SMU
SINGAPORE MANAGEMENT UNIVERSITY

School of
Computing and
Information Systems

Toward Intention Discovery for Early Malice Detection in Cryptocurrency

Ling Cheng[1], Feida Zhu[1,*], Yong Wang[1], Ruicheng Liang[2], Huiwen Liu[1]

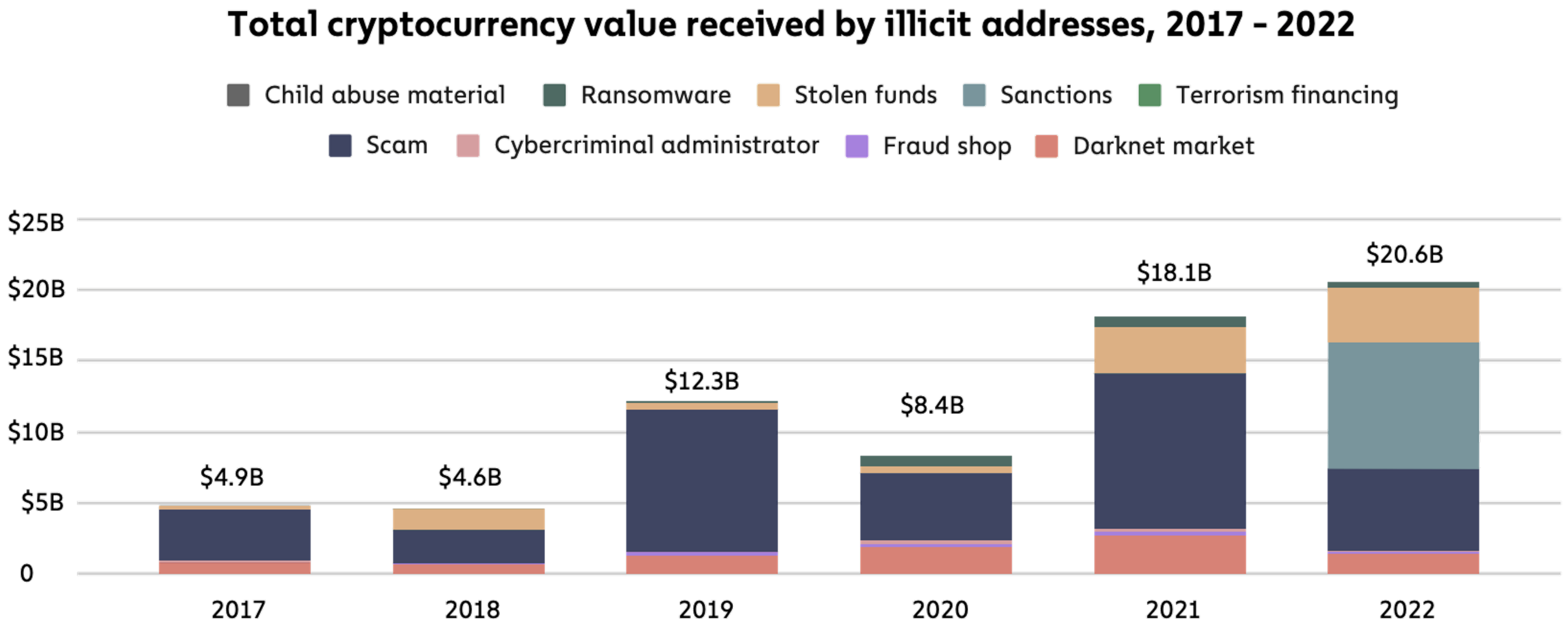
[1]School of Computing and Information Systems, Singapore Management University

[2]School of Management, Hefei University of Technology

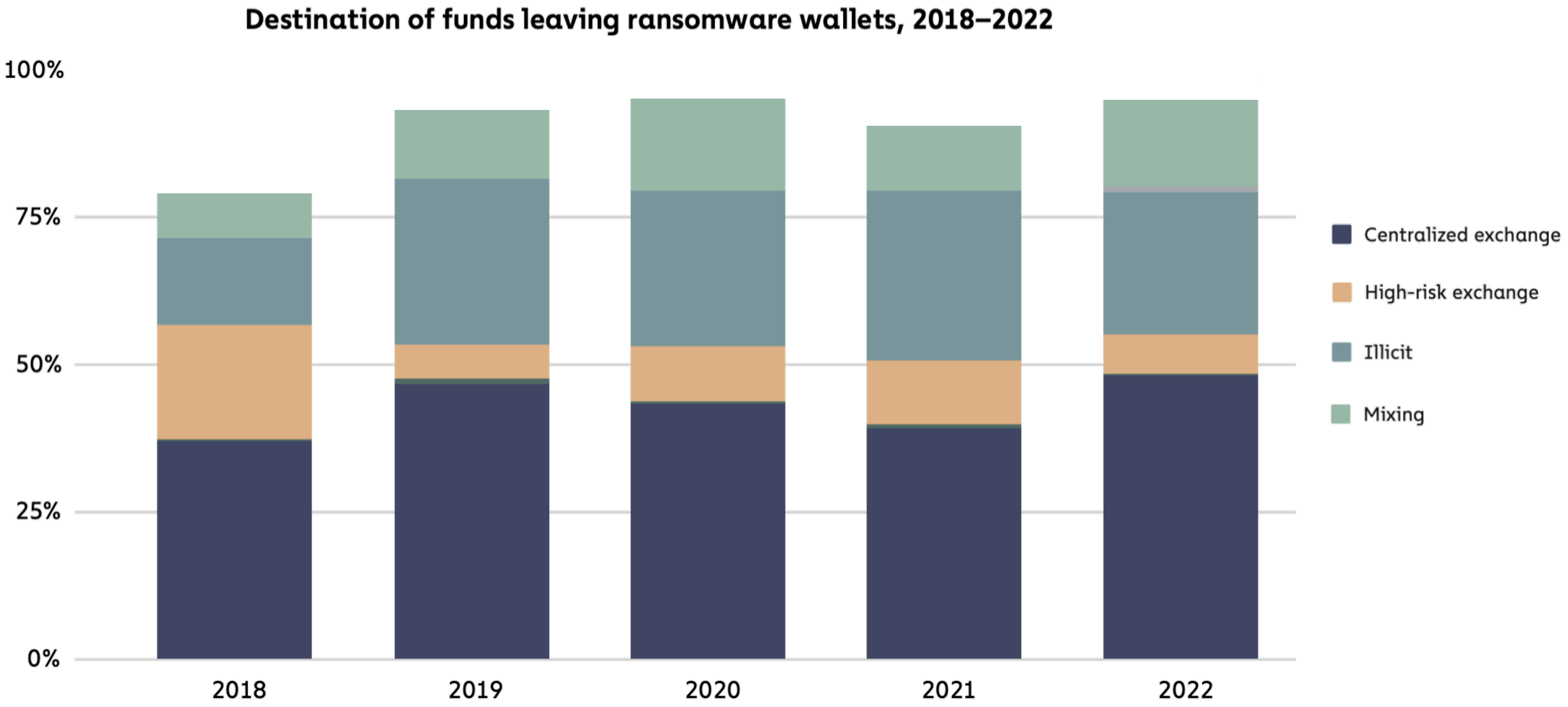
The 2023 IEEE Conference on Systems, Man, and Cybernetics (SMC 2023)
Honolulu, Oahu, Hawaii, USA
October 1-4, 2023

