

# Information and Knowledge Discovery on Cryptocurrency: A Security Perspective

Hands-on Tutorial at  
The 2024 IEEE International Conference on Big data (IEEE BigData 2024)



Feida ZHU, PhD  
Associate Professor



Ling CHENG, PhD  
PhD Student

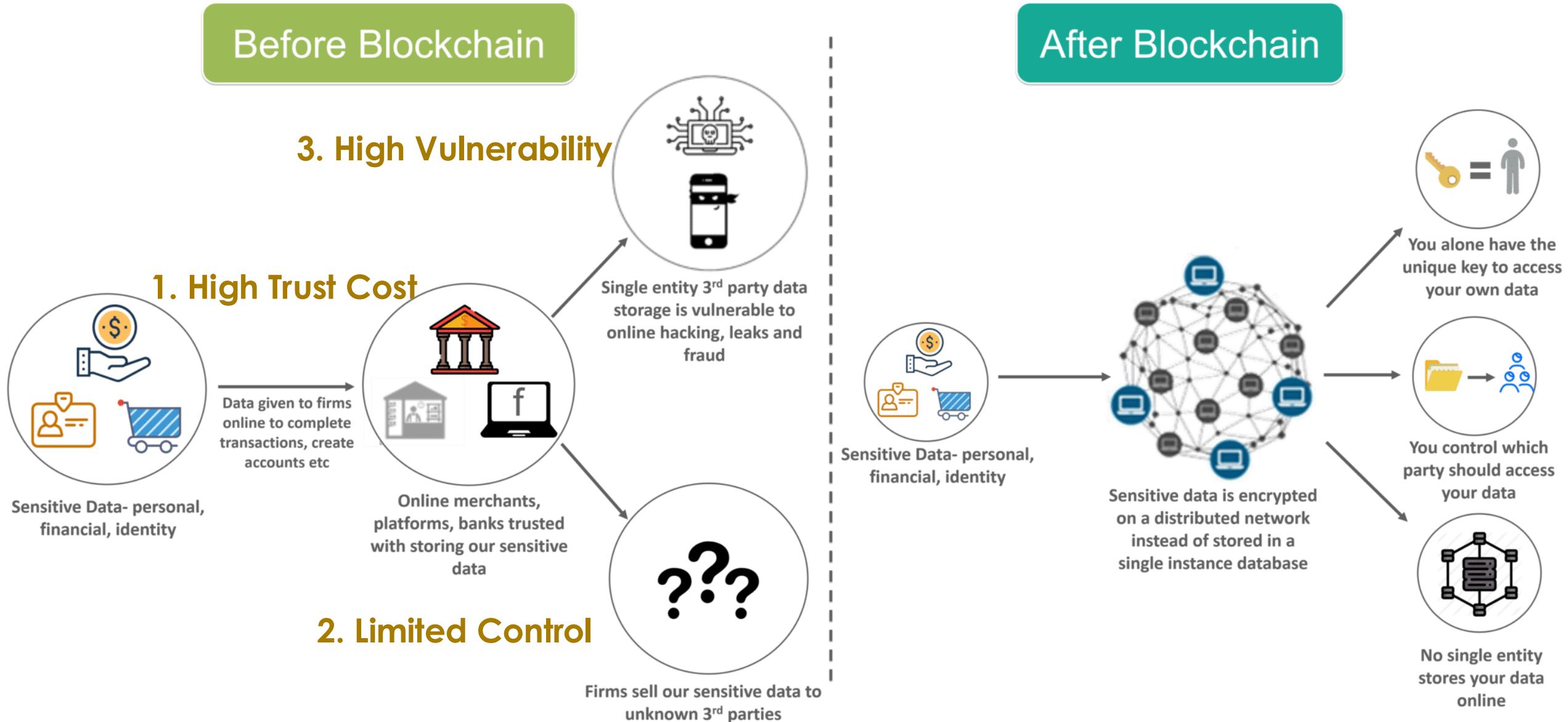
School of Computing and Information Systems  
Singapore Management University

- Introduction to Blockchain
- **Hands-on case 1:** Rat Trading Detection Example
- Traditional Methods on Crypto Crime Detection
- **Hands-on case 2:** NFT Wash Trading Detection Example
- Transfer Path-based Methods
- **Hands-on case 3:** Scam Detection Using Asset Transfer Path

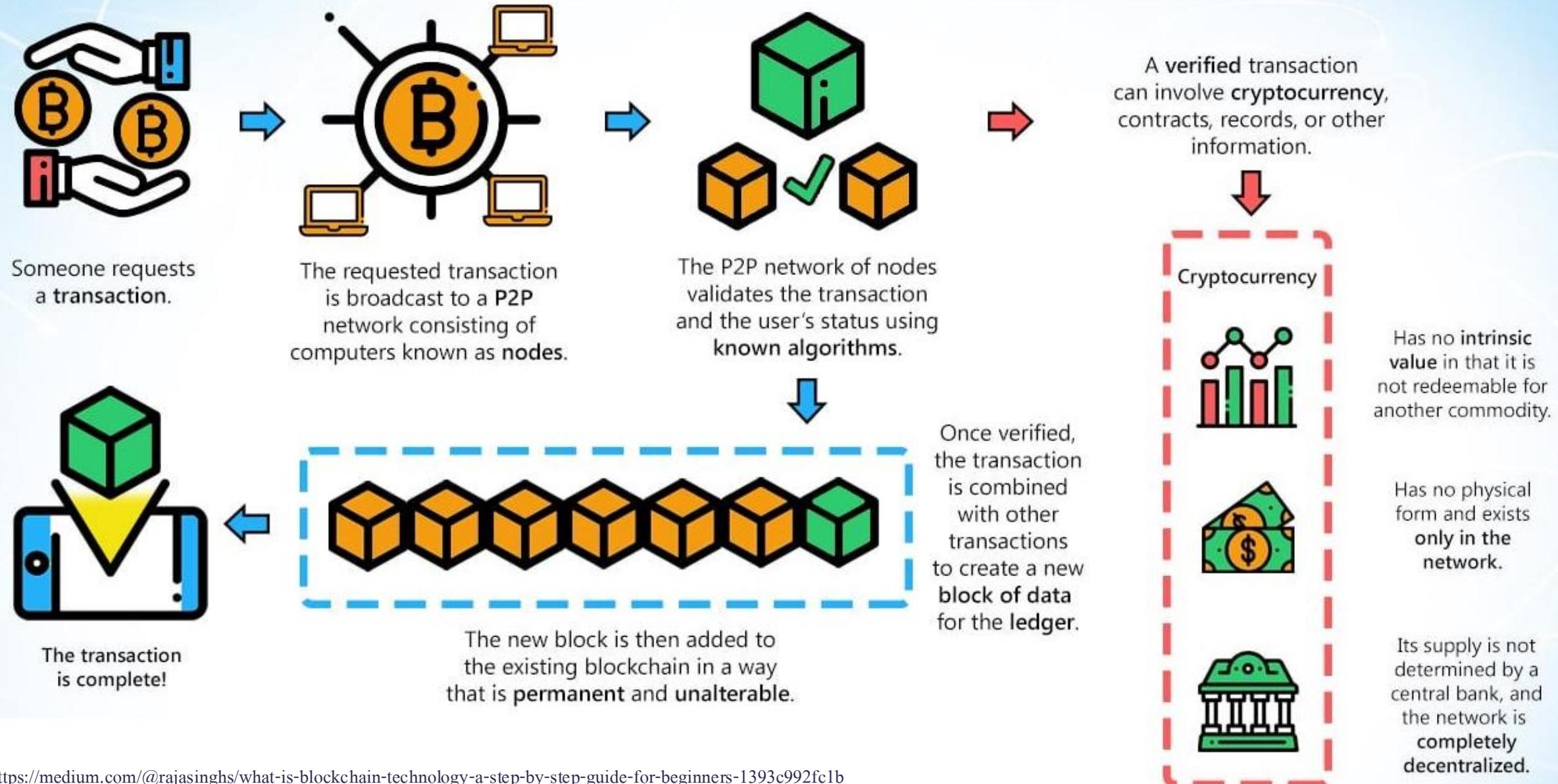
# Outline

- Introduction to Blockchain
- Hands-on case 1: Rat Trading Detection Example
- Traditional Methods on Crypto Crime Detection
- Hands-on case 2: NFT Wash Trading Detection Example
- Transfer Path-based Methods
- Hands-on case 3: Scam Detection Using Asset Transfer Path

# Why Blockchain?



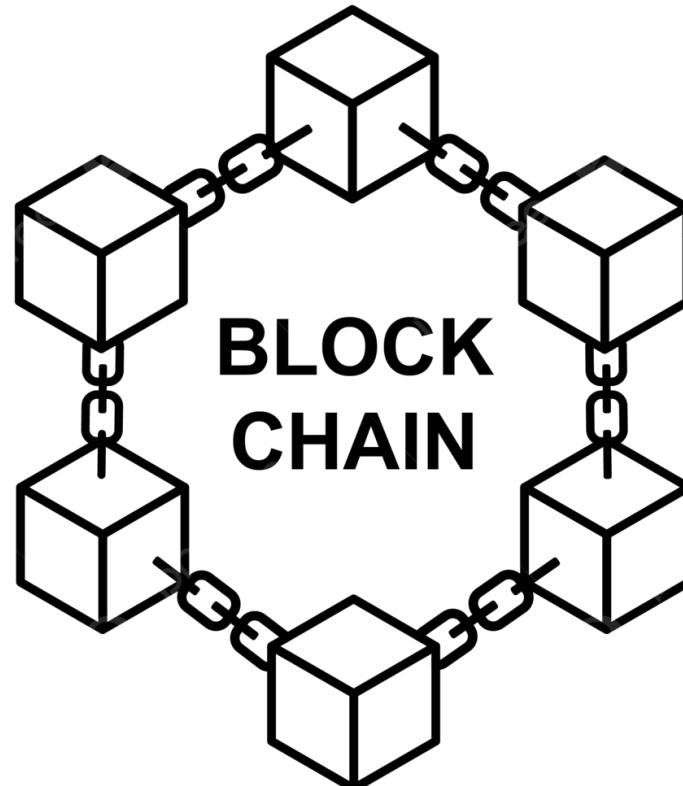
# What is Blockchain?



# Blockchain Properties

## Programmable

A blockchain is programmable.  
(i.e. Smart Contracts)



## Unanimous

All network participants agree to the validity of each of the records

## Anonymous

The identity of participants is anonymous

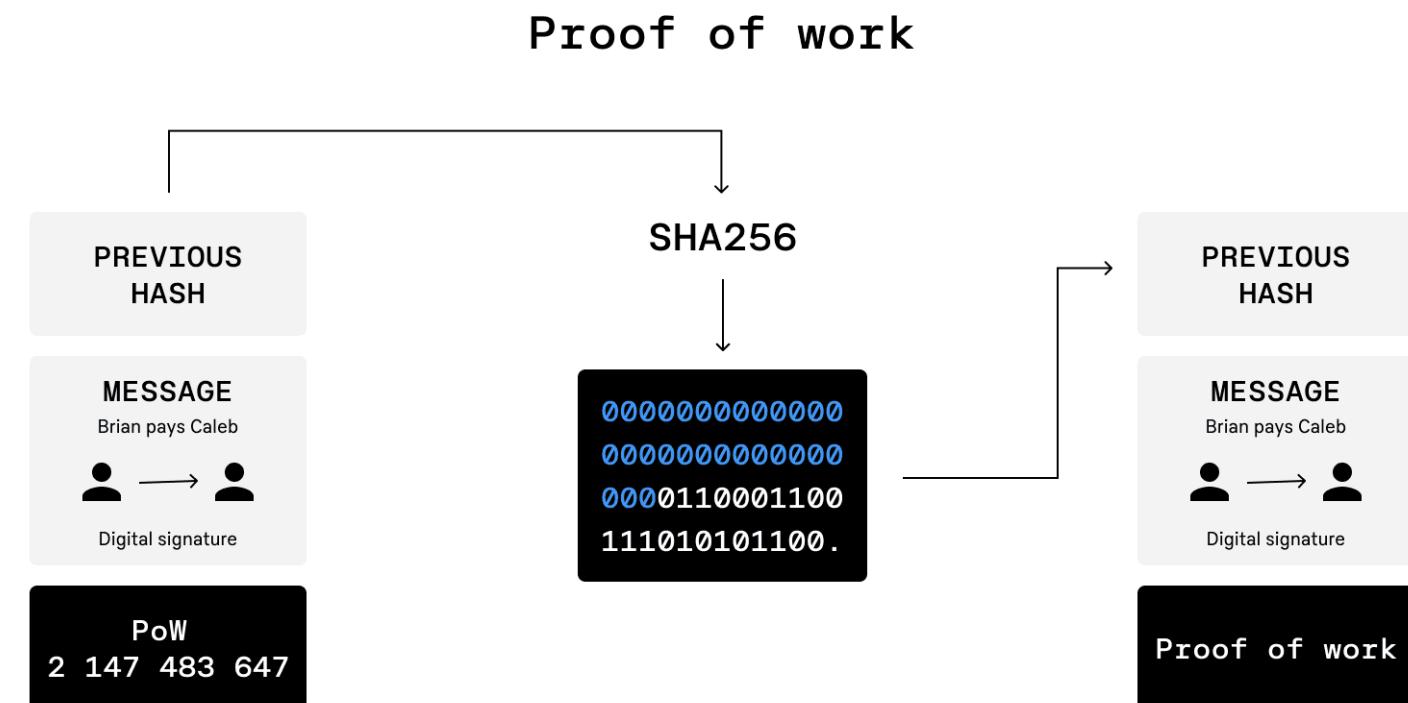
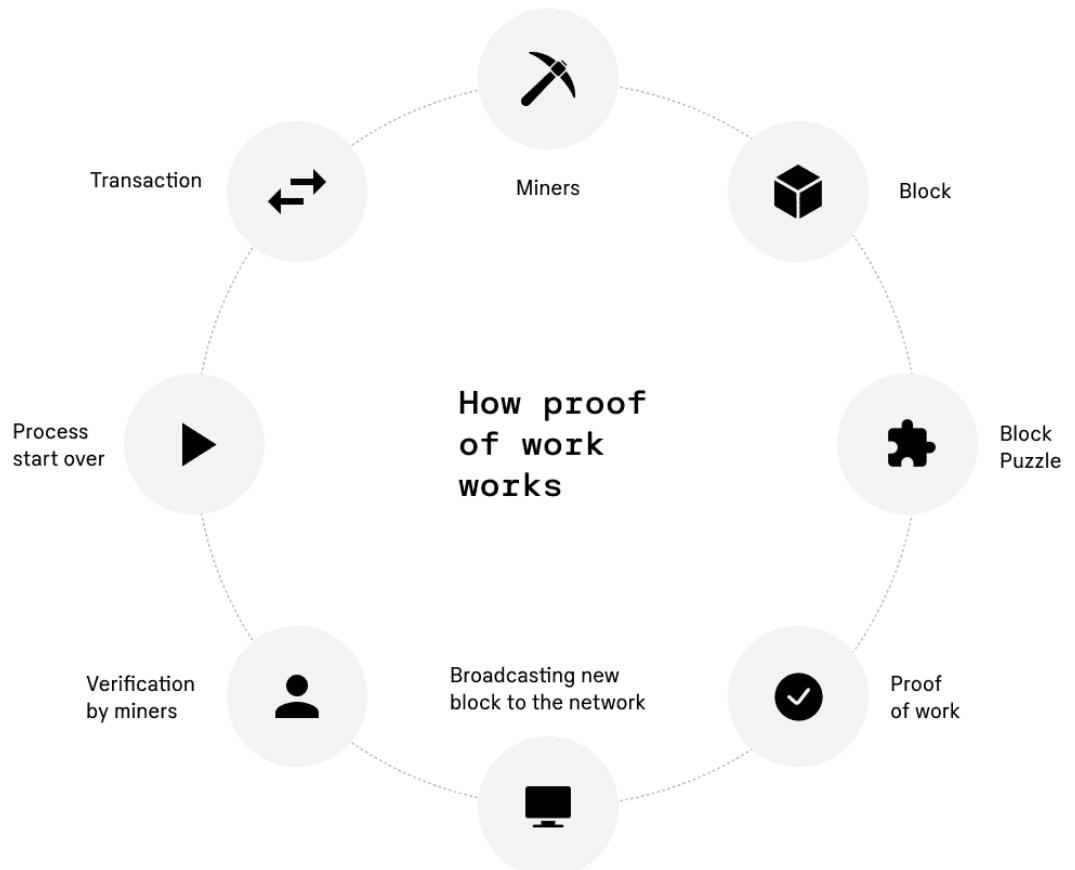
## Distributed

All network participants have a copy of the ledger for complete transparency.

## Immutable

Any validated records are irreversible and cannot be changed.

# What is Proof of Work?



[Online Demo Link](#)

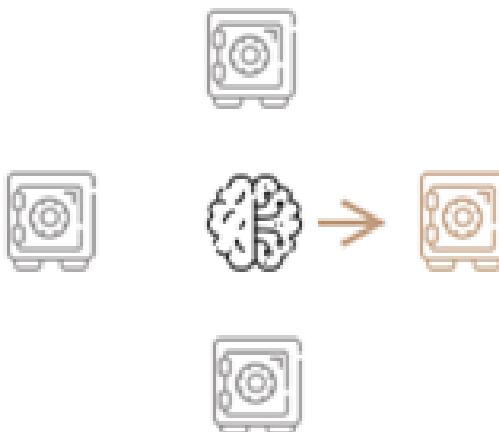
# What is Proof of Stake?

