Blockchain and App for virtual graffiti “Kokorobakari”

Yasutaka TSUKAMOTO* and Yoshifumi NAGANO**
(tsukamoto@profound-dt.co.jp) (nagano@saltfish.co.jp)

*Profound Design Technology Co.,Ltd.
**Saltfish Co.,Ltd.

Abstract This article introduces the virtual graffiti app "Kokorobakari" we are planning to develop. Kokorobakari is a DApps (Decentralized Applications) that runs on the Ethereum blockchain. Kokorobakari is an application that can be impressed on a blockchain on the spot and leave it as a memory, and at the same time, it can be donated to the area as an appreciation for the impression. Kokorobakari is more than just a virtual graffiti app, it has the potential to become a huge world-wide traveler's platform that moves people and money dynamically. Profound Design Technology (hereinafter PDT) has acquired a patent in Japan for the virtual graffiti system.

Key word : blockchain, Ethereum, DApps, donation, graffiti, traveler, moving, DApps, Platform

1. Introduction

Recently, blockchain technology has attracted attention as a distributed database. Until now, cryptocurrency such as bitcoin using blockchain technology has attracted attention. However, the expectation that blockchain technology can be applied to various fields, as well as the cryptocurrency, has been rising for several years.

Under such circumstances, so-called POC (Proof of Concept), which applies a blockchain and verifies its effect, is implemented in many fields. So we also considered areas that would be interesting if we applied a blockchain. In addition, our company, PDT had experience in designing ASICs (semiconductors) for mining Bitcoin in 2015 and had knowledge blockchain from before. Now, the advantages of blockchain viewed from the general user are as follows.

1 Data remains semi-permanently (everywhere on the earth)

2 It is hard to falsify the data

3 Data cannot be erased

4 There is no need to backup data

5 Easy to send money to others

The above No. 5 may be full of issues and details, but for the moment, I will not be addressing these.

We focused on No. 1 first and examined the blockchain application field. But are there many cases where you want to leave data semi-permanently in the first place? Japan's official documents should be kept for up to 30 years at most. we wonder how to use public blockchain resources to save for only 30 years. Of course, the story changes if a blockchain that can physically erase data appears in the future.

After various investigations, we thought that there would be graffiti on the road as a thing that falls under 1. There are various types of graffiti on the road, but for example, you may be impressed on the road and leave the impression as graffiti. However, it is not good to write such graffiti on buildings. However, I can understand the feeling that I want to scribble the impression and leave it as a memory.

So we came up with a "virtual graffiti". Instead of physically drawing graffiti on the actual building, characters, images, sounds, etc. are stored on the blockchain together with the position information, and are made into virtual graffiti. The saved graffiti is retrieved from the blockchain based on the position information when the site is visited again and is displayed on a smartphone or displayed using AR technology. Alternatively, after traveling, it is possible to display the visiting place on the map on the smartphone while at home and display the graffiti there. Also, since the graffiti data is stored in the block chain, it will remain semi-permanently.

Furthermore, because graffiti was stored in the blockchain, we considered whether a system could be built in connection with cryptocurrency. As a result, we thought that after the impression of the trip there were thanks and there was a donation ahead of thanks. However, because the word "donation" seems to look a little from above, we decided to call it "Kokorobakari" rather than a donation. The origin of the name of the virtual graffiti application Kokorobakari is "Kokorobakari". "Kokorobakari" is Japanese. It means "the heart only".

Chapter 2 explains the essence of blockchain technology. Many web sites and books do not explain much about the nature of blockchains. Sometimes you see something that has a wrong explanation. Chapter 3 gives an overview of the virtual graffiti app Kokorobakari. Finally, Chapter 4 discusses the possibilities of Kokorobakari.