Crypto-Crime Volume is Tremendous

School of
Computing and
Information Systems

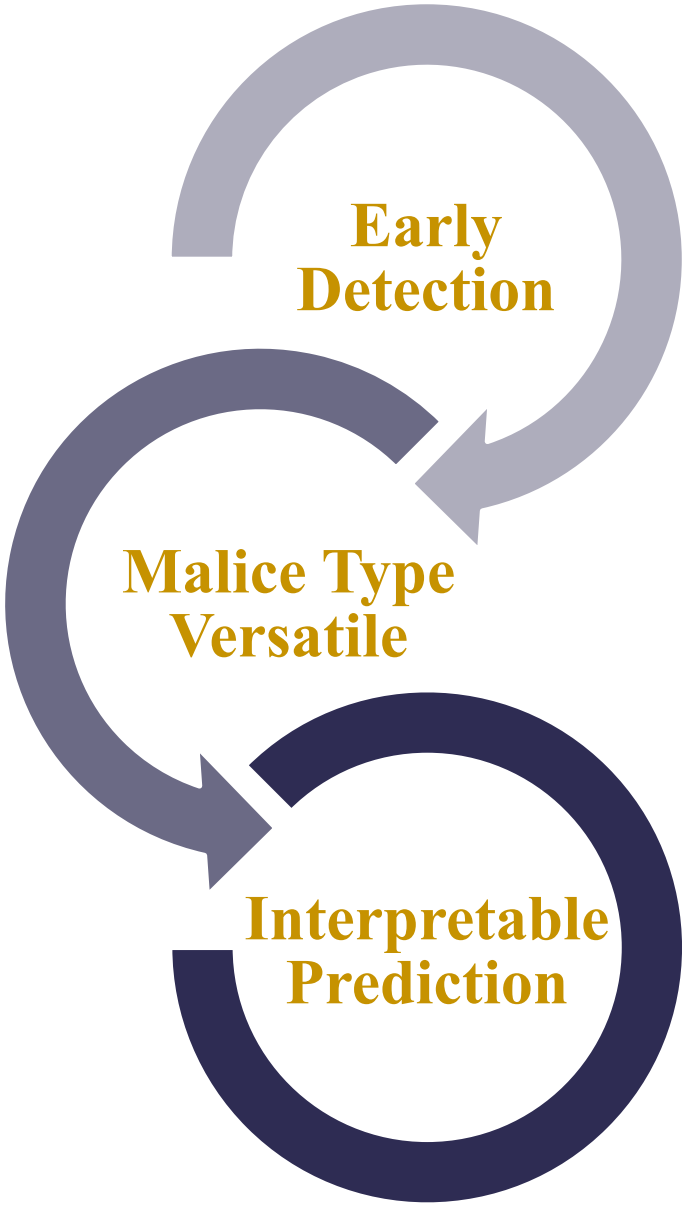


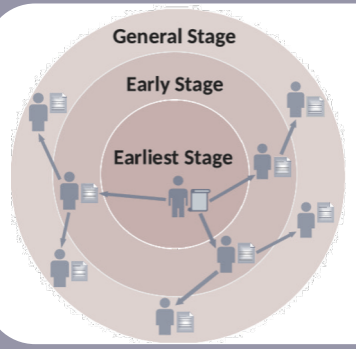
Destination of Illicit Asset



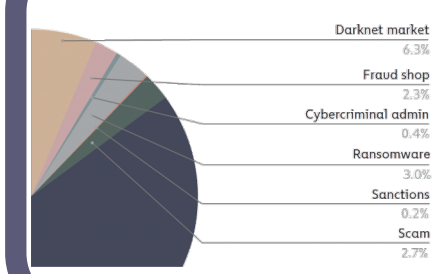
Ideal Model

School of
Computing and
Information Systems

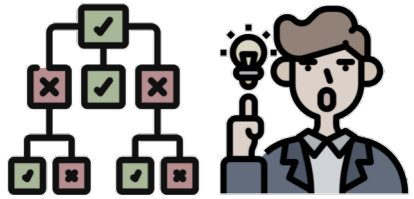




Most malice last for a short duration and cause damage if not be detected in the early stage.



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



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

Current Challenges

Current Challenges

School of Computing and Information Systems

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

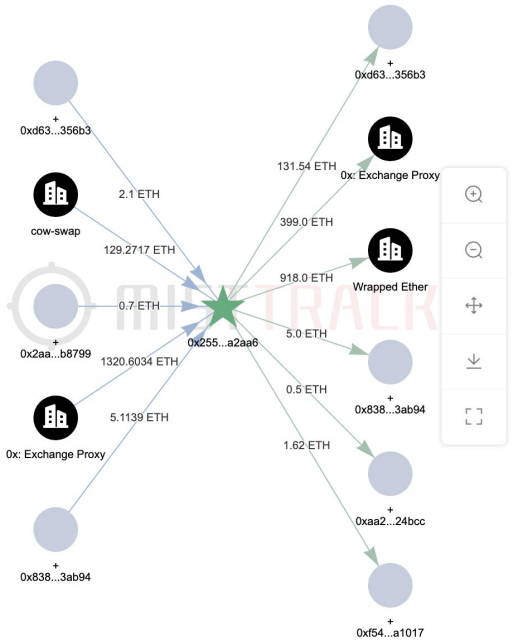
Jan 22, 2021

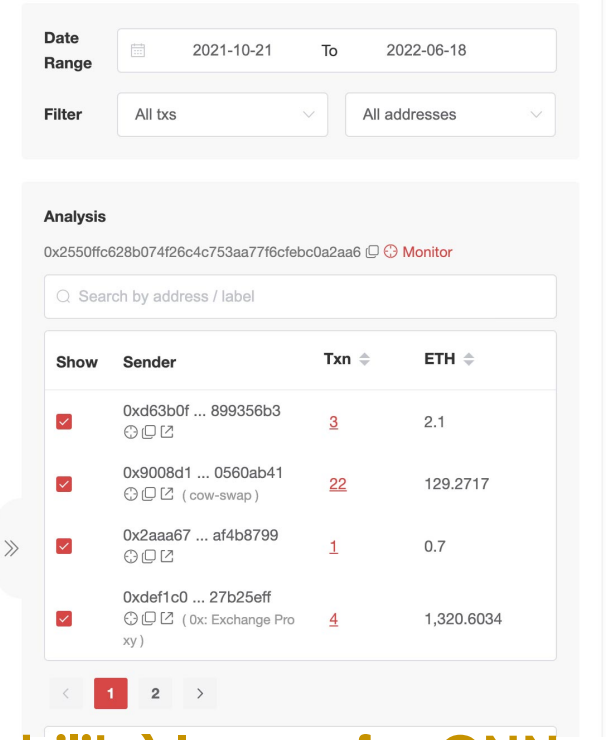
TOKYO -- Police in Japan have identified roughly 30 people for alleged involvement in illegal transactions stemming from 58 billion yen ($530 million at the time) worth of NEM cryptocurrency hacked from the Coincheck exchange three years ago, Nikkei has learned.

