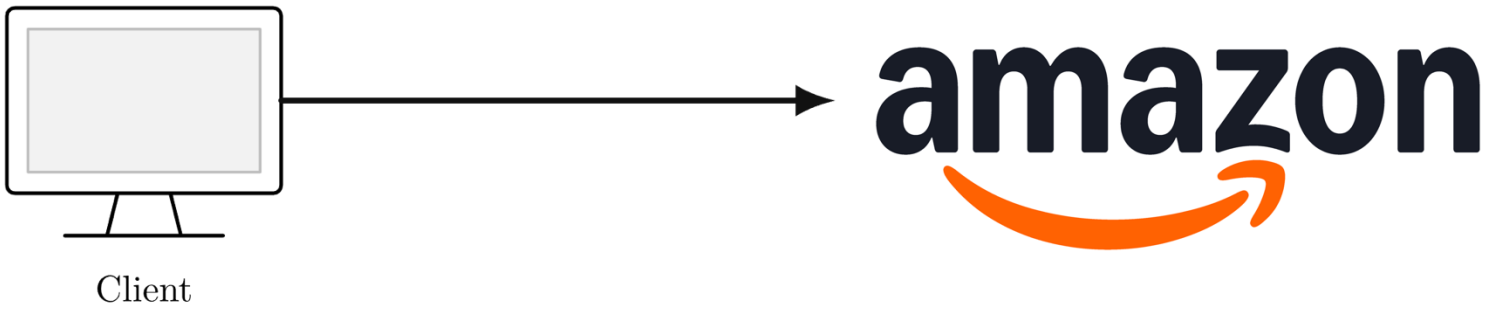
Darknet Markets in Principle

Tim K.

Buying on Amazon



Buying on Amazon



Buying on Amazon



Buying on Amazon



- Anonymity of the client

Buying on Amazon



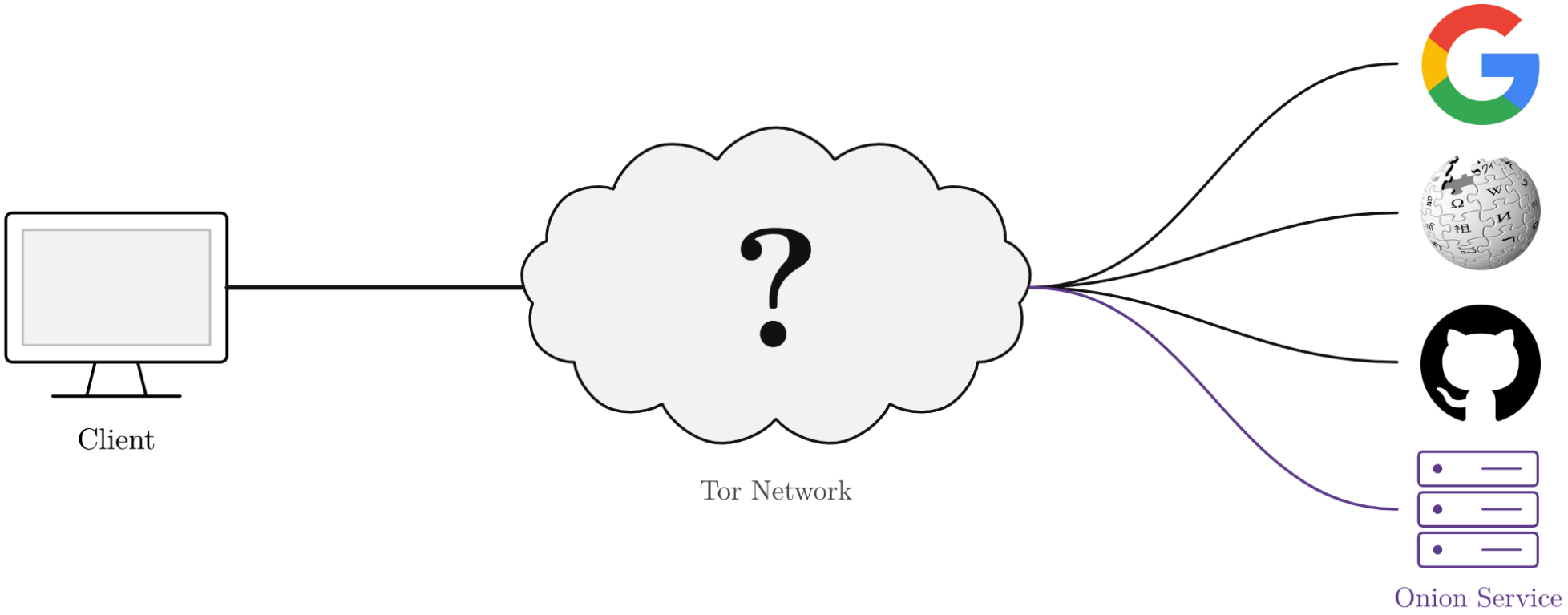
- Anonymity of the client
- Anonymity of the server

Buying on Amazon



- Anonymity of the client
- Anonymity of the server
- Anonymity of the payment

What is Tor?



Part I

How Tor Works

Single proxy vs. Tor circuit

Single proxy (VPN)



Single proxy vs. Tor circuit

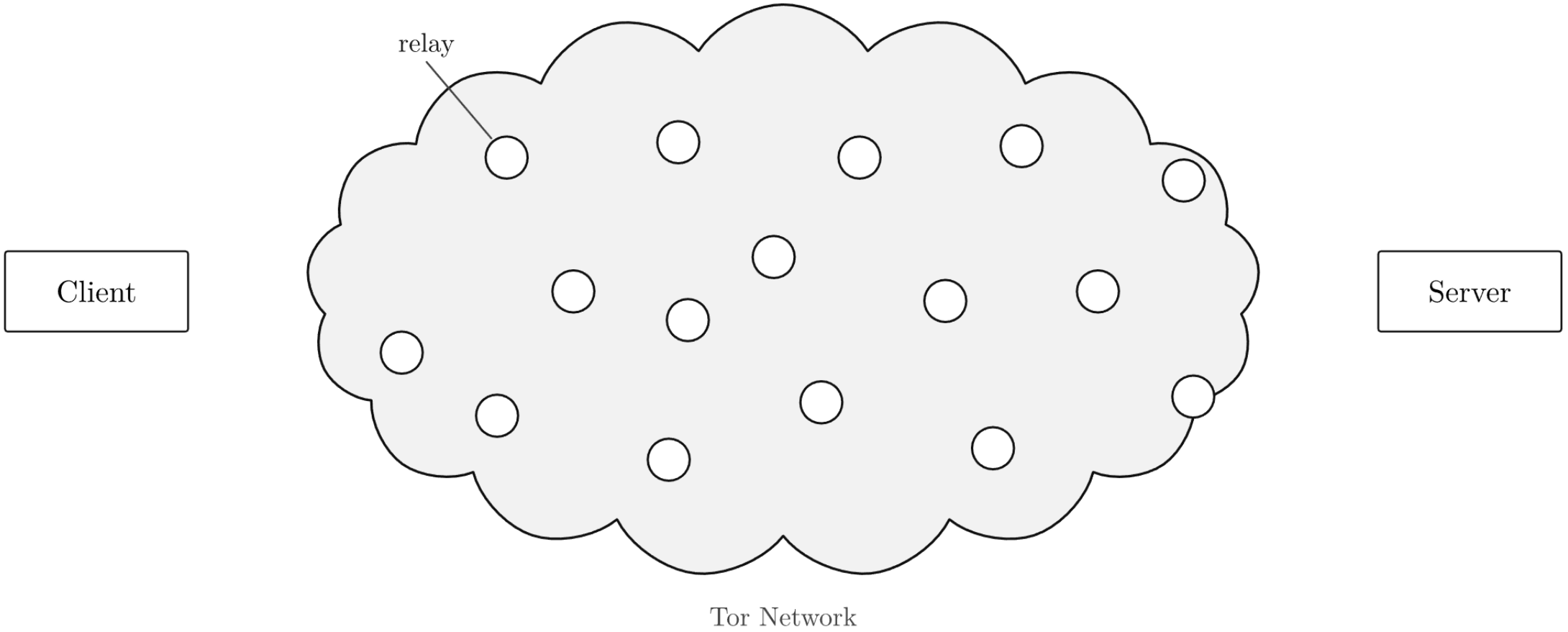
Single proxy (VPN)



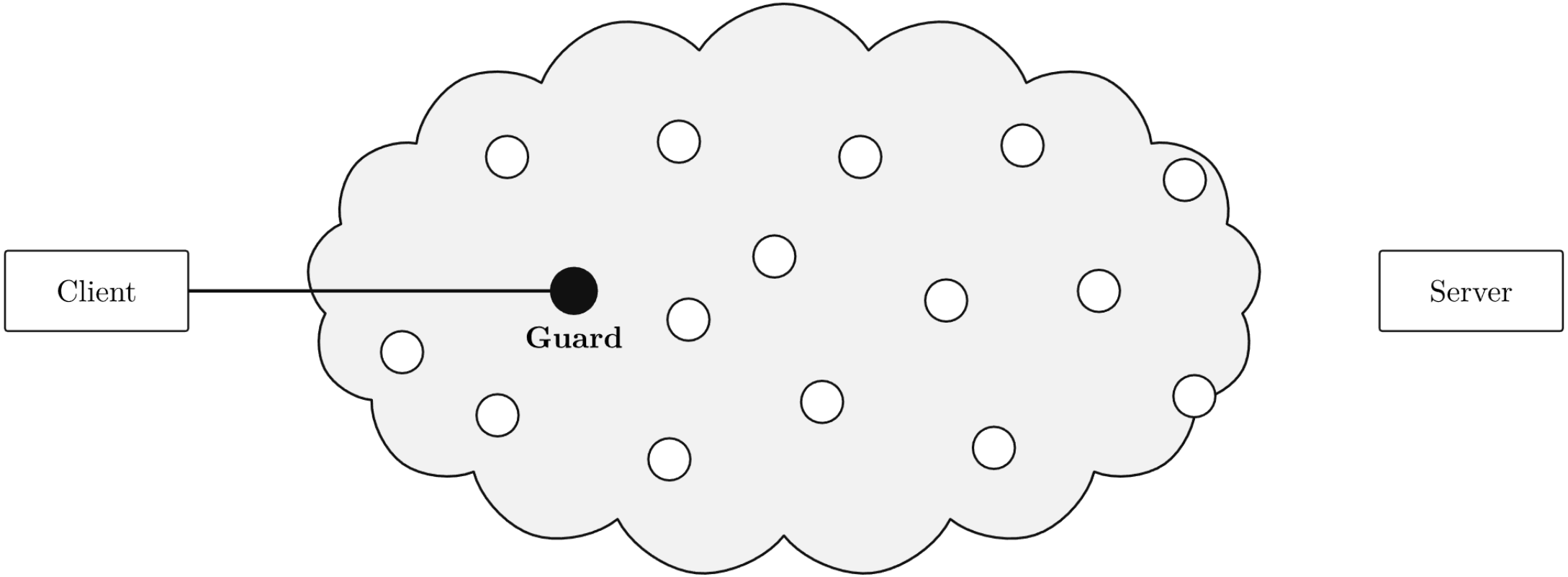
Three relays (Tor circuit)