2. Blockchain and DApps

2.1 History of Blockchain

Blockchain technology has gained in the limelight as it is used in one of the cryptocurrencies, Bitcoin. A person named Satoshi Nakamoto published a paper on Bitcoin in October 2008 on the Cryptography mailing list. And the source code was released in January 2009, and the operation of the Bitcoin network was started. Furthermore, it is still a mystery whether Satoshi Nakamoto is Japanese or who it is.

According to Satoshi Nakamoto's paper, he seems to have considered the following. The following is not a representation of his paper itself, but with some addition of our own interpretation.

- When considering a small amount of remittance, it is not realistic because banks and the like incur a large fee.
- If so, can you somehow send money directly between individuals?
- For that purpose, the person who receives the money needs to at least check the other's deposit balance (payment ability).
- How do you check the other's deposit balance without intermediaries like banks?
- Yes, you only need to know the contents of the other party's passbook (all transaction history, including transactions with other people).
- Save all transaction history (remittance history) of everyone in the world yourself.
- OK idea, but what do you do when your computer is down?
- If so, all people have to save the same contents of all transaction history (remittance history) of all people in the world.
- Then you don't have to do your own back up.
- But how do you keep the content of the data that many people have always the same?

The problem is the last question, "How do you always make the contents of the data that many people have the same?" Here, the data in which the contents of the transaction are stored is referred to as a "ledger". For example, if Mr. A receives a remittance of 100 yen to Mr. B, information such as remittance source A, remittance destination B and remittance amount of 100 yen is written in the ledger.

However, this "trade" can occur almost simultaneously around the world. Almost simultaneously with the remittance of Mr. A → Mr. B mentioned above, remittance of Mr. X → Y may occur on the other side of the earth. At this time, remittance information of Mr. A → B may be written first in the ledger stored by a certain person, and then remittance information of Mr. X → Y may be written after that. On the other hand, the remittance information of Mr. X → Y may be written first in the transaction register stored by another person, and then the remittance information of Mr. A → B may be written after that. This is not good, as the order of transactions in the two transaction ledgers is different. Of course, there are cases where there is no problem even if the trading order is different.

2.2 Blockchain is File Synchronization System

The data that stores the ledger for all transactions of everyone is called a blockchain. We will explain later why "block". The reality of blockchains is just a file. The size of the file is very large because it saves all the transaction history of everyone. As of April 17, 2019, the file size of the blockchain in Bitcoin is about 213 GB. More than 10,000 computers worldwide hold copies of this 213GB file with the same content. This is the reason why Bitcoin blockchain is also called distributed databases. However, in general, there are two types of "distributed databases". The first is the case where one data (file) is divided finely and the divided data is managed by a plurality of computers. The other is the case of copying (duplicating) and managing one data (file) on a plurality of computers. The bitcoin blockchain is the latter 'copy' type.

After all, 213GB × 10,000 = 2,130TB disks are used for bitcoin all over the world. It feels like a waste of resources, but I'm going to close my eyes here too.

As an aside, Satoshi Nakamoto's paper (1) does not use the term blockchain. In the paper, the expression chain of blocks is used. However, in the world, it is used as the word blockchain.

One question arises here. In order to participate in Bitcoin, do I have to save the entire a blockchain in hundreds of GB on my PC or smartphone? That is the point. In fact, there is no such need. So how do you know the other party's balance, but generally speaking, it will be taught by those who have saved the blockchain. However, it will be bad if the person who teaches me is a bad person. The technology in this area is called SPV (Simplified Payment Verification) in Bitcoin. We will not go over the details of SPV here.

Well, how do you save files (a blockchain) of the same contents in real time among more than 10,000 computers in the world? Keeping the contents of files always identical between computers is called "file synchronization". It seems that the computer specialists will ask me "a definition that is not childish", but I think it is not so wrong.

The first method that comes to mind as a way to synchronize

files is "First come first served". If there are many transactions happening around the world at the same time, many people (computers) want to write their transactions on the blockchain. At this time, one of them is decided on the first-come-first-served basis (for example, Mr. W), and the person writes his/her transaction in the blockchain he/she holds. Meanwhile, other people (computers) do not write their own transactions on the blockchain but copy the contents written by Mr. W on the blockchain to the blockchain they hold. This makes it possible to make all the contents of the blockchains existing all over the world the same.