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

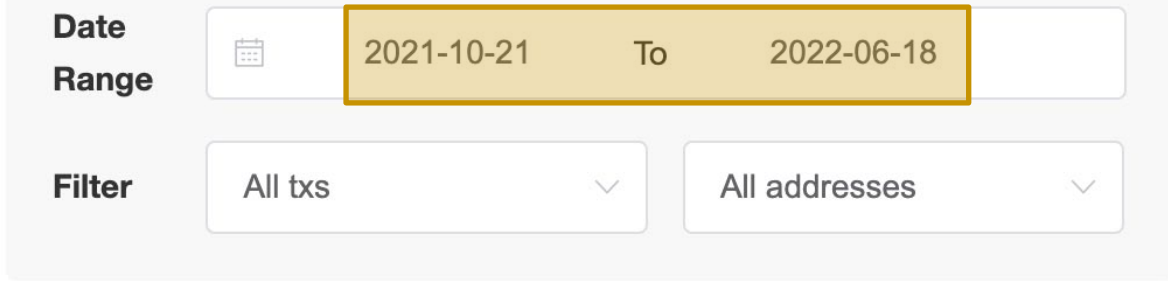
Jan 27, 2018

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



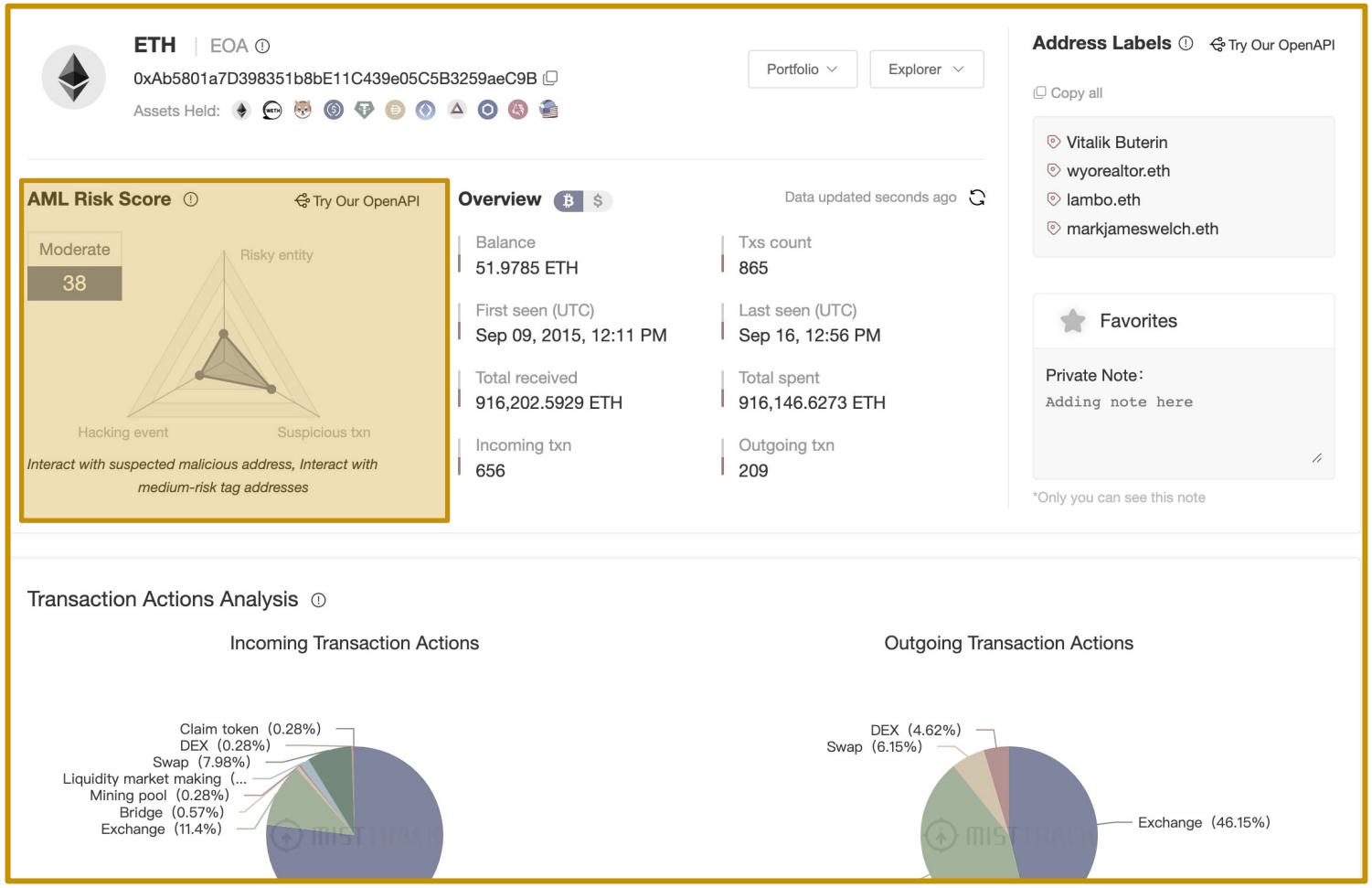


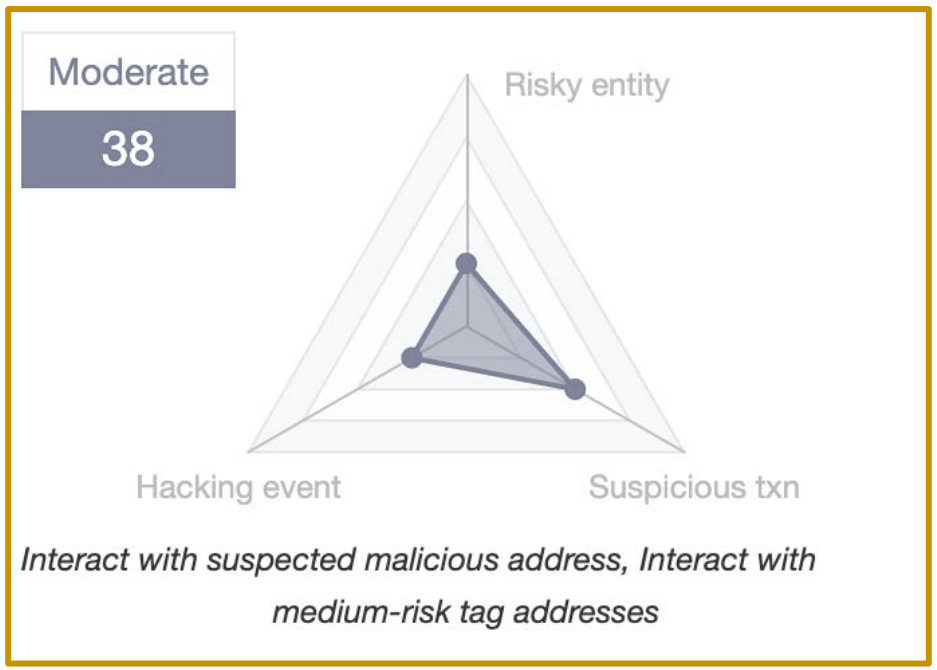
(Limited Info / Scalability) Issues for GNN



Current Challenges

Lack of Versatility



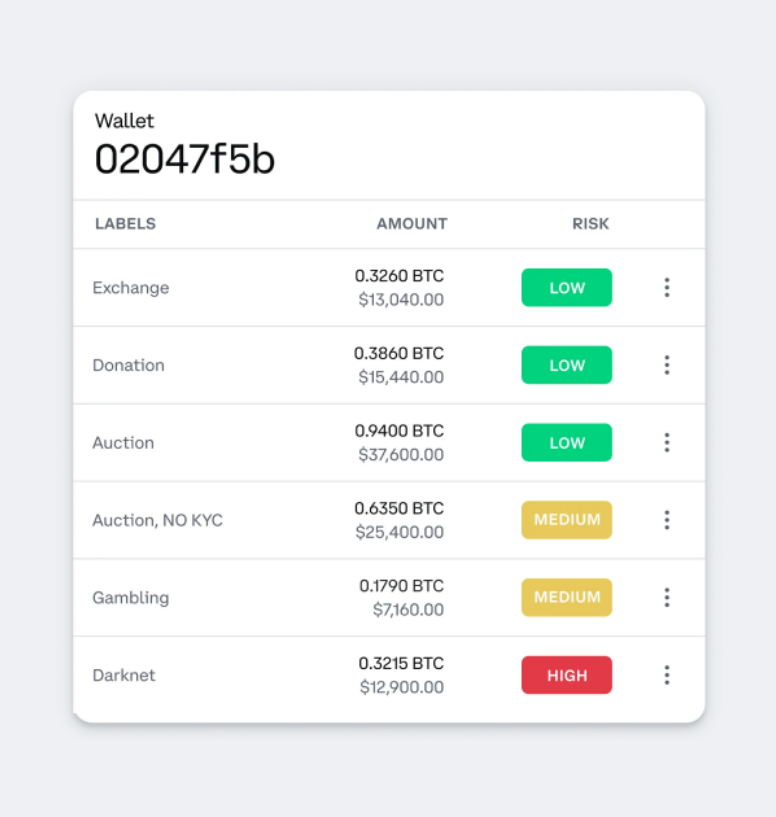


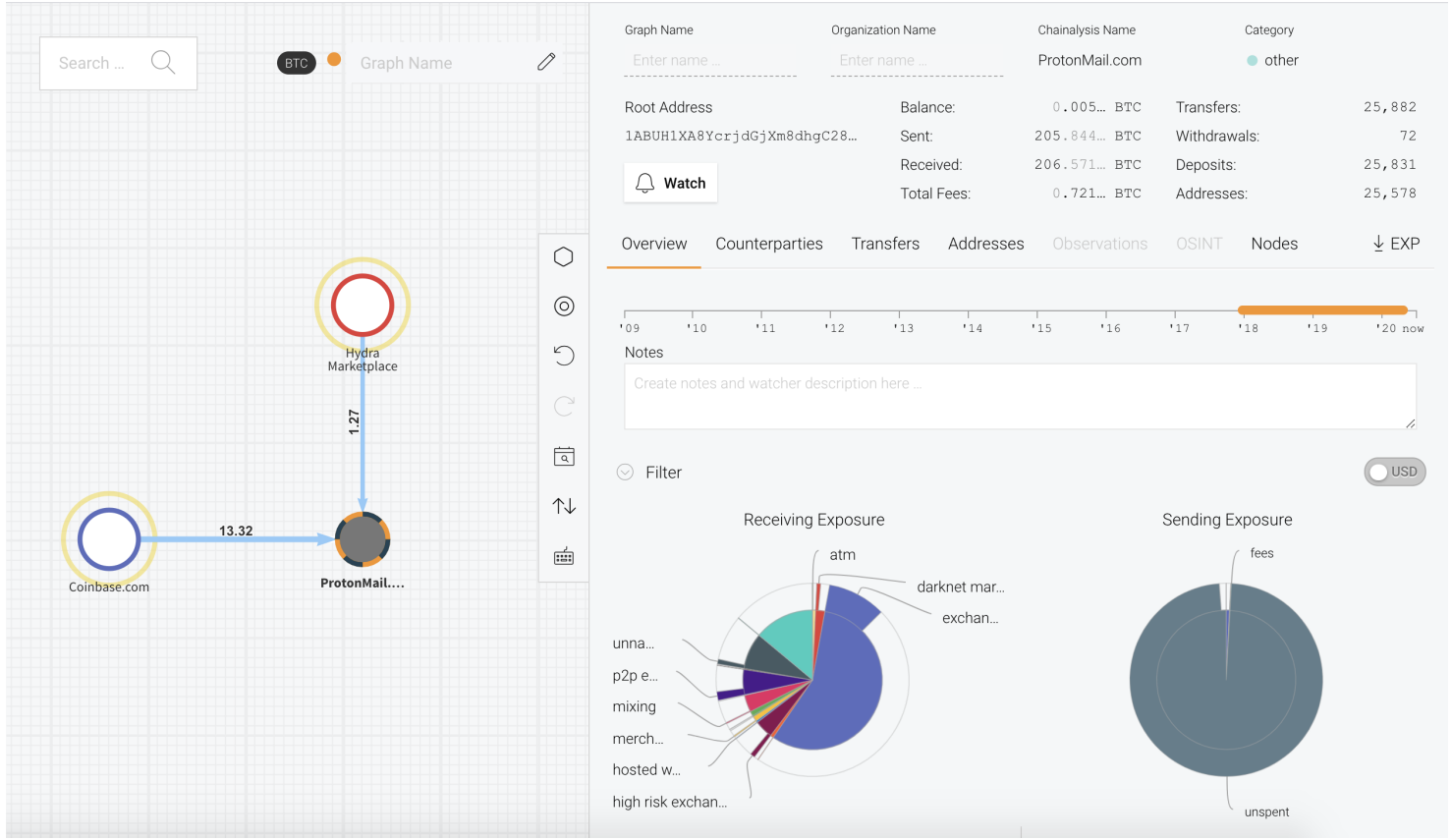
Most are based on interaction analysis with specific entities