Owner stakes their native tokens in staking pools



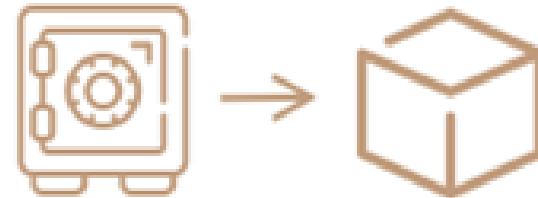
1

Algo pseudo-randomly selects next validator



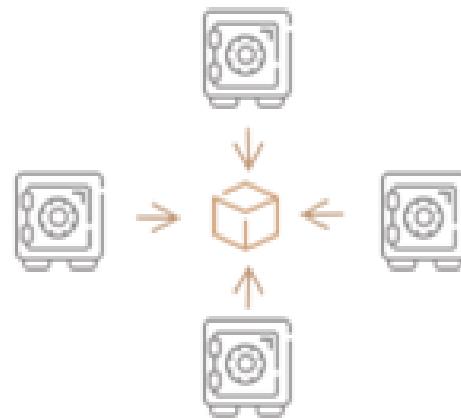
2

The selected validator proposes a block of transactions



3

Other validators verify and approve the transaction



4

The block is added to the existing blockchain



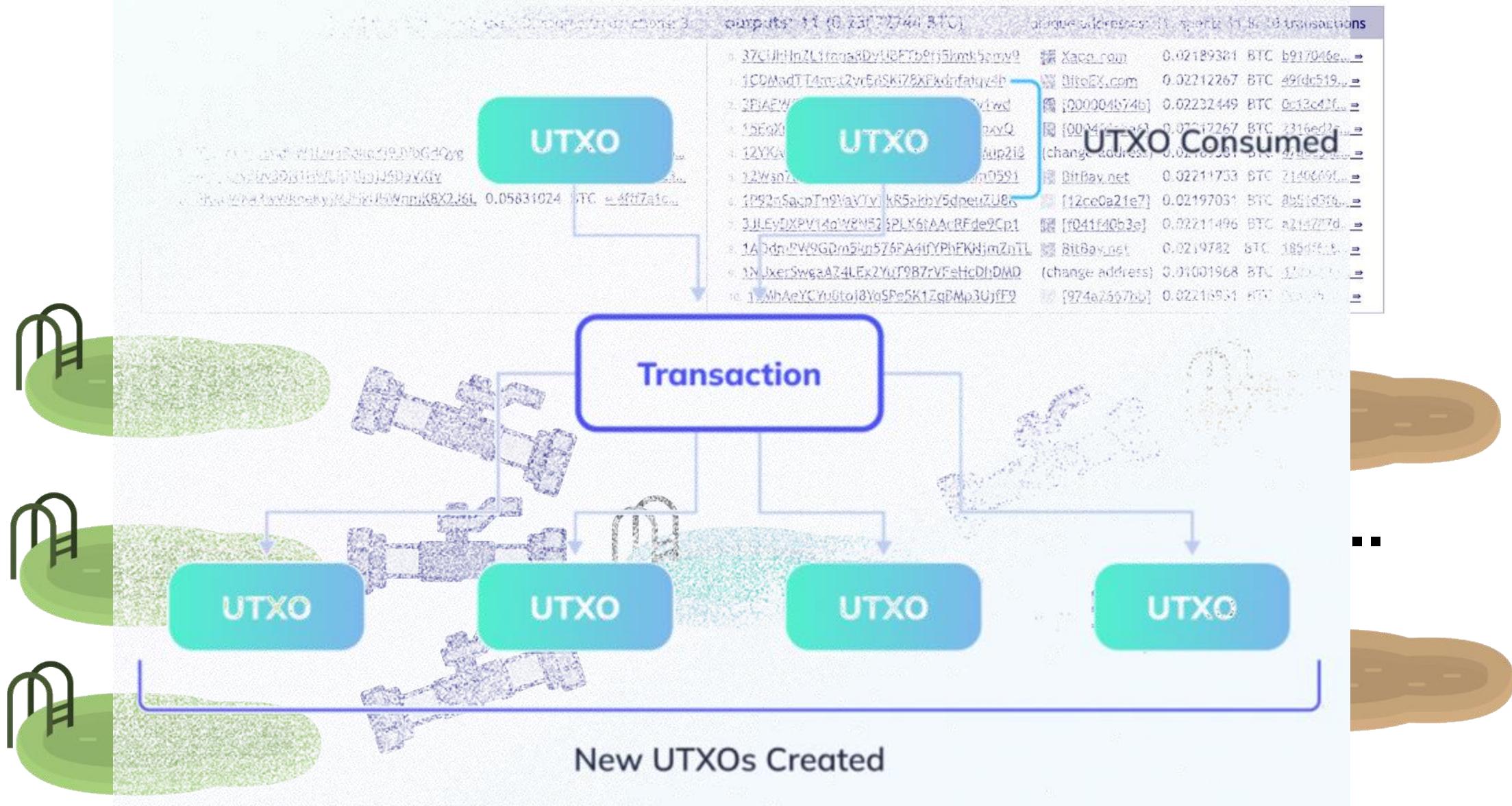
5

The validator earns a transaction fee



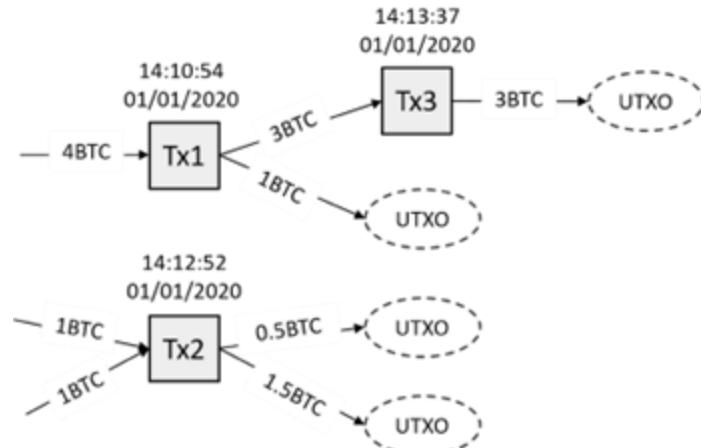
6

# BTC UTXO Transaction System

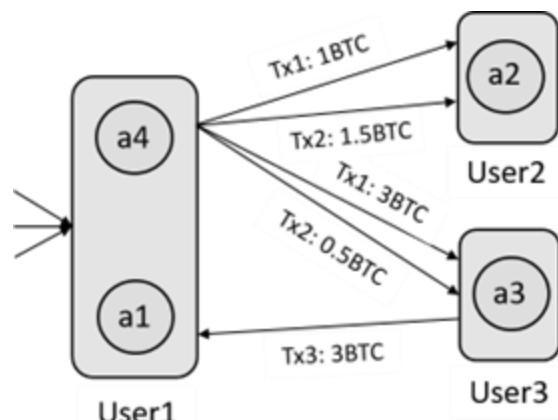


# BTC UTXO Transaction System

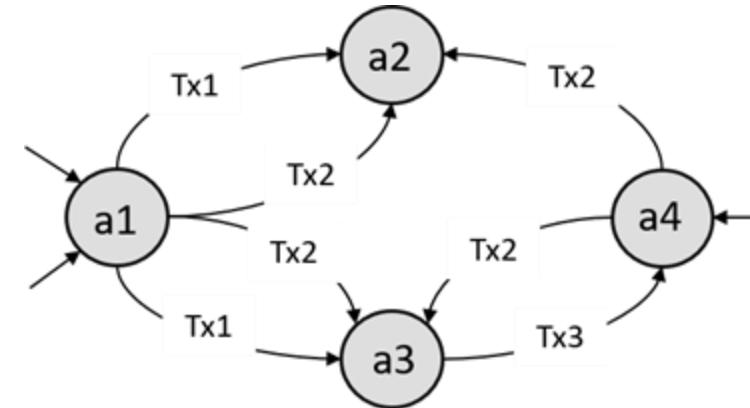
## ➤ BTC Transaction Network



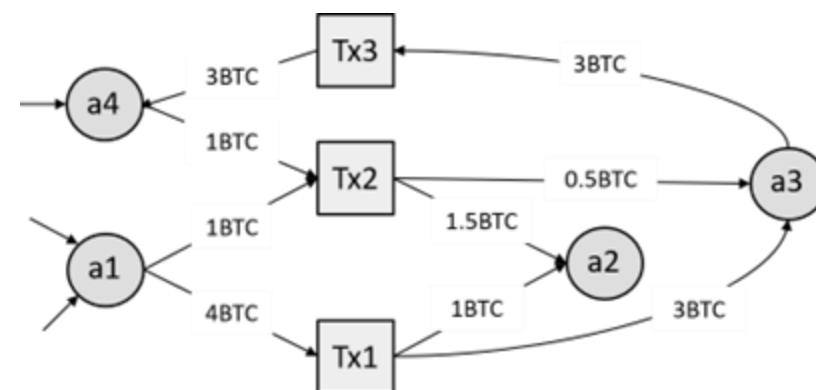
Transaction Network



User Network



Address Network



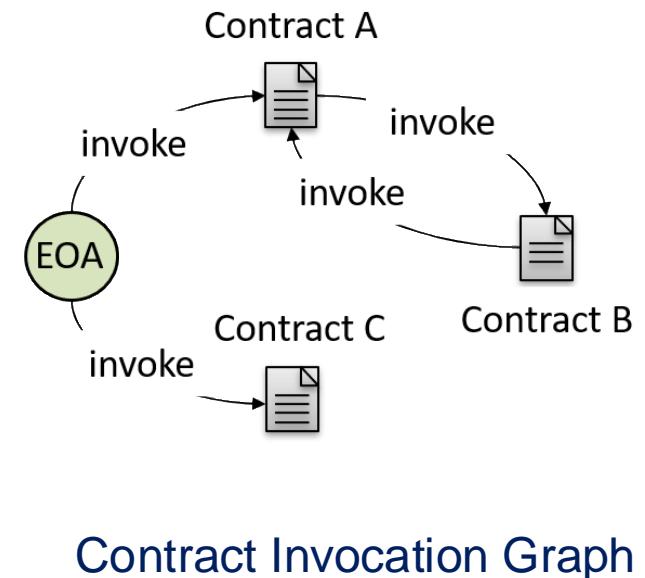
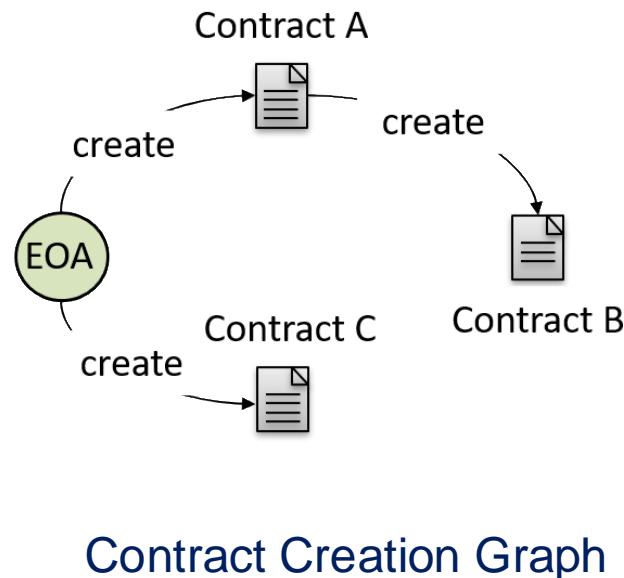
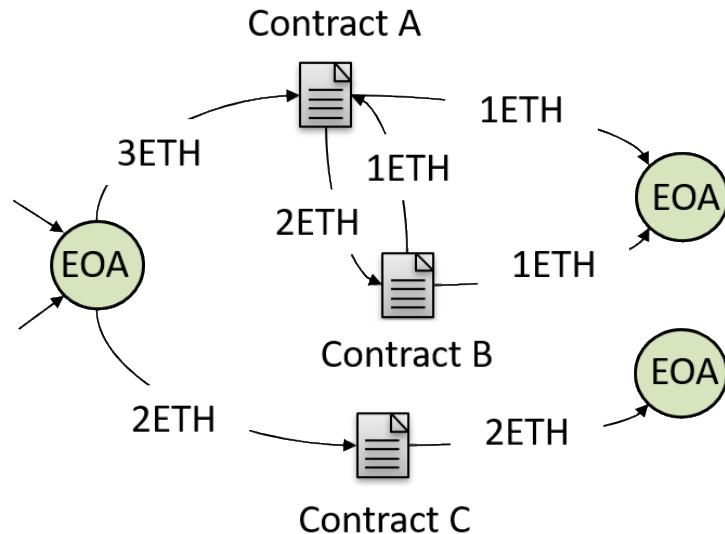
Hypergraph

1. Wu, Reid, F., Harrigan, M. "An analysis of anonymity in the Bitcoin system". Springer. pp. 197–223 (2013).

2. Pham, T., Lee, S. "Anomaly detection in the Bitcoin system-A network perspective". arXiv preprint (2016).

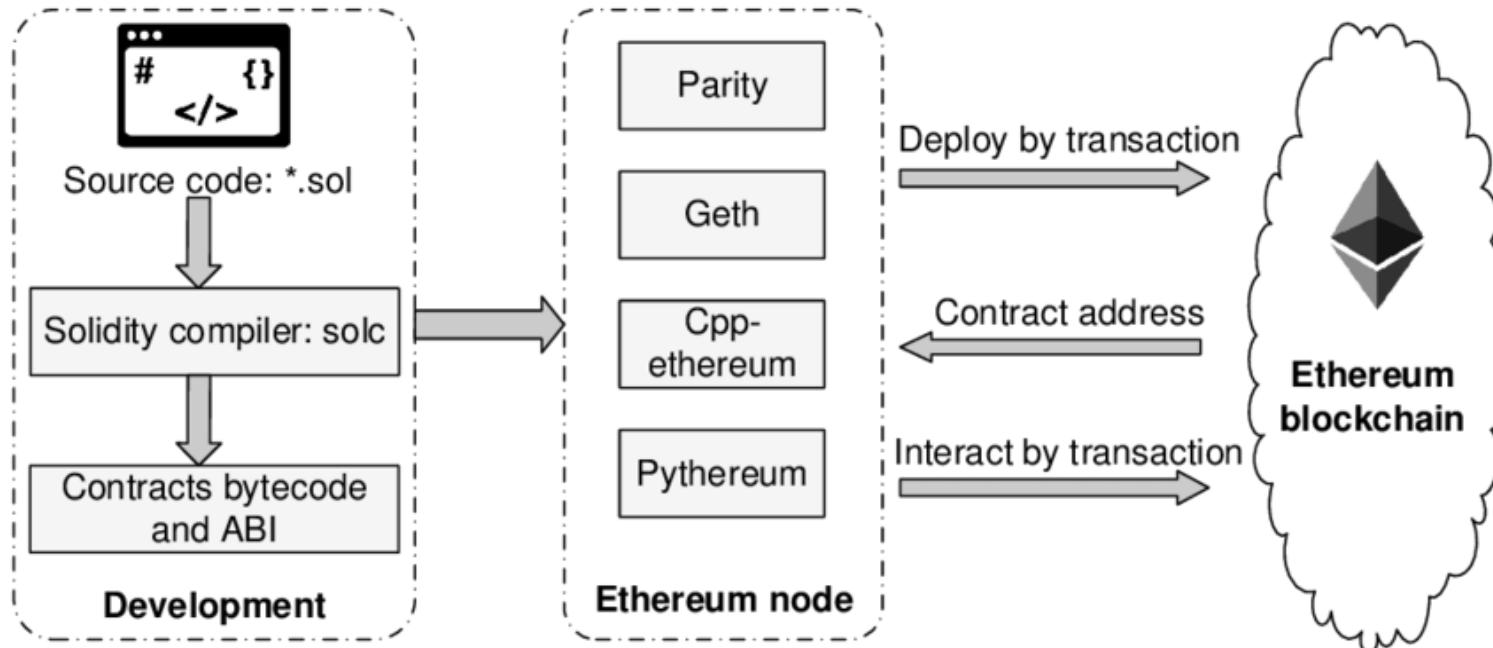
# ETH Account-based Transaction System

## ➤ ETH Transaction Network

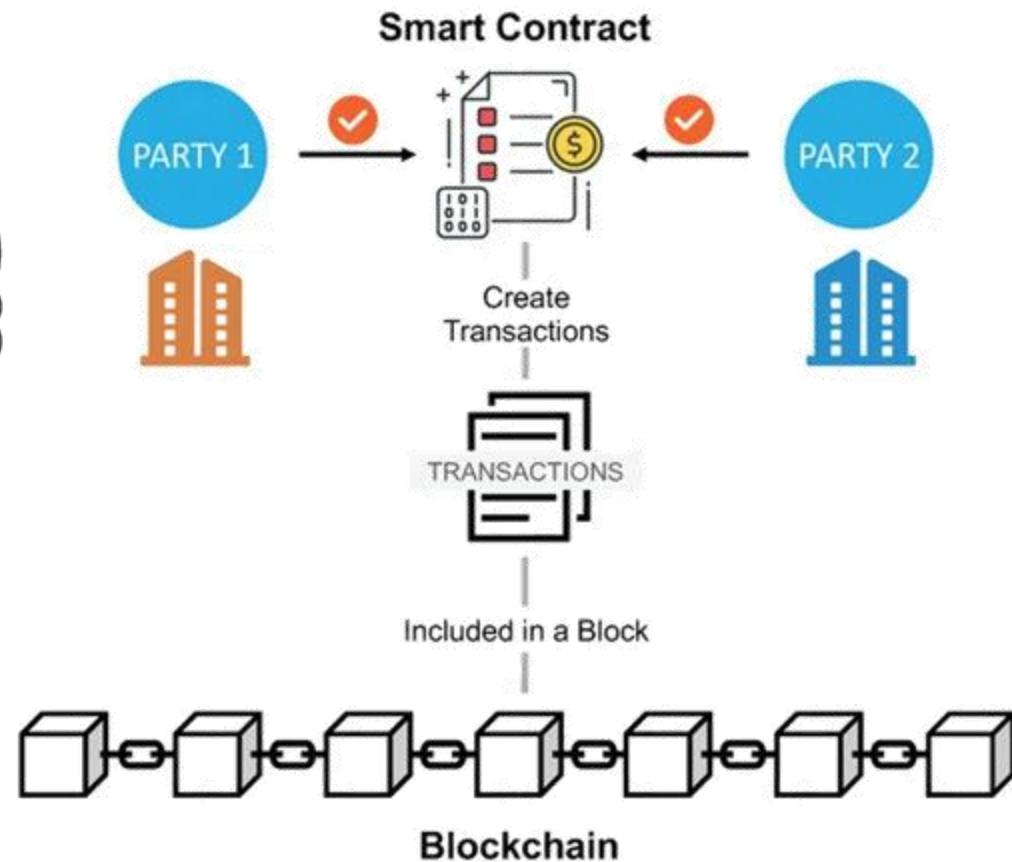


# Smart Contract

## ➤ ETH Smart Contract Deployment



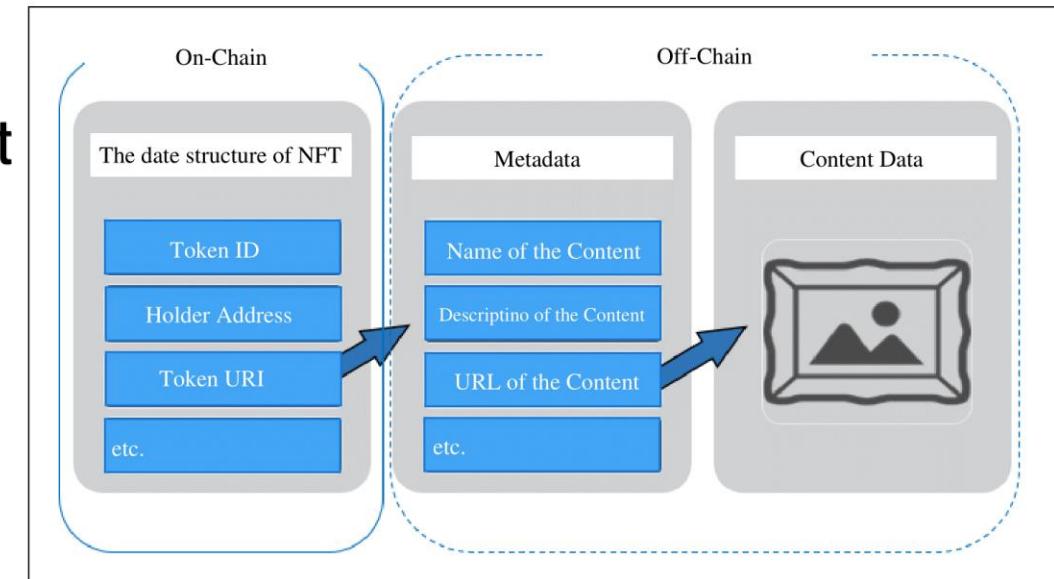
## ➤ Contract Interaction



**Ethereum nodes** are computers running Ethereum client software that participate in the Ethereum blockchain network. These nodes are responsible for **maintaining the blockchain**, **validating transactions**, **executing smart contracts**, and **sharing data** across the network.

# Non-Fungible Tokens (NFT)

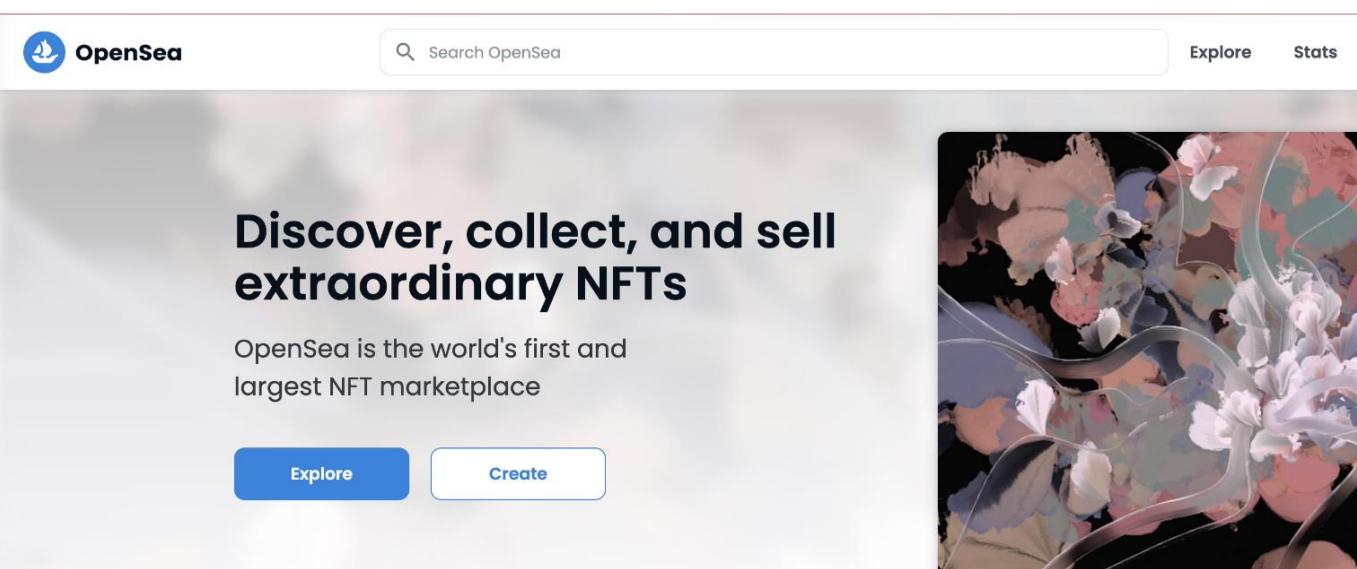
- A smart contract (e.g., ERC 721) to bond together the following information
  - A unique identifier ( identity)
  - A set of standard metadata to display the asset
    - Name
    - Description
    - Image
  - A secure file link (content)
- Metadata and associated files are deployed onto the InterPlanetary File System (IPFS), a secure, transparent, decentralized, and public blockchain to host asset metadata.



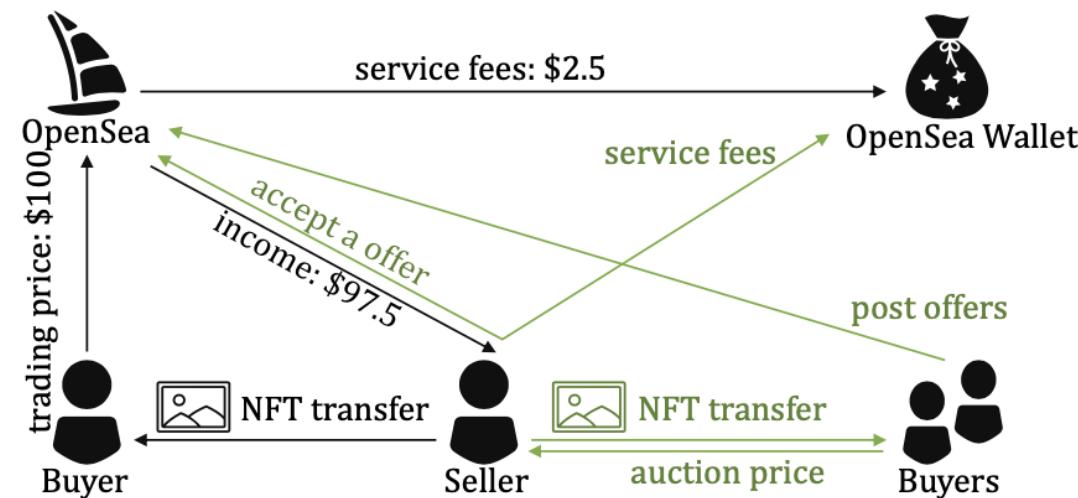
# NFT Marketplace

## OpenSea

Founded in Dec 2017 by Alex Atallah and Devin Finzer, OpenSea is a generalized marketplace set up to facilitate the trading of NFTs. It is by far the largest NFT marketplace by trading volume. It saw about \$3 billion in trading volume in September 2021 alone, making up more than 99% of the total market.



OpenSea Website



Two main ways to purchase NFTs on Opensea:  
Instant sale (Black) / Auction (Green)



BTC

Full-Node  
(Local)

API



ETH

Full-Node  
(Local)

API

## citp/BlockSci

A high-performance tool for blockchain science  
and exploration



## Blockchain.com APIs

Build bitcoin apps on top of our APIs for free. [API Terms of Service](#)

## ethereum/web3.py

A python interface for interacting with the Ethereum  
blockchain and ecosystem.



