UC SANTA BARBARA

SEC LAB

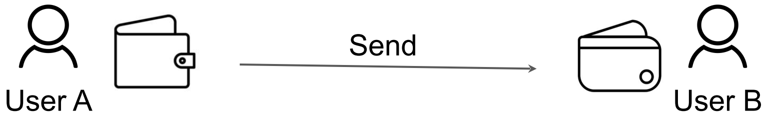
GuideEnricher: Protecting the Anonymity of Ethereum Mixing Service Users with Deep Reinforcement Learning

Ravindu De Silva

R. De Silva, W. Guo, N. Ruaro, I. Grishchenko, C. Kruegel, G. Vigna

Background

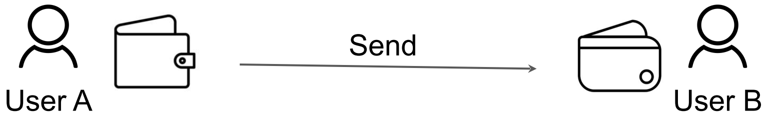
Transferring money over public blockchain.



# Block	From	Operation	Arguments	To
n	Addr. A	Transfer	…	Addr. B
. .				
..	…	…	…	...

Background

Transferring money over public blockchain.

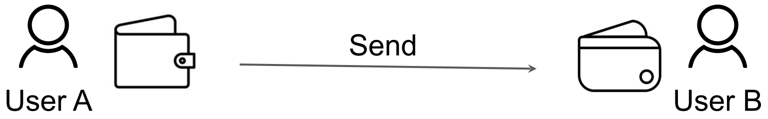


# Block	From	Operation	Arguments	To
n	Addr. A	Transfer	…	Addr. B
. .				
..	…	…	…	...

- All transactions throughout history are visible in public blockchains (e.g., Ethereum chain, Binance chain, Bitcoin, etc).
- Any actor can link and cluster transactions to reveal user identities to a certain extent, raising significant privacy concerns.

Background

Transferring money over public blockchain.

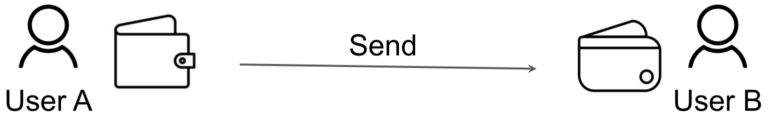


# Block	From	Operation	Arguments	To
n	Addr. A	Transfer	…	Addr. B
. .				
..	…	…	…	...

- All transactions throughout history are visible in public blockchains (e.g., Ethereum chain, Binance chain, Bitcoin, etc).
- Any actor can link and cluster transactions to reveal user identities to a certain extent, raising significant privacy concerns.
- Mixing services have been introduced to public blockchains over time under different cryptographic protocols.

Background

Transferring money over public blockchain.



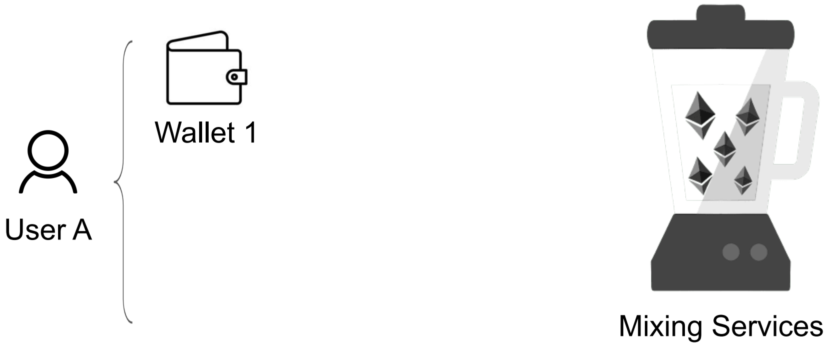
# Block	From	Operation	Arguments	To
n	Addr. A	Transfer	…	Addr. B
. .				
..	…	…	…	...

- All transactions throughout history are visible in public blockchains (e.g., Ethereum chain, Binance chain, Bitcoin, etc).
- Any actor can link and cluster transactions to reveal user identities to a certain extent, raising significant privacy concerns.
- Mixing services have been introduced to public blockchains over time under different cryptographic protocols.

Tornado Cash   Railgun   Cyclone Protocol

Background

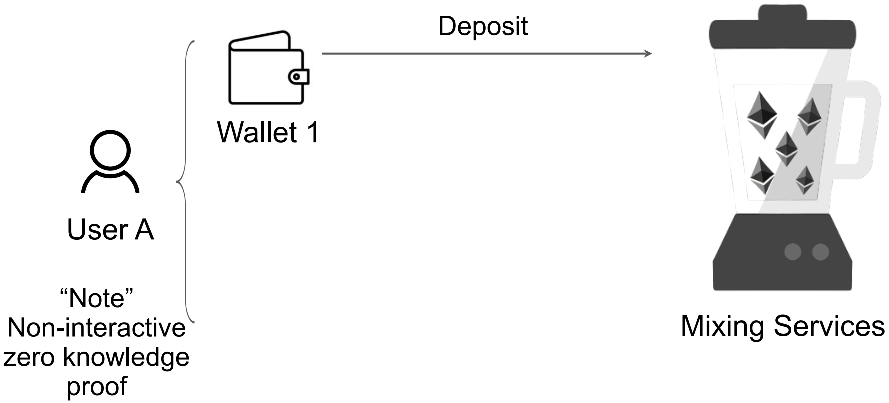
Transferring money over public blockchain using **Mixing Services.**



From	Operation	Argument	To
…	…	…	…
…	…	…	…
…	…	…	…

Background

Transferring money over public blockchain using **Mixing Services.**



Deposit

Wallet 1

User A

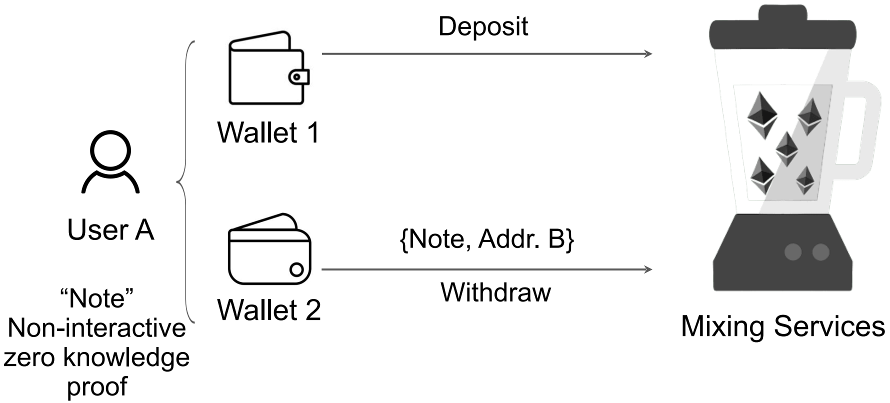
“Note”
Non-interactive
zero knowledge
proof

