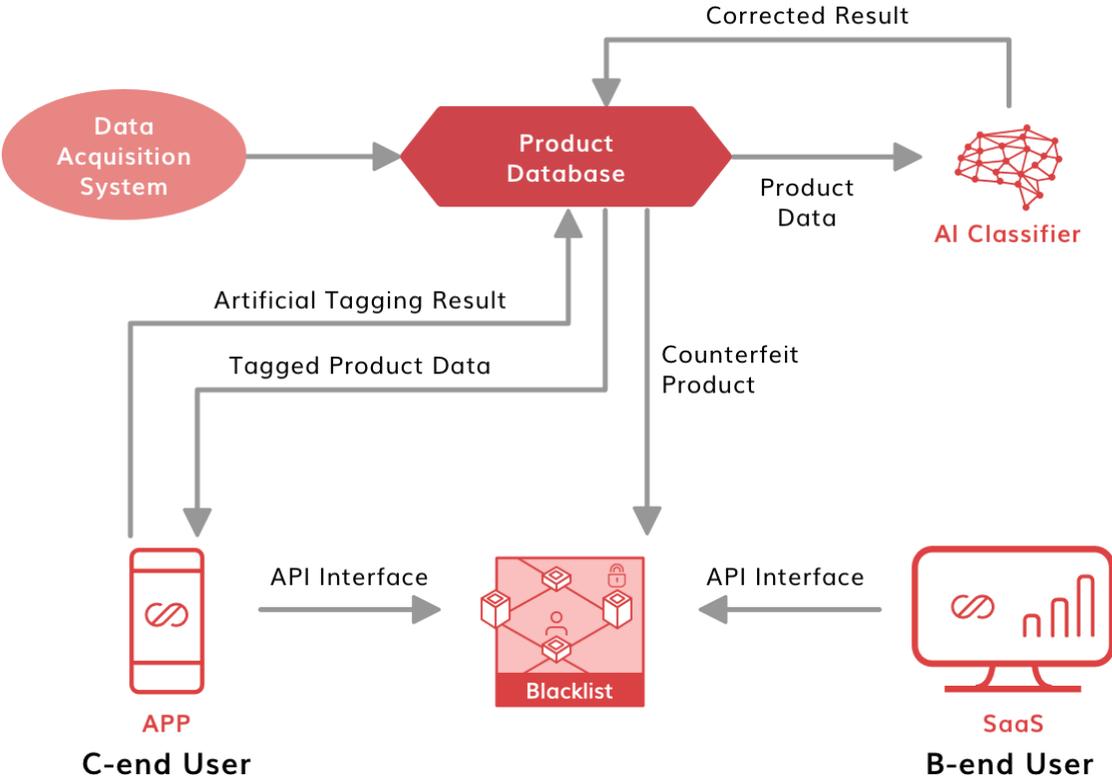
### 4.4.4 Future Phases

When the ecosystem moves beyond the mature state and has a high level of participation of, and a greater connection between, all categories of participants, the platform will come to include content which brands can leverage to reach out to consumers and also allow Brands to introduce loyalty programs to incentivize participants with platform specific

products and services. The simplyBrand platform and complete ecosystem will enter new, undefined territories as it begins to achieve its full potential of cleaning and strengthening global E-commerce; a potential which can only be understood in time.

# 5 Technology

The platform will begin by collecting product data from e-commerce platforms and storing them in the product database as vectors. The product data will then be transferred from the database to the classifier system so that the AI classifier can divide the products into authentic or counterfeit categories, which will be the two tags in the classification system. The products tagged as counterfeit will have their information transferred to the blacklist which is open to be accessed by platform users through the app or website. These same users will also be invited to participate in classifying products to help increase maturity of the AI classifier algorithm. Business users can log in to the SaaS platform to access the blacklist, take and fulfill enforcement tasks/orders, query a brand's risk analysis to understand the likelihood of their products being counterfeited, as well as a general overview of counterfeiting risk within a particular e-commerce platform and the overall industry.