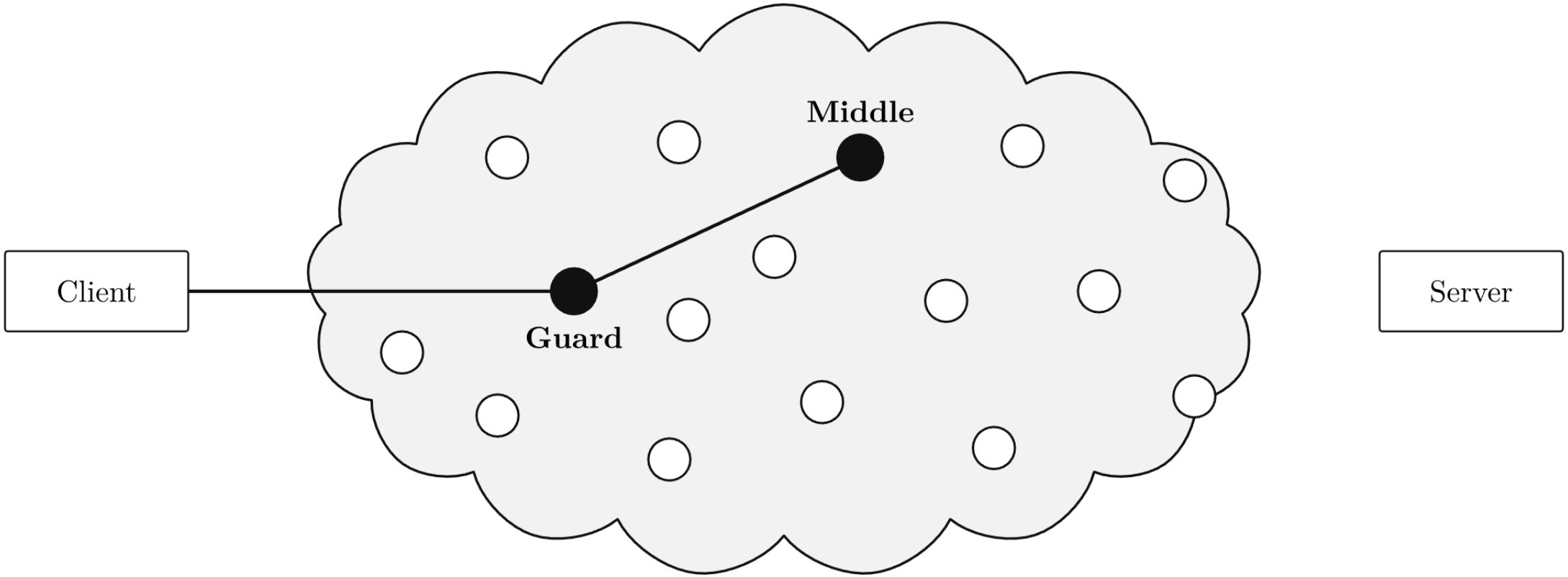
Tor relays



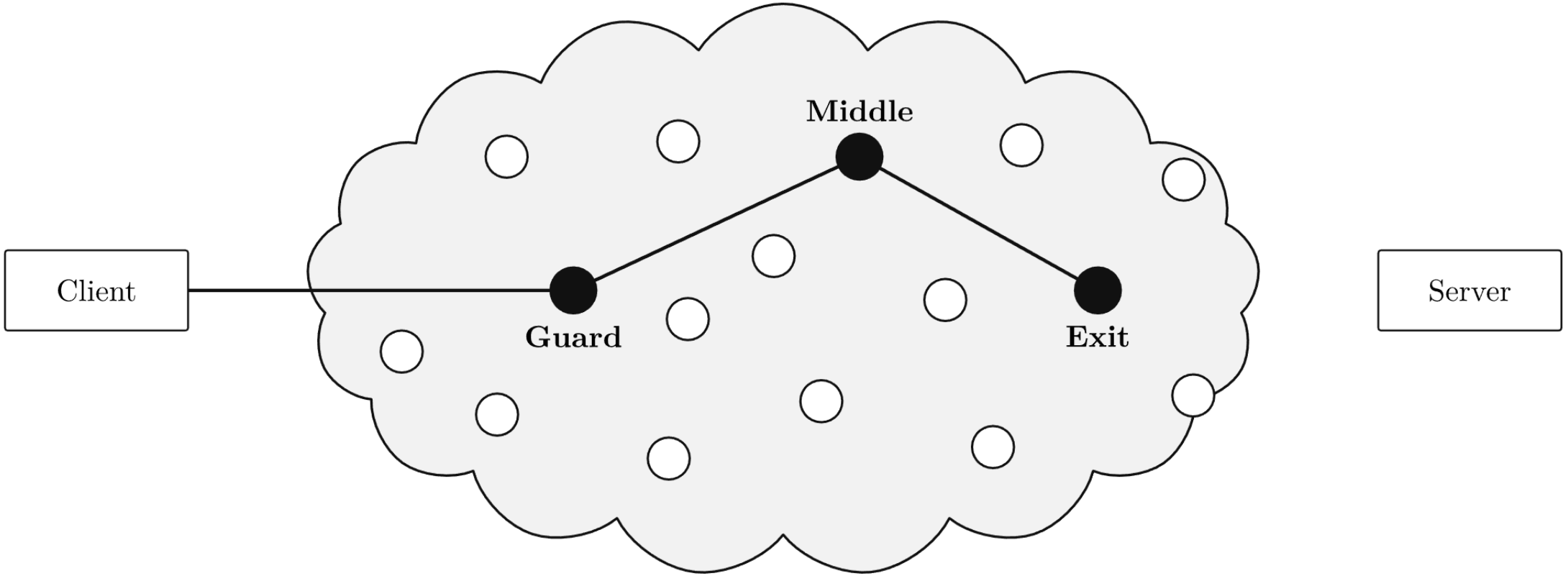
Tor relays



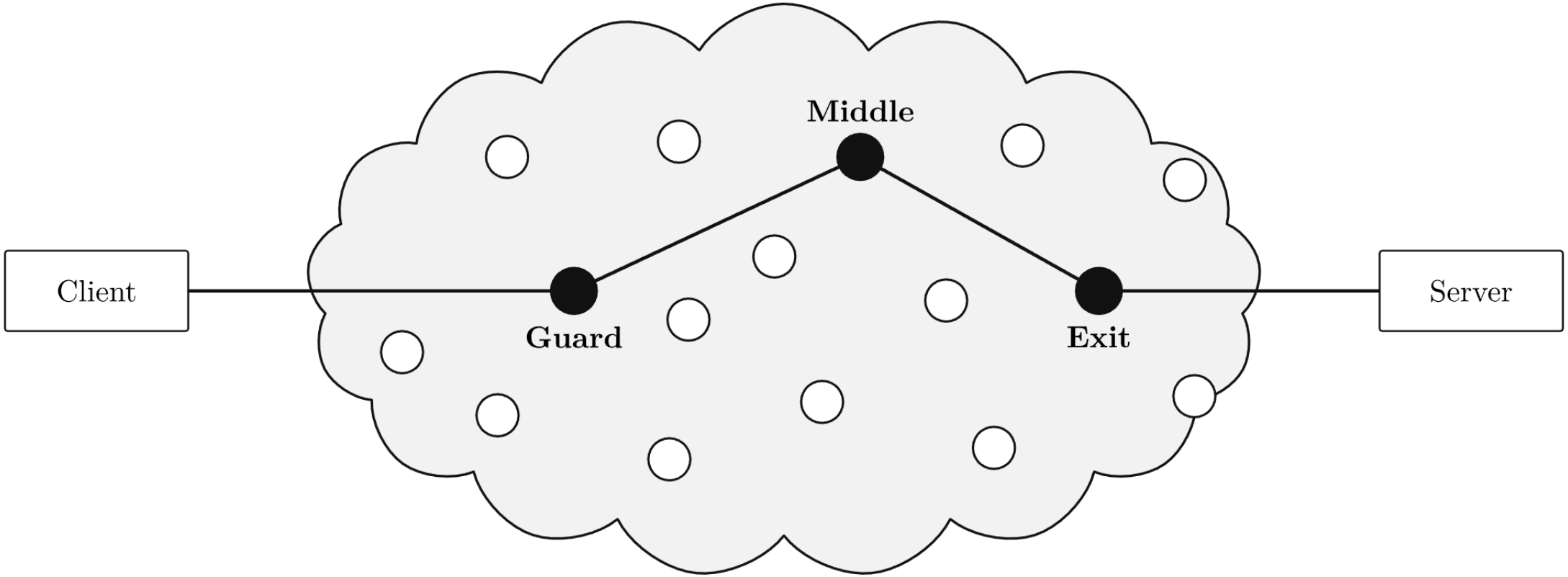
Tor relays



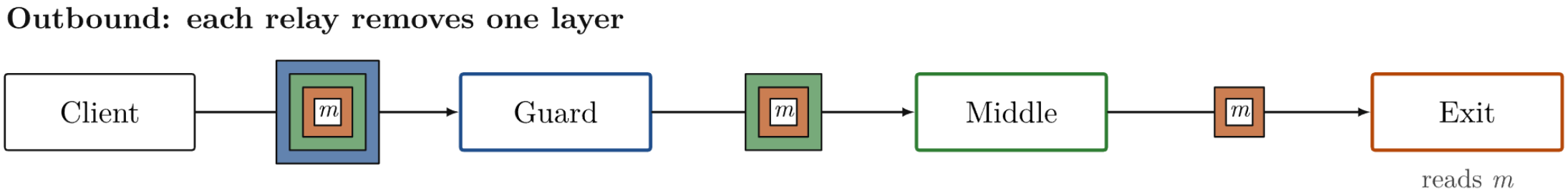
Tor relays



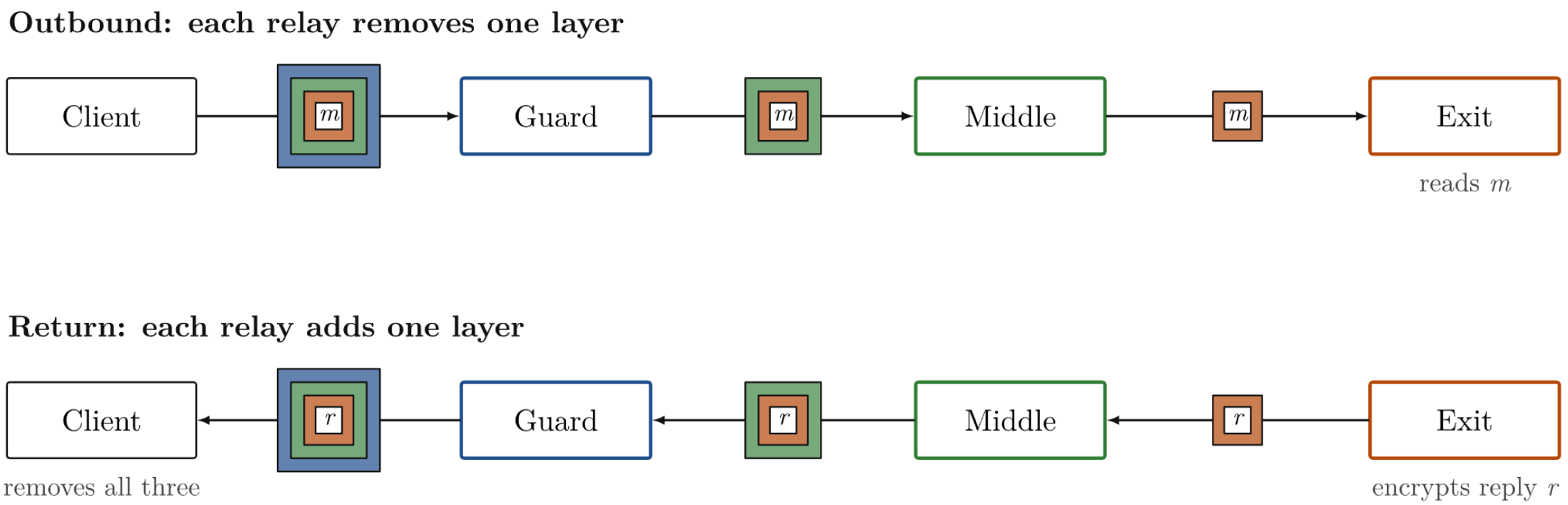
Tor relays



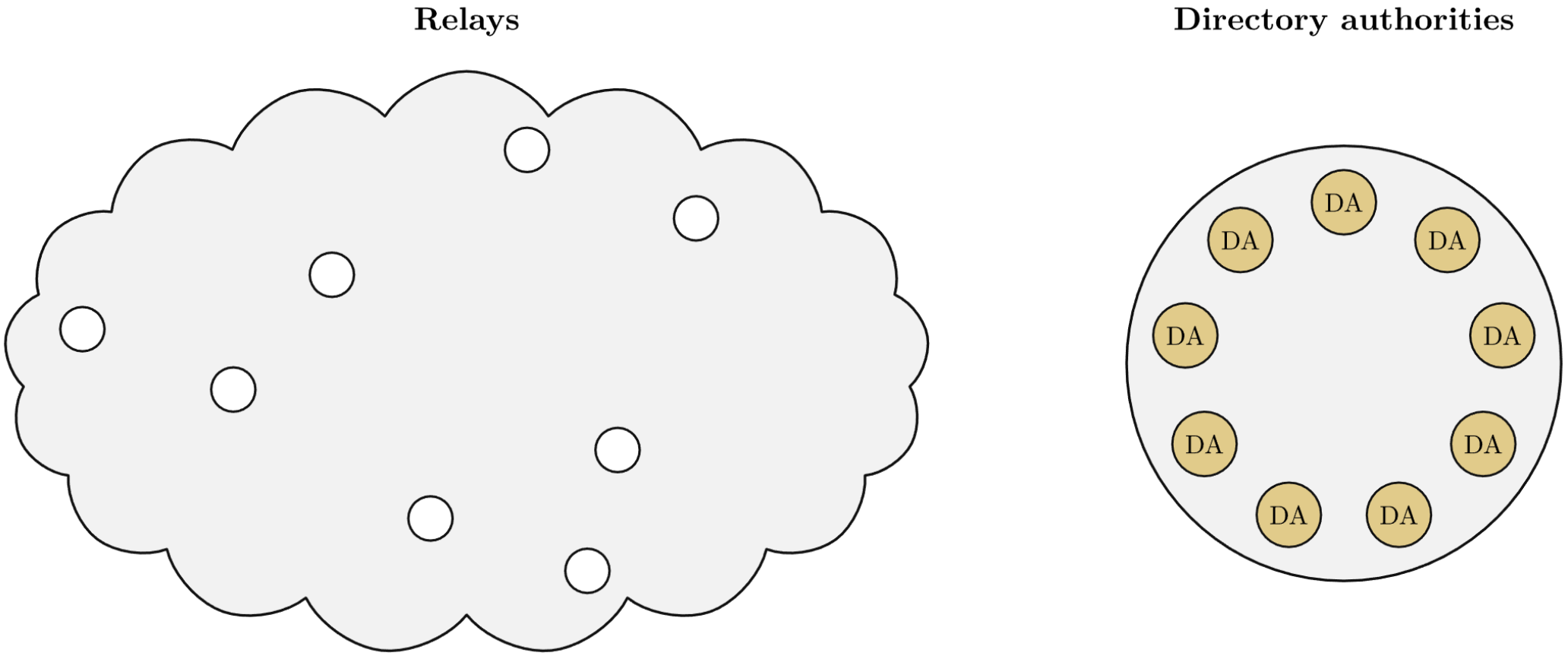
Layered encryption



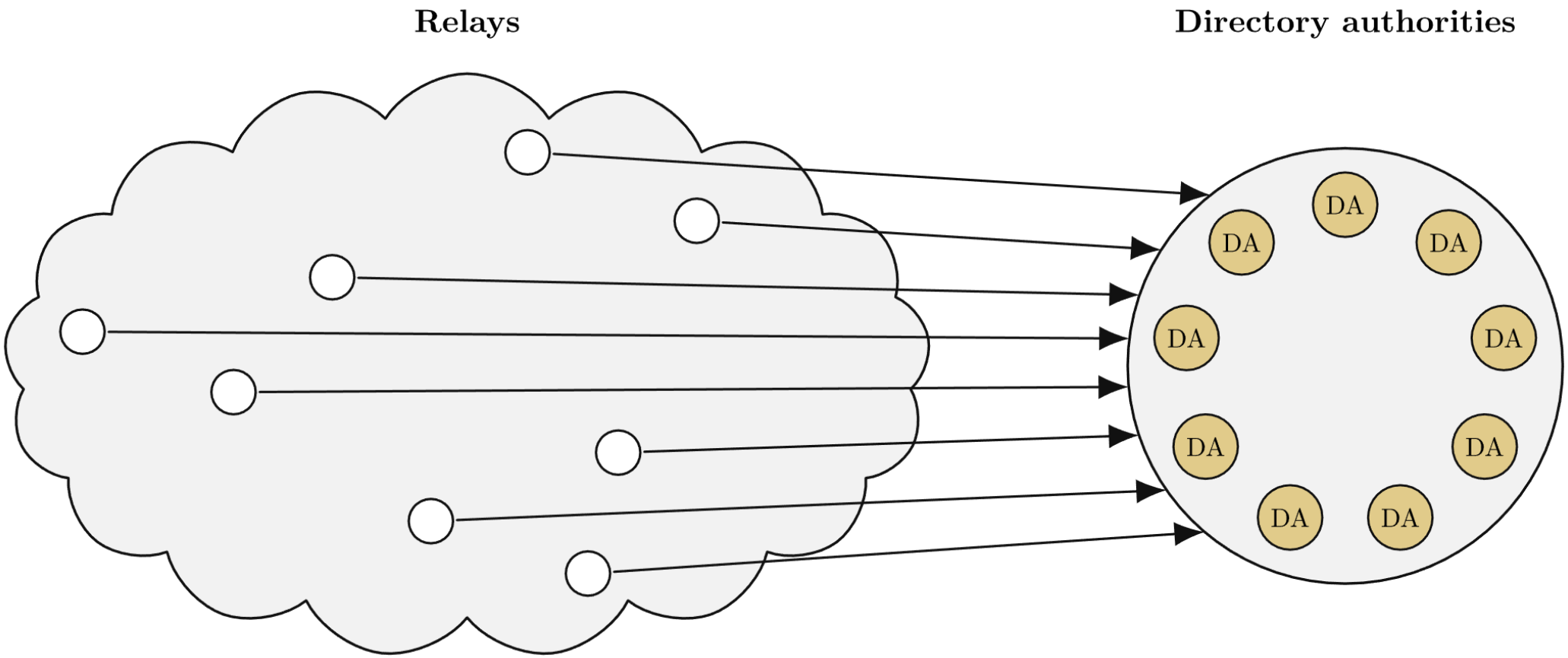
Layered encryption



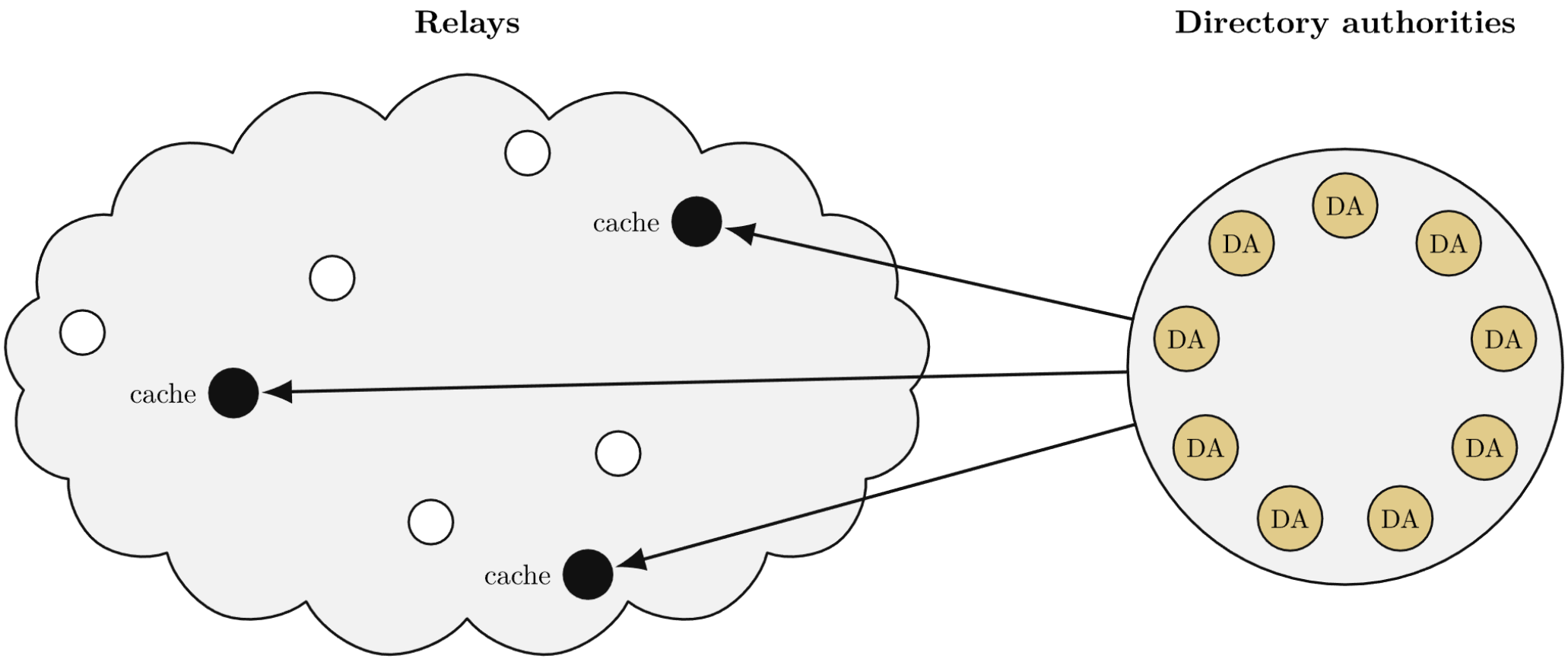
Directory consensus



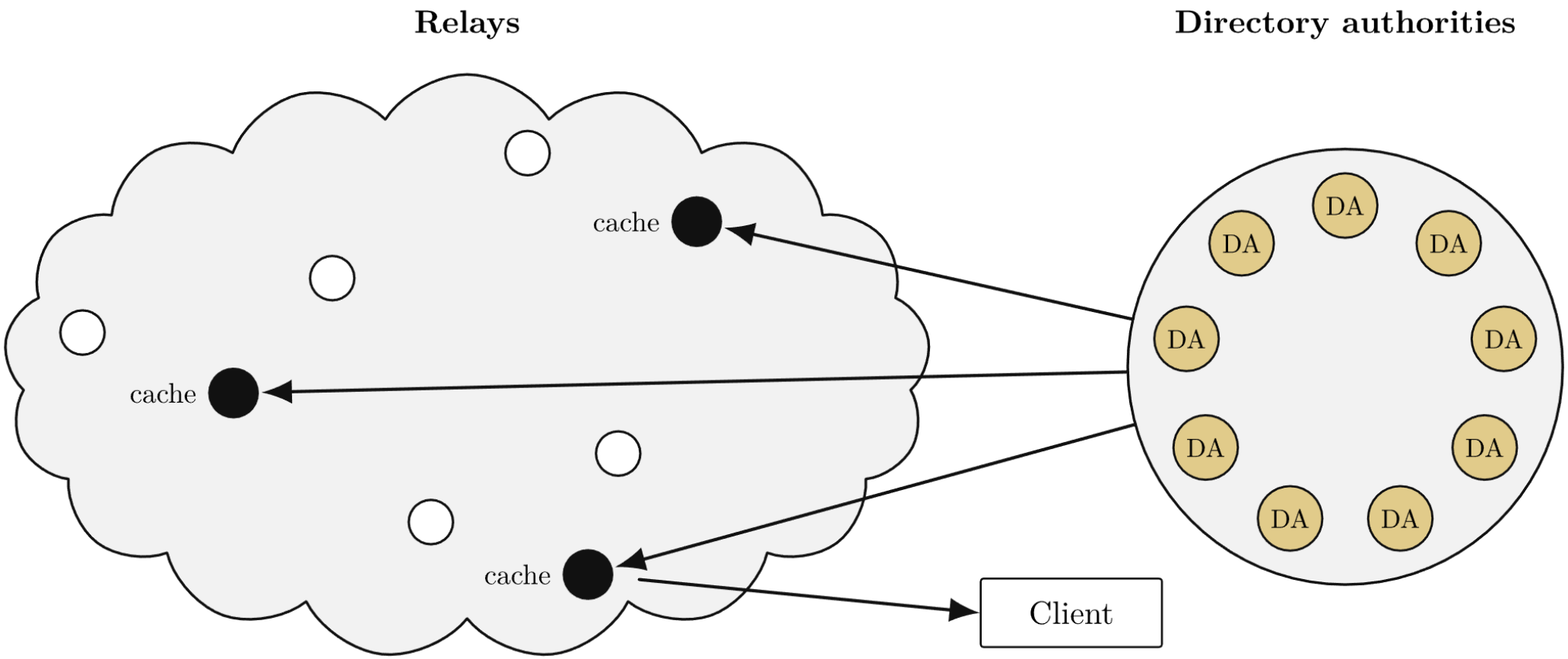
Directory consensus



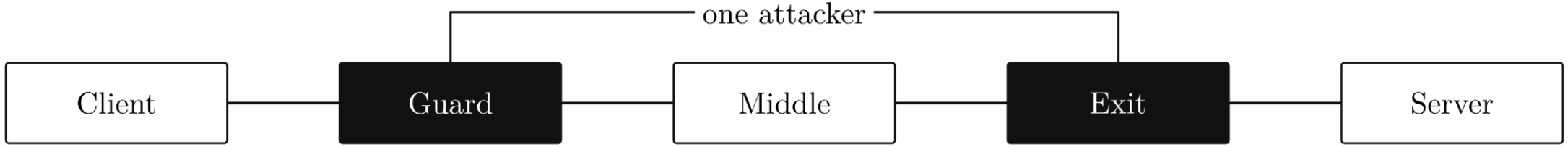
Directory consensus



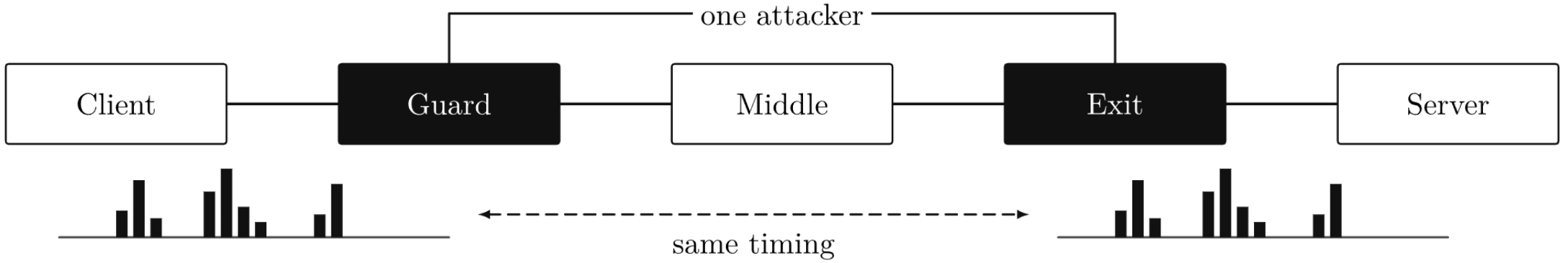
Directory consensus



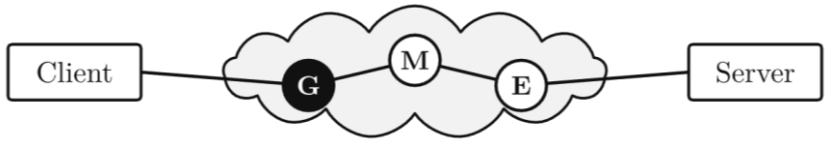
Controlling guard and exit

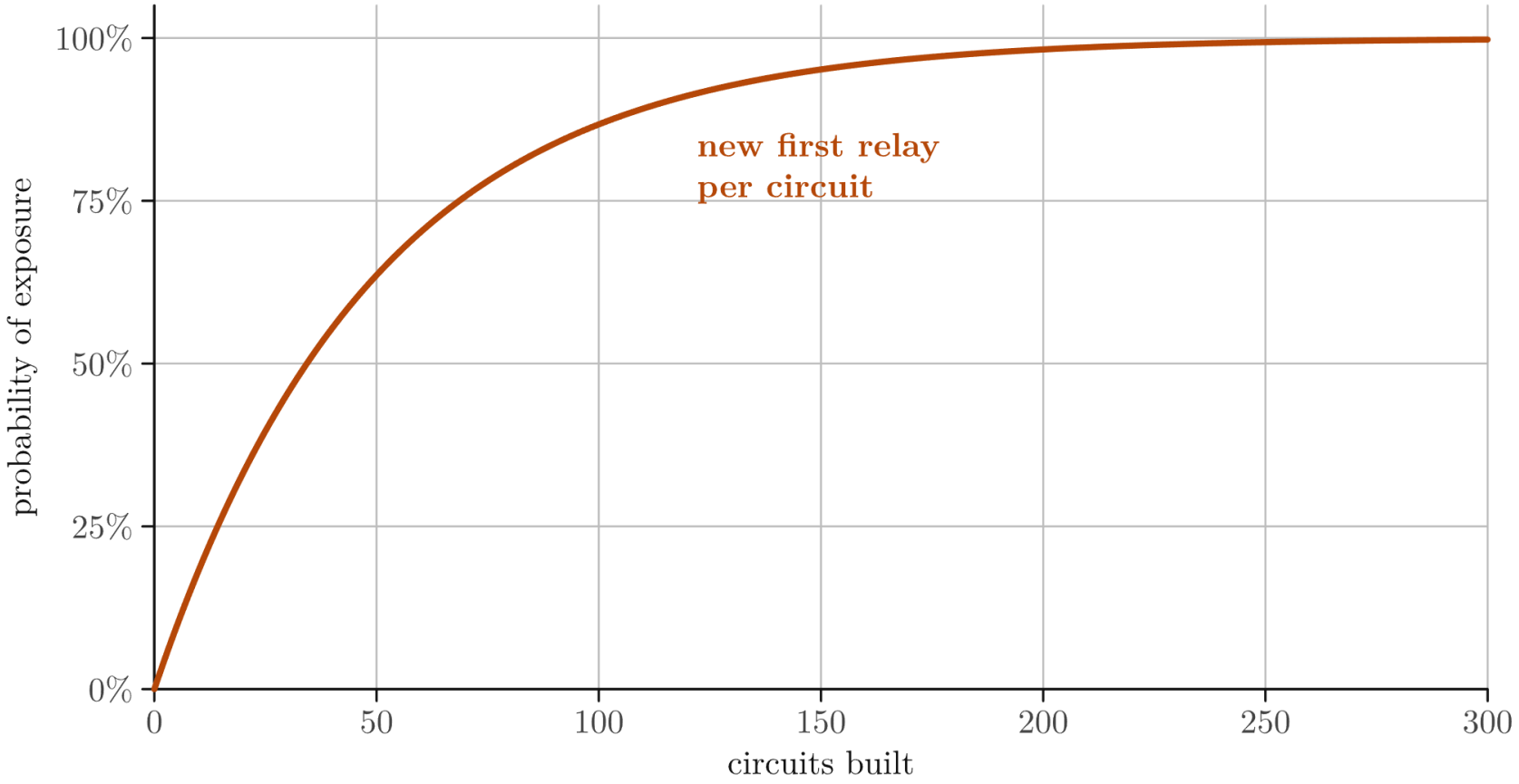


Controlling guard and exit



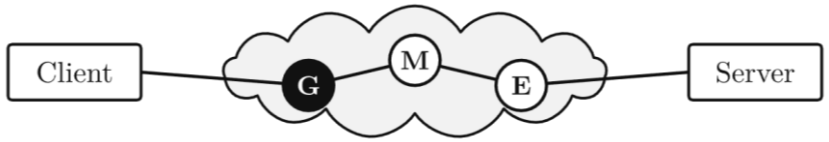
Guard selection

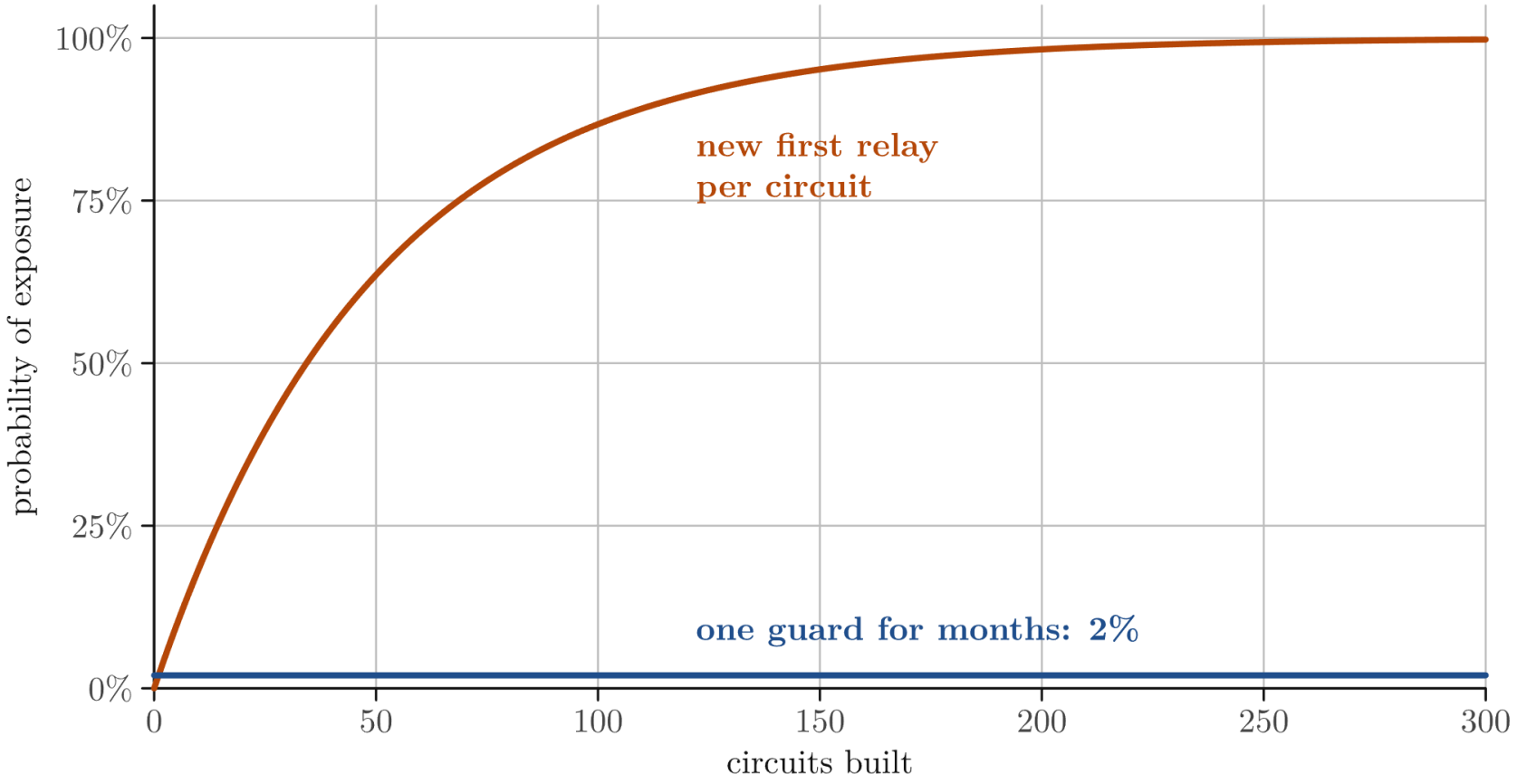




- Model: attacker runs 2% of guard bandwidth

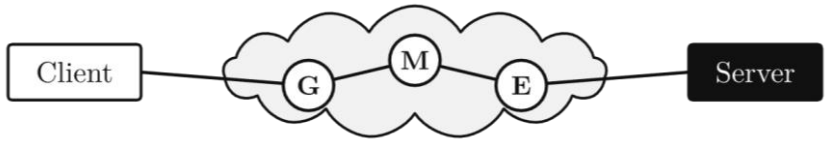
Guard selection





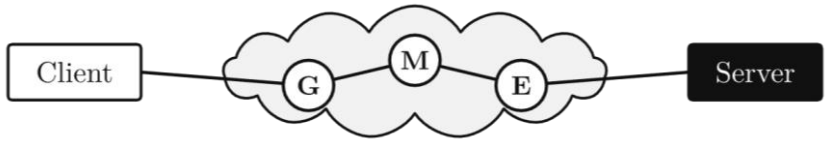
- Model: attacker runs 2% of guard bandwidth
- One guard for months: 98% of users never use a bad guard
- Same total risk, concentrated on fewer users
- Onion services: second hop pinned too (vanguards)

