



# **S2\_EYEZ for Klaytn Token Economies**

**June 2021**

**Chanhee Lee**

**Tokens are as important as cryptocurrency itself**

## Ethereum tokens are now more valuable than ETH itself

The BUIDL philosophy appears to be working, as the combined market cap of ERC20 tokens built on Ethereum has surpassed the network's native ETH.

By [Jose Antonio Lanz](#)

3 min read • Jul 14, 2020



## Mainnet vs token economies

### ⚡ External transaction

- Transactions initiated by 'external' accounts
- Exist on the blockchain mainnet

### ⚡ Internal transaction

- Transactions as a result of preceding transactions (like a byproduct of smart contract functionality)
- 'Not' exist on the blockchain mainnet

### ⚡ Token transfer

- Transactions that do exclusively token transfers
- Practically the same with a subset of internal transactions
- 'Not' exist on the blockchain mainnet

## Mainnet vs token economies

### ➤ External transaction

- Transactions initiated by 'external' accounts

Analyzing token transfers could be just as important as the mainnet!  
We need an appropriate way to do this quite unlike that of the mainnet.

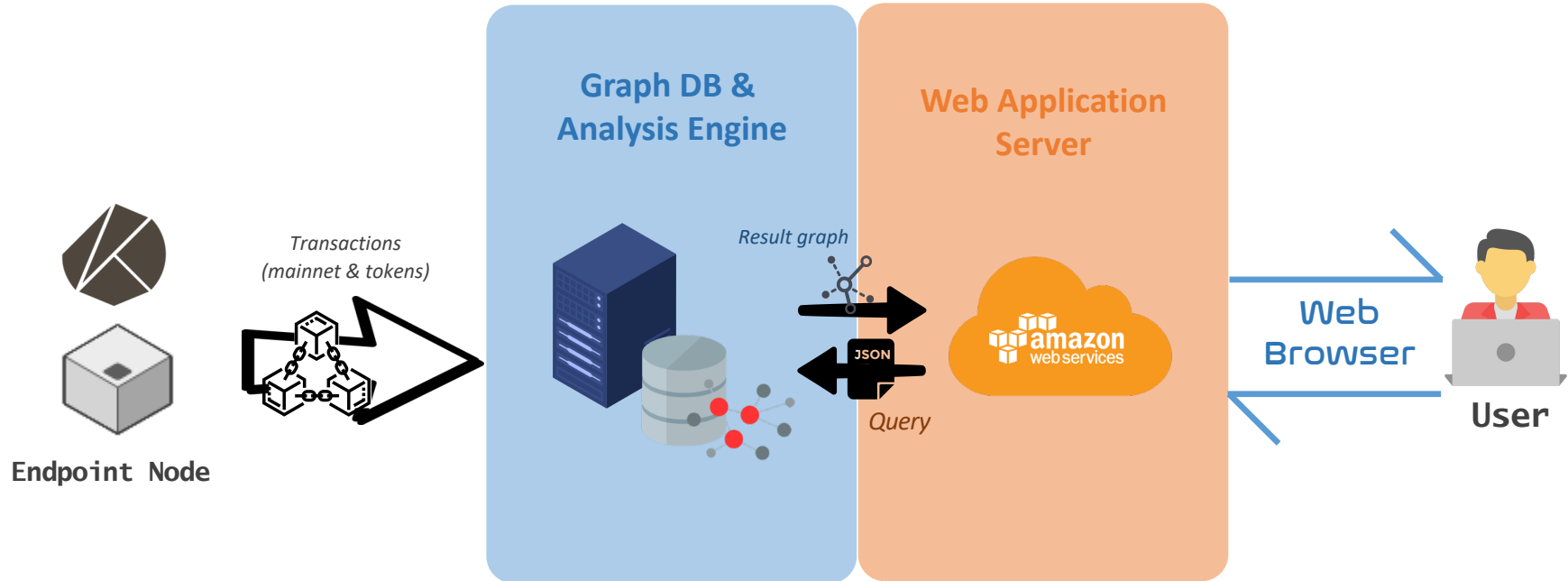
### ➤ Token transfer

- Transactions that do exclusively token transfers
- Practically the same with a subset of internal transactions
- 'Not' exist on the blockchain mainnet



# System Design

## Abstracted system architecture of S2\_EYEZ for Klaytn token economies



**eyez**

S2\_EYEZ for Klaytn



## Data structure of token transfer graph

### ➤ Two types of Vertex

- Address: address
- Transaction: transaction hash value, timestamp, amount and etc.