Mixing Services

From	Operation	Argument	To
Addr. A1	Deposit	…	TC
…	…	…	…
…	…	…	…

Background

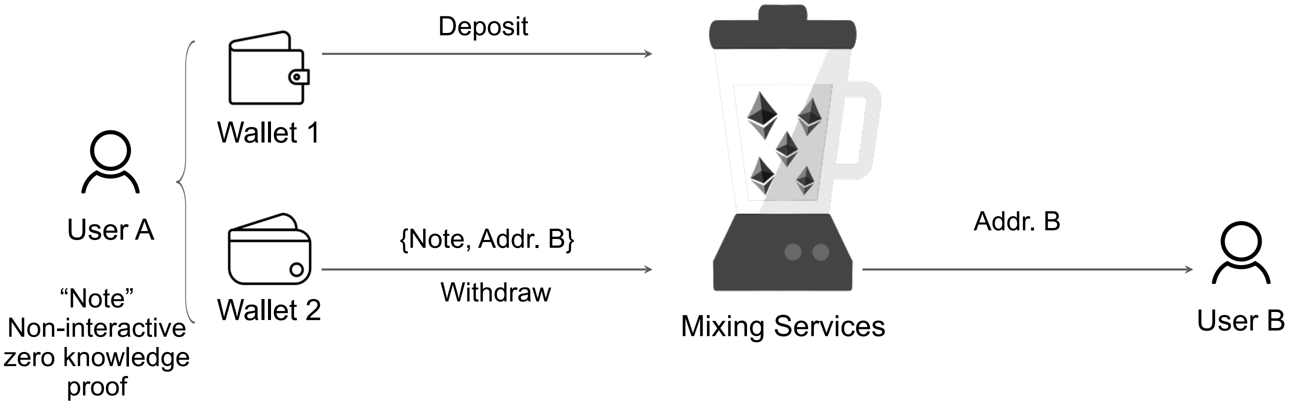
Transferring money over public blockchain using **Mixing Services.**



From	Operation	Argument	To
Addr. A1	Deposit	…	TC
…	…	…	…
…	…	…	…

Background

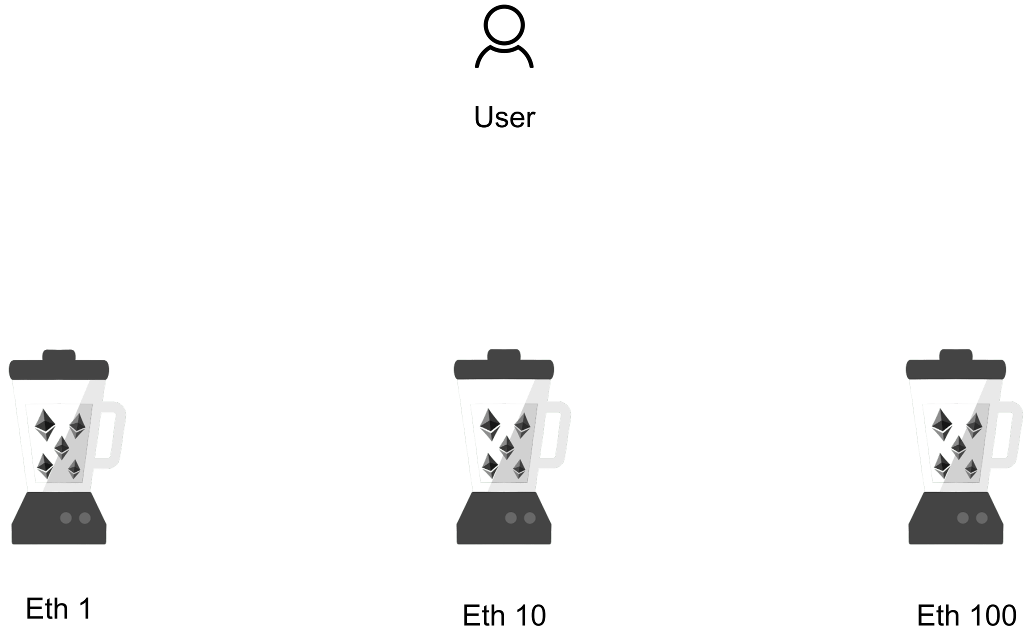
Transferring money over public blockchain using **Mixing Services.**



From	Operation	Argument	To
Addr. A1	Deposit	…	TC
Addr. A2	Withdraw	Note, Addr. B	TC
TC	Internal	…	Addr. B