Current Challenges

School of Computing and Information Systems

Lack of Interpretability

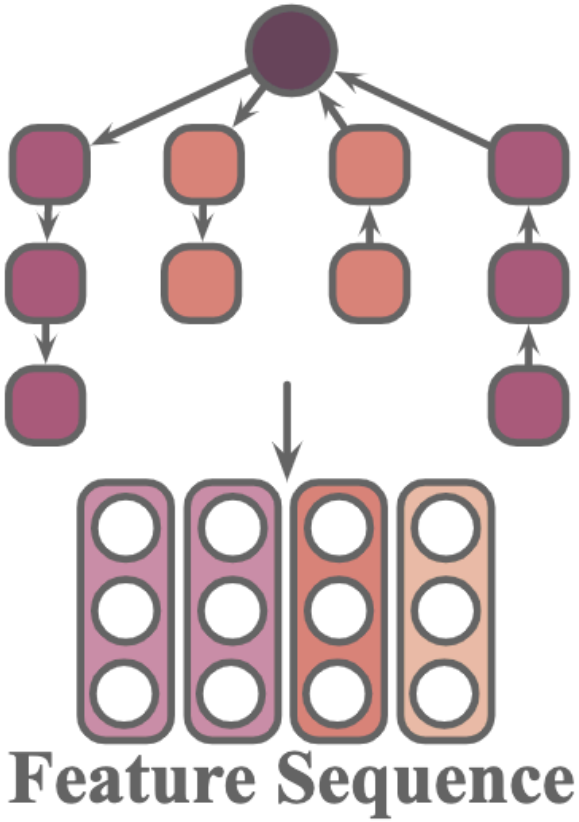




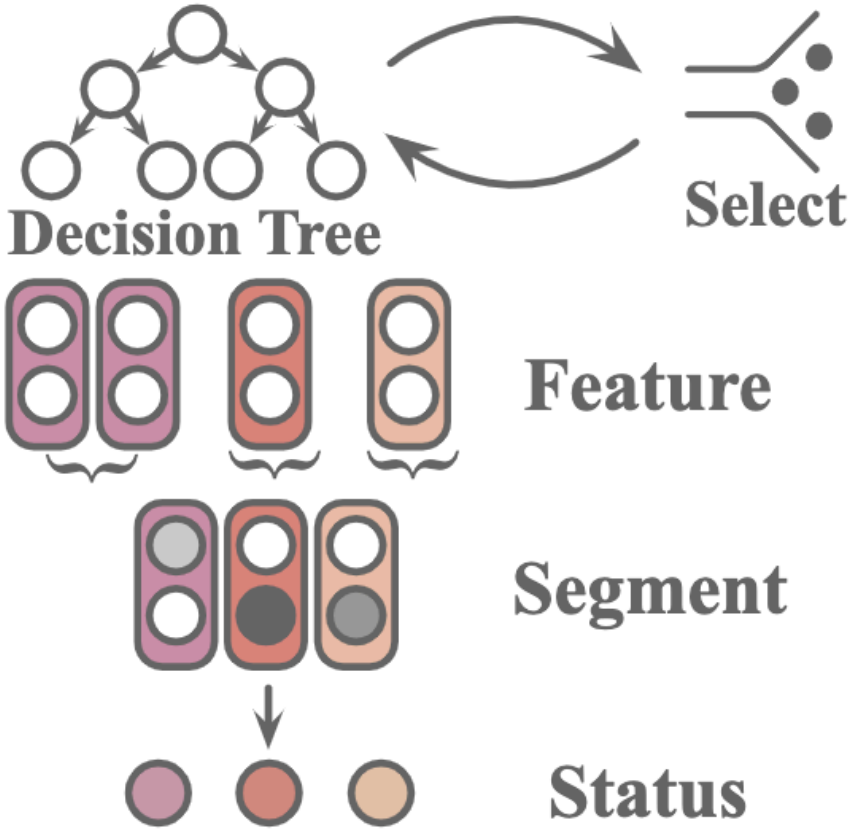
Investors need to tell real creditable projects from frauds.
Current models can hardly offer insights for their predictions.

Outline

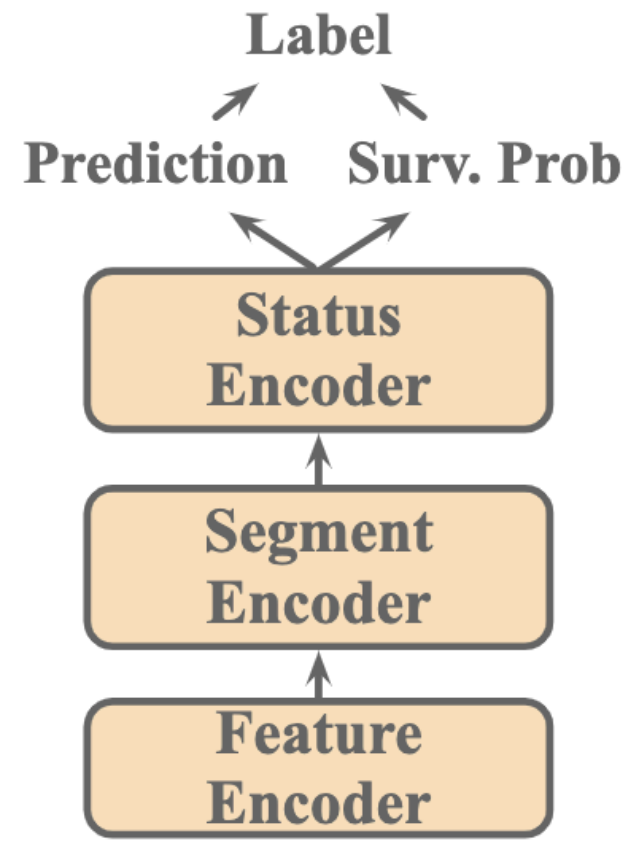
Path & Feature Preparation



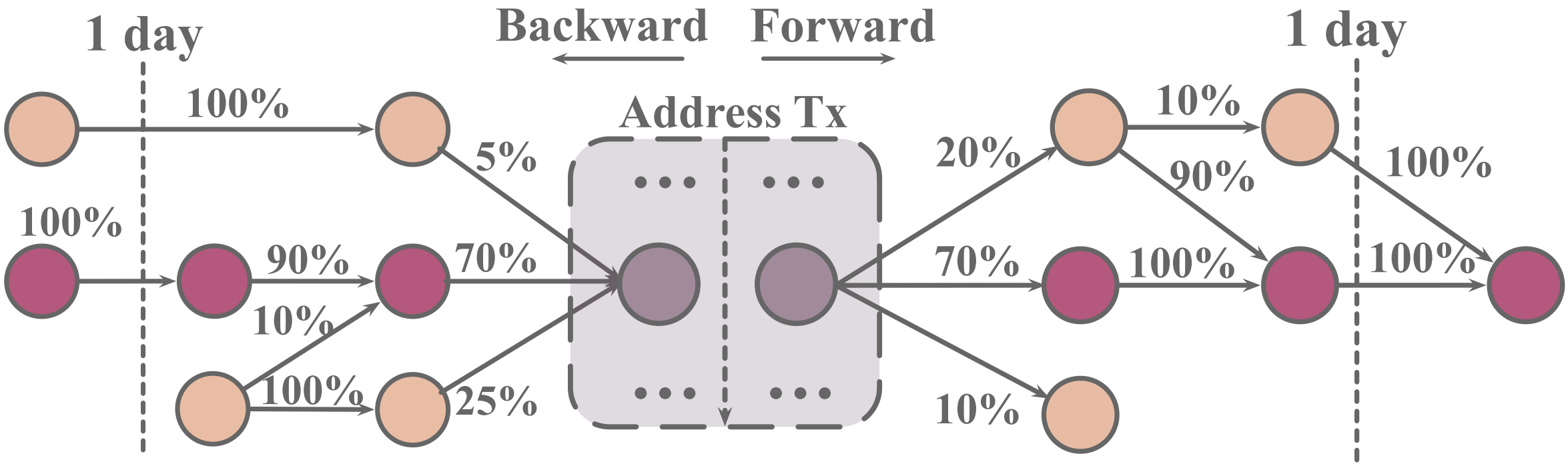
Feature Processing Status Proposal



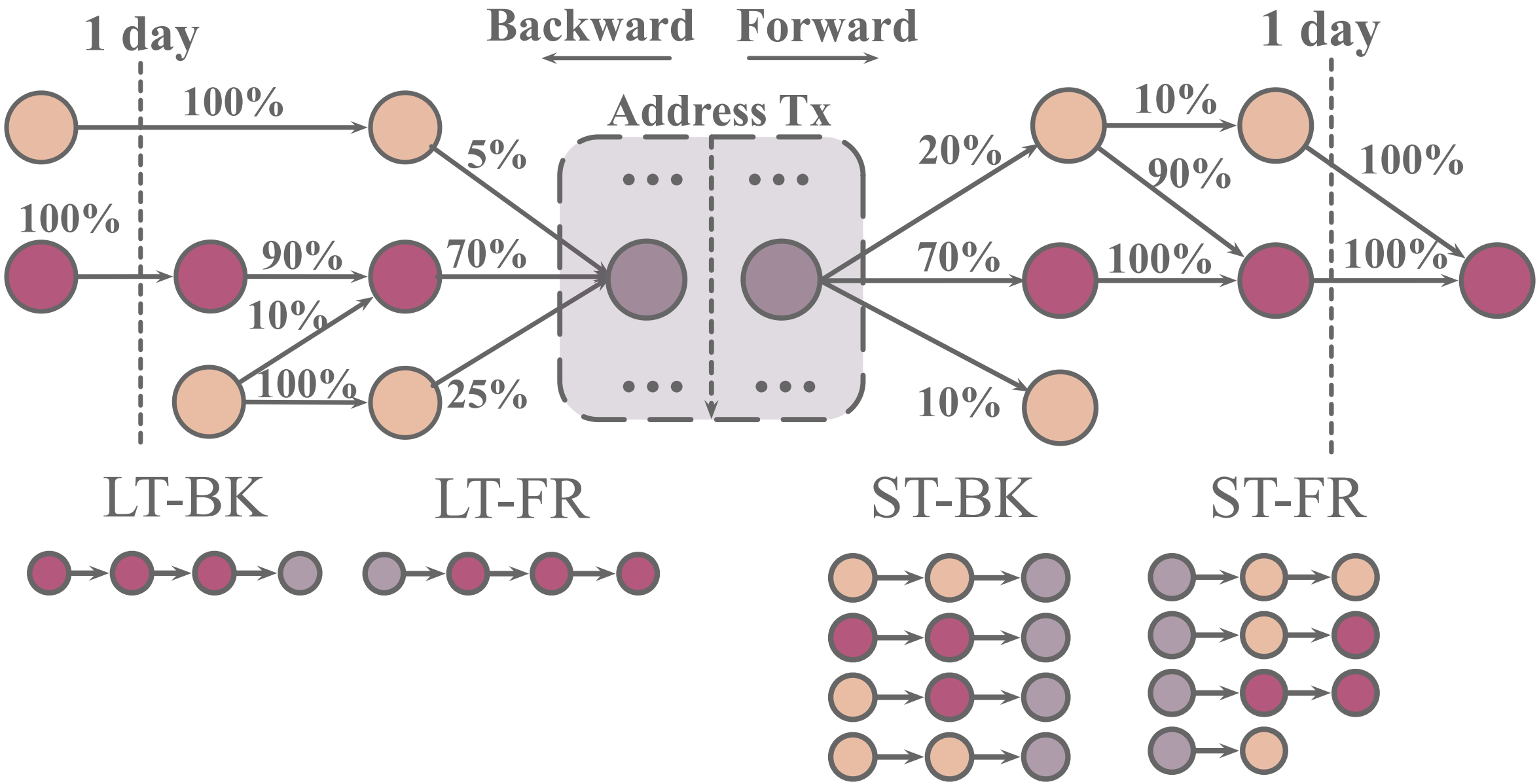
Prediction with Survival Prob.



