Klaytn Improvement Reserve: Project Proposal

Date: 2021.06.01

Summary

As the great success of Klaytn blockchain, the variety of blockchain applications(Bapps) provide their services on Klaytn token economies. KLAYSwap, the most representative case of them, has announced the swap protocol for Klaytn DeFi and built their own ecosystem named KSP tokenomics based on the Klaytn token economy. It is continuously growing the number of token economies of Klaytn and the volume of their transactions. This means that the token economies are not the tiny parts of the blockchain network anymore, and we need to consider that the tracking of token-related assets is essential to trace all financial transactions of the blockchain without any exception.

We have presented the high-performance development environment for the on-chain analysis of Klaytn mainnet in the previous project. Above and beyond that, we implement an analysis framework for Klaytn token transactions and release public web services to deploy such analysis frameworks. Our main goal for this project is providing a set of web applications to any one of the users to inspect the Klaytn mainnet transactions and token transfer flows for any purpose. Through the public web service we would support, the user could retrieve the transfer flows of all tokens and even refers to the mainnet transactions over the token economies.

In addition, we design the system to find abnormal transactions of the blockchain network. As some prioning studies, the majority of abnormal transactions of Ethereum blockchain was conducted by exploiting the vulnerabilities on token contracts. Also, common money laundering services use some token swap protocols to wash the black money. In this project, we first carefully scrutinize those kinds of well-known abnormalities of several cryptocurrencies and try to patternize their transaction behaviors. Then, we would look for the similarities and differences between those patterns and existing Klaytn token transactions.

Team (Individuals, Corporation) Introduction

S2W LAB[1] is a big data intelligence start-up specialized in Dark Web and Cryptocurrency analysis. We captured a massive amount of Dark Web data and established a Dark Web database. In the process of database establishment, natural language processing techniques are used to find links among multiple domains and among multiple time frames. The Dark Web data is analyzed by a unique AI-based multi-domain analytic engine. In the process of database establishment, natural language processing techniques are used to find links among multiple domains and among multiple time frames. We offer two main solutions, S2_XARVIS and S2_EYEZ, to clients. S2_XARVIS is a threat intelligence solution and S2_EYEZ is an AML(Anti Money Laundering) solution for cryptocurrencies.

With our unique solutions, S2W LAB is currently serving several clients in Dark Web analysis and Cryptocurrency tracking. Our main clients include intelligence agencies, Interpol, Military, Security agencies, and cryptocurrency service providers.

S2WLAB team

Since its establishment, S2W LAB has continuously recruited cyber security/data analysis specialists and has secured a large number of master/doctoral level R&D and analytic specialists. For this project, we will arrange five of the experts from S2W LAB who are best suited for this project.

Position	Name	Main career
Privacy		University of Michigan, MBA KAIST, B.S. Electrical Engineering Desire Lab, CEO
Privacy		Texas A&M University, Ph.D. Network Security KAIST, Associate professor (tenured)
Privacy		KAIST, M.S./Ph.D. Information Security Publish the cryptocurrency analysis paper in the top security conference *[NDSS'19]*
Privacy		KAIST, M.S. Information Security Expertise in big data analysis
Privacy		Korea Internet & Security Agency, Personal Data Protection Group Expertise in blockchain networks

[1] S2W LAB INC., https://en.s2wlab.com

Motivation

Recall from the previous KIR project of ours, we have presented the system to provide the analysis services of financial assets on Klaytn mainnet. The system has achieved the goal of efficient and effective analysis of blockchain data through a high-performance graph cache data system. The analyzer could obtain the graph format of Klaytn mainnet data as a result of our abstracted API calls. However, there is a limitation due to mainnet.
Although the Klaytn ecosystem has its own token economy, the graph of the blockchain we built has only had mainnet data. Thus, our system could not trace beyond the mainnet to the token economy. For instance, when someone transfers her tokens to the any other one, it is written on the Klaytn mainnet blockchain that she sends zero klay to someone she want to send(actually, the address of specific smart contract). The information of transferred assets(i.e., the amount of tokens) is located on the internal transactions of its mainnet transaction.
Therefore, malicious or any other purposes, anyone could hide their assets from our analysis system by using token transfers. To provide the concrete analysis result, we need to expand our system over the Klaytn mainnet to token economies.