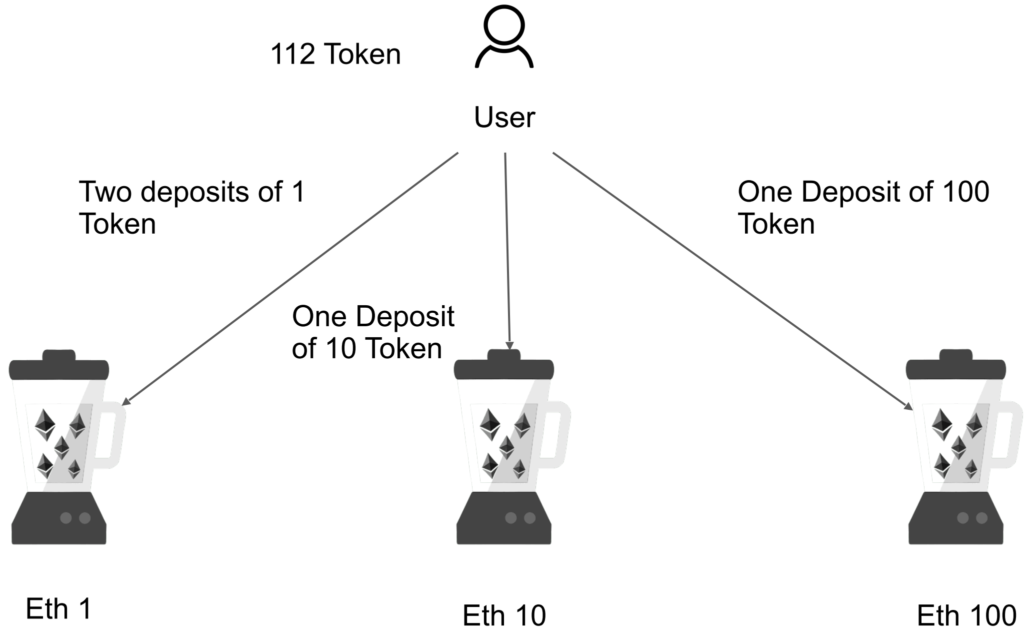
Background

Transferring money over public blockchain using **Mixing Services.**



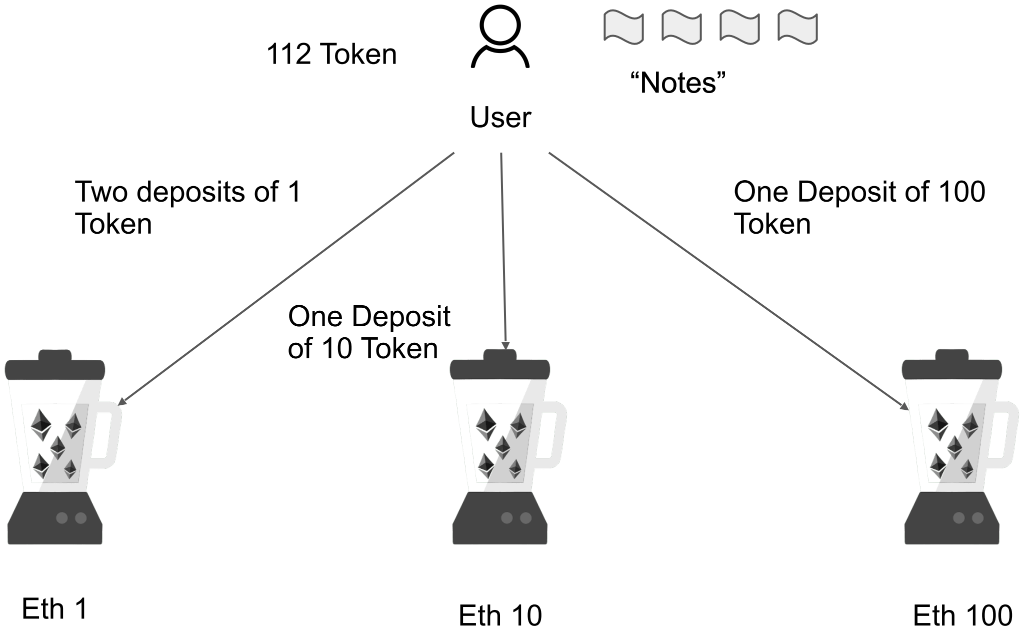
Background

Transferring money over public blockchain using **Mixing Services.**



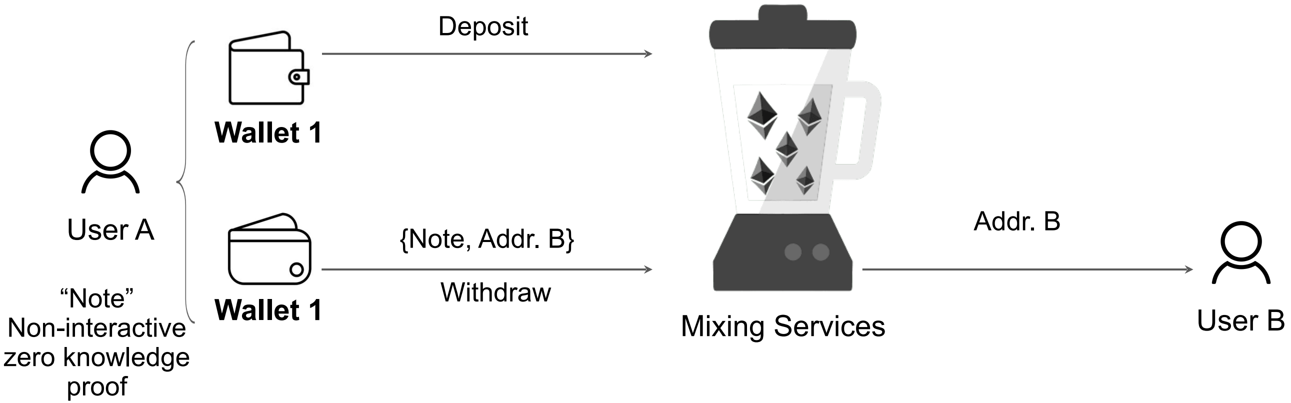
Background

Transferring money over public blockchain using **Mixing Services.**



Background

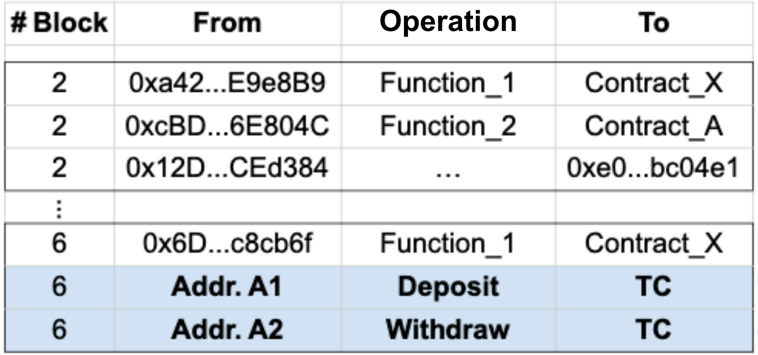
Anonymity **compromising** scenario #1 (Address Reuse)



From	Operation	Argument	To
Addr. A1	Deposit	…	TC
Addr. A1	Withdraw	Note, Addr. B	TC
TC	Internal	…	Addr. B

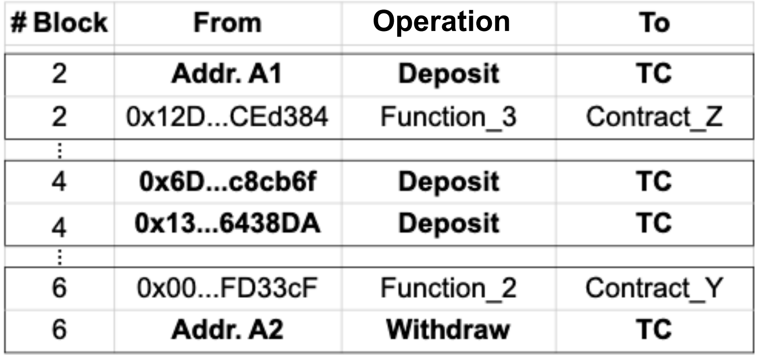
Background

Anonymity **compromising** scenario #2 (Improper waiting)



# Block	From	Operation	To
2	0xa42...E9e8B9	Function_1	Contract_X
2	0xcBD...6E804C	Function_2	Contract_A
2	0x12D...CEd384	…	0xe0...bc04e1
⋮			
6	0x6D...c8cb6f	Function_1	Contract_X
6	**Addr. A1**	**Deposit**	**TC**
6	**Addr. A2**	**Withdraw**	**TC**

TC transaction without waiting.



# Block	From	Operation	To
2	**Addr. A1**	**Deposit**	**TC**
2	0x12D...CEd384	Function_3	Contract_Z
⋮			
4	**0x6D...c8cb6f**	**Deposit**	**TC**
4	**0x13...6438DA**	**Deposit**	**TC**
⋮			
6	0x00...FD33cF	Function_2	Contract_Y
6	**Addr. A2**	**Withdraw**	**TC**

TC transaction with proper waiting.

Money transfer by User~A (from Wallet~A1 to Wallet~A2) via TC,
with different wait times between the deposit and withdrawal transaction.

Background

Guide Book

- After depositing, users should wait some amount of time before withdrawing to improve their privacy.

- Do not reuse the same address for both deposit and withdraw.

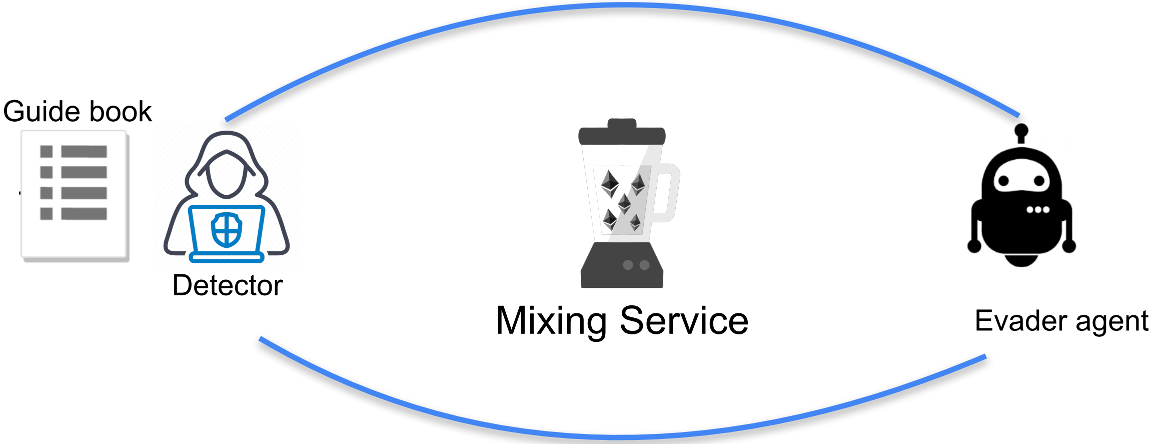
Motivation

- **Inadequate Guidebooks:**
  - Current guidebooks are incomplete.
  - Users unknowingly perform actions compromising their anonymity.

- **Postmortem Analysis Limitation:**
  - Existing methods identify patterns after deployment.
  - Lack of proactive discovery of anonymity-compromising patterns.