Layers in one packet




```
HTTP GET / HTTP/1.1  Host: google.com
```

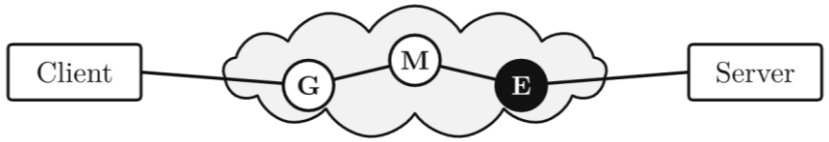
Layers in one packet

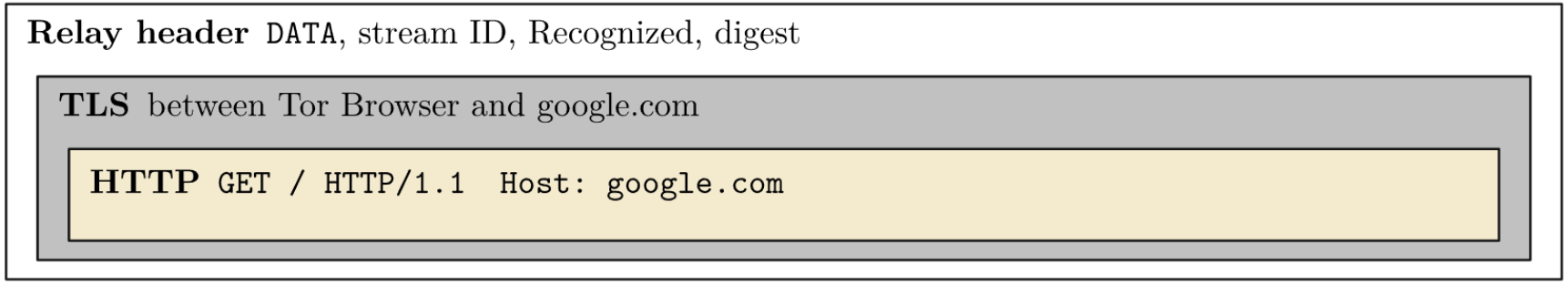


TLS between Tor Browser and google.com

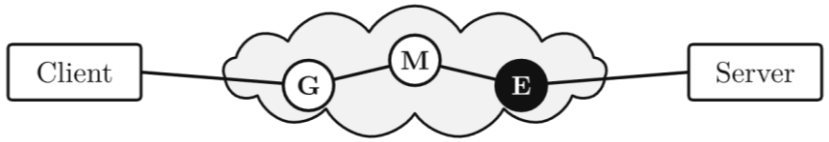
HTTP `GET / HTTP/1.1  Host: google.com`

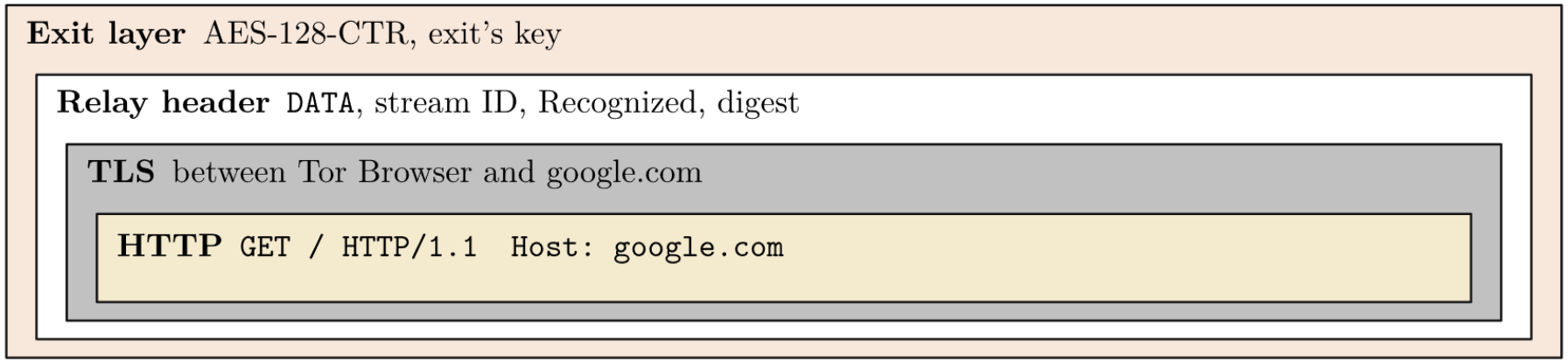
Layers in one packet



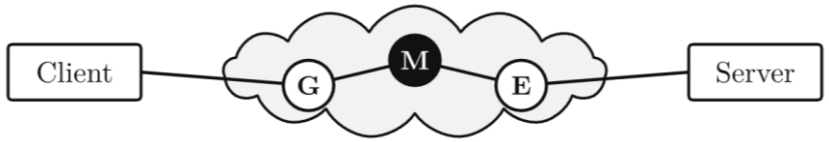


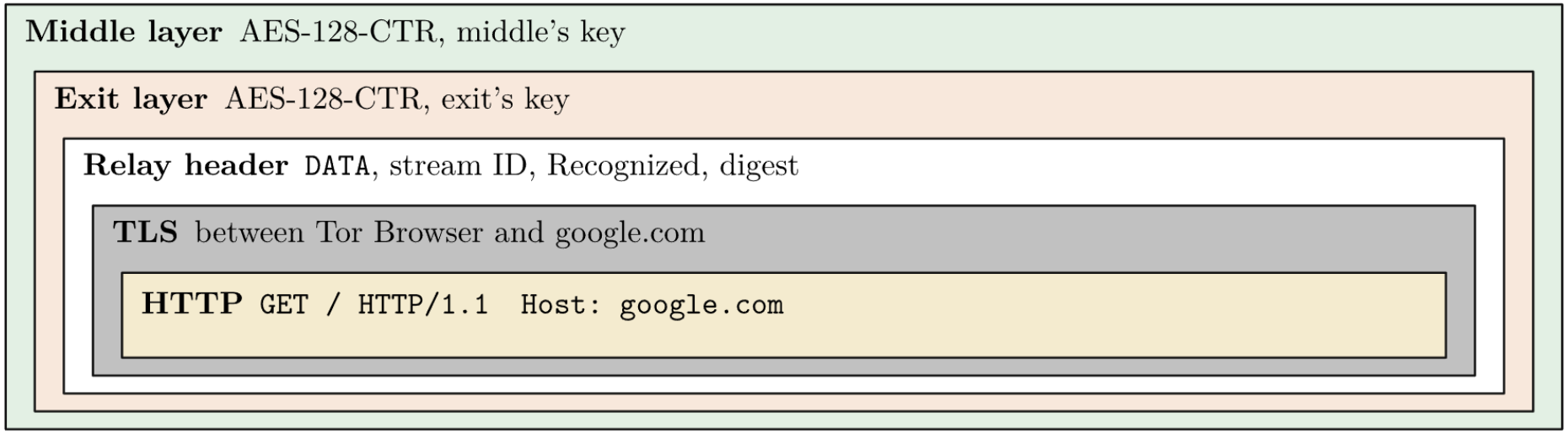
Layers in one packet



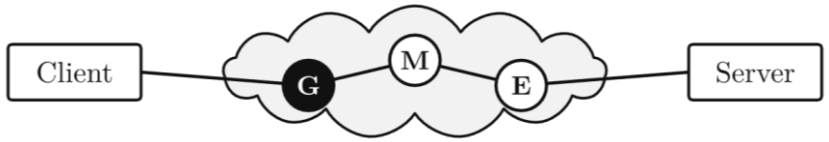


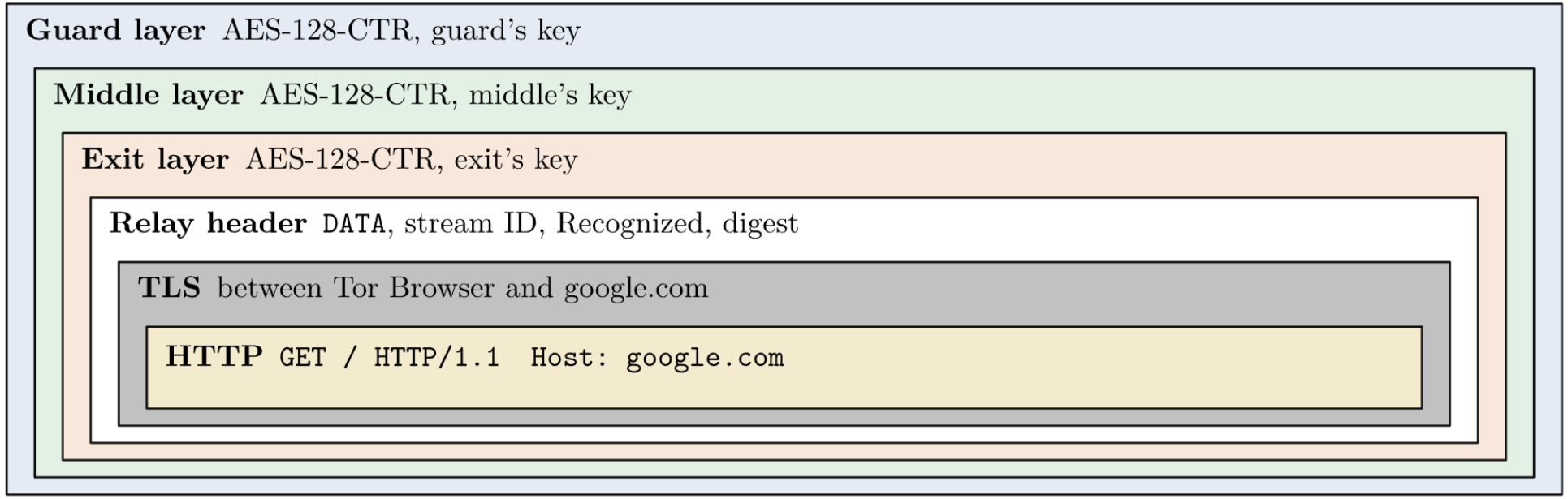
Layers in one packet



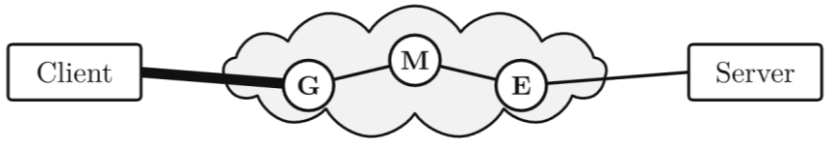


Layers in one packet





Layers in one packet



Cell circuit ID, command `RELAY`

Guard layer AES-128-CTR, guard's key

Middle layer AES-128-CTR, middle's key

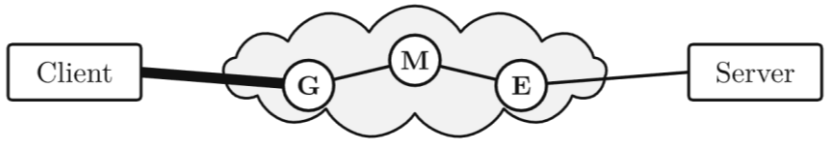
Exit layer AES-128-CTR, exit's key

Relay header `DATA`, stream ID, Recognized, digest

TLS between Tor Browser and google.com

HTTP `GET / HTTP/1.1  Host: google.com`

Layers in one packet



TLS link to the guard

Cell circuit ID, command `RELAY`

Guard layer AES-128-CTR, guard's key

Middle layer AES-128-CTR, middle's key

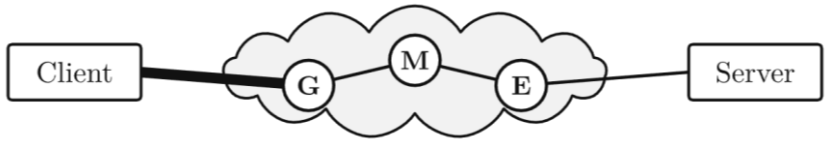
Exit layer AES-128-CTR, exit's key

Relay header `DATA`, stream ID, Recognized, digest

TLS between Tor Browser and google.com

HTTP `GET / HTTP/1.1  Host: google.com`

Layers in one packet



IP + TCP client → guard; the ISP sees only this layer

TLS link to the guard

Cell circuit ID, command `RELAY`

Guard layer AES-128-CTR, guard's key

Middle layer AES-128-CTR, middle's key

Exit layer AES-128-CTR, exit's key

Relay header `DATA`, stream ID, Recognized, digest

TLS between Tor Browser and google.com

HTTP `GET / HTTP/1.1  Host: google.com`

Part II

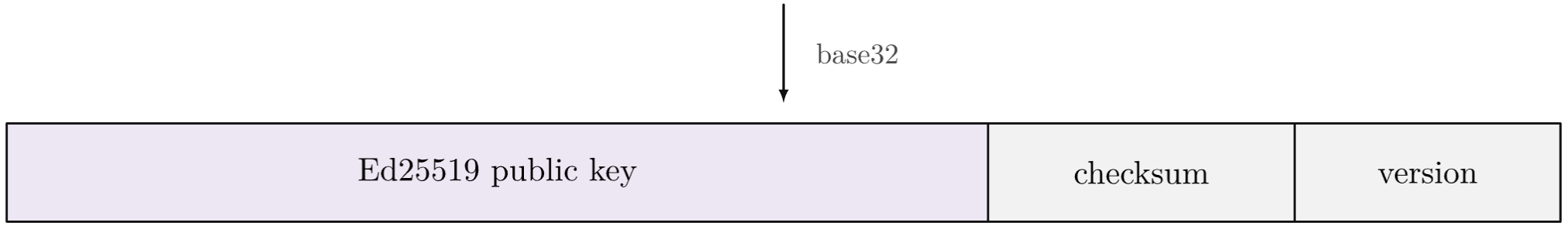
Onion Services

Onion addresses

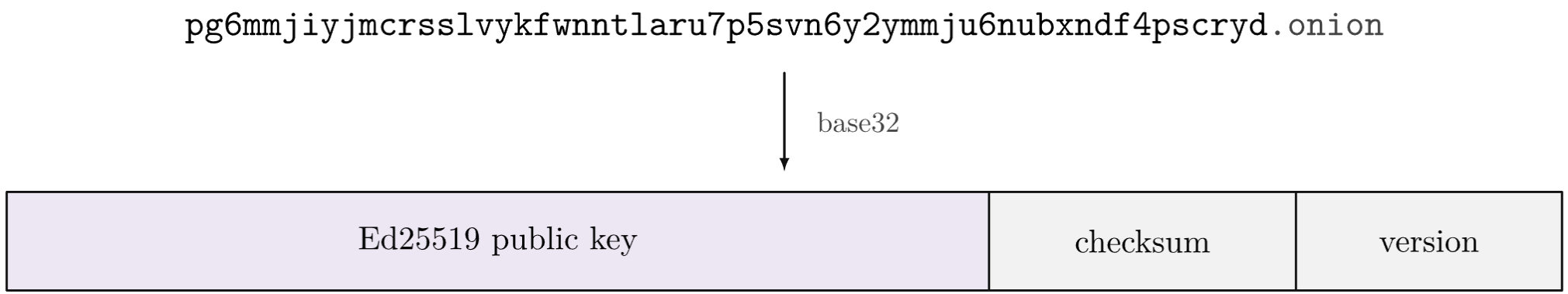
`pg6mmjiyjmcrsslvykfwnntlaru7p5svn6y2ymmju6nubxndf4pscryd.onion`