The question here is how to decide the winner of the "first come, first served". It is necessary to make everyone compete for something because "earliest wins". In the case of Bitcoin, we adopted a certain "calculation problem" as competition. This "calculation problem" has the following features.

- It takes time. About 10 minutes for bitcoins. (If it is a calculation problem that will end soon, some people will finish the calculation at the same time)
- The contents of the calculation problem are all different. (If everyone solves the same problem, some people will finish the calculation at the same time)
- You can not guess the answer to "calculation problems".
- It takes time to solve, but you can check in a moment whether the correct answer is correct. (because everyone needs to be able to verify in a short time that you are the best.)
- You can adjust the level of difficulty of the calculation (because it is necessary to raise the level of difficulty and take time if there are people who calculate quickly)

The act of solving this "calculation problem" is called "mining". In other words, the purpose of "mining" is to determine for each transaction the only person (computer) who writes the transaction history in the blockchain. After all, it is the goal of mining to synchronize blockchain files. The main purpose is not to prevent tampering or tampering detection. I wrote "Every deal" here, but it is slightly different. In fact, a certain number of transactions are put together into one block, and the block is written in the blockchain. The "block" of the blockchain is this "some amount of aggregated transaction information". The reason for using "block" units is that solving the "calculation problem" for each transaction takes time to fix the transaction.

Mining means "mining in mines", but it has nothing to do with file synchronization. Nevertheless, the reason for mining is that if you solve the calculation problem faster than anyone else and writes the transaction history in the blockchain, you will get bitcoins as a reward. To put it a little more accurately, a new bitcoin is issued and sent to you. This is referred to as mining as compared to the mining of gold in mines. The reason why you can get rewards is that you have to keep the computer running for a long time to solve the calculation problem, and the electricity bill will not be a fool. If you don't have a reward (if you can't expect it) then no one may mine. There is a controversy about this part, but I will keep it from this topic as the topic gets further away from Kokorobakari. By the way, the idea of giving a "calculation problem" and deciding one person is not the original idea of Satoshi Nakamoto (2) (3).

2.3 SHA-256 and Nonce

The blockchain in Bitcoin adopts the "SHA-256 + Nonce" method as the "calculation problem" described above. These are explained on various websites and books, so we would like you to refer to them. Also, the story of SHA-256 and Nonce is not the essence of a blockchain. The essence is to decide "one person". And there is SHA-256 and Nonce as one of the decision methods, and it is a story that Satoshi Nakamoto adopted it. we think that. If you make a mistake, please point out.

2.4 Blockchain without Mining?

In Bitcoin, the difficulty of calculation is adjusted so that it takes about 10 minutes to go. If there are people who finish the calculation early, the difficulty of the calculation will be raised. Since mining takes about 10 minutes, there is a time lag between the occurrence of a transaction and the recording of the transaction in the blockchain. Bitcoin cannot be used for transactions that do not like this time lag.

By the way, the question of why “10 minutes” is raised in Bitcoin comes out. Unfortunately, I could not find the ground for 10 minutes. It is likely that people will raise hands at the same time as it is a minute, and if it takes 60 minutes, it will take too long to confirm the deal, so maybe it was decided that it was about 10 minutes.

So there are blockchains in the world that are singing fast trading. Some of them don't mine. As for how you decide one person "earning first" without mining, there is a tricky. The trick lies in the total number of computers that store a blockchain.

With Bitcoin, the total number of computers storing the blockchain changes from day to day. This is because anyone can participate in the Bitcoin network. On the other hand, in blockchains that do not mine, the total number of computers that store the blockchain is predetermined. If the total number of computers storing data is known in advance, there seems to be a way to determine one. For example, there is an algorithm called Paxos, but it is too difficult for us to understand.

