KERI

Key Event Receipt Infrastructure

The Economics of Its & Bits

Digital Identity

Freedom Privacy Control Security

Core Public Utility Technology Forum
Dynamic Data Economy
2020/09/10
Samuel M. Smith Ph.D.
sam@samuelsmith.org

some graphics from flatiron.com or freepik.com

Image courtesy of 1zoom.me https://www.1zoom.me/en/wallpaper/343518/z3749.9/&original=1
Drawing of photo courtesy of Wallpaper Safari ttps://wallpapersafari.com/w/wFYJpS

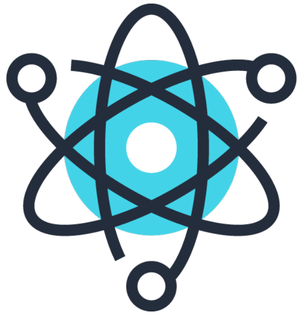
Economics

value — creation and capture

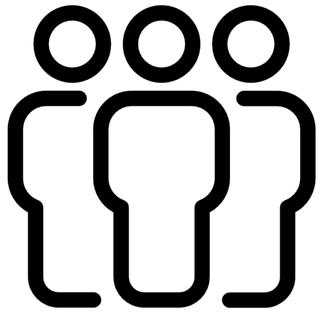
$\frac{\text{control}}{\text{value}}$ — extraction, exchange, and exploitation

security

its



atoms



physical security

control

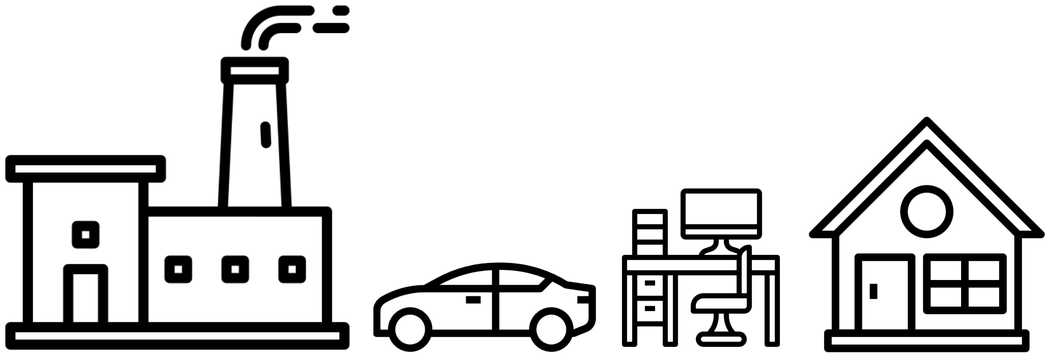
value

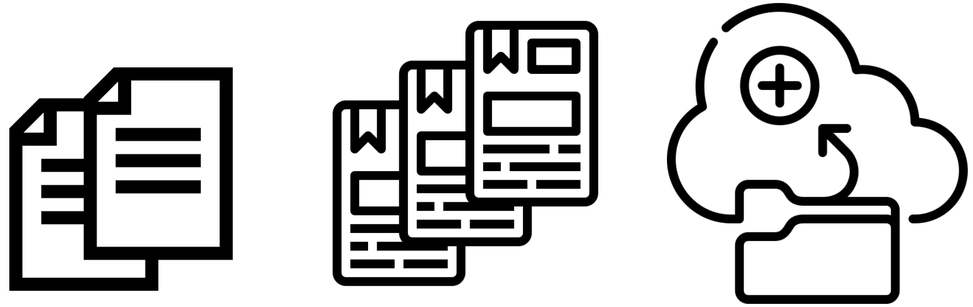
bits

digital information

Informational security

security?





60 Years of Its & Bits

Revenue

1960

1960 Fortune 20 Revenue

Rank	Company	Revenues ($ millions)
1	General Motors	11,233
2	Exxon Mobil	7,911
3	Ford Motor	5,357
4	General Electric	4,350
5	U.S. Steel	3,643
6	Mobil	3,093
7	Gulf Oil	2,713
8	Texaco	2,678
9	Chrysler	2,643
10	Esmark	2,476
11	AT&T	2,315
12	DuPont	2,114
13	Bethlehem Steel	2,056
14	Amoco	1,957
15	CBS	1,911
16	Armour	1,870
17	General Dynamics	1,812
18	Shell Oil	1,810
19	Boeing	1,612
20	Kraft	1,606

1980

1980 Fortune 20 Revenue

Rank	Company	Revenues ($ millions)
1	Exxon Mobil	79,107
2	General Motors	66,311
3	Mobil	44,721
4	Ford Motor	43,514
5	Texaco	38,350
6	ChevronTexaco	29,948
7	Gulf Oil	23,910
8	IBM	22,863
9	General Electric	22,461
10	Amoco	18,610
11	ITT Industries	17,197
12	Atlantic Richfield	16,234
13	Shell Oil	14,431
14	U.S. Steel	12,929
15	Conoco	12,648
16	DuPont	12,572
17	Chrysler	12,002
18	Tenneco Automotive	11,209
19	AT&T	10,964
20	Sunoco	10,666

2000

2000 Fortune 20 Revenue

Rank	Company	Revenues ($ millions)
1	General Motors	189,058
2	Wal-Mart Stores	166,809
3	Exxon Mobil	163,881
4	Ford Motor	162,558
5	General Electric	111,630
6	IBM	87,548
7	Citigroup	82,005
8	AT&T	62,391
9	Altria Group	61,751
10	Boeing	57,993
11	Bank of America Corp.	51,392
12	SBC Communications	49,489
13	Hewlett-Packard	48,253
14	Kroger	45,352
15	State Farm Insurance Cos	44,637
16	Sears Roebuck	41,071
17	American Intl. Group	40,656
18	Enron	40,112
19	TIAA-CREF	39,410
20	Compaq Computer	38,525

2020

2020 Fortune 20 Revenue

Rank	Company	Revenues ($ millions)
1	Walmart	523,964
2	Amazon.com	280,522
3	Exxon Mobil	264,938
4	Apple	162,558
5	CVS Health	256,776
6	Berkshire Hathaway	256,776
7	UnitedHealth Group	242,155
8	McKesson	214,319
9	AT&T	181,193
10	AmerisourceBergen	179,589
11	Alphabet	161,857
12	Ford Motor	155,900
13	Cigna	153,566
14	Costco Wholesale	152,703
15	Chevron	146,516
16	Cardinal Health	145,534
17	JPMorgan Chase	142,422
18	General Motors	137,237
19	Walgreens Boots Alliance	136,866
20	Verizon	131,868

Market Value

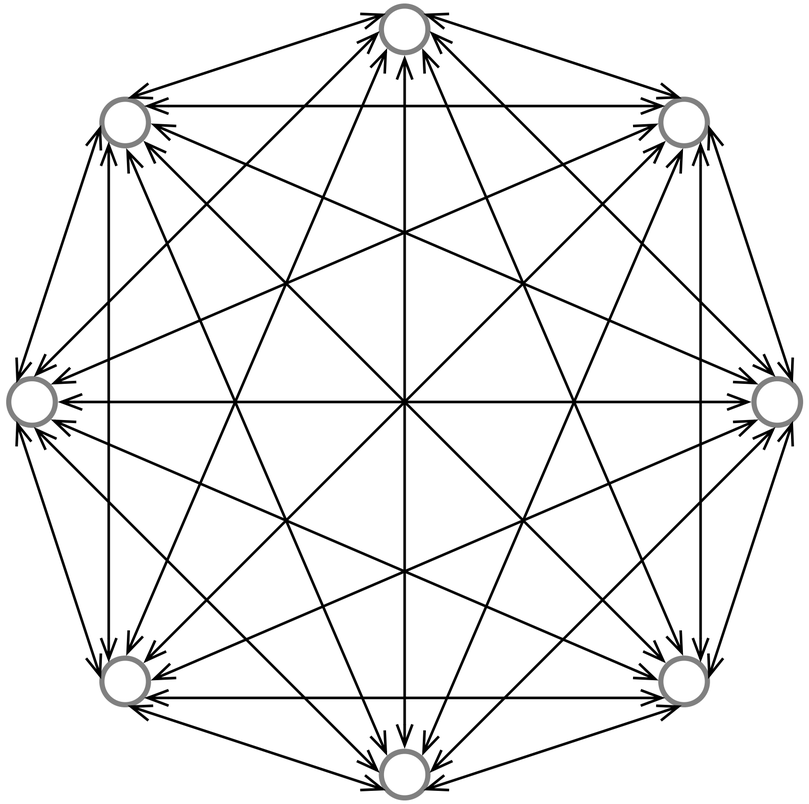
2020

2020 Fortune 20 Market Value

Rank	Company	Market Value ($ millions)
1	Microsoft	1,199,550
2	Apple	1,112,641
3	Amazon.com	970,680
4	Alphabet	798,905
5	Facebook	475,455
6	Berkshire Hathaway	442,897
7	Johnson & Johnson	345,705
8	Walmart	321,803
9	Visa	316,199
10	JPMorgan Chase	276,750
11	Procter & Gamble	271,640
12	Mastercard	242,794
13	UnitedHealth Group	236,555
14	Intel	231,662
15	Verizon	222,220
16	AT&T	209,388
17	Home Depot	200,665
18	Merck	195,141
19	Coca-Cola	189,983
20	Bank of America	185,227

Networks Effects

Network scaling law: How network value scales with number of participants.



Value = Reach

Metcalfe's Law

$$v = a \cdot N$$

$$V = a \cdot N \cdot N = a \cdot N^2$$

https://medium.com/selfrule/meta-platforms-and-cooperative-network-of-networks-effects-6e61eb15c586

How do we *recapture* the value in our data?

1- Retake control of our data

2- Leverage cooperative network effects

Retake control of our data

Human *Basis-of-Trust*

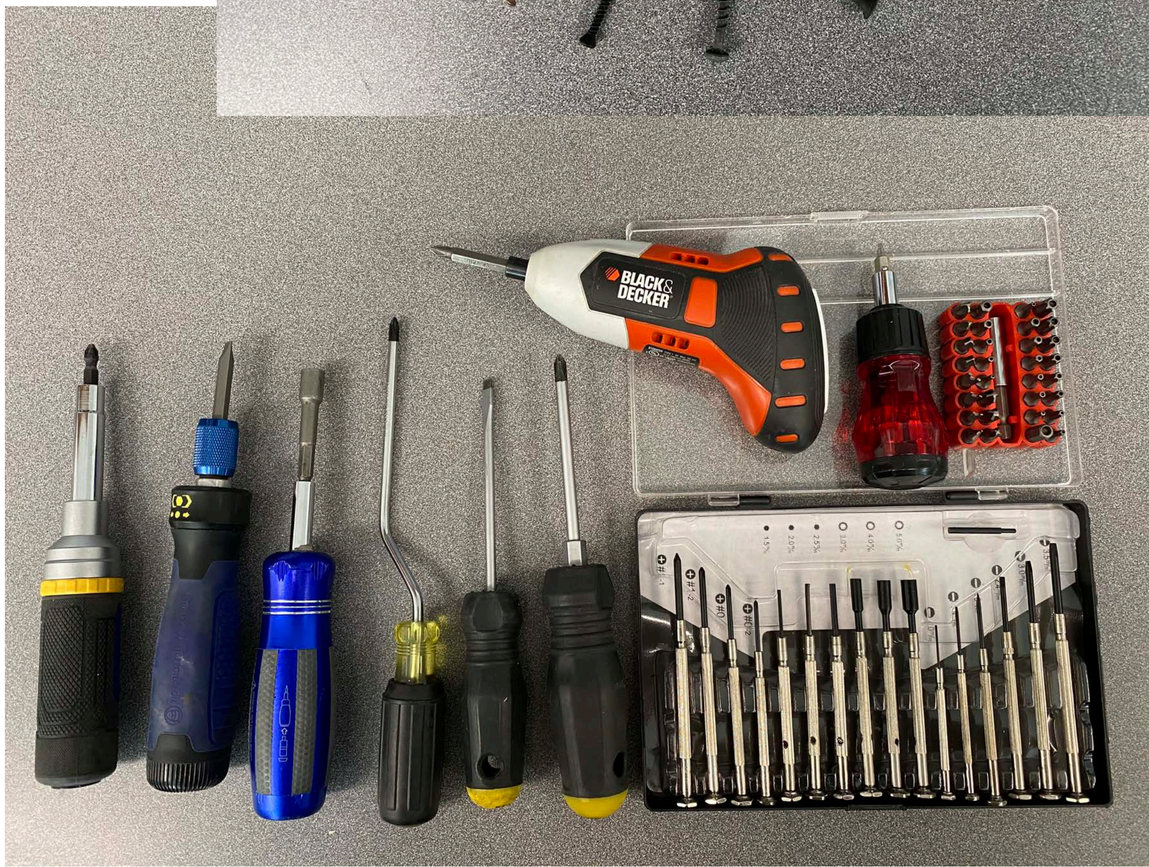
“in person”

I can know you – therefore I can trust you

“on the internet”

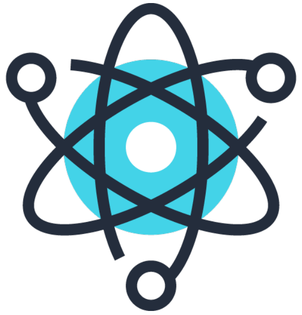
I can’t really know you – therefore I can’t really trust you

Toolkits



Only have one set of tools for truly secure data control!

its

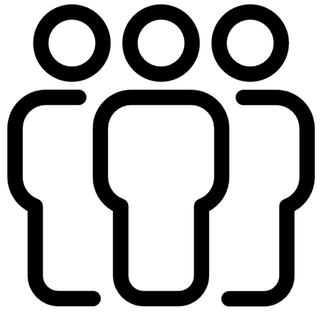


bits

control

value

atoms



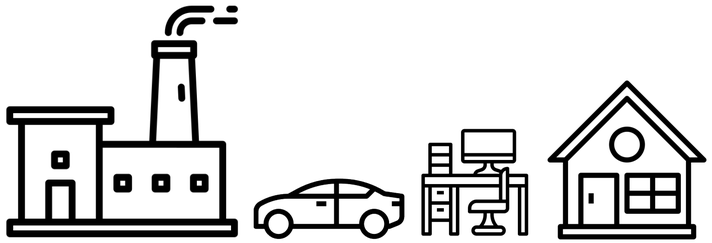
physical security

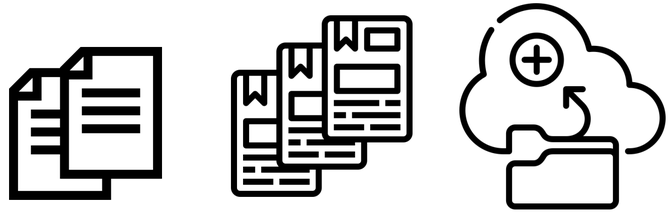
digital uniqueness

Entropy

digital information

Informational security





Entropy Derived Tools

Cryptographic one-way functions …

hashes, ECC scalar multiplication…
digital signatures, ZKPs …

Information uniqueness from captured entropy

To retake control of our data we must first retake control of our identifiers.

self-certifying pseudonymous identifiers

Key Event Receipt Infrastructure (KERI)

https://arxiv.org/abs/1907.02143

Replace human *basis-of-trust* with cryptographic *root-of-trust.*

With verifiable digital signatures from asymmetric key crypto –
we may not trust in "*what*" was said, but we may trust in "*who*" said it.

We may *verify* that the *controller* of a private key, (*the who*), made a statement
but not the validity of the statement itself.

The *root-of-trust* is *consistent attribution* via verifiable integral non-repudiable statements

We may build trust over time in *what* was said via histories
of verifiably attributable (to *whom*) consistent statements i.e. *reputation*.