Onion addresses

`pg6mmjiyjmcrsslvykfwnntlaru7p5svn6y2ymmju6nubxndf4pscryd.onion`



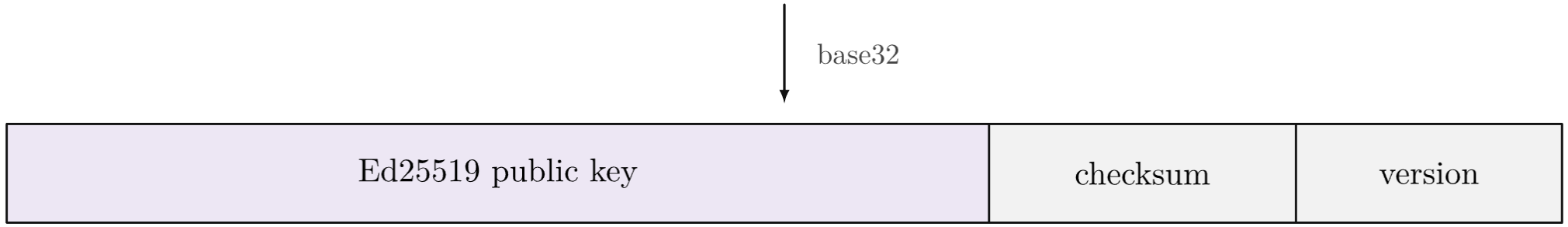
Onion addresses



Self-authenticating

Onion addresses

`pg6mmjiyjmcrsslvykfwnntlaru7p5svn6y2ymmju6nubxndf4pscryd.onion`

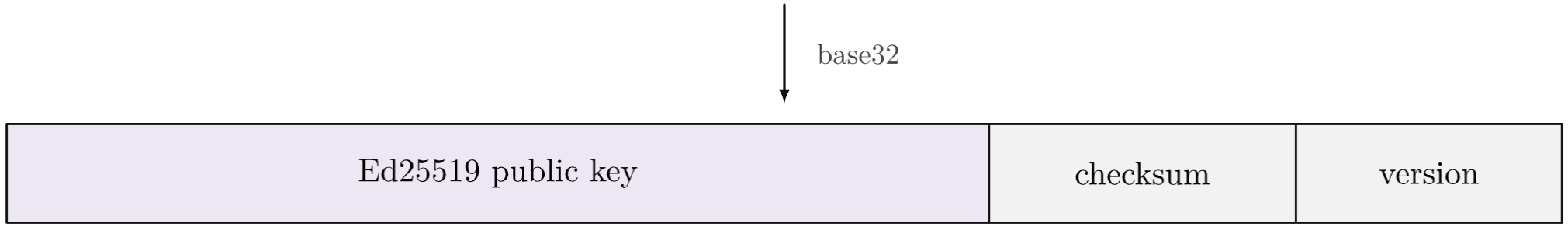


Self-authenticating

Self-issued

Onion addresses

`pg6mmjiyjmcrsslvykfwnntlaru7p5svn6y2ymmju6nubxndf4pscryd.onion`

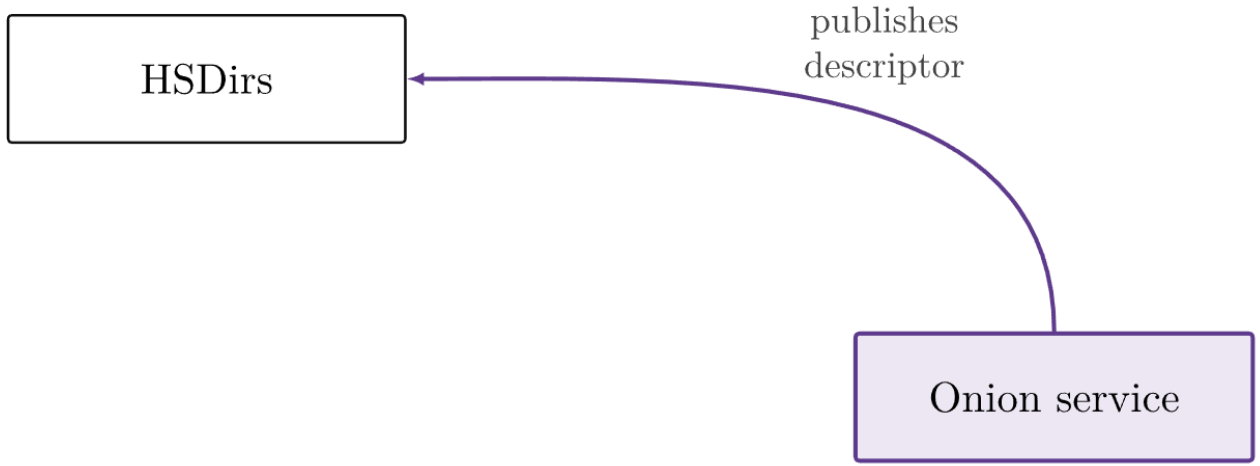


Self-authenticating

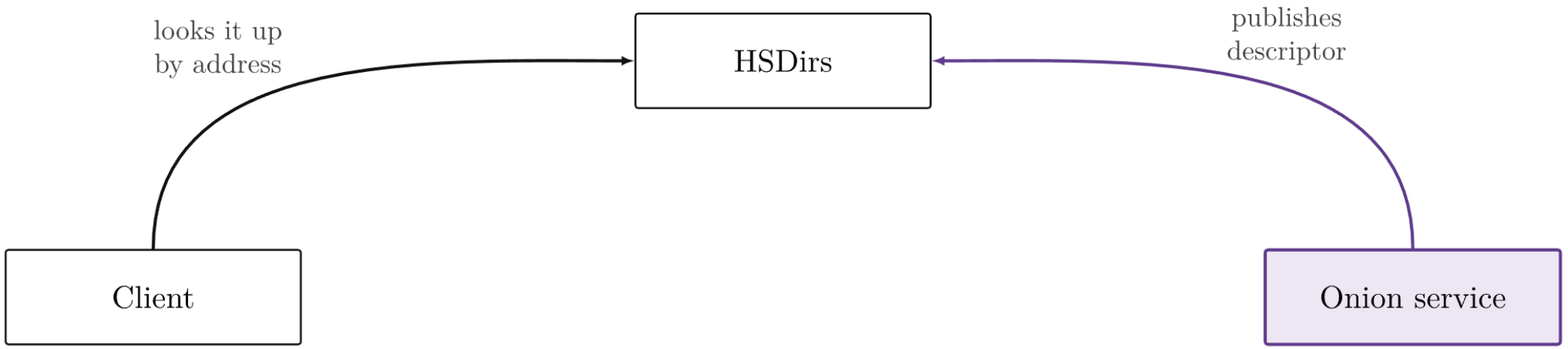
Self-issued

Transferable

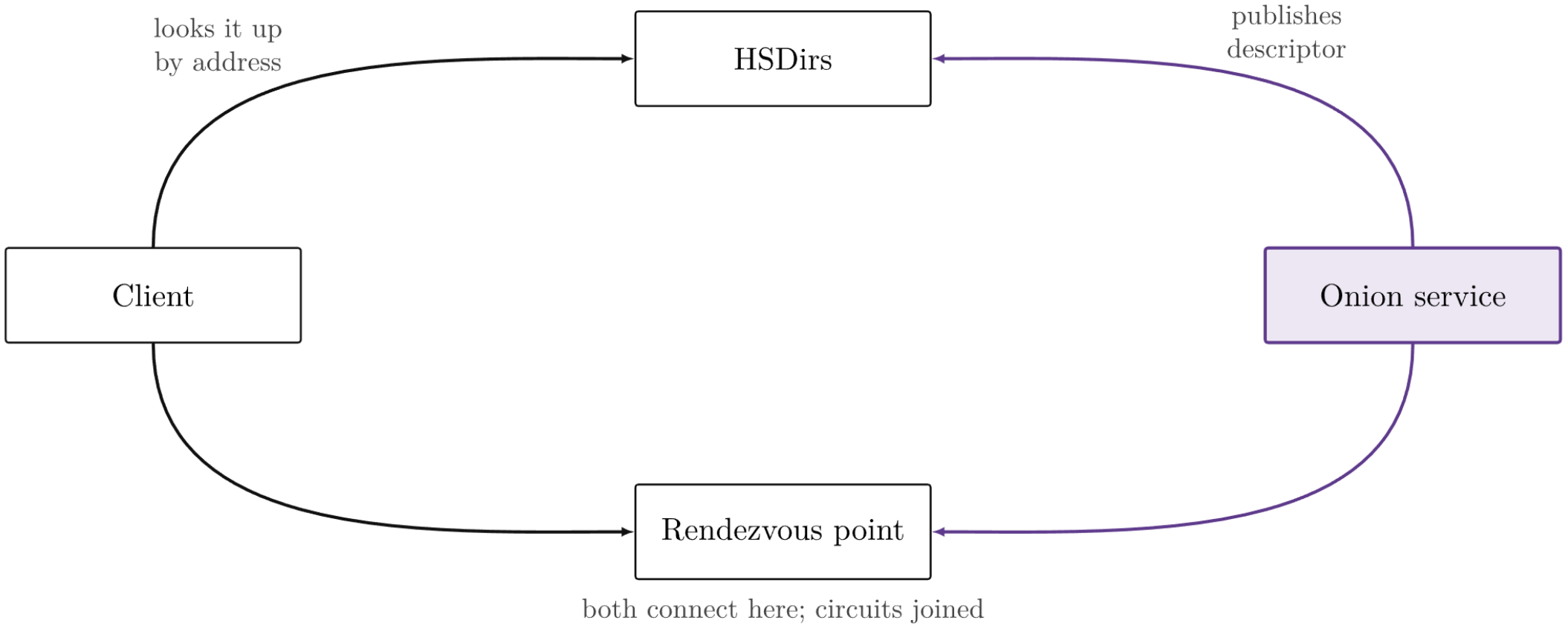
Reaching an onion service



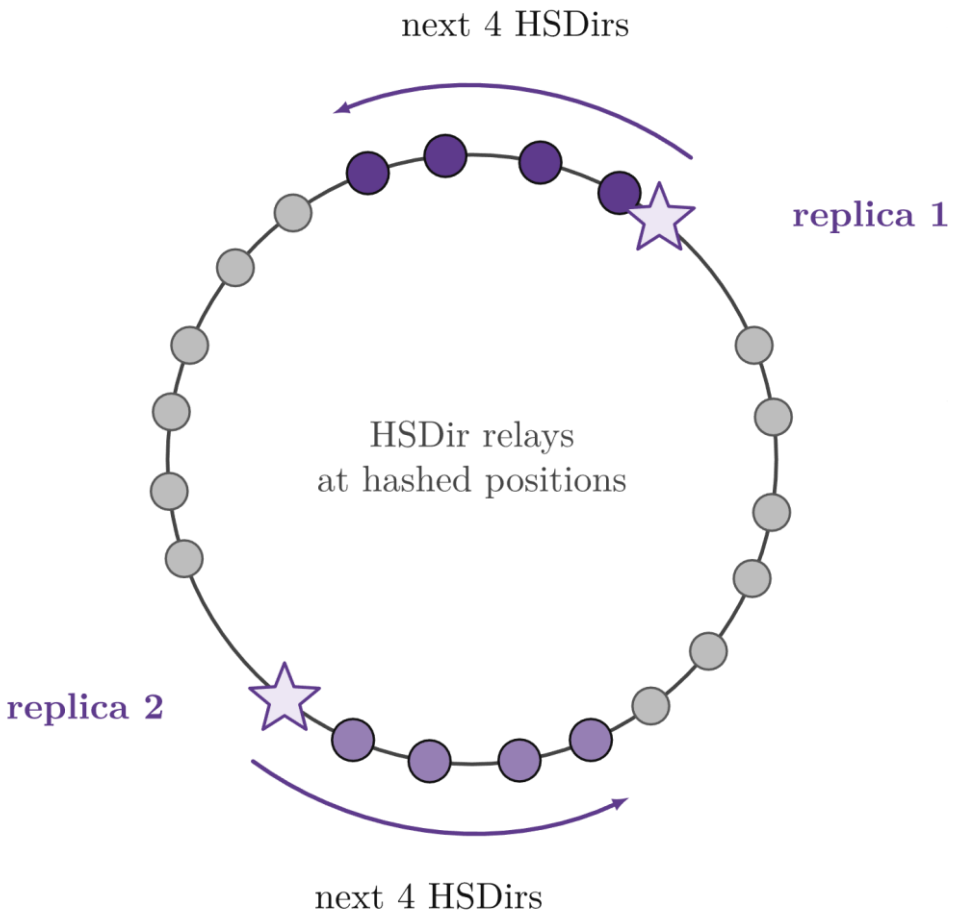
Reaching an onion service



Reaching an onion service



HSDir hash ring

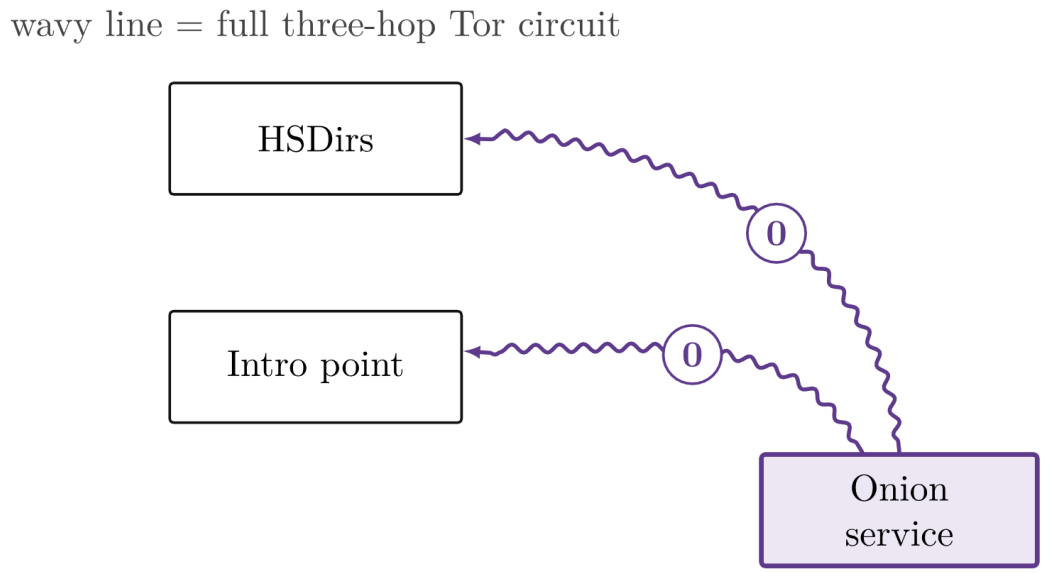


Placement

Redundancy

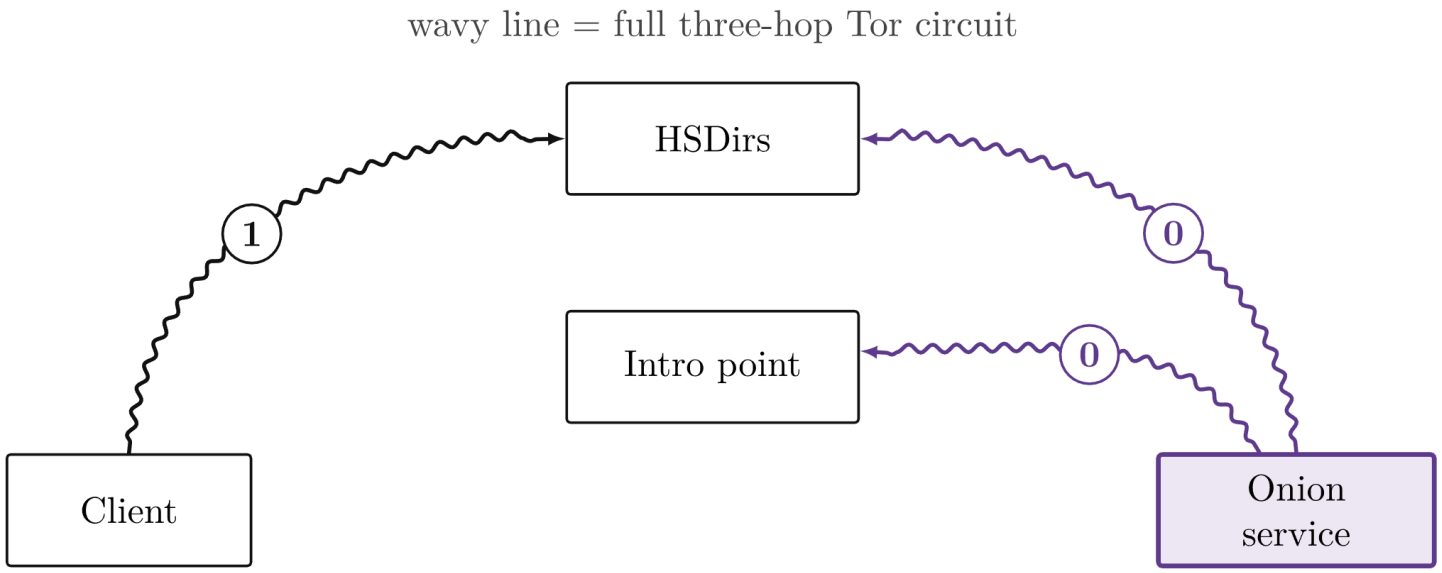
Daily randomness

Rendezvous protocol



0 Service: circuits to 3 intro points, descriptor uploaded

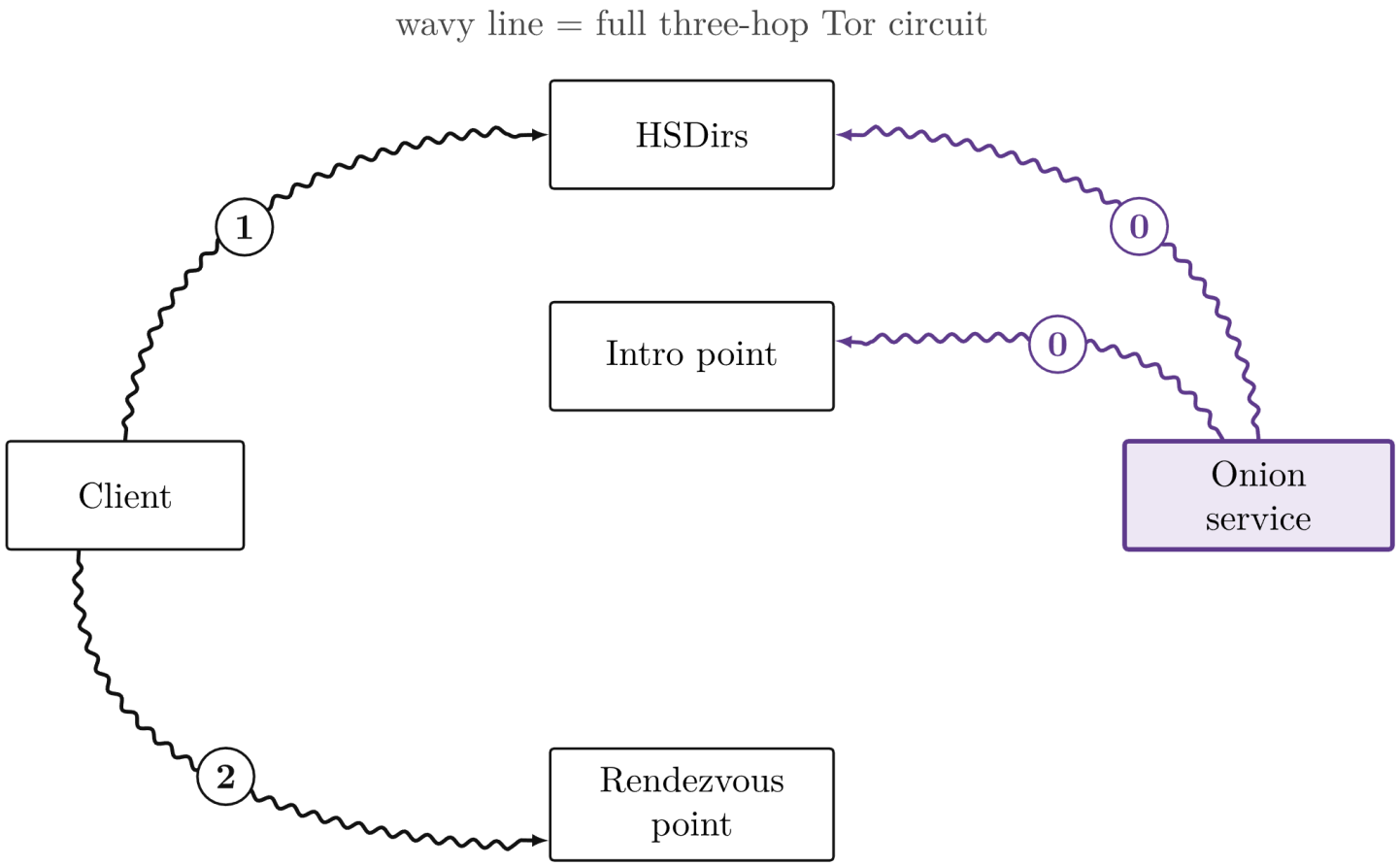
Rendezvous protocol



0 Service: circuits to 3 intro points, descriptor uploaded

1 Client fetches descriptor, decrypts with address

Rendezvous protocol

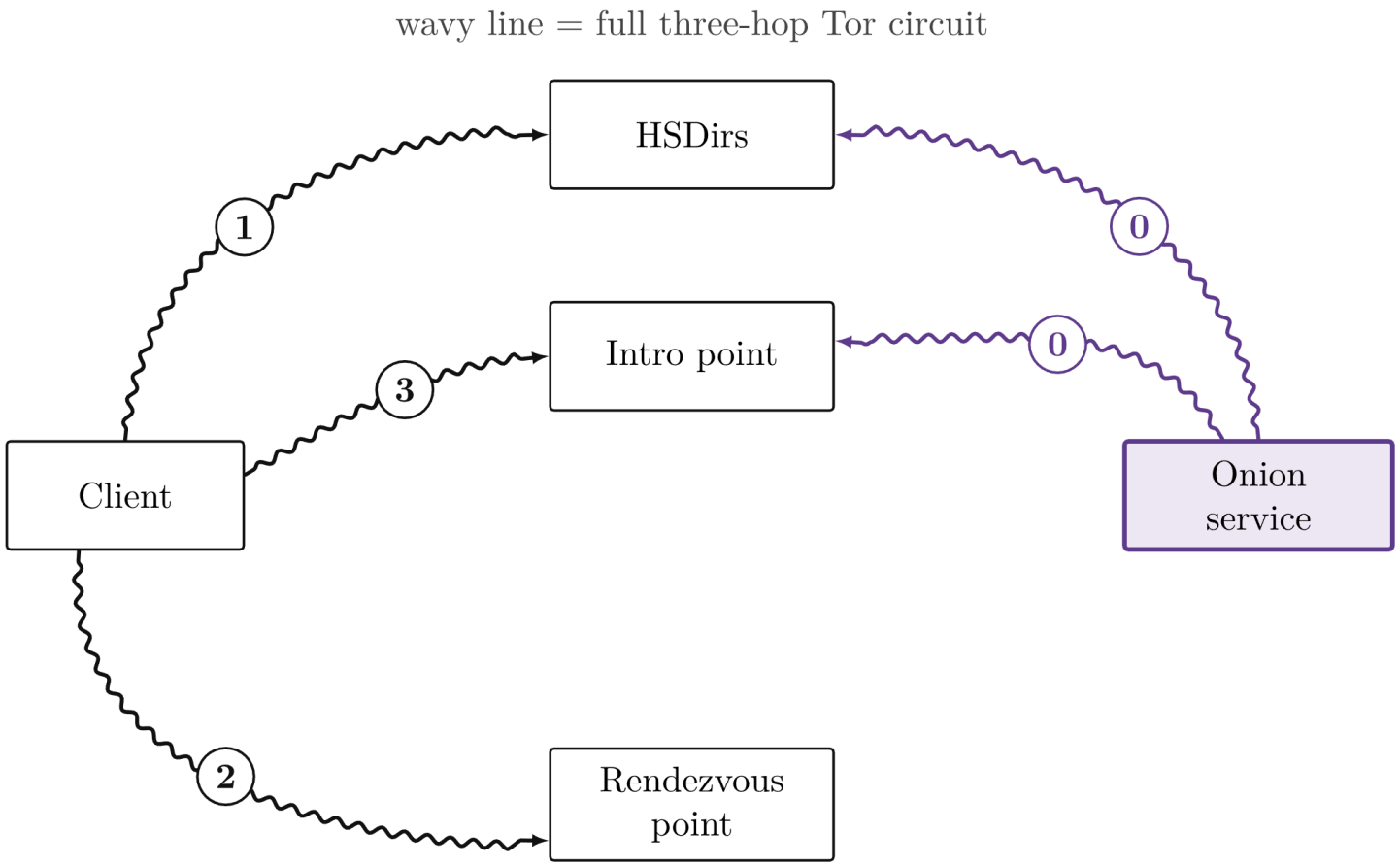


0 Service: circuits to 3 intro points, descriptor uploaded

1 Client fetches descriptor, decrypts with address

2 Client picks rendezvous point, leaves random cookie

Rendezvous protocol



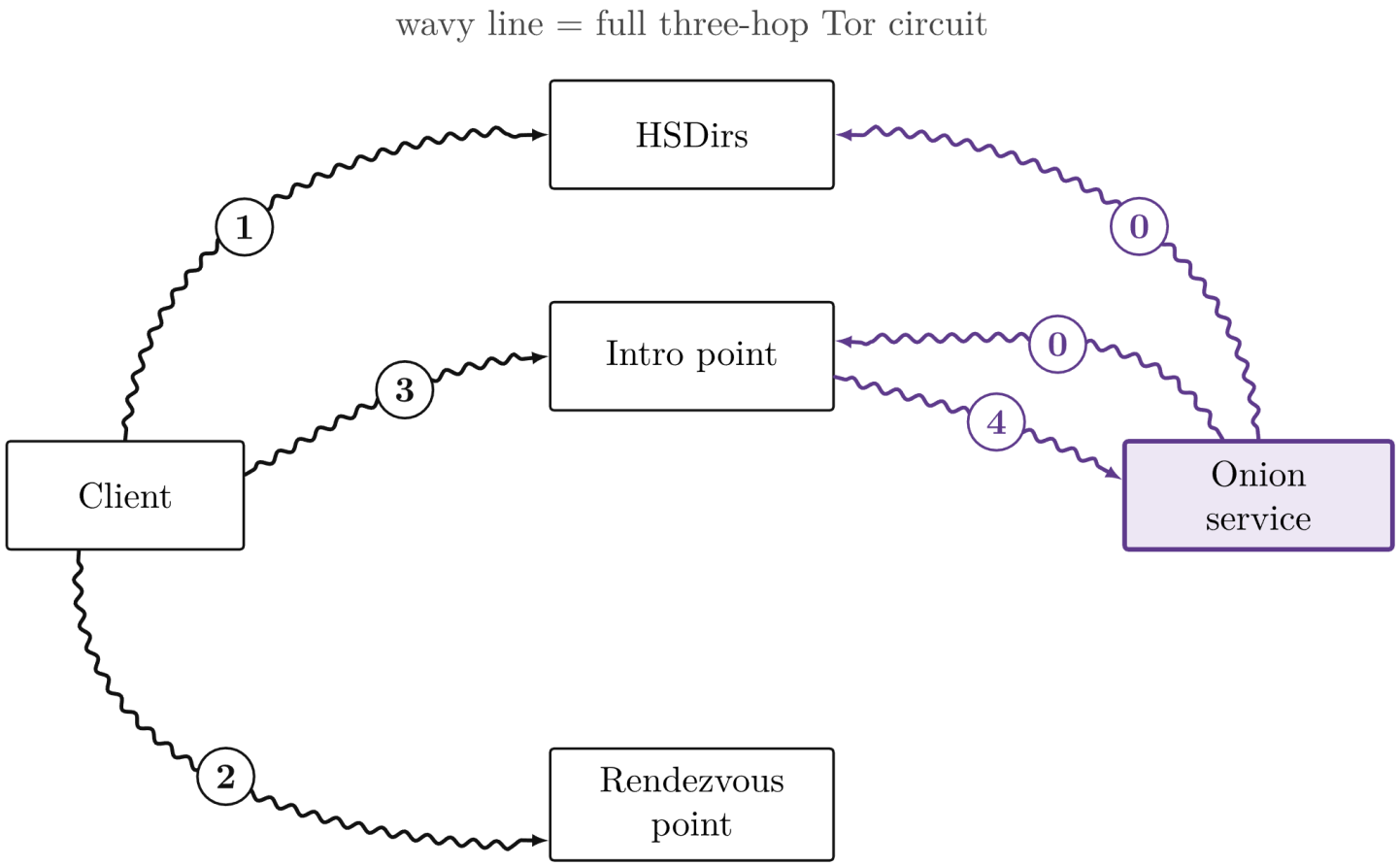
0 Service: circuits to 3 intro points, descriptor uploaded

1 Client fetches descriptor, decrypts with address

2 Client picks rendezvous point, leaves random cookie

3 INTRODUCE1 via intro point: cookie + rendezvous point, encrypted to service

Rendezvous protocol



0 Service: circuits to 3 intro points, descriptor uploaded

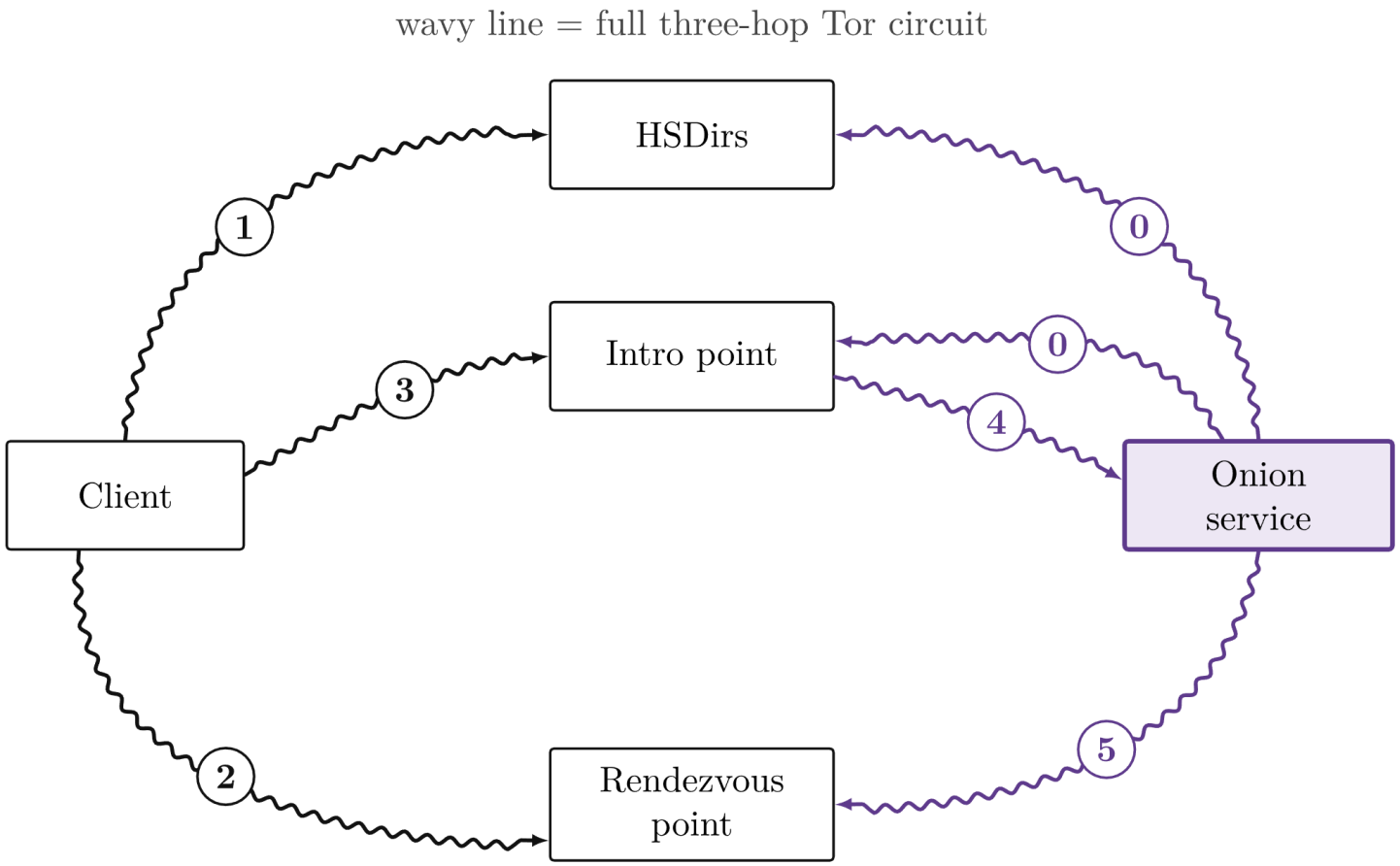
1 Client fetches descriptor, decrypts with address

2 Client picks rendezvous point, leaves random cookie

3 INTRODUCE1 via intro point: cookie + rendezvous point, encrypted to service

4 Intro point forwards it (INTRODUCE2)

Rendezvous protocol



0 Service: circuits to 3 intro points, descriptor uploaded

1 Client fetches descriptor, decrypts with address

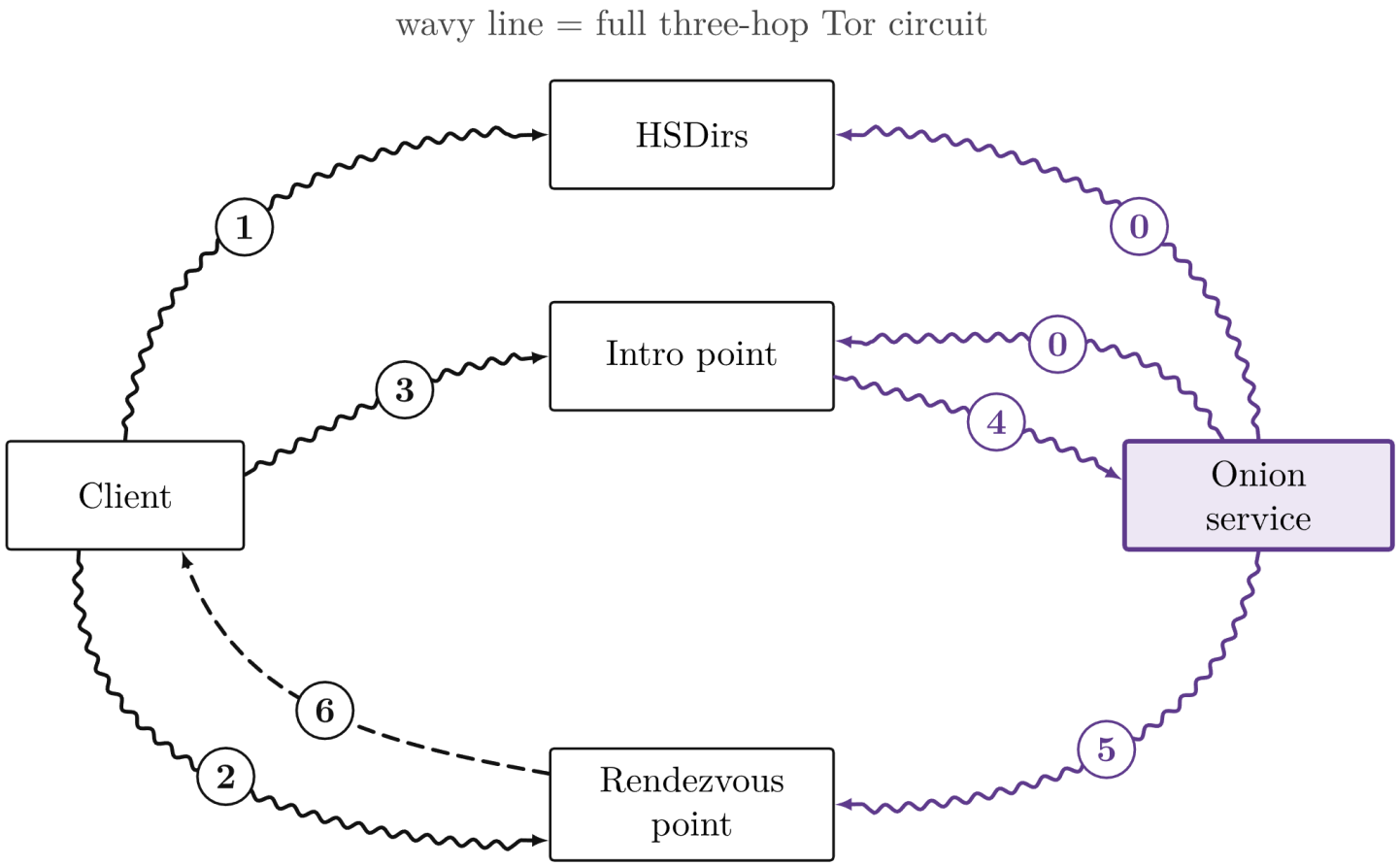
2 Client picks rendezvous point, leaves random cookie

3 INTRODUCE1 via intro point: cookie + rendezvous point, encrypted to service

4 Intro point forwards it (INTRODUCE2)

5 Service builds circuit to rendezvous point

Rendezvous protocol



0 Service: circuits to 3 intro points, descriptor uploaded

1 Client fetches descriptor, decrypts with address

2 Client picks rendezvous point, leaves random cookie

3 INTRODUCE1 via intro point: cookie + rendezvous point, encrypted to service

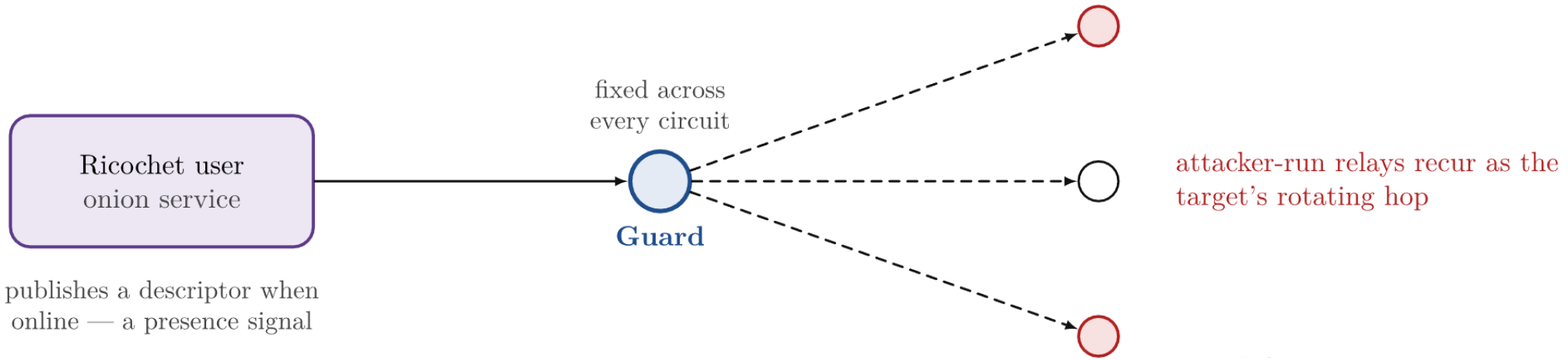
4 Intro point forwards it (INTRODUCE2)

5 Service builds circuit to rendezvous point

6 Rendezvous point joins both circuits

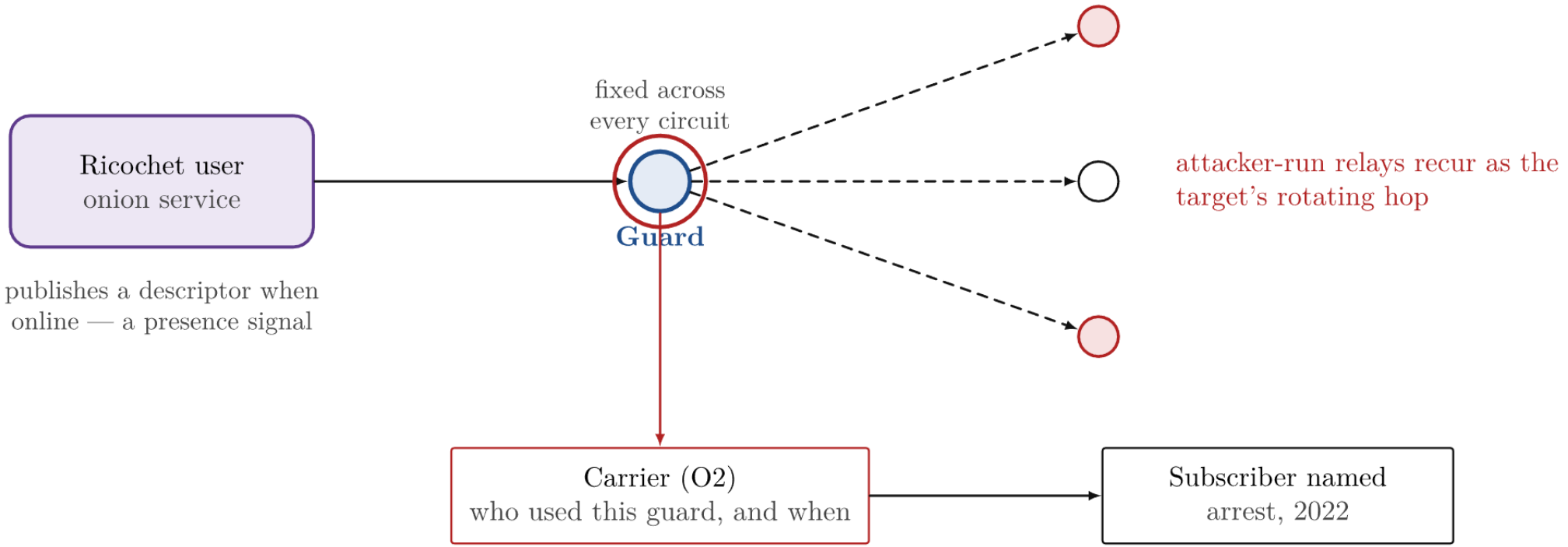
Protocol isn’t bulletproof

Guard discovery attack



NDR Panorama and STRG_F, Sept 2024; Tor Project, "Is Tor still safe to use?", 2024.

Guard discovery attack



NDR Panorama and STRG_F, Sept 2024; Tor Project, "Is Tor still safe to use?", 2024.

KAX17

2017–2021	One operator; relays with no contact info, added in bulk
Scale	Up to ~900 relays at once; mostly guard and middle positions

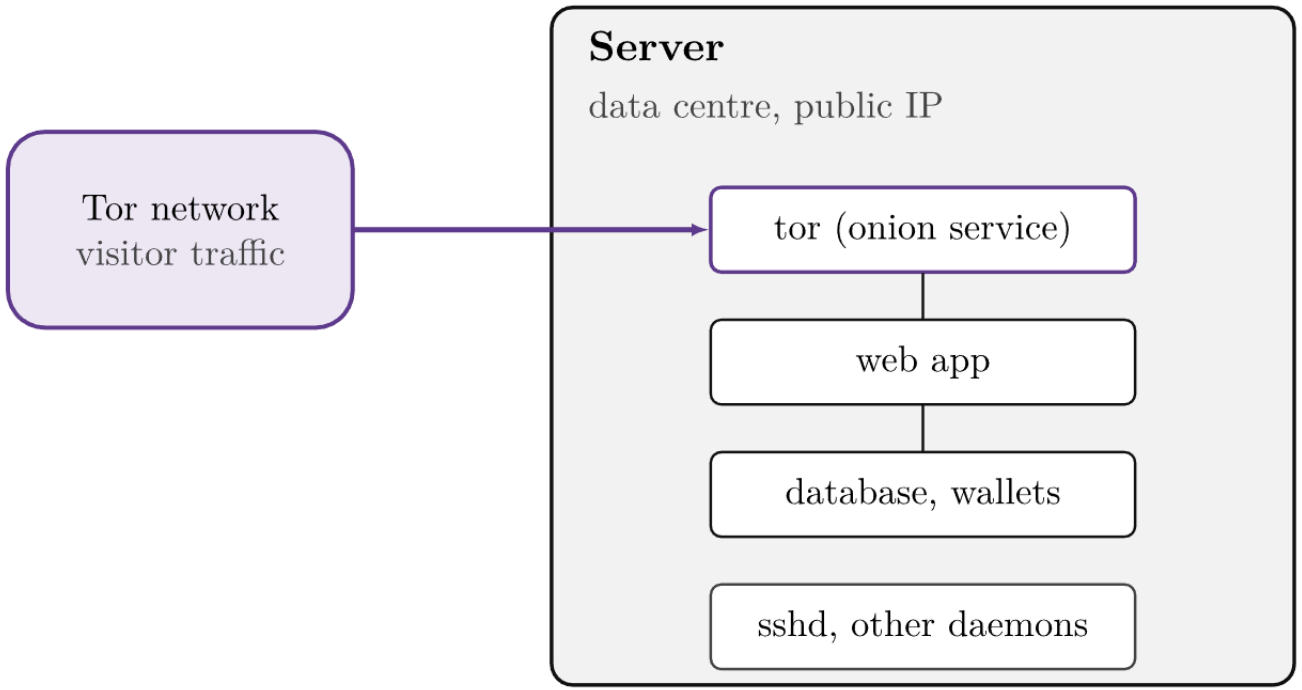
nusenu, 2021; Tor Project relay removals, 8 Nov 2021.

KAX17

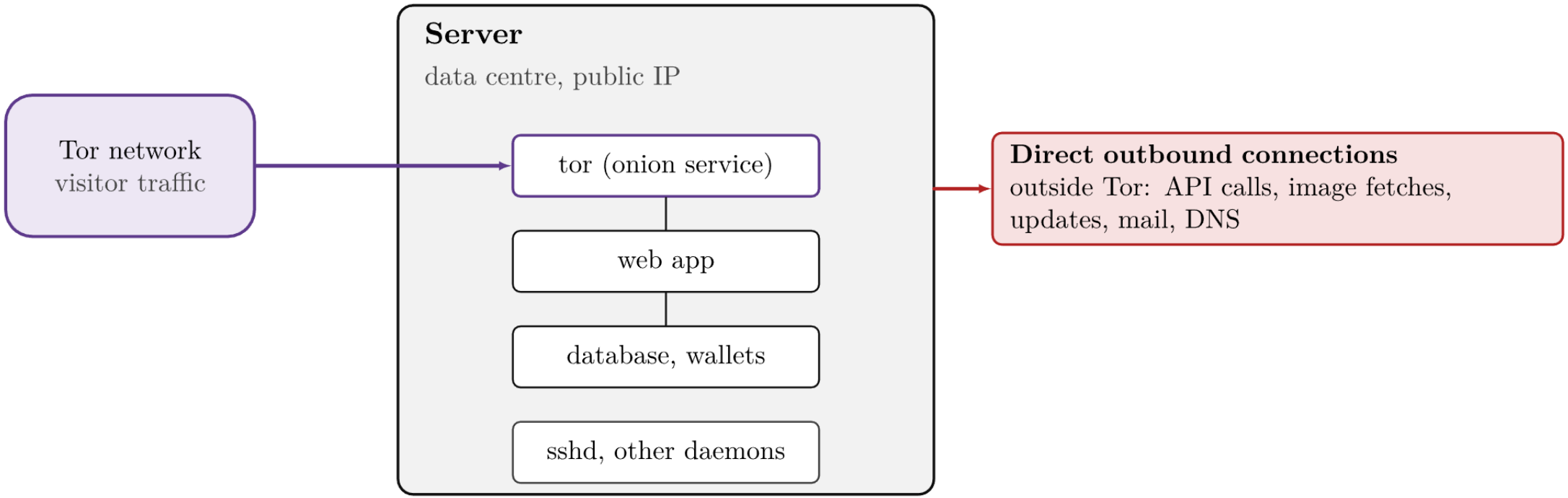
2017–2021	One operator; relays with no contact info, added in bulk
Scale	Up to ~900 relays at once; mostly guard and middle positions
Reach	~16% chance to be a user's guard, ~35% a middle hop
Risk	Position enough for correlation

nusenu, 2021; Tor Project relay removals, 8 Nov 2021.