There are several reasons why the inspection of token transactions is essential.

1. Explosive growth of tokens
   For the last few years, the token ecosystems of crypto currencies have achieved a noticeable increase of both the volume and the number of times for financial transactions. As a result, the volume of Ethereum token transactions exceeds that of its mainnet. In this situation, when it comes to tracking the assets of the blockchain network, careful analysis of its token economies is significant as much as the mainnet. The Klaytn is not an exception and thus, the Klaytn token economies repeat sudden rise with the continuous growth of its mainnet.

2. Malicious use of tokens
   Various blockchain applications bring the opportunity to open new kinds of brightness services. However, the adversaries gaze at those trends in their own ways and exploit the things. This means that the token economies are also vulnerable to new kinds of cyber attacks on cryptocurrency networks.
   For instance, the flash loan attack exploits vulnerabilities on DeFi applications to get margins. In the case of bZx, the adversary has utilized several digital assets including ethereum, USDC tokens and WBTC tokens to launch the attack. One of the other cases, in Harvest finance, the attacker uses USDT and USDC tokens. The thing is that this kind of attack needs only a single transaction on the mainnet during the entire attack process even if it requires many times of transactions. The details of the attack procedure have moved onto the floor with the token transfers and internal transactions of it.
   Therefore, to deal with security threats on the blockchain, the methods to scrutinize token transactions over the mainnet become an indispensable part of the blockchain network.

3. Anti-Money Laundering(AML) mechanisms
   The wide variety of services on the blockchain for black money are one of major threats on cryptocurrency ecosystems. In general, the majority of black money entered into the cryptocurrency ecosystem has transformed into white money and goes out. The black money went through the transformation of several types of digital assets including mainnet and token assets in the money laundering. That is, we could find out such abnormalities on the blockchain network by analyzing transfers of cryptocurrencies all together including tokens.

Also, the current version of S2_EYEZ for Klaytn provides only a set of APIs to analyze Klaytn transactions and it has a limitation to provide clear visibility of transactions to users. Thus, we would like to make the S2_EYEZ system a more user-friendly form by providing our services as a format of web application.

Therefore, as a long-term contributor to the Klaytn ecosystem with continuous growth, we believe that providing analysis mechanisms for token transfers would help the success of the Kalytn network by making that more secure.

Project Description

Summary of our previous KIR project.

In our last KIR project, we have proposed an on-chain analysis framework specifically focusing on financial transactions of Klatn blockchain. The system provides a well-structured development environment for implementing a wide range of on-chain analysis applications. However, there are two limitations on the S2_EYEZ for Klaytn.

- Lack of internal transactions
  Basically, the S2_EYEZ supports the analysis of external transactions of Klaytn blockchain only. It could not track the financial flows on internal transactions of Klaytn and thus, token transfers are not visible to the system that only affects mainnet transactions. Thus, in this project, we propose an analysis framework for Klaytn token economies and address various technical issues about Klaytn token transactions..

- Hard to use
  Our system is not user friendly. We deliver our services as a format of development environment. Thus, communicating with the system is not hard to application developers who want to implement their own functionalities on the Klaytn blockchain. To maximize aims to contribute to Klaytn ecosystem, we would like to provide intuitive interfaces for anyone interested in Klaytn network.

The scope of key contributions of this project in comparison with our previous KIR project is as below.

	Base Networks	**Users**	**Delivery Methods**
S2_EYEZ in former	Klaytn Mainnet	Application Developers	Development Environments
S2_EYEZ for now	Token Economies	Anyone on the Internet	Public Web Services

System design

Now, S2_EYEZ supports tracking the financial assets on Klaytn mainnet. Token economies already have a huge impact on the Klaytn ecosystem as much as its mainnet and it would be increased from now on with the further success of Klaytn. In this project, we want to expand our services over the mainnet to token economies and by doing so, we believe that S2_EYEZ could contribute to make the Klaytn more secure.