Four A's of Secure Data Control

Author: creator, source-of-truth
Authentic: provable origin, root-of-trust
Authorized: consent, loci-of-control
Authoritative: accurate, reputable

A^4 data control securely established via self-certifying pseudonymous identifiers

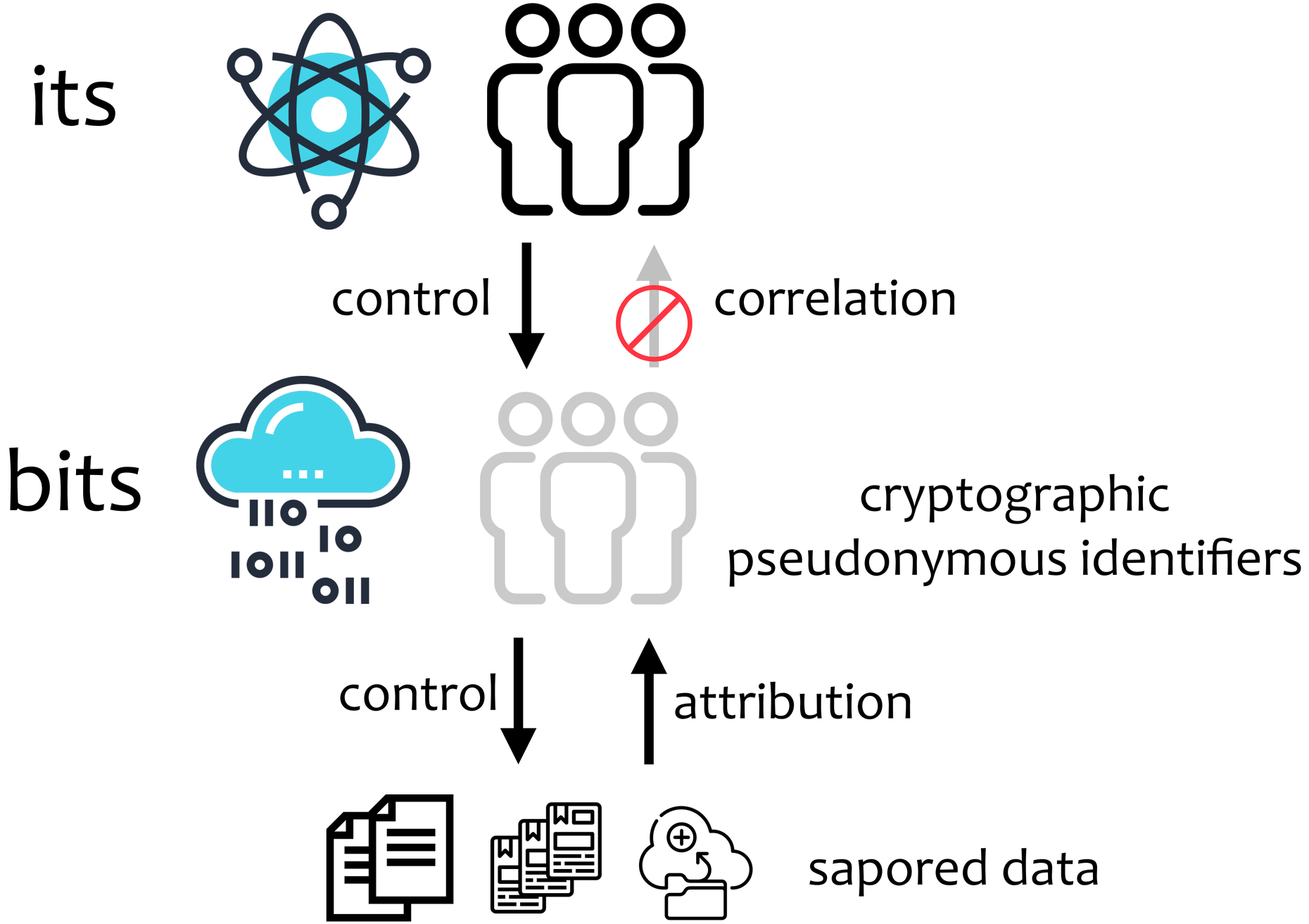
Sapored Data

Sapor: *noun*

the quality in a substance that affects the sense of taste; savor; flavor.

Sapored data may be securely provenanced to its author(s).
Sapored data value extraction may be securely attributed to its authors.

Sapored data supply chains.
Enable consumer pull in addition to regulatory push.
Conscious consumers of *Sapored data* drive compliance.
Circular data economy network effects.


its
control
correlation
bits
cryptographic
pseudonymous identifiers
control
attribution
sapored data

Strong

Weak

Privacy?

Weak

Strong Privacy

un-correlated interactions over *unbounded* time and space.

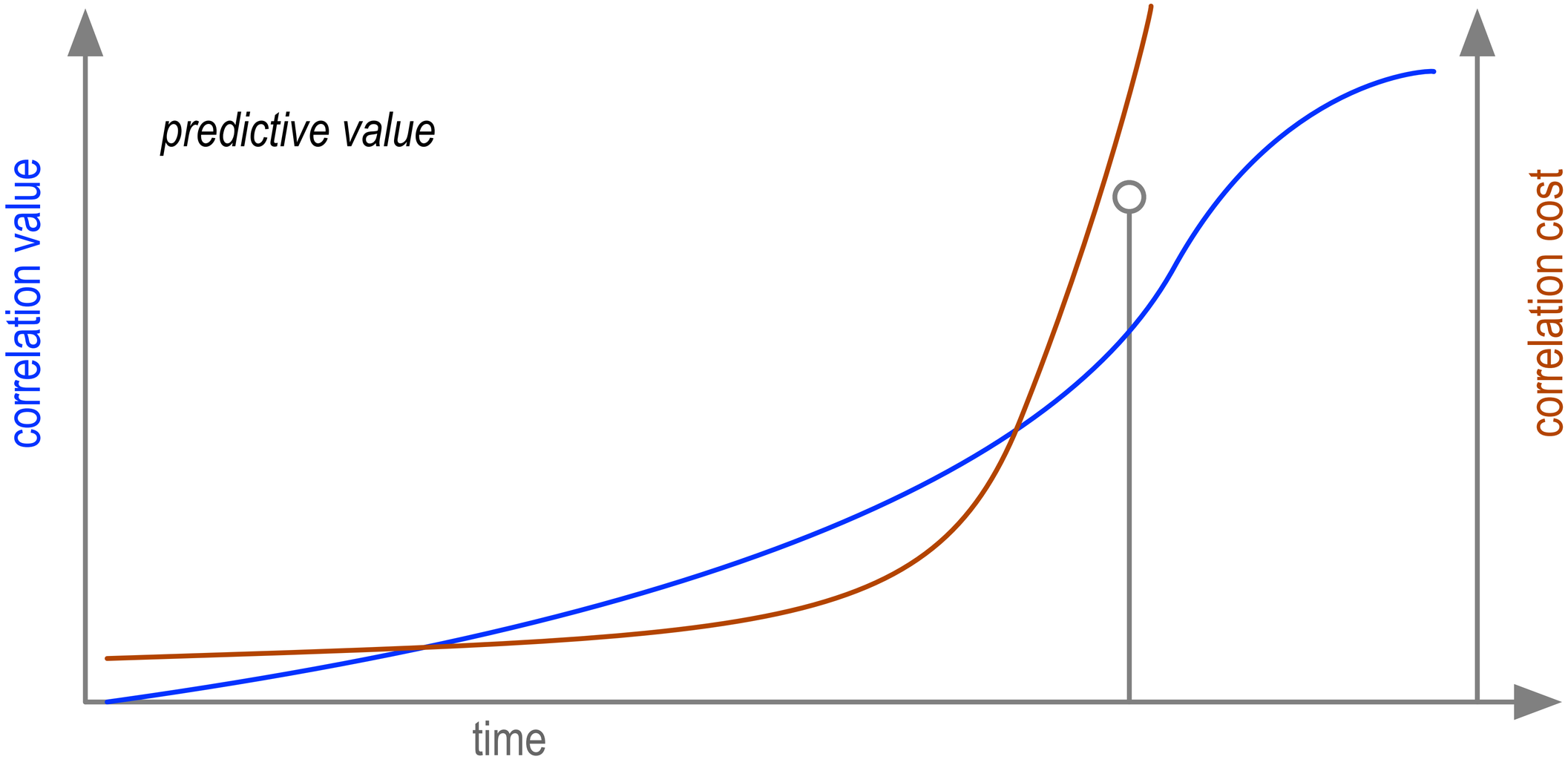
Super aggregators and state actors have effectively unlimited storage and compute capacity. Eventually all disclosed data will be at least statistically correlatable.

Weak Privacy

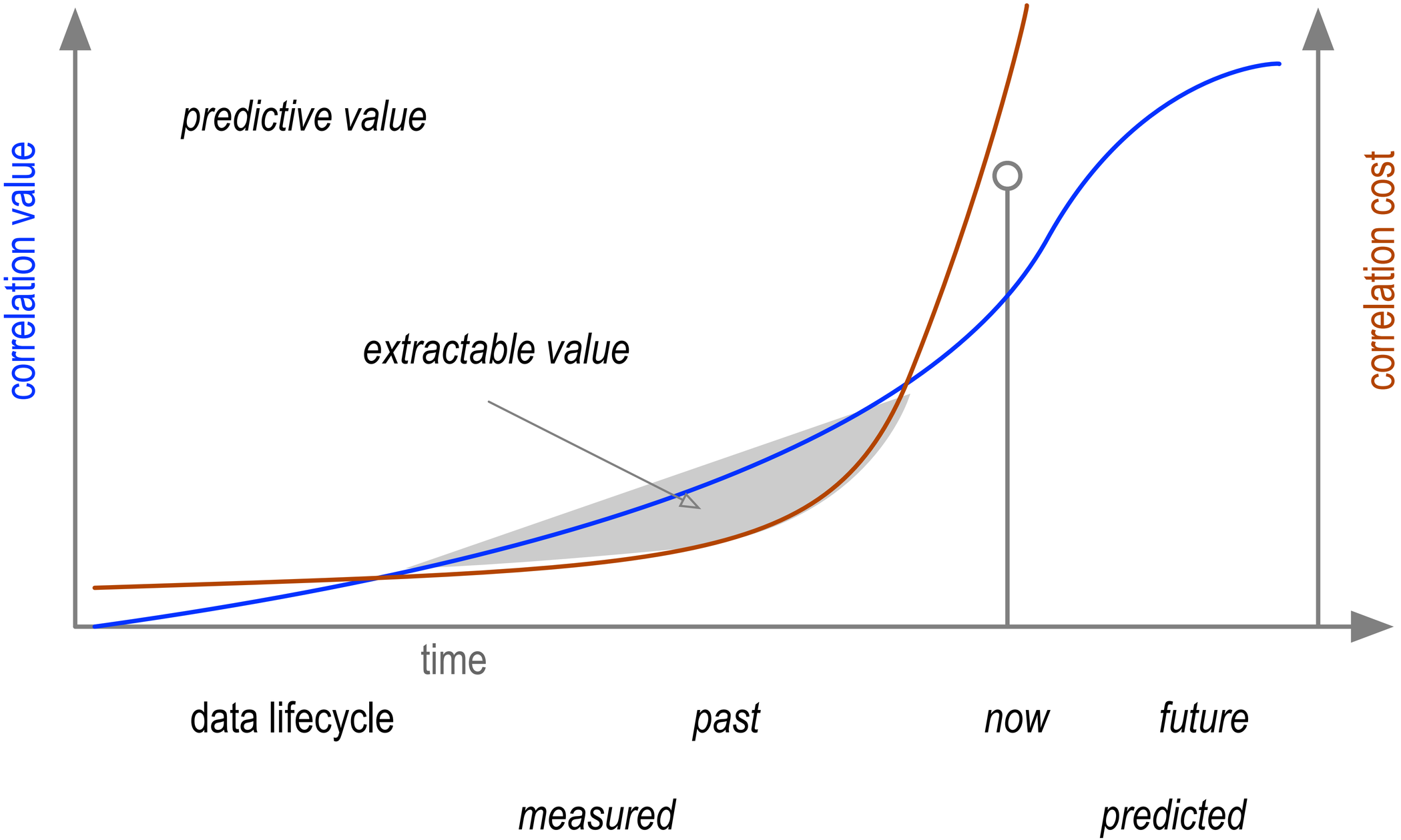
un-correlated interactions over *bounded* time and space.

When the cost of correlation exceeds the value of correlation the data will become un-correlated (de-correlated).

