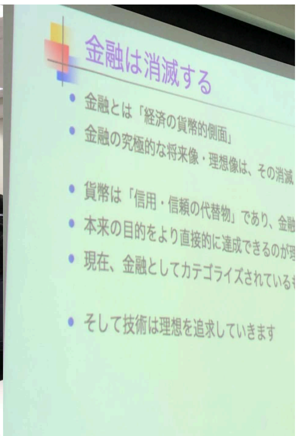
Todai Finance Innovation Program Lecture 13

The 13th lecture of the Todai Finance Innovation Program, which served as the final lecture in the technology series, was held at the Kojima Conference Hall at The University of Tokyo Hongo Campus on 5th December 2017. The theme for the lecture was “Blockchain and the Financial System”, with the timing of the lecture coinciding with the current surge in price of Bitcoin that has brought it to the forefront of financial news of late. We invited guest lecturer Dr. Kenji Saito, who currently lectures at Keio University’s Faculty of Environment and Information Studies while concurrently holding numerous other positions including Representative Director of Academy Camp, Chief Science Officer at BlockchainHub Inc. and CEO at Beyond Blockchain Inc. Dr. Saito after graduating from his Master of Engineering Program in Computer Science at Cornell University, has been performing research on digital currencies and P2P networks and is considered an expert in the field.

ブロックチェーン/DLT の現状
ブロックチェーン (主として「空中」はグローバル)
Bitcoin (ザ・ブロックチェーン)
Open Assets Protocol (OAP)
(ビットコインブロックチェーン上に任
Ethereum (分散アプリケーションのため
Enterprise Ethereum Alliance
その他の分散レッジャー (DLT) (主として「空中」は
Hyperledger (Linux Foundation)
Fabric (IBM/DAH), Sawtooth (Intel), Iroha (ソラ
などの開発が進行中
Corda (R3), Tangle (IOTA), BBc-1 (我々)
本当に記録の内容も存在も誰にも否定できない
記録の確かさを誰でも確認できると本当に言え


金融は消滅する
金融とは「経済の貨幣的側面」
金融の究極的な将来像・理想像は、その消滅
貨幣は「信用・信頼の代替物」であり、金融
本来の目的をより直接的に達成できるのが理
現在、金融としてカテゴライズされている
そして技術は理想を追求していきます

What is Blockchain and why did it arise?

Our current society relies on financial institutions such as banks to send money from one person to another. Although in Japan, people may not see why this is considered a risk, recently in countries such as India there have indeed been instances where notes have become void and people have been frozen out of their bank accounts. Due to the lack of trust in such existing systems, the digital currency bitcoin was created by an anonymous figure going by the name Satoshi Nakamoto to “make it possible to send the money you have now whenever you want and not to let anyone stop you from doing it.” Blockchain refers to the technology that was designed to send these bitcoin, and relies on the principle of sending digital coins using digital signature and pairs of public / private keys while maintaining public records of transactions. If you compare blockchain to a newspaper, 1 page of the newspaper is a ‘block’ and inside this block there are lots of articles. The blocks (pages of newspaper) are linked together to form a blockchain (the entire newspaper), and it is here where promises between two parties may be fixed. The reason that the system is operated by everyone is that if there was any one person in charge of operation, the service could be stopped at any time at his / her will.

Although the purpose of blockchain has already been touched upon slightly in the previous paragraph, broadly speaking it was designed to achieve the following three main goals:

⑴ To preserve and maintain records of content and their existence that cannot be denied by anyone

⑵ Anyone can check whether ⑴ is indeed being followed

⑶ Prevent ⑴ & ⑵ being stopped by anyone

It must be remembered that the 3 goals listed above are only aims and nothing more, in other words although blockchain was developed to fulfill the outlined goals, it does not necessarily mean that they are truly being fulfilled. Further details will be provided on the limitations of the current blockchain system later in the report, including lack of real-time usability (hence not suited for use in IoT devices), lack of scalability and lack of sustainability, which has led Dr. Saito to develop a new system to replace it called BBc-1 (Beyond Blockchain One).