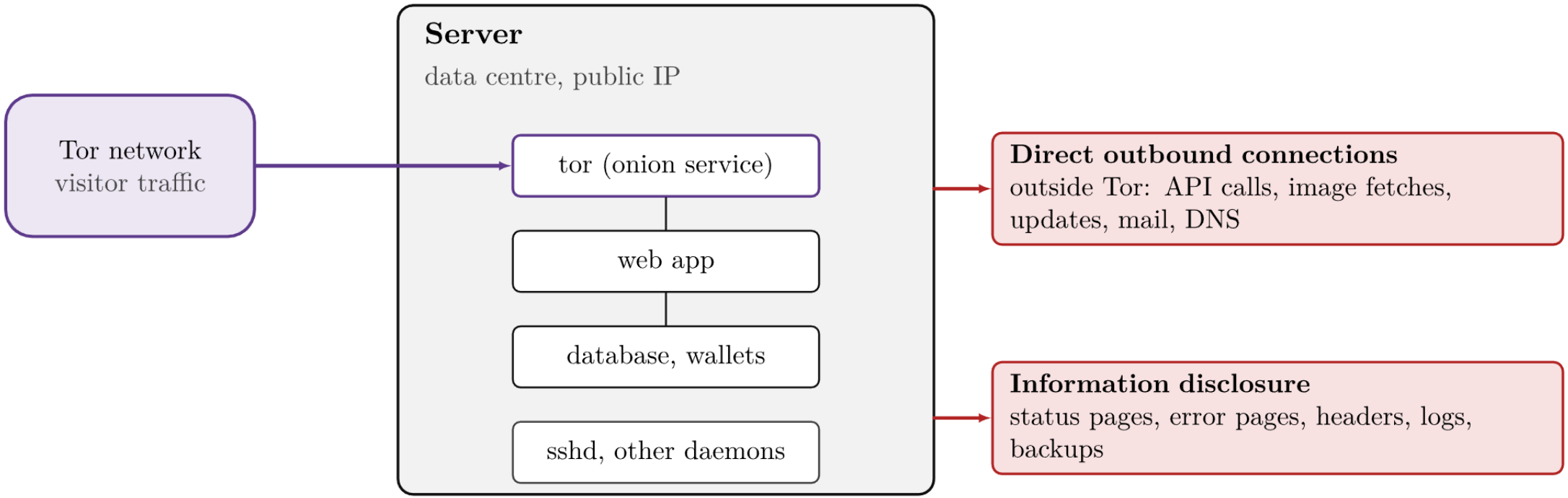
Server-side exposure



Server-side exposure



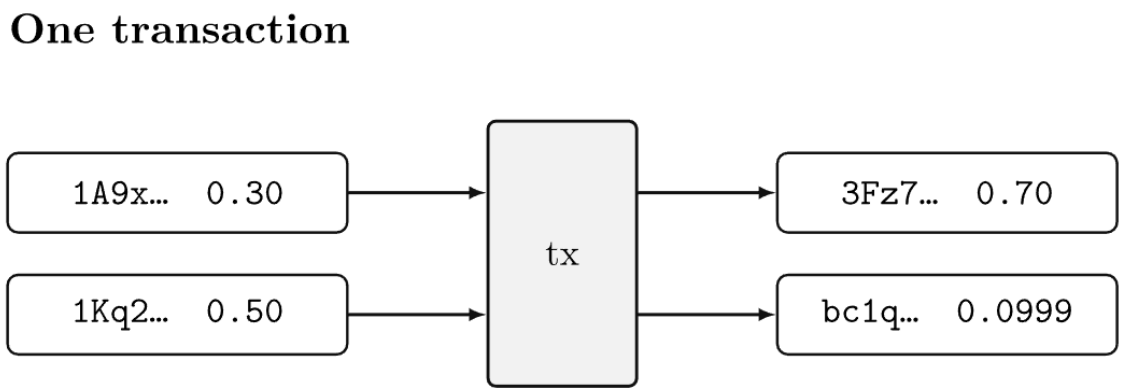
Server-side exposure



Part III

Anonymous Payments

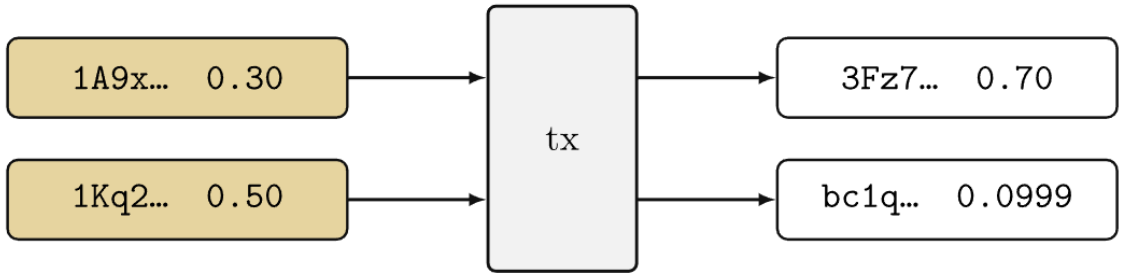
Bitcoin transaction analysis



Meiklejohn et al., “A Fistful of Bitcoins”, IMC 2013.

Bitcoin transaction analysis

Clustering heuristics

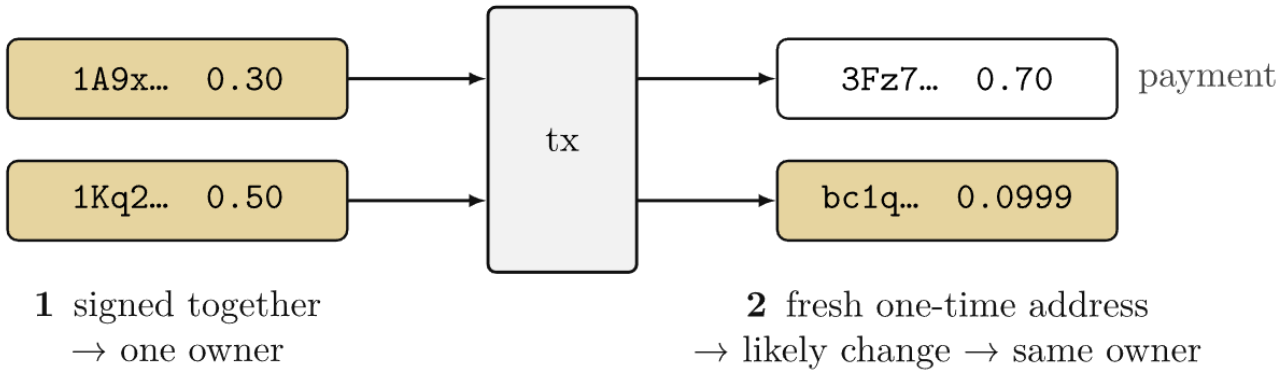


1 signed together
→ one owner

Meiklejohn et al., "A Fistful of Bitcoins", IMC 2013.

Bitcoin transaction analysis

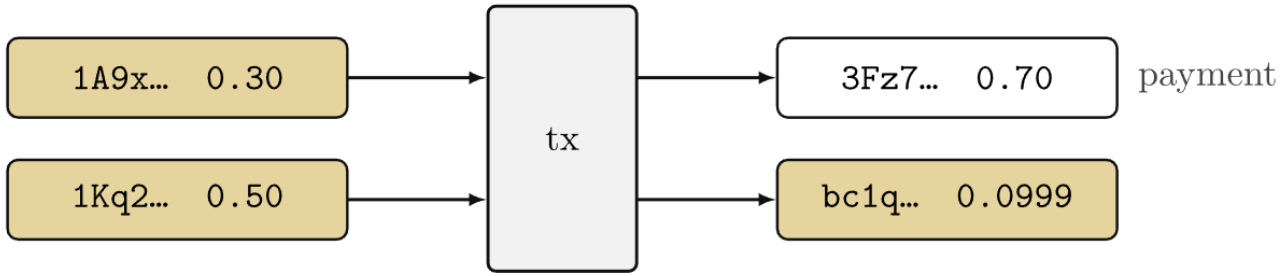
Clustering heuristics



Meiklejohn et al., "A Fistful of Bitcoins", IMC 2013.

Bitcoin transaction analysis

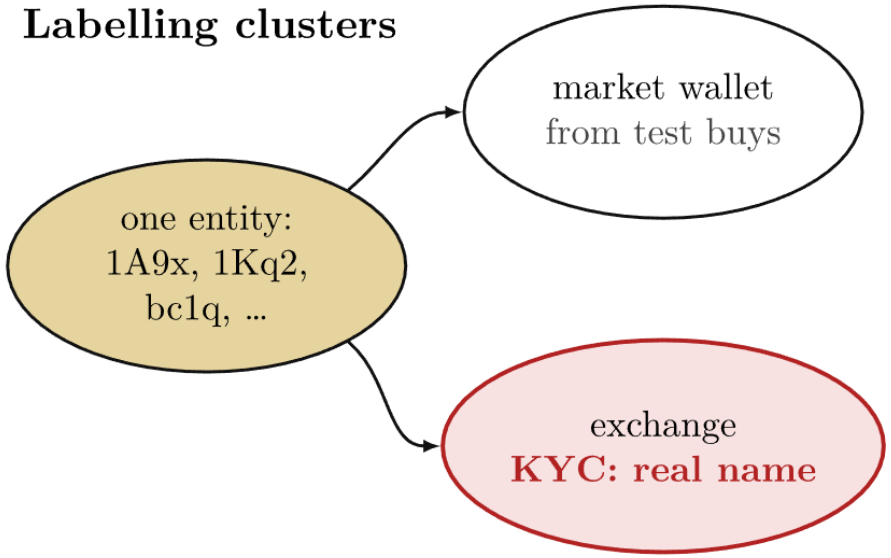
Clustering heuristics



1 signed together → one owner

2 fresh one-time address → likely change → same owner

Labelling clusters

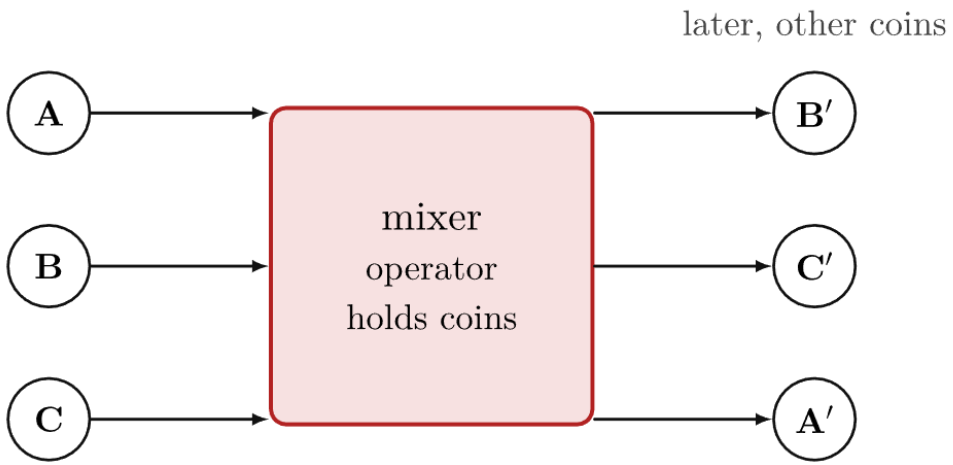


label sources: test purchases, seized servers, subpoenas, public tags

Meiklejohn et al., "A Fistful of Bitcoins", IMC 2013.

Mixers and CoinJoin

Custodial mixer

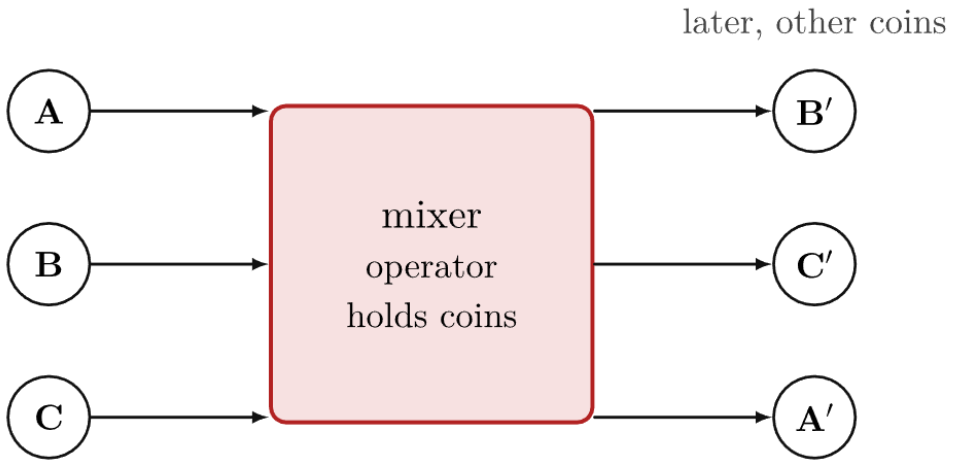


operator holds input–output mapping

US DOJ releases, 8 Nov 2024 and 19 Nov 2025.

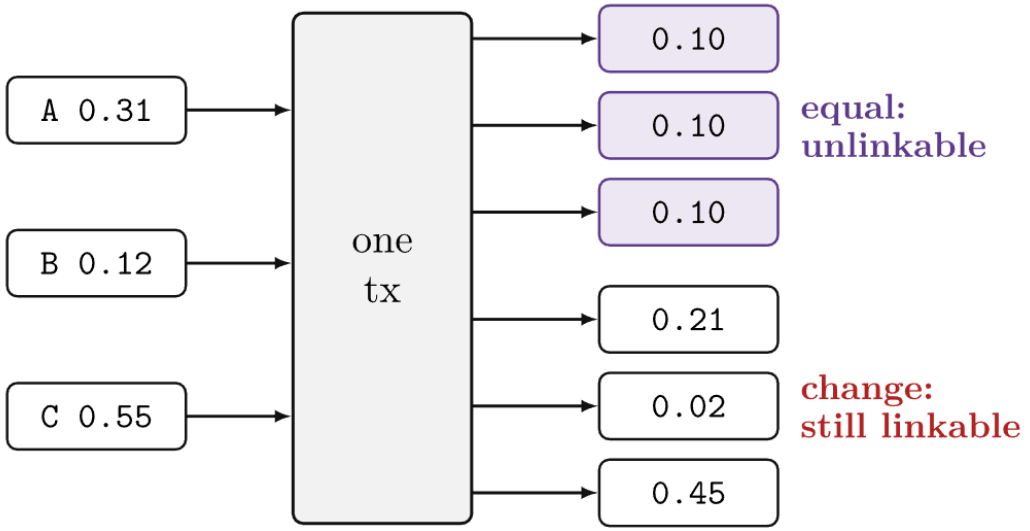
Mixers and CoinJoin

Custodial mixer



operator holds input–output mapping

CoinJoin

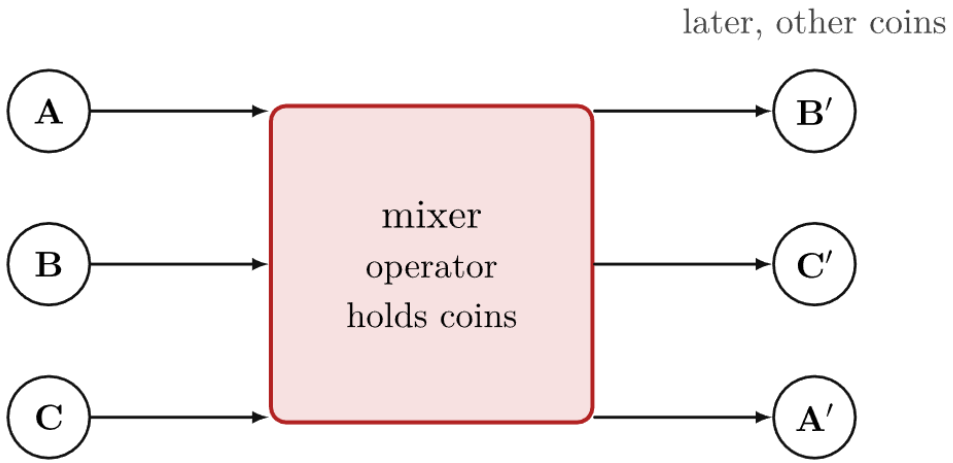


no custody; coordinator required;
amounts and timing still leak

US DOJ releases, 8 Nov 2024 and 19 Nov 2025.

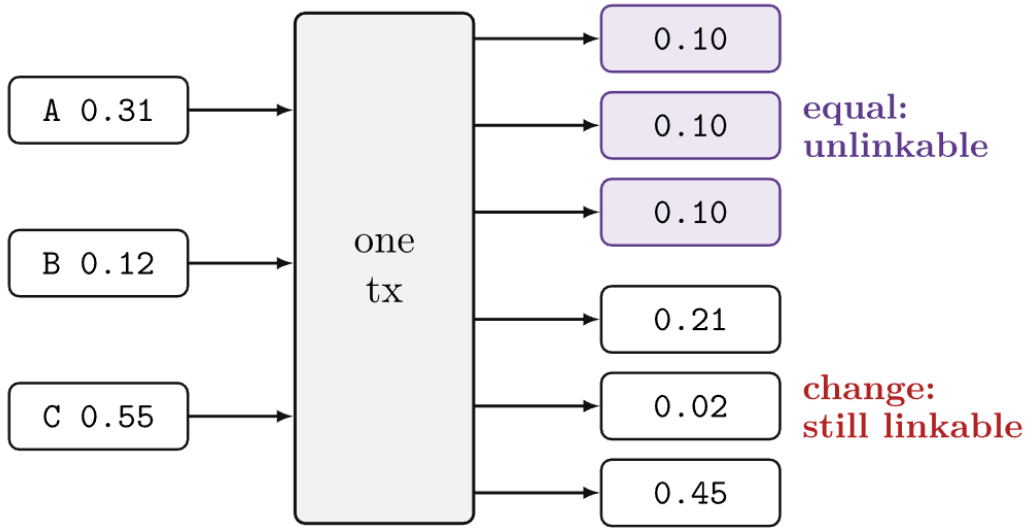
Mixers and CoinJoin

Custodial mixer



operator holds input–output mapping

CoinJoin



no custody; coordinator required;
amounts and timing still leak

Bitcoin Fog

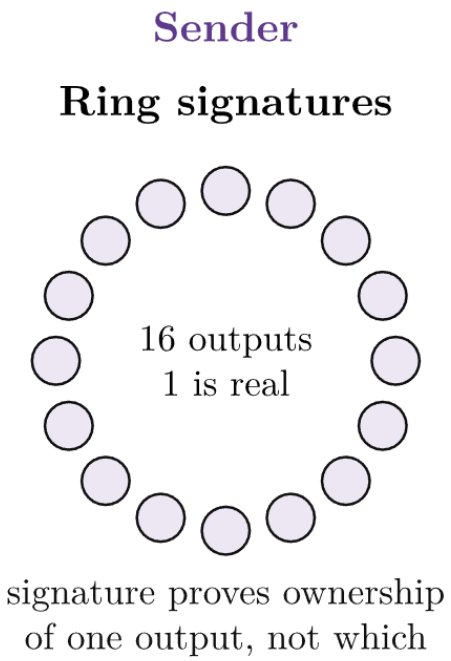
Samourai Wallet

US DOJ releases, 8 Nov 2024 and 19 Nov 2025.

Can we design a transaction system that hides the sender, the recipient and the amount?

Monero

Monero

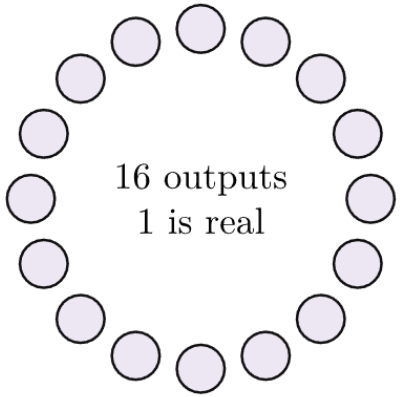


Ring size 16, Bulletproofs+: since Aug 2022 upgrade

Monero

Sender

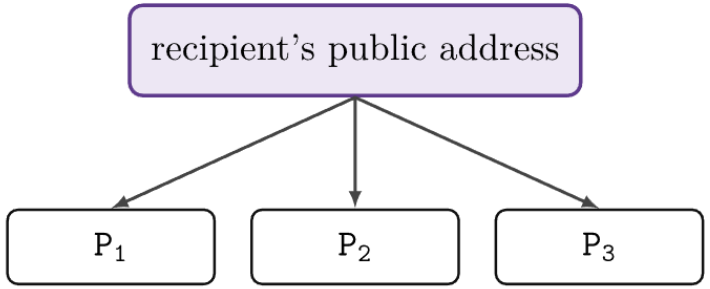
Ring signatures



signature proves ownership of one output, not which

Recipient

One-time addresses



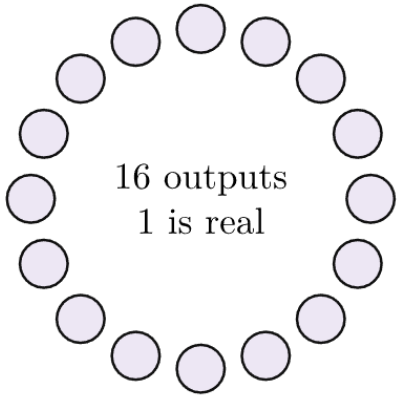
fresh key per payment; found only with recipient's view key

Ring size 16, Bulletproofs+: since Aug 2022 upgrade

Monero

Sender

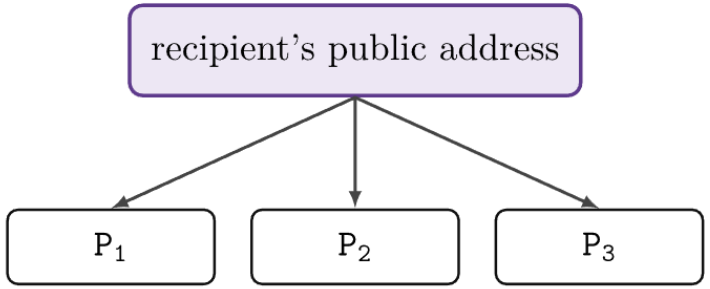
Ring signatures



signature proves ownership of one output, not which

Recipient

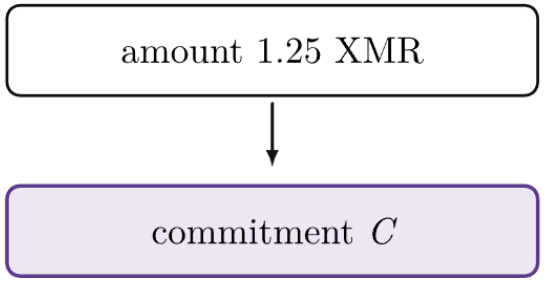
One-time addresses



fresh key per payment; found only with recipient's view key

Amount

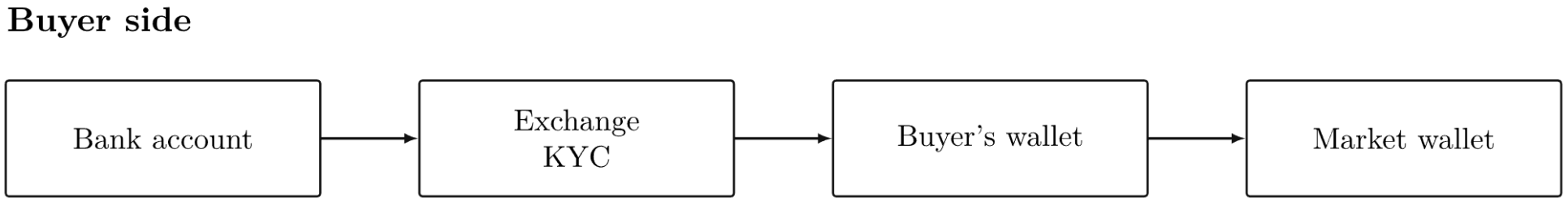
RingCT



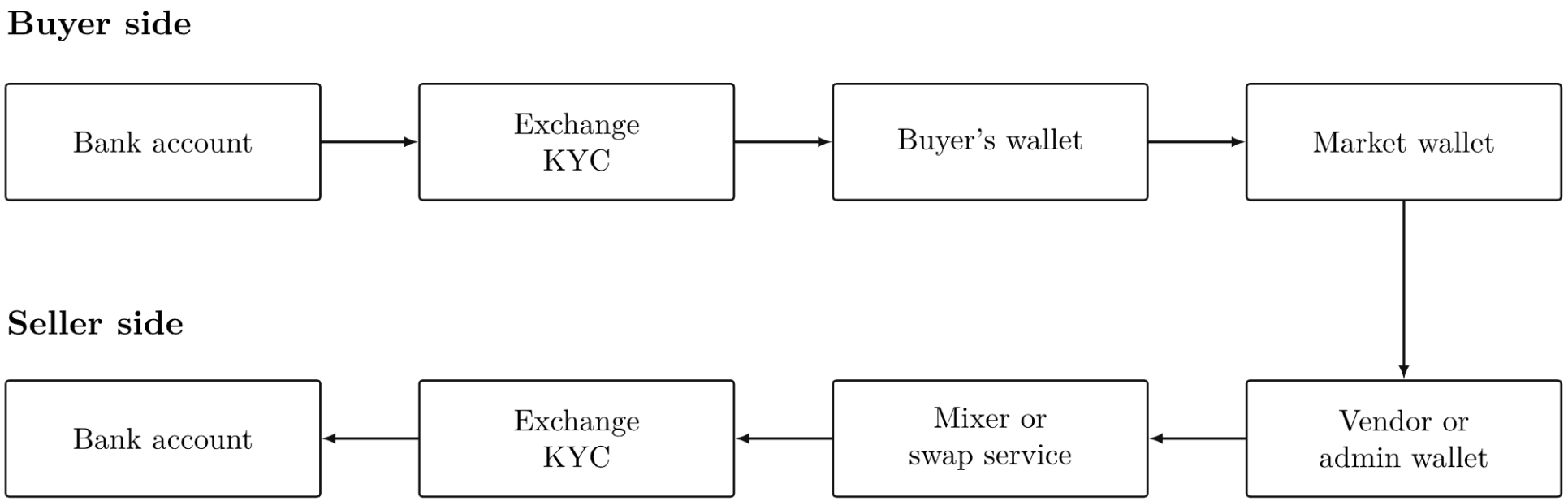
range proof (Bulletproofs+): valid amount, value hidden