## ETHERSCAN

The Ethereum Block Explorer

# Outline

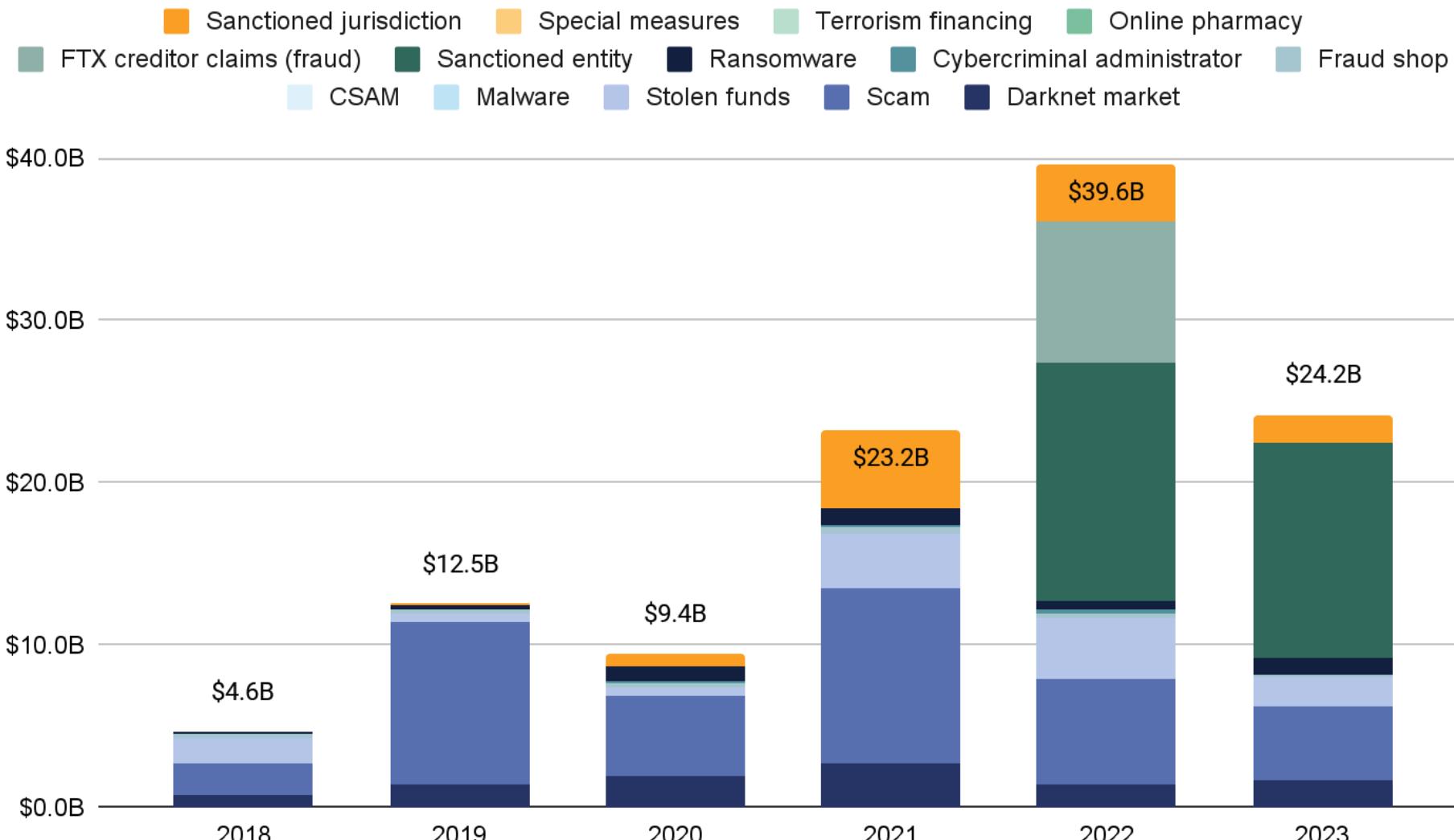
- Introduction to Blockchain
- **Hands-on case 1:** Rat Trading Detection Example
- Traditional Methods on Crypto Crime Detection
- **Hands-on case 2:** NFT Wash Trading Detection Example
- Transfer Path-based Methods
- **Hands-on case 3:** Scam Detection Using Asset Transfer Path

# Outline

- Introduction to Blockchain
- **Hands-on case 1:** Rat Trading Detection Example
- Traditional Methods on Crypto Crime Detection
- **Hands-on case 2:** NFT Wash Trading Detection Example
- Transfer Path-based Methods
- **Hands-on case 3:** Scam Detection Using Asset Transfer Path

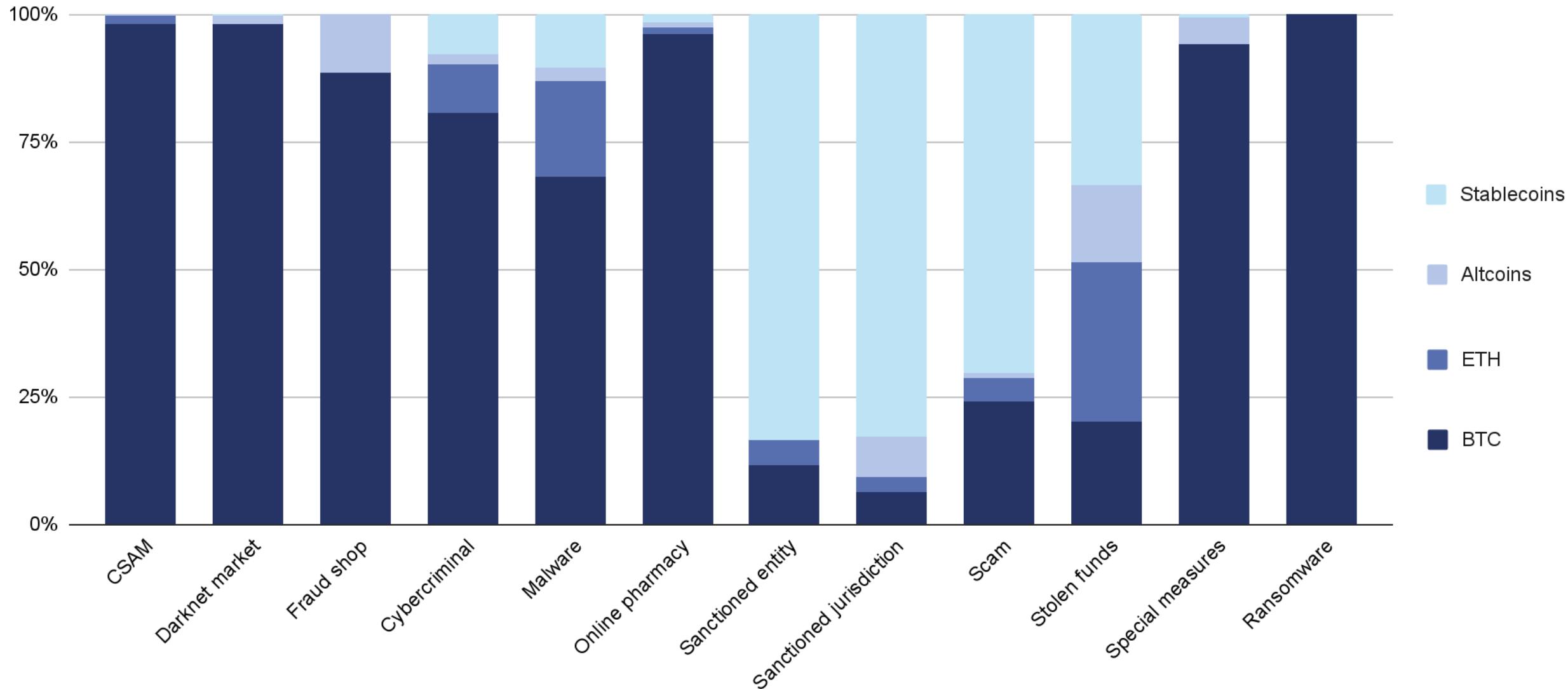
# Crypto-Crime Volume is Tremendous

Total cryptocurrency value received by illicit addresses



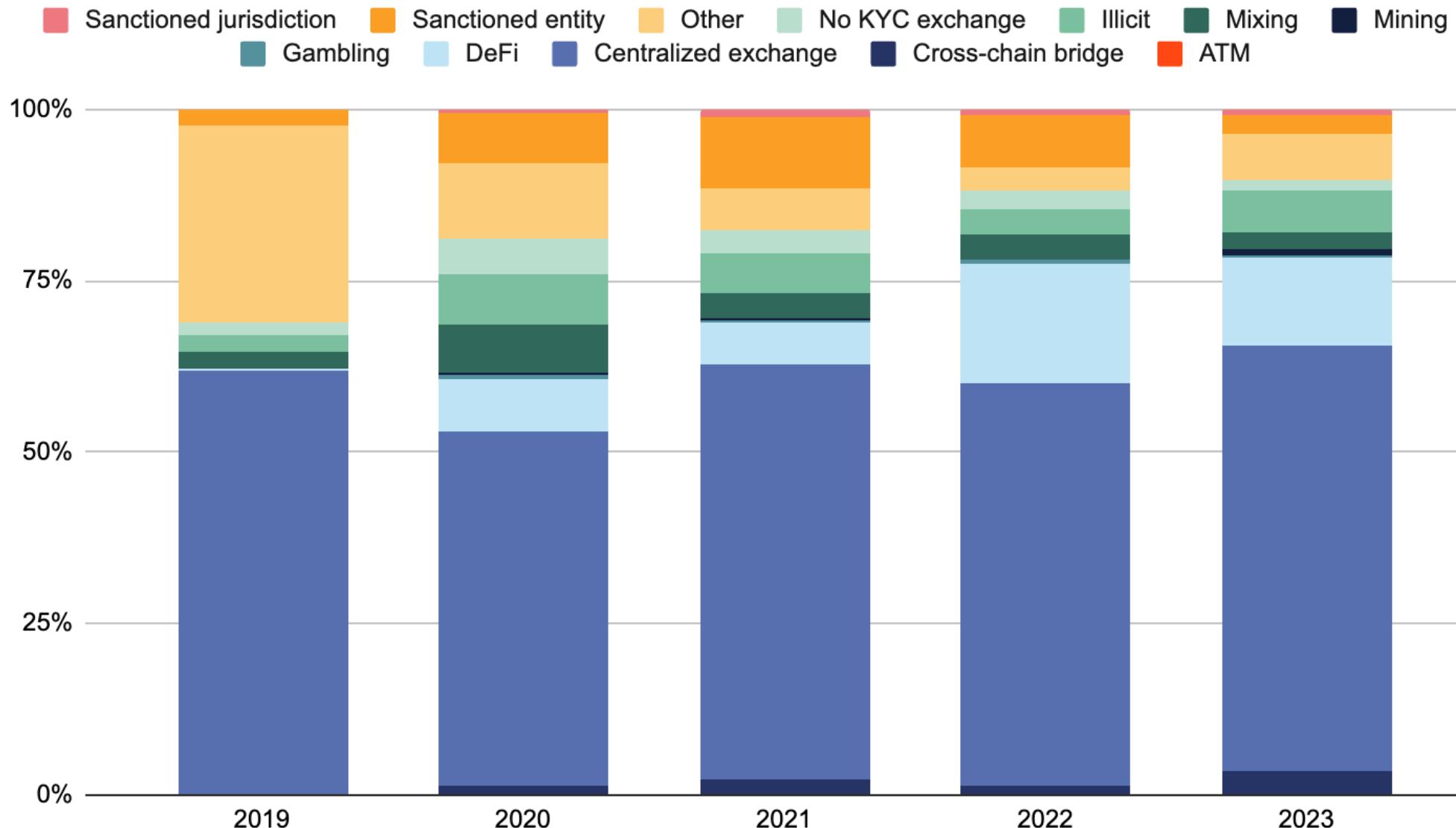
# Asset Type of Various Illicit Transactions

Illicit transaction volume by crime category and asset type

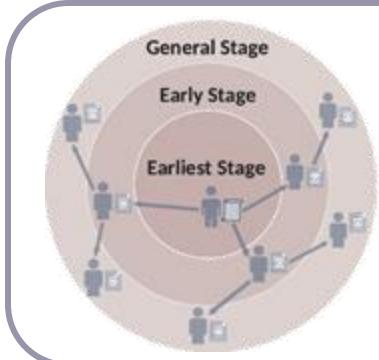
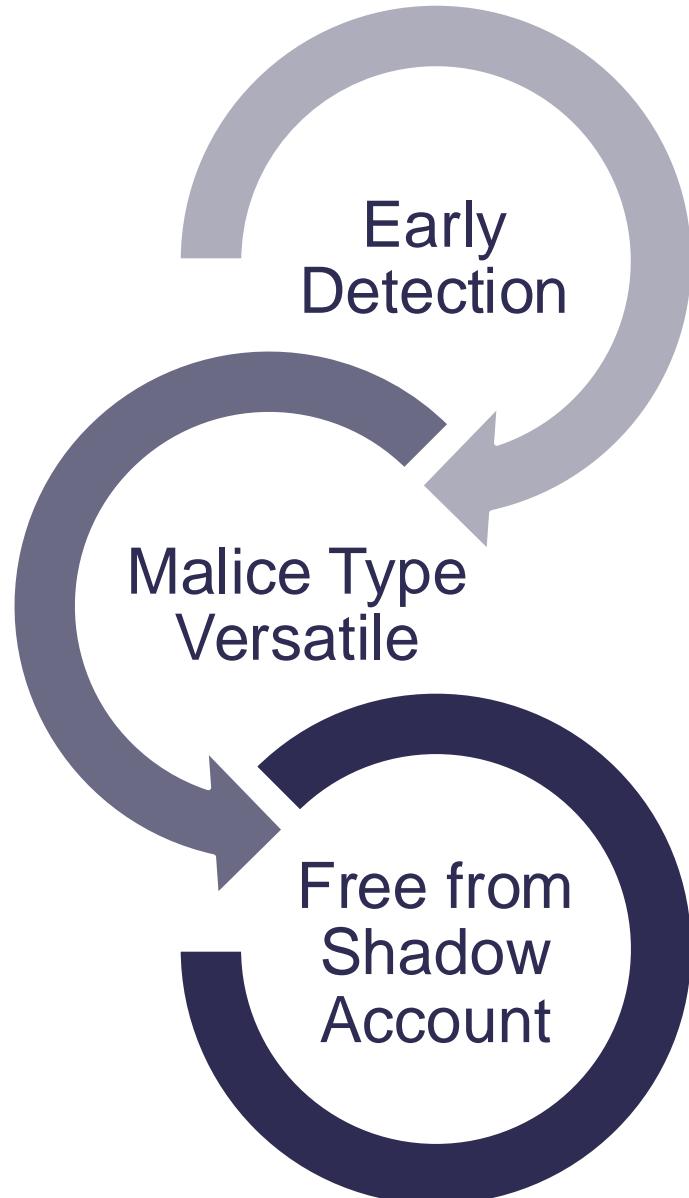


# Destination of Illicit Asset

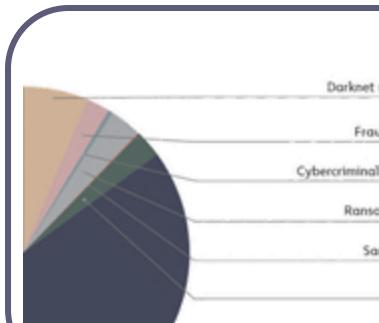
## Destination of funds leaving illicit wallets



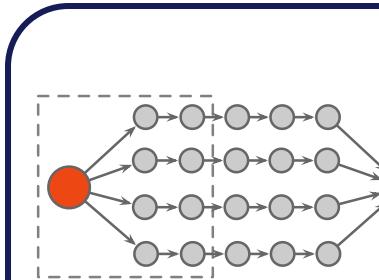
# Ideal Model



Most malice last for a short duration and cause damage if not be detected in the early stage.



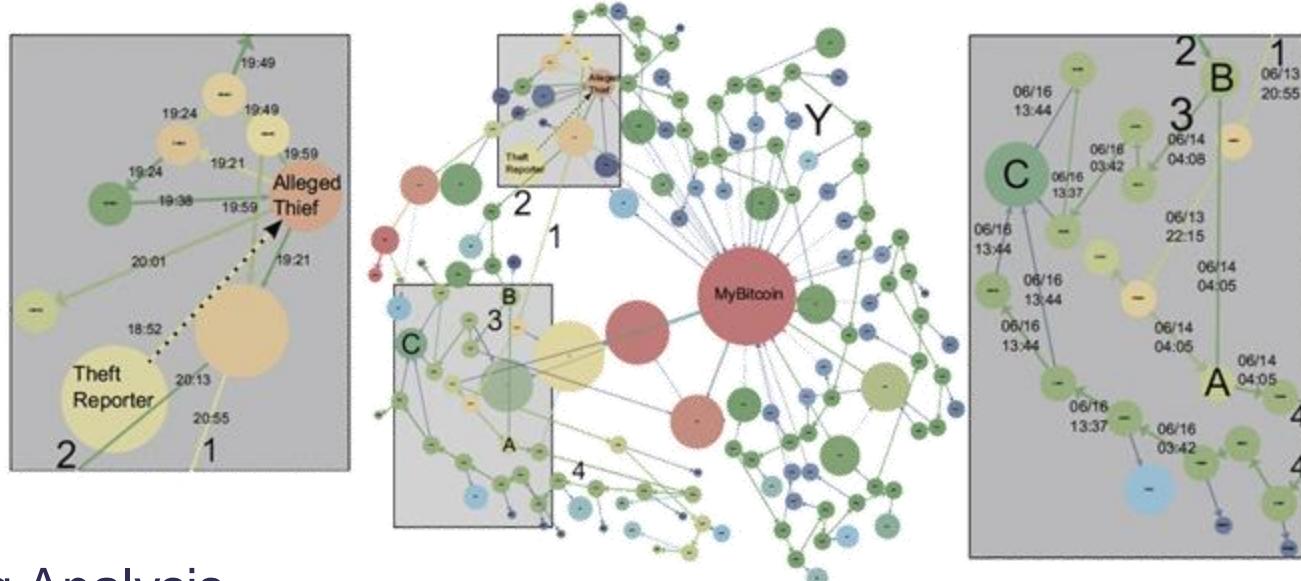
Malice types are constantly evolving. Manually-engineered features for a specific type cannot be generalized to others.



Most address transaction network methods suffer shadow address issues. These addresses introduce extremely long transfer chain.

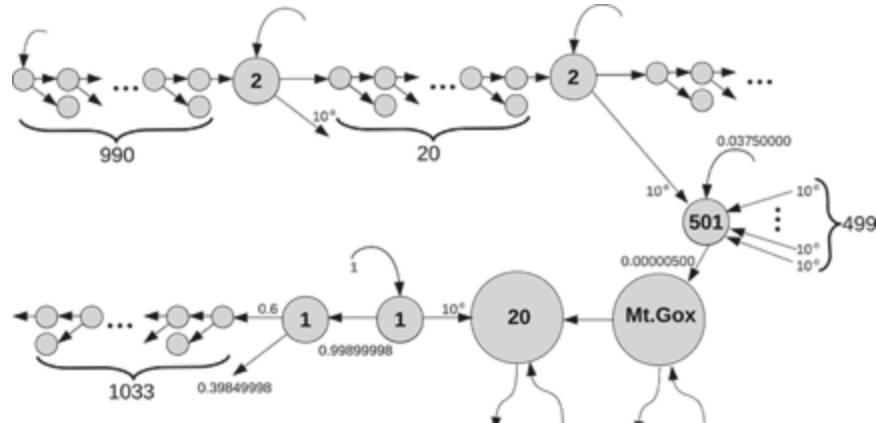
# Current Methods

## Visualization Based



- Scatter Center
- Hierarchical Transition
- Long Chain
- Self Loop

## Tracking Analysis



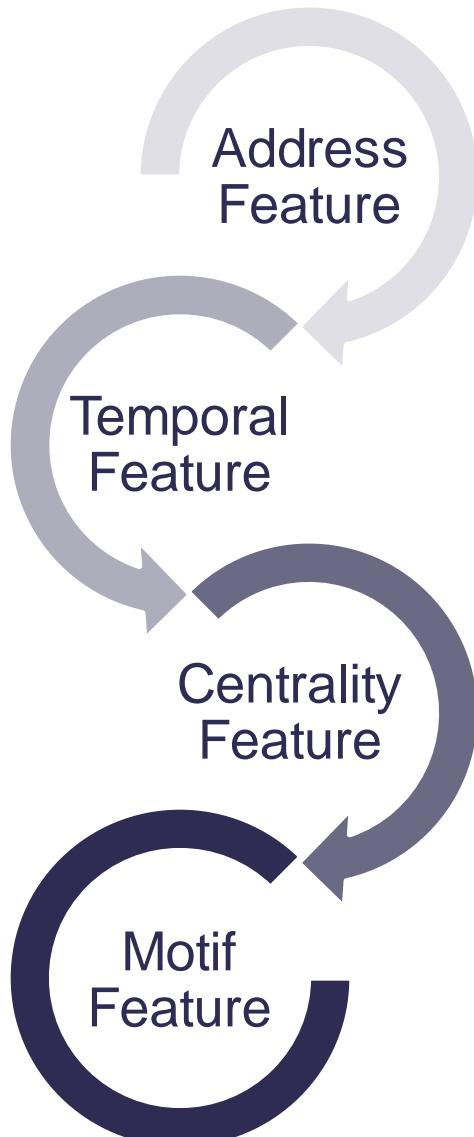
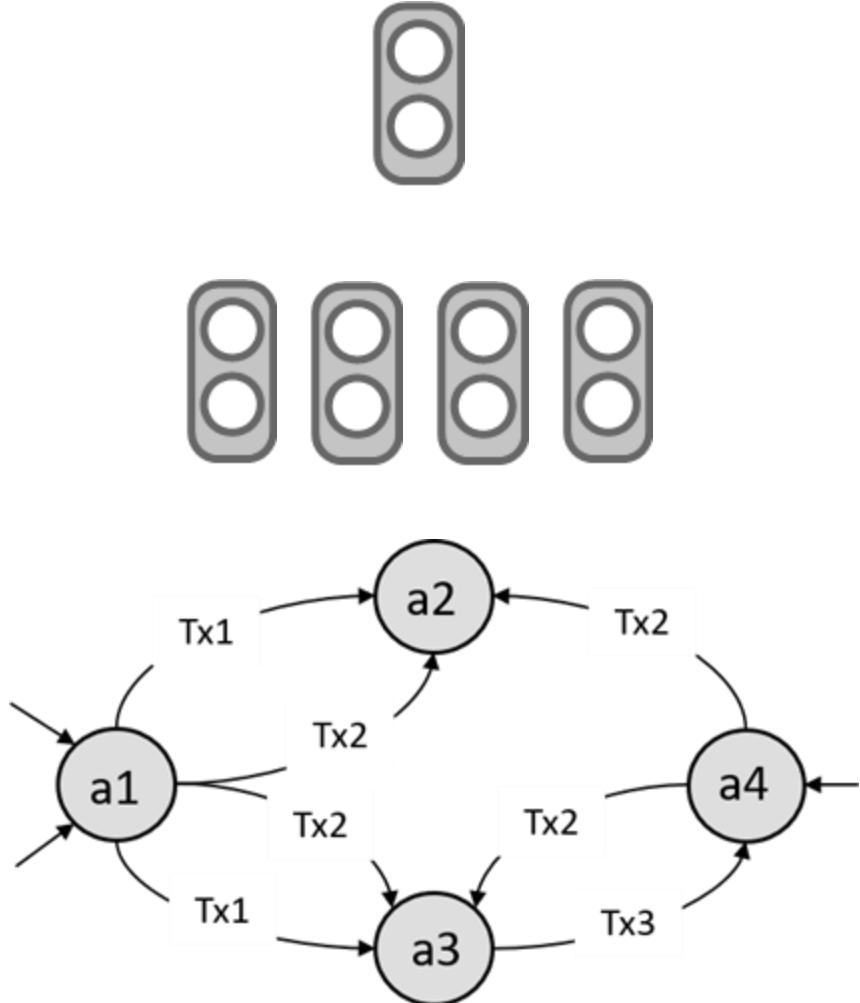
- Off-Chain Information
- Amount Analysis
- Money Source Tracking
- Temporal Pattern
- Heuristic Rule

1. Dorit Ron. "Quantitative Analysis of the Full Bitcoin Transaction Graph". FC(2012).

2. Chen, Shijian, et al. "The dark side of nfts: A large-scale empirical study of wash trading." Proceedings of the 15th Asia-Pacific Symposium on Internetworks. 2024

# Current Methods

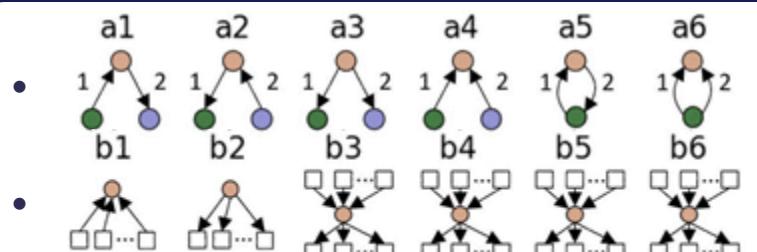
## Feature Engineering



- Total Token Received
- Token Balance
- Number of In/Out Transactions
- Number of Sibling Account