## 5.1

# Distributed Data Acquisition System

The distributed data acquisition system will be a cloud-based system which is designed with high system scalability and dynamic scale-out capability so that it can handle the throughput from scanning a large scale of E-commerce platforms continuously. The data will be collected by means of searching a number of keywords and images across E-commerce platforms around the world. The data will be filtered and cleaned via STORM Cluster and then stored into the ElasticSearch cluster.

## 5.2

# Product Info Database

After data collection takes place, it will be transferred to a distributed database via ETL for natural language processing, semantic analysis, opinion extraction, topic analysis, image recognition etc. This will transform each piece of product info data into sets of quantified data called vectors. These vectors will be input into the AI classifier.

## 5.3

# AI Classification System

An AI system is used to classify authentic and counterfeit products which is built, modeled and trained by data scientists and SMEs (subject matter experts) with training datasets. New datasets will be collected to help to further train the AI. Thus, as new datasets are



## 5.4

# Blockchain

Blockchain technology is irreplaceable in our solution because we will be implementing two major features using blockchain technology: tokens for incentivizing and staking, and to publish immutable information about counterfeit retailers.

Blockchain technology has a couple of features that enhances our solution, namely distributed and immutability. Being a distributed ledger means that an identical ledger will be possessed by all the nodes in the whole network. Any inconsistent information will be considered invalid because these information will not be accepted in a consensus-based network. As a result, information in the blocks cannot be altered by a single person or entity. In addition, the ledger is designed with a chain-structure of information blocks and connected in chronological order. Each block contains a hash from the previous block. A hash is generated by a one-way function, and the input would be the information contained in the block. As a result, information contained in the previous blocks will be impossible to change or erase, in other words, immutable.

And by leveraging these features, we will be able to release in-erasable information of counterfeit retailers on the blockchain. The products tagged with counterfeit labels will be stored on the blacklist system, which will be published on the blockchain afterwards. A smart contract will be used to store the record of counterfeit retailers (those who sell fake items). The smart contract allows anyone to query the list of counterfeit retailers and take actions accordingly. Since the data on blockchain cannot be erased, the information of counterfeit retailers will always be traceable.

In addition, simplyBrand Token, SBA, is a token based on ERC20. It will be used for payments and staking in the ecosystem.

# 6 Token Design

This section will focus on explaining how the joining parties will earn tokens by using the platform. We will be only focusing on describing how the system works. Other information, such as the actual amount of rewards, will be announced after the platform is online.

## 6.1 Rewarding Mechanism

The user can earn rewards by participating in activities on the platform. Under normal circumstances and operations, users will not lose their staking tokens. But only in the situation highlighted in Section 4.3.4 will the participants lose token.

### 6.1.1 Verification Rewards

(Base points: 0.15 token for a set of product information)

When platform users participate in counterfeit verification activities, they will receive tokens in accordance with the accuracy rate from verifying a set of product information.

For example, if the verification result from user A match the final consensus, and the current reward is 0.15 token for a set of product information, then the user can receive 0.15 tokens. If the verification result from user B doesn't match the final consensus, and the current reward is 0.3 token, but because the results don't match, user B will not be able to receive the token rewards.

Once the user submitted 10 sets of valid verifications, the system will calculate an accuracy rate of the verifications. If the accuracy rate is lower than 70%, they will still be rewarded for the correct verifications, but will also be recorded with a "failed work" rating. Please check Section 4.3.4 for more details on how "failed work" will be dealt with.

### 6.1.2 Rewards from reporting URLs

(Base points: 1 token for 1 URL)

When a user sees a certain online store selling counterfeit products, they can report the URL of the page selling counterfeits to our platform. They will only receive token rewards if the URL is verified to be selling fake products. In other words, they won't be rewarded if the verification shows that the URL is selling legitimate products. The system will calculate the correction rate once 10 URLs are reported, and if the URL selling counterfeits falls under 6, then a "failed work" rating will be recorded.

### **6.1.3 Rewards of reporting fake goods received from online stores**

When a user places an order online and ends up receiving a fake product, they can report it back to our platform with the photo of the product and also the invoice of purchasing the product. Once the information is verified, they will be rewarded with 10 tokens.