Asset Transfer Path



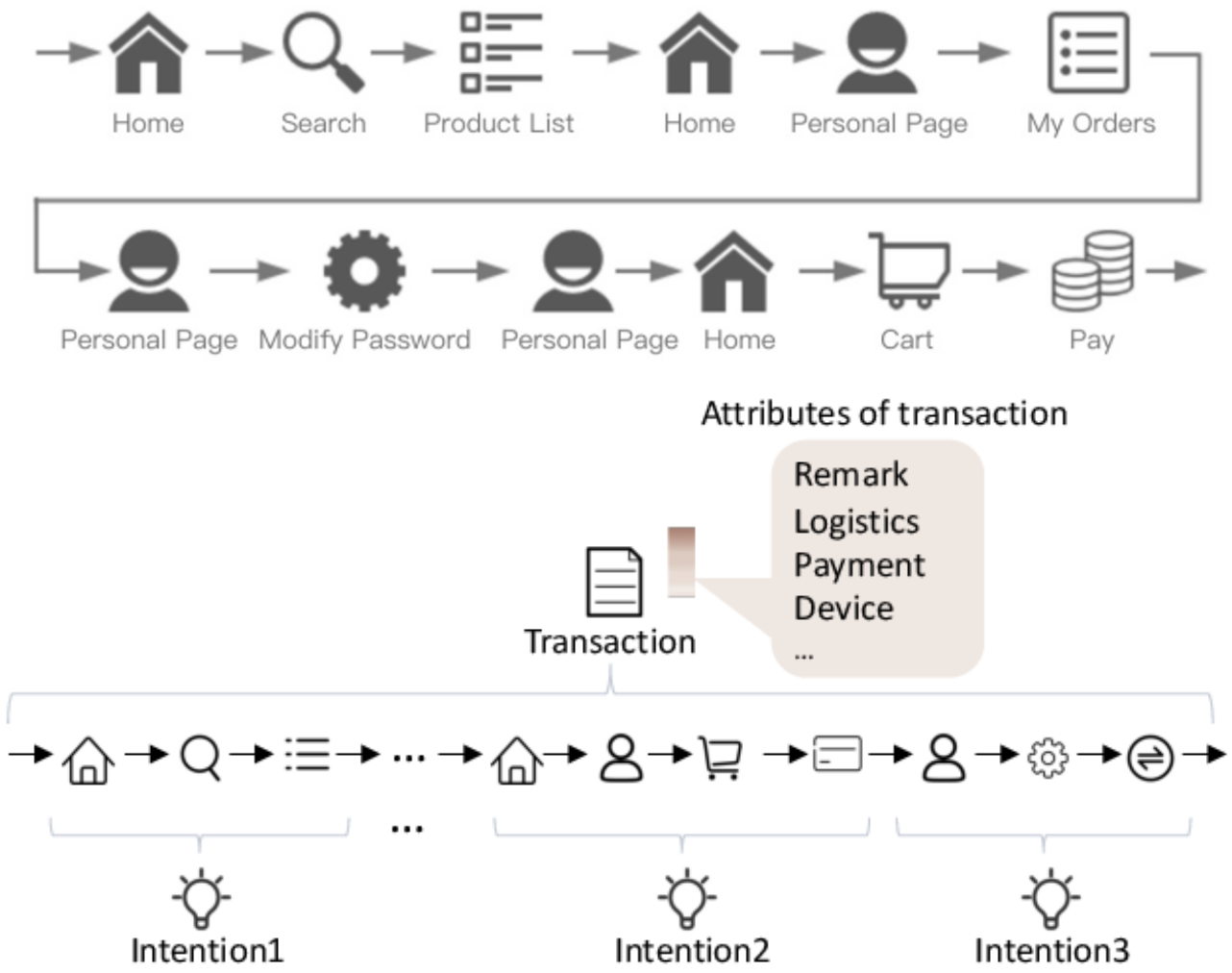
Asset Transfer Path

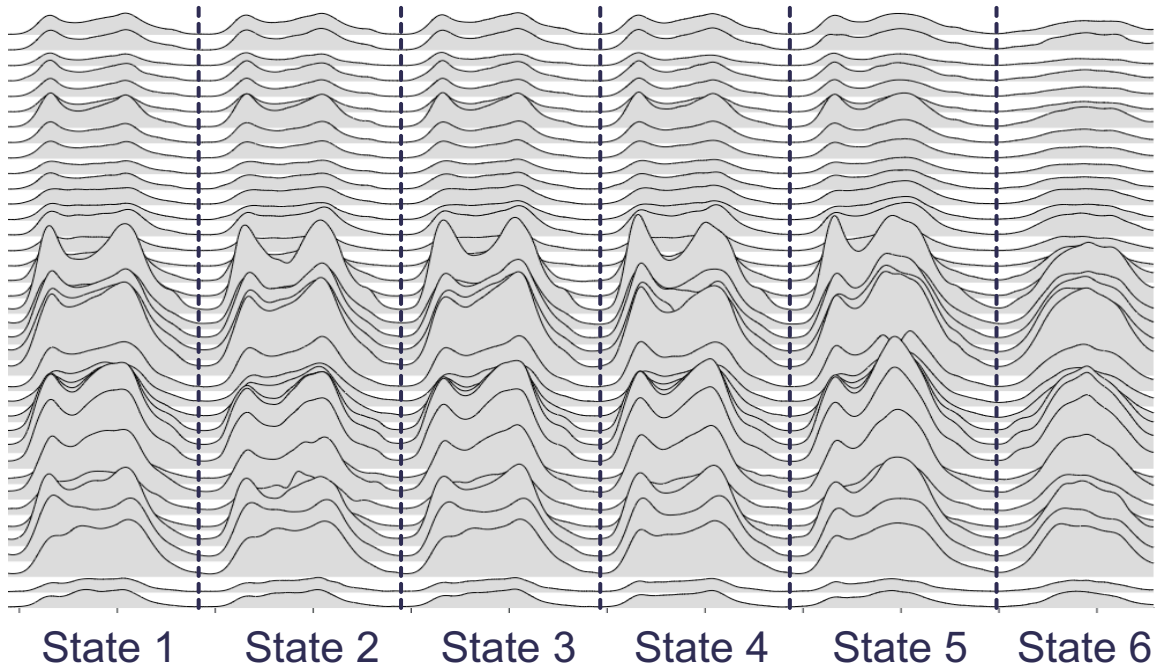


Intention Monitor

Intention Monitor

School of
Computing and
Information Systems





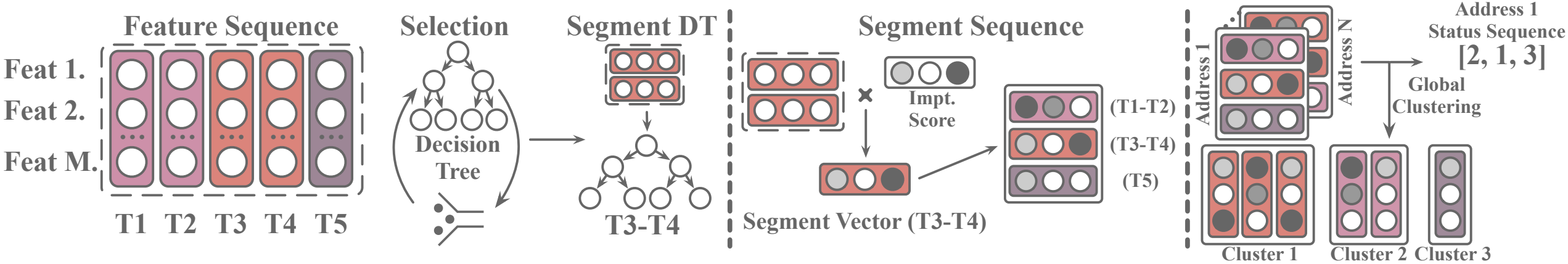
Status → Action → Intention

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

School of
Computing and
Information Systems

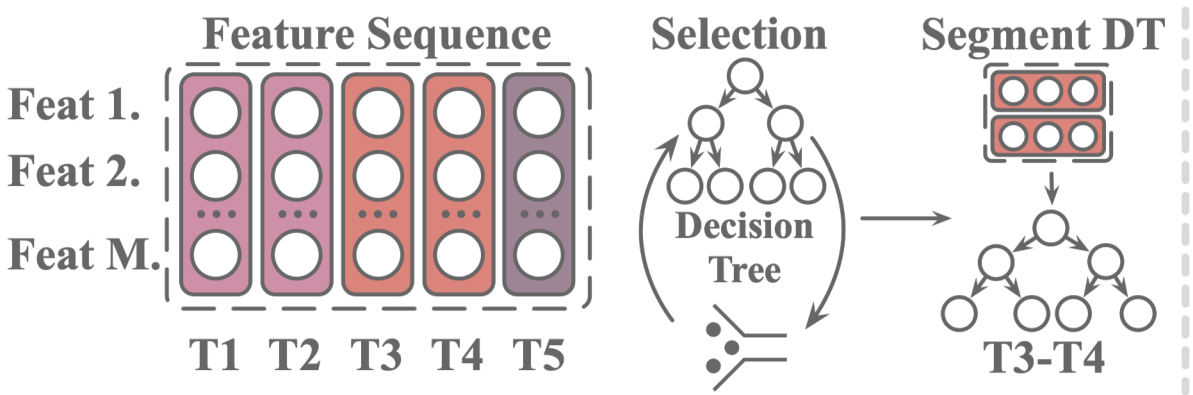
Overview of Intention Monitor



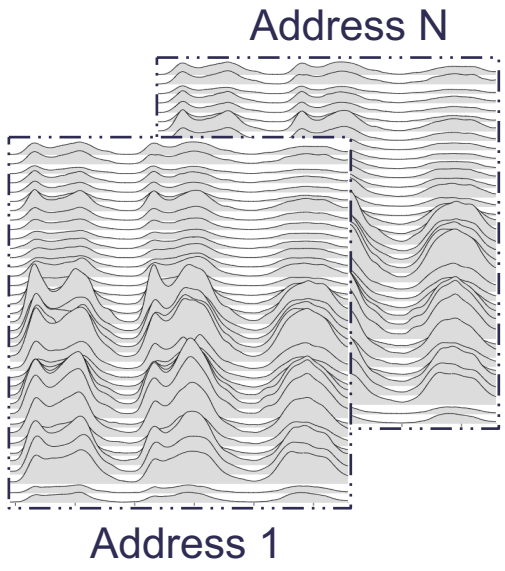
How to propose status from temporal feature sequences?