After all, blockchains that do not mine cannot change the number of computers that store the blockchain. The question is whether to use blockchains with mining or blockchains without mining, but Kokorobakari's topic goes off, so I hope we can discuss that point on another occasion.

2.5 Overview of DApps

Kokorobakari is an application that runs on smartphones, etc., but the core part is DApps that runs on the Ethereal blockchain. DApps is an abbreviation of Decentralized Applications and is sometimes referred to as Dapps or dApps. It is common at this time to use Solidity, a proprietary programming language for Ethereum, to develop DApps that run on Ethereum. Also, Ethereum is one of the many cryptocurrencies as the Bitcoin. Ethereal is used because only the transaction information can be stored in the bitcoin blockchain, while applications (programs) and variables can also be stored in the Ethereum blockchain. Even the Bitcoin can save small programs in a blockchain, but they can not save complex programs.

For example, the following functions are convenient as a programming language for DApps development.

- The connection to the blockchain can be described simply
- Remittance on the blockchain can be described simply
- Access to variables on the blockchain can be described simply
- The setting of access authority can be simply described for the variables on the blockchain.
- Description using object orientation is possible

As a language corresponding to the above, Ethereum provides a programming language called Solidity. Several books (4) (5) have been published on Solidity, so please refer to them.

After writing source code in Solidity, use the solidity compiler to generate executable files or DApps. Compiled files are written into the blockchain. The end user will then invoke and execute DApps on the blockchain.

We will explain using Figure 1 because we think that normally you cannot understand even if it is said to call DApps on the blockchain and execute it.

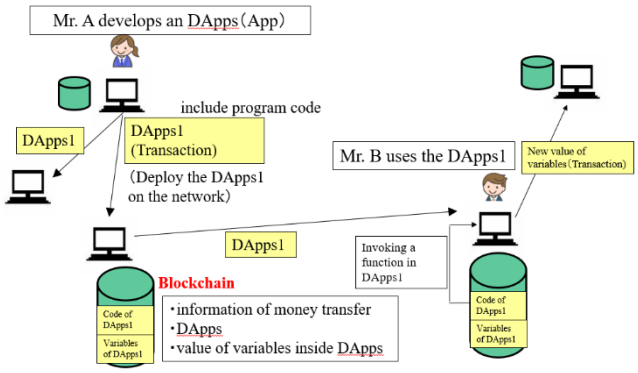

Figure 1　Deployment and Invoking of DApps

Figure 1 shows that Mr. A develops DApps and Mr. B uses that DApps.

Mr. A writes DApps1 compiled using Solidity compiler into the blockchain. At this time, DApps1 is transferred to computers in the world storing the blockchain. In Figure 1, DApps1 is transferred to Mr. B and written on the blockchain held by Mr. B. As mentioned in Section 2.2, Mr. B does not have to save the entire blockchain.

When Mr. B executes DApps1, Mr. B starts DApps1 on the blockchain. The method of activation will be described later. As a result of activating DApps1 and using DApps1, when a value of a variable in DApps is changed, the variable and the changed value are written on the blockchain. Of course, the change is propagated to computers around the world storing the blockchain.

Since the execution results are stored in the blockchain, computers around the world connected to the Ethernet network execute DAapss1 and compare the results with Mr. B's results. For example, Mr. C executes DApps 1 for checking, and if the result is different from Mr. B, it is assumed that Mr. B has made something wrong, and Mr. C discards the data. As a result, incorrect results are not propagated on the network. It's useless to run the same DApps on every computer on the network, but I'll keep my eyes on it.

After that, programming terminology comes out for a while. If you can not understand the contents, please move to Chapter 3 Kokorobakari. There are no particular obstacles to understanding Kokorobakari even if you move.