### **6.1.4 Rewards for taking down an URL**

(Base points: 10 tokens for taking down 1 URL)

Enforcement agencies will take the URLs from our platform and report them back to the E-commerce platform. Once the URLs have been taken down by the E-commerce platform, enforcement agencies can receive rewards by reporting the result back to our platform, and receiving confirmation of the result by the platform.

## **6.2 Mining Mechanism**

At the beginning of the platform establishment, in order to incentivize more individuals to join the platform and participate in our anti-counterfeiting activities, the platform will prepare 13.5% of the total token supply for early users to mine. The amount of tokens that can be mined will decrease over time, so the earlier a user joins and participates, the more tokens

they will be rewarded. Once all of the reserved token are mined, the rest of the activities will receive the rewards designed in section 6.1.

If R is the reward received from mining, and X is the sequence of work, then the formula for the mining mechanism is:

$$R = 4 - X x \frac{1}{16,875,000}$$

According to this formula, the first job finished and confirmed will receive an additional 4 tokens, and the last job will be the 67,483,129th one, with the participant able to receive 0.001 token as the mining bonus.

## 6.3 Balancing Mechanism

A balancing mechanism will also be embedded in the platform, allowing all jobs to be done efficiently. The two factors in the balancing mechanism are as follows:

“Base Point”: Selected jobs will be endowed with a fixed base point value according to the cost, including the time and efforts needed to get a job done. The harder the job is, the higher the base point will be. The value of the base point cannot be 0.

“Supply-Demand Multiplier”: the supply-demand multiplier is a 0.1 to 2.0 value with 0.1 intervals in between each value. Each job that has been given a base point will also be given a value of the multiplier which will be updated every 10 minutes.

The platform will maintain an average number of each pending work, and compare it with the current status to define the multiplier. For example, the platform has an average of 100 URLs waiting to be verified, but there are only 50 pending URLs, then the multiplier will be higher. To give another example, if the platform has an average of 200 verified URLs waiting to be reported to the E-commerce platforms, but currently there are only 50 verified URLs waiting to be reported, then the multiplier will be lower.

So the final reward of a job will be defined by “base points” times “supply-demand multiplier”.

For example, if the base point for a job is 1, and the supply-demand multiplier is 0.8, then the participants that choose to participate in this job at this moment will receive ( $1 \times 0.8 = 0.8$ ) tokens once the job is verified.

## 6.4

# Total Token Reward

To conclude, the final reward will be a combination of the following factors:

- Original designed token rewards for this job (the “base point” mentioned in Section 6.3)
- Accuracy rate (only applicable in several conditions)
- Supply-demand multiplier (only applicable in several conditions)
- The number of times that the work has been repeated (only applicable in several conditions)

## 6.5

# Token Flow

Our platform is tokenized in order to facilitate the establishment and operation of the whole ecosystem.

- Crowdsourced participants can receive tokens as rewards, and can either use them to purchase brand privileged items on our platform or sell them on exchanges
- Enforcement agencies can receive tokens as rewards, and can sell them on exchanges

- Brands can buy tokens from exchanges, and purchase brand-protection services on our platform
- Third-party service providers can buy tokens from exchanges, and purchase information on our platform



# 7 Roadmap



## TIMELINE

- 2013.05**  
simplyBrand started to provide big data and AI solution for brands
- 2017.10**  
Anticipated anti-counterfeit demand from existing customers, received RFP
- 2018.05**  
Kickoff simplyBrand.io blockchain solution project with marketplace verification MVP
- 2018.10**  
Crowdsourcing MVP
- 2018.11**  
PoC1 Impact Calculator
- 2018.12**  
PoC2 Counterfeit Risk Detector
- 2019.04**  
SaaS application for Brands and Blacklist on Blockchain release
- 2019.07**  
SaaS application for Enforcement Agencies online
- 2019.11**  
Verification - Crowdsourcing online
- 2020.02**  
Integrates 3rd parties application online

# 8 Team

## **Kaufman Chang**

Founder/CEO

As the founder of multiple startups, including ventures in cloud computing software, big data security software and biotech, Kaufman is well known for developing strategies to use big data and analytics solutions to help a variety of brands and businesses. Kaufman leveraged his background in cyber security and brand protection to unite blockchain and AI in his latest vision to strengthen digital commerce against counterfeiting. Previously, Kaufman held a number of key roles at Trend Micro for over 15 years where he used cloud computing to help businesses resolve digital safety issues. Kaufman graduated from the University of Chicago Booth School of Business with an MBA.