GuideEnricher

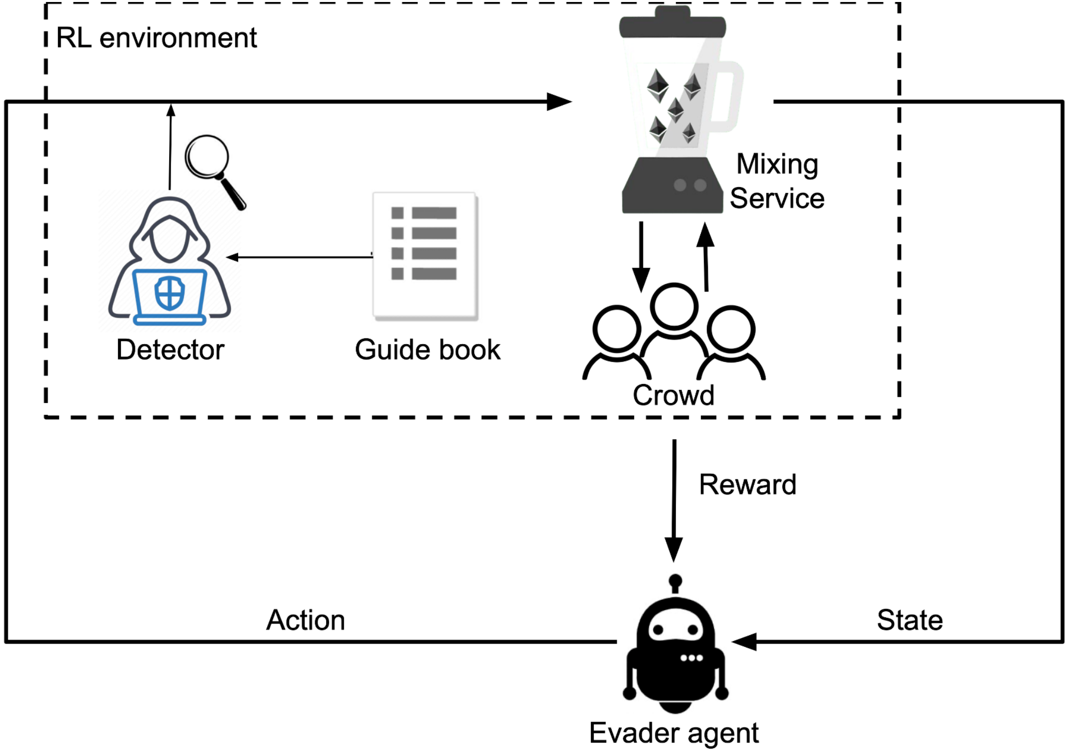
Proactive method to enrich guidebooks using Deep Reinforcement Learning (DRL)



Extracting **unknown anonymity-compromising patterns** as the Evader Agent **formulates strategies to evade Detector.**

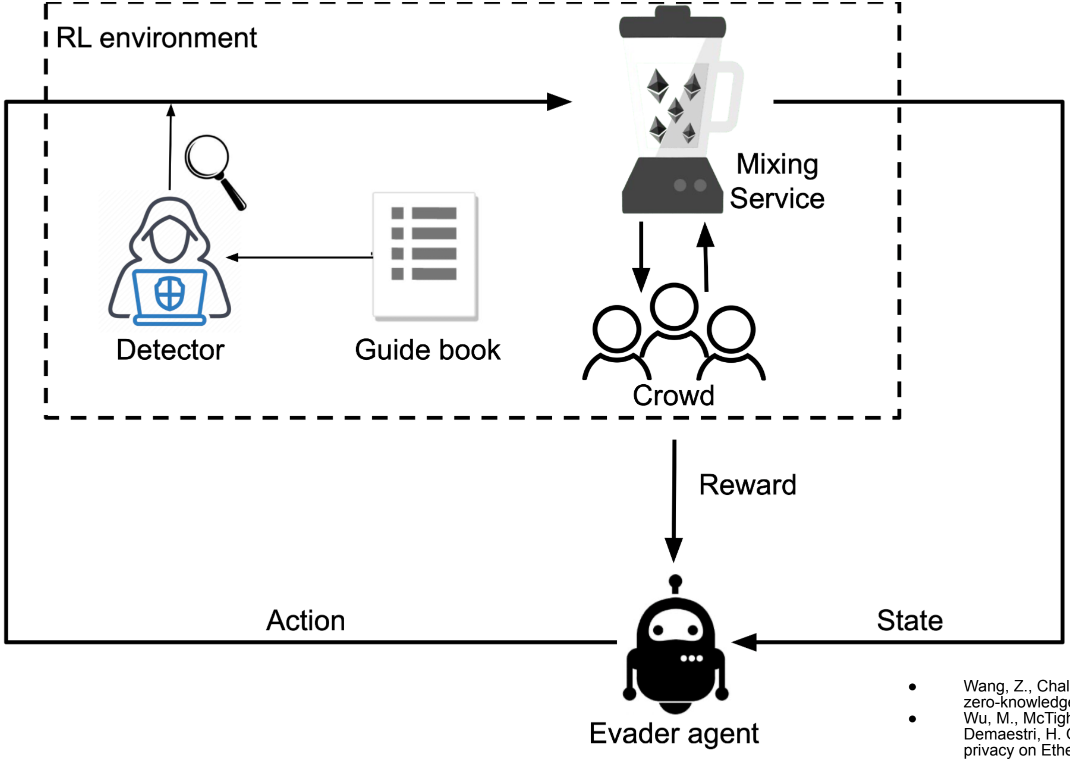
GuideEnricher

Proactive method to enrich guidebooks using Deep Reinforcement Learning (DRL)



GuideEnricher

Proactive method to enrich guidebooks using Deep Reinforcement Learning (DRL)

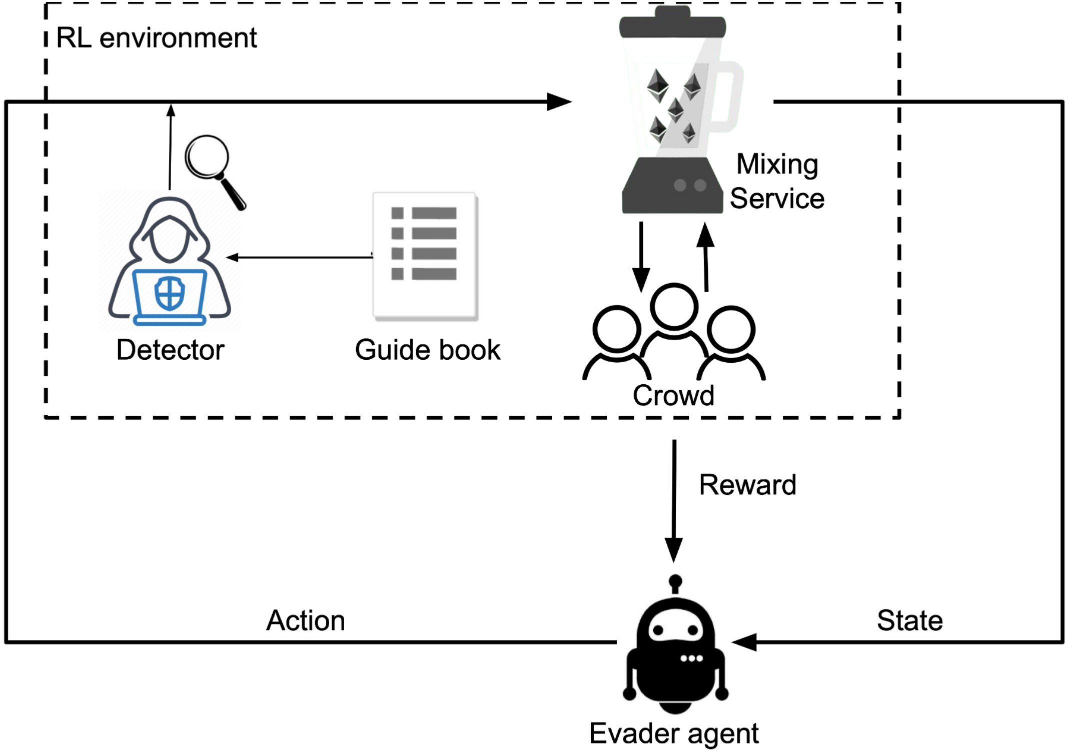


Guide Book	
1. Address Match	An address is used for both depositing and withdrawing.
2. Unique Gas Prices	A pair of deposit and withdrawal transactions with same gas price.
3. Linked ETH Addresses	Two distinct addresses have transaction history outside the mixing services.