Ring size 16, Bulletproofs+: since Aug 2022 upgrade

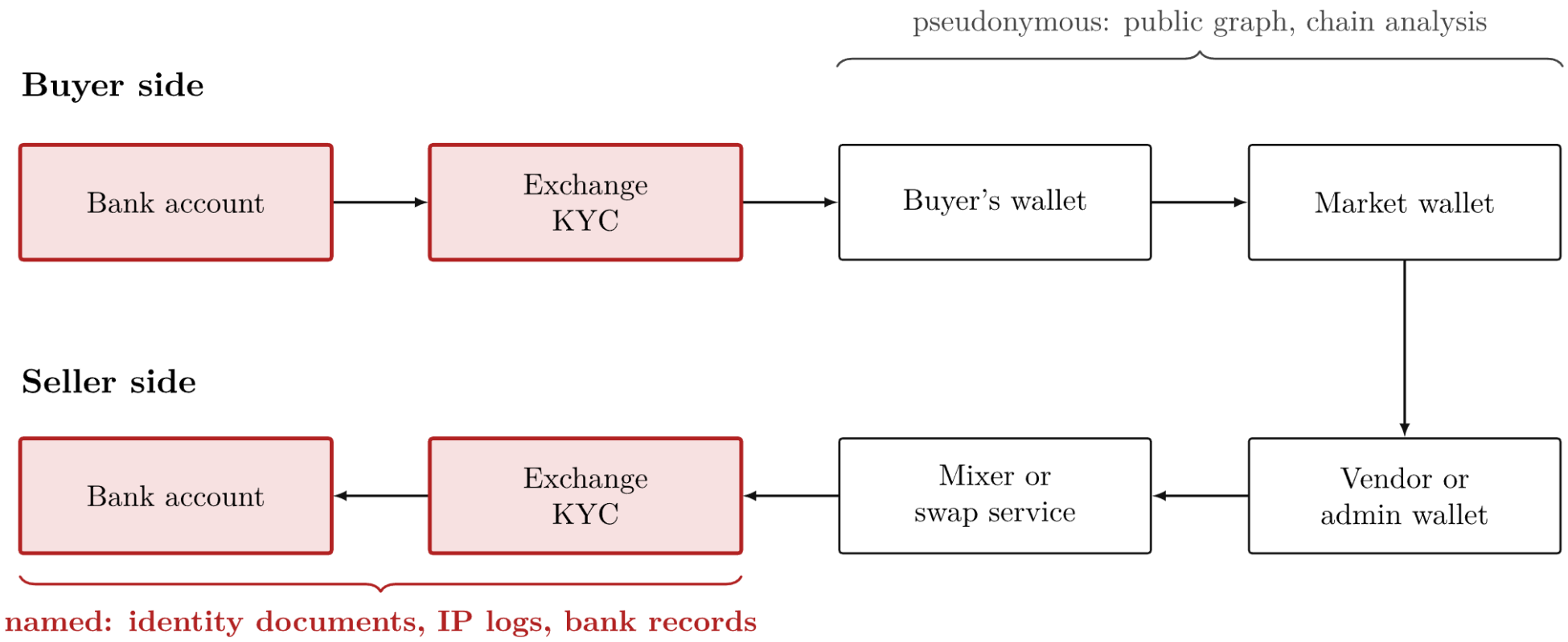
On-ramps and off-ramps



On-ramps and off-ramps



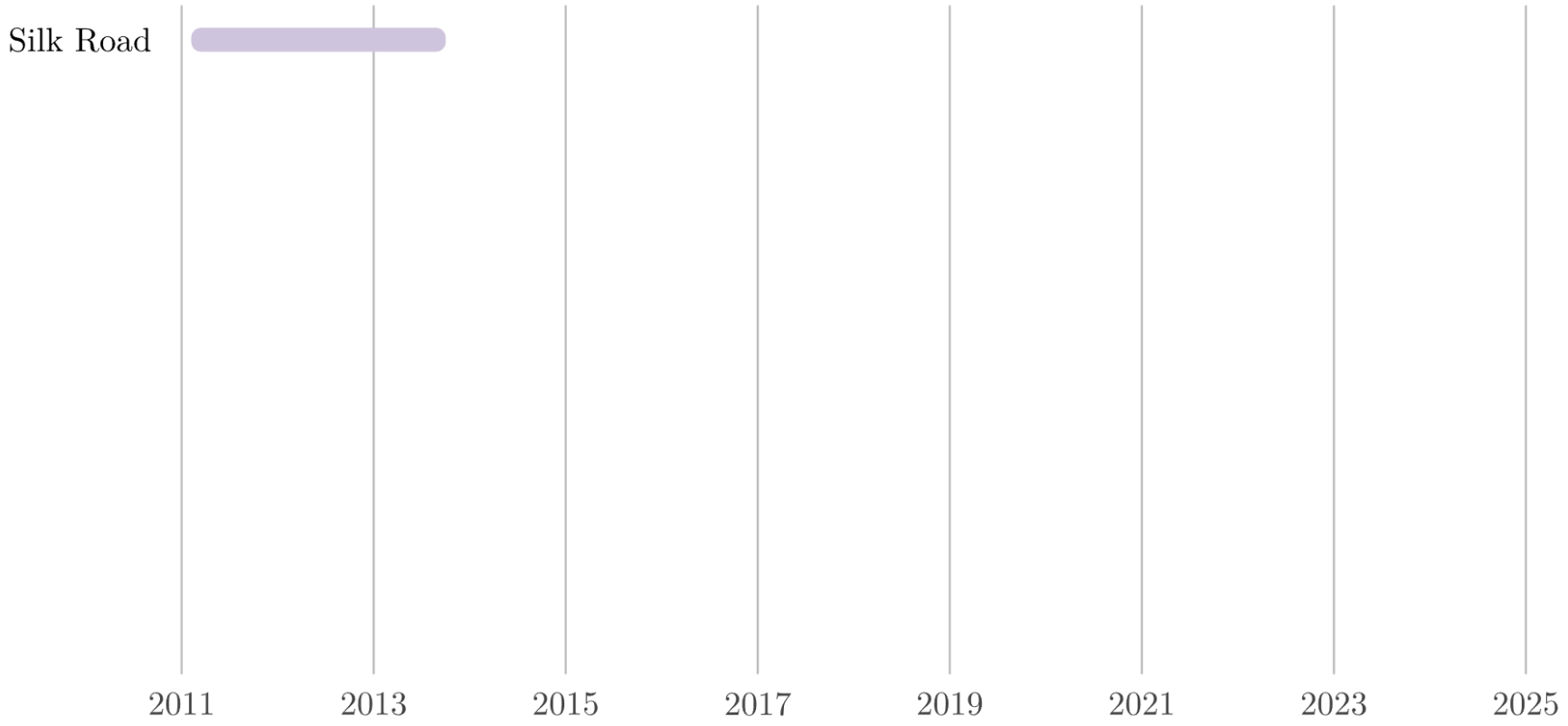
On-ramps and off-ramps



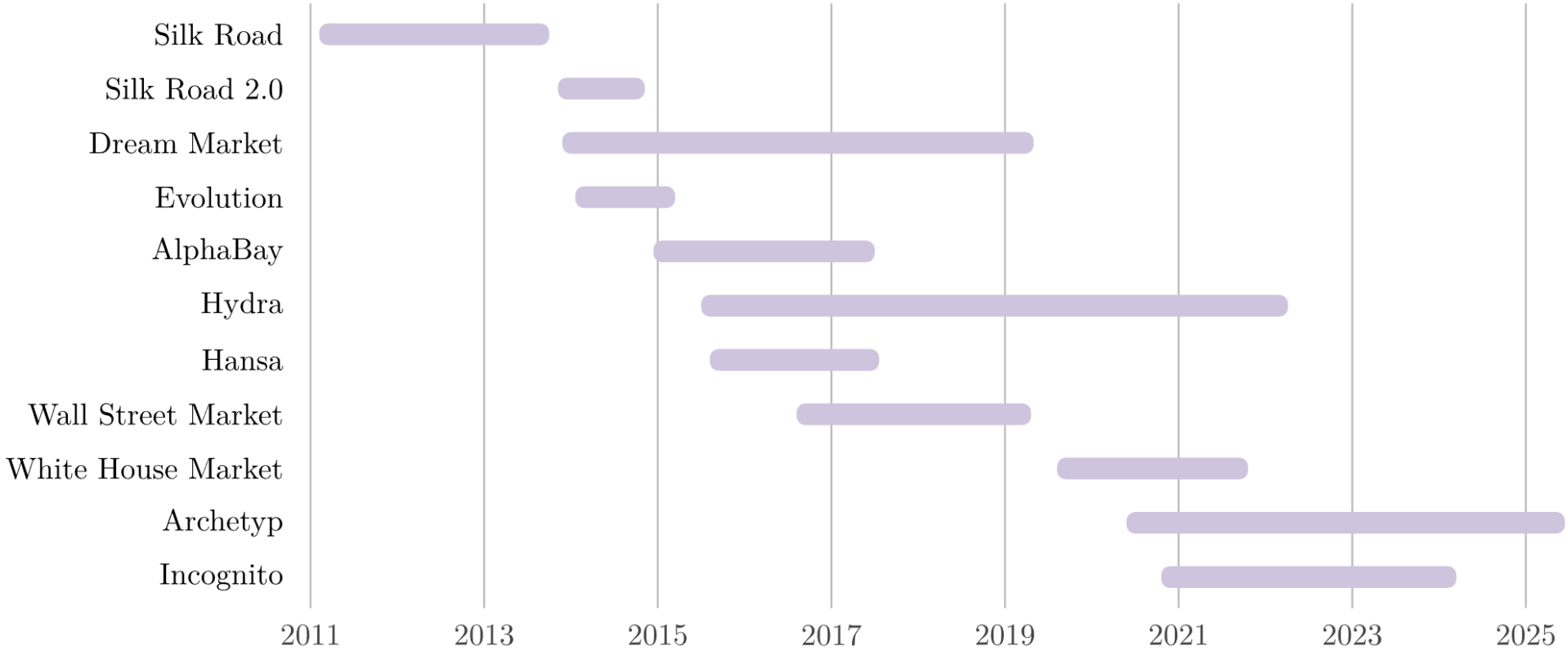
Part IV

Darknet Markets

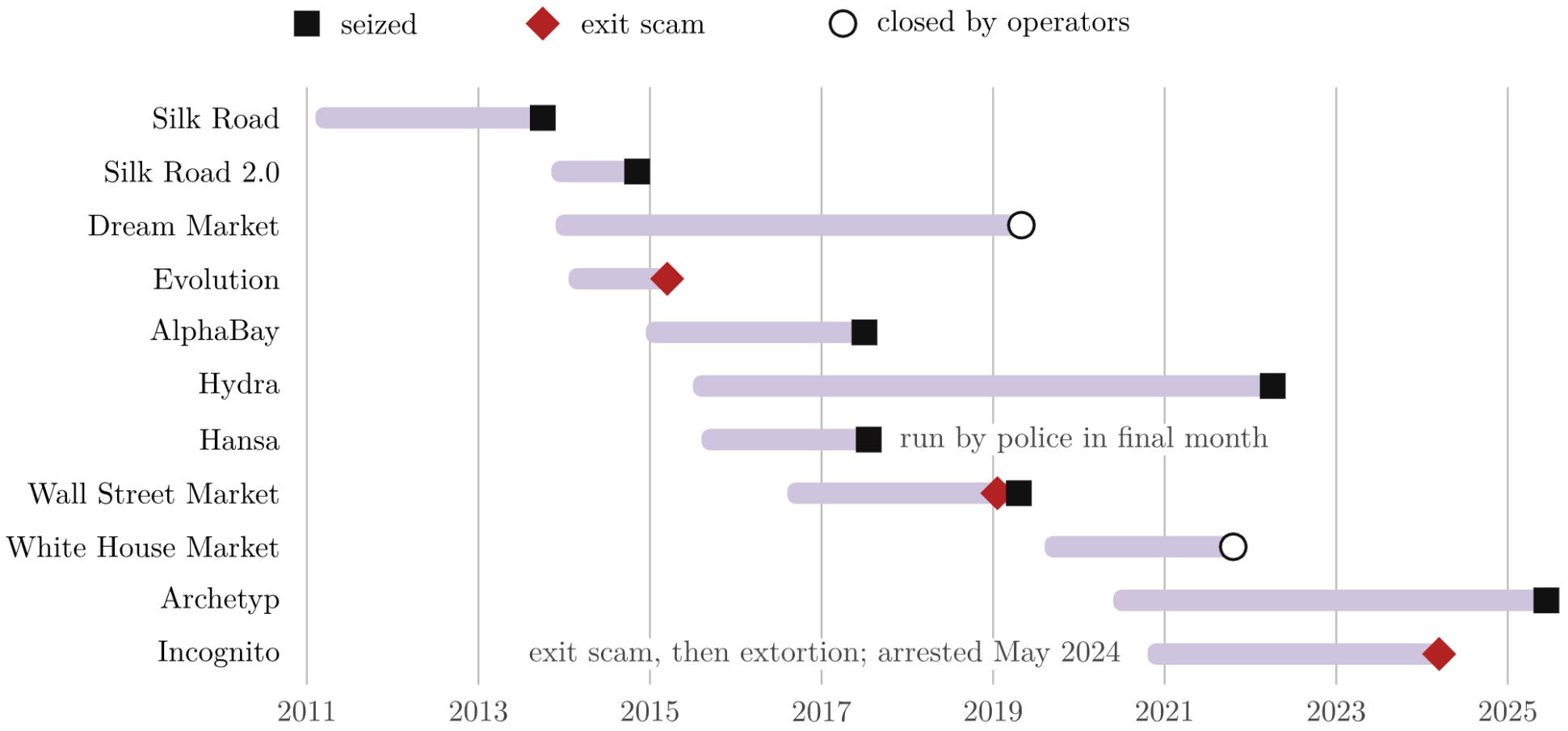
Market timeline, 2011–2025



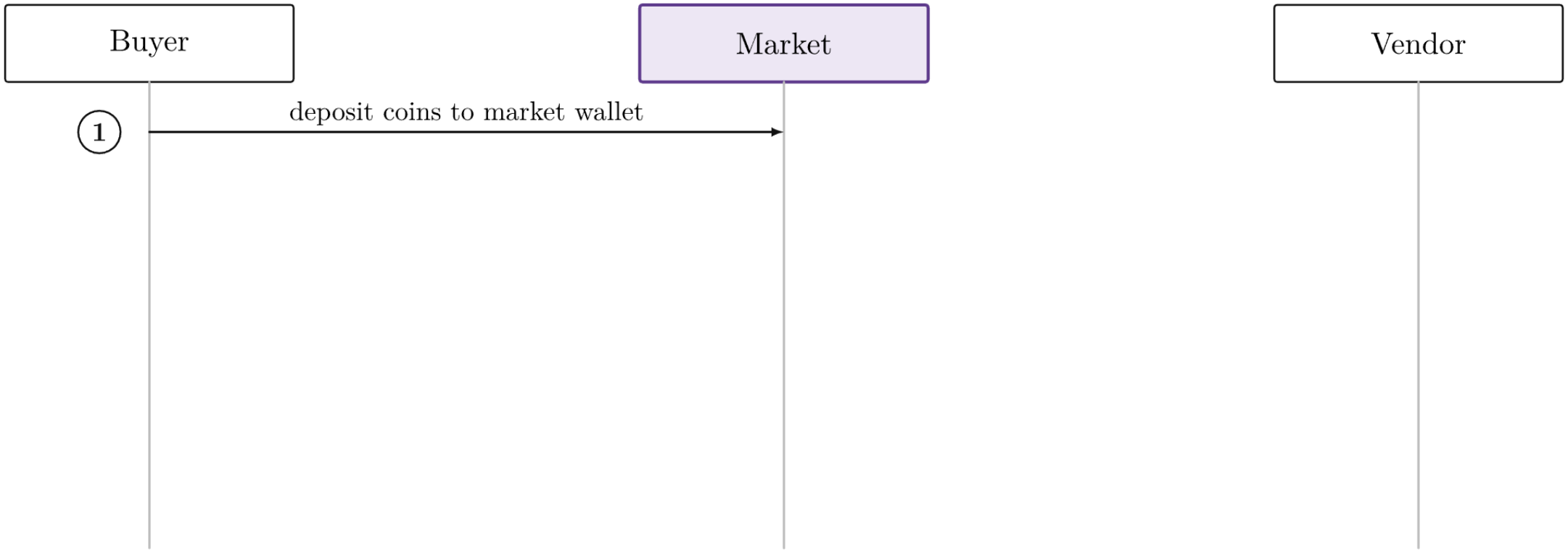
Market timeline, 2011–2025



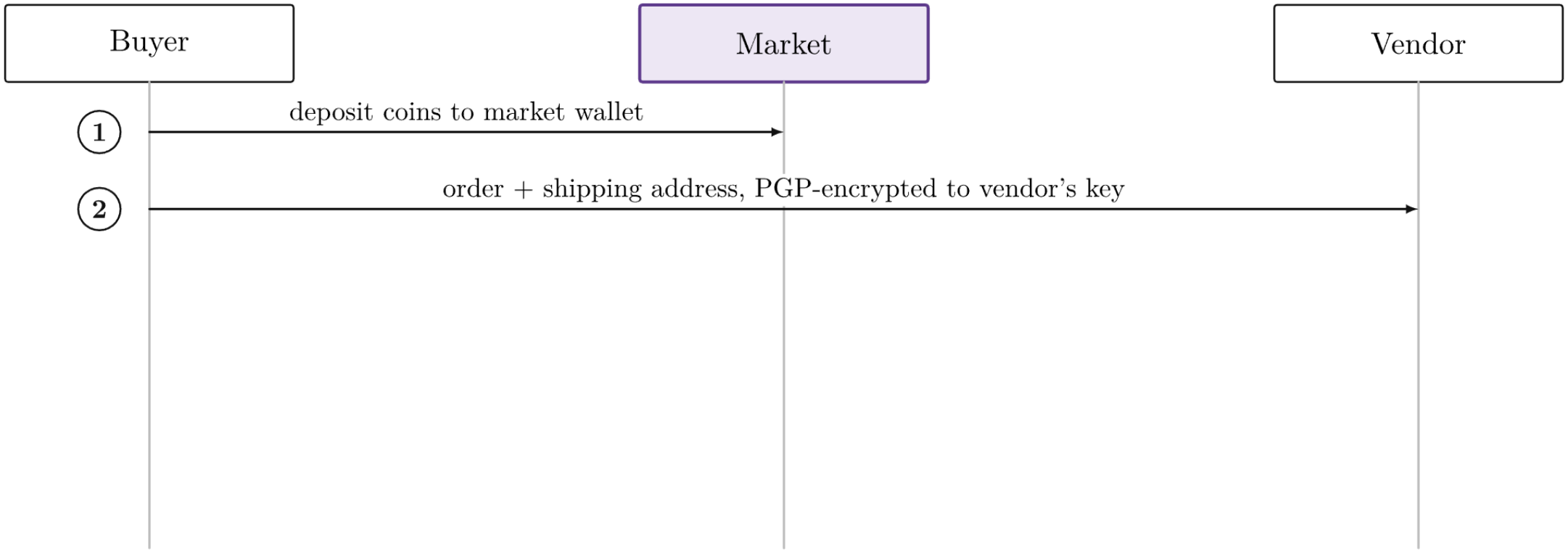
Market timeline, 2011–2025



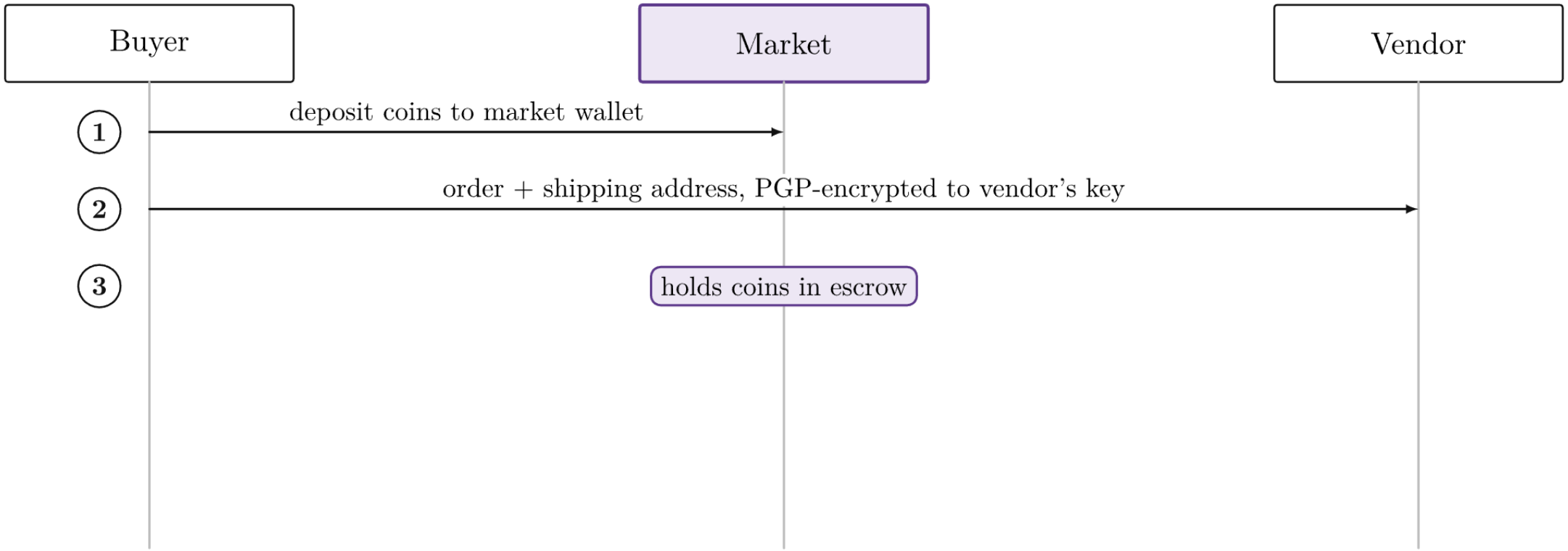
Purchase flow and escrow



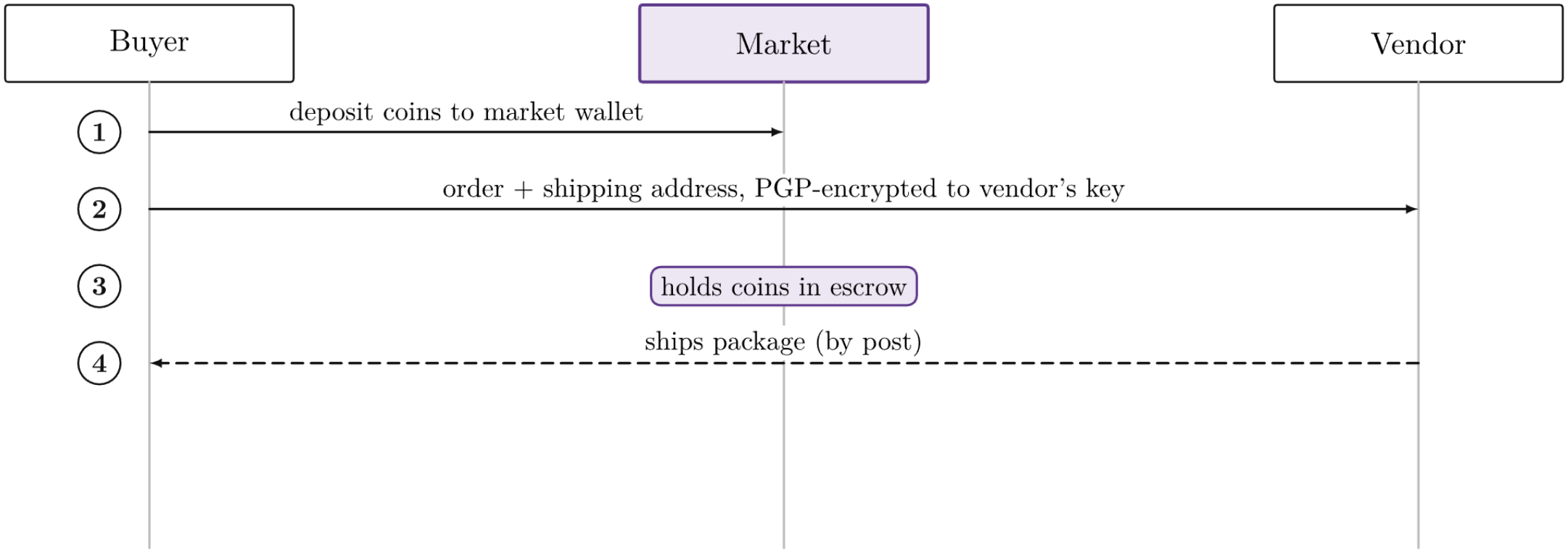
Purchase flow and escrow



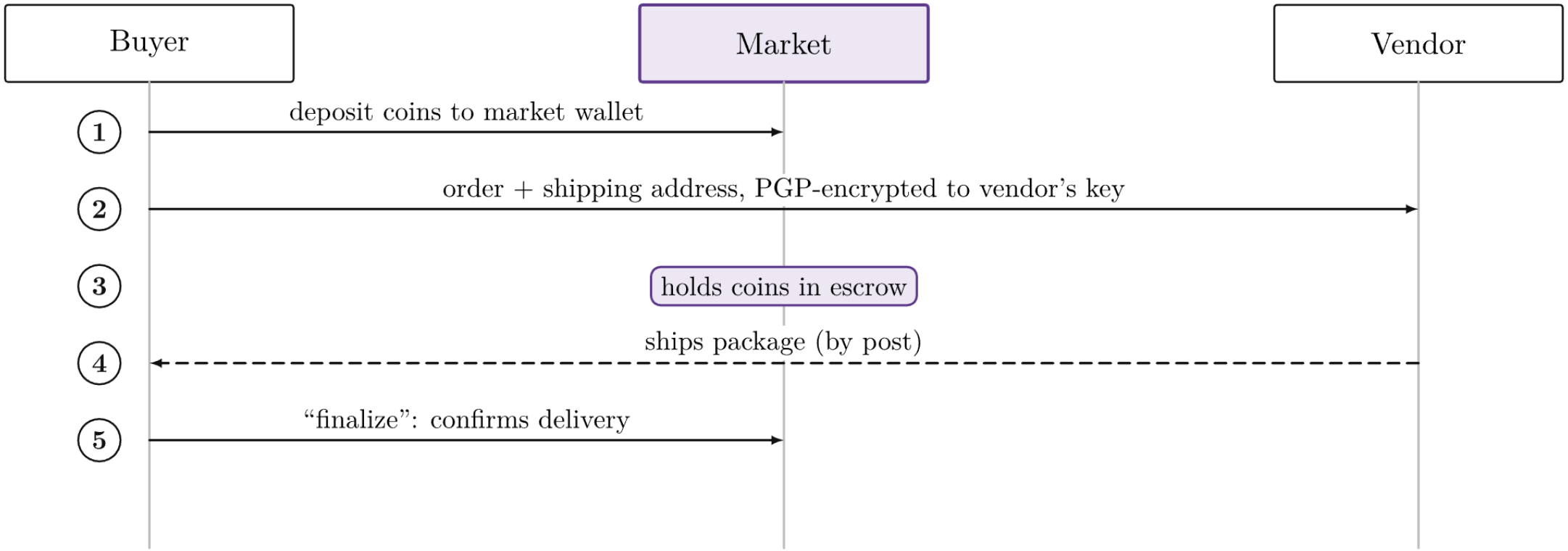
Purchase flow and escrow



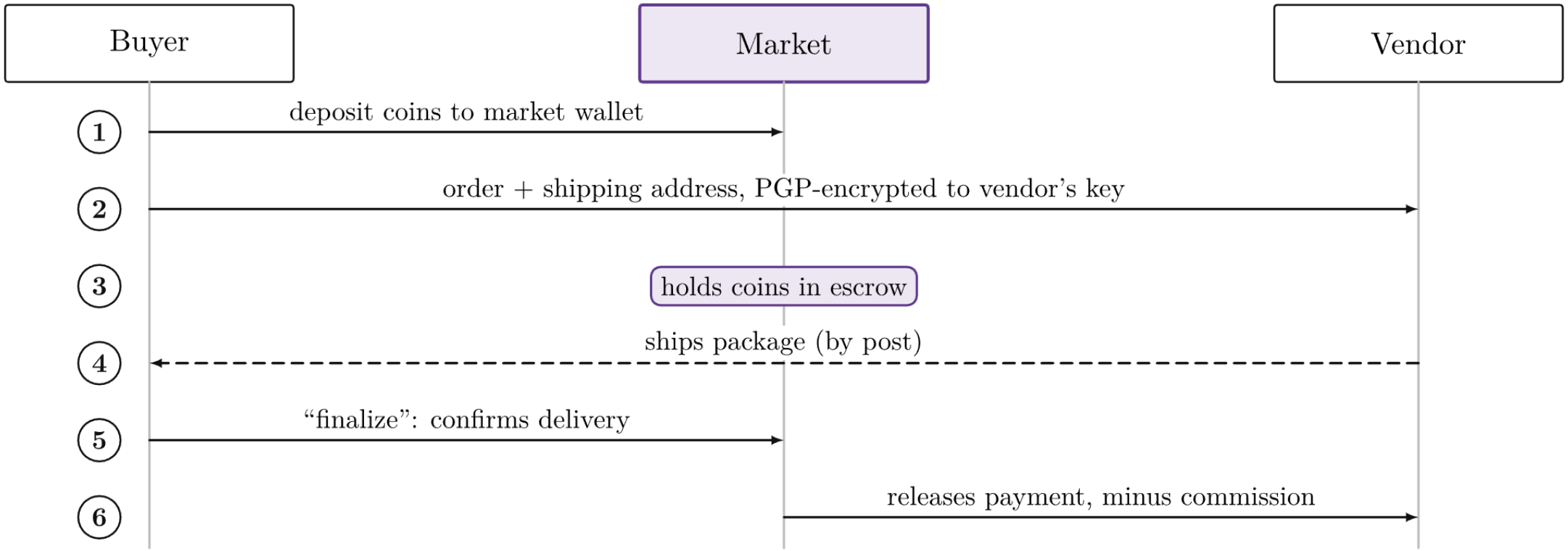
Purchase flow and escrow



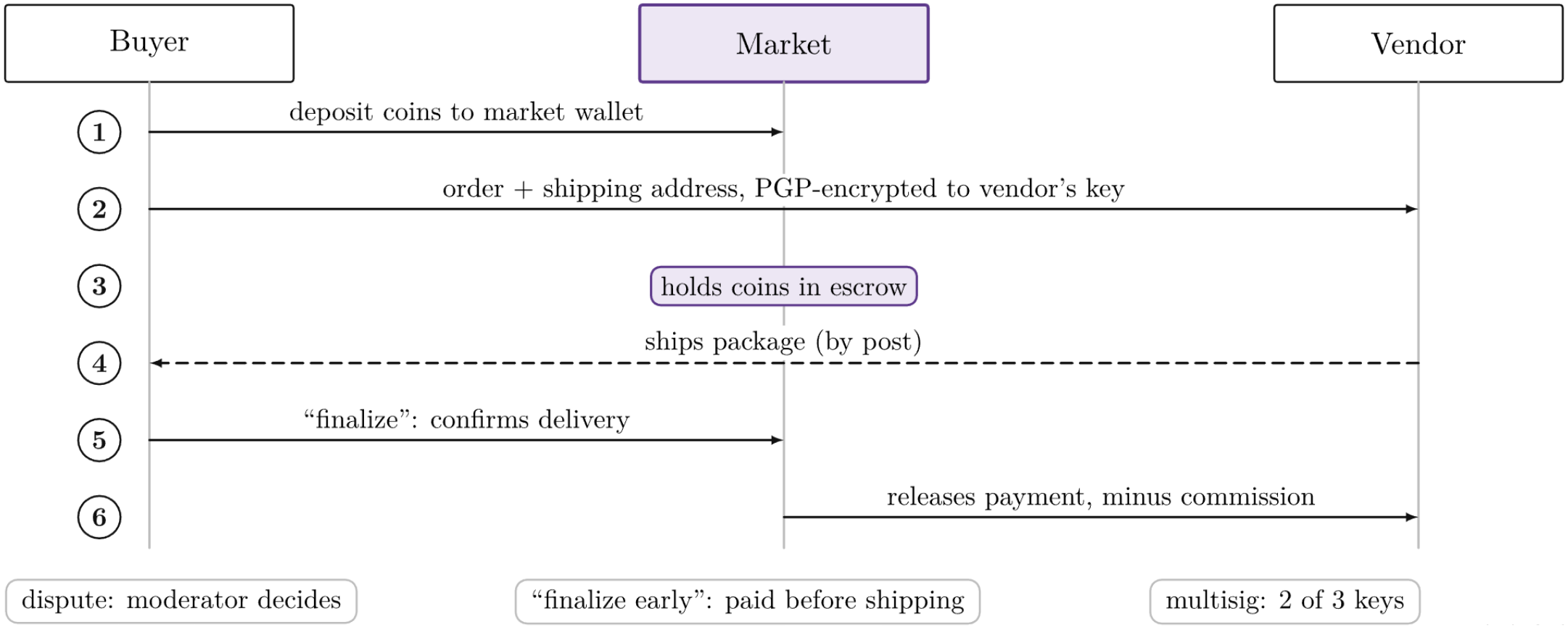
Purchase flow and escrow



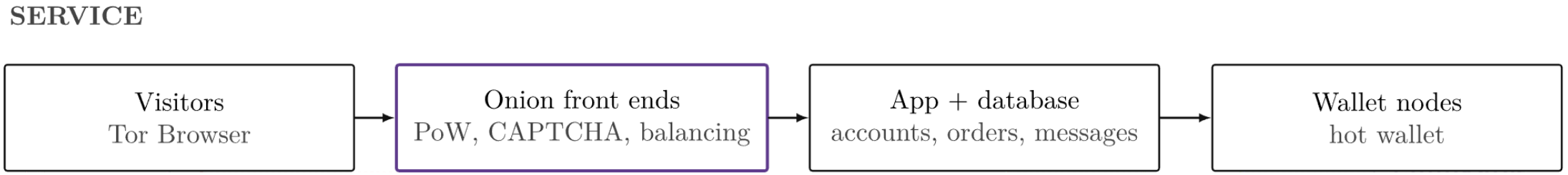
Purchase flow and escrow



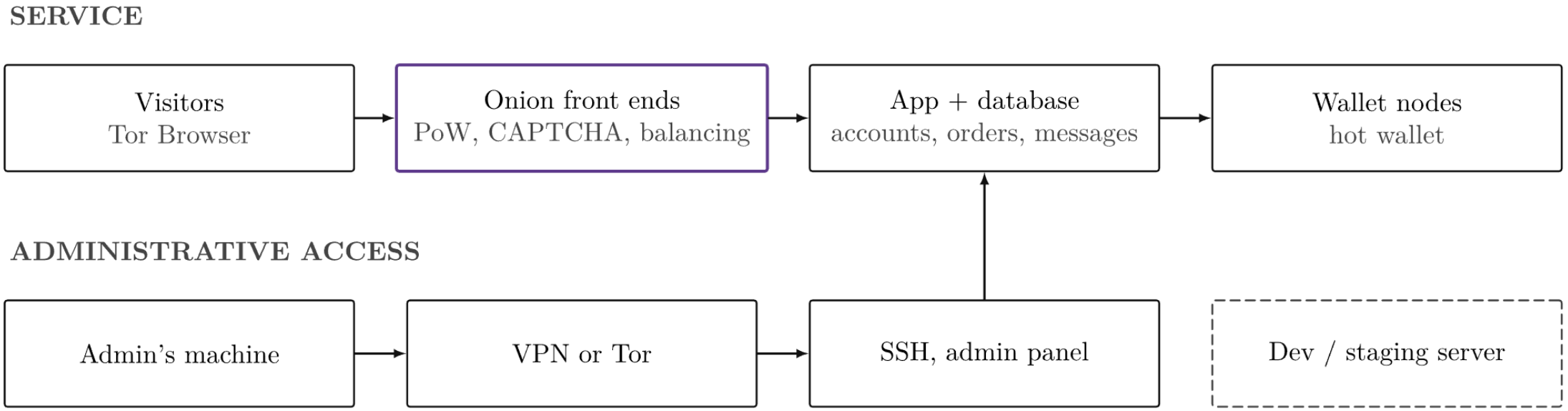
Purchase flow and escrow



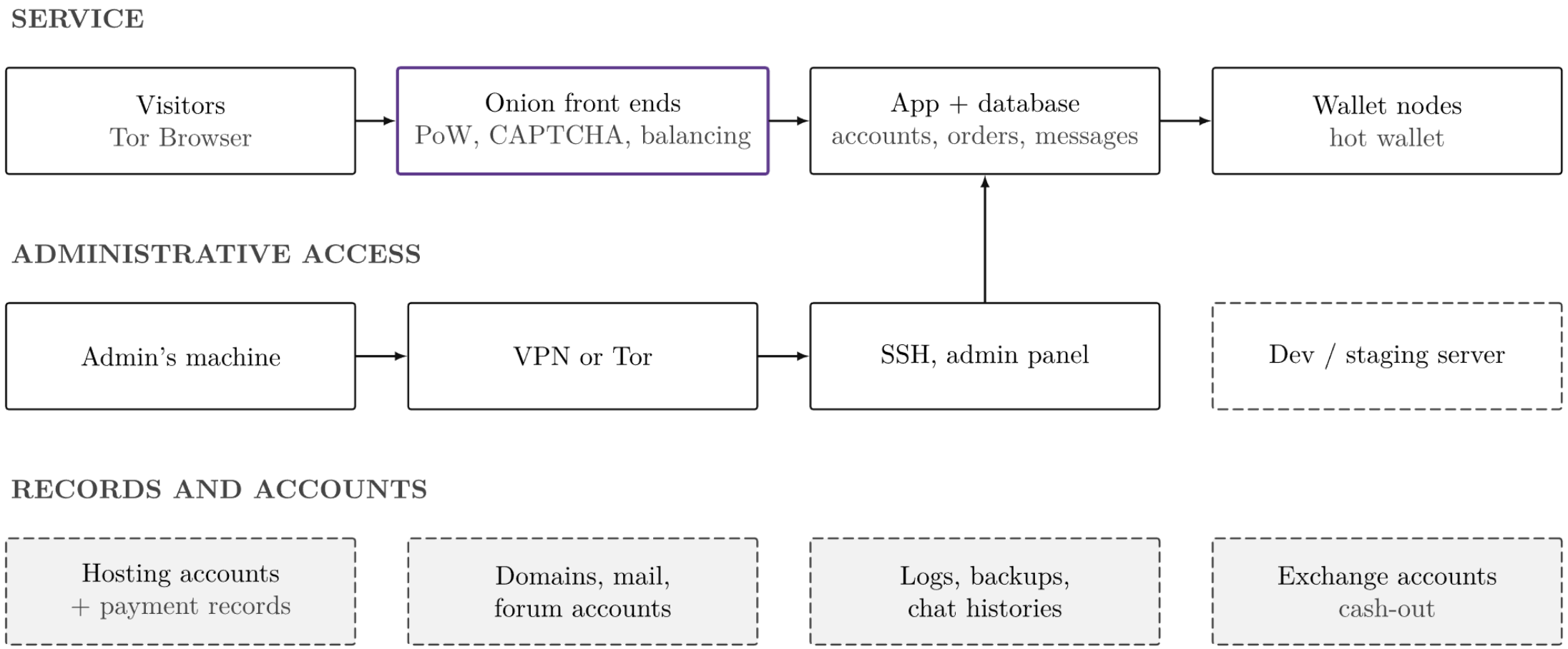
Market infrastructure



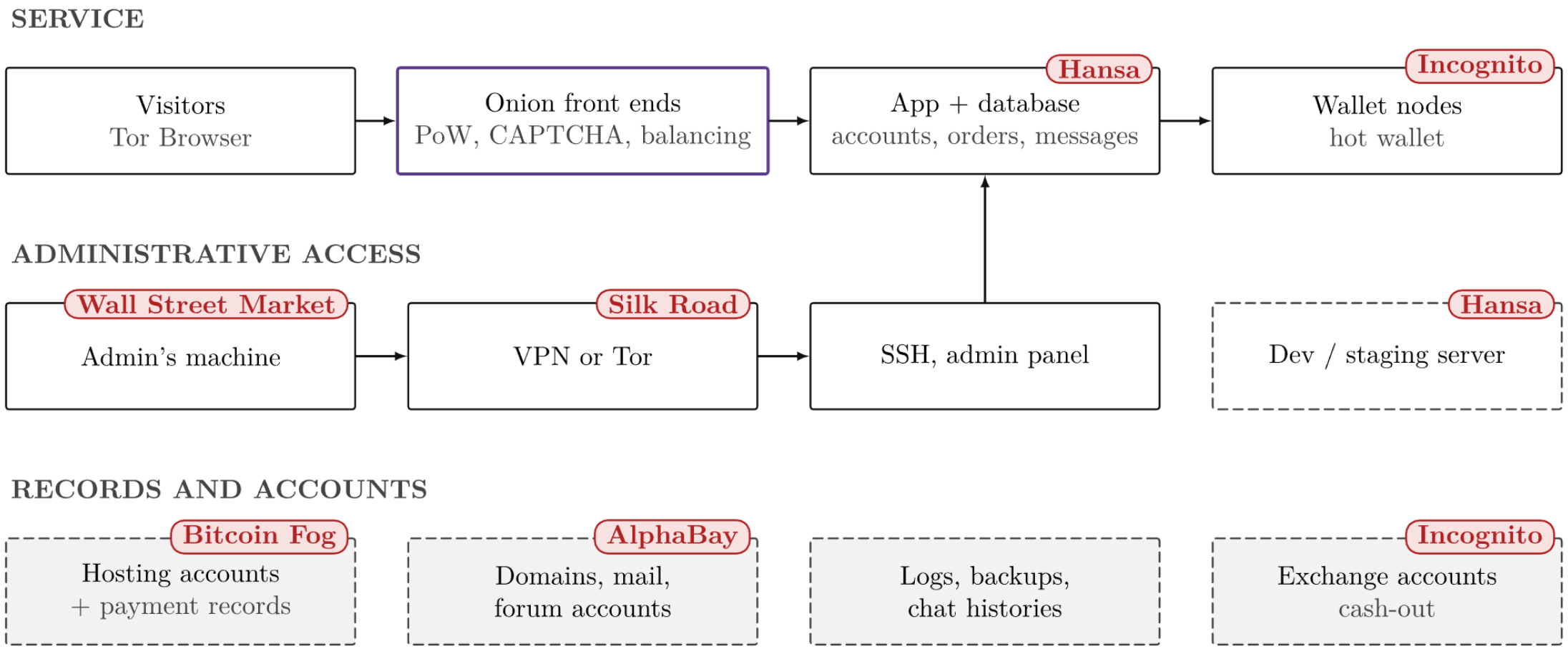
Market infrastructure



Market infrastructure



Market infrastructure



Part V

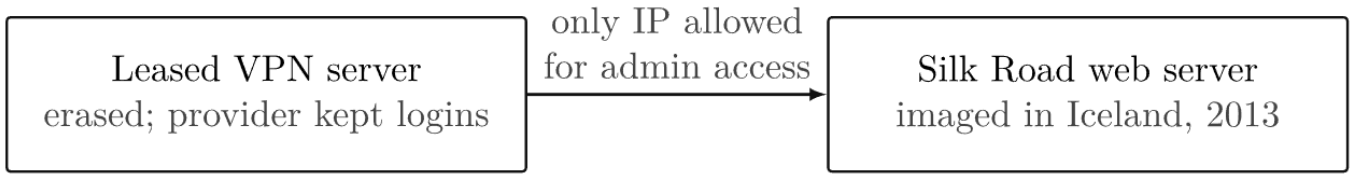
Case Studies

Silk Road, 2013

Admin access through a VPN

Life sentence, 2015; pardoned, January 2025

Admin access path (complaint ¶ 41)

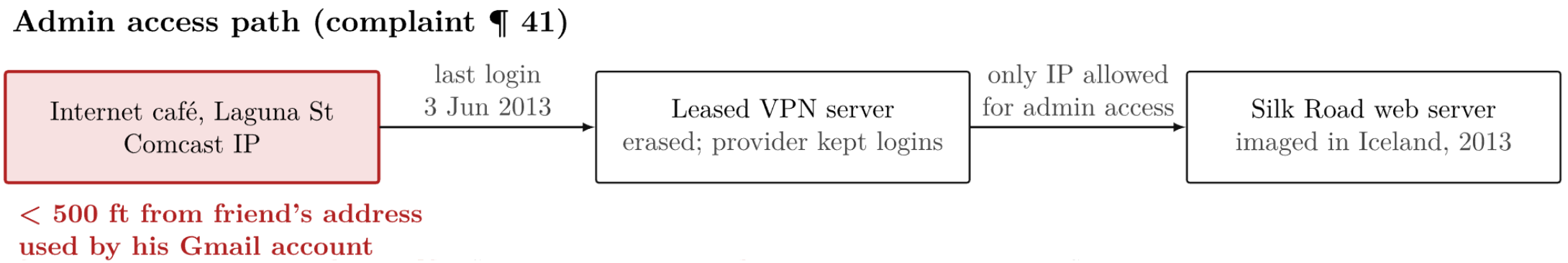


US v. Ulbricht, criminal complaint, S.D.N.Y., Sept 2013, ¶¶ 34–43.

Silk Road, 2013

A VPN login from a café

Life sentence, 2015; pardoned, January 2025



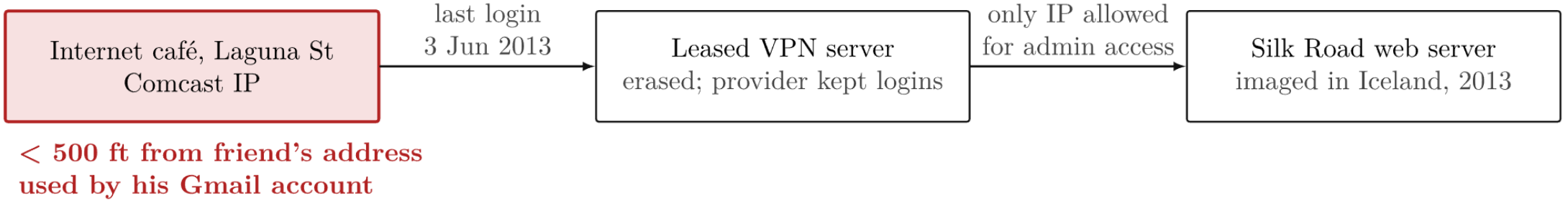
US v. Ulbricht, criminal complaint, S.D.N.Y., Sept 2013, ¶¶ 34–43.

Silk Road, 2013

A reused forum handle

Life sentence, 2015; pardoned, January 2025

Admin access path (complaint ¶ 41)



Online identity (complaint ¶¶ 34–43)



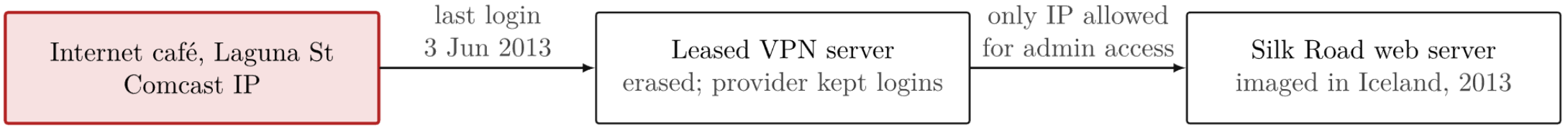
US v. Ulbricht, criminal complaint, S.D.N.Y., Sept 2013, ¶¶ 34–43.

Silk Road, 2013

A coding question under his name

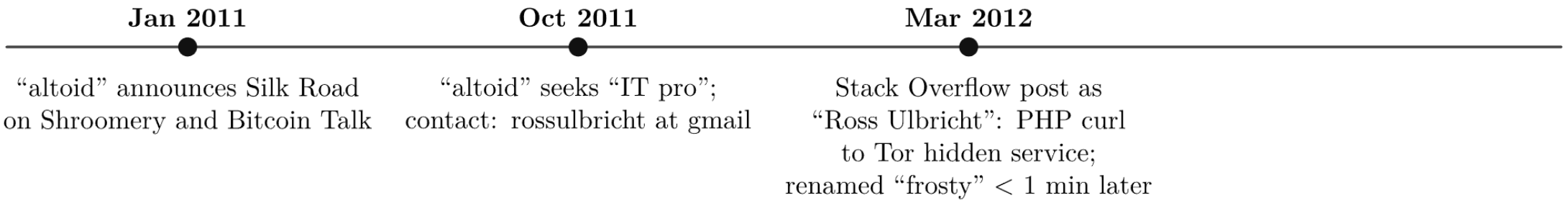
Life sentence, 2015; pardoned, January 2025

Admin access path (complaint ¶ 41)



< 500 ft from friend's address used by his Gmail account

Online identity (complaint ¶¶ 34–43)



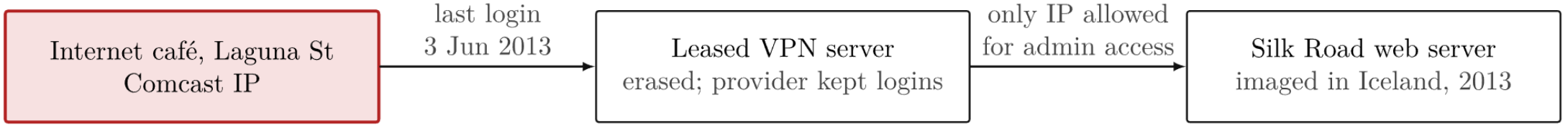
US v. Ulbricht, criminal complaint, S.D.N.Y., Sept 2013, ¶¶ 34–43.

Silk Road, 2013

Where the two trails meet