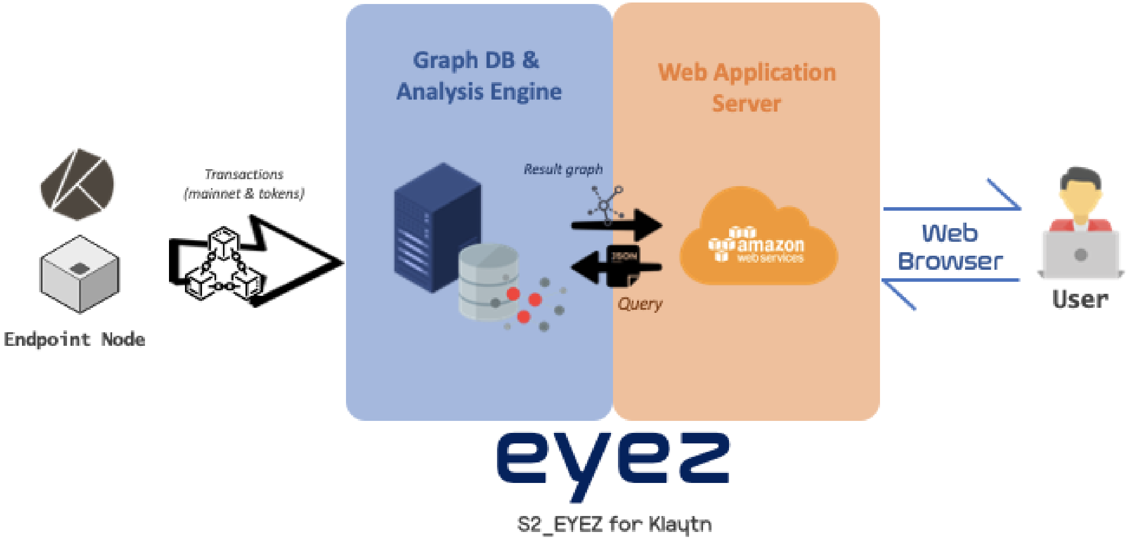


Figure 1. S2_EYEZ design for Klaytn token economies

The abstracted system architecture of S2_EYEZ for token economies is shown in Figure 1. The system provides web services to users with two subsystems, a blockchain node and a EYEZ framework.

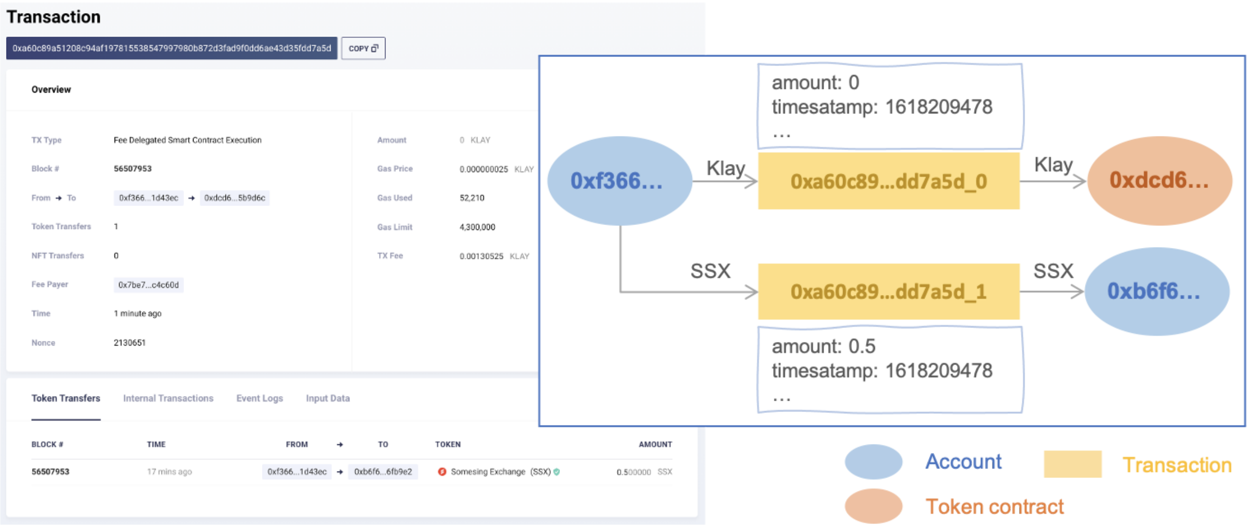
During the set-up period, the S2_EYEZ extracts the entire internal transactions of the Klaytn blockchain and stores it as a format of graph data to get the token transfers. It's not a short-term operation but it requires it to be done just once for the whole lifetime. After successfully launching the system, the S2_EYEZ collects the latest block information whenever a new block on Klyatn is generated.