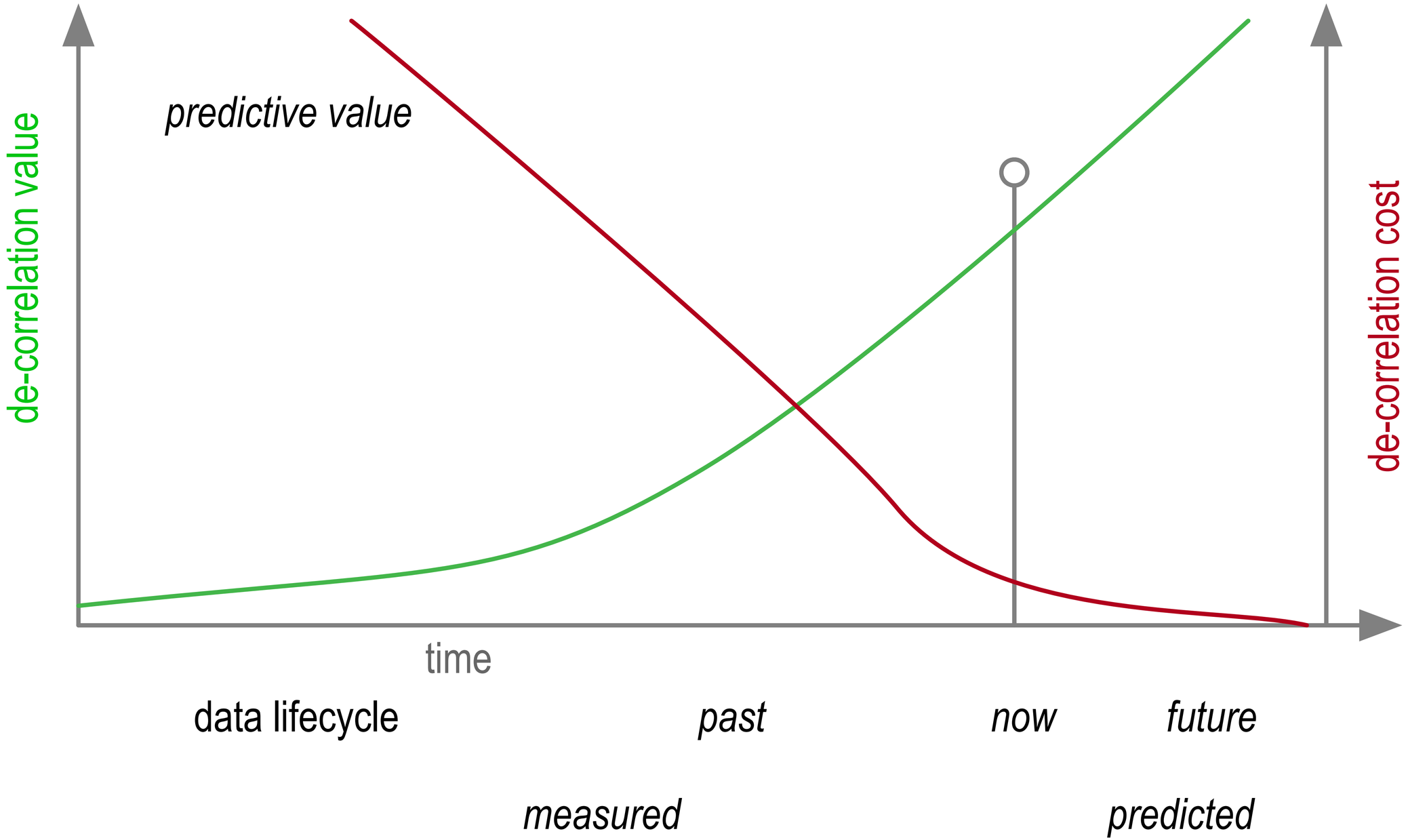
Economics of Correlator



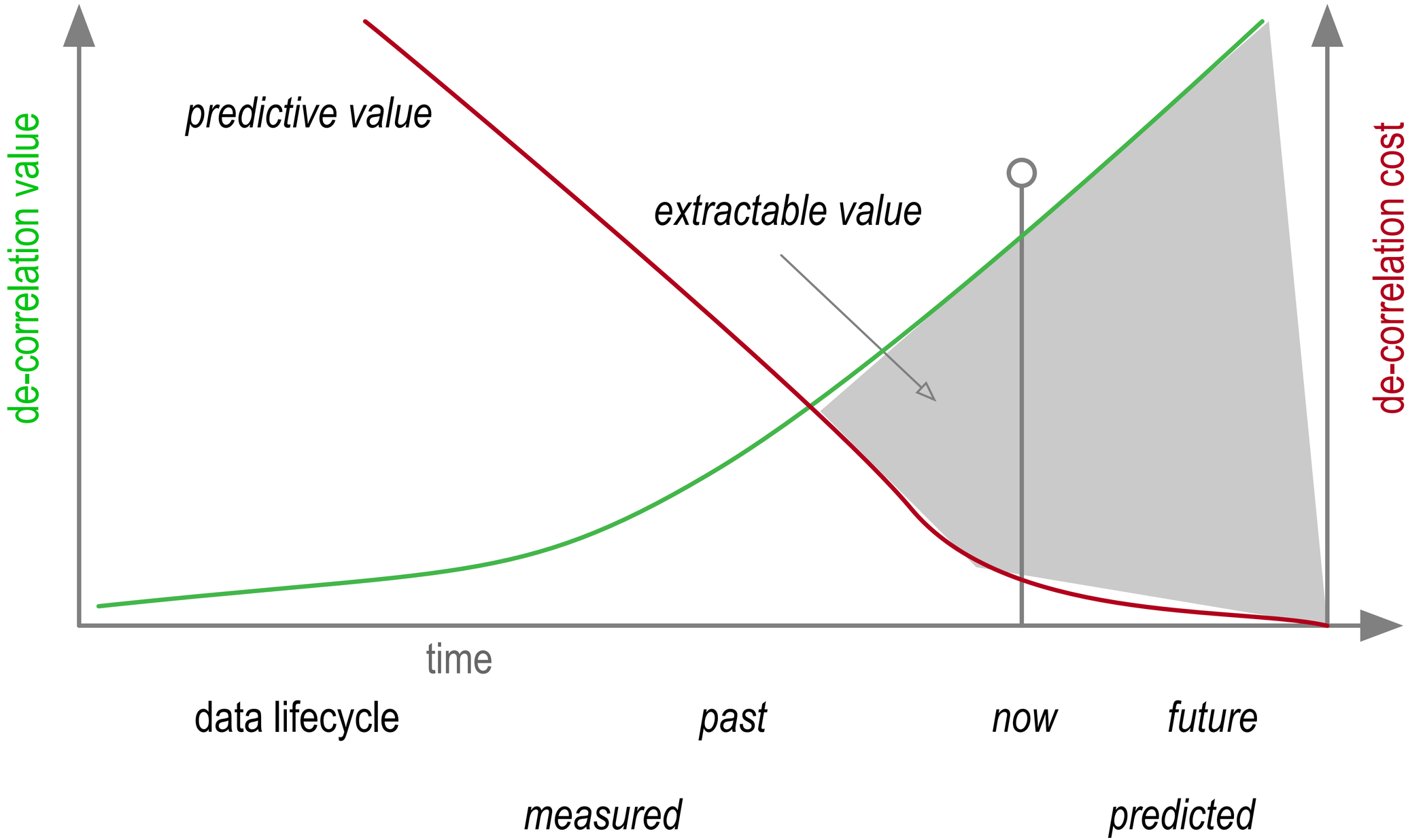
Economics of Correlator: Value Extraction



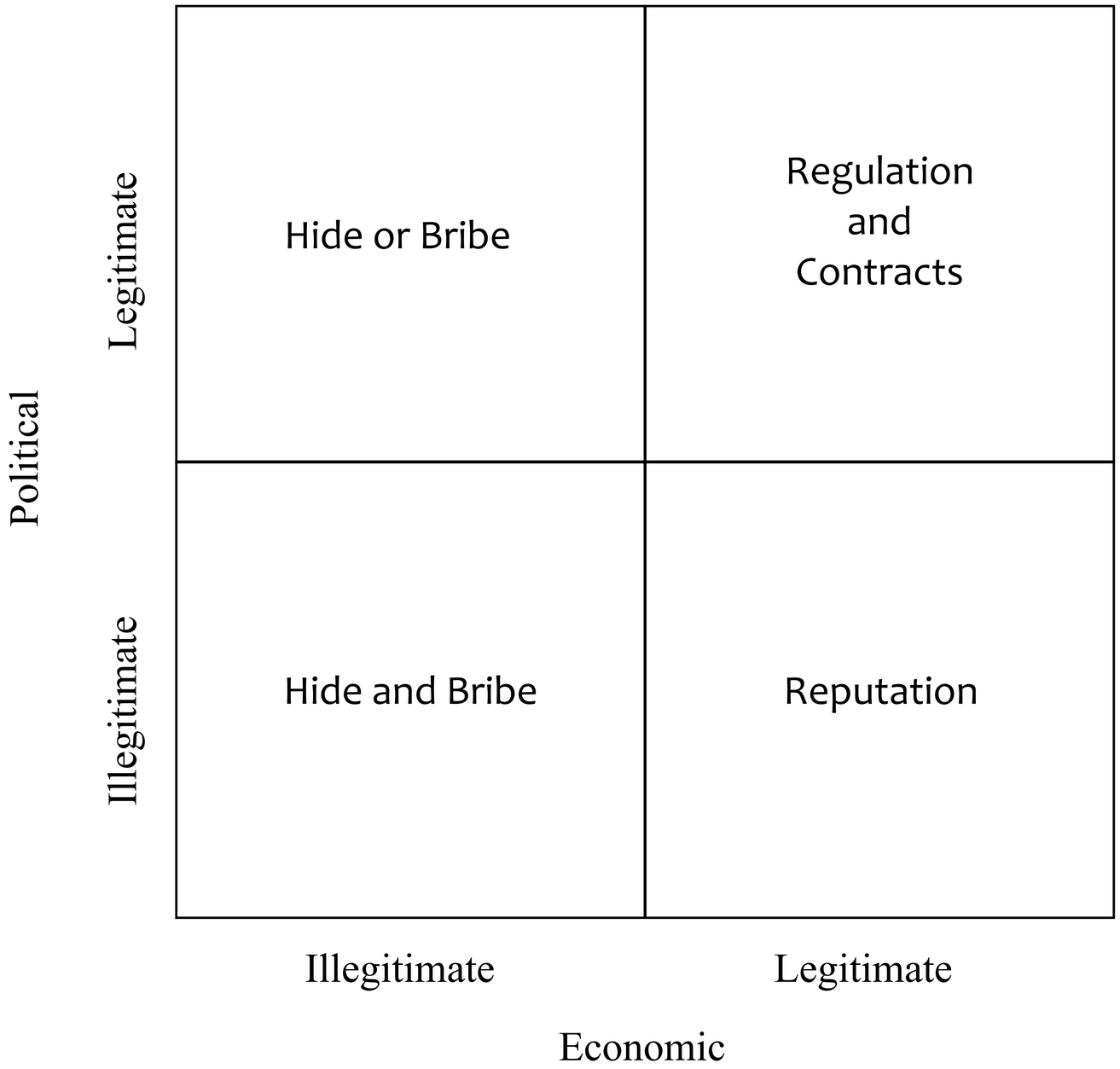
Economics of De-correlator



Economics of De-correlator: Value Extraction



Operating Regimes



Freedom

balanced

Freedom from …	Freedom to …
exploitation (commercial)	extract value(commercial)
intimidation (political)	build relationships (social)
censorship (political)	build community (political)

possibility of erasure = possibility of censorship

anonymity = loss-of-value from attribution

fairness = requires data attribution

Solution

A4 Pseudonymity

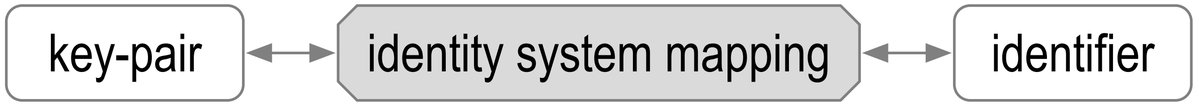
Ledger-less Identity
“*truly decentralized*”

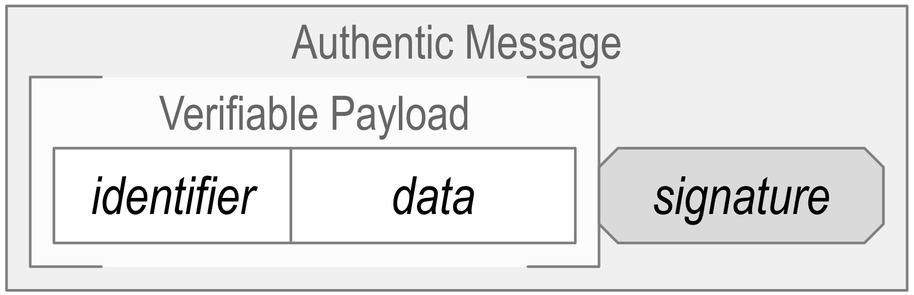
Separable Identifier Trust Bases
“truly forgettable”

KERI

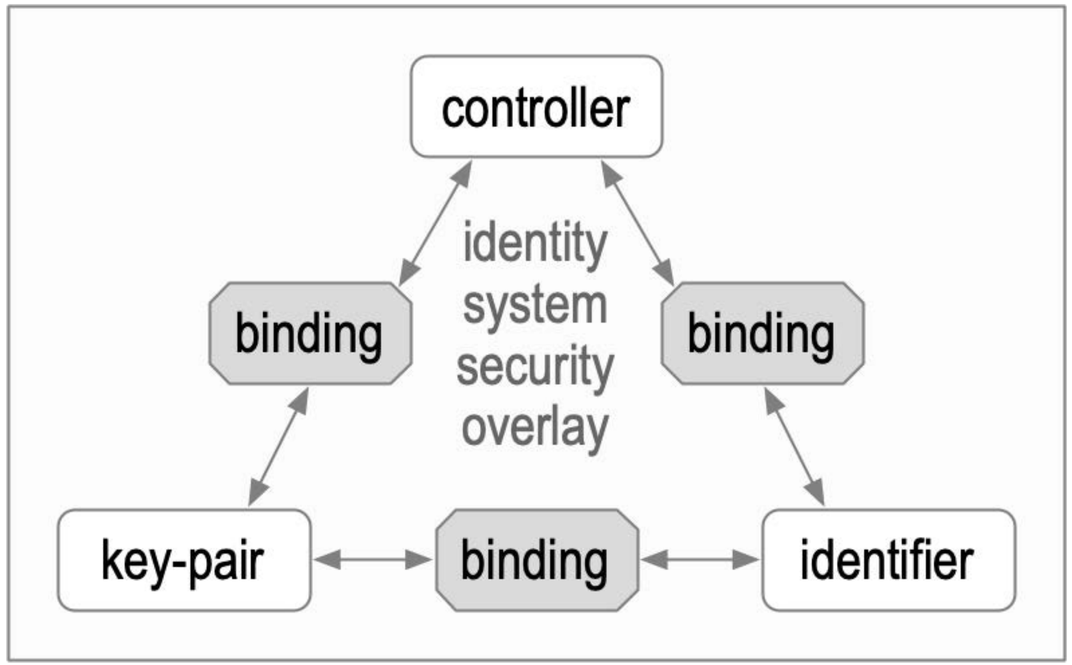
Identity System Security Overlay

Establish authenticity of IP packet's message payload.



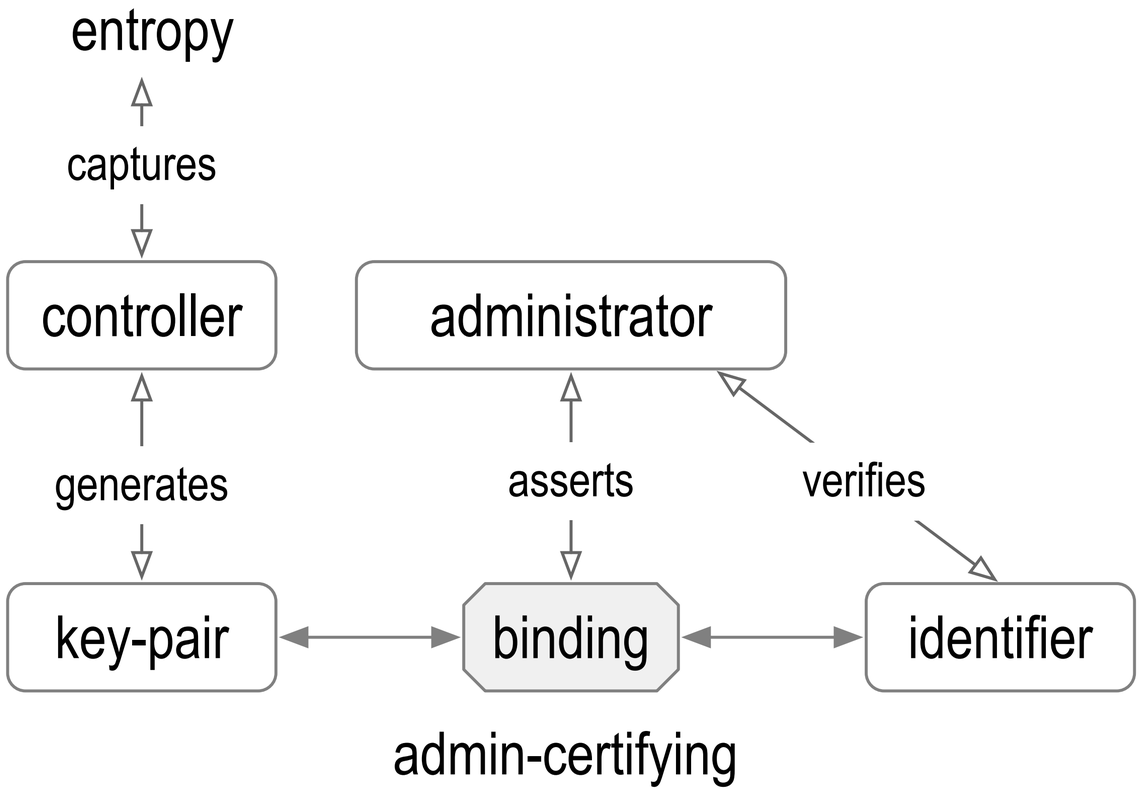


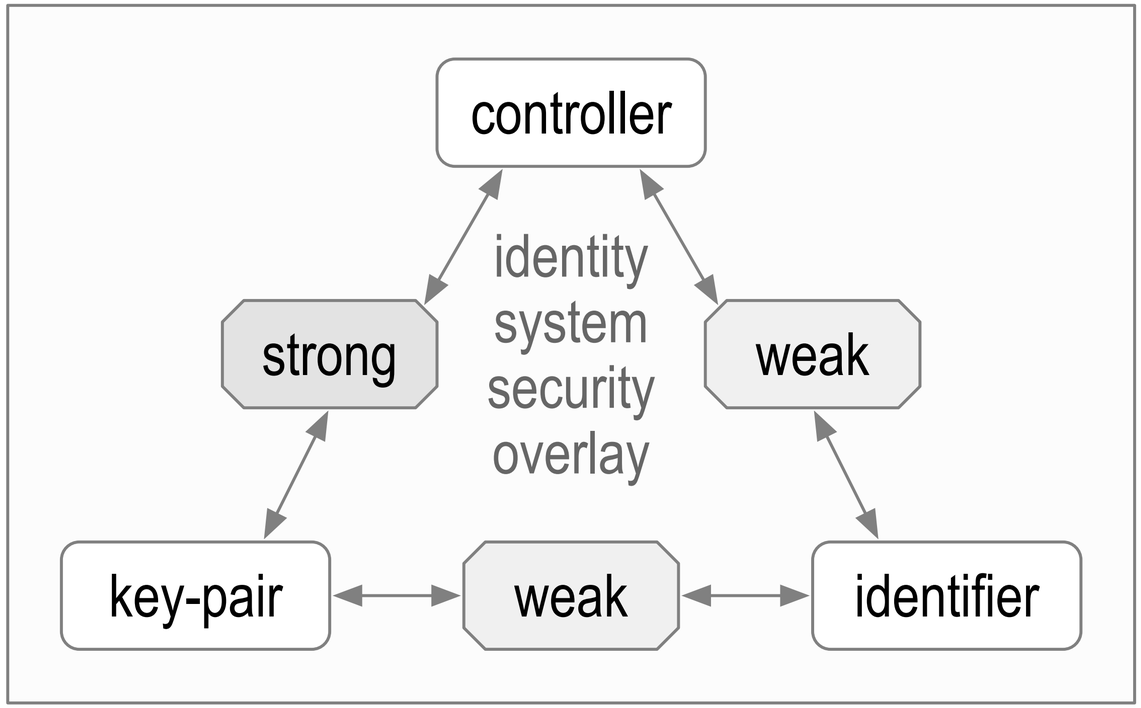
The overlay's security is contingent on the mapping's security.