Mechanism of blockchain – Beaker / Newspaper Analogy

The mechanism behind bitcoin and blockchain can be explained using a physical model comparable to obtaining liquid from a beaker and keeping records of exchanges of this liquid on a public newspaper. Firstly, let us say there is a central tank full with 21 million cm^3 (total supply of bitcoin) of a valueless liquid (i.e. bitcoin: no value on its own but has value for exchange), and each person wants to obtain some of this liquid for exchange purposes. Here, each person can have as many beakers as they want to hold their portion from the central tank, each of which can hold 1 / 100 millionth cm^3 of liquid (bitcoin). All these beakers are placed in a public space, and each person possesses lids for the number of beakers they own. The lids of the beakers have the name of the person who a person would like to send their liquid containing beaker to. Hence once the sender closes their beaker with a lid containing the name of their desired recipient, the beaker may now only be opened by that recipient using his / her private key.

So how do people obtain the liquid from the central tank in the first place? This is a random process that is not operated by anyone, where each person under the same conditions has a sort of raffle box of their own and draws from it at their own pace (although strictly speaking whoever can draw the fastest has an advantage). On average every 10 minutes someone gets a hit on the raffle and can obtain 12.5 cm^3 of liquid from the central tank and transfer it to the beakers that they own (Bitcoin Mining).

A few conditions exist for the model outlined above in order to make it functional. One important condition is that once a beaker is opened by a recipient using his / her private key, all of the liquid must be transferred to other beakers (i.e. not possible to keep some for later. This facilitates the accurate tracing of exchanges in liquid between parties). Furthermore, the people who succeed in the draw of the raffle (those who succeed in Bitcoin Mining) also serve as auditors and keep records of exchanges on pages of a public newspaper (proof of existence). In return for this, they receive the little amounts of liquid left clinging to beakers when transfers of liquid between beakers are made as a handling fee. Finally, if the same page number occurs twice in the newspaper (can occur if two people succeed in the raffle at almost the exact same time), the page that is part of the longer fork is considered to be valid (the reason for this will be explained later "The Nakamoto Consensus"). Bitcoin and blockchain are just things where the principles outlined in this physical model have been implemented digitally.

Major Issue with blockchain

People say that it is not possible to tamper with blockchain but this is not true as it is possible at a certain cost. The blocks in blockchain are linked together as each page includes the digest of the previous page at the page top (referred to as Cryptographic Hash Function Message Digest). Many people misunderstand that the long process to change each summary on subsequent pages is what prevents people tampering with records held in blockchain. However, in reality this can be performed in seconds. It is rather something called the "Proof of Work" that prevents this from being done easily. "Proof of Work" requires the creation of each digest so that it is below a particular 256-bit hash target. The smaller the hash target is, the harder it is for miners to obtain a fitting digest, and because this hash target is so small it is considered next to impossible to tamper with records stored in blockchain. It takes an average of 10 minutes for people to create one page (mining) with a digest that is below the hash target (for reference, altogether people are making 15,000 quadrillion draws of the raffle in the physical model described in the previous section per second). The key to successfully tampering with the records held within blockchain lies in taking advantage of the Nakamoto Consensus outlined below.

The Nakamoto Consensus refers to everyone following the fork that has been mined the most because it is logically the hardest to tamper with according to the methods mentioned in the paragraph above. However, from the perspective of computer science, The Nakamoto Consensus is not actually functioning as a consensus as if someone inputs a lot of cost so that they can edit the summaries contained on existing pages at a faster pace than the creation of new pages by miners (eventually catching up and creating new pages faster than current miners), it is possible to reverse the consensus and people will think the fork that the person has edited is the true fork. This is one of the major problems with the current blockchain system. At the same time, it is worth mentioning that there are technologies that are currently in circulation which are not even blocks nor chains, and are better than blockchain if they are properly designed. However, some Distributed Ledger Technology (DLT) utilizes hash chain but has no Proof of Work. This means that they can easily be tampered with and what is most frightening is the fact that such services are not uncommon. Therefore the utmost care must be taken when making a choice to utilize such services.