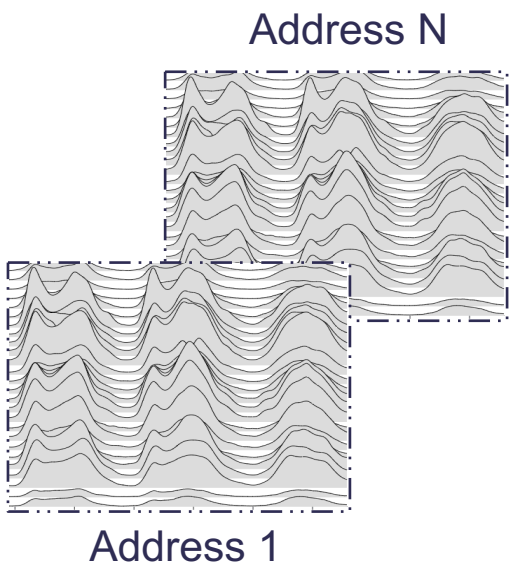
Intention Monitor

School of
Computing and
Information Systems

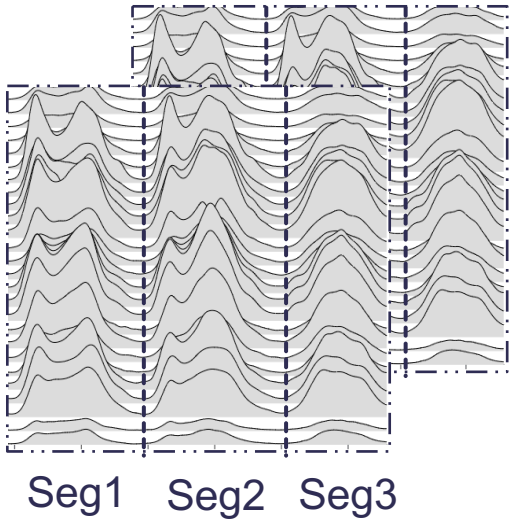


Step-1 Feature Selection & Segmentation



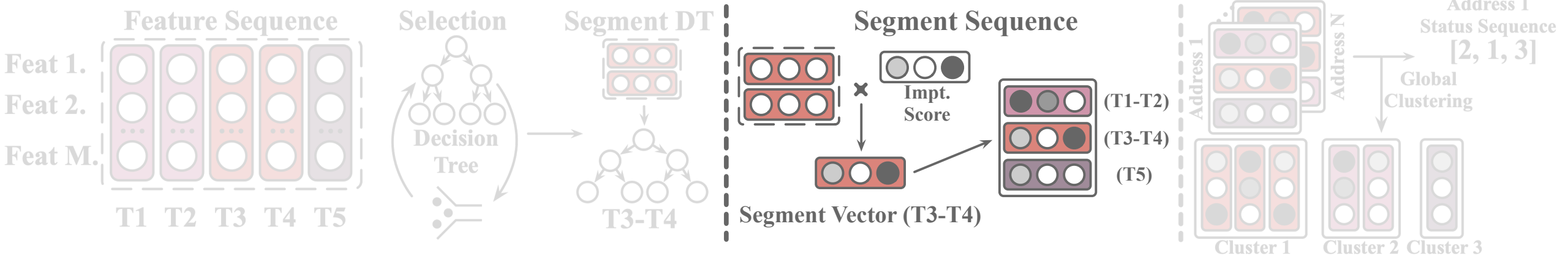


Segment →

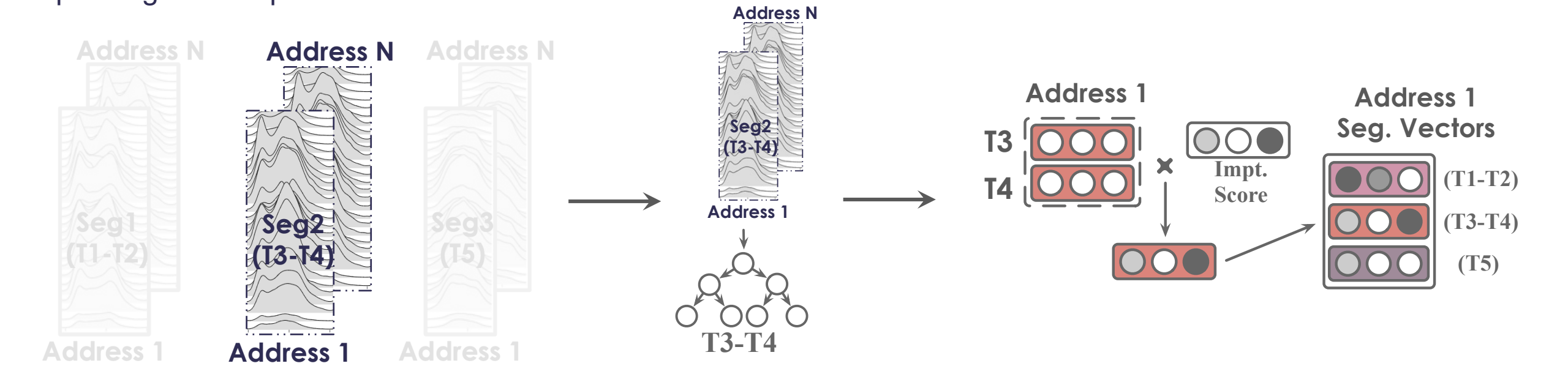


Intention Monitor

School of
Computing and
Information Systems

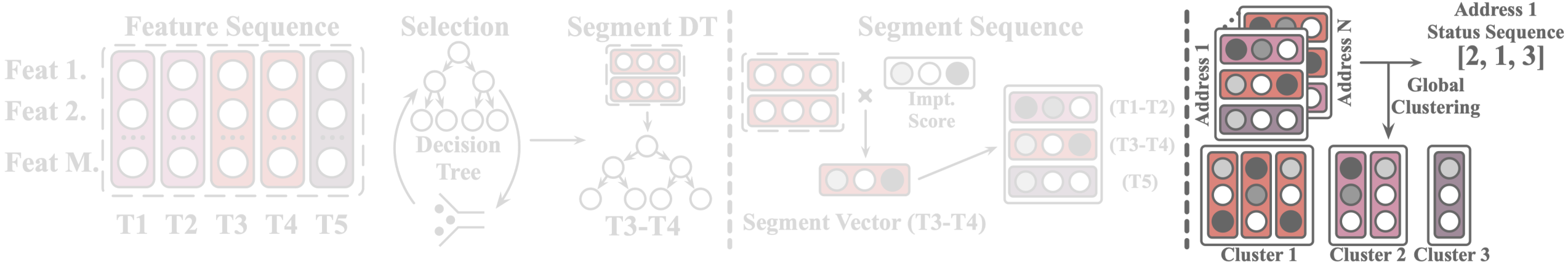


Step-2 Segment Representation

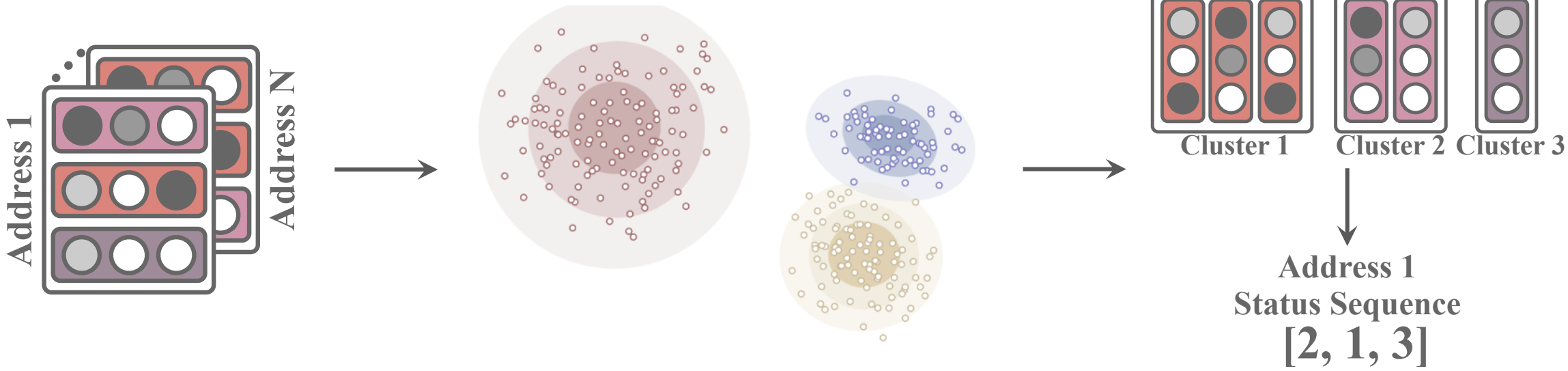


Intention Monitor

School of
Computing and
Information Systems

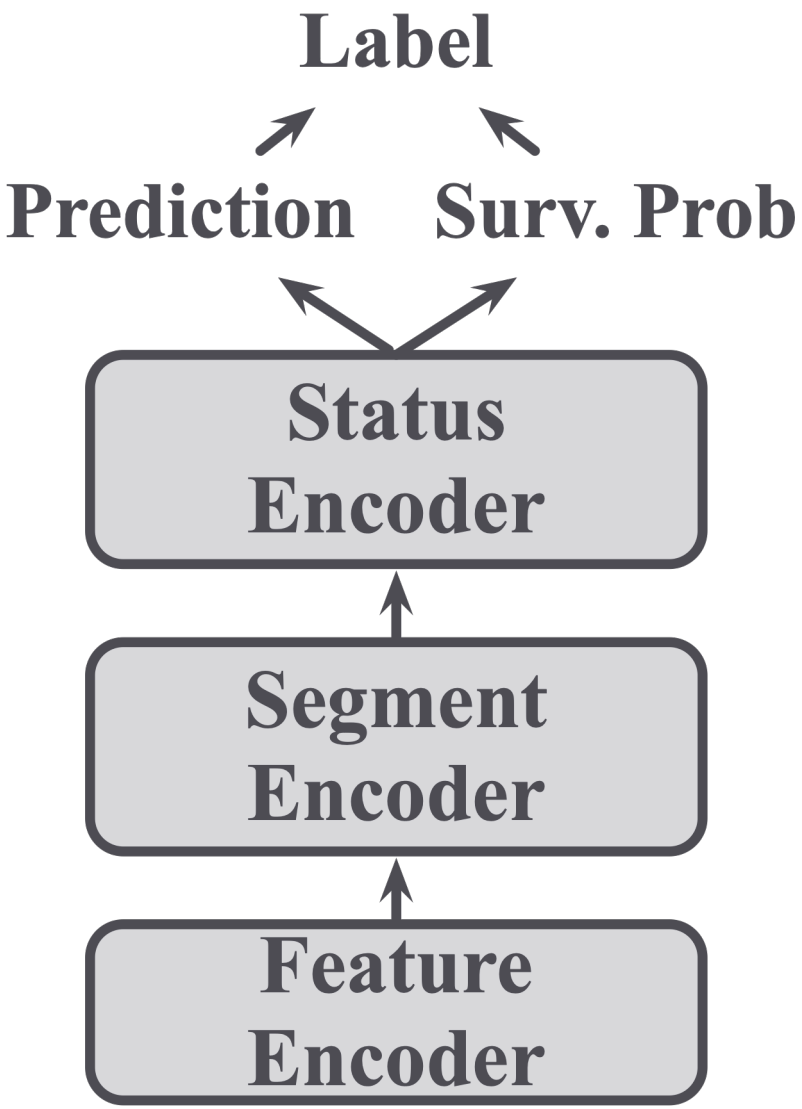


Step-3 Status Proposal



Prediction with Survival Analysis

Predictor

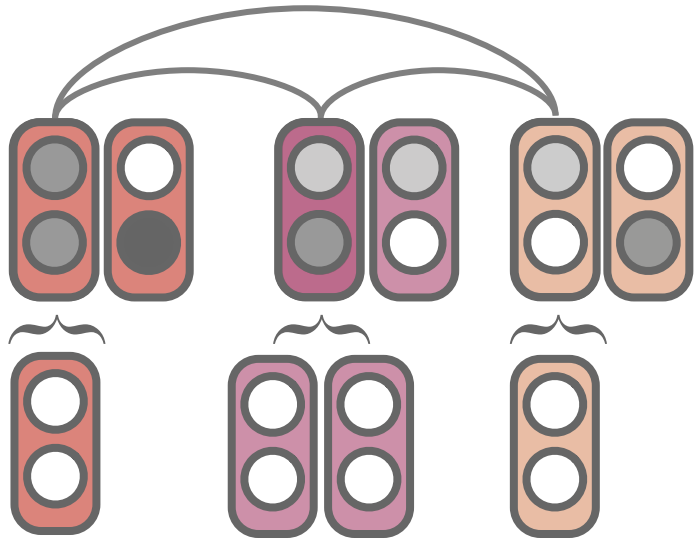


$$f^p = \sum_{i=b^p}^{e^p} \alpha_i f_i,\ \alpha_i = \exp(a_i) / \sum_{k=b^p}^{e^p} \exp(a_k),$$

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

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

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

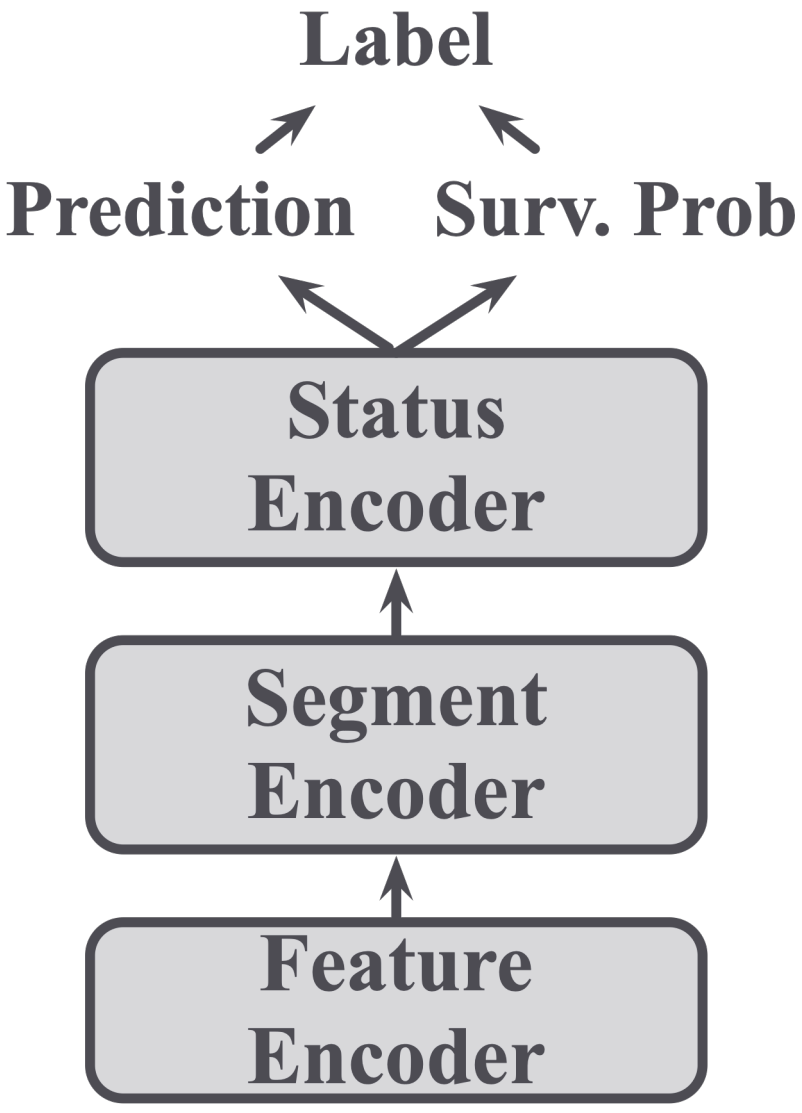


Feature Sequence (in hours)

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

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

Predictor



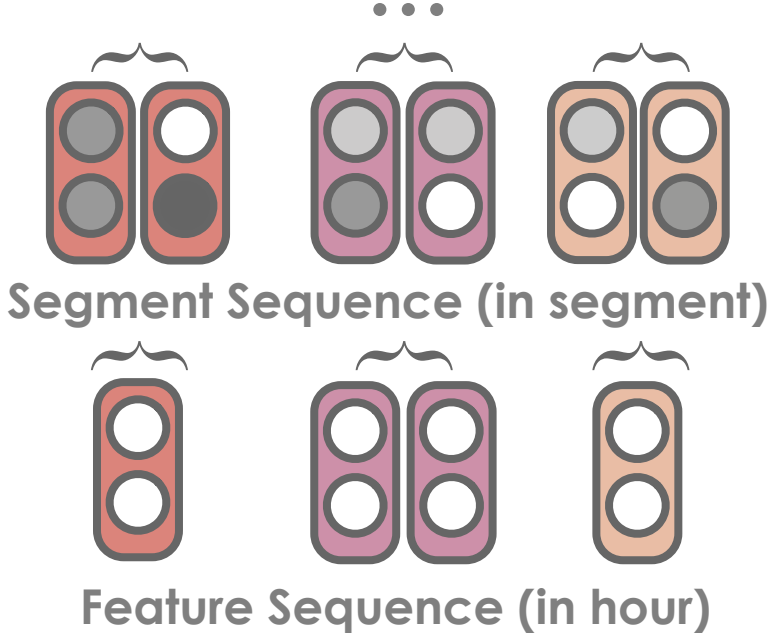
$$\hat{y}^t = S(t) * y^t + (1 - S(t)) * \hat{y}^{t-1}$$

$$y^p = \text{Sigmoid}(W^l * \bar{u}^p)$$

$$\lambda_t = ln(1 + \exp(W^{hz}\bar{u}^p)),$$

$$S(t) = exp(-\sum_{k=1}^{t} \lambda_k),$$

$$\bar{u}^p = Avg(\{\hat{u}^i\}_i^p)$$



Case Analysis

Case Analysis

Case Recap

Transaction e8b406091959700dbffc

ff30a60b190133721e5c39e89bb5fe23c5a554ab05ea

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

0.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ a98a74df...
1.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ dc03c5e9...
2.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ b3ca84de...
3.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 35f86114...
4.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ a3b14077...
5.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ d4aff83a...
6.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ af920705...
7.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 9afce068...
8.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ bd01d62c...
9.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ e50b5154...
10.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 1374e3cd...
11.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ d91ccfc1...
12.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ d42c2d3b...
13.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 156d3abe...
14.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 246b49ac...
15.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ dc22a158...
16.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 715f4cbd...
17.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 27c8f9e0...
18.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 8eef5bc2...
19.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 49c0b2d9...
20.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ fbcaa6f2...
21.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ bf45ad7b...
22.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 234e6c60...
23.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 08056916...
24.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ 032ffd2d...
25.	1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s	100.	BTC	⇐ faa33c7e...