Identifier Issuance

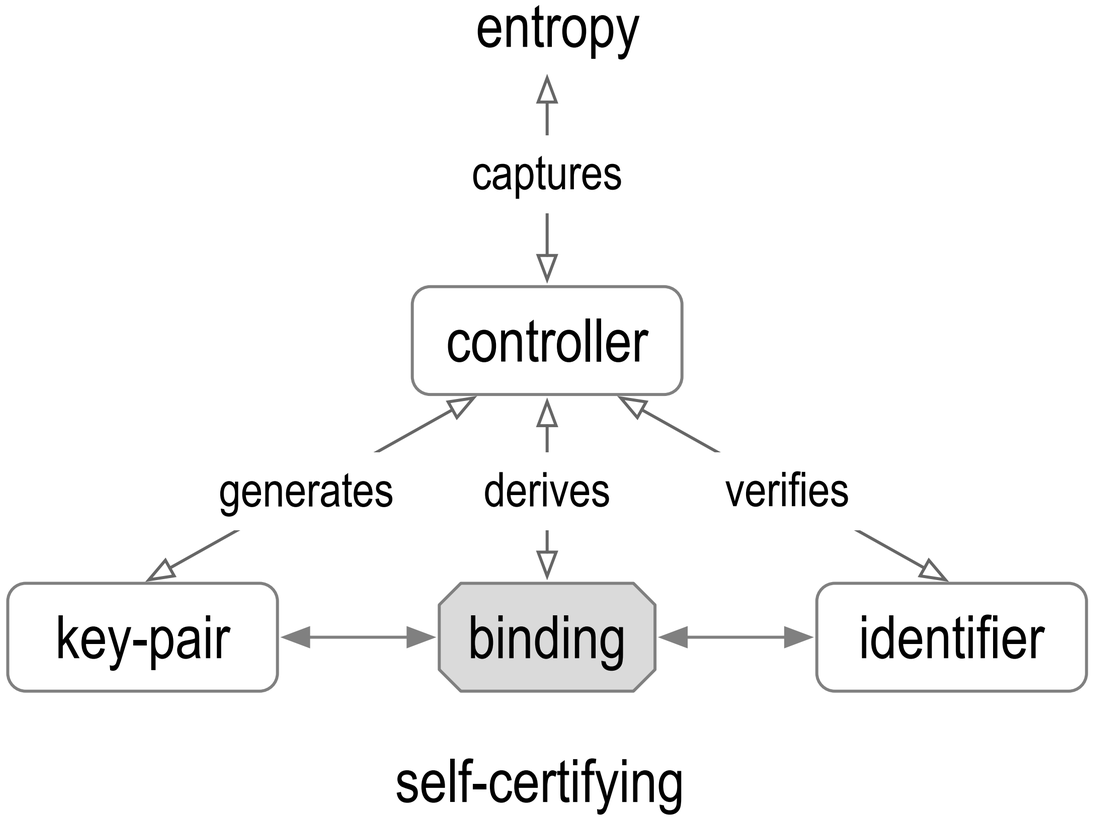
Administrative Identifier Issuance and Binding

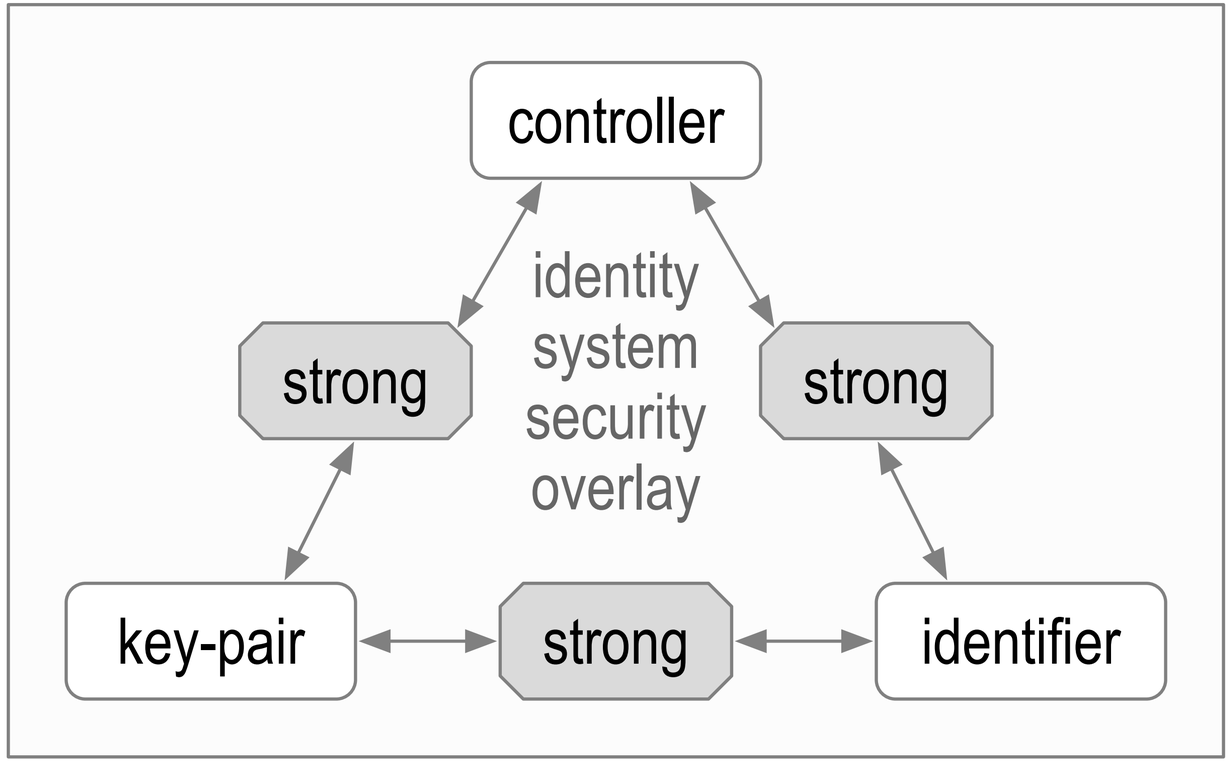




Admin-Certifying Identifier Issuance

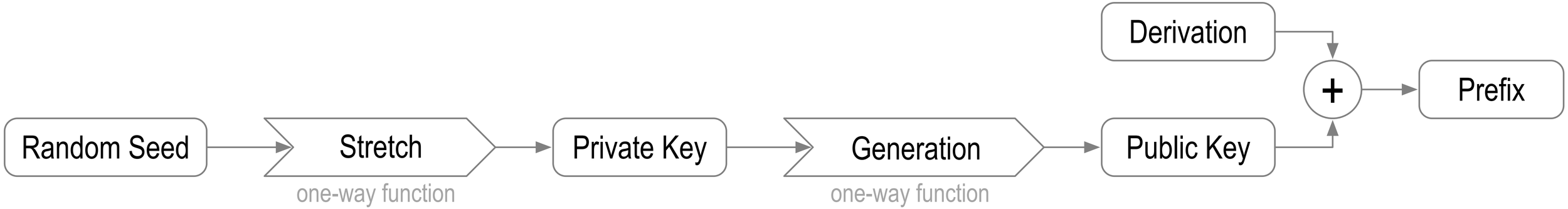
Self-Certifying Identifier Issuance and Binding

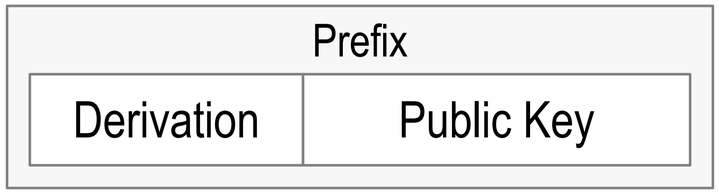


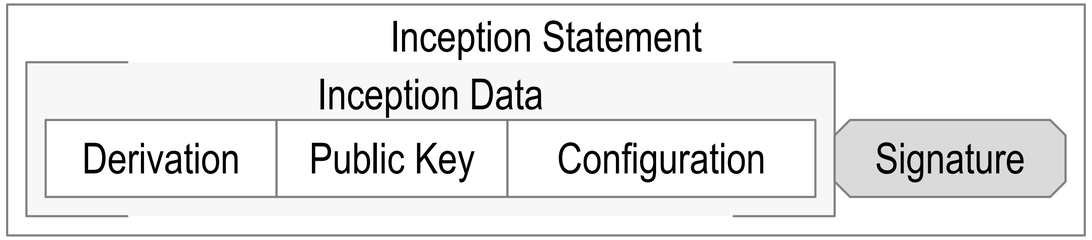


Self-Certifying Identifier Issuance

Basic SCID



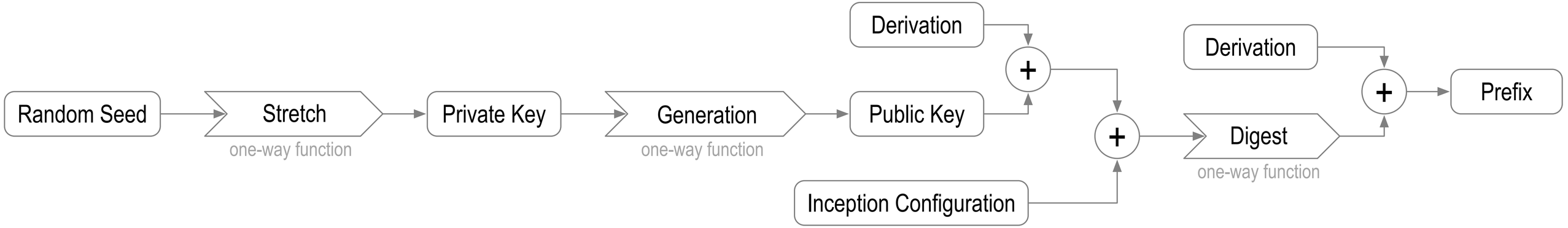


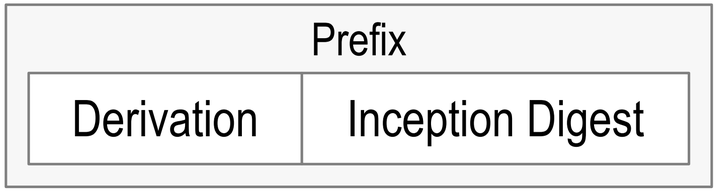


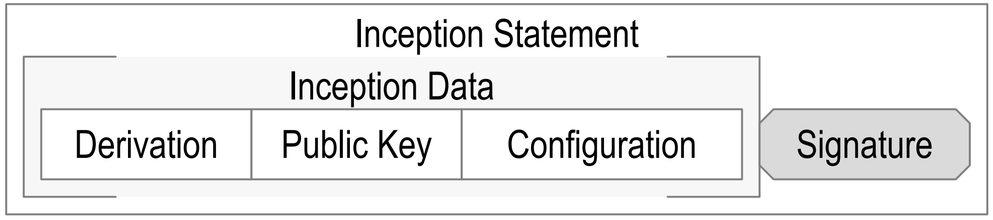
`BDKrJxkcR9m5u1xs33F5pxRJP6T7hJEbhpHrUtlDdhh0`

`did:un:BDKrJxkcR9m5u1xs33F5pxRJP6T7hJEbhpHrUtlDdhh0/path/to/resource?name=secure#really`