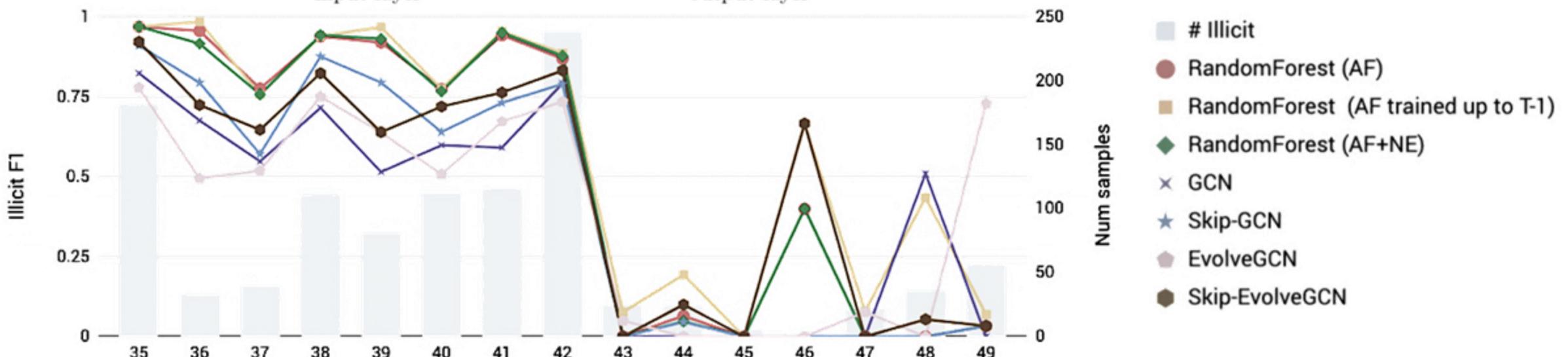
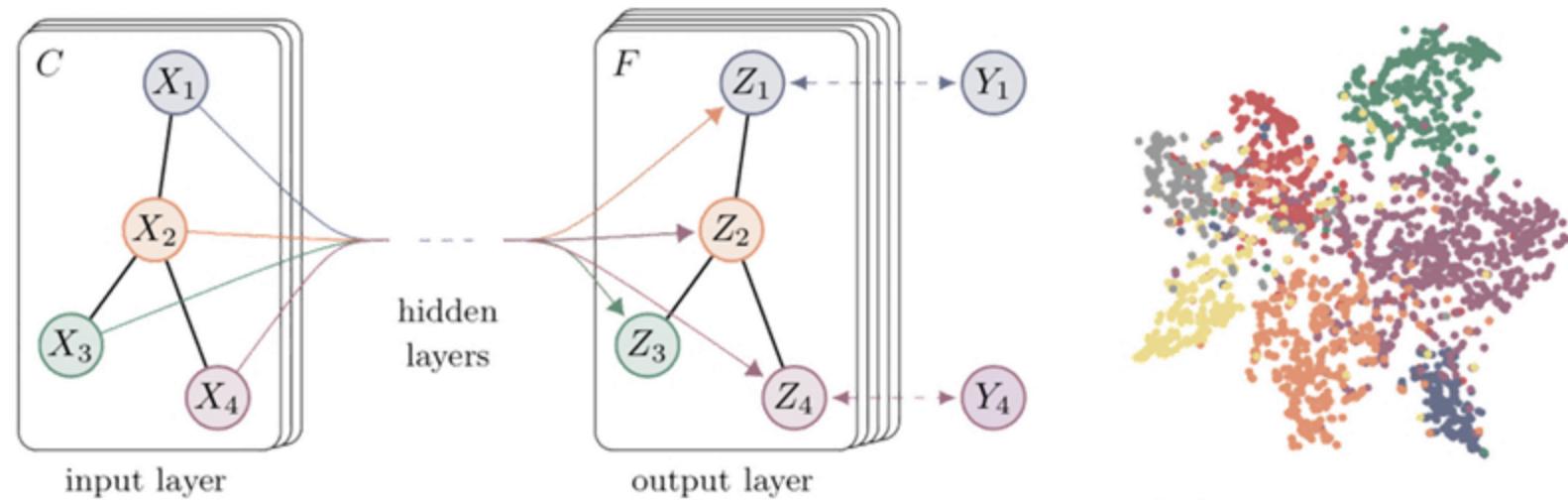
- Number of Active weeks
- Number of entity traded/week
- Number of receive/send days
- Activity period duration

- In/Out Degree
- Betweenness Centrality
- Closeness Centrality
- PageRank



# Current Methods

## Graph Neural Network



1. M. Weber, *et al.* “Anti-Money Laundering in Bitcoin: Experimenting with Graph Convolutional Networks for Financial Forensics” SIGKDD Workshop, 2019

2. M. Bartoletti, *et al.* “Data Mining for Detecting Bitcoin Ponzi Schemes” CVCBT, 2018

## Current Challenges

# Current Challenges

## Ineffective For Early Detection

### Hack of Binance of May 7, 2019. The path through Chipmixer

All of the transactions from table 1 were made in the time period from 06:41 to 15:17 on 2019-06-13 UTC. Our algorithm allows to determine the relationship between deposit transactions and transactions withdrawing BTC from Chipmixer and belonging to the same entity that made the deposit transaction. Using our algorithm, we found transactions that hackers used to withdraw funds from Chipmixer.

January 22, 2021 02:20 JST

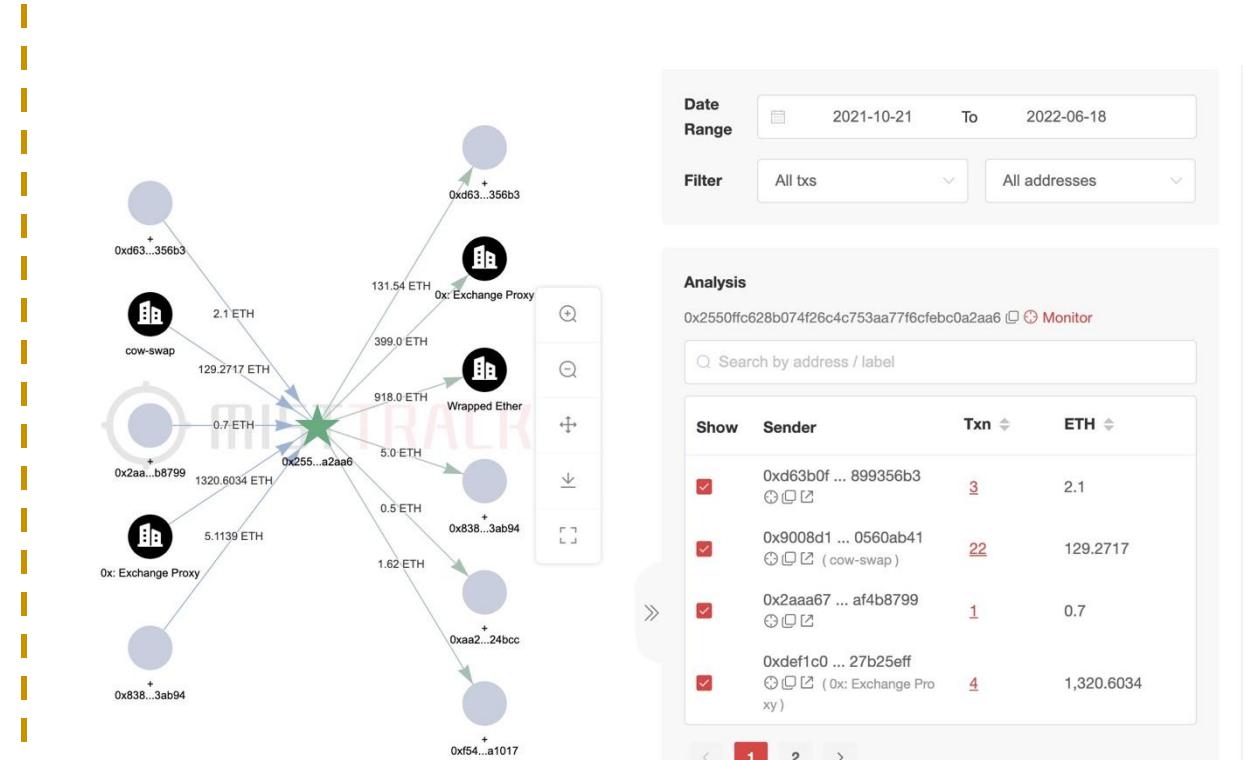
**Jan 22, 2021**

TOKYO -- Police in Japan have identified roughly 30 people for alleged involvement in illegal transactions stemming from 58 billion yen (\$530 million at the time) worth of NEM cryptocurrency hacked from the Coincheck exchange three years ago, Nikkei has learned.

The individuals have either been arrested or their cases have been referred to the prosecutors' office, according to a source familiar with the situation.

**Jan 27, 2018**

The [2018 attack](#) on one of Japan's leading cryptocurrency exchanges rattled investors and prompted increased regulatory oversight of the industry.



(Limited Info / Scalability) Issues for GNN

Date Range	2021-10-21	To	2022-06-18
Filter	All txs	All addresses	

# Current Challenges

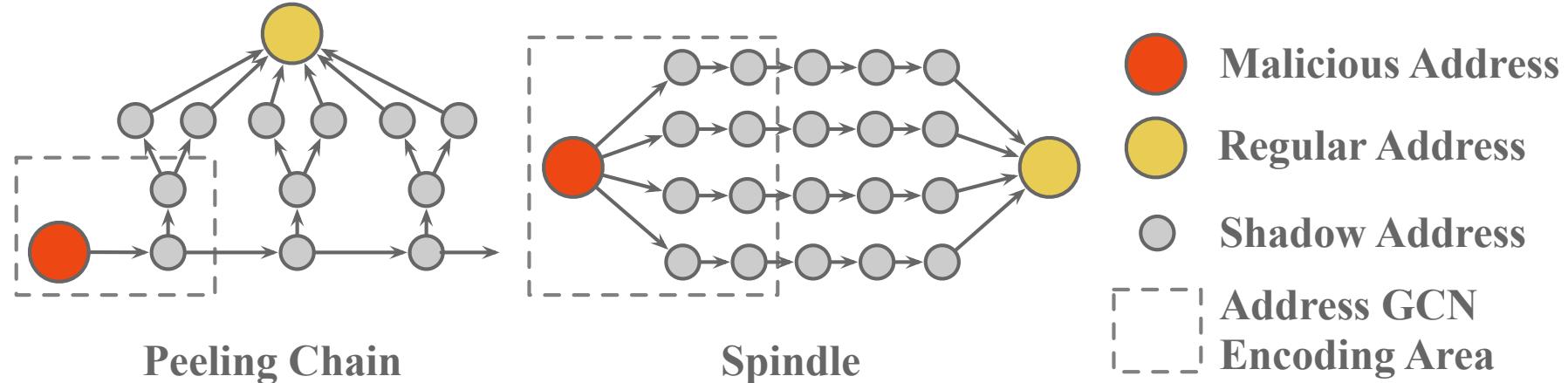
## Lack of Versatility

Ref.	Title	Authors	Publication Type	Year
[1]	A novel methodology for HYIP operators' Bitcoin addresses identification	K Toyoda et al.	Journal	2019
[2]	Improving Bitcoin ownership identification using transaction patterns analysis	TH Chang et al.	Journal	2020
[3]	Bitcoin mixing detection using deep autoencoder	L Nan et al.	Conference	2018
[4]	Identifying Bitcoin users using deep neural network	W Shao et al.	Conference	2018
[5]	Detecting mixing services via mining Bitcoin transaction network with hybrid motifs	J Wu et al.	Journal	2021
[6]	Bitcoin theft detection based on supervised machine learning algorithms	B Chen et al.	Journal	2021
[7]	Data mining for detecting Bitcoin Ponzi schemes	M Bartoletti et al.	Conference	2018
[8]	Anomaly detection in Bitcoin information networks with multi-constrained meta path	R Zhang et al.	Journal	2020
[9]	Characterizing and detecting money laundering activities on the Bitcoin network	Y Hu et al.	Journal	2019

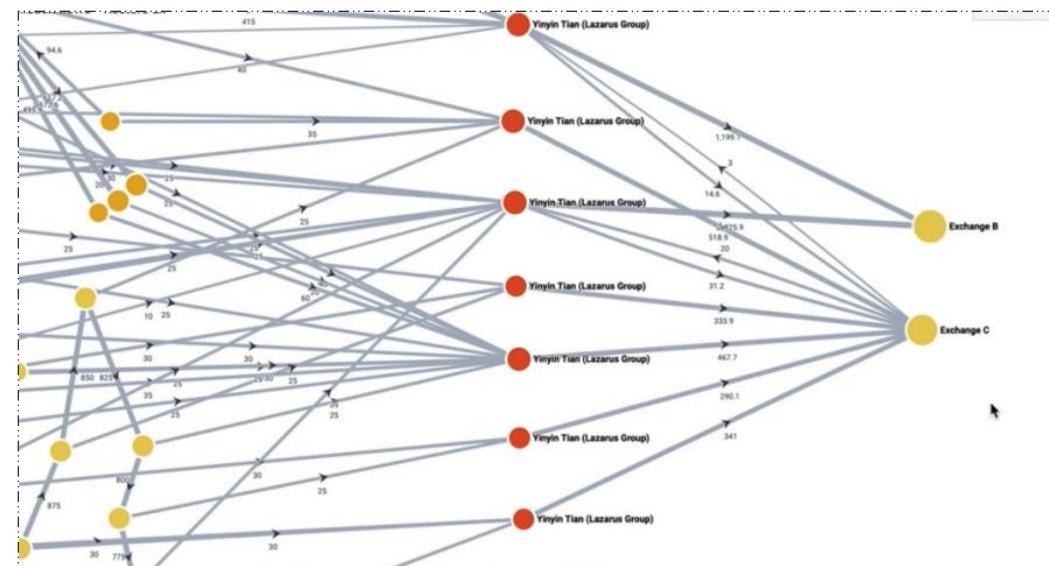
Most are based on interaction analysis with specific entities

# Current Challenges

## Suffer Shadow Account Issue



**ELLIPTIC**



1. <https://www.elliptic.co/blog/elliptic-analysis-bitcoin-bitfinex-theft>

2. [https://www.elliptic.co/hubfs/Elliptic\\_Using%20Blockchain%20Analysis%20to%20Mitigate%20Risk%202022%20sanctions.pdf](https://www.elliptic.co/hubfs/Elliptic_Using%20Blockchain%20Analysis%20to%20Mitigate%20Risk%202022%20sanctions.pdf)

# Outline

- Introduction to Blockchain
- **Hands-on case 1:** Rat Trading Detection Example
- Traditional Methods on Crypto Crime Detection
- **Hands-on case 2:** NFT Wash Trading Detection Example
- Transfer Path-based Methods
- **Hands-on case 3:** Scam Detection Using Asset Transfer Path

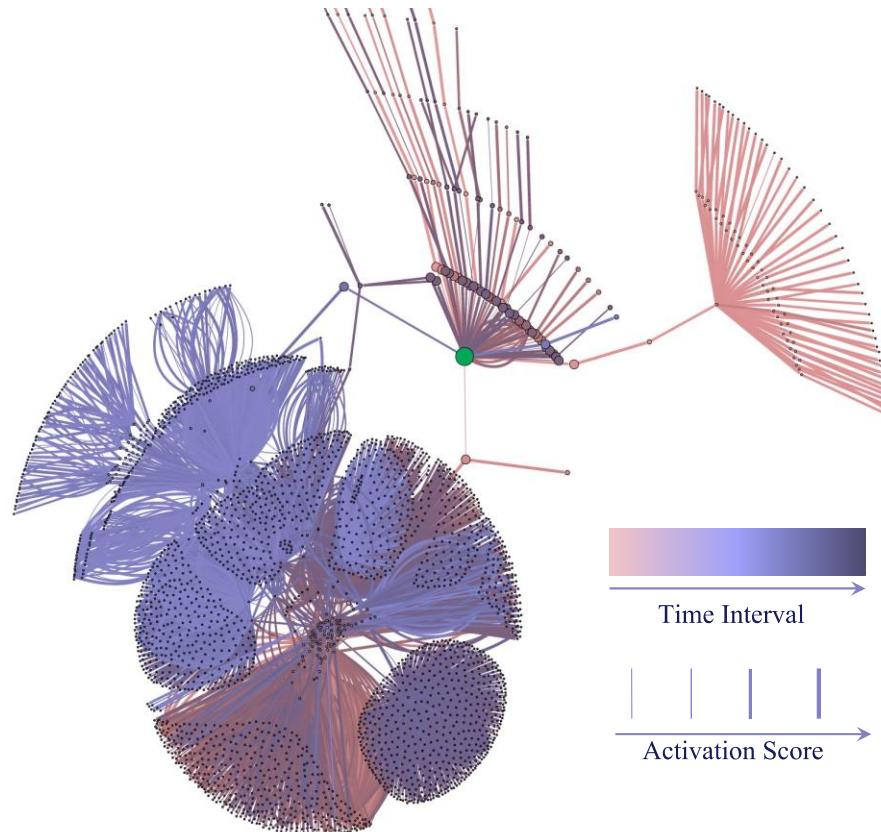
# Outline

- Introduction to Blockchain
- **Hands-on case 1:** Rat Trading Detection Example
- Traditional Methods on Crypto Crime Detection
- **Hands-on case 2:** NFT Wash Trading Detection Example
- Transfer Path-based Methods
- **Hands-on case 3:** Scam Detection Using Asset Transfer Path

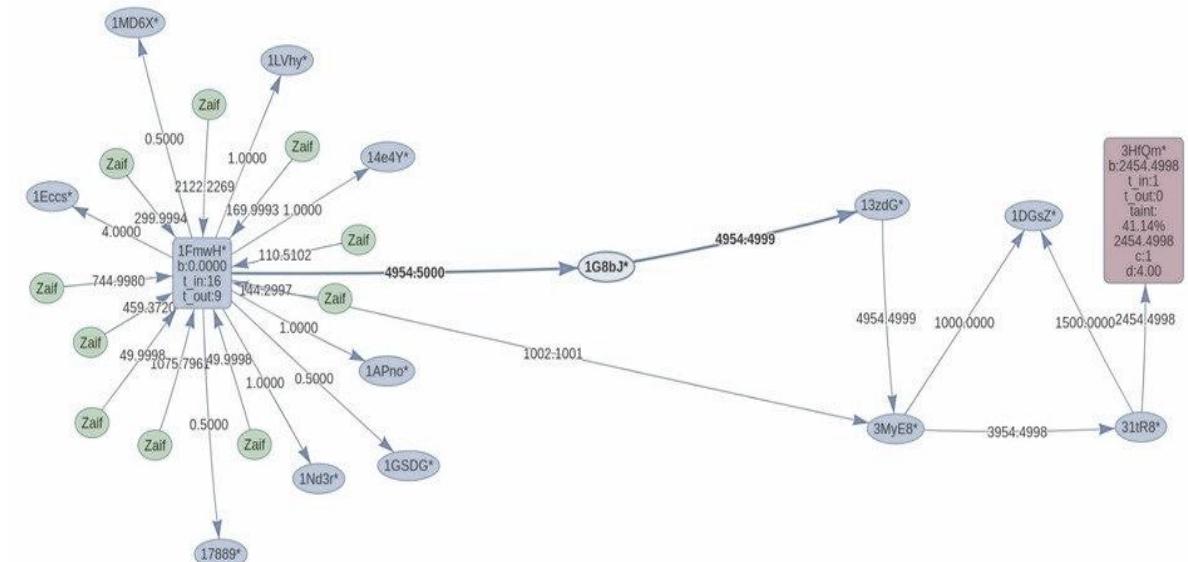
## Asset Transfer Path

# Asset Transfer Path

Asset Transfer Path  
of a Ponzi Scheme Address in One Hour



Address Transaction Graph  
of a Ponzi Scheme Address in Six Days



# Asset Transfer Path

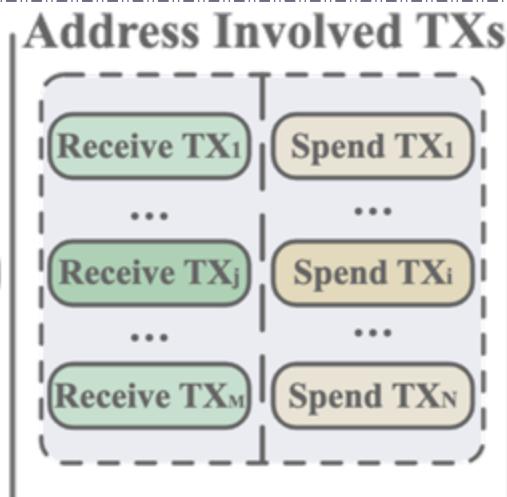
inputs: 3 (0.23154944 BTC)	unique addresses: 3, source transactions: 3	outputs: 11 (0.23072744 BTC)	unique addresses: 11, spent: 11 in 10 transactions
0. <a href="#">1AJCCxhKguHMdPW1Lw3RdkqXj9JVbGdQyg</a> 0.16311193 BTC <a href="#">99411a66...</a> 1. <a href="#">1CwXs1tbv5Dv3DN1HWLiit7thnjJ6DaVXfv</a> 0.01012727 BTC <a href="#">e224de23...</a> 2. <a href="#">1QGK4uWK43wWkheKyjMJHkUHWnmK8X2J6L</a> 0.05831024 BTC <a href="#">4fff7a1c...</a>		0. <a href="#">37CUkHnZL1fana8DVUBFTb9fj5kmk5amv9</a> 1. <a href="#">1CDMadTT4mzt2yrEBSKi78XFkdnfaiqy4h</a> 2. <a href="#">3PIAFWjTj8C29PbaKDju6SVb342rZZy1wd</a> 3. <a href="#">15EqXrJzeFhw63RBACXD5s4DgfcPvCpxvQ</a> 4. <a href="#">12YKAG1ARHFJTBNHu3v3pWgg3dZXMuP2i8</a> (change address) 5. <a href="#">12Wsn7Dvi8r97uDyRaMptkQKCvh8mD591</a> 6. <a href="#">1P92nSacpTn9VaVTvTkR5akbV5dpeuZU8R</a> 7. <a href="#">3JLEyDXPV14oW8N526PLX6tAAcRFde9Cp1</a> 8. <a href="#">1AQdmPW9GDm5kn576RA4ifYPhFKNmjmZnTL</a> 9. <a href="#">1NUxerSwgaAZ4LEx2YuT9B7rVFeHcDhDMD</a> (change address) 10. <a href="#">16MhAeYCYu8toj8YqSPe5K1ZqBMp3UjfF9</a>	Xapo.com 0.02189381 BTC <a href="#">b917046e...</a> BitoEX.com 0.02212267 BTC <a href="#">49fdc519...</a> [000004b74b] 0.02232449 BTC <a href="#">0c13c42f...</a> [0004fdeba6] 0.02212267 BTC <a href="#">2316ed2c...</a> (change address) 0.02189381 BTC <a href="#">47ddc53b...</a> BitBay.net 0.02211753 BTC <a href="#">7140669f...</a> [12ce0a21e7] 0.02197031 BTC <a href="#">8b51d3f6...</a> [f041f40b3e] 0.02211496 BTC <a href="#">a214787d...</a> BitBay.net 0.0219782 BTC <a href="#">185df6c8...</a> (change address) 0.01001968 BTC <a href="#">47ddc53b...</a> [974a2667bb] 0.02216931 BTC <a href="#">0cac457c...</a>