For example, consider a name list as an example of data rewritten from the outside. For example, if roster data is described as an array of structures in a DApps, the array data is stored in the blockchain including the array data. And when adding data to roster data, add the data onto the blockchain via the DApps. Note that it doesn’t always mean new values can be written on the blockchain for all variables in DApps. Which variables can be rewritten externally is set in the DApps source code.

So far, we have described the distribution and execution of DApps roughly, but we think there are still questions. Do GUIs (Graphical User Interfaces) also be written in DApps and stored on the blockchain? That is the point. In the case of Ethereum, data can not be written on the blockchain for free at this time. In the case of FIG. 1, Mr. A who is the distributor of DApps 1 needs to pay some cryptocurrency (Ethereum) to distribute DApps on the blockchain. This is called "gas" in Ethereum. Moreover, the larger the writing size, the more gas is required. For this reason, distributing large DApps, including GUIs, on the blockchain is not a good idea at this time. So, what to do is usually write the GUI part using JavaScript etc, and place it on a normal local disk

instead of the blockchain. On the other hand, Solidity describes only the data that you want to manage on the blockchain and the program that manages that data and puts it on the blockchain. The situation is shown in Fig.2.

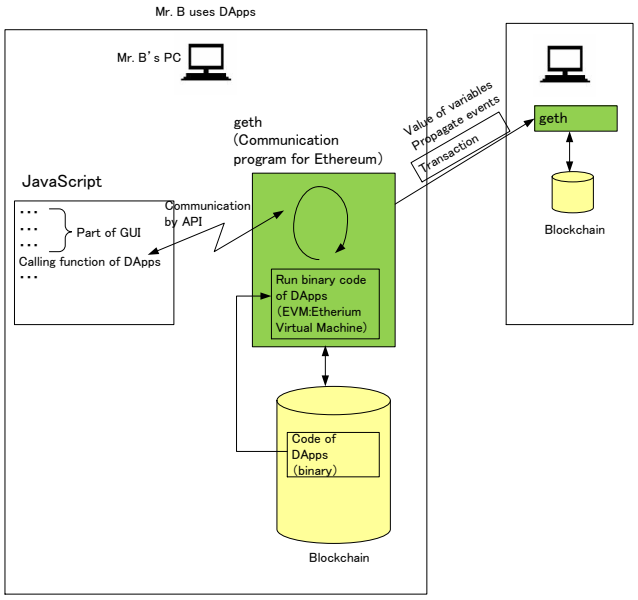

Figure 2　JavaScript and DApps

Figure 2 shows Mr. B using DApps. Mr. B first starts the GUI described in JavaScript. Then launch DApps from the menu on the GUI. On B's computer, a program called geth (Go Ethereum) is always running, and it accepts block data sent from an adjacent computer. If you want to join Ethereum, you only need to install the geth on your computer. Depending on the setting, geth also performs mining. By the way, geth is an abbreviation of Go Ethereum, but Go means Go language. The Go language is a programming language developed by Google.

When DApps is launched, binary code (compiled program) of DApps stored in the blockchain is executed by EVM (Ethereum Virtual Machine). This is similar to Java's intermediate byte code being executed by the JVM (Java Virtual Machine). EVM is not stored in the blockchain but exists in the geth.

The person who needs to pay for gas is not only Mr. A who distributes DApps. When Mr. B executes DApps, he rewrites the data in DApps and stores the data in the blockchain, so he still needs to pay gas.

Actually, it is necessary to understand the following keywords to develop and operate (use) DApps in Ethereum.

- MetaMask
- Truffle
- Ganache

I will omit the details.

3. Kokorobakari

3.1 Overview of Kokorobakari

When visiting a tourist destination, people would like to scribble on buildings as evidence of the visit. In other words, visitors (tourists) want to leave footprints. Graffiti is considered to be a universal desire for humanity. However, it is forbidden to actually do graffiti on ruins or cultural properties.