- Wang, Z., Chaliasos, S., Qin, K., Zhou, L., Gao, L., Berrang, P., Livshits, B., & Gervais, A. (2023). "On how zero-knowledge proof blockchain mixers improve, and worsen user privacy." *arXiv*.
- Wu, M., McTighe, W., Wang, K., Seres, I. A., Bax, N., Puebla, M., Mendez, M., Carrone, F., De Mattey, T., Demaestri, H. O., Nicolini, M., & Fontana, P. (2022). "Tutela: An open-source tool for assessing user-privacy on Ethereum and Tornado Cash." *arXiv*.

GuideEnricher

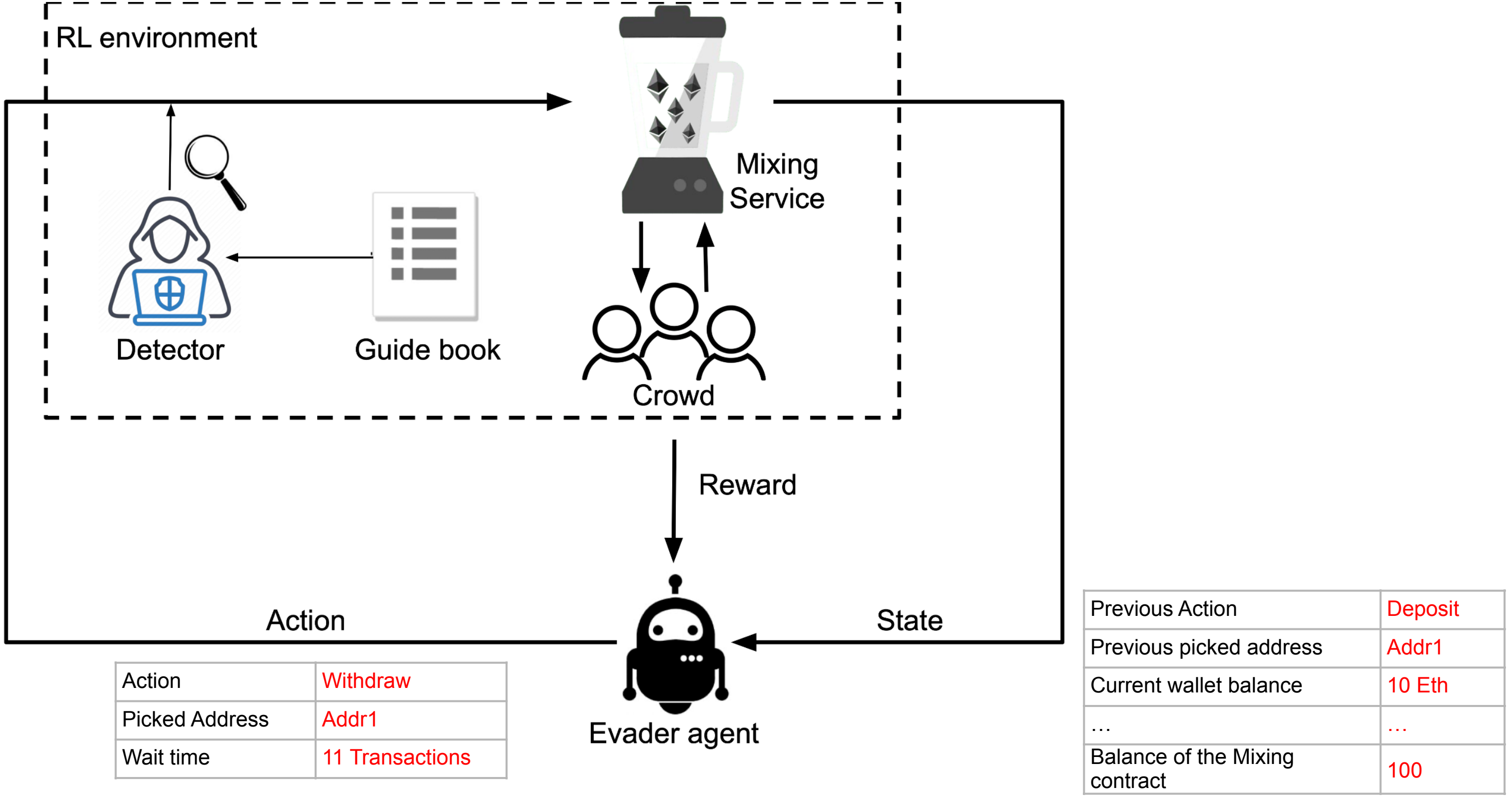
One **step** of Evader agent



Previous Action	Deposit
Previous picked address	Addr1
Current wallet balance	10 Eth
…	…
Balance of the Mixing contract	100

GuideEnricher

One **step** of Evader agent

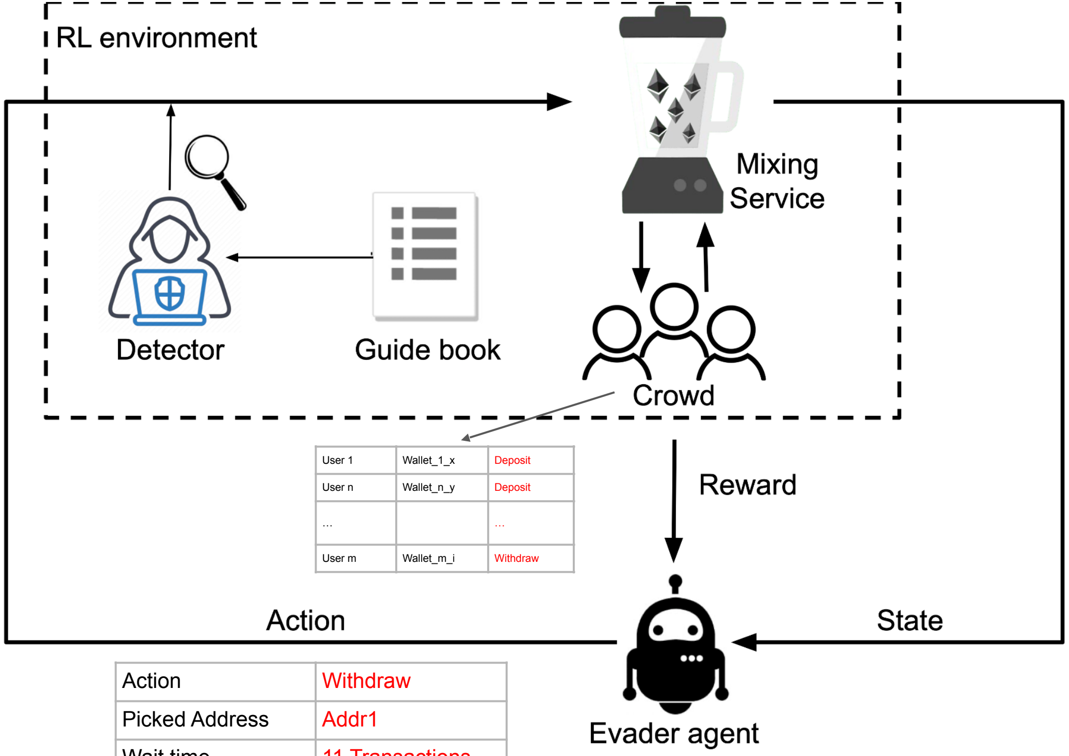


Action	Withdraw
Picked Address	Addr1
Wait time	11 Transactions

Previous Action	Deposit
Previous picked address	Addr1
Current wallet balance	10 Eth
…	…
Balance of the Mixing contract	100