## **Ronnie Ng**

Co-Founder/CMO

Over the course of the past 15 years, Ronnie has worked across Asia where he has founded and sold multiple start-up companies, including a media consulting company and an English language learning institute with 45 branches throughout China. In 2013, Ronnie co-founded simplyBrand, a big data intelligence company with the ultimate goal of bringing a blockchain-based solution to brand protection. Ronnie graduated from the University of Chicago Booth School of Business with an MBA.

## **Frank Shi**

Technical Director

Frank has been engaged in data processing for more than 10 years and possesses rich experience in AI technology, cryptography and blockchain architecture. Previously, Frank worked for CIC where he built the distributed data collection system. Frank's experience in AI, along with his vast knowledge of blockchain architecture, will be used to couple these technologies to create a disruptive new solution that will see people and brands working together to fight counterfeiting. Frank graduated from China Normal University with a BS in Software Engineering.

## **Aleen Zhang**

Product Director

Aleen has a varied background including, product research, interaction design, SaaS application development, as well as experience in transaction data and transaction ledgers within blockchain ecosystems. Currently, Aleen is in charge of data platform and product user R&D, as well as demand mining and blockchain architecture. Aleen's knowledge of blockchain technology has helped drive this project from a simple thought into a great reality by bringing together AI and blockchain to create the new core simplyBrand platform. Aleen graduated from Hunan University of Commerce with a BA in Advertising.

## **Ada Yao**

Research Director

Ada has almost 20 years of experience in consumer research and business development, focusing on managing research projects, defining business development goals and building SaaS products for clients. Currently, Ada heads the planning and research department for blockchain development. Ada's industry knowledge and experience in blockchain has driven the development of the simplyBrand blockchain model through her concise and data backed research. Ada graduated from Inner Mongolia University of Finance and Economics with a BS in Finance and Taxation.

## **Rita Yang**

Business Development Director

Rita possesses a background in sales and business development in blockchain, having served in positions around Asia. She is now working to develop long term client relationships, manage accounts and analyze data for existing clients, including AI output data. Rita's understanding of the scope of blockchain in the Asia-Pacific region has helped to define clear goals for simplyBrand to ensure that this project results in tangible solutions for brand protection strategies. Rita graduated from Donghua University with a BS in Information Management.

## **Hsin-Chi Tsao**

Design Director

Hsin-Chi is an award-winning graphic artist and commercial designer that received a Bronze at the Cannes Advertising Festival in 2015 and the IF Concept Award in Package Design in 2013, among others. Her expertise in design and artistry has won her a number of global clients, including New Balance, Ford, HSBC and Ant Financial. Hsin-Chi uses her expertise and vast experience to produce evocative and high-quality imagery to fully define simplyBrand's visual identity. Hsin-Chi graduated from National Taiwan University with a Master's in Commercial Design.

## **Oleksandra Zavertailo**

Community Manager

Oleksandra is a marketing professional having 1 year of prior experience in risk controls cross-border investment. She is a native Ukrainian who has lived in China for more than 5 years. Her stint as Programme Assistant at the ESSCA School of Management sparked her interest in blockchain technology. She holds a Master's degree in International Relations from East China Normal University and a Bachelor's degree in Chinese Language from Kyiv National University of Taras Shevchenko.

## **Thibault Laville**

Marketing Manager

Thibault is a French citizen, born in New Caledonia. He has more than 2 years of experience in digital marketing with QPSoftware, Pernod Ricard and Keli Media. An MBA graduate from ESSCA School of Management in digital marketing and E-business.