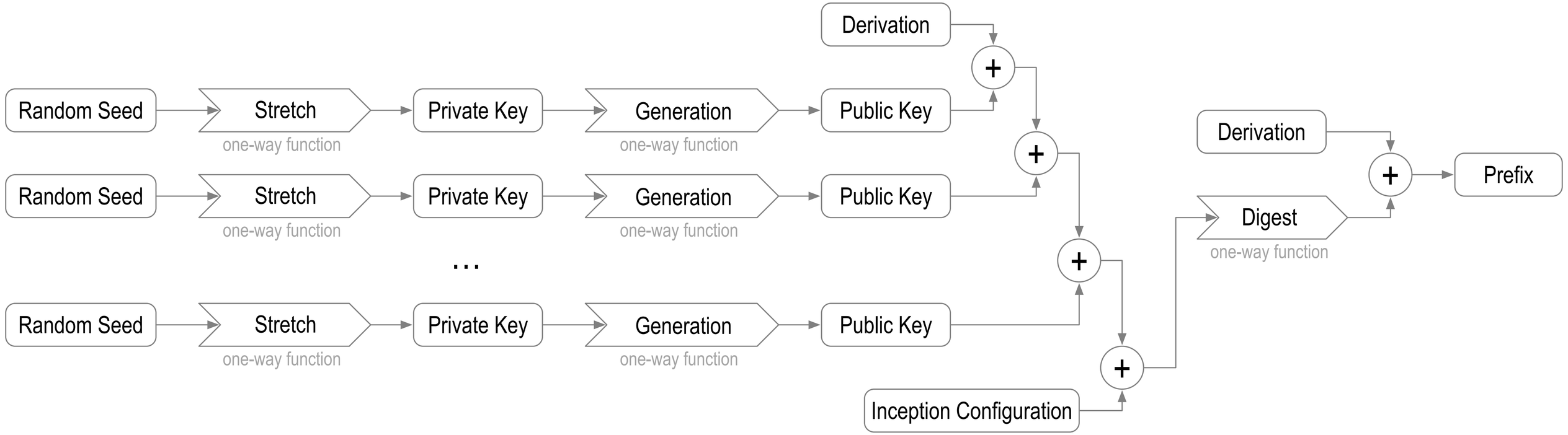
Self-Addressing SCID

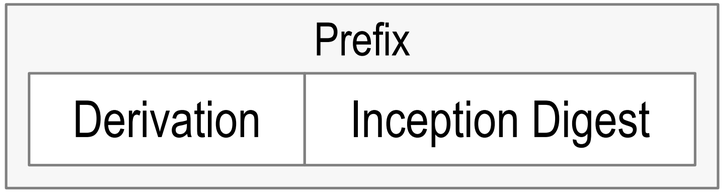


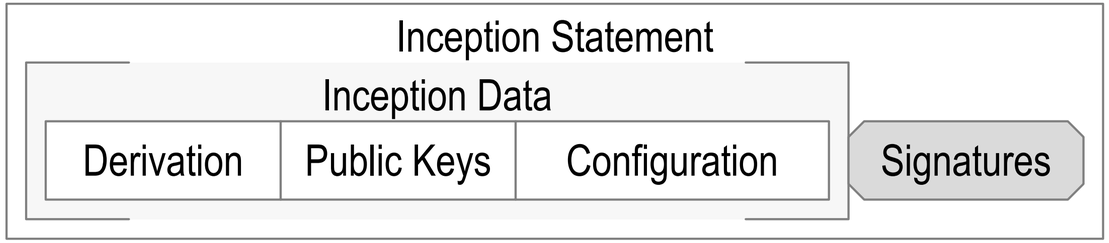




Multi-Sig Self-Addressing



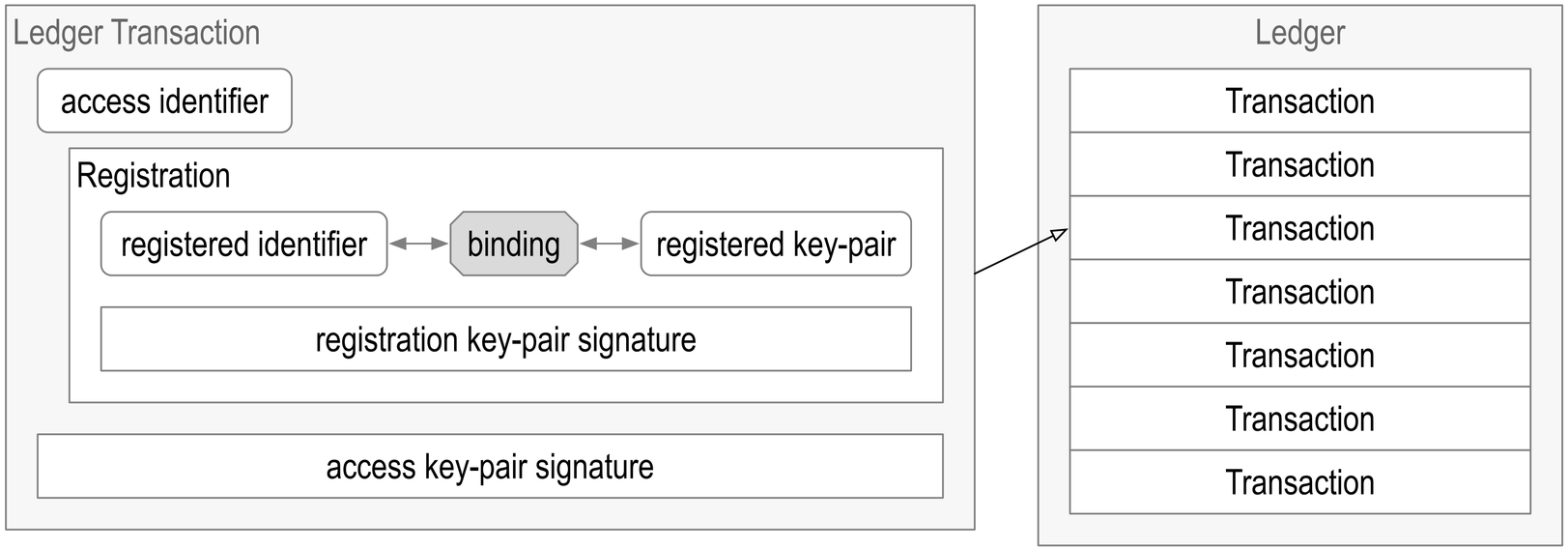


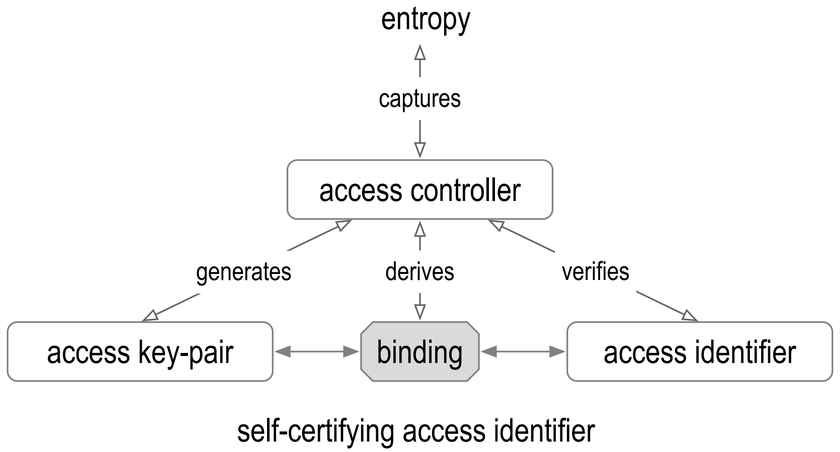


EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148

did:un:EXq5YqaL6L48pf0fu7IUhL0JRaU2_RxFP0AL43wYn148/path/to/resource?name=secure#really

Ledger Registration





The access identifier may have a self-certifying primary root-of-trust, but the registered identifier does not, even if its format appears to be self-certifying.

Autonomic Identifier (AID) and Namespace (AN)

auto nomos = self rule

autonomic = self-governing, self-controlling, etc.

An *autonomic* namespace is

self-certifying and hence *self-administrating.*

AIDs and ANs are *portable* = truly self-sovereign.

autonomic prefix = self-cert + UUID + URL = universal identifier

Zooko's Trilemma

Desirable identifier properties: secure, decentralized, human meaningful

Trilemma: May have any two of the three properties but not all three.

One way to sort of solve the trilemma is to uniquely register a human meaningful identifier on a ledger controlled by a different identifier that is secure and decentralized but not human meaningful.

Unified Identifier Model

AID: Autonomic Identifier (primary)

self-managing self-certifying identifier with cryptographic root of trust

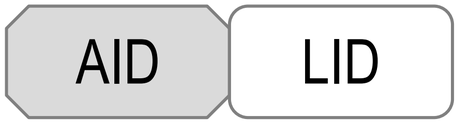
secure, decentralized, portable, universally unique

LID: Legitimized Identifier (secondary) from `aid|lid` couplet

lid = human meaningful identifier

legitimized within trust domain of given AID by authorization from AID controller

authorization is verifiable to the root-of-trust of AID



KEY Event Based Provenance of Identifiers

KERI enables cryptographic *proof-of-control-authority* (*provenance*) for each identifier.

A *proof* is in the form of an identifier's *key event receipt log* (KERL).

KERLs are *End Verifiable*:

End user alone may verify. Zero trust in intervening infrastructure.

KERLs may be *Ambient Verifiable*:

Anyone may verify *anylog*, *anywhere*, at *anytime*.

KERI = self-cert root-of-trust + certificate transparency + KA^{2}CE + recoverable + post-quantum.

KERI for the *DID*ified

KERI non-transferable ephemeral with derivation code ~ did:key

KERI private direct mode (one-to-one) ~ did:peer

KERI public persistent indirect mode (one-to-any) ~ Indy interop, did:sov etc

KERI = did:un (did:uni, did:u) (all of the above in one method)

`did:un:`*`prefix`*`[:`*`options`*`][/`*`path`*`][?`*`query`*`][#`*`fragment`*`]`

KERI Agnosticism and Interop

KERI itself is completely agnostic about anything but the *prefix* !

`???:prefix[:options][/path][?query][#fragment]`

The KERI layer establishes control authority over a *prefix*

Any and *All* namespaces that share the same *prefix* may share the same KERI trust basis for control establishment over that *prefix* and hence that namespace.

Interop happens in a layer above the KERI layer

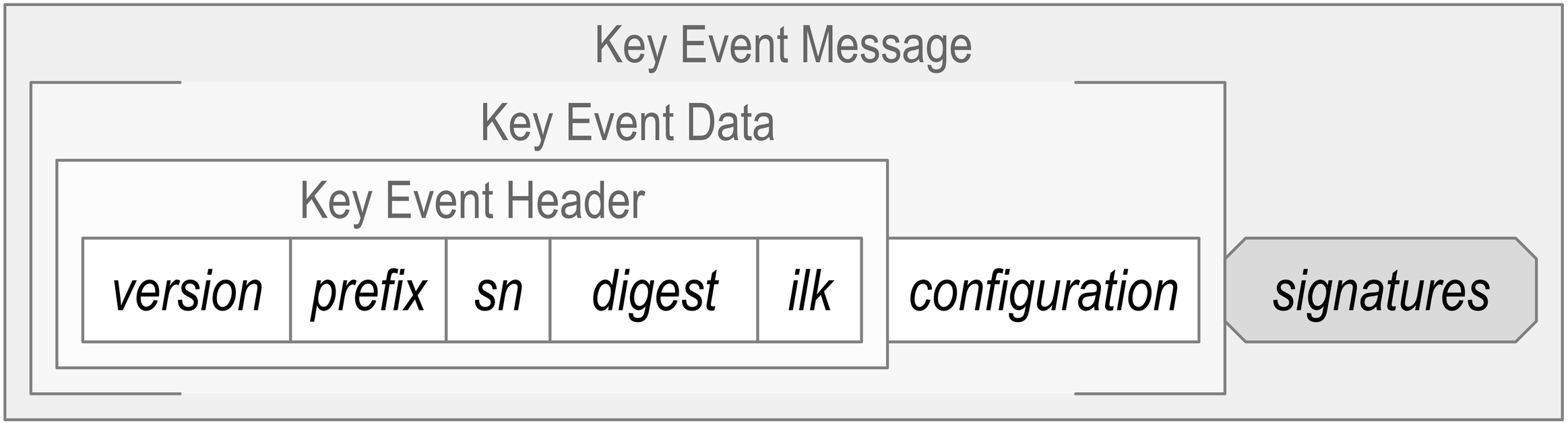
All we need for bootstrapping interop is some indication that the *prefix* inside identifier is KERI based (KERI trust basis).

Self-Certifying Identifier Prefixes

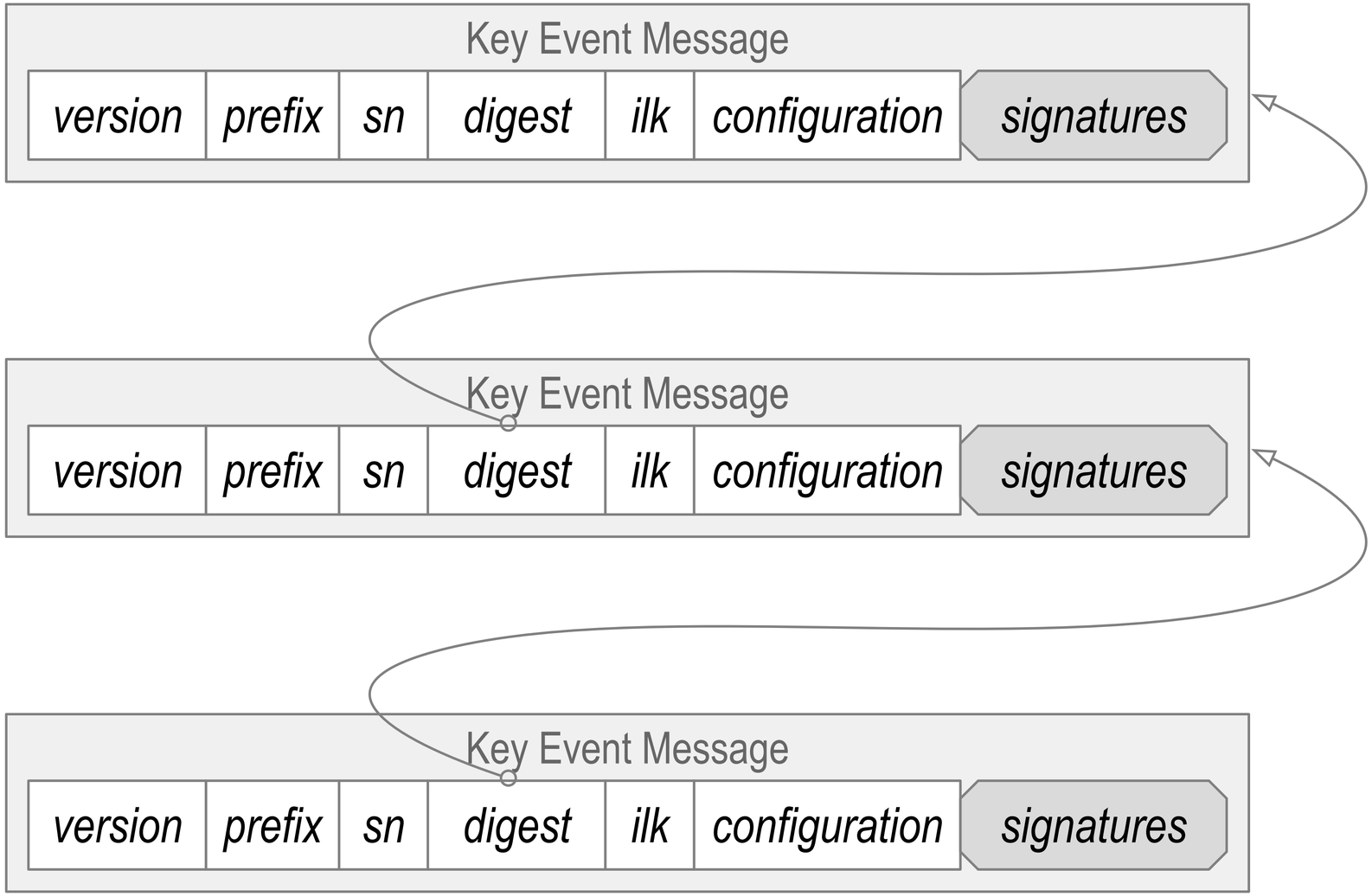
All crypto material appears in KERI in a fully qualified representation that includes a derivation code prepended to the crypto-material.

Identifier prefixes are fully qualified crypto-material.

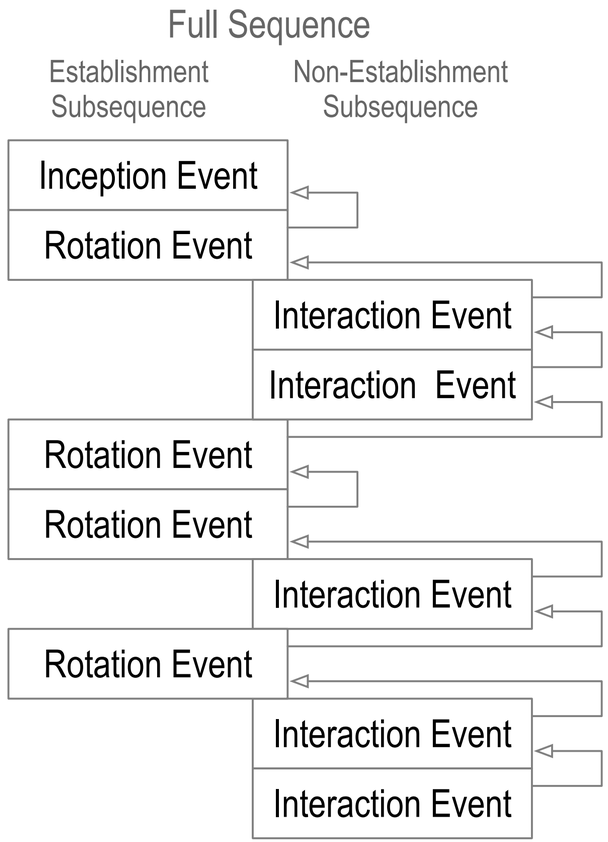
Key Event Message



Event Chaining



Inconsistency and Duplicity



inconsistency: lacking agreement, as two or more things in relation to each other

duplicity: acting in two different ways to different people concerning the same matter

Internal vs. External Inconsistency

Internally inconsistent log = not verifiable.

Log verification from self-certifying root-of-trust protects against internal inconsistency.

Externally inconsistent log with a purported copy of log but both verifiable = duplicitous.