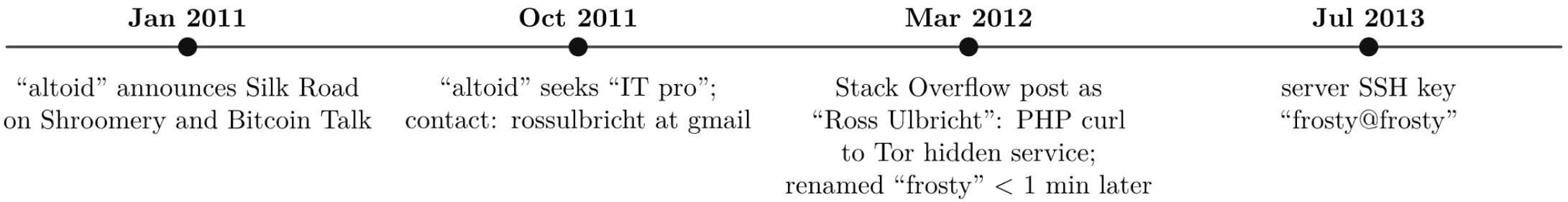
Life sentence, 2015; pardoned, January 2025

Admin access path (complaint ¶ 41)



< 500 ft from friend's address used by his Gmail account

Online identity (complaint ¶¶ 34–43)



US v. Ulbricht, criminal complaint, S.D.N.Y., Sept 2013, ¶¶ 34–43.

AlphaBay, 2017

Personal email in system-generated mail

Died in custody, 12 July 2017

Mail headers, 2014 `Pimp_Alex_91@hotmail.com`

US v. Cazes, civil forfeiture complaint, E.D. Cal., Jul 2017, as reported; DOJ, 20 Jul 2017.

AlphaBay, 2017

Personal email in system-generated mail

Died in custody, 12 July 2017

Mail headers, 2014	`Pimp_Alex_91@hotmail.com`
Handle	“Alpha02”

US v. Cazes, civil forfeiture complaint, E.D. Cal., Jul 2017, as reported; DOJ, 20 Jul 2017.

AlphaBay, 2017

Personal email in system-generated mail

Died in custody, 12 July 2017

Mail headers, 2014	`Pimp_Alex_91@hotmail.com`
Handle	“Alpha02”
Identity	EBX Technologies

US v. Cazes, civil forfeiture complaint, E.D. Cal., Jul 2017, as reported; DOJ, 20 Jul 2017.

AlphaBay, 2017

Personal email in system-generated mail

Died in custody, 12 July 2017

Mail headers, 2014	`Pimp_Alex_91@hotmail.com`
Handle	“Alpha02”
Identity	EBX Technologies
Arrest, 5 July 2017	Bangkok

US v. Cazes, civil forfeiture complaint, E.D. Cal., Jul 2017, as reported; DOJ, 20 Jul 2017.

Hansa, 2017

Police takeover

Admins arrested in Germany, 20 June 2017



Dutch National Police and Europol, 20 Jul 2017; Wired, "Operation Bayonet", Mar 2018.

Hansa, 2017

Police takeover

Admins arrested in Germany, 20 June 2017



Dutch National Police and Europol, 20 Jul 2017; Wired, "Operation Bayonet", Mar 2018.

Hansa, 2017

Police takeover

Admins arrested in Germany, 20 June 2017

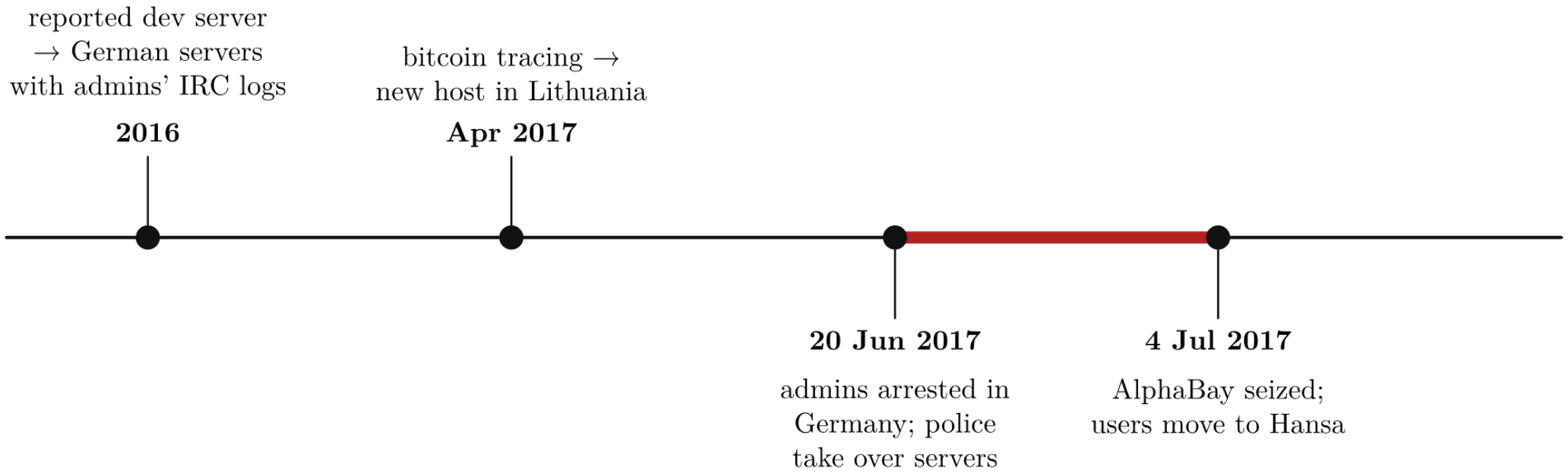


Dutch National Police and Europol, 20 Jul 2017; Wired, "Operation Bayonet", Mar 2018.

Hansa, 2017

Police takeover

Admins arrested in Germany, 20 June 2017

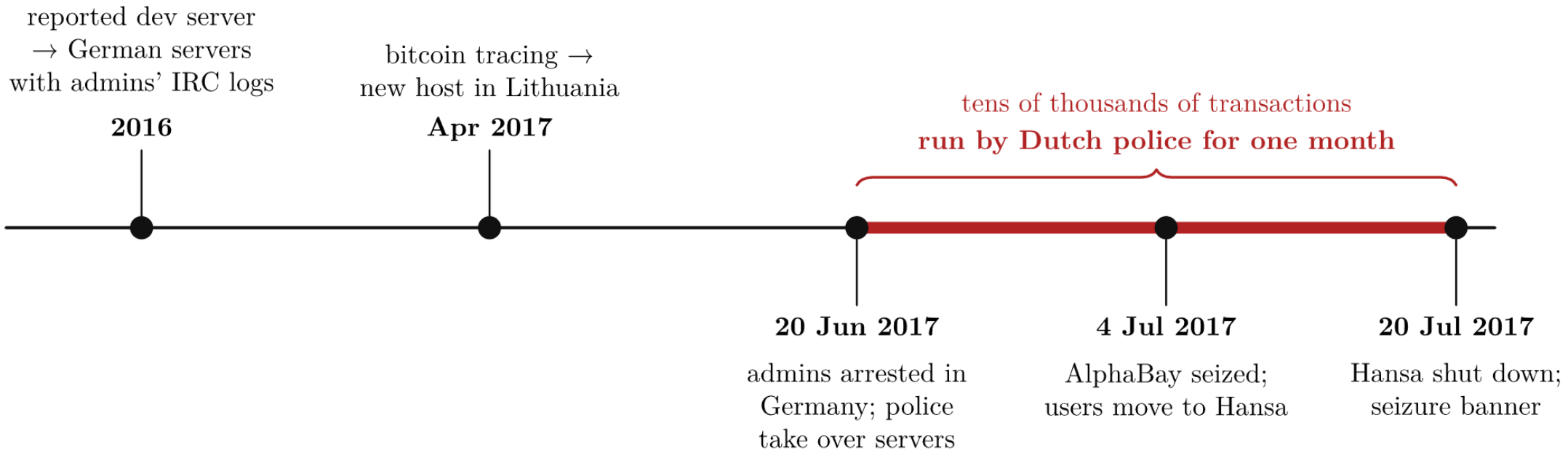


Dutch National Police and Europol, 20 Jul 2017; Wired, "Operation Bayonet", Mar 2018.

Hansa, 2017

Police takeover

Admins arrested in Germany, 20 June 2017

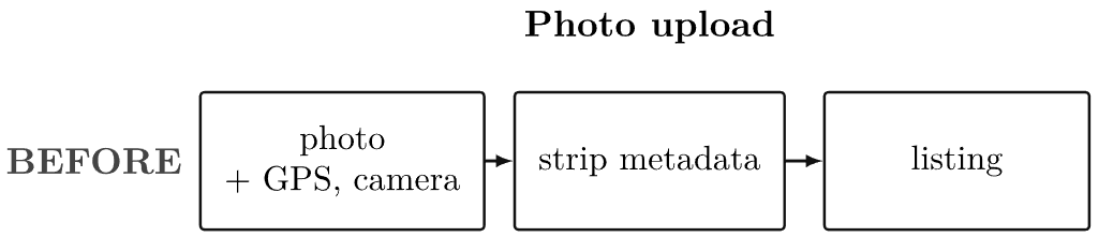


20 June – 20 July 2017: site operated by Dutch National Police

Dutch National Police and Europol, 20 Jul 2017; Wired, "Operation Bayonet", Mar 2018.