The EYEZ core framework has two submodules, graph cache system and web application server. The graph cache system builds the Klaytn transactions as the format of graphs and it runs a graph-based analysis engine specially designed for blockchain data. The web application server publicly provides web services to users to communicate with the blockchain data(i.e., token transfers). When the user requests come to the server, it sends a graph search query request to the graph cache and responses to the requests with the query result data.

We can get an accomplishment of our goal through three main parts of this project:

Building the token transaction graph.

Basically, S2_EYEZ deals with blockchain data as the format of graph representation to trace the flow of financial assets efficiently. We have designed that the system constructs and maintains a single unitary graph for all token economies apart from the mainnet. This made the system easily trace the token transfers from one to others such as token swap.
Also, we extract token transfer data from the event logs of blockchain. The smart contracts which are abided by KIP-7 and KIP-17 utilize a set of transfer functions depicted in the protocol to transfer tokens from one to another. From the logs, we gather valuable information we need to track including related addresses and the amount of transferred tokens for every single transaction. Finally, the extracted token transfer data will be reformatted as a graph representation, nodes and edges.



Transaction

0xa60c89a51208c94af197815538547997980b872d3fad9f0dd6ae43d35fdd7a5d

Overview

TX Type: Fee Delegated Smart Contract Execution
Block #: 56507953
From → To: 0xf366...1d43ec → 0xdcd6...5b9d6c
Token Transfers: 1
NFT Transfers: 0
Fee Payer: 0x7be7...c4c60d
Time: 1 minute ago
Nonce: 2130651

Amount: 0 KLAY
Gas Price: 0.000000025 KLAY
Gas Used: 52,210
Gas Limit: 4,300,000
TX Fee: 0.00130525 KLAY

BLOCK #	TIME	FROM	→	TO	TOKEN	AMOUNT
56507953	17 mins ago	0xf366...1d43ec	→	0xb6f6...6fb9e2	Somesing Exchange (SSX)	0.500000 SSX