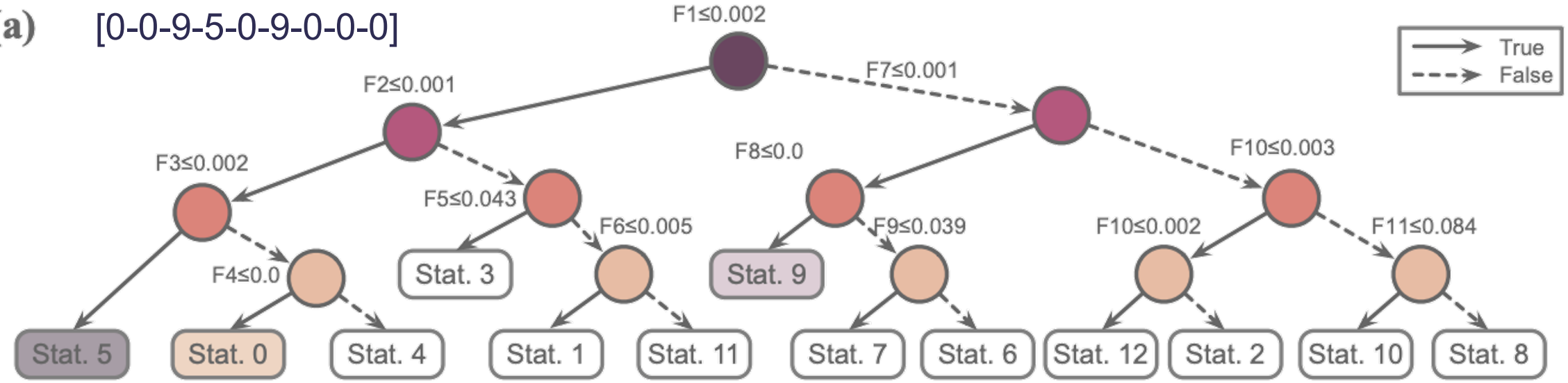
outputs: 44 (7074.18107031 BTC) unique addresses: 44, spent: 43 in 33 transactions

0.	bc1qp6k6tux6g3gr3sxw94g9tx4l0cjtu2pt65r6xp	[2e5ac3b67e]	555.997	BTC	6884775a... ⇒
1.	bc1qqp8pwq277d30cy7fjpvhcvhgztvs7v0nudgul5	[7f9e9afd92]	463.9975	BTC	8b1e6213... ⇒
2.	32LZ4wWwEhTzwtqAm2gPauktYZb5kQ6C5a	CoinPayments.net	0.0026	BTC	ccfe4342... ⇒
3.	3BMEXuoRza9EimRGSHGrwPmyFNUqWFpu8t	[0888b50bb7]	0.0746535	BTC	bf941a31... ⇒
4.	bc1qld27dqu6wrl4tmjdr8tl55qavmghwrr4ldh7qn	[7f9e9afd92]	473.9975	BTC	8b1e6213... ⇒
5.	3BMEXtMSkRt3wwXKytg7Nj86utJeSbwFHx	[51a9905c41]	0.17787495	BTC	be06bb29... ⇒
6.	bc1q8m9h3atn4cqeqhu3ekswdqxchp3g7d4v3qv3wm	[487907e868]	567.997	BTC	90ae2064... ⇒
7.	14QZ2wB8b8ZQNgb978Lwptdc8Vhv5aZQM2	[195be6cf37]	0.01944165	BTC	728f59a9... ⇒
8.	3L8JcsWNa3kuVaQJxAE1hhcoBT17rcJA6b	[00002dbb51]	0.01493527	BTC	db3e5299... ⇒
9.	bc1q7p6edvd4zvtya8uj366c23dan8pvlp503spucu	[66b7fc2922]	468.9975	BTC	bb0b41c2... ⇒
10.	bc1q93ecep2338dy9aauwyvh4g22t49rnedxl8z0tj	[589beb5a81]	0.1995	BTC	a8801564... ⇒
11.	bc1ql0wlnu80l8kctjzkzlzd72sdjqwuvruvgepceq	[7f9e9afd92]	383.998	BTC	8b1e6213... ⇒
12.	bc1q3ldtrr6xtpx8jam5gw68aaexz2wtluj0qullvr	[2377c0f10b]	189.999	BTC	7e615f3e... ⇒

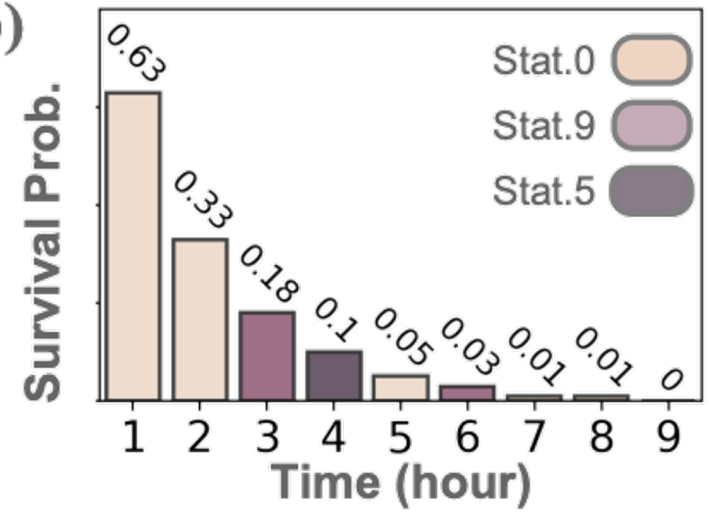
Case Analysis

Sample Address Analysis

(a) [0-0-9-5-0-9-0-0-0]



(b)



(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)

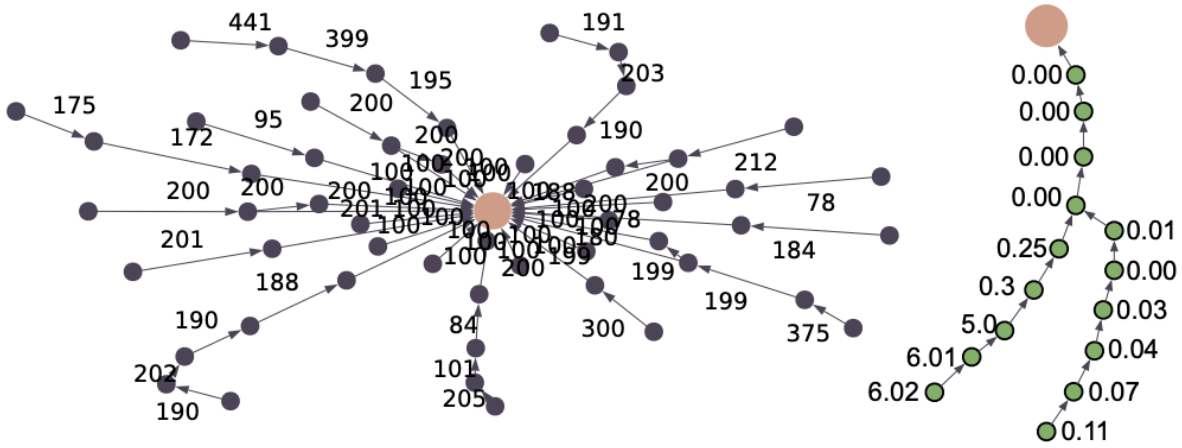
F11: LT-FR-Max-Input-Amt (Std)

Case Analysis

School of Computing and Information Systems

Sample Address Analysis

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



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.

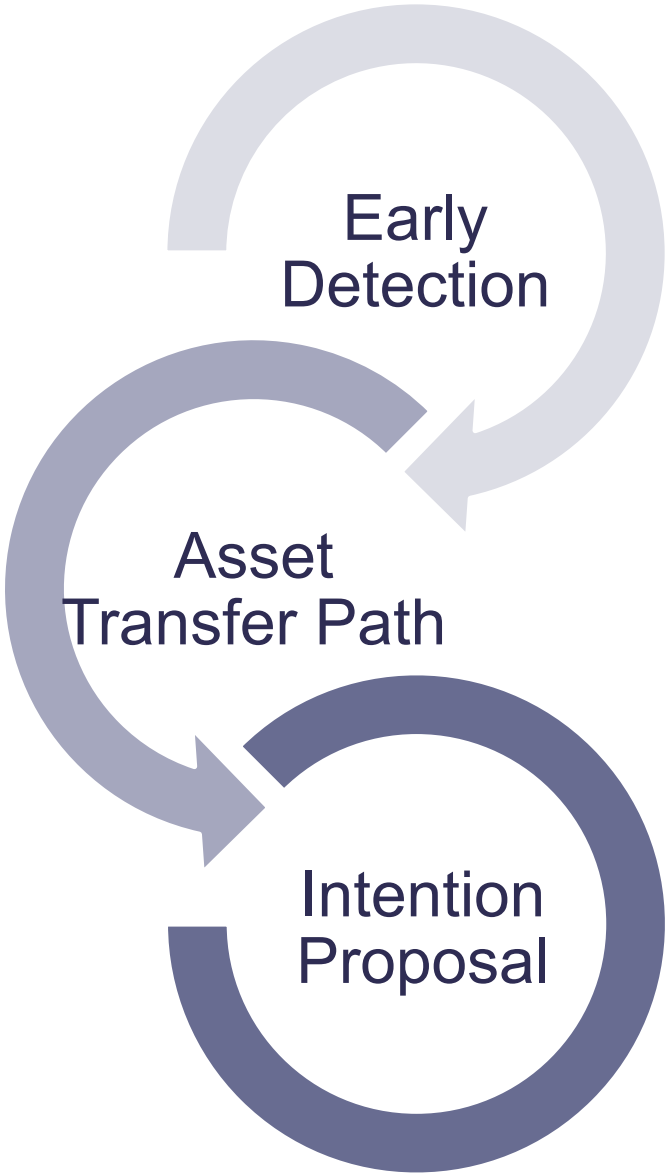
However, some possible reasons why an address with these characteristics could be considered malicious include:

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

School of
Computing and
Information Systems



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

Thanks for Listening