# Asset Transfer Path

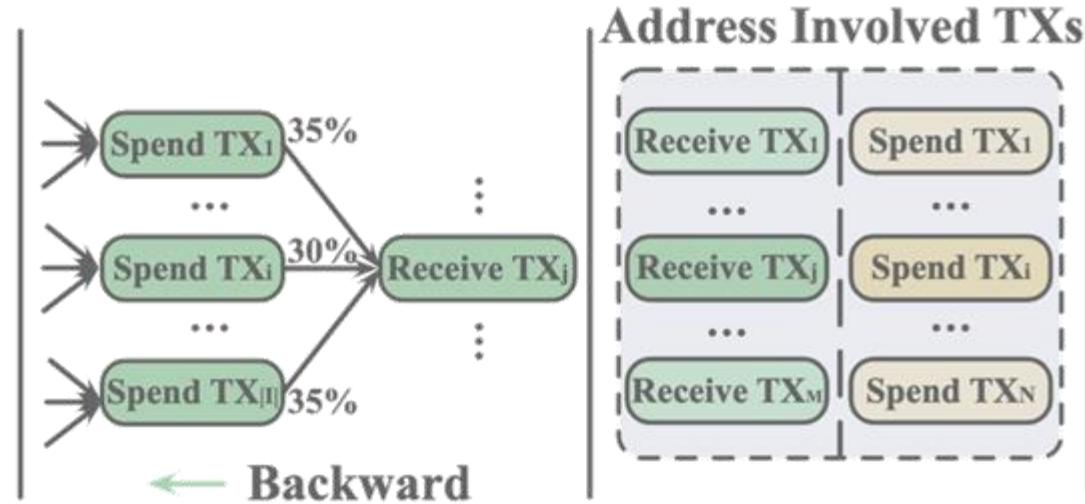
**Address 12Wsn7Dvi8r97uDRyRaMptkQKCvh8mD591**

date	received/sent	balance	transaction
2019-05-13 04:05:33	+0.00027707	0.00027707	<a href="#">c5fdd21f3e1aa3fe47e6ef30c067258c083995cdc626ffa8de3bc28c9497d40c</a>
2018-04-17 05:53:01	-0.00070748	0.	<a href="#">cd132839ee9171502c861fccalab473f72182c116a2eb0ac74c5a80faa128f42</a>
2018-04-16 13:00:59	-0.00009949	0.00070748	<a href="#">d59ec4527a33d182688d5f29b1c751f1f1999229377689264d945d96731e3f65</a>
2017-03-26 18:24:51	+0.00070748	0.00080697	<a href="#">lcb9943096cb1e71f0db154eac4e01f0fa68307c817eb831329cb566bf113f55</a>
2017-02-15 12:25:02	-0.0199187	0.00009949	<a href="#">46b3d8c98a8844c5f9246d48e0010fbf3c58b2b044d22964723b1e20ec0db84b</a>
2017-02-14 18:13:06	+0.0199187	0.02001819	<a href="#">2e7b537040427834801084709de62e40c689f9e87b7ea469d6c529316fa2c901</a>
2017-01-25 21:52:11	-0.02211753	0.00009949	<a href="#">7140669f90bb802bdcedd891f8889798c0cb39a5c7f5e99d2e9c44e7c1393b04</a>
2017-01-25 06:08:46	+0.02211753	0.02221702	<a href="#">d8f68e3bf4fea09bd2faa6cee294fecb1502611f1d590cfa4d42a9b2ccb578bd</a>



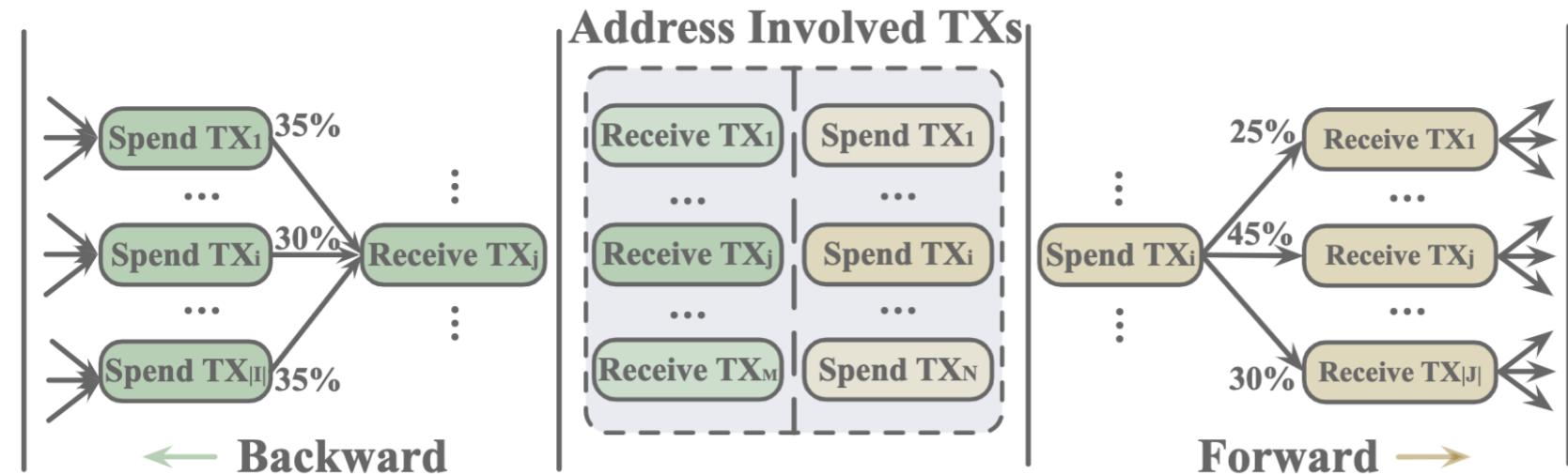
# Asset Transfer Path

inputs: 3 (0.23154944 BTC)	unique addresses: 3, source transactions: 3	outputs: 11 (0.23072744 BTC)	unique addresses: 11, spent: 11 in 10 transactions
0. <a href="#">1AJCCxhKquHMdPW1Lw3RdkqXj9JVbGdQyg</a> 1. <a href="#">1CwXs1tbv5Dv3DN1HWLii7thnjJ6DaVxfv</a> 2. <a href="#">1QGK4uWK43wWkheKyjMJHkUHWnmK8X2J6L</a>	0.16311193 BTC <a href="#">= 99411a66...</a> 0.01012727 BTC <a href="#">= e224de23...</a> 0.05831024 BTC <a href="#">= 4fff7a1c...</a>	0. <a href="#">37CUkHnZL1fana8DVUBFTb9fj5kmk5amv9</a> 1. <a href="#">1CDMadTT4mzt2yrEBSKi78XFkdnfaiqy4h</a> 2. <a href="#">3PiAFWjTj8C29PbaKDju6SVb342rZZy1wd</a> 3. <a href="#">15EqXrJzeFhw63RBACXD5s4DgfcPvCpxvQ</a> 4. <a href="#">12YKAG1ARHFJTBNhu3v3pWgg3dZXMuP2i8</a> 5. <a href="#">12Wsn7Dvi8r97uDRyRaMptkQKCvh8mD591</a> 6. <a href="#">1P92nSACPtn9VaVTvTkR5akbV5dpeuZU8R</a> 7. <a href="#">3JLEyDXPV14oW8N526PLX6tAAcRFde9Cp1</a> 8. <a href="#">1AQdmPW9GDm5kn576RA4ifYPhFKNjmZnTL</a> 9. <a href="#">1NUxerSwgaAZ4LEX2YuT9B7rVFeHcDhDMD</a> 10. <a href="#">16MhAeYCYu8toj8YqSPe5K1ZqBMp3UjfF9</a>	Xapo.com 0.02189381 BTC <a href="#">b917046e...</a> → BitoEX.com 0.02212267 BTC <a href="#">49fdc519...</a> → [000004b74b] 0.02232449 BTC <a href="#">0c13c42f...</a> → [0004fdeba6] 0.02212267 BTC <a href="#">2316ed2c...</a> → (change address) 0.02189381 BTC <a href="#">47ddc53b...</a> → BitBay.net 0.02211753 BTC <a href="#">7140669f...</a> → [12ce0a21e7] 0.02197031 BTC <a href="#">8b51d3f6...</a> → [f041f40b3e] 0.02211496 BTC <a href="#">a214787d...</a> → BitBay.net 0.0219782 BTC <a href="#">185df6c8...</a> → (change address) 0.01001968 BTC <a href="#">47ddc53b...</a> → [974a2667bb] 0.02216931 BTC <a href="#">0cac457c...</a> →



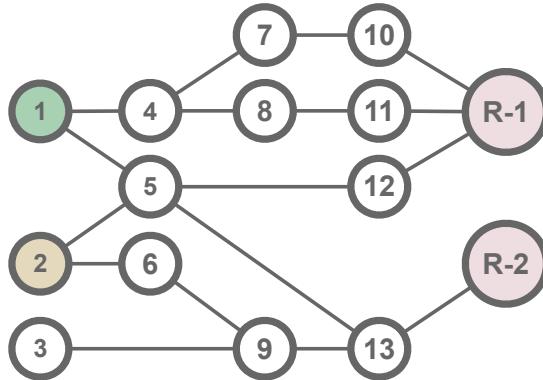
# Asset Transfer Path

inputs: 9 (11.93696663 BTC)	unique addresses: 9, source transactions: 9	outputs: 3 (11.93656663 BTC)	unique addresses: 3, spent: 3 in 3 transactions
0. <a href="#">1MNT5jyLgGT4LLHLxb4rBR4WwvPRwdm29T</a> 1. <a href="#">16HLm2oN8RQiw59MLf8MVYK5dHLB3Uopif</a> 2. <a href="#">12nqKog2nZYdD2SRpc7cHC1cWHQMhMvbPm</a> 3. <a href="#">1HWC1FL2oiTYSjBx3aFT9wXDjw69bDJYGs</a> 4. <a href="#">1428rdeHpxxubM78iSuQwN3YQEExas2uEX5</a> 5. <a href="#">1L3C72iVEGkTe3tSGMo9i8KQp4cLLa12fo</a> 6. <a href="#">14kLma2S3mgkG9gscuccujyrwLfPkPFAz1ie</a> 7. <a href="#">16eDbjoZDfqE4CABfthLtGEzwHUGjzoV82</a> 8. <a href="#">15fvnjndHFpvw6ZiP2NaNRCCofJPokwBBJ</a>	2.67453808 BTC ↳ <a href="#">e48bfa1c...</a> 0.97887336 BTC ↳ <a href="#">08ec7df8...</a> 1.08136061 BTC ↳ <a href="#">197ce3b0...</a> 0.48990209 BTC ↳ <a href="#">e93dc2c1...</a> 0.64988311 BTC ↳ <a href="#">54c3203c...</a> 5.00401953 BTC ↳ <a href="#">02848604...</a> 0.54212169 BTC ↳ <a href="#">5ebad0a7...</a> 0.50807124 BTC ↳ <a href="#">c8d51223...</a> 0.00819692 BTC ↳ <a href="#">2faef535...</a>	0. <a href="#">1DcCYAB5JoCCFittnTehFYhHX5P2uKMpw3</a> 1. <a href="#">15xboUZd3Tmaq3P9fhqxJ2muuZYLw5pWQX</a> 2. <a href="#">1G25ESCWCUGxaimhqvd2PNcZ6seSg9HnzC</a>	[1e3a5d41d2] 11.88 BTC <a href="#">3c725cf9... ↳</a> [429c2956d3] 0.04876971 BTC <a href="#">fc8c6309... ↳</a> [434d20f284] 0.00779692 BTC <a href="#">49bb8226... ↳</a>

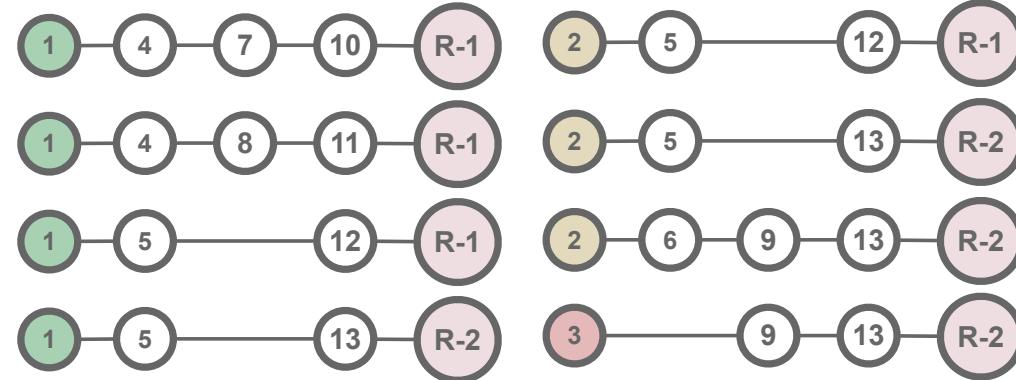


# Asset Transfer Path Graph

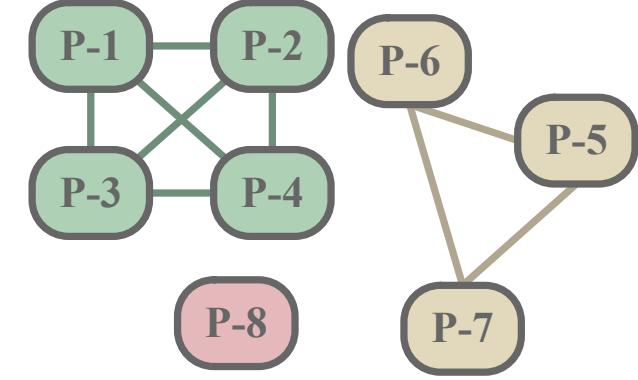
Asset Flow of Receive TX



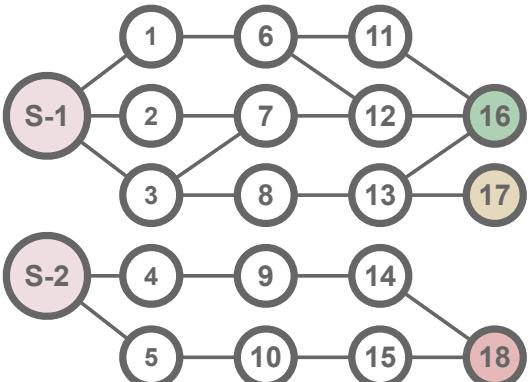
Backward Asset Transfer Path



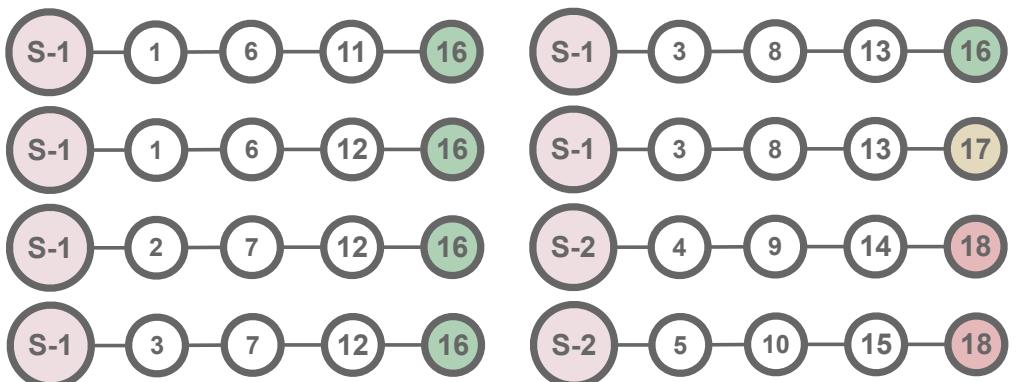
Backward Path Graph



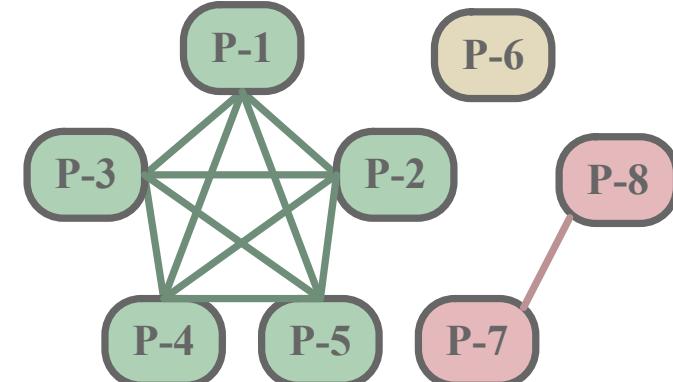
Asset Flow of Spend TX



Forward Asset Transfer Path

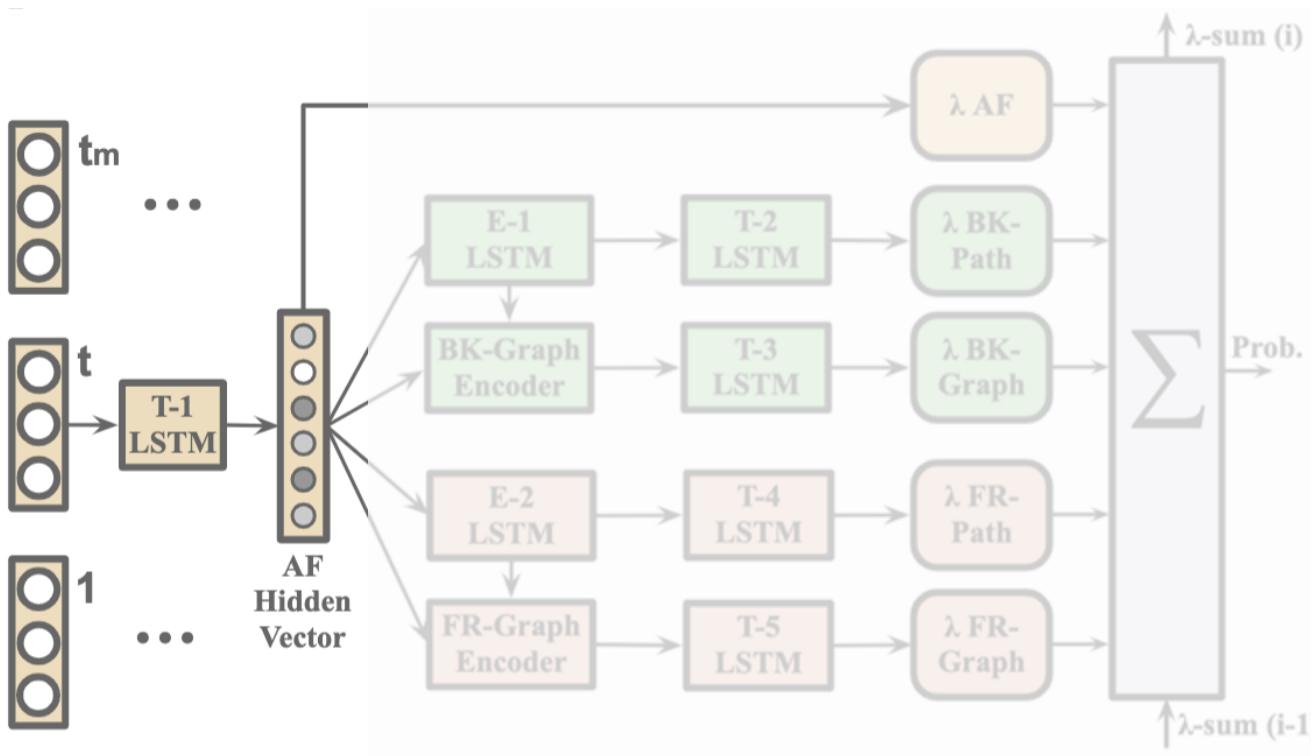


Forward Path Graph



# Evolve Path Tracer

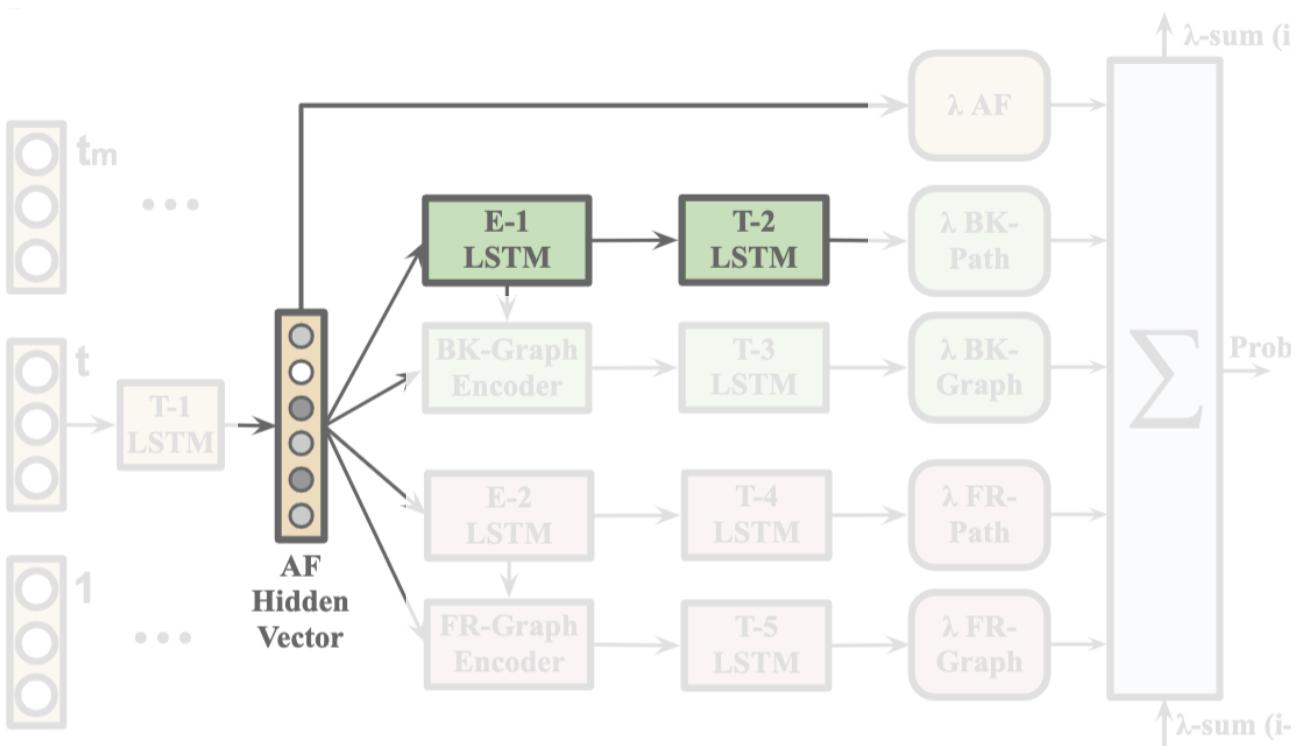
# Evolve Path Tracer



- Input current AF into T1 LSTM to get the T1 hidden vector  $h_t^{T_1}$ .

$$h_t^{T_1}, c_t^{T_1} = \text{LSTM}^{T_1}(f_t^u, h_{t-1}^{T_1}, c_{t-1}^{T_1})$$

# Evolve Path Tracer



- Concatenate  $h_t^{T_1}$  with  $h_{t-1}^{T_2}$  to generate parameters for **E1-LSTM**, encodes paths to path vectors.

$$h_j^{E_1}, c_j^{E_1} = \text{LSTM}^{E_1}([h_t^{T_1} || h_{t-1}^{T_2}], h_{j-1}^{E_1}, c_{j-1}^{E_1})$$