amount: 0
timesatamp: 1618209478
…

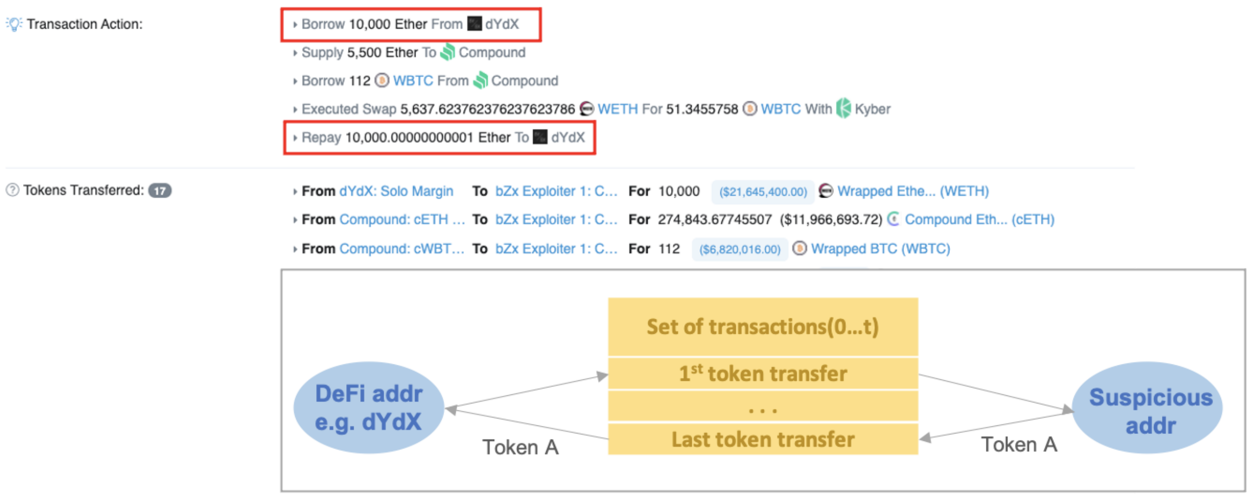
amount: 0.5
timesatamp: 1618209478
…

Figure 2. Abstracted description of graph construction example.

Figure 2 describes the example of building token transfer graphs. The transaction has a single token transfer beside a mainnet transaction as a zero klay transmission. In this case, we make three address nodes including two for wallets and one for a token contract. Also, there are two transaction nodes, one for mainnet and another for a token transfer. Each node of transactions has a unique identifier as the combination of a transaction hash value and a numeric index. We assign zero as an index value for the mainnet transaction and the numbers in order from one to many for token transfers. Some additional information about transactions such as tx fee and gas limit are stored in the external file database system for further analysis. Also, the type of transferred token is indicated as a property of each edge.

Searching out abnormal transactions.

If we could patternize the abnormal transactions, then we can disclose other unknown abnormalities by measuring the similarity between any other transactions and the patterns we built.



Transaction Action:

- Borrow 10,000 Ether From dYdX
- Supply 5,500 Ether To Compound
- Borrow 112 WBTC From Compound
- Executed Swap 5,637.623762376237623786 WETH For 51.3455758 WBTC With Kyber
- Repay 10,000.00000000001 Ether To dYdX

Tokens Transferred: 17

- From dYdX: Solo Margin To bZx Exploiter 1: C... For 10,000 ($21,645,400.00) Wrapped Ethe... (WETH)
- From Compound: cETH ... To bZx Exploiter 1: C... For 274,843.67745507 ($11,966,693.72) Compound Eth... (cETH)
- From Compound: cWBT... To bZx Exploiter 1: C... For 112 ($6,820,016.00) Wrapped BTC (WBTC)

Figure 3. Transactional behavior pattern of flash loan attack.

As an example, Figure 3 shows the transaction actions about one of the famous attack cases on the blockchain called the flash loan attack. We could find an unique behavior of transaction patterns to conduct the attack from the careful analysis of the attack. As you could see from the figure, this attack starts from to borrow WETH tokens from a defi service provider and be completed to repay such WETH tokens to the defi.

Let's bring the actions to the graph architecture of S2_EYEZ. With the graph representation, we could figure out significant characteristics of the transactions easily. In this example, the first and last token transfers are made by the same two addresses which have an exactly opposite role of sender and receiver. In addition, the amount of transferred tokens is also certainly the same as each other.

In this project, we will define as many as behavior patterns of token transfers from the existing transaction samples and then implement an analysis framework to detect those patterns on Klaytn token economies.

Public web services for tracking digital assets of Klaytn networks.