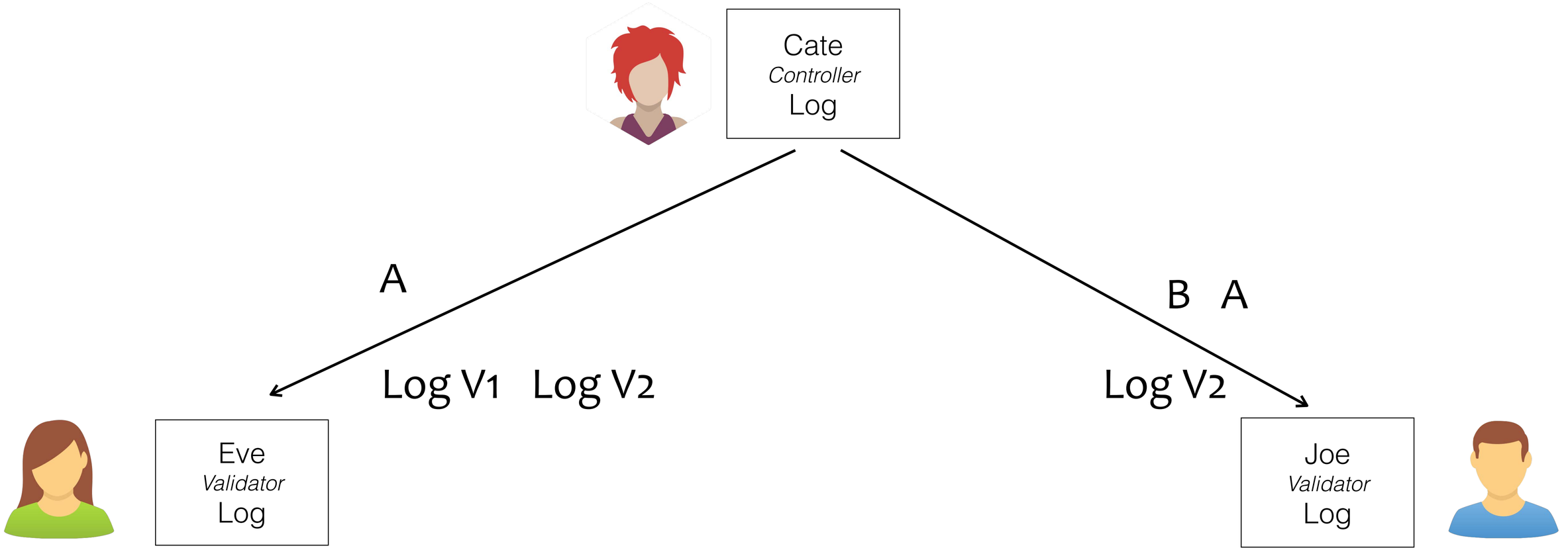
Duplicity detection protects against external inconsistency.

Duplicity Game

Cate promises to provide a consistent pair-wise log.

Local Consistency Guarantee

How may Cate be duplicitous and not get caught?



private (one-to-one) interactions

Duplicity Game

Service promises to provide a consistent log to anyone.

Local Consistency Guarantee

How may Cate/Service/Agent be duplicitous and not get caught?

Cate
Controller
Log

Truncate Log

Delete Log

Service/Agent
Controlled by Cate
Log

A

B A

Log V1 Log V2

Log V2

Eve
Validator
Log

Joe
Validator
Log

highly available, private (one-to-one) interactions

Duplicity Game

Service promises to provide exact same log to everyone.

Global Consistency Guarantee

How may Cate and/or service be duplicitous and not get caught?

Cate
Controller
Log

Breaking the promise of global consistency is a provable liability.

Global consistency may only matter after A and B need to interact not before.

Service
Controlled by Cate
Log

?

isolate network

A

log V1

Doug
Global Duplicity
Log

A Truncate Log

Delete Log

log V2

isolate network

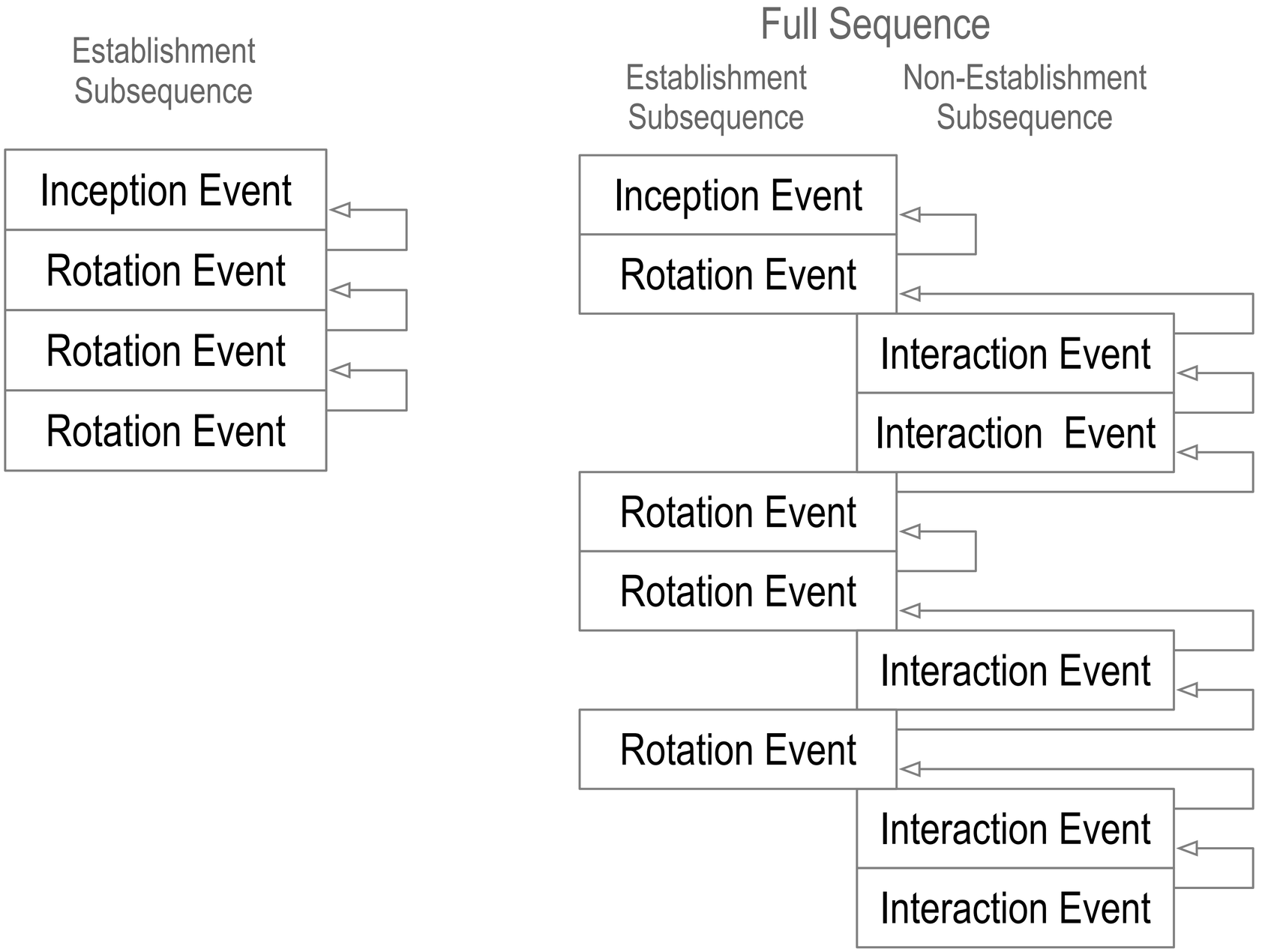
Eve
Validator
Log

Ambient Duplicity Detection

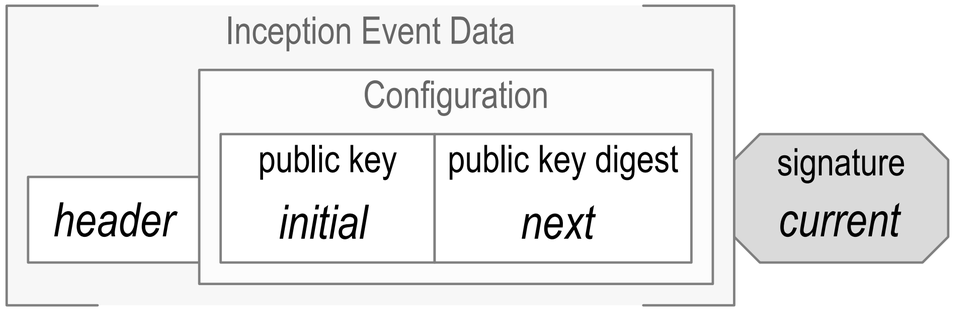
Joe
Validator
Log

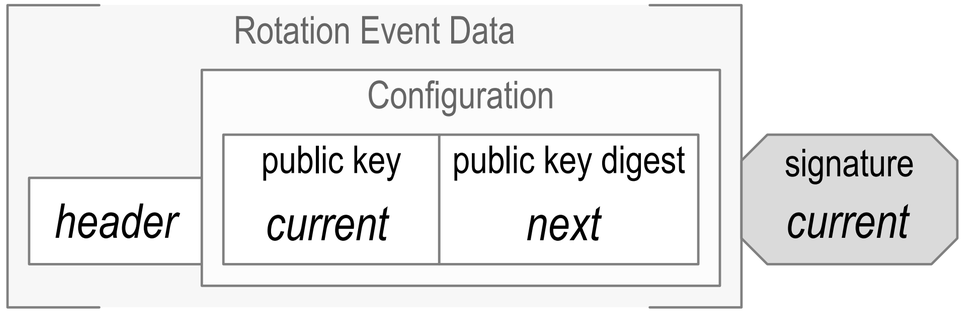
global consistent, highly available, and public (one-to-any) interactions