### ➤ Single type of Edge

- Directed(Incoming/Outgoing) edge: transfer(token) type

### ➤ External data store

- Supplementary data about transactions such as tx fee, gas used and limit



## The monolithic vs microstructure of multiple token types

### Monolithic Graph

#### Pros.

- **Usability**
  - Easily track the multiple token transfers at once
- **Singleton**
  - Generalized data structure

#### Cons.

- **Irrelevant information trace**
  - Traverse token transactions irrelevant to a requested token type

### Micro Graph

#### Pros.

- **Good for single type of token**
  - Traverse transactions of a specified token type only

#### Cons.

- **Additional cost**
  - Reference of a string of graph to trace token transfers over one token type
- **Hard to maintenance**
  - Maintenance of an individual graph structure for every single token type

# Graph Construction 3/3

## Example:

0xa60c89a51208c94af197815538547997980b872d3fad9f0dd6ae43d35fdd7a5d

### Transaction

0xa60c89a51208c94af197815538547997980b872d3fad9f0dd6ae43d35fdd7a5d

COPY

#### Overview

Success 



TX Type	Fee Delegated Smart Contract Execution	Amount	0 KLAY
Block #	56507953	Gas Price	0.000000025 KLAY
From → To	0xf366...1d43ec → 0xdc6...5b9d6c	Gas Used	52,210
Token Transfers	1	Gas Limit	4,300,000
NFT Transfers	0	TX Fee	0.00130525 KLAY
Fee Payer	0x7be7...c4c60d		
Time	1 minute ago		
Nonce	2130651		

#### Token Transfers

Internal Transactions

Event Logs

Input Data

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

# Graph Construction 3/3

## Example:

0xa60c89a51208c94af197815538547997980b872d3fad9f0dd6ae43d35fdd7a5d

### Transaction

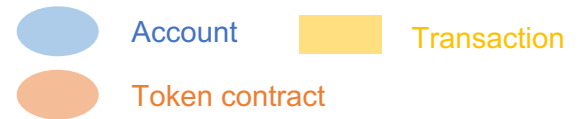
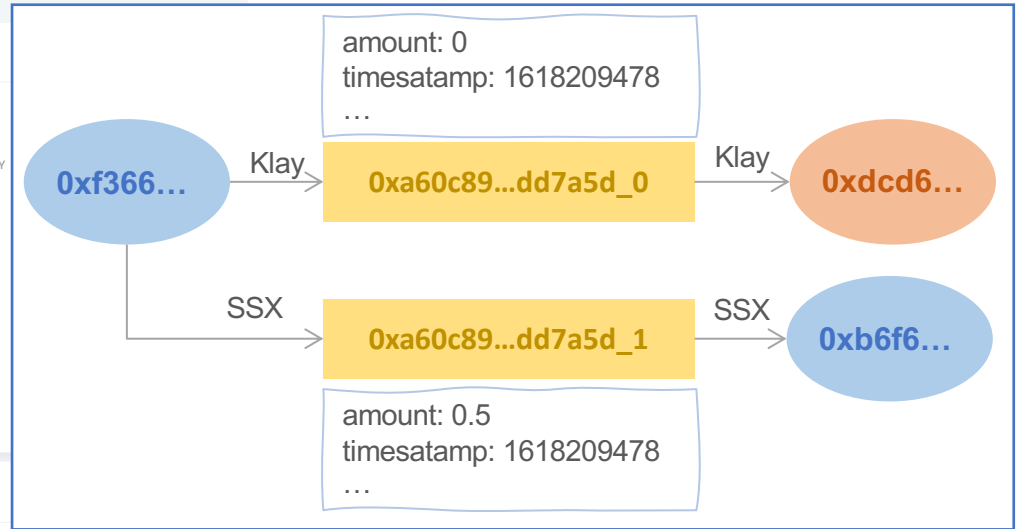
0xa60c89a51208c94af197815538547997980b872d3fad9f0dd6ae43d35fdd7a5d COPY