A system to replace blockchain: Beyond Blockchain One (BBc-1)

Given the shortcomings of the current blockchain system, Dr. Saito is currently involved in the development of BBc-1, which sets out to achieve what blockchain originally intended to do. Furthermore, it sets out to address the current major limitations of the blockchain system. For example, at present as mining succeeds at an average pace of once every ten minutes (in case of Bitcoin), the activity is stochastic so has no potential for implementation in real time (hence why not suited for IoT devices). In addition, blockchain lacks scalability (expand when needed by inputting cost, and decrease when not necessary) as it is a form of replication technology. Finally, there is presently no room for experimentation in blockchain. If you look at the evolution of the Internet, when people come up with a good idea they are able to test it first and if it goes well people adopt it, so there is a system set up where only the successful things get evolved. On the other hand, if you look at the case of blockchain, people interpret new additions differently and some miners may accept it while others may not, which can lead history to fork.

What the near future holds?

Currently the bitcoin price is going up rapidly, but it is a very dangerous position. If the price of bitcoin increases, the incentive for mining also increases, so miners will introduce more cost so that it is possible to draw the raffle faster and obtain more hits. This will lead to greater frequency of hits, so every 2016 blocks the hash target will be adjusted so the interval between hits is once again on average ten minutes, subsequently leading to difficulty getting harder. If while all of this is happening the price of bitcoin happens to fall, at some point the cost of mining may no longer match the incentive (profit) so people may stop mining resulting in a large increase in block intervals making Bitcoin harder to use. This could trigger a vicious cycle so that more miners will stop mining and the block intervals will get longer and longer, eventually causing the system to come to a halt. At present there are still many people buying bitcoin for investment purposes, but if these buyers were to disappear the above scenario could become a very real possibility. Furthermore, if the above scenario were to occur with other digital cryptocurrency systems such as Ethereum, the applications they are used for will also come to a stop.

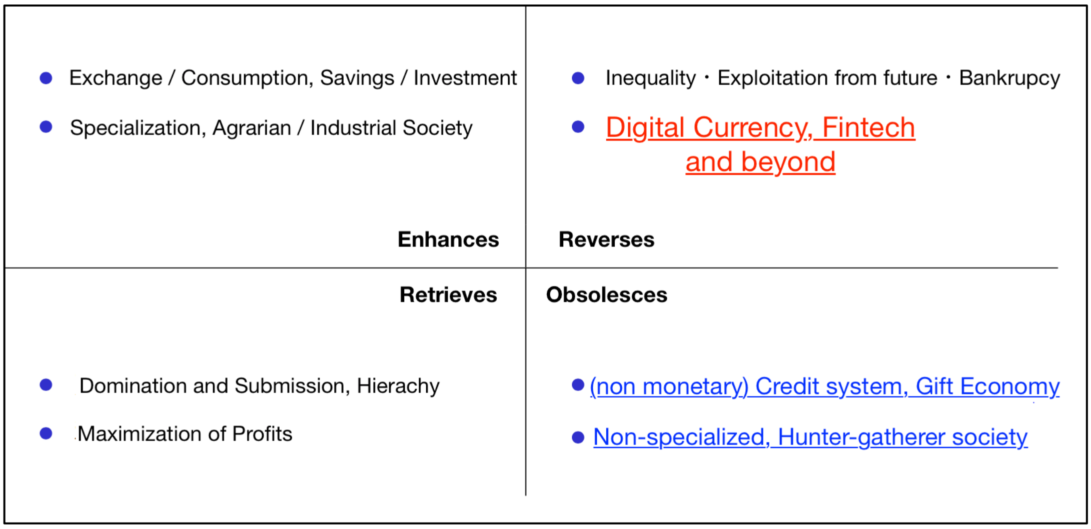
What the distant future holds?