GuideEnricher

One **step** of Evader agent



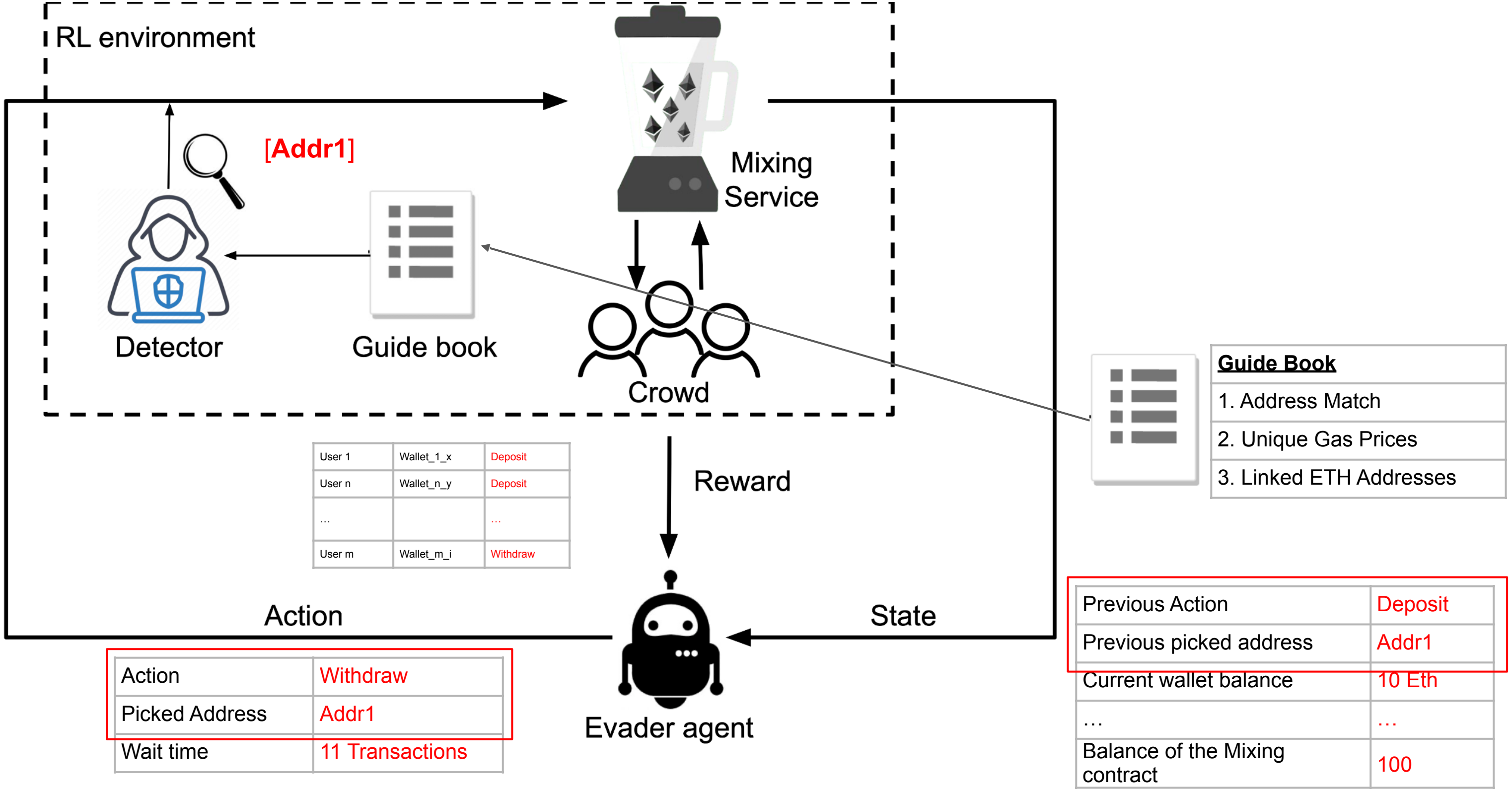
User 1	Wallet_1_x	Deposit
User n	Wallet_n_y	Deposit
…		…
User m	Wallet_m_i	Withdraw

Action	Withdraw
Picked Address	Addr1
Wait time	11 Transactions

Previous Action	Deposit
Previous picked address	Addr1
Current wallet balance	10 Eth
…	…
Balance of the Mixing contract	100

GuideEnricher

One **step** of Evader agent



User 1	Wallet_1_x	Deposit
User n	Wallet_n_y	Deposit
…		…
User m	Wallet_m_i	Withdraw

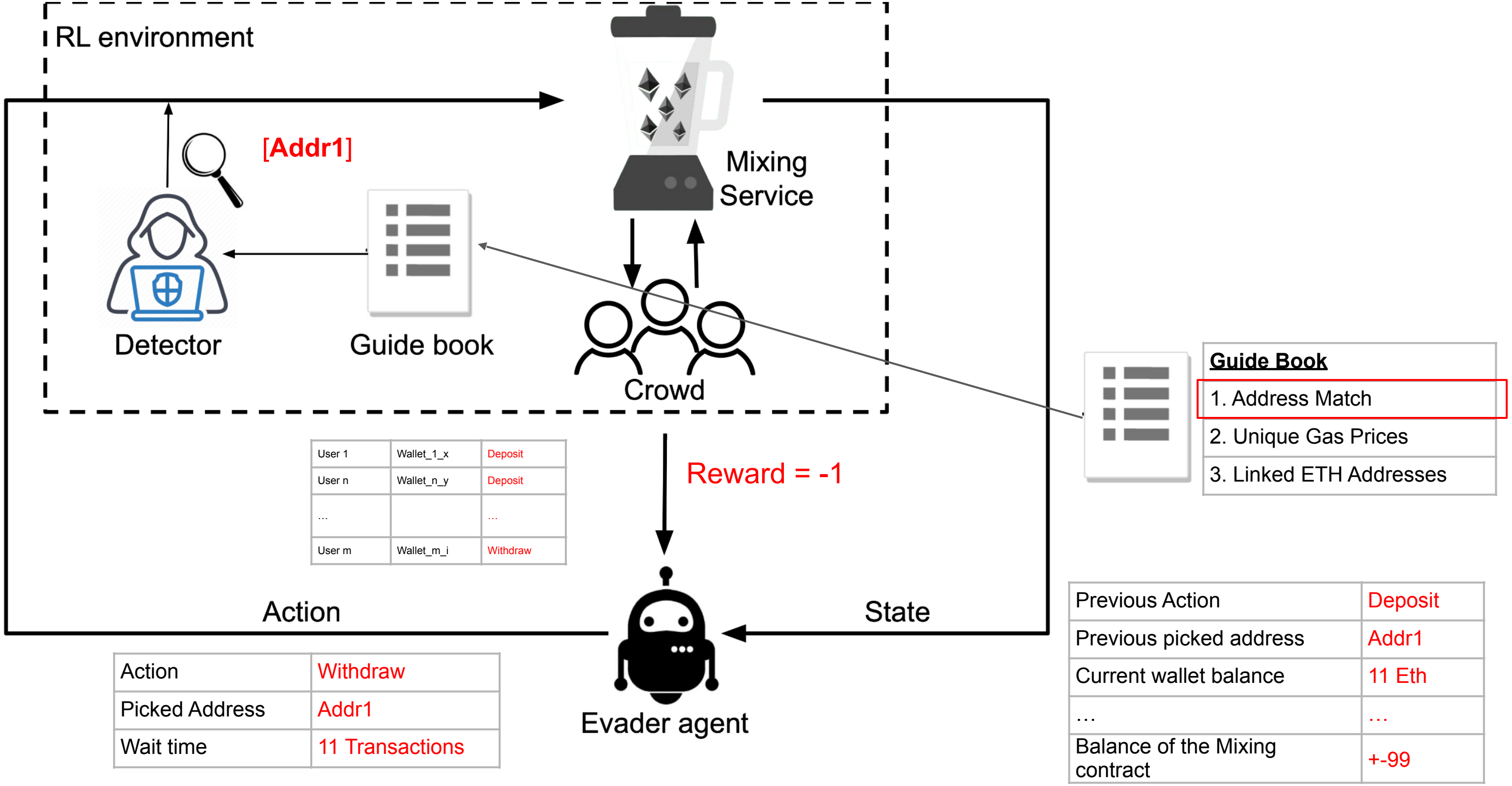
Guide Book
1. Address Match
2. Unique Gas Prices
3. Linked ETH Addresses