**Evolve Kernel**

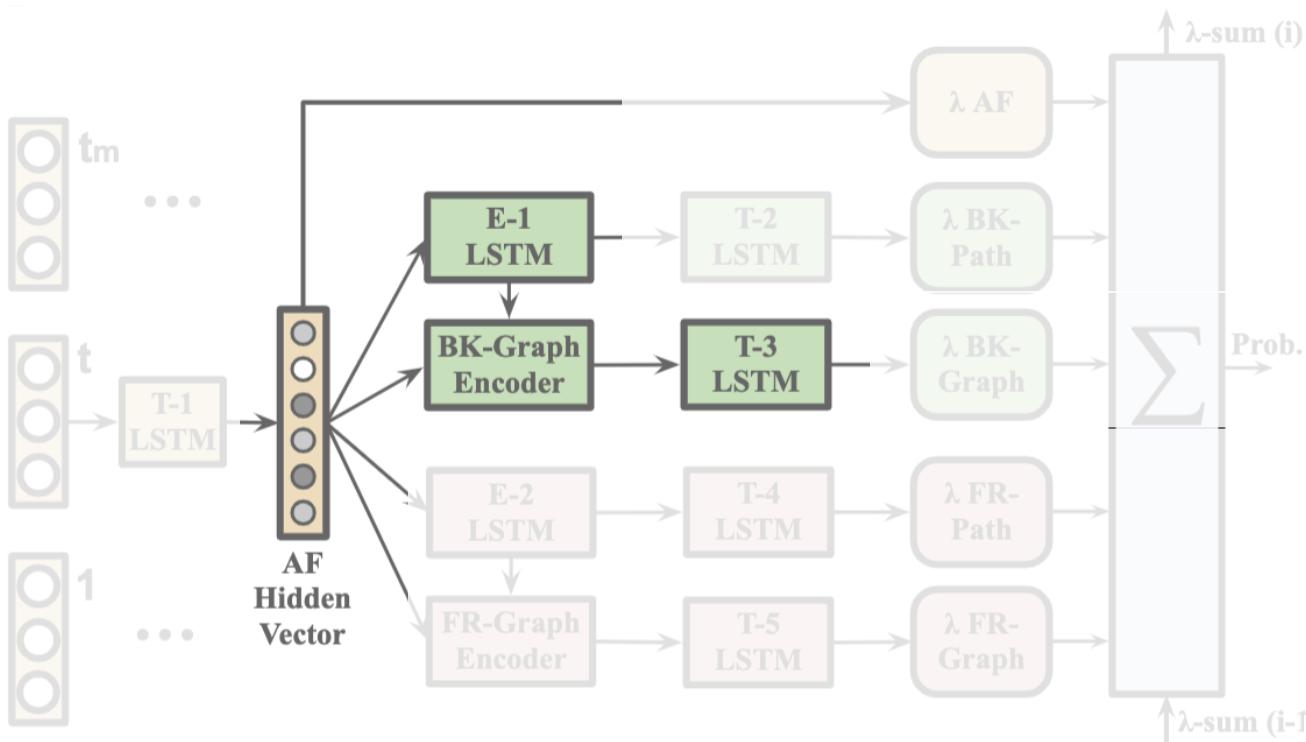
- Then **weighted sum** them to update **T2-LSTM**  $h_t^{T_2}$

$$a_{i,t}^j = W^{a,j} \tanh(W^{p,u} [f_{i,t}^p || h_t^{T_1}]); \quad \alpha_{i,t}^j = \text{Softmax}(a_{i,t}^j),$$

$$\hat{f}_t^p = \sum_{j=1}^{N_{E_1}} \hat{f}_t^{p,j}; \quad f_t^{p,j} = \sum_{i=1}^{N_{E_1}} \alpha_{i,t}^j f_{i,t}^p,$$

$$h_t^{T_2}, c_t^{T_2} = \text{LSTM}^{T_2}(\hat{f}_t^p, h_{t-1}^{T_2}, c_{t-1}^{T_2})$$

# Evolve Path Tracer



- Concatenate  $h_t^{T_1}$  with  $h_{t-1}^{T_3}$  to generate parameters for BK-Graph Encoder to update path vectors with graph info. Similarly, weighted sum them to update T3-LSTM  $h_t^{T_3}$ .

$$H_t^g = [h_t^{T_1} || h_{t-1}^{T_3}], \quad \text{Evolve Kernel}$$

$$f_t^g = \sigma(\tilde{\mathcal{D}}^{-\frac{1}{2}} \tilde{\mathcal{A}} \tilde{\mathcal{D}}^{-\frac{1}{2}} (f_t^p W^g H_t^g)),$$

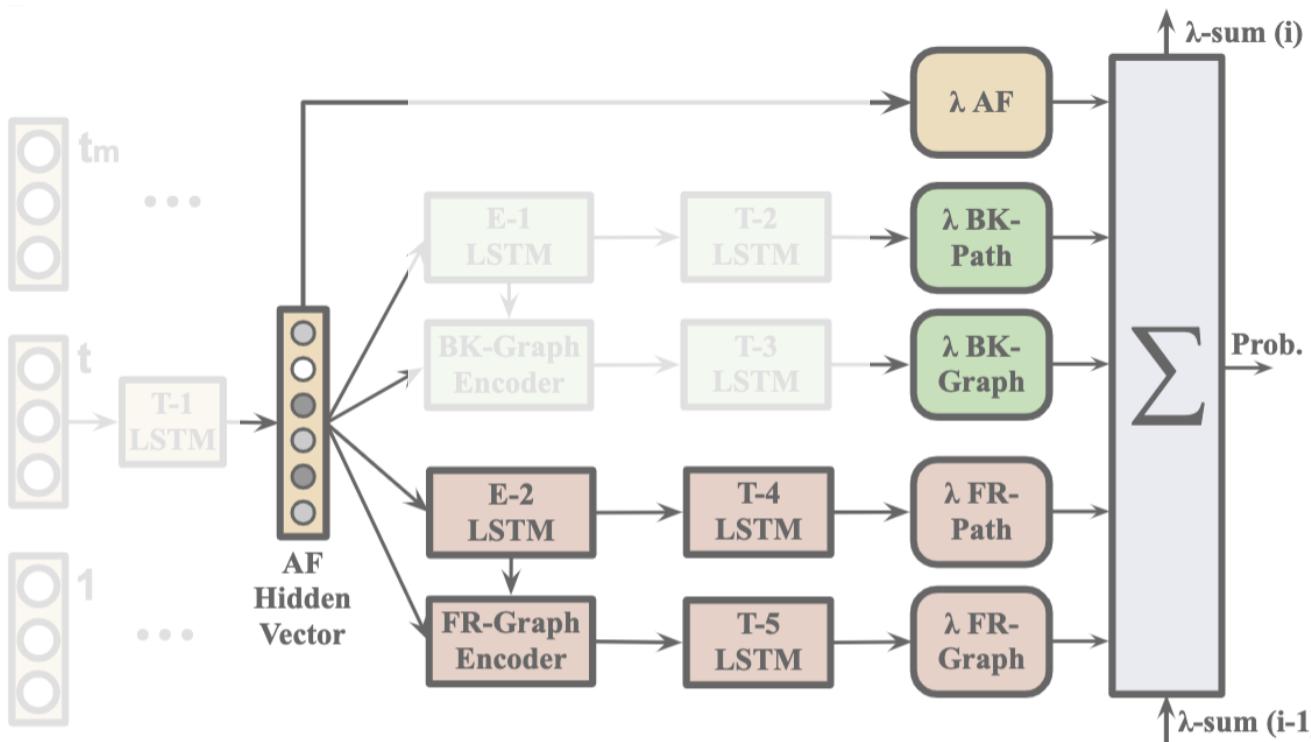
$$\tilde{\mathcal{A}} = \mathcal{A} + I; \quad \mathcal{A}_{i,:j} = (W^e H_t^g) S_{i,j},$$

$$\tilde{\mathcal{D}} = \text{diag}\left(\sum_j (A_{i,j} + I_{i,j})\right),$$

$$h_t^{T_3}, c_t^{T_3} = \text{LSTM}^{T_3}(f_t^g, h_{t-1}^{T_3}, c_{t-1}^{T_3}).$$

# Evolve Path Tracer

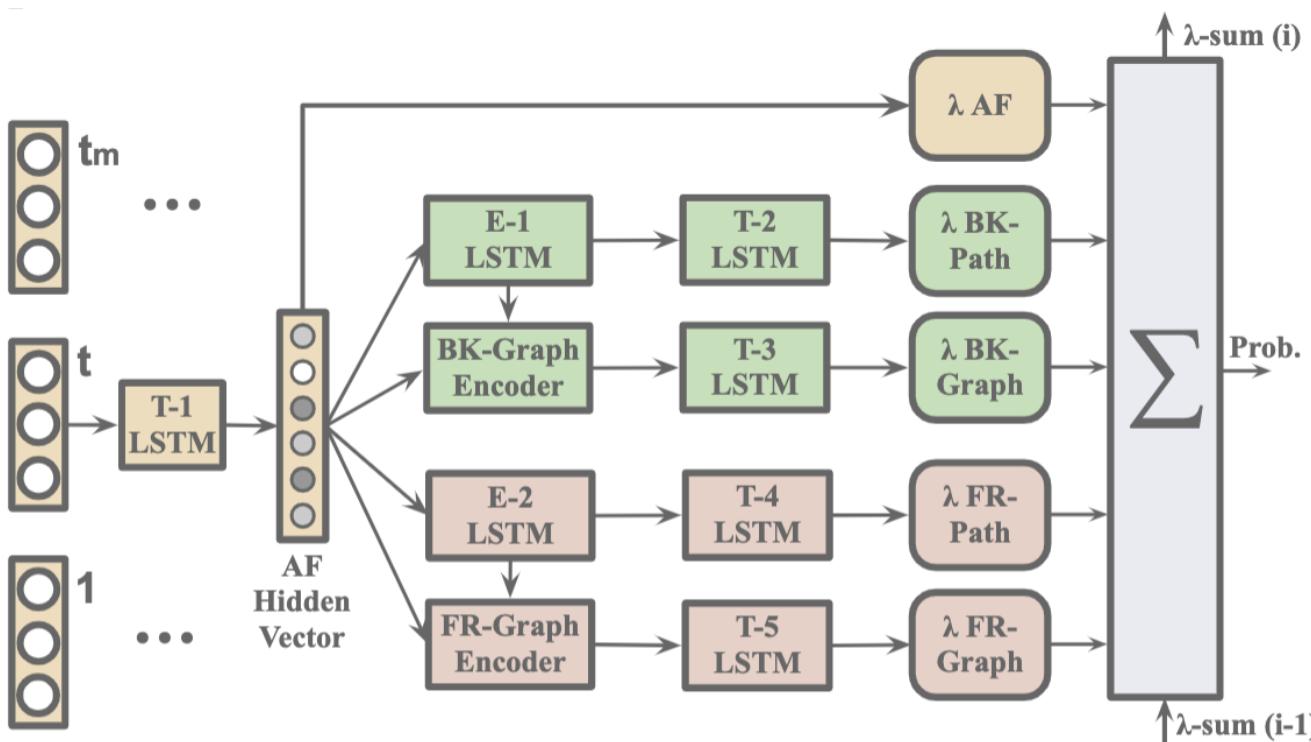
- Same processing for the **forward branch**, use  $h_t^{T_1} \sim h_t^{T_5}$  to predict the current label for the given address.



$$\lambda_{j,t} = \tanh(W_{T_j}^{hz} h_t^{T_j}),$$

$$\hat{y}^t = \exp(-\text{ReLU}(\sum_{i=1}^t \sum_{j=1}^5 \lambda_{j,i})),$$

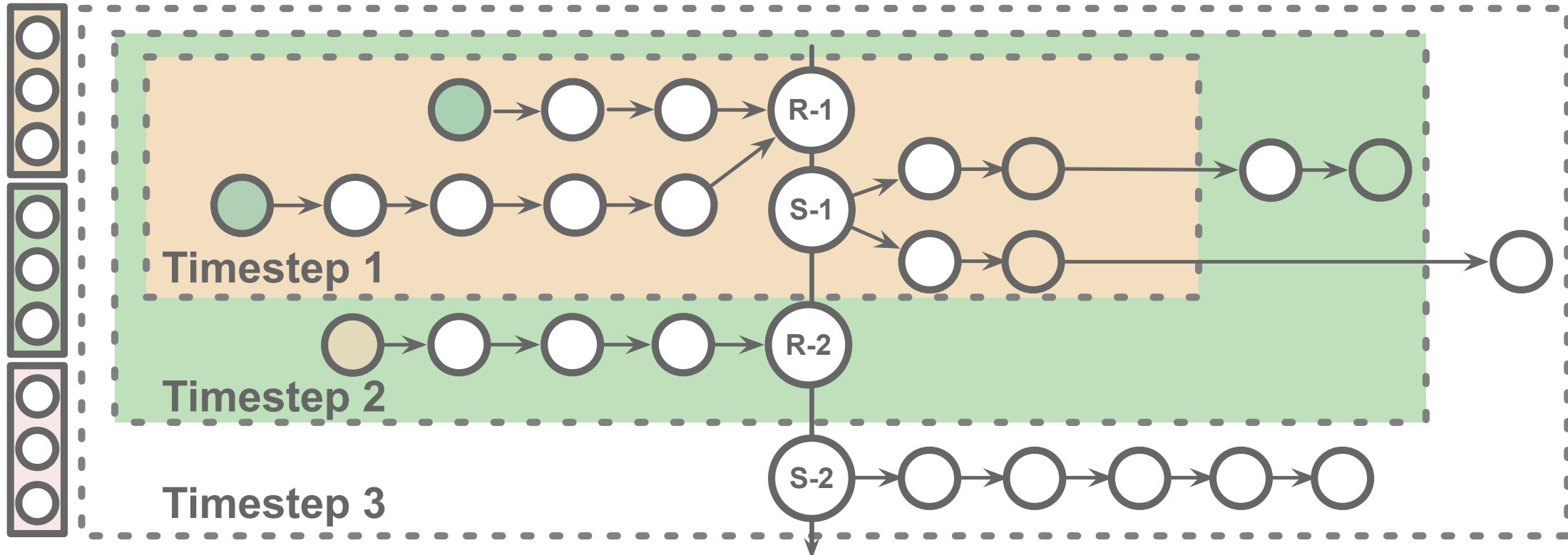
# Evolve Path Tracer



- Input **current AF** into T1 LSTM to get the T1 hidden vector  $h_t^{T1}$ .
- Concatenate  $h_t^{T1}$  with **previous hidden vectors** of T2 and T3 LSTM ( $h_{t-1}^{T2}, h_{t-1}^{T3}$ ) to generate parameters for **E1-LSTM** and **BK-Graph Encoder**.
- E1-LSTM encodes paths to **path vectors**. Then **weighted sum** them to update T2-LSTM  $h_t^{T2}$ .
- BK-Graph Encoder updates path vectors with **graph info**. Similarly, **weighted sum** them to update T3-LSTM  $h_t^{T3}$ .
- **Same processing** for the **forward branch**, use  $h_t^{T1} \sim h_t^{T5}$  to predict the current label for the given address.

# Asset Transfer Path

## Evolution of Asset Transfer Path



# Experiments

- Basic Settings

**Table 1: Dataset Statistics**

Type	Definition	Posi.	Nega.	P/N(%)
H	Hack and steal tokens	302	6582	4.03
R	Encrypt data for ransoms	3224	21100	15.28
D	Illegal BTC darknets	5838	109937	5.31

$$F1^E = \frac{\sum_{i=1}^N F1_i / \sqrt{i}}{\sum_{i=1}^N 1 / \sqrt{i}},$$

$$F1^C = \frac{\sum_{i=1}^{N-1} \sqrt{i} \times F1_i \times \mathbb{1}_{y_c}(y_i)}{\sum_{i=1}^{N-1} \sqrt{i}},$$

- Ablation Study

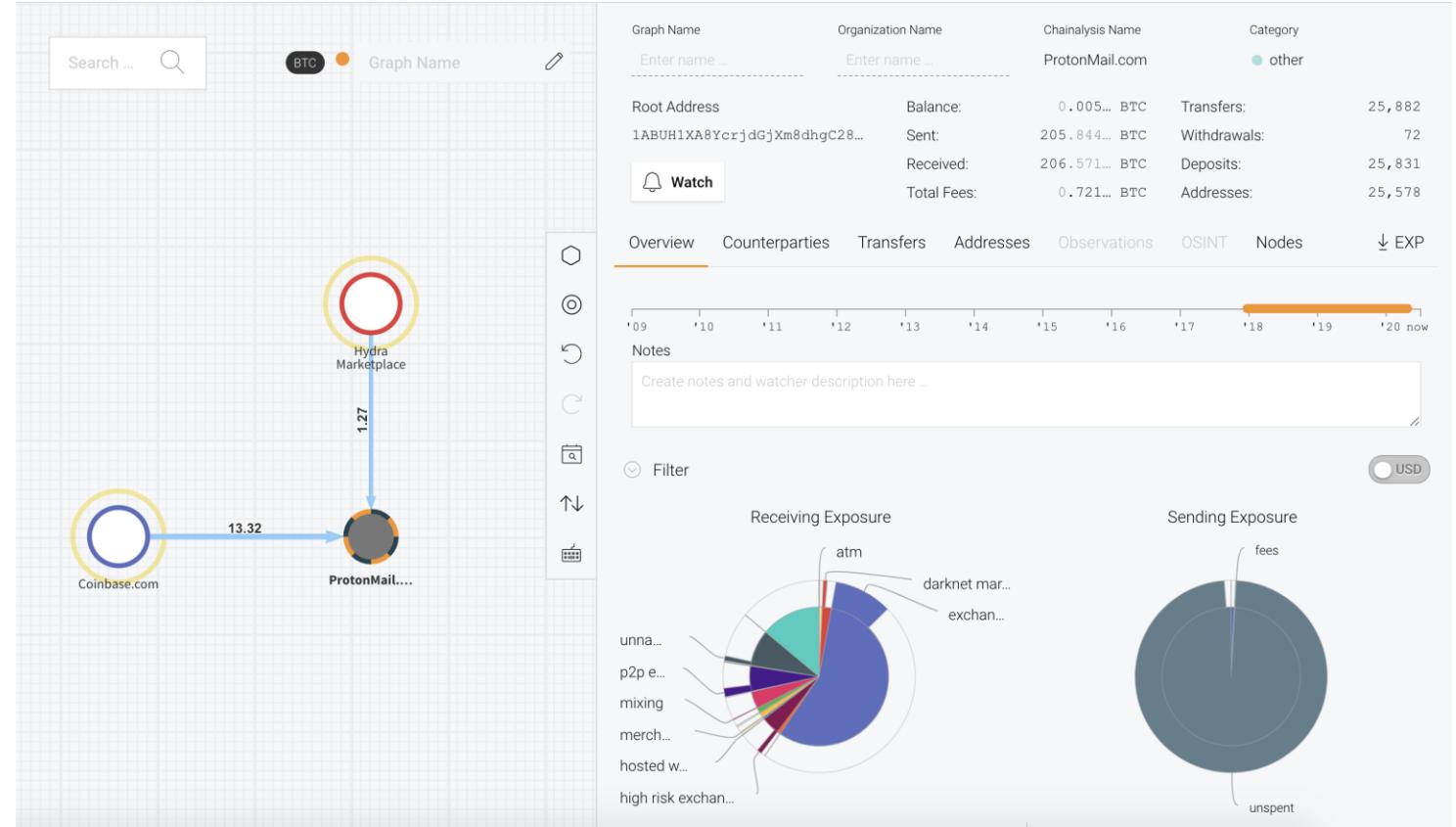
	Model	Acc.	Prec.	Rec.	$F1^E$	$F1^C$
H	AF	0.920	0.309	<b>0.590</b>	0.389	0.412
	+Path	0.954	0.537	0.546	0.509	0.538
	+Graph	<b>0.965</b>	<b>0.686</b>	0.476	0.545	0.559
	+Evolve	0.961	0.606	0.553	<b>0.551</b>	<b>0.576</b>
R	AF	0.911	0.710	0.632	0.626	0.628
	+Path	0.929	0.727	0.805	0.760	0.765
	+Graph	0.927	0.696	<b>0.875</b>	0.773	0.776
	+Evolve	<b>0.937</b>	<b>0.735</b>	0.871	<b>0.795</b>	<b>0.798</b>
D	AF	0.961	0.619	0.571	0.611	0.604
	+Path	0.961	0.611	0.693	0.649	0.650
	+Graph	0.960	0.586	<b>0.804</b>	0.678	0.678
	+Evolve	<b>0.963</b>	<b>0.626</b>	0.758	<b>0.685</b>	<b>0.685</b>

# Analysis of Address Intention (Illicit Activity)

# Current Challenges

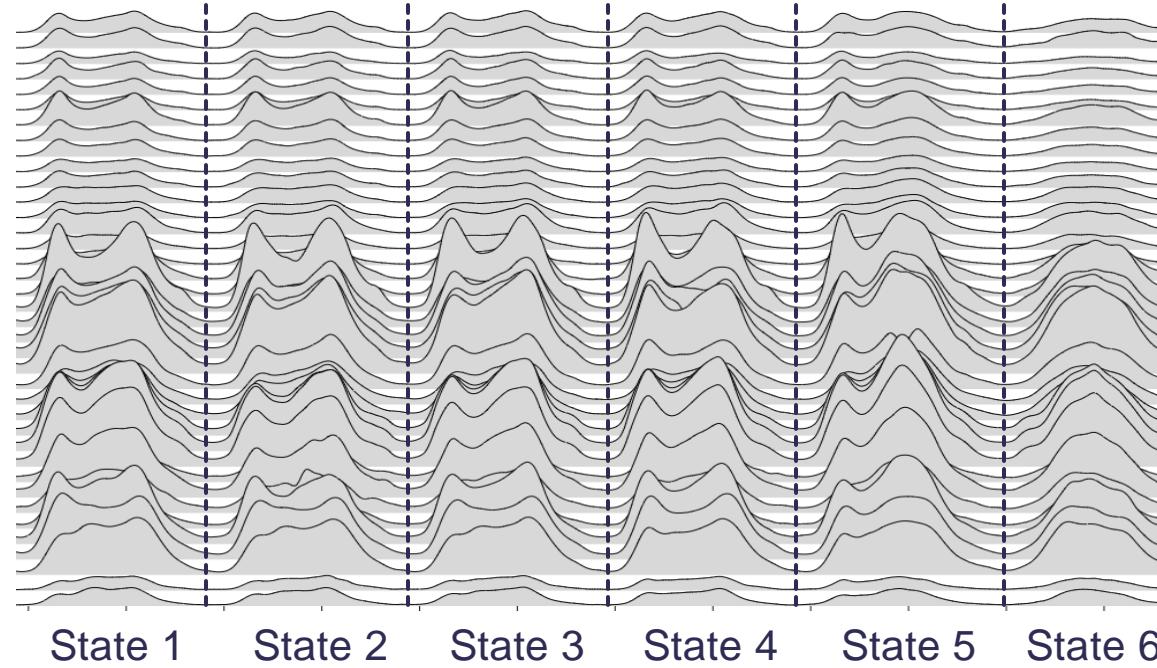
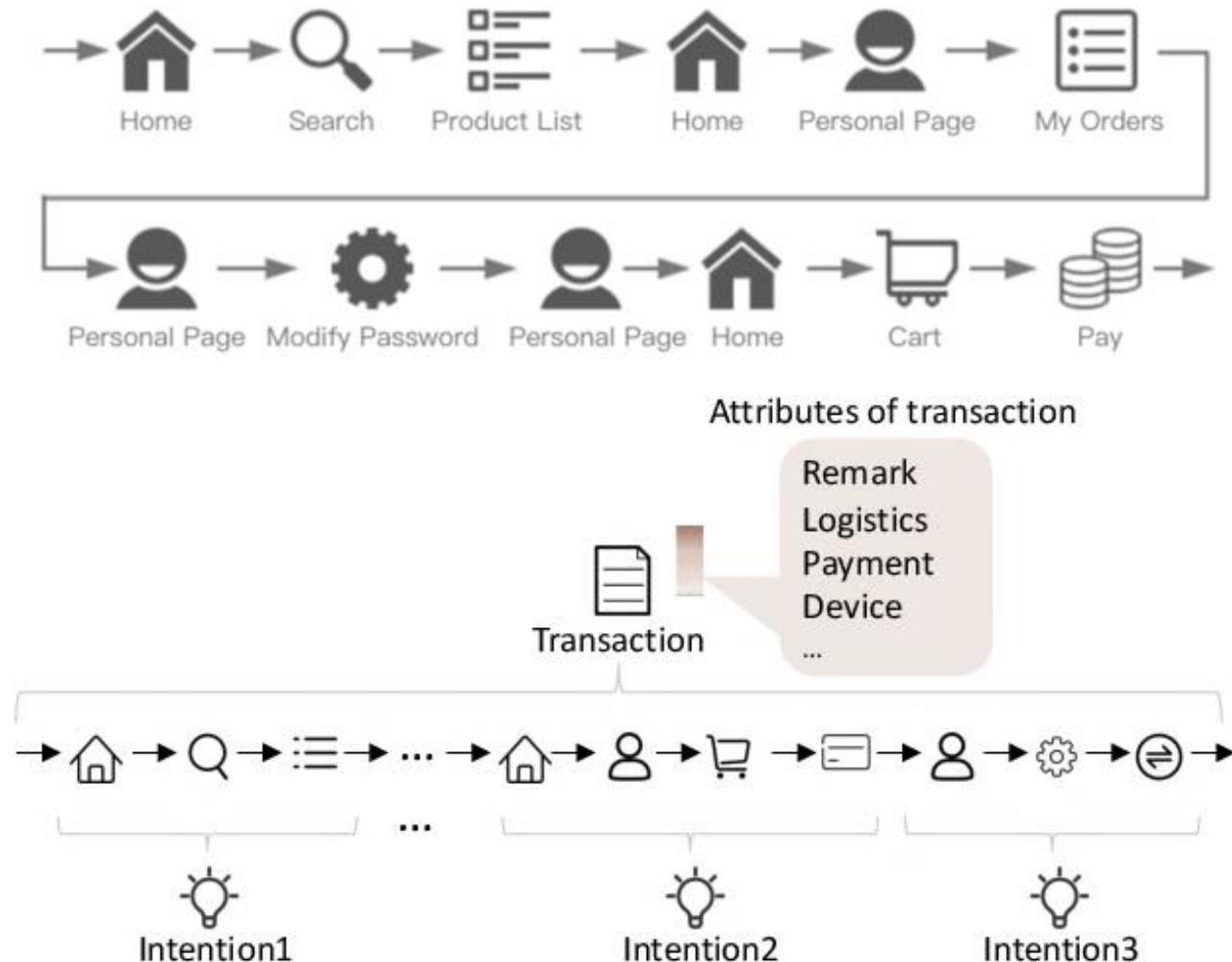
## Lack Of Interpretability

Labels	Amount	Risk
Exchange	0.3260 BTC \$13,040.00	LOW
Donation	0.3860 BTC \$15,440.00	LOW
Auction	0.9400 BTC \$37,600.00	LOW
Auction, NO KYC	0.6350 BTC \$25,400.00	MEDIUM
Gambling	0.1790 BTC \$7,160.00	MEDIUM
Darknet	0.3215 BTC \$12,900.00	HIGH



Investors need to tell real creditable projects from frauds.  
Current models can hardly offer insights for their predictions.