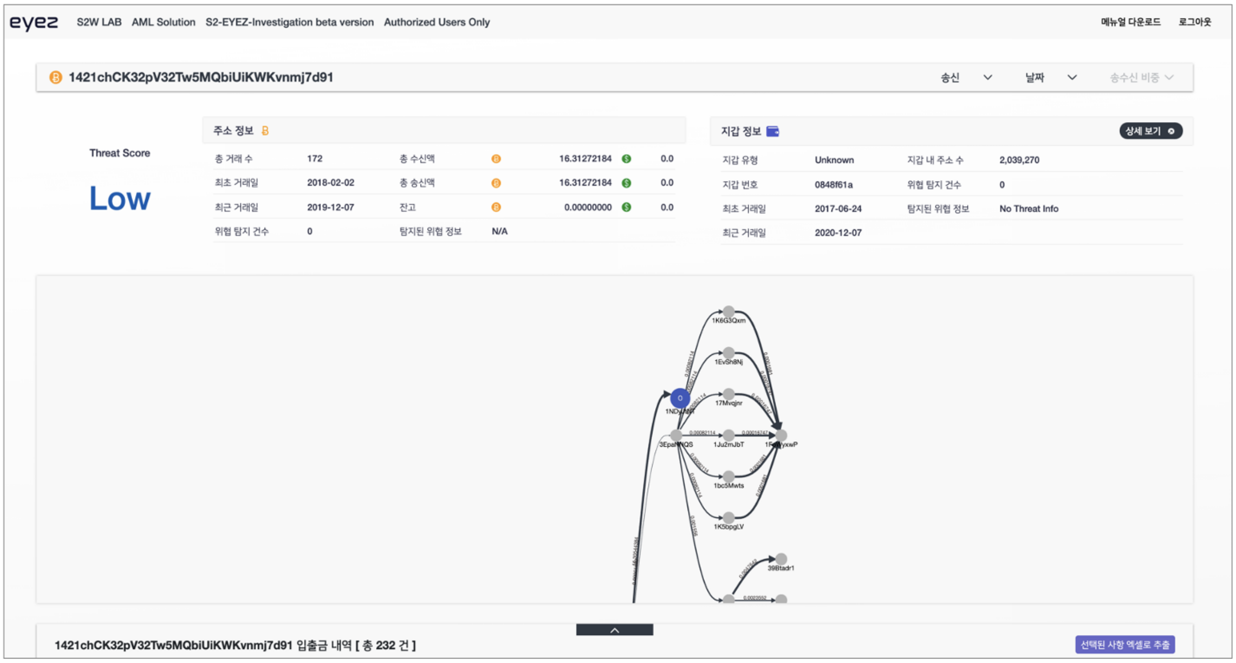
We plan to release public web services to explore Klaytn transactions including both maintnet and token economies. The user tracks the transfers of Klay and tokens starting from an address she wants to inspect through the web services. Also, it is possible to observe only relevant transactions by setting some parameters such as transaction timestamp, hop limit and amount limits to provide well-refined graph data as a result. The web application also provides the basic information of an address such as balance.

One of the other meaningful web applications is the graph traverse function which starts from a specific transaction. This would be good for the two or more correlated token economies, especially about the transaction across Klay transportation on the mainnet. And then, the internal behaviors such as token transfers are located in the transactions of token economies. There is no guarantee that the wallet address on the mainet will appear on the token economies too. The only thing to connect the mainnet to other token networks is a transaction hash value because every internal transaction has an exactly same hash value with their mainnet transaction with an incremental index. Thus, we would traverse the token transfer graph starting from a specific transaction hash for the correlational analysis between the mainnet and token economies.

The following table shows the abstracted description of our web applications. We plan to develop four main applications on the Klaytn mainnet and token economies respectively.

Application	Cypress	Token Economies
Address Information	The basic information of an address. - klay balance - first/last tx time - the number of txs - etc.	The basic information of an address. - token balances - first/last token transfer time - the number of token transfers - etc.
Transaction Graph	Deposit/withdrawal transaction graph starting from an address.	Deposit/withdrawal token transfer graph starting from an address or a tx hash value.
Shortest Path	The shortest path information between two addresses on the mainnet transaction graph.	The shortest path information between two addresses on the token transfer graph.
Abnormal transactions	Analysis about abnormal transactions on the mainnet.	Analysis about the abnormalities of token transfers.