In the virtual graffiti app Kokorobakari we are planning to develop, in order to meet such desires, the tourist took photos at visiting places, doodled on the photos, and the location information (GPS data) and photos taken Register a doodle picture as a set on the blockchain. we will call this a virtual graffiti. Of course, there may be no letters but only letters. Since graffiti is written into the blockchain, it remains semi-permanently. You also do not have to make a backup yourself. The first version of Kokorobakari plans to save only letters.

If the tourist clicks (taps) the corresponding place on the map application, and the location and the position information at which the picture was taken a match, a doodle picture is displayed on a smartphone or the like. In addition, when a tourist approaches the visiting place, a doodle picture is displayed on a smartphone or the like. Figure 3 shows the display image of Kokorobakari. Here is an example of leaving only letters as graffiti.

Figure 3　Image of Kokorobakari

We are also impressed by the journey. There are various types of impressions. The scenery impresses us, I am impressed by the hospitality, and the types of impression are different from one another. And we think that there are thanks at the end of the impression. Furthermore, one would like to express gratitude in some form. It is all the more so if you are impressed. Kokorobakari is an application that helps to express the "thank you" in the form of "only heart". Kokorobakari's "virtual graffiti" can both convey the feeling of "only heart" by remittance of

cryptocurrency.

3.2 Technical Issues

There are several issues to be solved in the development of Kokorobakari. For example, end users need to understand wallets. For those who are not familiar with cryptocurrency, it is difficult to understand the wallet concept. You also need to understand the secret keys needed to use the wallet and their storage. Until the concept of a wallet and the secret key becomes common general knowledge, it is necessary to make them invisible to Kokorobakari end users.

Another issue is how to secure the credibility of the recipients. Even if you think that you used Kokorobakari to donate to the art museum you are visiting, the donation destination may actually be a bad guy in the name of the art museum. It is a so-called fraud.

It is also a problem when storing large data such as images in a block chain. When storing large data in a blockchain, it is necessary to pay a large amount of "gas" described above. Also, the blockchain file itself is becoming huge, so it is not realistic at this point. In fact, the first version of Kokorobakari will save only letters (text) in the blockchain. However, with Ethereal, there is a possibility that large data can be stored, if a technology called Swarm is used. Swarm is a mechanism that divides large files into small pieces and distributes the divided files to each computer for storage. Similar to Winny, which was popular in Japan in the 2000s. By the way, Winny is still working.

It is also necessary to consider measures against graffiti, violent graffiti, crime etc. against public order and morals. This is not a story that is limited to Kokorobakari, but the same is true for ordinary SNS etc. Unfortunately, current blockchain technology cannot delete the data once written to the blockchain later. However, it is possible to hide certain graffiti from Kokorobakari. If a graffiti to be deleted is found, Kokorobakari hides the graffiti. Although various methods can be considered about the method of making it invisible, it omits here. It is also a problem of how to find the graffiti to be deleted, but AI technology is likely to be very active here. It is also possible that Kokorobakari checks in advance to prevent inappropriate graffiti in the first place. Since it becomes difficult to check for inappropriate graffiti if it includes images, sounds, etc. as graffiti data, there may be an idea that the graffiti should be limited to characters only.

3.3 Use case of Kokorobakari

Figure 4 shows an example of using Kokorobakari via a travel agency.