# Intention Monitor



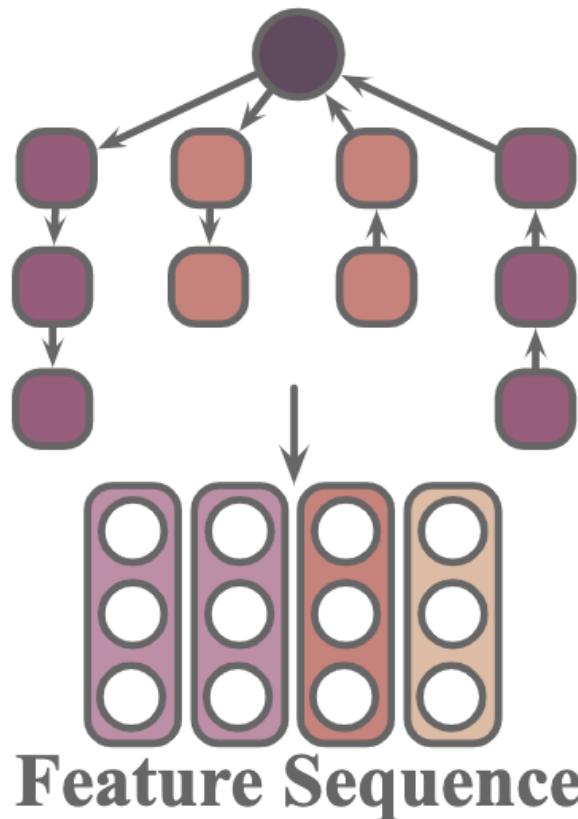
Status → Action → Intention

1. Liu, Can, et al. "Fraud transactions detection via behavior tree with local intention calibration." SIGKDD. 2020

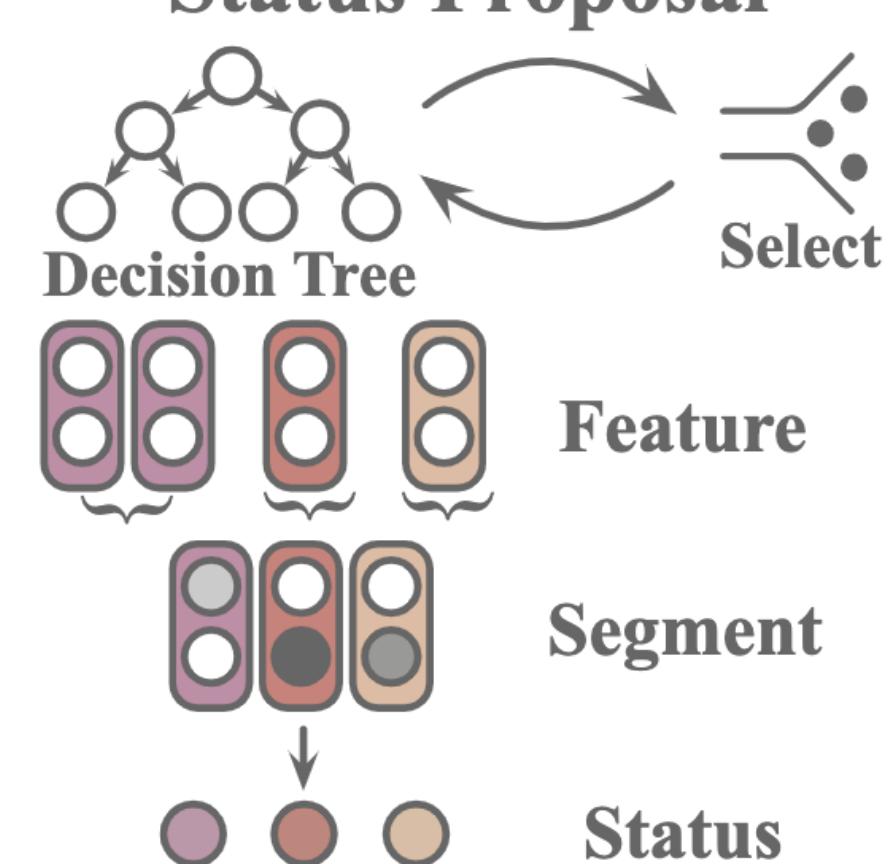
2. Liu, Can, et al. "Intention-aware heterogeneous graph attention networks for fraud transactions detection." SIGKDD. 2021

# Outline

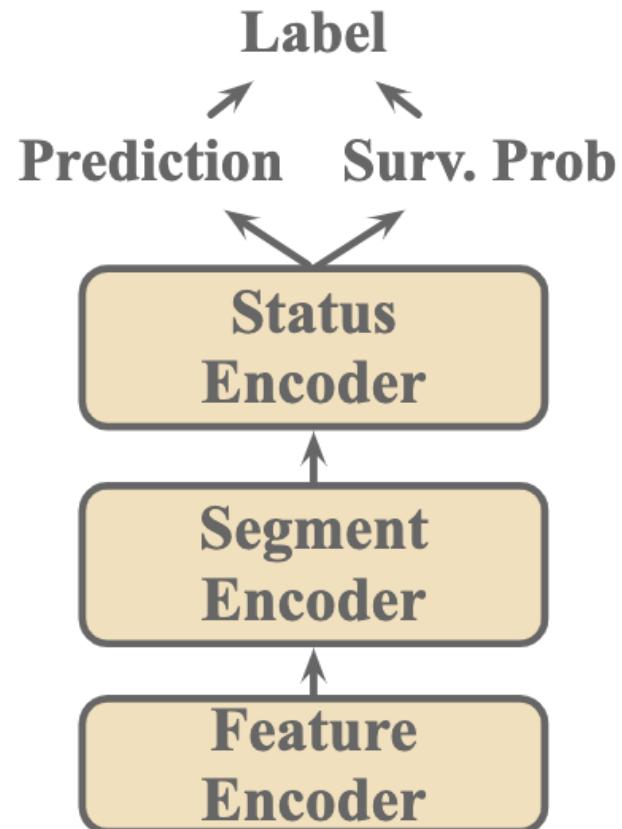
## Path & Feature Preparation



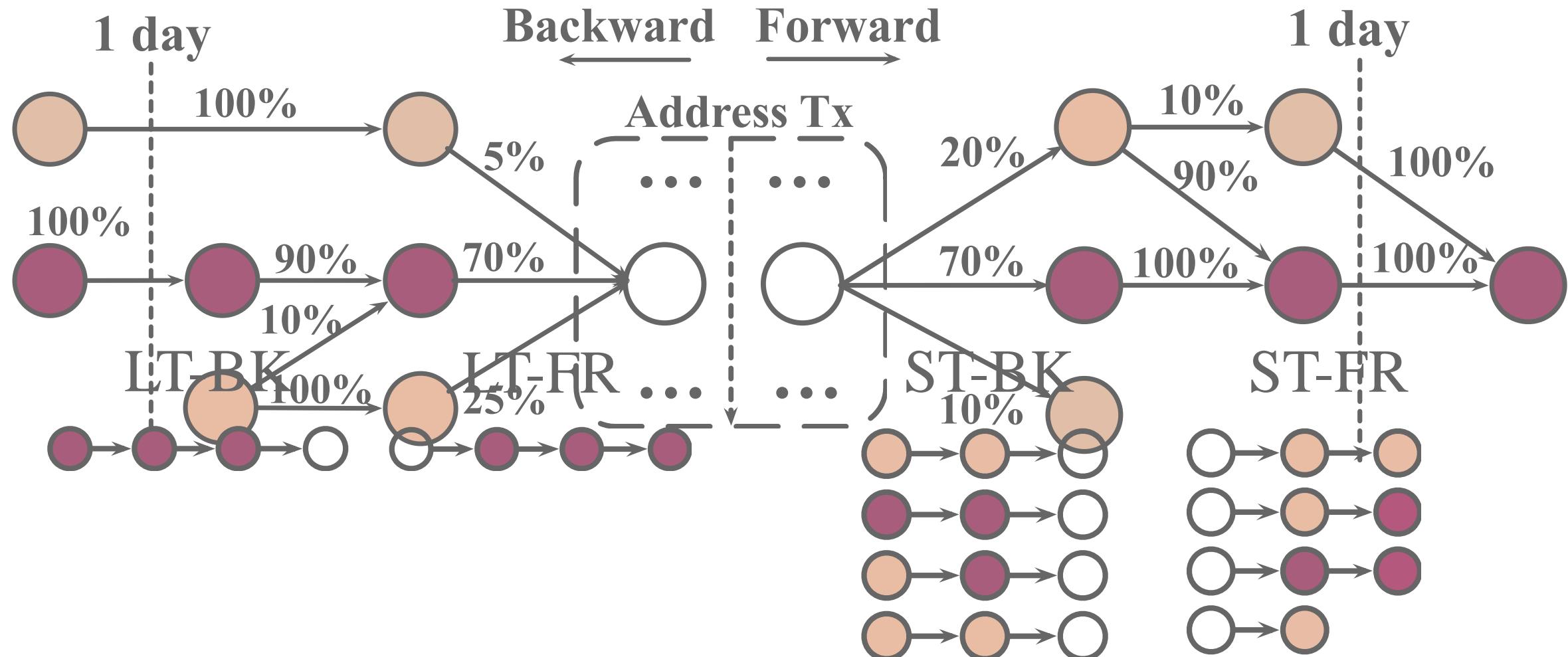
## Feature Processing Status Proposal



## Prediction with Survival Prob.

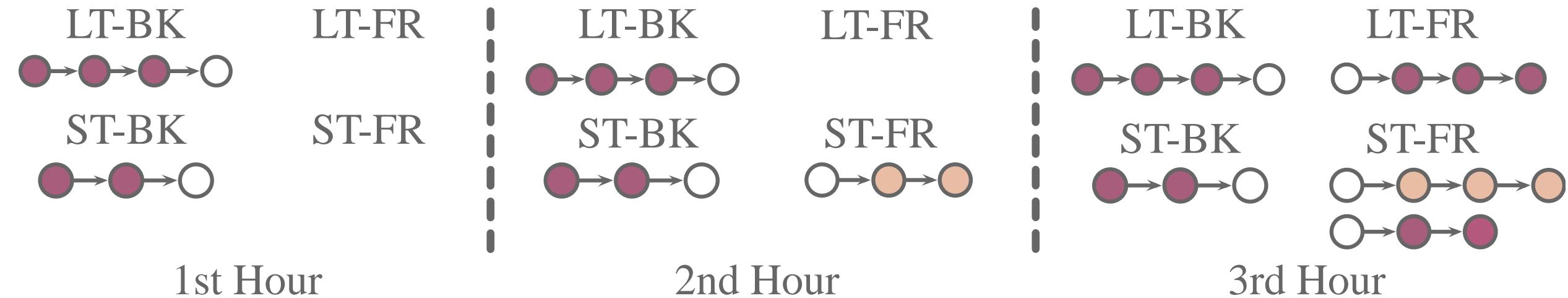


# Asset Transfer Path



# Asset Transfer Path

## Evolution of Asset Transfer Path

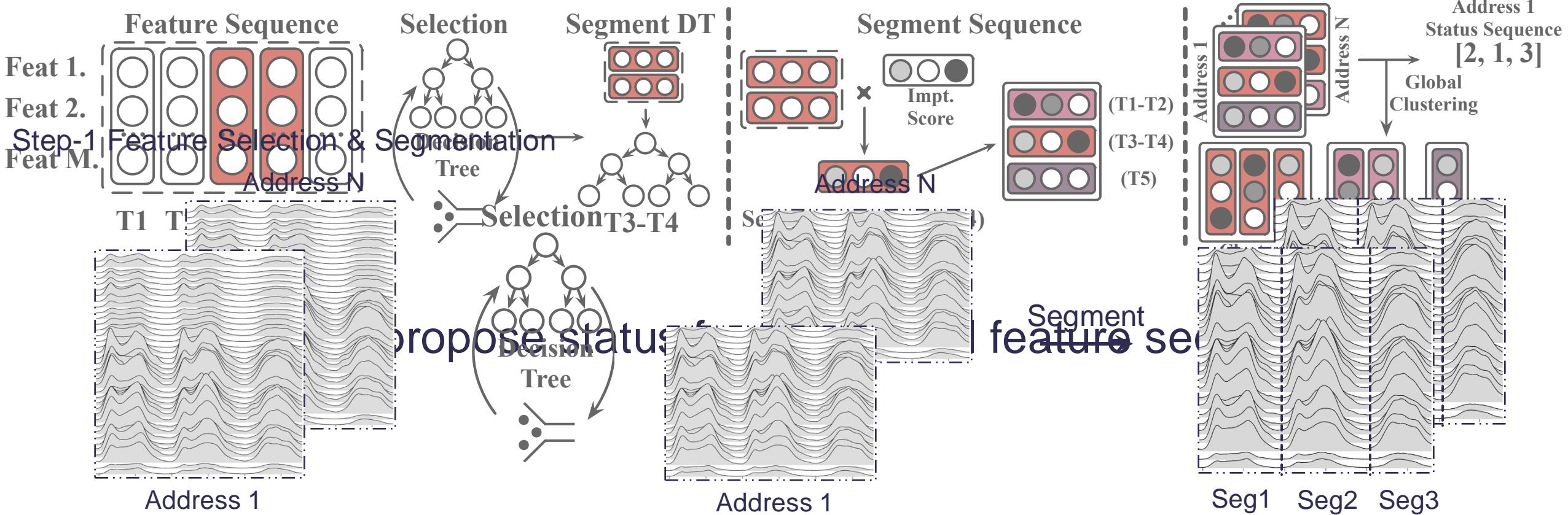


# Asset & Path Features

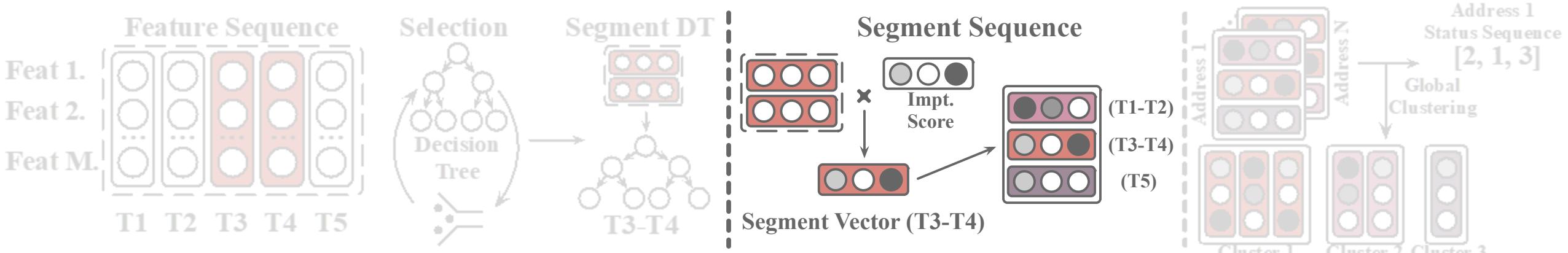
Feature Type	Aspect	Feature	Num.	Complement
Address	Balance	Balance	1	None
	Tx Count	Number of spend (receive) tx (by now/recent one hour) Ratio of spend tx to receive tx (by now/recent one hour)	4 2	None None
	Tx Frequency	Max spend (receive) tx number per hour	2	None
	Abnormal Tx	Number of spend (receive) tx with 0 amount	2	None
	Temporal Info	Time of max hourly spend (receive) tx number Time difference between max hourly spend and receive	2 1	None None
	Activity	Active hour number and active rate	2	None
	Path-Count	Path number	1	None
Path (LT/ST)-(BK/FR)	Path-Length	Hop (height)-length	2	Min,Max,Std
	Tx Amount	Max (min) input (output) amount	4	Min,Max,Std
	Tx Structure	Max (min) input (output) tx number	4	Min,Max,Std
	Connectivity	Path's max (min) activation score	2	Min,Max,Std

# Intention Monitor

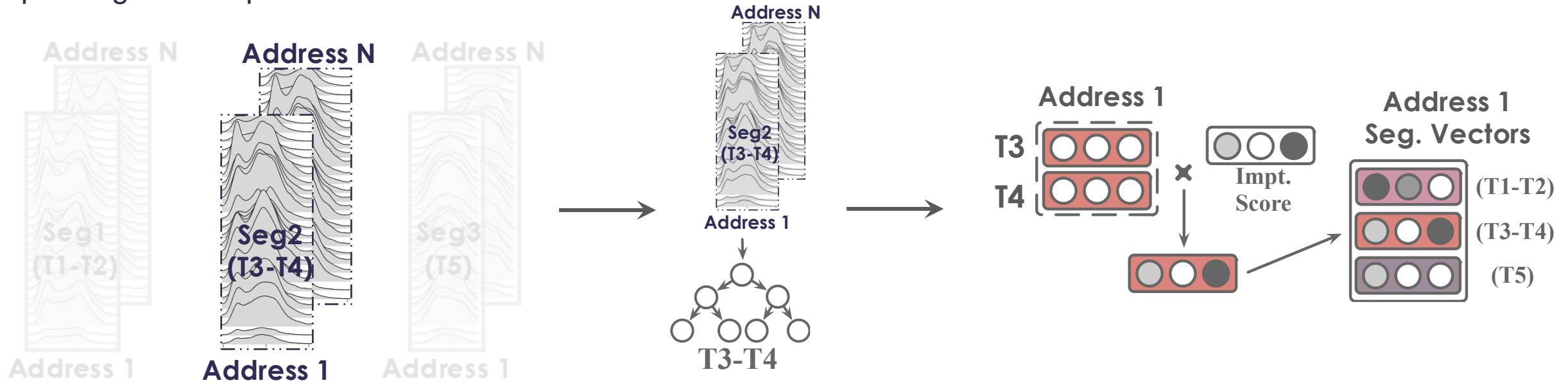
## Overview of Intention Monitor



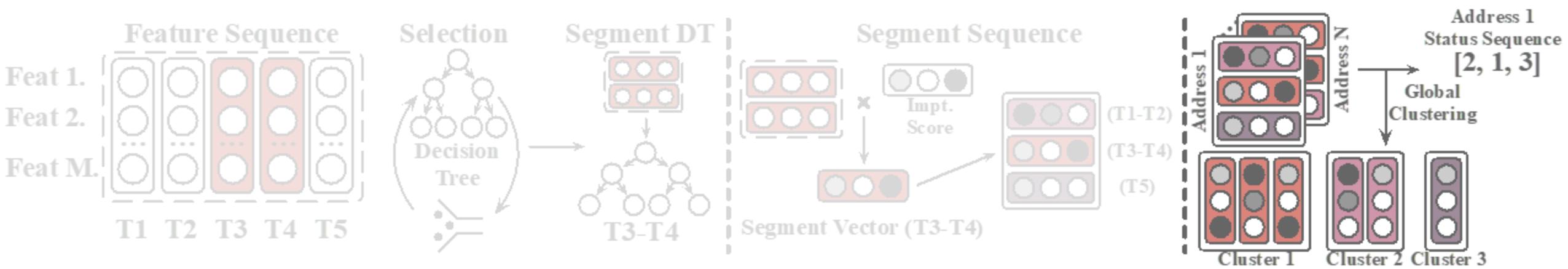
# Intention Monitor



## Step-2 Segment Representation



# Intention Monitor

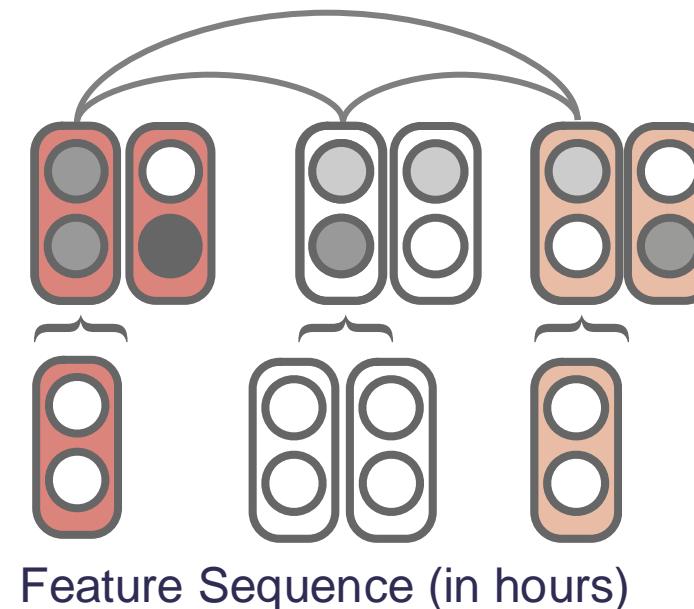
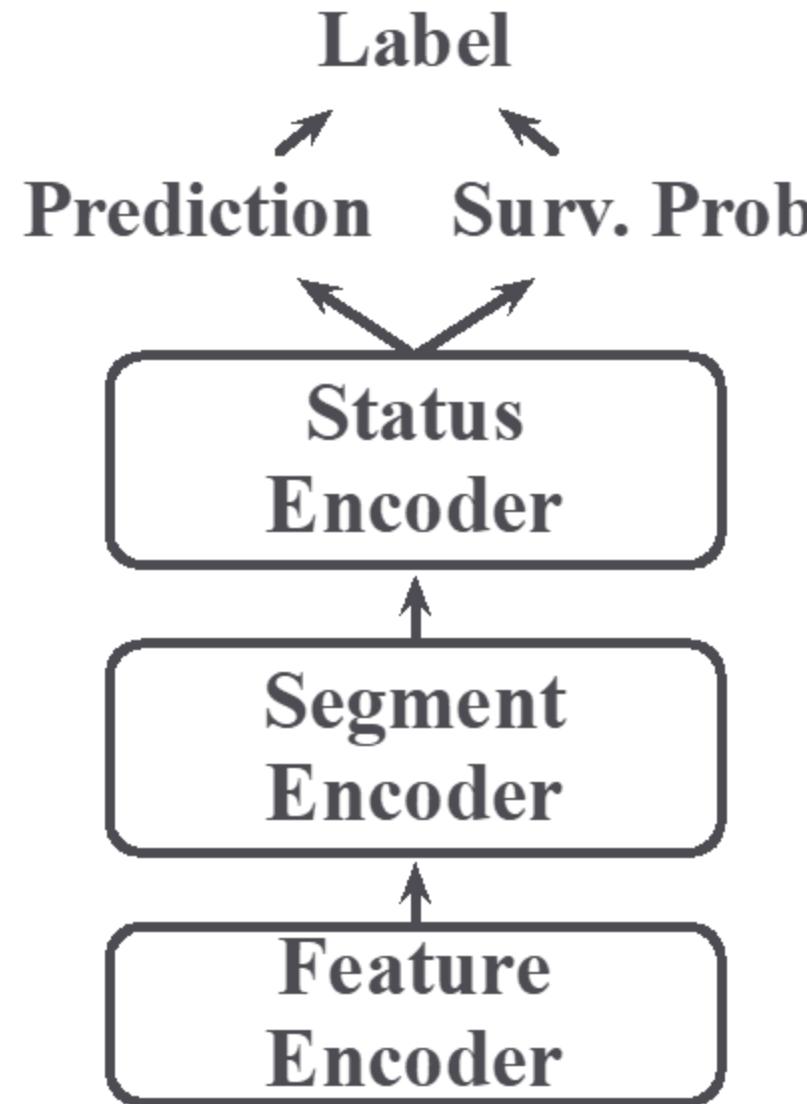