At this moment, we are already operating web applications to track digital assets on the bitcoin network as a private web service for some korean secret agency. Below is one of the web pages from our private web applications. When a user enters a bitcoin address into the system to analyze, the system provides an analysis result as a format of graph including relational transactions and also basic information of an address such as cluster data, the number of transactions and threat score. We would like to serve useful analysis applications for Klaytn mainnet and token economies like the way of ours for bitcoin.



₿ 1421chCK32pV32Tw5MQbiUiKWKvnmj7d91

Threat Score

Low

주소 정보 ₿

총 거래 수	172	총 수신액	₿	16.31272184	$	0.0
최초 거래일	2018-02-02	총 송신액	₿	16.31272184	$	0.0
최근 거래일	2019-12-07	잔고	₿	0.00000000	$	0.0
위협 탐지 건수	0	탐지된 위협 정보	N/A			

지갑 정보

지갑 유형	Unknown	지갑 내 주소 수	2,039,270
지갑 번호	0848f61a	위협 탐지 건수	0
최초 거래일	2017-06-24	탐지된 위협 정보	No Threat Info
최근 거래일	2020-12-07		

1421chCK32pV32Tw5MQbiUiKWKvnmj7d91 입출금 내역 [총 232 건]

선택된 사항 엑셀로 추출

Project Milestones and Schedule

Date(MM/DD)	**Project**	**Details**	**Criteria**
07/01-**08/31**	Design/ Implement	- Conduct preliminary research on Klaytn token economies to figure out technical requirements for the project. - Implement an initial prototype of S2_EYEZ for Klaytn token economies.	**[Milestone #1]** * Technical report on the details of framework design for kalytn token economies.
09/01-**10/31**	Implement/ Measurement	- Define functional specifications about general or specialized purposes of token economies. - Find out unknown abnormal transactions from the Klaytn blockchain. - Performance evaluation of the web applications.	**[Milestone #2]** * Technical report on the details of abnormal transactions of Klaytn.
11/01-**12/31**	Deployment/ Operation	- Deploy a S2_EYEZ framework instance to support publicly available web services to users.	**[Milestone #3]** * Public web service of S2_EYEZ for Klaytn token economies.

Key Deliverables

There are two main outputs of this project as follows.

1. Web services
   We plan to publish an open web service to any of users have interested in the analysis of Klaytn blockchain network. Our web service would include two main analysis regions(i.e., cypress and token economies) and each region has several functionalities.

   - Mainnet

Function	Description	inputs	outputs
Address information	Providing the basic information of an address.	An address.	The basic information of an address such as balance, transaction time.
Transaction flow tracking	Providing the details of deposit or withdrawal transactions of an address.	An address.	A relational graph of deposit or withdrawal list starting from an address to addresses three-hop far away.
Relational analysis	Figuring out the relational transaction path between two addresses	Two addresses.	The path from an address to another as a graph format of data.

   - Token Economies

Function	Description	inputs	outputs
Address information	Providing the basic information of an address.	An address, token types.	The basic information of an address such as token balance, token transfer time.
Transfer information	Providing the details of token transfers belong to a transaction.	A transaction hash value, token types.	The detailed information of token transfers such as transferred amount, token symbol.

Token transfer flow tracking	Providing the details of deposit or withdrawal token transfers of an address.	An address, token types.	A relational graph of deposit or withdrawal token list starting from an address to addresses three-hop far away.
Relational analysis	Figuring out the relational token transfer path between two addresses	Two addresses, token types.	The token transfer path from an address to another as a graph format of data.
Abnormal pattern matching	Reveal the malicious transactions related with an address	An address	The information discovered abnormal transaction patterns of an address.

2. Technical report

The technical reports we would publish include kinds of research materials about token economies and web application specifications to refer Klaytn blockchain data for analysis purposes. To achieve the goals of this project, we design the system architecture specialized for the analysis of token economies. Basically, the system consists of a graph database and an analysis engine and these are quite different from the analysis system of other domains, even Klaytn mainnet.
For instance, in the mainnet, there is only a huge single transaction graph with klay transactions. However, the token transfer graph consists of multi graphs with several token types. Also, token transfers triggered by a mutual transaction could have the same transaction hash value with different indexes in contrast to each mainnet transaction having a unique hash value. The details about our system including those kinds of design considerations are described in the technical reports.