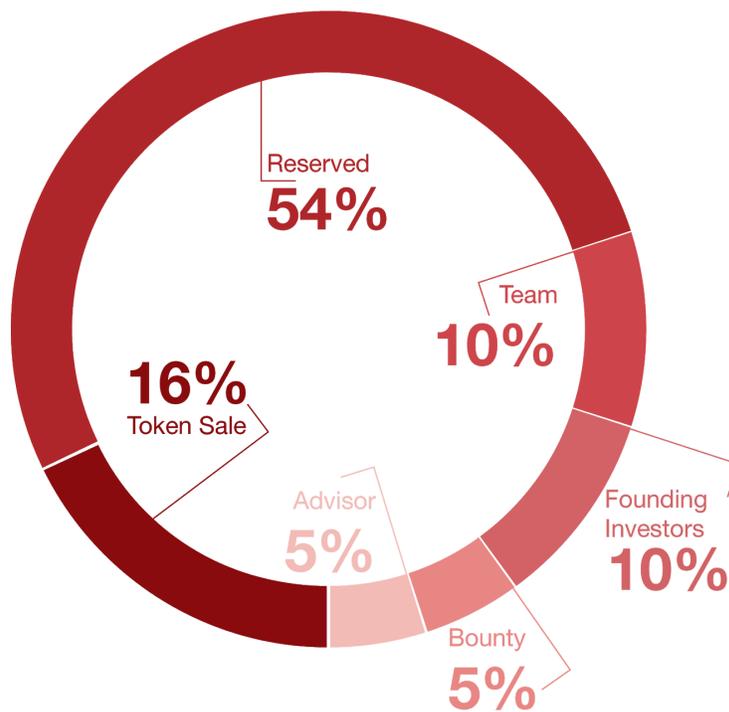
9

Token Sale Plan

# 9.1 Token Design

Token Supply <b>1,000,000,000</b>	Type <b>ERC20</b>
--------------------------------------	----------------------

# 9.2 Token Allocation



# 9.3

## Fund allocation



# DISCLAIMER

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

The information below may not be exhaustive and does not imply a contractual relationship. While we have made every effort to ensure that all information in this whitepaper is accurate and up-to-date, the material in no way constitutes professional advice. simplyBrand does not guarantee, and accepts no legal liability whatsoever arising from or connected to, the accuracy, reliability, currency, or completeness of the information in this whitepaper. Potential SBA TOKEN buyers and holders should seek appropriate independent professional advice prior to relying on or entering into any commitment or transaction based on information published in this whitepaper, which is purely published for reference purposes. SBA TOKEN are not intended to constitute securities 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 or a solicitation for investment in securities in any jurisdiction. simplyBrand does not provide any opinion on advice to purchase, sell, or otherwise transact with SBA TOKEN and this whitepaper shall not form the basis of, or be relied upon in connection with any contract or purchasing decision. No person is bound to enter into any contract or binding legal commitment in relation to the sale and purchase of SBA TOKEN, and no cryptocurrency or other form of payment is to be accepted based on this whitepaper. The primary purpose of purchasing SBA TOKEN is for the use of simplyBrand services. While simplyBrand has a system in place that may result in the growth in value of SBA TOKEN, and a secondary market for SBA TOKEN may be available, simplyBrand does not take legal responsibility for any loss in value of SBA TOKEN. Please understand that the SBA TOKEN is not a security but meant for use within the simplyBrand ecosystem to pay for all SimplyBrand services.

SBA TOKEN may have no value and there is no guarantee or representation of liquidity for SBA TOKEN. simplyBrand and its representatives are not and shall not be responsible for or liable for the market value of SBA TOKEN, the transferability and/or liquidity of SBA TOKEN and/or the availability of any market for SBA TOKEN through third parties or otherwise.

## **IMPORTANT**

Citizens and residents (tax or otherwise) of The People's Republic of China, hereafter referred to as "The Country", or other Persons of The Country are not eligible to purchase SBA TOKEN during the public sale. "Person of The Country" is defined as a natural person, residing in The Country, or any entity organized or incorporated under the laws of The Country. SBA TOKEN are not a security and do not provide any equity ownership, dividends or otherwise control over simplyBrand, which is applicable information for citizens, Green Card holders and residents of the United States of America. If you are unsure of the regulatory requirements, which frequently change, consult your legal or financial advisor as to your eligibility to purchase SBA TOKEN in the Token Distribution Event.

 simplyBrand.io

 <https://t.me/simplyBrand>