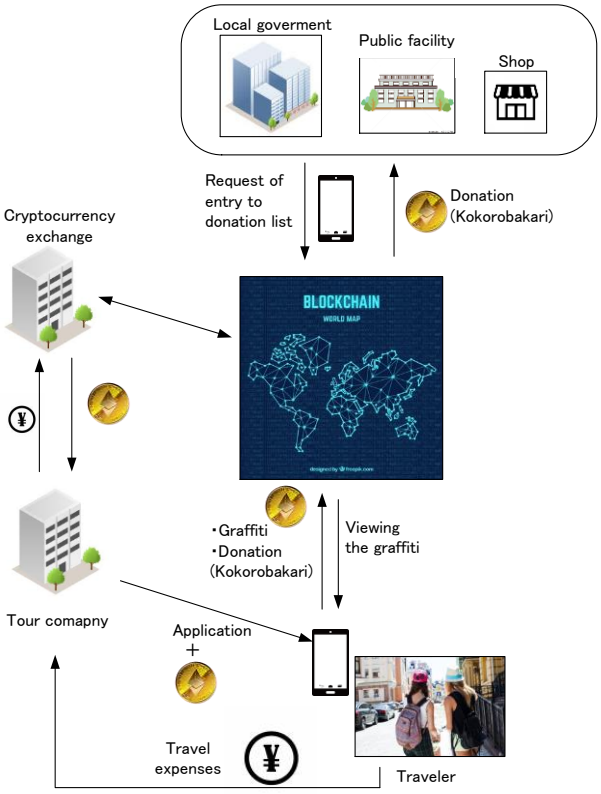

Figure 1 Usage of Kokorobakari via travel agency

The traveler pays the travel fee to the travel agency. The travel company converts part of the travel cost (for example, about 500 yen) into cryptocurrency and distributes it to the traveler along with the virtual graffiti application Kokorobakari. The traveler makes a donation within the cryptocurrency range distributed by the travel agency. This allows the traveler to hide bothersome things like wallets and secret keys. However, there is also the problem of how to handle the cryptocurrency that has not been used up. There are some ideas for this, but I will omit it here.

Of course, users who can manage their own wallets and private keys can also make donations from their own wallets. However, in this case, Kokorobakari needs to be linked with the user's wallet.

On the other hand, people who want to donate, such as local governments, public facilities, and stores register themselves in the donation list in advance using a smartphone. When they register themselves, they will also register their addresses. The address here is not an e-mail address, but an address on Ethereum.

If a travel company could use Kokorobakari exclusively, it could lead to a major differentiation from other travel companies. This is just an example. Of course, Kokorobakari could be open source, and people around the world could use it freely.

4. The possibility of Kokorobakari

Kokorobakari can be used not only in ordinary tourism but also in the mountains and the sea. For example, a scene where you visit the middle of the Pacific Ocean, pick up big fish, impress them, and donate them to conserve marine resources. In addition, you can see the middle of the Pacific Ocean with Google maps etc. while staying at home, and you can see your graffiti and the graffiti of others in it as it expands gradually, and it remains semi-permanently. We think it is interesting to see new discoveries and encounters by looking at them. In addition, as not only longitude and latitude but also altitude can be recorded as position information, you can also use the altitude and depth of the sea for graffiti search. Alternatively, if Pokemon go and Kokorobakari can be linked, it may be possible to extend the game by connecting Pokemon's locality and donations to it.

Various ideas are likely to emerge around Kokorobakari ideas. We want to spread Kokorobakari as a traveler's platform to the world. If you introduce Kokorobakari to other people, you will be able to lively talk to everyone if it has many functions. Perhaps the most interesting point is that Kokorobakari can also be a platform for an unprecedented social system that connects people with compassion. It's an exaggeration, but it's a great app for things to talk to about. Also, some of the people who listened to Kokorobakari gave some nice comments such as:

“ I can not wait for Kokorobakari using a blockchain. It seems
that you can make any donation from "Kokorobakari".
- To the conductor of refreshing announcement in
a crowded train
-The roadside trees are beautiful. To city hall park green
Space section managing
-A nursery school child who always greets me. To the
nursery
In this way, it seems that "Kokorobakari" is likely to change the world.”

Kokorobakari is currently under development and is scheduled to be released at the end of December 2019.

References

1) Bitcon:A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf
2) http://www.cypherspace.org/hashcash/
3) Pricing via Processing or Combatting Junk Mail, Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings
4) Mayukh Mukhopadhyay, Ethereum Smart Contract Development(2018) Packt Publishing
5) 加嵜長門,篠原 航(2018) ブロックチェーンアプリケーション開発の教科書, Chapter 7 マイナビ出版