Action	Withdraw
Picked Address	Addr1
Wait time	11 Transactions

Previous Action	Deposit
Previous picked address	Addr1
Current wallet balance	10 Eth
…	…
Balance of the Mixing contract	100

GuideEnricher

One **step** of Evader agent



User 1	Wallet_1_x	Deposit
User n	Wallet_n_y	Deposit
...		...
User m	Wallet_m_i	Withdraw

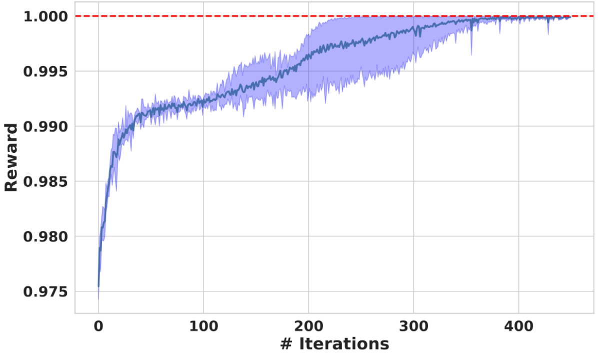
Action	Withdraw
Picked Address	Addr1
Wait time	11 Transactions

Guide Book
1. Address Match
2. Unique Gas Prices
3. Linked ETH Addresses

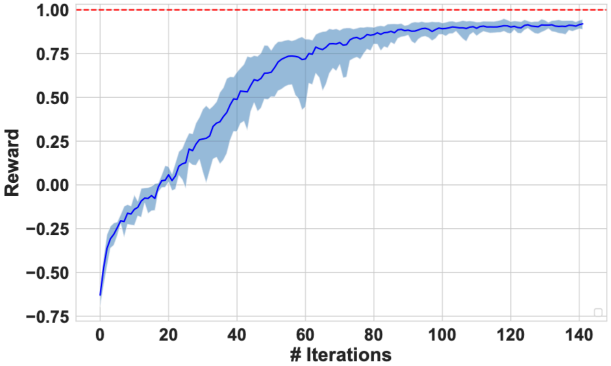
Previous Action	Deposit
Previous picked address	Addr1
Current wallet balance	11 Eth
…	…
Balance of the Mixing contract	+-99

Training Phase

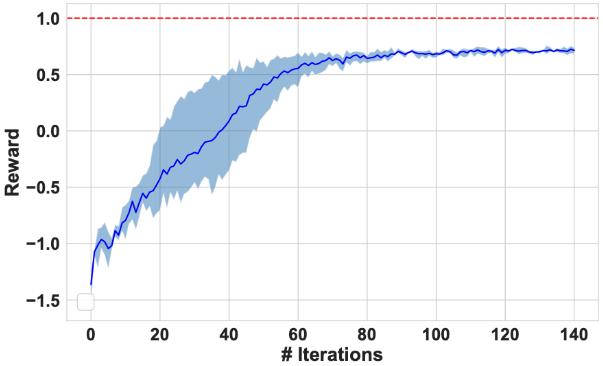
Generalizability to other mixing services. (#3 wallets with 3 tokens each, transfer to any of #247 empty wallets)



GuideEnricher on Tornado Cash.



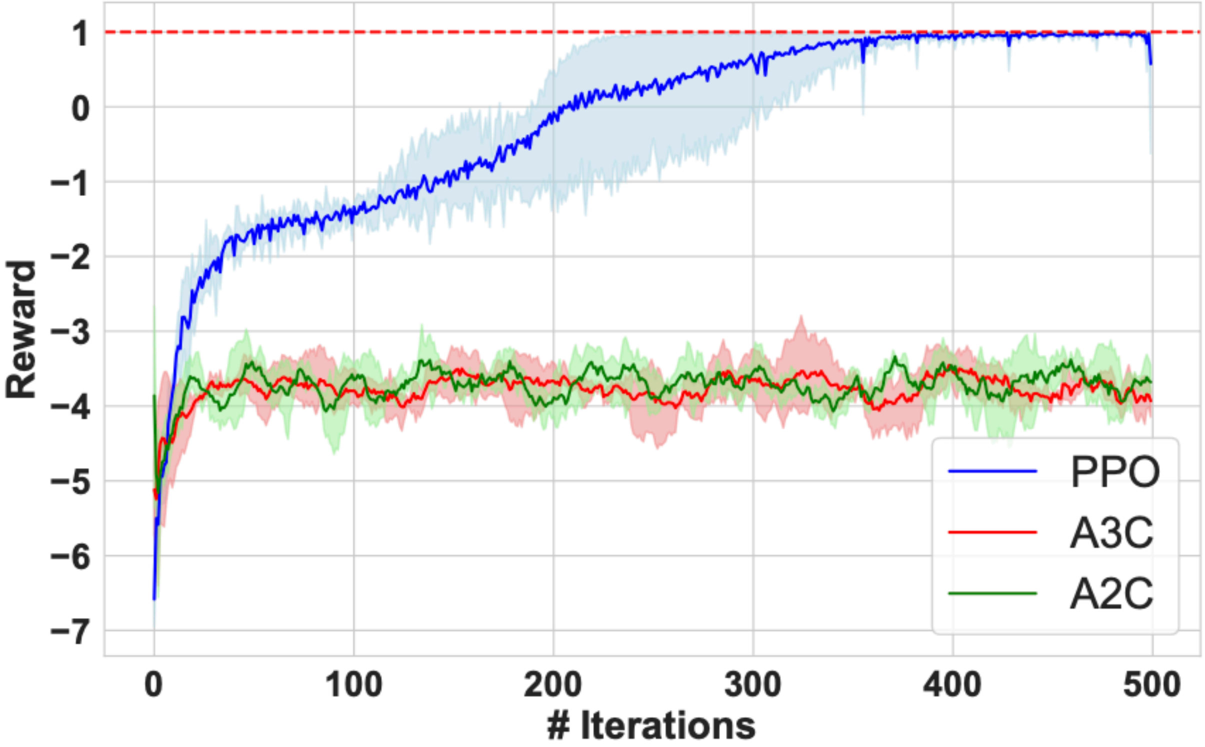
GuideEnricher on Tornado Cash Nova.



GuideEnricher on Railgun.