Hansa, 2017

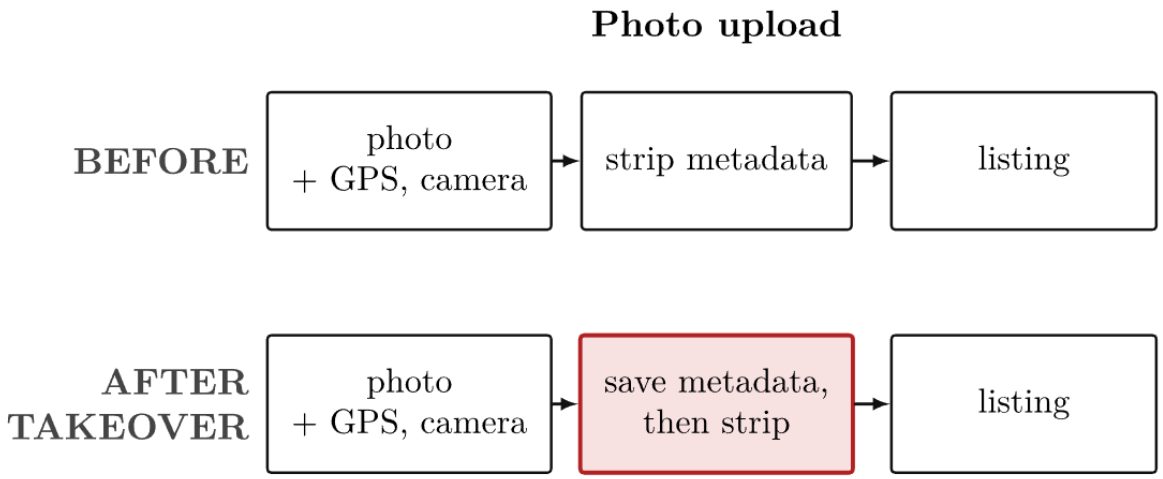
Changes under police control



Dutch National Police and Europol, 20 Jul 2017; Wired, “Operation Bayonet”, Mar 2018.

Hansa, 2017

Changes under police control

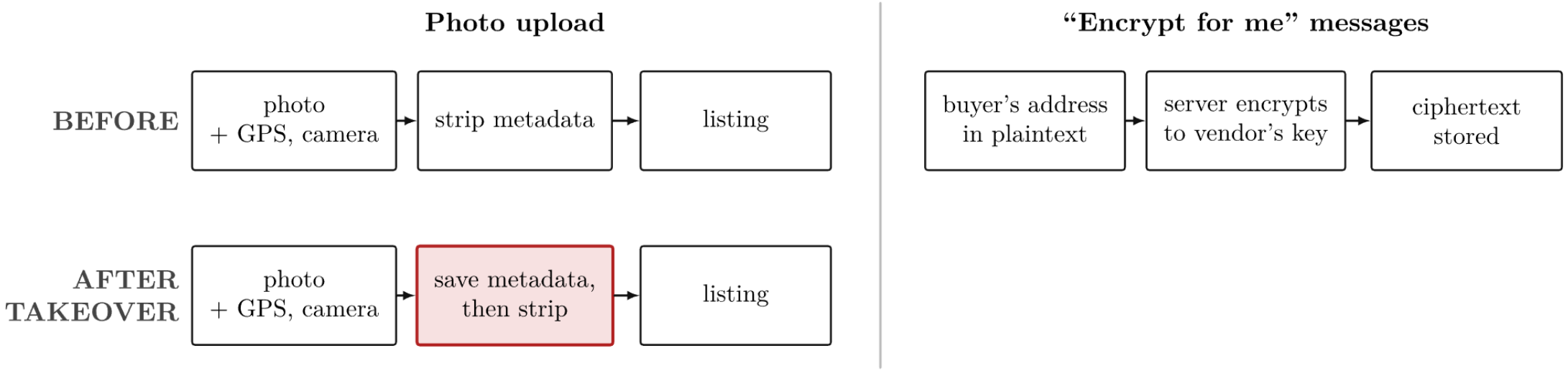


Photos wiped

Dutch National Police and Europol, 20 Jul 2017; Wired, “Operation Bayonet”, Mar 2018.

Hansa, 2017

Changes under police control

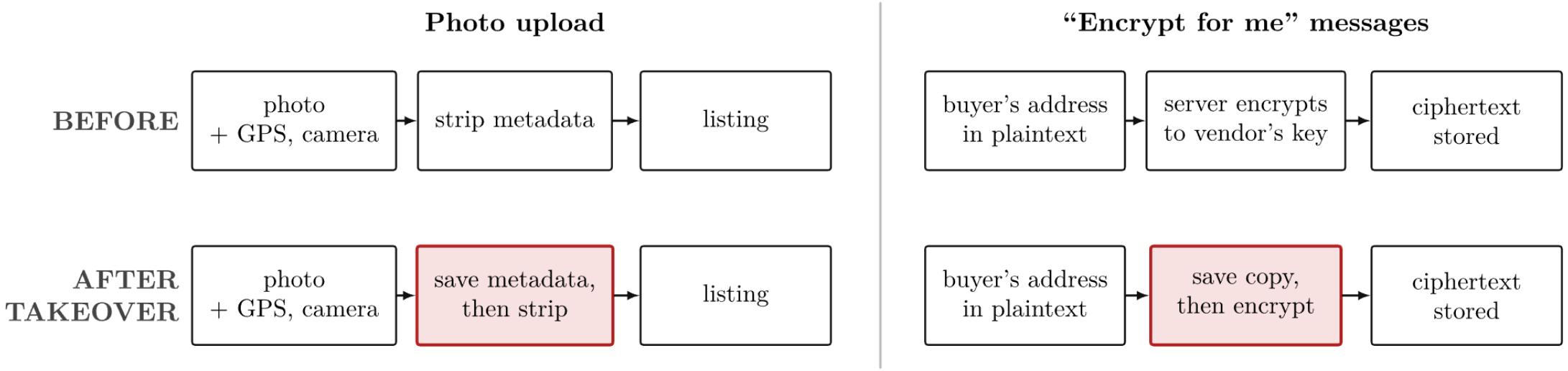


Photos wiped

Dutch National Police and Europol, 20 Jul 2017; Wired, "Operation Bayonet", Mar 2018.

Hansa, 2017

Changes under police control

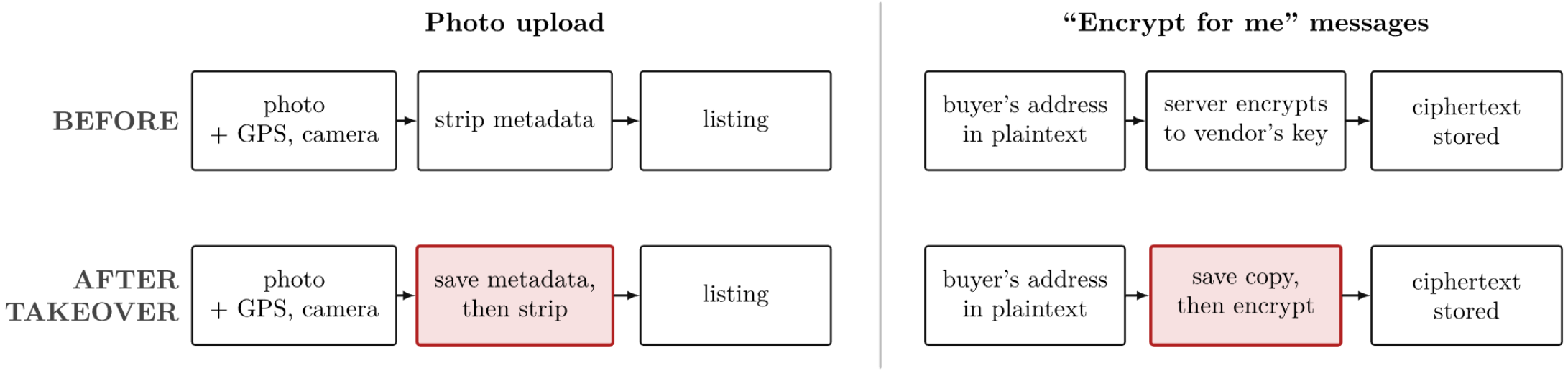


Photos wiped

Dutch National Police and Europol, 20 Jul 2017; Wired, "Operation Bayonet", Mar 2018.

Hansa, 2017

Changes under police control



Photos wiped

Passwords logged

Beacon file

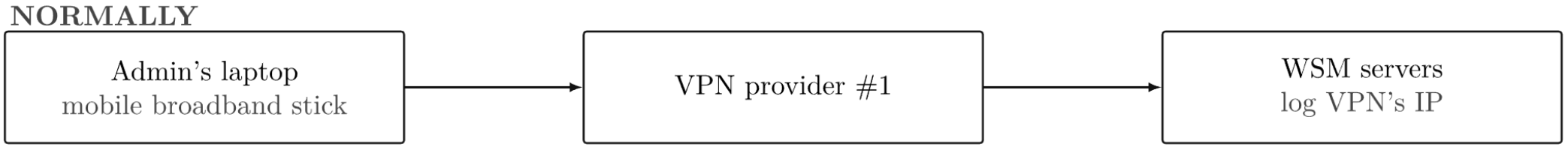
~10,000 addresses

Dutch National Police and Europol, 20 Jul 2017; Wired, "Operation Bayonet", Mar 2018.

Wall Street Market, 2019

VPN failure, admin's real IP

Admins arrested 23–24 April 2019

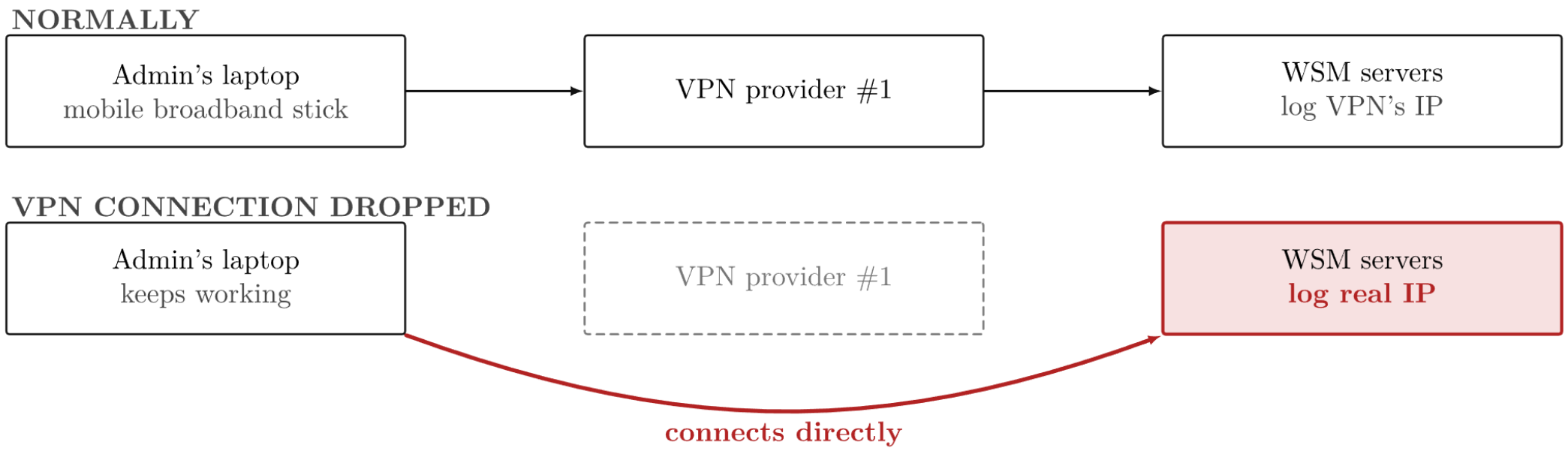


US v. Lousee, Kalla & Frost, complaint, C.D. Cal., May 2019, ¶¶ 23–25; DOJ, 3 May 2019.

Wall Street Market, 2019

VPN failure, admin's real IP

Admins arrested 23–24 April 2019

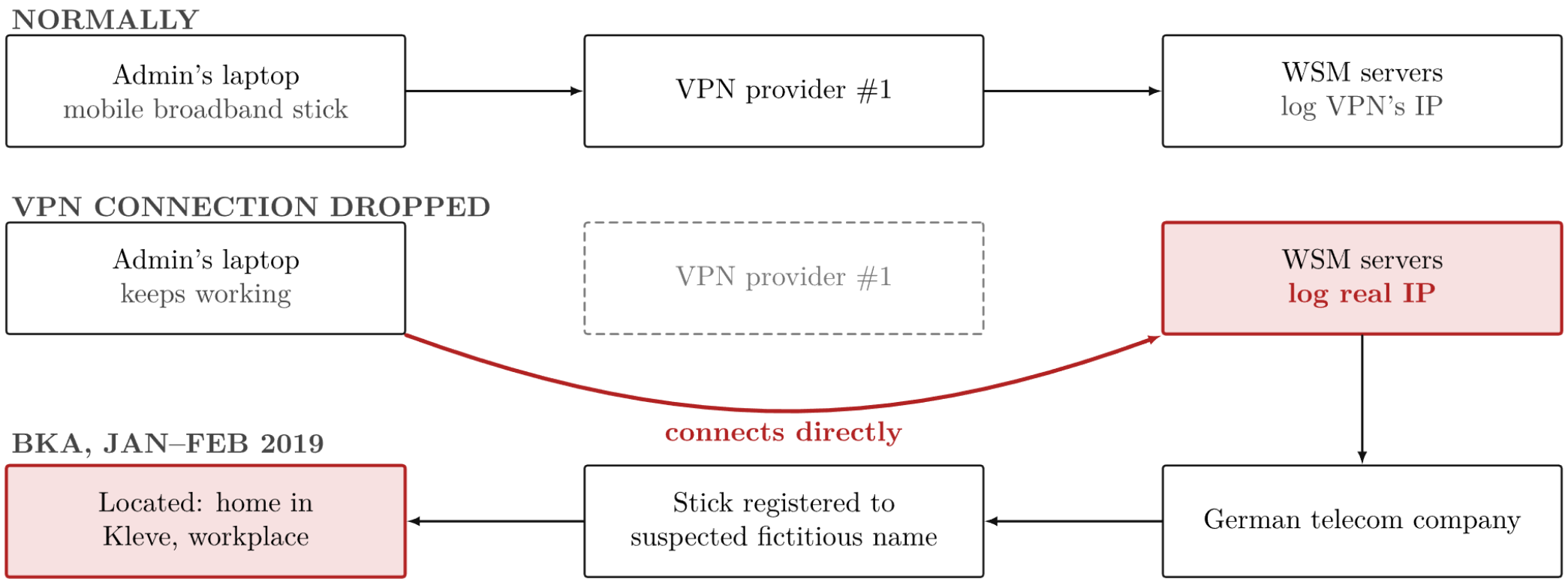


US v. Lousee, Kalla & Frost, complaint, C.D. Cal., May 2019, ¶¶ 23–25; DOJ, 3 May 2019.

Wall Street Market, 2019

VPN failure, admin's real IP

Admins arrested 23–24 April 2019



US v. Lousee, Kalla & Frost, complaint, C.D. Cal., May 2019, ¶¶ 23–25; DOJ, 3 May 2019.

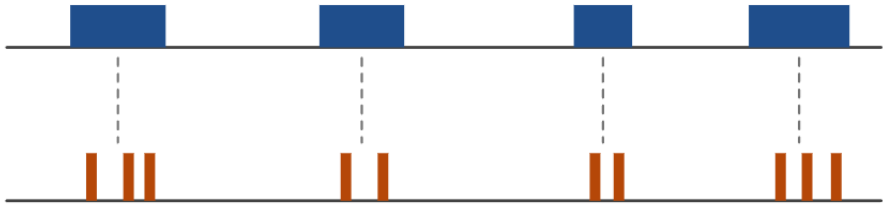
Wall Street Market, 2019

Connection timing, PGP key reuse

Admin “Kronos”: connection timing

his VPN never failed

home line (in his mother’s name)
connects to VPN provider #2



admin-only actions on WSM

times match; later admitted being “Kronos”

US v. Lousee, Kalla & Frost, complaint, C.D. Cal., May 2019, ¶¶ 27–31.

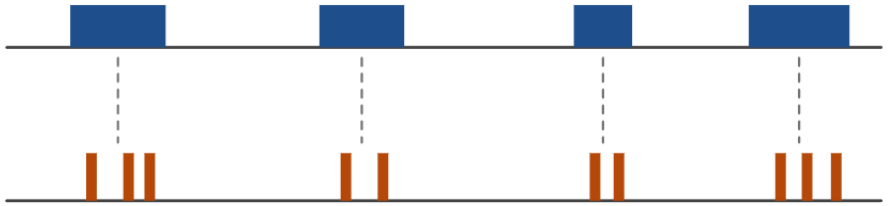
Wall Street Market, 2019

Connection timing, PGP key reuse

Admin “Kronos”: connection timing

his VPN never failed

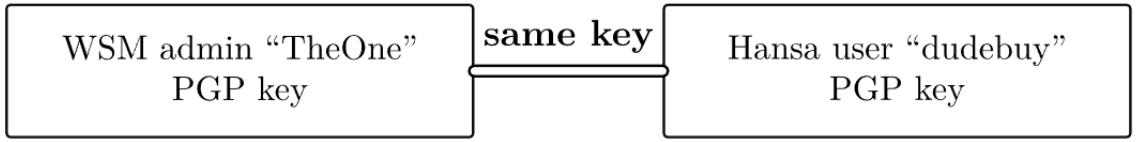
home line (in his mother’s name)
connects to VPN provider #2



admin-only actions on WSM

times match; later admitted being “Kronos”

Admin “TheOne”: PGP key reuse



Hansa data: seized 2017

US v. Lousee, Kalla & Frost, complaint, C.D. Cal., May 2019, ¶¶ 27–31.

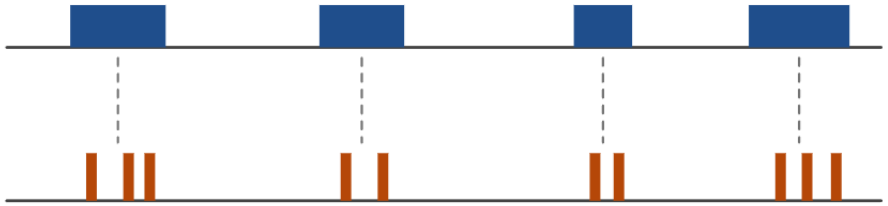
Wall Street Market, 2019

Connection timing, PGP key reuse

Admin "Kronos": connection timing

his VPN never failed

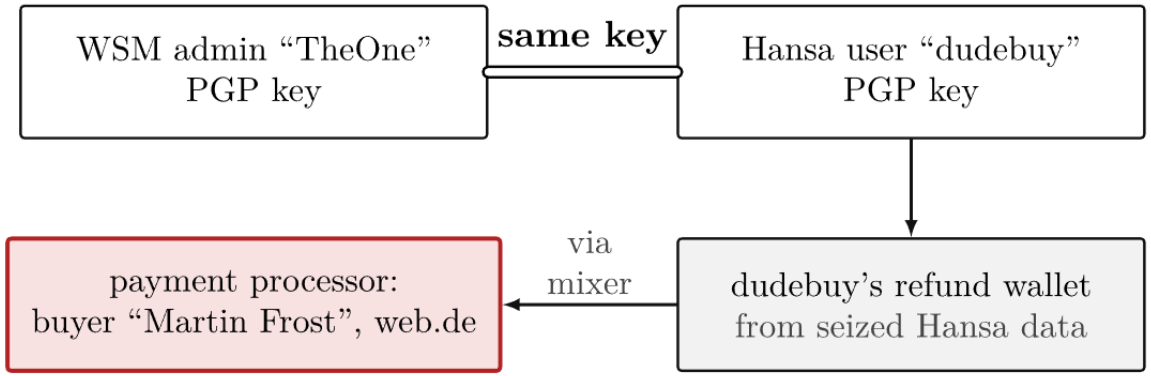
home line (in his mother's name)
connects to VPN provider #2



admin-only actions on WSM

times match; later admitted being "Kronos"

Admin "TheOne": PGP key reuse



Oct 2016: marketing firm paid via processor; gaming accounts tied to his email

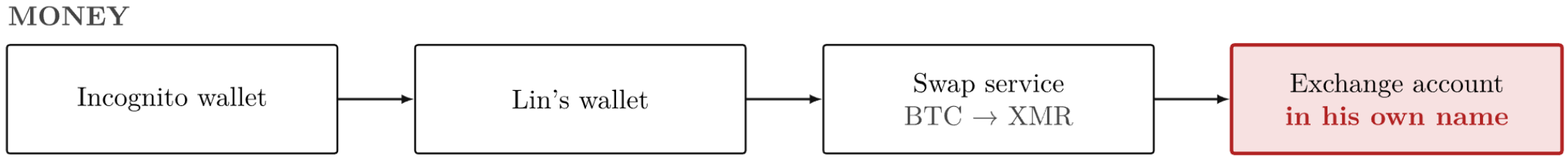
Hansa data: seized 2017

US v. Lousee, Kalla & Frost, complaint, C.D. Cal., May 2019, ¶¶ 27–31.

Incognito Market, 2024

Cryptocurrency exchange KYC records

Pleaded guilty Dec 2024; 30 years, Feb 2026



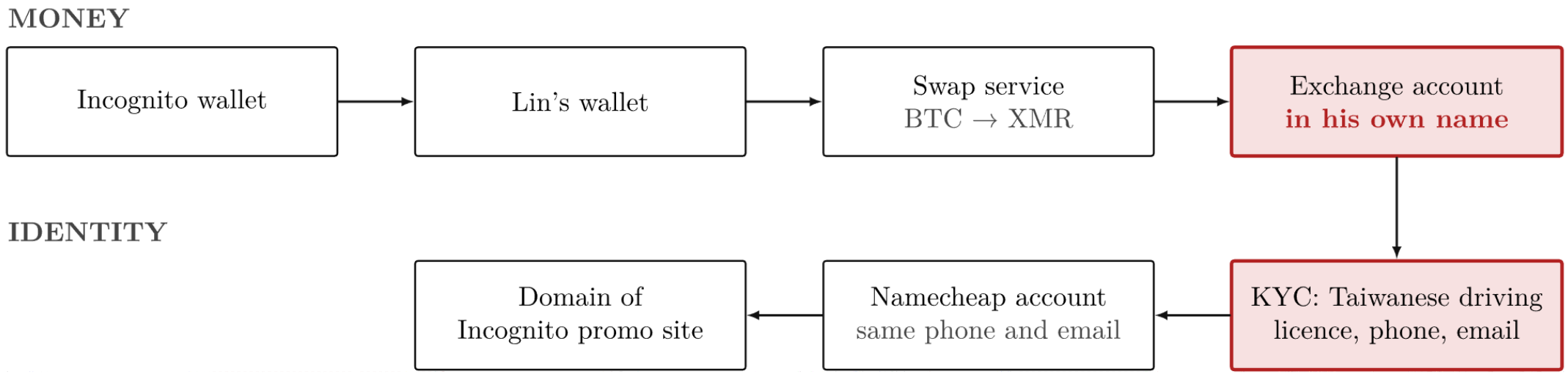
Oct 2020 – Mar 2024; $105M+ in drugs; 400,000+ buyer accounts

DOJ (S.D.N.Y.), May 2024 and 3 Feb 2026; complaint details as reported.

Incognito Market, 2024

Cryptocurrency exchange KYC records

Pleaded guilty Dec 2024; 30 years, Feb 2026



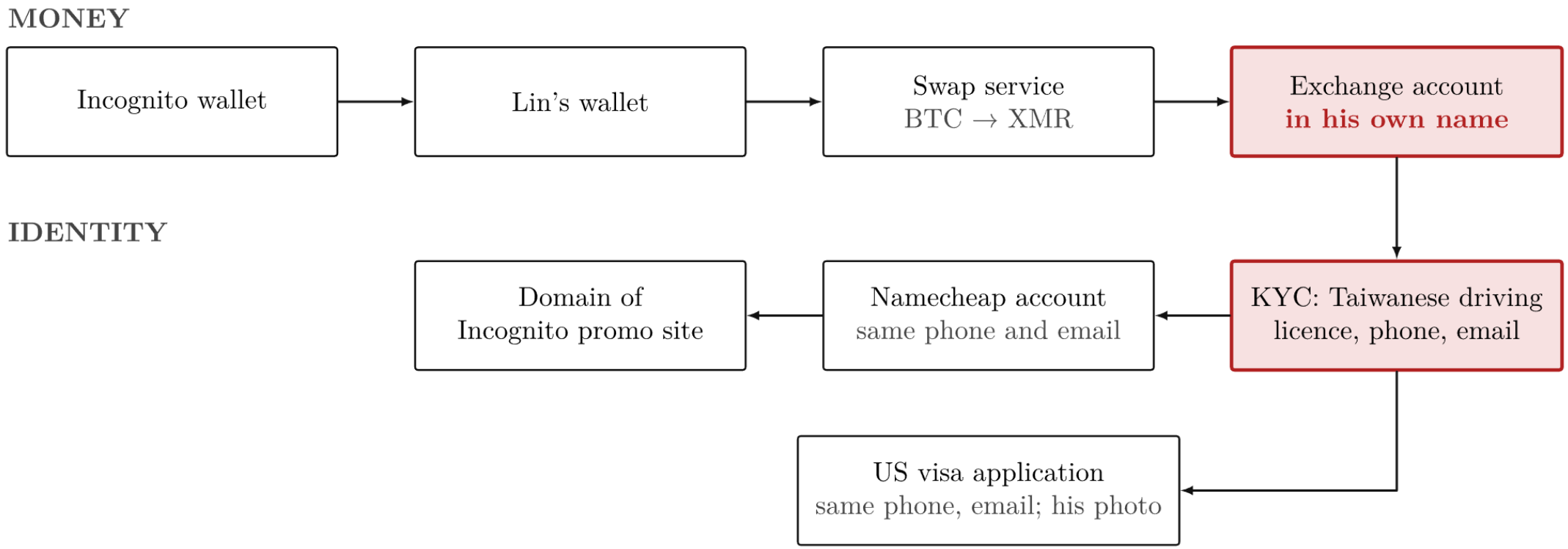
Oct 2020 – Mar 2024; $105M+ in drugs; 400,000+ buyer accounts

DOJ (S.D.N.Y.), May 2024 and 3 Feb 2026; complaint details as reported.

Incognito Market, 2024

Cryptocurrency exchange KYC records

Pleaded guilty Dec 2024; 30 years, Feb 2026



Oct 2020 – Mar 2024; $105M+ in drugs; 400,000+ buyer accounts

DOJ (S.D.N.Y.), May 2024 and 3 Feb 2026; complaint details as reported.

Case summary

Case	Identifying information	Layer
Silk Road, 2013	VPN login records; handles reused since 2011	admin access, identity
AlphaBay, 2017	personal email in site mail headers	configuration
Hansa, 2017	dev server → chat logs; then platform takeover	hosting, platform
Wall Street Market, 2019	dropped VPN, ISP timing, reused PGP key	network, identity
Incognito, 2024	exchange account, domain in his name	money
Bitcoin Fog, 2021	2011 exchange records linked to hosting payments	money

Every case: identifying information from outside the Tor protocol

Thanks

Tim K.

tkudabae@uwaterloo.ca

References

Court filings and official statements

[1] US v. Ulbricht, S.D.N.Y.: complaint, Sept 2013; Tarbell declaration, Sept 2014; suppression ruling, Oct 2014.

[2] US v. Cazes, civil forfeiture complaint, E.D. Cal., Jul 2017; DOJ, 20 Jul 2017.

[3] US v. Lousee, Kalla & Frost, complaint, C.D. Cal., May 2019; DOJ and BKA, 3 May 2019.

[4] US v. Rui-Siang Lin, S.D.N.Y.: DOJ, May 2024 and 3 Feb 2026.

[5] US v. Farrell, W.D. Wash., order of 23 Feb 2016.

[6] Bitcoin Fog: DOJ, 8 Nov 2024. Samourai Wallet: DOJ, 19 Nov 2025.

[7] Dutch National Police and Europol on Hansa, 20 Jul 2017; Europol on DisrupTor (Sep 2020) and RapTor (May 2025).

Background

[8] “How Tor Works: building it up from the ordinary internet” (handout); spec.torproject.org.

[9] Tor Project, “relay early” traffic confirmation attack advisory, 30 Jul 2014.

[10] Tor Project, Arti 2.5.0 release notes (Counter Galois Onion), 30 Jun 2026.

[11] A. Greenberg, “Operation Bayonet”, Wired, Mar 2018; Tracers in the Dark, 2022.

[12] Meiklejohn et al., “A Fistful of Bitcoins”, IMC 2013.

[13] Möser et al., “An Empirical Analysis of Traceability in the Monero Blockchain”, PoPETs 2018.

[14] R. Graham, Errata Security, Oct 2014; Malwarebytes, Apr 2019; ZDNet, May 2019; AFP and DCD on the Cyberbunker, 2019–21.