**Overview**

TX Type	Fee Delegated Smart Contract Execution	Amount	0 KLAY
Block #	56507953	Gas Price	0.000000025 KLAY
From → To	0xf366...1d43ec → 0xdc6...5b9d6c	Gas Used	52,210
Token Transfers	1	Gas Limit	4,300,000
NFT Transfers	0	TX Fee	0.00130525 KLAY
Fee Payer	0x7be7...c4c60d		
Time	1 minute ago		
Nonce	2130651		

**Token Transfers** Internal Transactions Event Logs Input Data

BLOCK #	TIME	FROM	TO	TOKEN	AMOUNT
56507953	17 mins ago	0xf366...1d43ec	0xb6f6...6fb9e2	<span>Someing Exchange (SSX)</span>	0.500000 SSX



# Abnormal Transactions

The image features a dark, almost black background. In the center, the text "Abnormal Transactions" is written in a bold, white, sans-serif font. Below the text, there is a complex, glowing network of white lines and nodes, resembling a data visualization or a complex web structure. The nodes are small circles, and the lines connect them in a dense, interconnected pattern. The overall effect is that of a digital or network-based environment.

## Malicious usages

### ➤ Money Laundering

- Black(e.g., hacked) money
- Bitcoin
  - n:m transactions
- Ethereum
  - DeFi(DEX, swap)
  - e.g) the case of KuCoin hack: Synthetix, Uniswap, KyberSwap

### ➤ Transaction Abuse

- Arbitrage, Oracle manipulation







# Transaction Patterns

## Case study on transaction abuse: flash loan attack

### Transaction Action:

- › Borrow 10,000 Ether From  dYdX
- › Supply 5,500 Ether To  Compound
- › Borrow 112  WBTC From  Compound
- › Executed Swap 5,637.62376237623786  WETH For 51.3455758  WBTC With  Kyber
- › Repay 10,000.000000000001 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)
- › From bZx: Vault To 0xb017c9936f927... For 0.000091505033541987 (\$0.20)  Wrapped Ethe... (WETH)
- › From 0xb017c9936f927... To bZx ETH iToken For 0.000082354530187789 (\$0.18)  Wrapped Ethe... (WETH)
- › From bZx ETH iToken To bZx: Vault For 4,698.019801980198019822 (\$10,169,051.78)  Wrapped Ethe... (WETH)
- › From 0xb0200b0677dd8... To bZx: Vault For 1,300 (\$2,813,902.00)  Wrapped Ethe... (WETH)
- › From bZx: Vault To 0xb017c9936f927... For 5,637.623762376237623786 (\$12,202,862.14)  Wrapped Ethe... (WETH)
- › From 0xb017c9936f927... To Kyber: Contract For 5,637.623762376237623786 (\$12,202,862.14)  Wrapped Ethe... (WETH)
- › From Kyber: Contract To Kyber: Reserve W... For 5,637.623762376237623786 (\$12,202,862.14)  Wrapped Ethe... (WETH)

Scroll for more

# Transaction Patterns

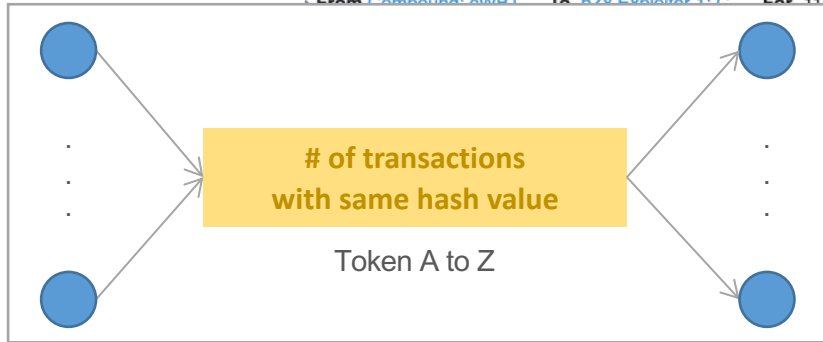
## Case study on transaction abuse: flash loan attack

Transaction Action:

- › Borrow 10,000 Ether From dYdX
- › Supply 5,500 Ether To Compound
- › Borrow 112 WBTC From Compound
- › Executed Swap 5,637.62376237623786 WETH For 51.3455758 WBTC With Kyber
- › Repay 10,000.000000000001 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: cWBTC ... To bZx Exploiter 1: C... For 112 (\$6,820,016.00) Wrapped BTC (WBTC)
- › 00091505033541987 (\$0.20) Wrapped Ethe... (WETH)
- › 00082354530187789 (\$0.18) Wrapped Ethe... (WETH)
- › 98.019801980198019822 (\$10,169,051.78) Wrapped Ethe... (WETH)
- › 00 (\$2,813,902.00) Wrapped Ethe... (WETH)
- › 37.623762376237623786 (\$12,202,862.14) Wrapped Ethe... (WETH)
- › 37.623762376237623786 (\$12,202,862.14) Wrapped Ethe... (WETH)
- › 37.623762376237623786 (\$12,202,862.14) Wrapped Ethe... (WETH)



# Transaction Patterns

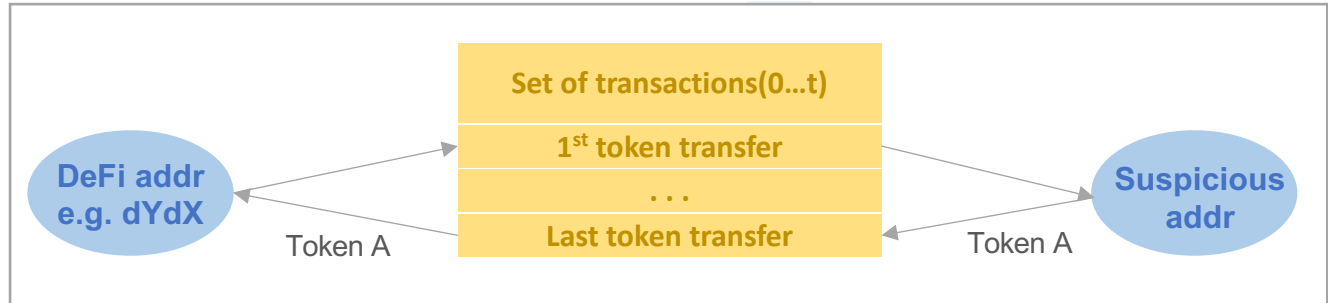
## Case study on transaction abuse: flash loan attack

Transaction Action:

- ▶ Borrow 10,000 Ether From dYdX
- ▶ Supply 5,500 Ether To Compound
- ▶ Borrow 112 WBTC From Compound
- ▶ Executed Swap 5,637.62376237623786 WETH For 51.3455758 WBTC With Kyber
- ▶ Repay 10,000.000000000001 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: cWBTC... To bZx Exploiter 1: C... For 112 (\$6,820,016.00) Wrapped BTC (WBTC)







# Web Services

## Delivery method of S2\_EYEZ

### ➤ **As-Is: development environments(APIs)**

- Hard to use to people in general without any background knowledge about software developments
- Visible only for Klaytn forum users

### ➤ **To-Be: public web services**

- Fully open to public
- Give a clear view of analysis result

## Example: private web services for BTC analysis

eyeZ S2W LAB AML Solution S2-EYEZ-Investigation beta version Authorized Users Only 메뉴얼 다운로드 로그아웃

1421chCK32pV32Tw5MQbiUIKWKvnmj7d91 송신 ▾ 날짜 ▾ 송수신 비종 ▾

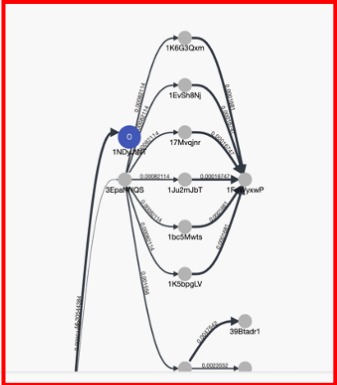
Threat Score

# Low

주소 정보 ⓘ				지갑 정보 ⓘ			
총 거래 수	172	총 송금액	16.31272184	지갑 유형	Unknown	지갑 내 주소 수	2,039,270
최초 거래일	2018-02-02	총 송신액	16.31272184	지갑 번호	0848f61a	위협 탐지 건수	0
최근 거래일	2019-12-07	잔고	0.00000000	최초 거래일	2017-06-24	탐지된 위협 정보	No Threat Info
위협 탐지 건수	0	탐지된 위협 정보	N/A	최근 거래일	2020-12-07		