Step-3 Status Proposal



# Prediction with Survival Analysis

# Predictor



$$f^p = \sum_{i=b^p}^{e^p} \alpha_i f_i, \quad \alpha_i = \exp(a_i) / \sum_{k=b^p}^{e^p} \exp(a_k),$$

$$a_i = W^a \tanh(W^{f,u}[f_i, u^p]),$$

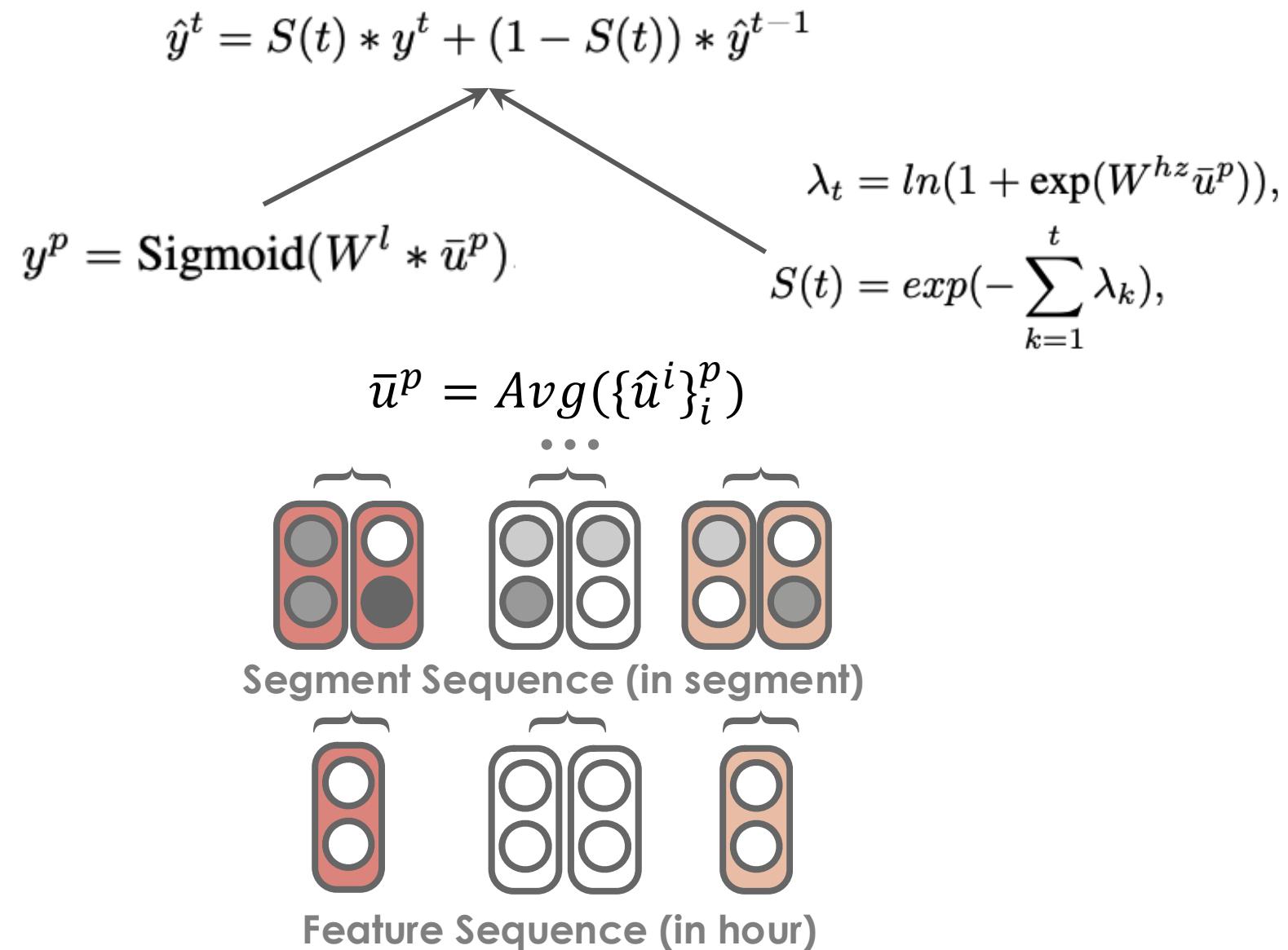
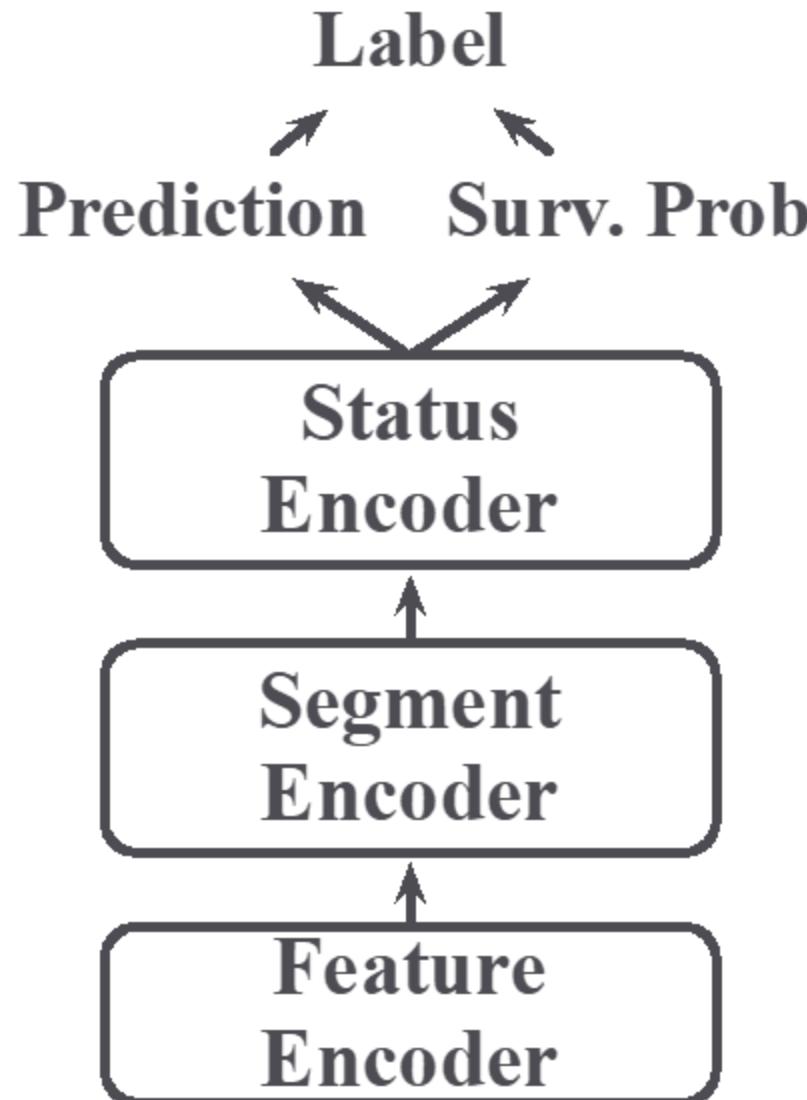
$$F^p = \{\hat{f}^i\}_{i=1}^{p^*} = \text{Concat}(H_1^p, \dots, H_h^p, \dots, H_{N_h}^p)W^O,$$

$$H_h^p = \text{Softmax}\left(\frac{(QW_h^Q)(KW_h^K)^T}{\sqrt{d}}\right)VW_h^V,$$

$$\tilde{g}^i = W^g \tanh(W^{f,g}[g^i, \hat{f}^i]),$$

$$\tilde{u}^i = W^u \tanh(W^{g,u}[u^i, \hat{g}^i]),$$

# Predictor



# Case Analysis

# Case Analysis

## Case Recap

Transaction **e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea**

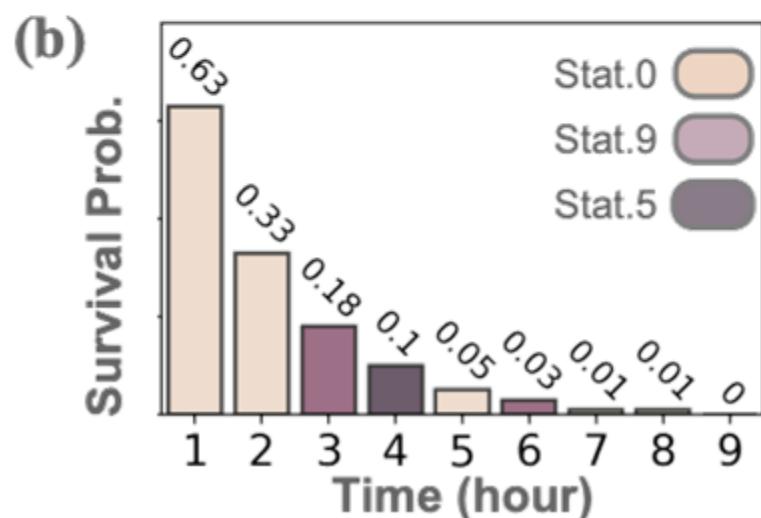
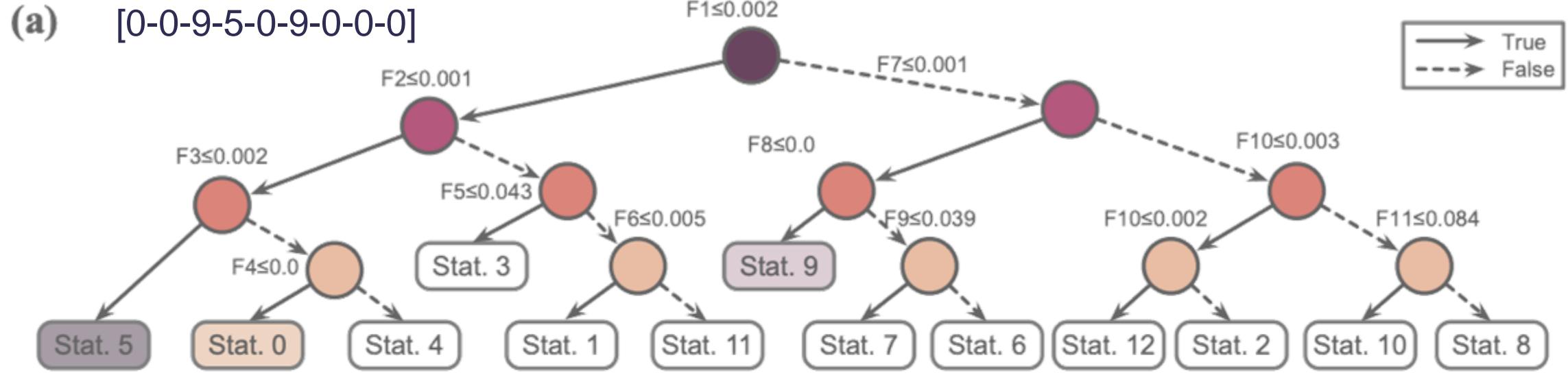
7,000  
Exchanges  
by Mark

Txid	e8b406091959700dbffcff30a60b190133721e5c39e89bb5fe23c5a554ab05ea
Included in block	575013 (as a transaction number 138)
Time	2019-05-07 17:17:18
Sender	 Binance.com
Fee	0.01188 BTC (99.15 satoshis/byte)
Size	11982 bytes

inputs: 71 (7074.19295031 BTC) unique addresses: 2, source transactions: 71		outputs: 44 (7074.18107031 BTC) unique addresses: 44, spent: 43 in 33 transactions	
0. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">e98a74df...</a>	
1. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">dc03c5e9...</a>	
2. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">b3ca84de...</a>	
3. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">35f86114...</a>	
4. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">a3b14077...</a>	
5. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">d4aff83a...</a>	
6. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">af920705...</a>	
7. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">9afce068...</a>	
8. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">bd01d62c...</a>	
9. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">e50b5154...</a>	
10. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">1374e3cd...</a>	
11. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">d91ccfc1...</a>	
12. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">d42c2d3b...</a>	
13. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">156d3abe...</a>	
14. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">246b49ac...</a>	
15. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">dc22a158...</a>	
16. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">715f4bcd...</a>	
17. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">27c8f9e0...</a>	
18. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">8eef5bc2...</a>	
19. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">49c0b2d9...</a>	
20. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">fbcaa6f2...</a>	
21. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">bf45ad7b...</a>	
22. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">234e6c60...</a>	
23. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">08056916...</a>	
24. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">032ffd2d...</a>	
25. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">faa33c7e...</a>	
.. <a href="#">1NDyJtNTjmwk5xPNhgAMu4HDHigtobu1s</a>	100. BTC	<a href="#">95200466</a>	
0. <a href="#">bc1qp6k6tux6g3gr3sxw94g9tx4l0cjtu2pt65r6xp</a>		<a href="#">[2e5ac3b67e]</a>	555.997 BTC <a href="#">6884775a...</a>
1. <a href="#">bc1qp8pwq277d30cy7fjpvhcvhgztvs7v0nudgul5</a>		<a href="#">[7f9e9af9d2]</a>	463.9975 BTC <a href="#">8b1e6213...</a>
2. <a href="#">32LZ4wWwEhTwztqAm2gPauktYZb5kQ6C5a</a>		<a href="#">[CoinPayments.net]</a>	0.0026 BTC <a href="#">ccfe4342...</a>
3. <a href="#">3BMEXuoRza9ElmRGSHGrwPmyFNuqWFpu8t</a>		<a href="#">[0888b50b7]</a>	0.0746535 BTC <a href="#">bf941a31...</a>
4. <a href="#">bc1qlld27dqu6wr1tmjdr8t55qvamvhgrwrr4ldh7qn</a>		<a href="#">[7f9e9af9d2]</a>	473.9975 BTC <a href="#">8b1e6213...</a>
5. <a href="#">3BMEXTMSkRt3wwXKytg7Nj86utJeSbwFhx</a>		<a href="#">[51a9905c41]</a>	0.17787495 BTC <a href="#">be06bb29...</a>
6. <a href="#">bc1q8m9h3atn4cqeqhu3ekswdqlxchp3g7d4v3qv3wm</a>		<a href="#">[487907e868]</a>	567.997 BTC <a href="#">90ae2064...</a>
7. <a href="#">14QZ2wB8bZQNgb978Lwptdc8Vhv5aZQM2</a>		<a href="#">[195be6cf37]</a>	0.01944165 BTC <a href="#">728f59a9...</a>
8. <a href="#">3L8JcsWNa3kuVaQjAx1hhcoBT17rcJA6b</a>		<a href="#">[00002dbb51]</a>	0.01493527 BTC <a href="#">db3e5299...</a>
9. <a href="#">bc1q7p6edvd4zvtya8uj366c23dan8pvlp503spucu</a>		<a href="#">[66b7fc2922]</a>	468.9975 BTC <a href="#">bb0b41c2...</a>
10. <a href="#">bc1q93ecep2338dy9aauyvh4g22t49rnedx18z0tj</a>		<a href="#">[589beb5a81]</a>	0.1995 BTC <a href="#">a8801564...</a>
11. <a href="#">bc1ql0wlnu80l8kctjzkzlzd72sdjqwuvruvgepceq</a>		<a href="#">[7f9e9af9d2]</a>	383.998 BTC <a href="#">8b1e6213...</a>
12. <a href="#">bc1q3ldtrr6xtpx8jam5gw6aaexz2wtlujoqullvr</a>		<a href="#">[2377c0f10b]</a>	189.999 BTC <a href="#">7e615f3e...</a>

# Case Analysis

## Sample Address Analysis



- (c)
- F1: LT-BK-Max-Input-Num (Std)
  - F2: ST-BK-Min-Input-Num (Max)
  - F3: Life-time
  - F4: Spend-Tx-Num (Full-Time)
  - F5: ST-BK-Path-Num
  - F6: ST-BK-Hop-Length (Min)
  - F7: ST-BK-Min-output-Amt (Max)
  - F8: ST-BK-Hop-Length (Max)
  - F9: ST-FR-Height-Length (Std)
  - F10: LT-FR-Min-Trust (Std)
  - F11: LT-FR-Max-Input-Amt (Std)

# Case Analysis

## Sample Address Analysis

[0-0-9-5-0-9-0-0-0]

### The Hack

Binance has been fairly forthcoming about the hack, detailing its impact in [a blog post](#) from Binance CEO Zhao Changpeng. “The hackers used a variety of techniques, including phishing, viruses and other attacks,” wrote Zhao. “**The hackers had the patience to wait, and execute well-orchestrated actions through multiple seemingly independent accounts at the most opportune time.** The transaction is structured in a way that passed our existing security checks.”

The hacker received 568 BTCs through 71 input TXs with no output.



At the 13th hour, it received 0.00008642 BTC.



At the 21st hour, it transferred out all its BTC.

### Status 0

- Asset comes from a single source.
- No spend transaction.

### Status 9

- The asset was obtained from a single source through a bunch of transitions.
- Each transition “peels” a certain amount off before passing it onto the receiver.

### Status 5

- Still no spending transactions after the initial asset received from a single source at the early beginning.

# Case Analysis



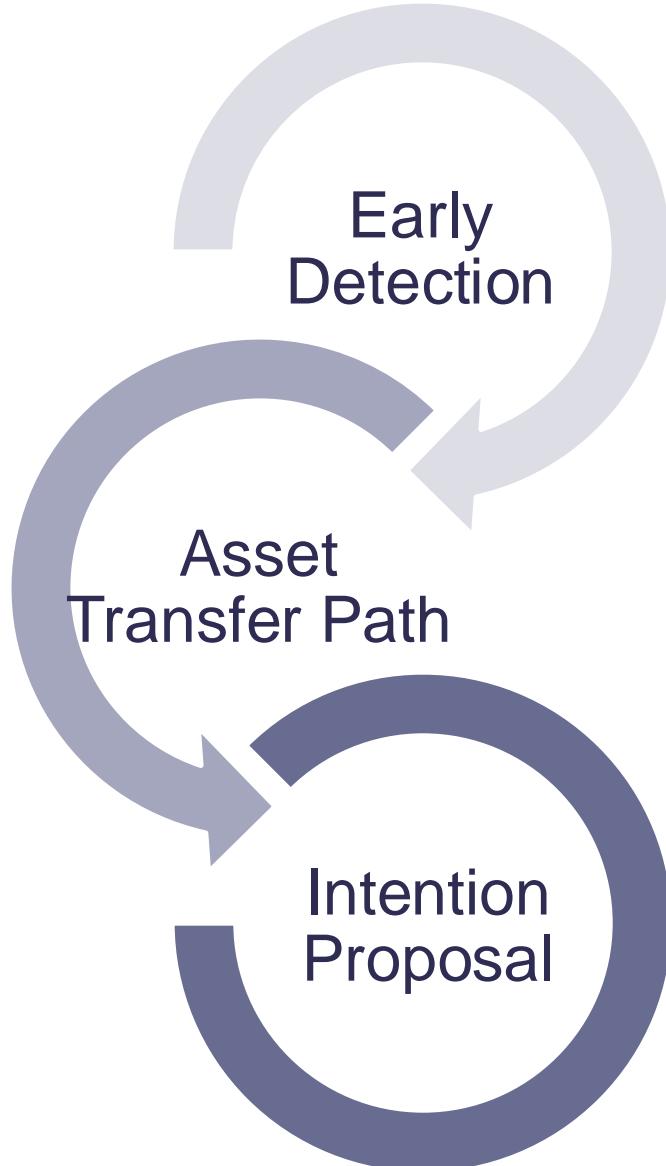
Based on the five transaction characteristics you provided, it is difficult to determine whether an address is classified as a "malicious" address without additional context or information.

However, some possible reasons why an address with these characteristics could be considered malicious include:

1. The single source of the asset may be associated with illicit activity, such as theft or fraud.
2. The lack of spending transactions could indicate that the asset is being hoarded for future illicit purposes, such as money laundering or financing illegal activities.
3. The "peeling" of a certain amount off each transition could be a way to obfuscate the source of the funds and avoid detection by authorities.
4. The fact that the asset was obtained from a single source through a series of transitions may be an attempt to distance the funds from their original illicit source.

It's important to note that without more information or context, it's impossible to definitively classify an address as "malicious." However, the transaction characteristics you provided do raise some red flags and may warrant further investigation.

# Conclusion



- Illicit early detection is necessary in BTC system.
- Asset flow gives more information at an early stage.
- Intention motifs can profile suspicious patterns.

# Outline

- Introduction to Blockchain
- **Hands-on case 1:** Rat Trading Detection Example
- Traditional Methods on Crypto Crime Detection
- **Hands-on case 2:** NFT Wash Trading Detection Example
- Transfer Path-based Methods
- **Hands-on case 3:** Scam Detection Using Asset Transfer Path