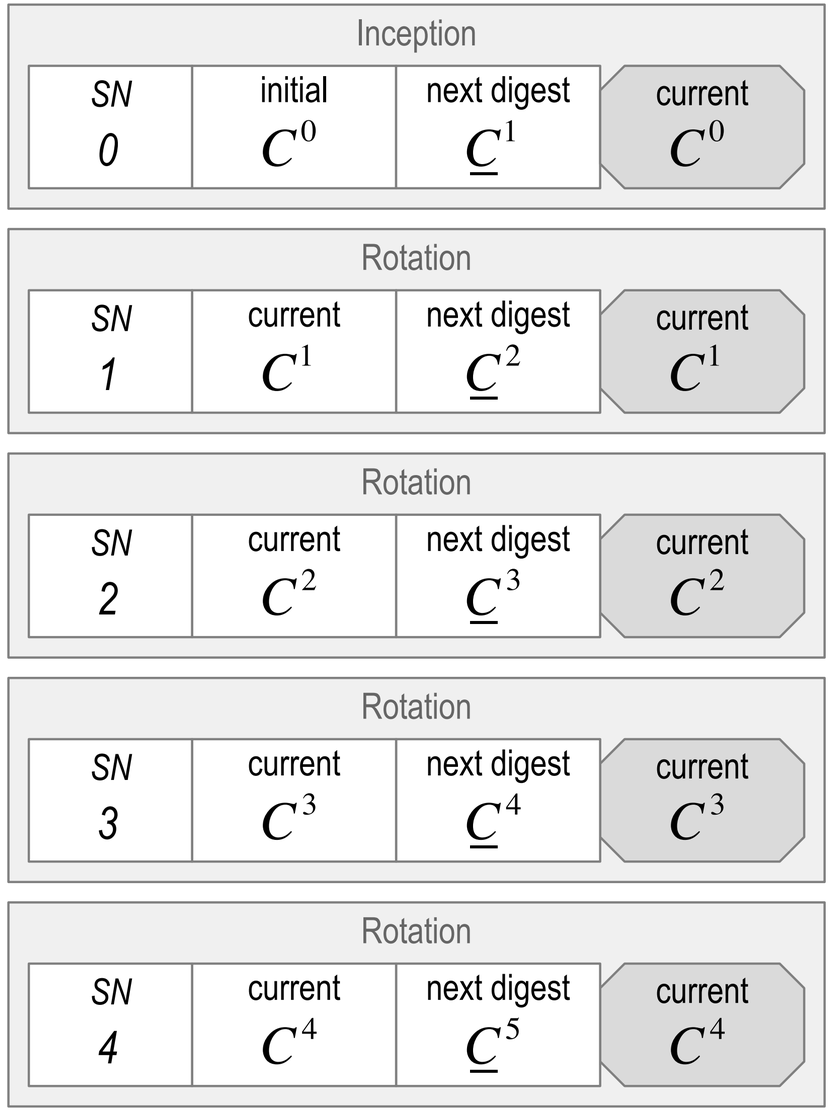
Event Sequencing



Pre-Rotation

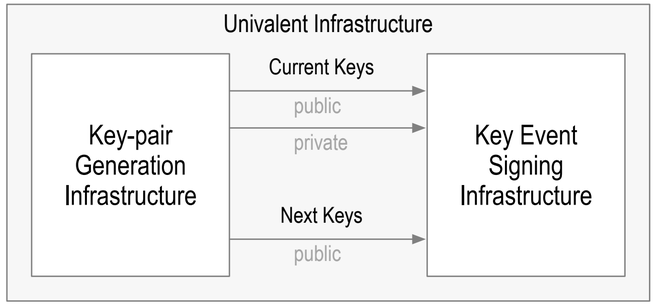


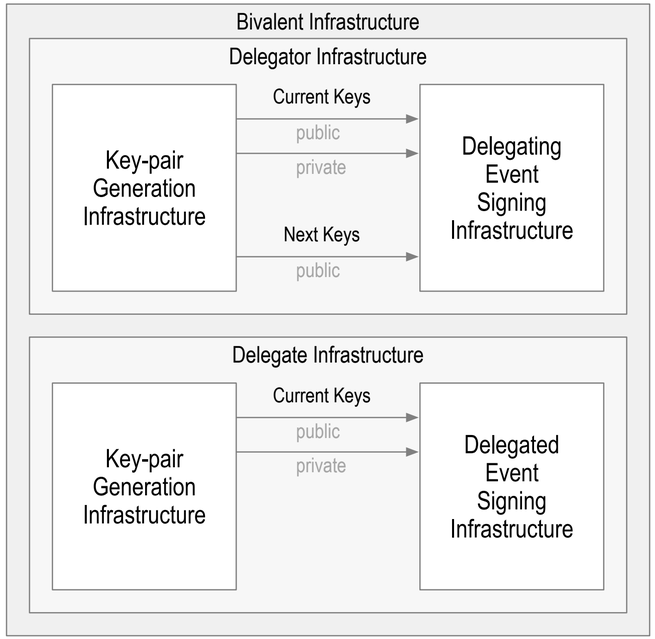


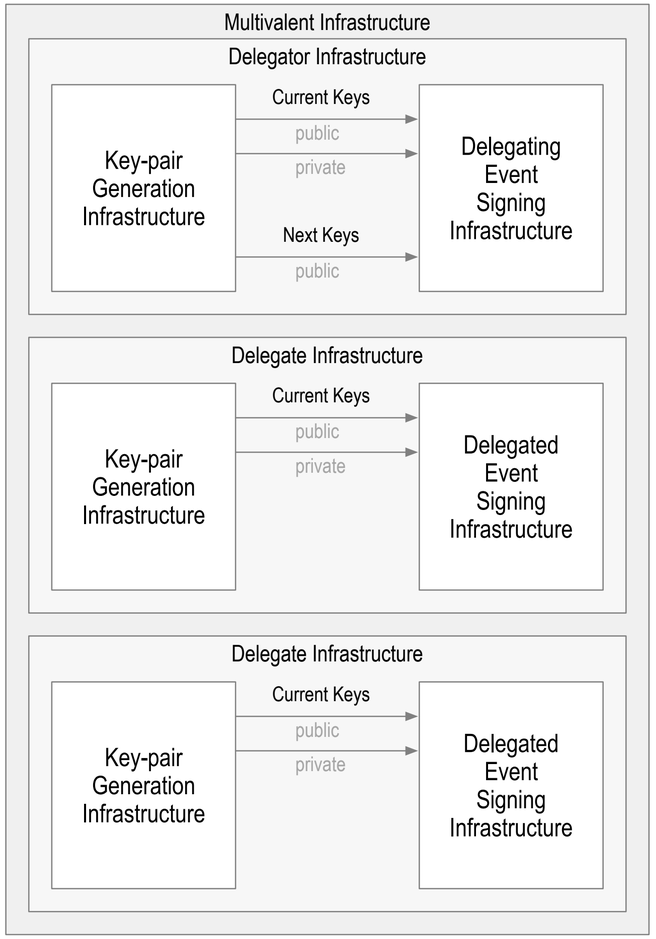


Digest of *next* key(s) makes pre-rotation post-quantum secure

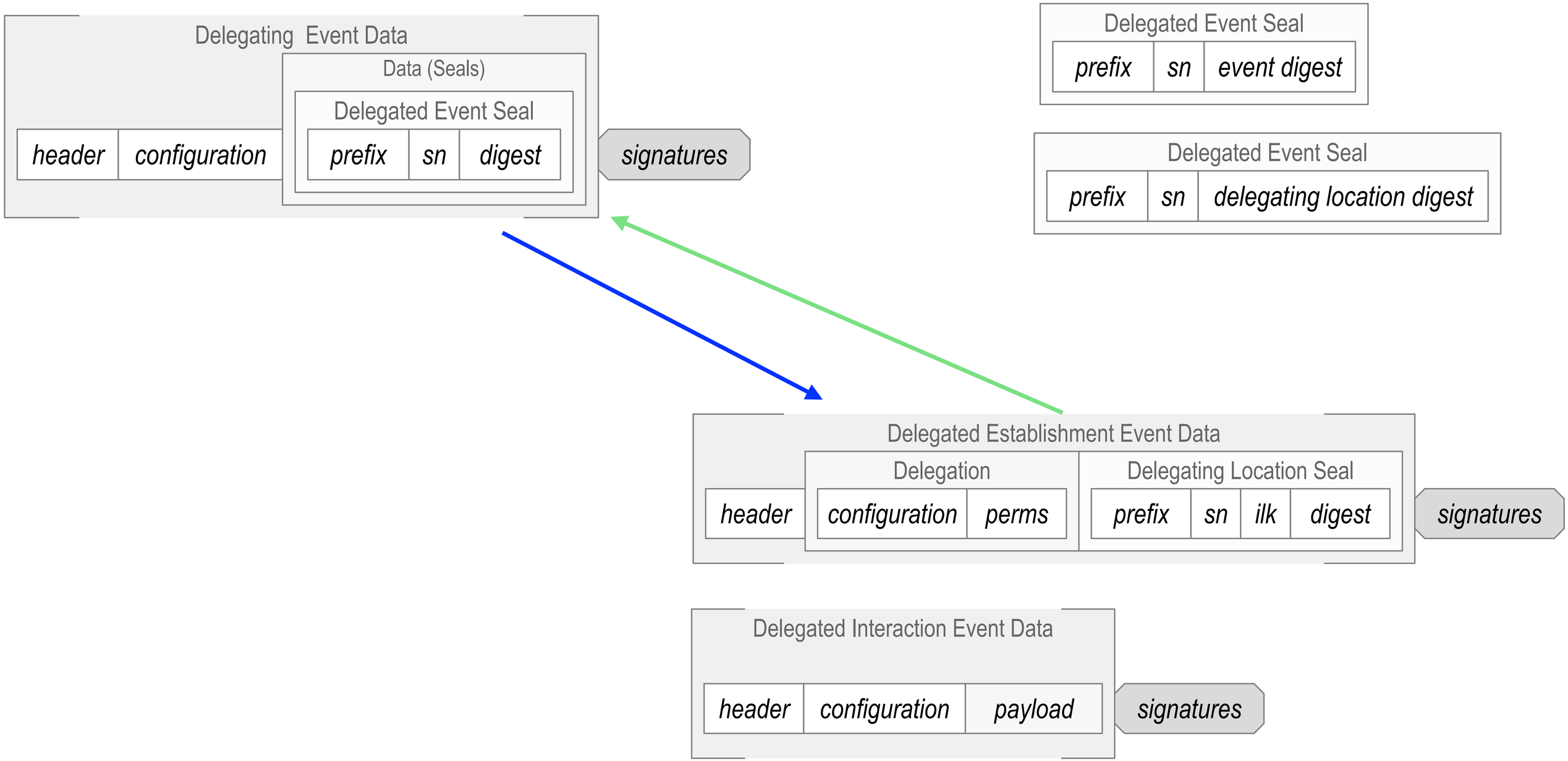
Key Infrastructure Valence



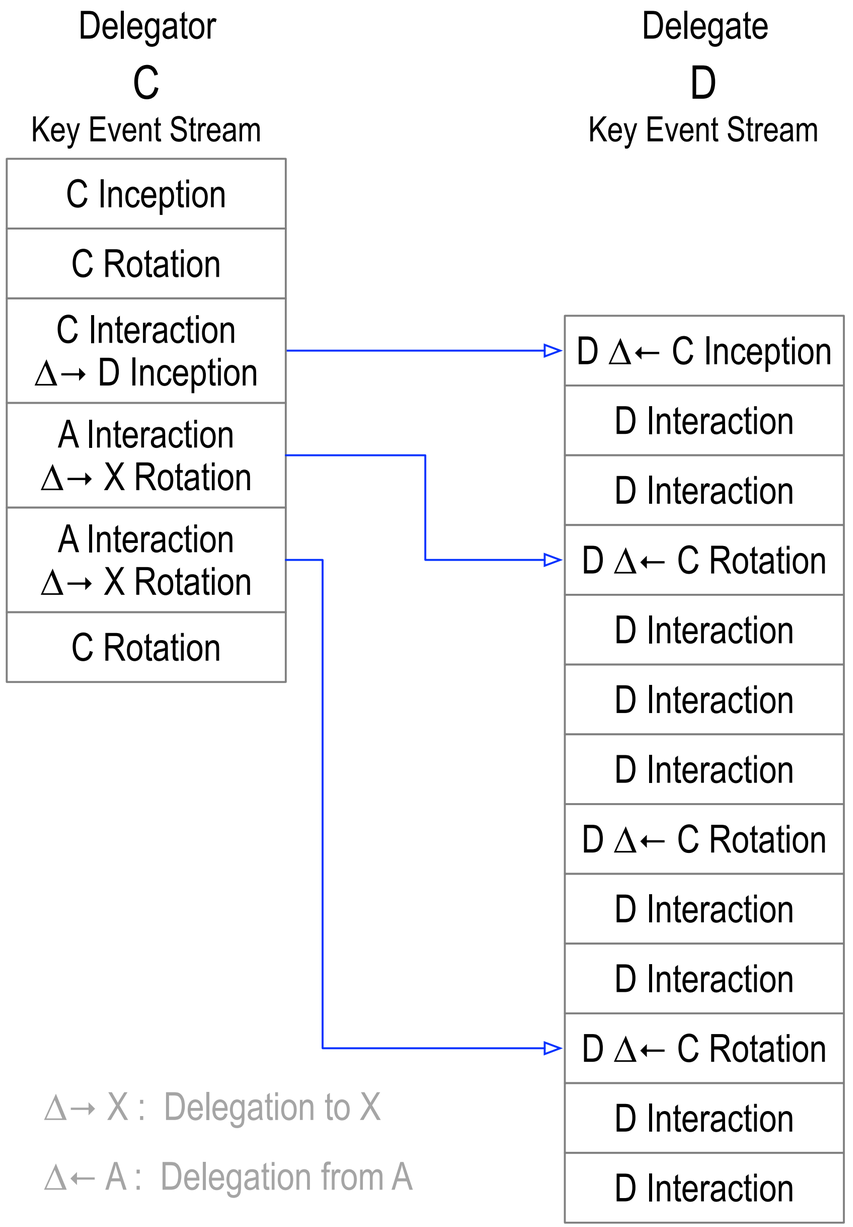




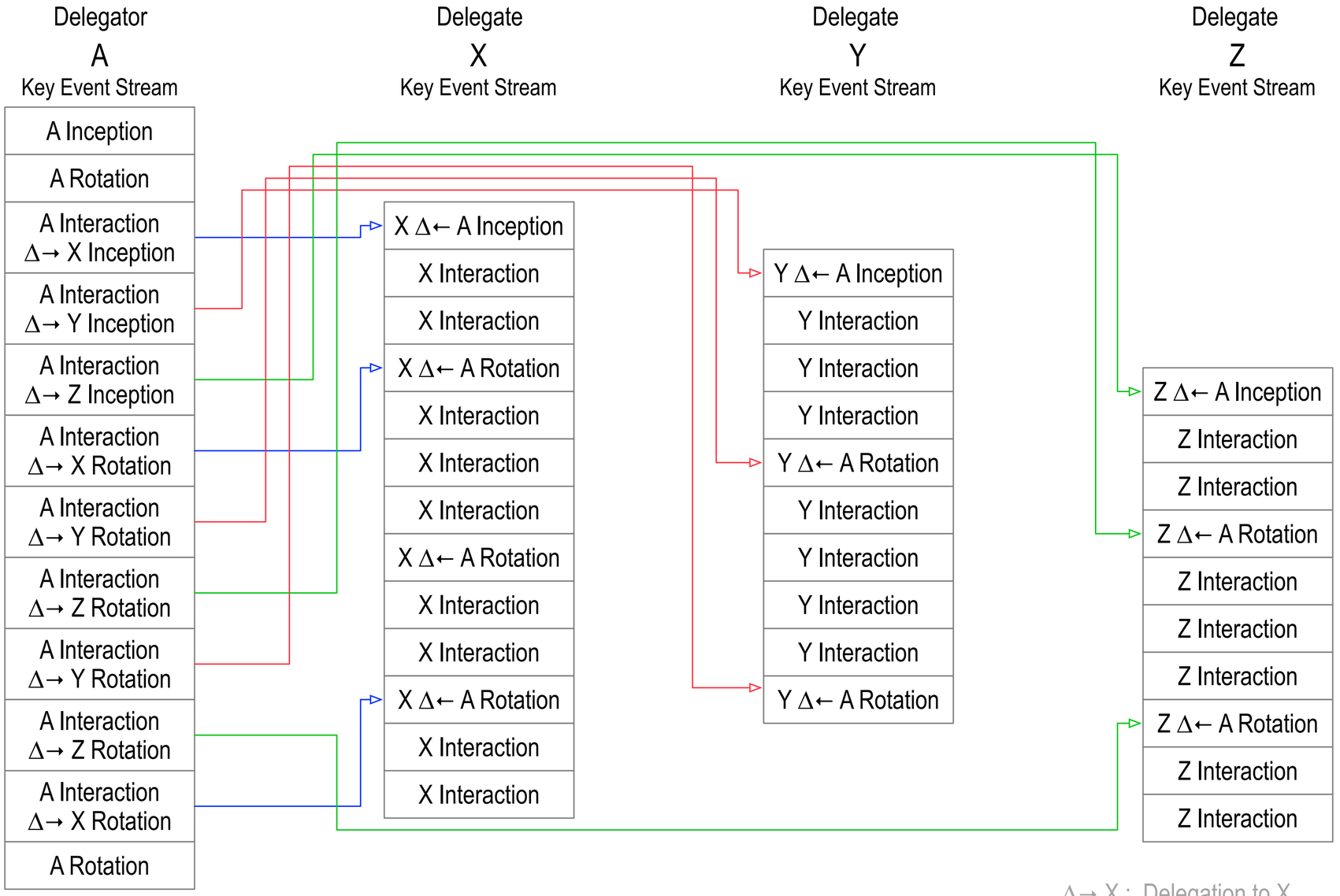
Delegation (Cross Anchor)



Interaction Delegation



Scaling Delegation via Interaction

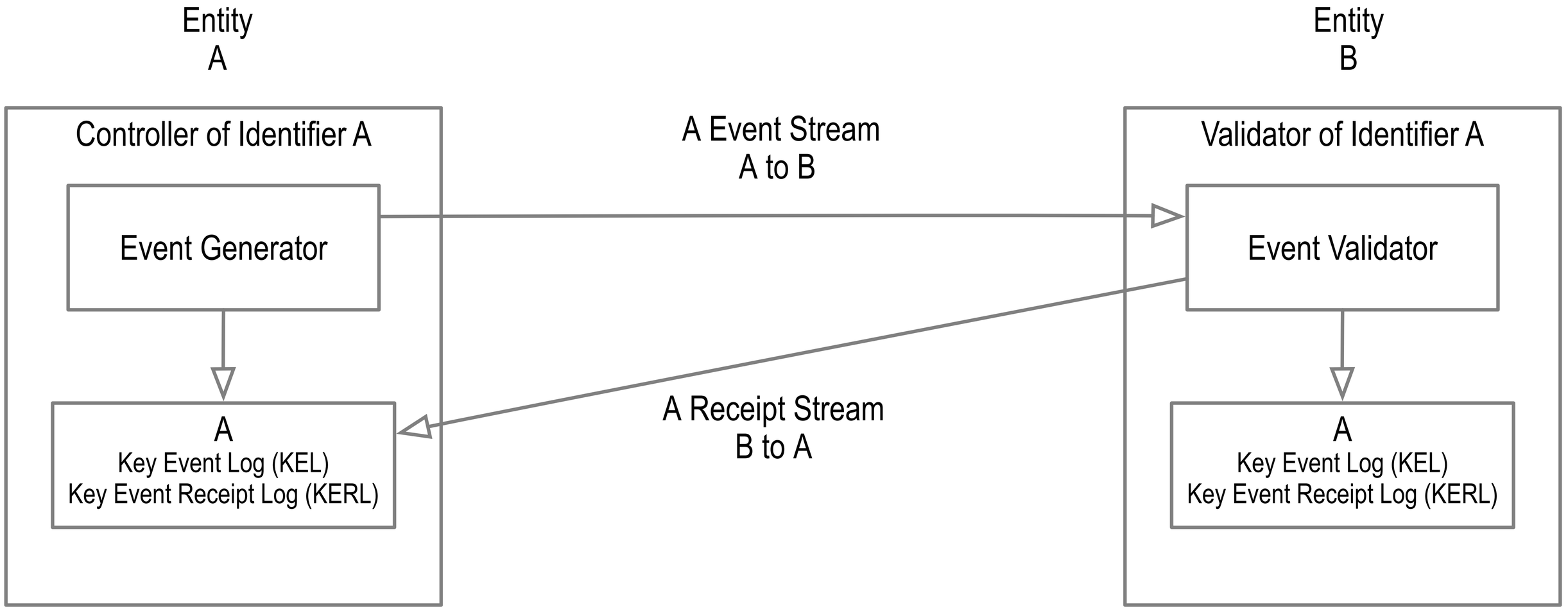


Protocol Operational Modes

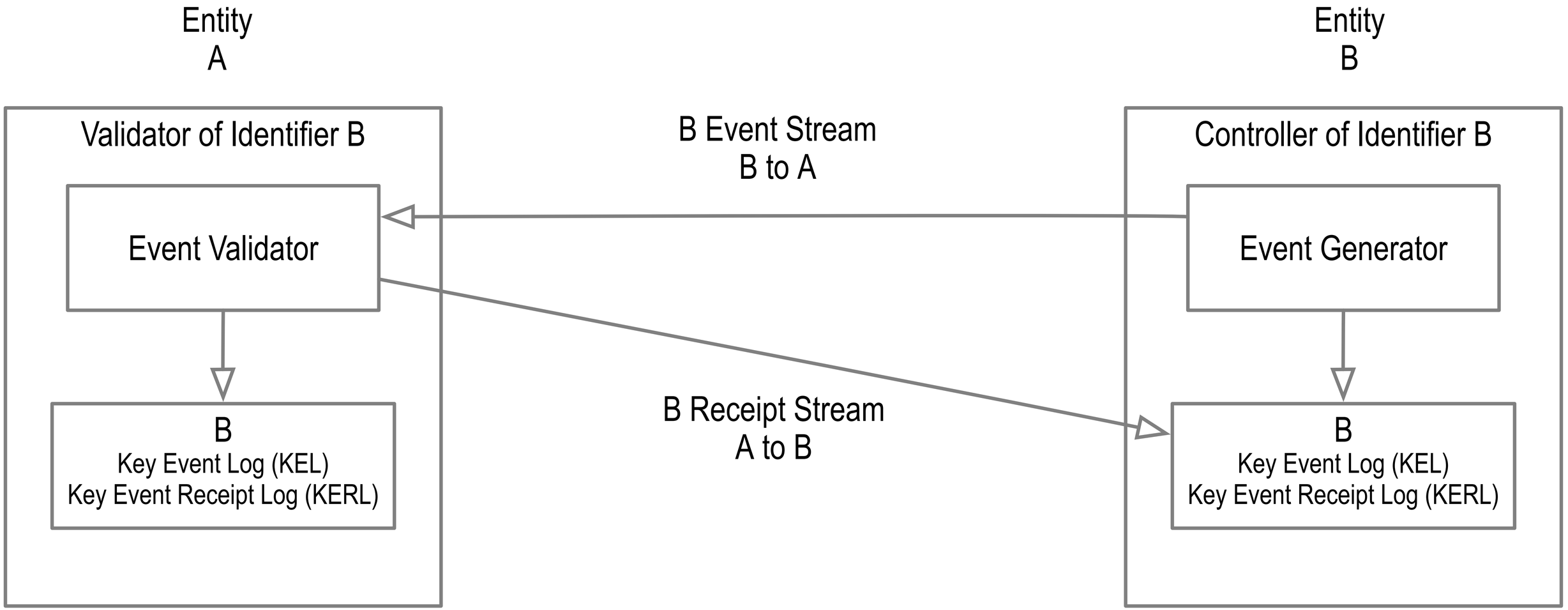
Direct Event Replay Mode (one-to-one)