Aside from the basis of transaction analysis, we maintain our focus on the need of abnormal detection on blockchain networks. In this regard, the technical report we would publish includes kinds of research materials about abnormalities on Klaytn transactions. At first, we would like to patternize the transactions generated by well-known abusing cases. Then, we build each one of those patterns as a graph format of data and it will be listed up. From the patterns we defined, we will try to find out any unknown abnormalities from all existing transactions on the blockchain. This would be done by conducting a pattern matching algorithm specially designed for blockchain data on the Klaytn transactions from head to toe.

Budget

The project price consists of i) product implement & development fee, ii) server rental fee and iii) operating and maintenance fee. Engineers participating in this project are in charge of implementing S2_EYEZ for Klaytn token economies and deploying an analysis framework to provide public open APIs to Klaytn forum users. Also, a server rental fee is required to develop and operate the framework. The licensing (operating and maintenance) fee is mostly charged to resolve any issues from the users as well as provide technical support.

1. **Product development & maintenance fee**

Task	Weekly wage	No. engineers	Estimated weeks	Total
Development & Maintenance	$5,000 per engineer	2	16	$160,000
Testing & QA	$5,000 per engineer	1	4	$20,000
SUM				$180,000

S2W LAB charges $5,000 per engineer-week applied to three engineers participating in development, and testing periods. $180,000 in total will be charged to accomplish implementing S2_EYEZ for Klaytn token economies and providing research findings as a format of technical report.

2. **Development & deployment server fee**

Specification (Amazon EC2)	Price (seoul)	No. nodes	Price sum (6 months)
c5.4xlarge (Cypress EN node)	0.68 USD/hour	1	$2,978
r5.24xlarge (framework core)	6.048 USD/hour	2	$52,980
m5.large (web application server)	0.096 USD/hour	1	$420
SUM			$56,378

* Server rental fee is charged for *6 months*.

3. **Product licensing fee: S2_EYEZ Basic* for token economies**

No. of requests (per month)	Flat rate
Price (USD)	$10,000

* S2_EYEZ Basic includes the *top 10* token economies of Klaytn.

S2W LAB offers a flat rate licensing fee, which is a special pricing model for contributing Klaytn ecosystem. The license under the flat rate provides unlimited access to open APIs as well as all features without any additional charges. *All APIs with full features are publicly open to Klaytn forum users who want to use transaction analysis functions or build their own custom applications under the blockchain analysis framework.* The fee mostly includes an operating cost and maintenance efforts to resolve any issues and provide technical support to the users. The monthly licensing fee will be charged during the last two months in the project when a framework is available.

4. Total budget

Category	Budget	Remarks
Cost of labor	$180,000	6 months
Server	$56,000	6 months *(rounding down to $100)*
Licensing	$20,000	2 months
SUM	**$256,000**	

The total estimated cost is summarized in the table above.

5. Expected Klay funding plan

Milestone	Budget	(Expected) Date [MM/DD]
Milestone #1	$80,000	08/31
Milestone #2	$80,000	10/31
Milestone #3	$96,000	12/31
SUM	**$256,000**	

S2W LAB will publish key deliverables at each milestone. The last column in the table above describes the expected date of each milestone. After confirmation by the reviewer, the Klay funding is expected to be paid in installments.

Attachments

Proposal presentation slides.

https://drive.google.com/file/d/1LvbamFYBMZ-tRCCT1iSZ8Xmypr3ibf00/view?usp=sharing

Proposal presentation video.

https://drive.google.com/file/d/1hFmNlrcdfhEeEE-NuITIrMSm9R-Qqy4y/view?usp=sharing

UI design / Sitemap / and so on …

This field is blank.

Feedback

This field is blank.