상세 보기 getting details

basic information



transaction graph

1421chCK32pV32Tw5MQbiUIKWKvnmj7d91 입출금 내역 [ 총 232 건 ] 선택된 사항 역으로 추출

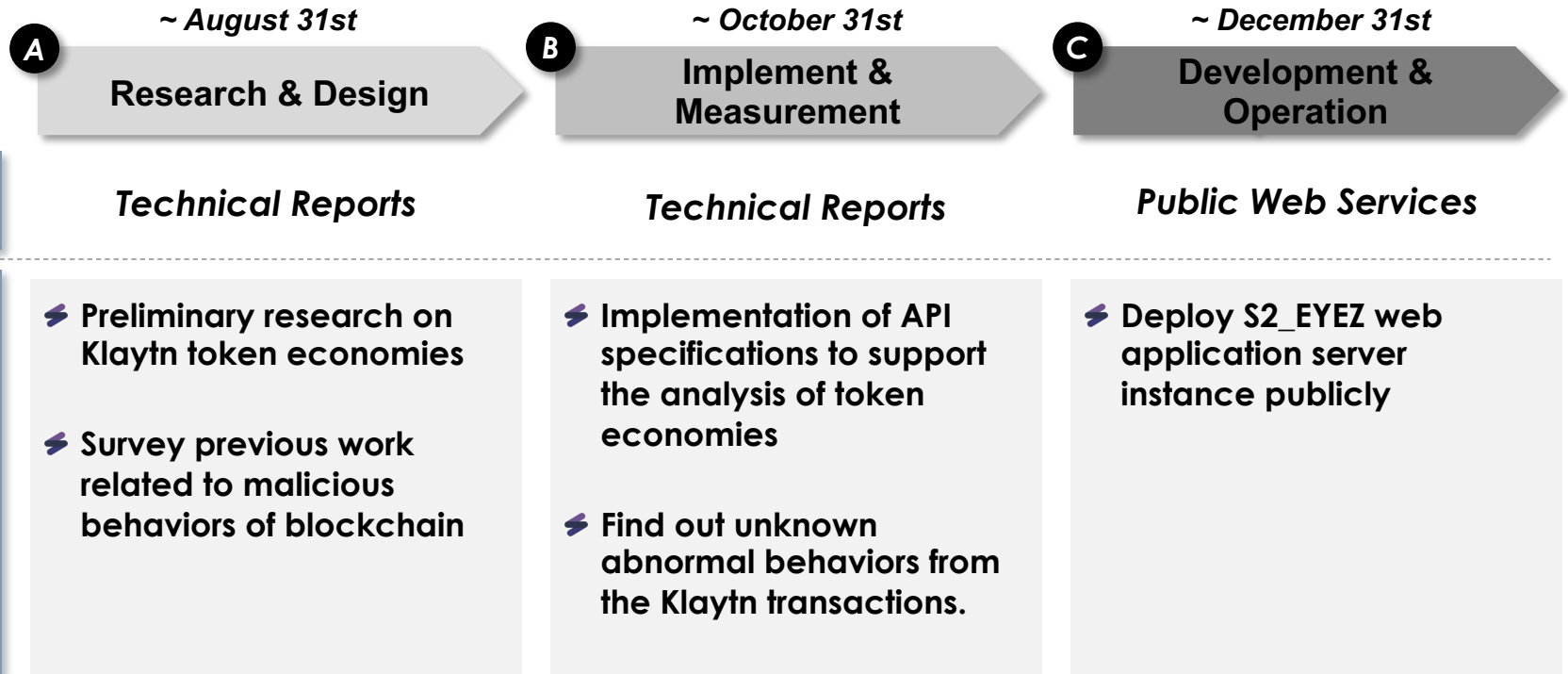
data exportation

## Web application services to support the analysis of token transfers

Name	Description	Inputs	Outputs
Financial Flow Tracking	Providing the details of financial transaction flows of an address	An address	A relational graph of transaction flows rooted from an address
Correlation Analysis	Generating the combination of transaction data from the mainnet and token economies	A hash value of a transaction	A relational graph of transaction information related to the requested transaction
Shortest Path	Figuring out the shortest path between two addresses	Two addresses	A path data from an address to another
Pattern Matching	Finding out what transaction patterns a wallet has	An address, a specific transaction pattern	A graph of a matched transaction pattern

# Milestones

## Milestones and schedule



---

# THANK YOU



**MAKE THE WORLD MORE SAFE AND SECURE**

Chanhee Lee, [leemember@s2wlab.com](mailto:leemember@s2wlab.com)

---