Training Phase

PPO vs A2C and A3C (GuideEnricher on Tornado Cash)



Extracting Anonymity-Compromising Patterns

Combined both **training** and **testing** episodes across different simulations. **Filtered** out episodes with **evading rates below 90%.**

Clustering utilizing **DBSCAN** and **K-means**. Chose episodes **near the centroid** of each cluster.

Examine representative episodes to find **anonymity-compromising patterns**

Enriching GuideBook

Unknown Anonymity-Compromising Pattern #1

Guide Book	
2. Unique Gas Prices	**A pair** of deposit and withdrawal transactions with same gas price.

# Block	From	Gas Price	Method	To	
	. .				
n	0xa03...49e8B9	g2	Function1	Contract_Y	
n	0xcBD...Fe6E80	g2	Function4	Contract_A	
n	**Addr. A1**	**g2**	**Deposit**	**TC**	⇦
n	**Addr. A2**	**g2**	**Deposit**	**TC**	⇦
n	**Addr. A3**	**g2**	**Deposit**	**TC**	⇦
n	**Addr. A4**	**g2**	**Withdraw**	**TC**	⇦

Enriching GuideBook

Unknown Anonymity-Compromising Pattern #1

Guide Book	
2. Unique Gas Prices	**A pair** of deposit and withdrawal transactions with same gas price.

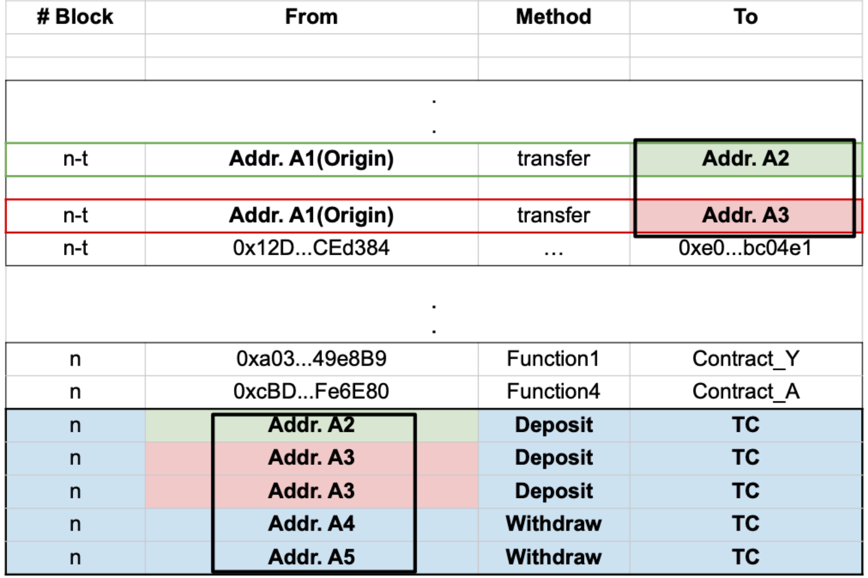
# Block	From	Gas Price	Method	To
		. .		
n	0xa03...49e8B9	g2	Function1	Contract_Y
n	0xcBD...Fe6E80	g2	Function4	Contract_A
n	**Addr. A1**	**g2**	**Deposit**	**TC**
n	**Addr. A2**	**g2**	**Deposit**	**TC**
n	**Addr. A3**	**g2**	**Deposit**	**TC**
n	**Addr. A4**	**g2**	**Withdraw**	**TC**

Guide Book	
2. Unique Gas Prices	**A pair** of deposit and withdrawal transactions with same gas price.
2. Unique Gas Prices (multi)	**A group** of deposit and withdrawal transactions with same gas price.

Enriching GuideBook

Unknown Anonymity-Compromising Pattern #2

Guide Book	
3. Linked ETH Addresses	Two distinct addresses have transaction history outside the mixing services.

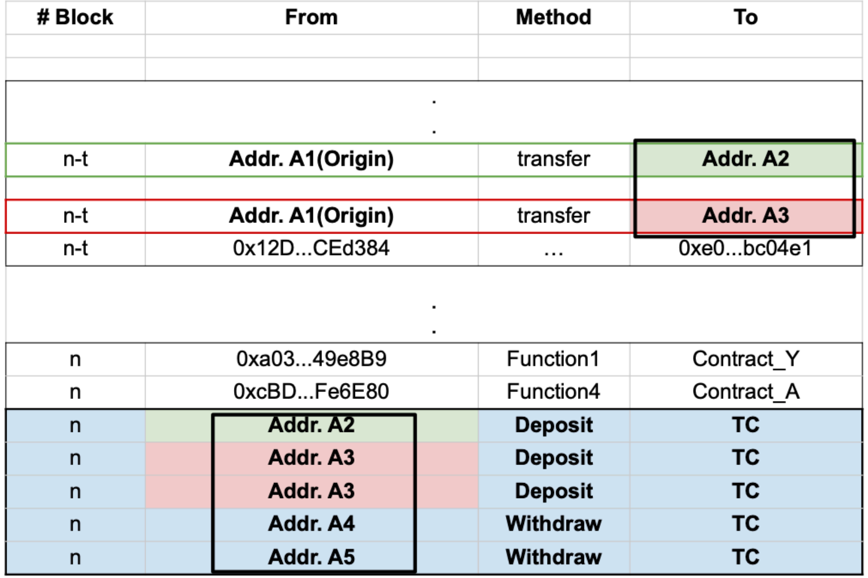


# Block	From	Method	To
	.		
	.		
n-t	**Addr. A1(Origin)**	transfer	**Addr. A2**
n-t	**Addr. A1(Origin)**	transfer	**Addr. A3**
n-t	0x12D...CEd384	…	0xe0...bc04e1
	.		
	.		
n	0xa03...49e8B9	Function1	Contract_Y
n	0xcBD...Fe6E80	Function4	Contract_A
n	**Addr. A2**	**Deposit**	**TC**
n	**Addr. A3**	**Deposit**	**TC**
n	**Addr. A3**	**Deposit**	**TC**
n	**Addr. A4**	**Withdraw**	**TC**
n	**Addr. A5**	**Withdraw**	**TC**

Enriching GuideBook

Unknown Anonymity-Compromising Pattern #2

Guide Book	
3. Linked ETH Addresses	Two distinct addresses have transaction history outside the mixing services.



# Block	From	Method	To
	.		
	.		
n-t	**Addr. A1(Origin)**	transfer	**Addr. A2**
n-t	**Addr. A1(Origin)**	transfer	**Addr. A3**
n-t	0x12D...CEd384	…	0xe0...bc04e1
	.		
	.		
n	0xa03...49e8B9	Function1	Contract_Y
n	0xcBD...Fe6E80	Function4	Contract_A
n	**Addr. A2**	**Deposit**	**TC**
n	**Addr. A3**	**Deposit**	**TC**
n	**Addr. A3**	**Deposit**	**TC**
n	**Addr. A4**	**Withdraw**	**TC**
n	**Addr. A5**	**Withdraw**	**TC**

Guide Book	
3. Linked ETH Addresses	Two distinct addresses have transaction history outside the mixing services.
6. Token distribution.	Transfer of tokens to unused "fresh" wallets immediately before the interaction with mixer.

Contributions:

1. We design and develop GuideEnricher, a **DRL-driven method** that simulates user interactions with mixing services to facilitate guidebook construction.
2. We evaluate GuideEnricher on multiple mixing services, and demonstrate that GuideEnricher can facilitate **extracting anonymity-compromising patterns without requiring significant human effort**.
3. We present the usage of GuideEnricher in continuously enriching the guidebook by iteratively updating the rule-based detector and our evaders.

github.com/ucsb-seclab/GUIDE-ENRICHER