Science fiction prototyping is a useful technique for showing how a particular technology you are developing may be used in society in the future. Dr. Saito believes that there is a real possibility that the monetary economy system will die out in the future and along with the financial system. The reason he gave for this is that they are both replaceable systems, in other words, if you can do what you originally wanted to do in the first place there is no need for them anymore. This means that the fading out of such systems becomes our ideal, and history has shown that technology advances towards achieving our ideals. The costs of production, distribution, and consumption will decrease so the things that an individual can do will increase (empowerment). In turn, the things an individual can perform without relying on the financial system will increase, so relatively the power of the monetary economy system will also decrease (embodied by the rise of the sharing economy at present). People often ask whether people will be willing to leave an industry that is so profitable and simply put the answer is yes they will. With the monetary system the only base principle is the pursuit of profits, so we will try to do things as cheap as possible. If we take this way of thinking to the extreme we will not use money at all in a sort of sharing economy that we are starting to see lately (although services such as Airbnb and Uber are currently being run by companies, technology will allow for this to be done independently).

Dr. Saito introduced the tetrad of media effects as a means of examining the effects on society of any technology/medium by dividing its effects into four categories and displaying them simultaneously. It was initially proposed by Marshall McLuhan and is based on asking the following four questions:

1) What does the medium enhance?
2) What does the medium make obsolete?
3) What does the medium retrieve that had been obsolesced earlier?
4) What does the medium reverse or flip into when pushed to extremes?

Applying this logic to the financial monetary economy system we obtain the following:



● Exchange / Consumption, Savings / Investment ● Specialization, Agrarian / Industrial Society **Enhances**	● Inequality・Exploitation from future・Bankrupcy ● Digital Currency, Fintech and beyond **Reverses**
Retrieves ● Domination and Submission, Hierachy ● Maximization of Profits	**Obsolesces** ● (non monetary) Credit system, Gift Economy ● Non-specialized, Hunter-gatherer society

(Translation of Lecture Slide 19)

Bruce Sterling released a science fiction work in 1998 called "Maneki Neko" which depicts Japan as a gift society with people following the orders of their phones that are connected to a series of other people who are all trying to do small acts for each other, to help each other out. Dr. Saito's prediction for the future follows a similar path to that of "Maneki Neko" in that people will no longer be conscious of the monetary economy and the change has already begun as seen with Amazon Go launched in Seattle in 2016. With Amazon Go, whatever people add to their basket automatically gets added to their bill, and any applicable coupons would be applied by the computer system so that customers no longer need to line up at registers, but more importantly their consciousness of the monetary economy is made thinner.

There are various digital currencies emerging, particularly on the national level so that governments can properly collect all the tax due, leaving people unable to hide their money and evade tax. However, Bitcoin has already shown that as long as the incentive of price increase exists, digital currencies serve little use as true stores of value. In this sense, the simple spread of E-money usage has the potential to bring about considerable change, as ATM's would become unnecessary and there would no longer be any need to pay handling fees.

Final Words

Since 2011 Dr. Saito has been organizing Academy Camp for children in Fukushima and has been working with primary and intermediate school children about new technology such as digital fabrication and deep learning. It includes activities such as scanning other people's bodies and printing them using 3D printers and constructing an AI that identifies things as either cats or dogs. People tend to forget that it is these children that will be responsible for the financial and social systems of the near future, so we must involve them from an early age, and not just discuss things between adults. In that sense, Sweden is highly advanced and the education system there teaches kids that they are the ones responsible for thinking about and creating the rules for society.

The second point Dr. Saito emphasized was that although there has been much discussion about who should be responsible for accidents caused by self-driven cars and such, at the end of the day these are all problems of ethics and we humans must be the ones to decide between what is acceptable and what is not. AI is only there to implement these decisions for us. For example, there is the classic example of the trolley problem where the brake on a trolley is broken, and it is moving forward on the track, and you are by the point adjuster of the track. If you don't do anything 5 people will get run over, if you adjust the track point then 1 person will get run over. What should you do? Therefore, we must remember that such problems of ethics are problems that can only be solved by humans and should not place this responsibility on AI.