Indirect Event Replay Mode (one-to-any)

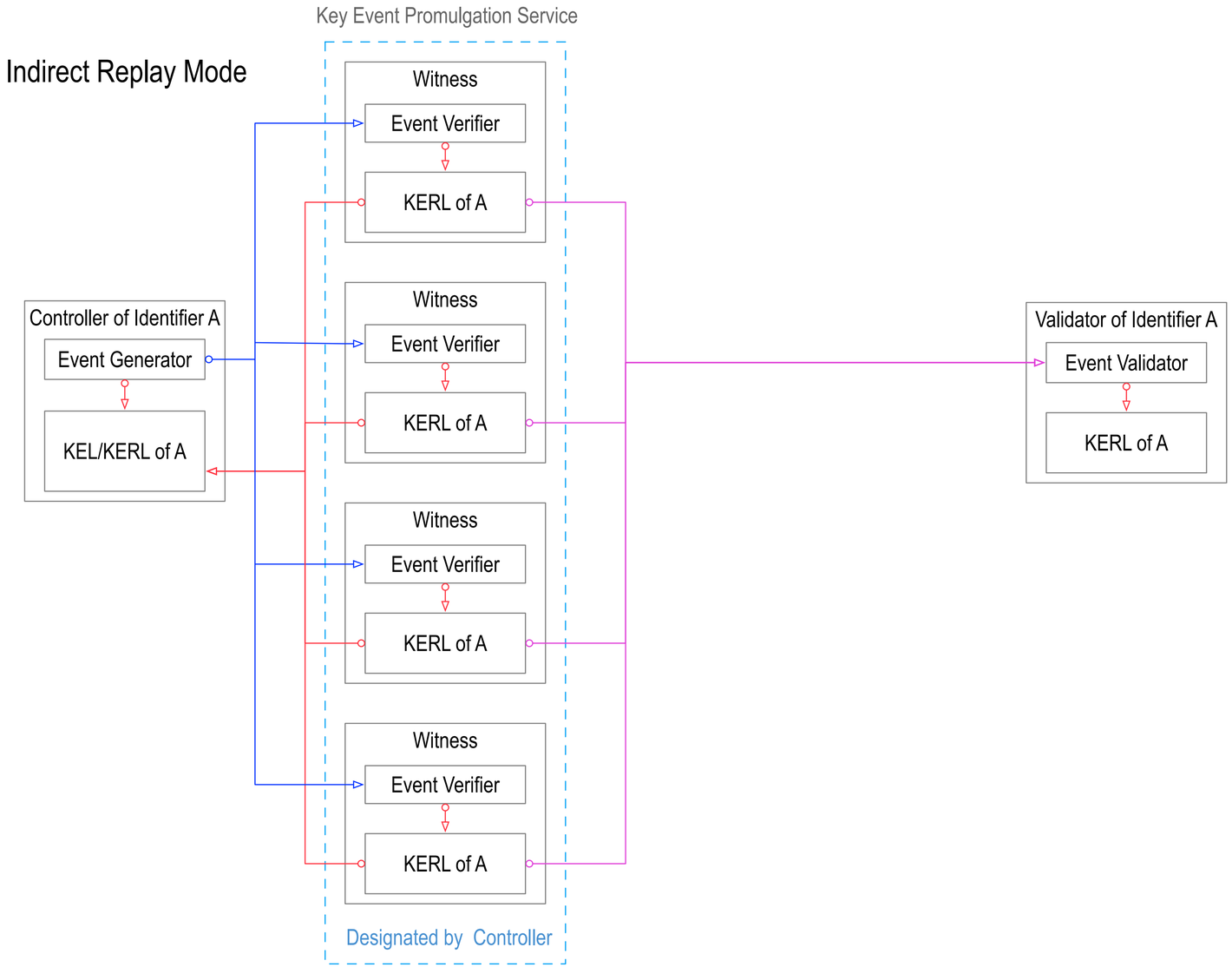
Direct Mode: A to B



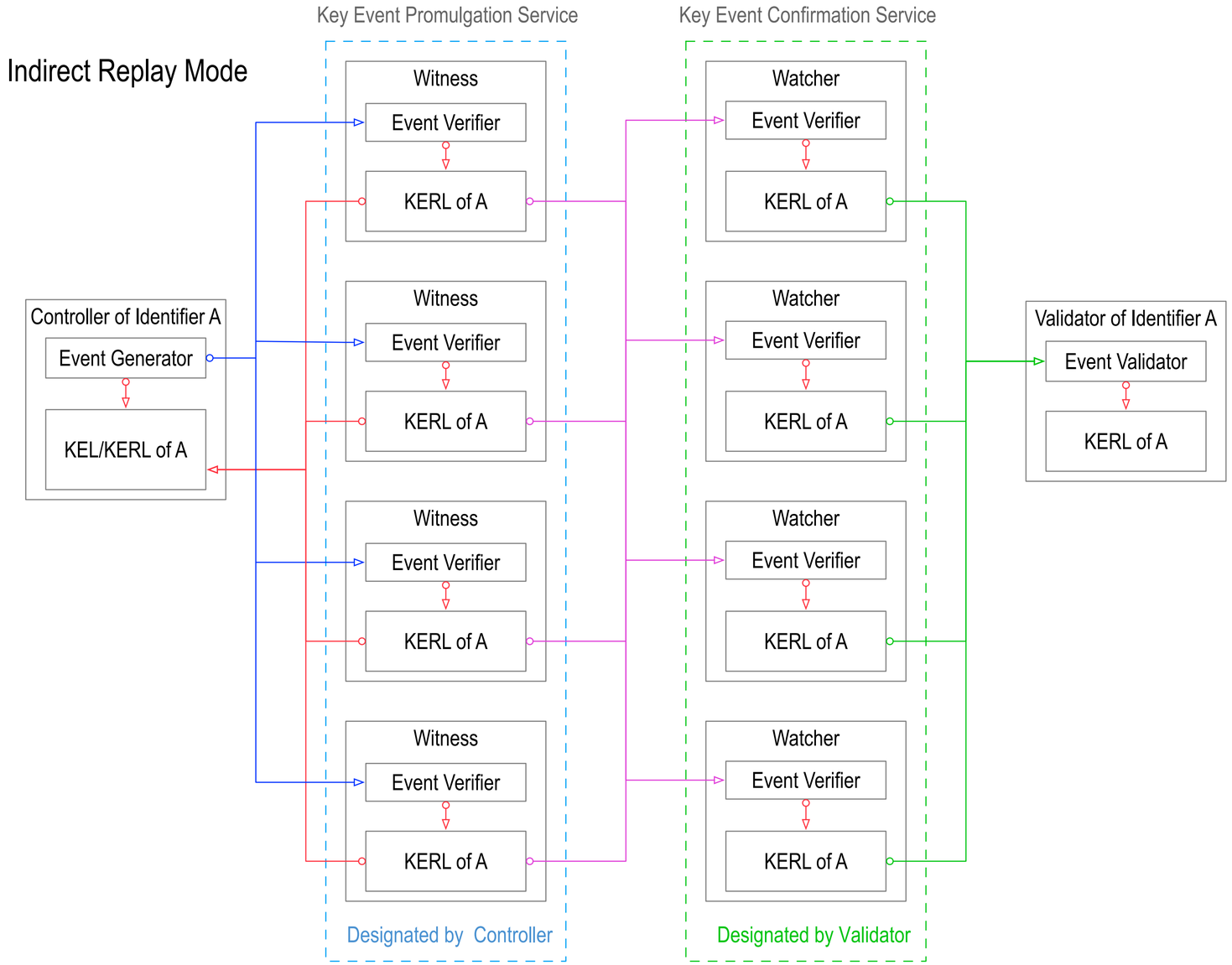
Direct Mode: B to A



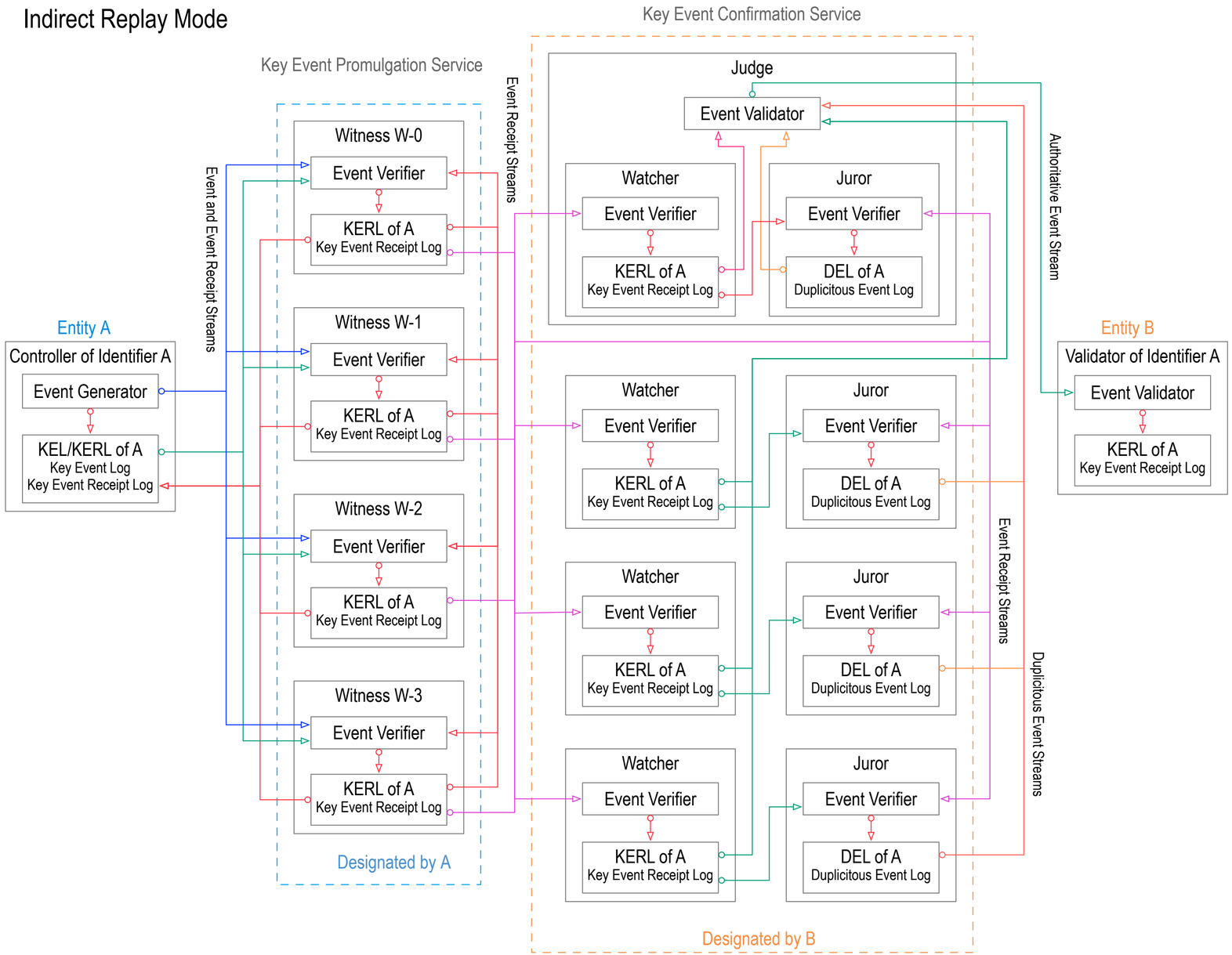
Indirect Mode Promulgation Service



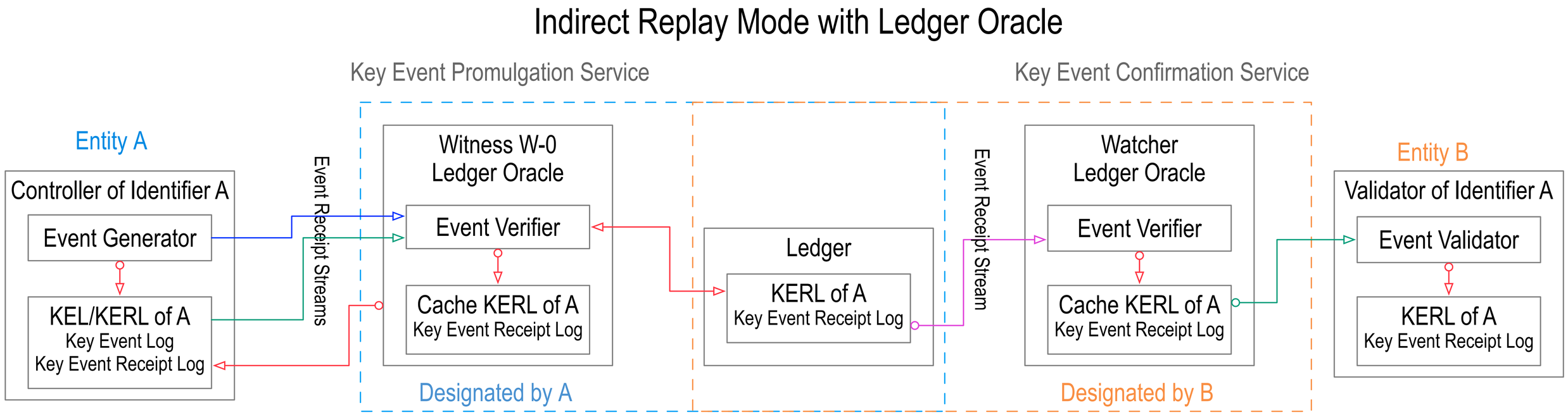
Indirect Mode
Promulgation and Confirmation Services



Indirect Mode Full



Indirect Mode with Ledger Oracles



Separation of Control

Shared (permissioned) ledger = *shared control* over *shared data*.

Shared *data* = *good*, shared *control* = *bad*.

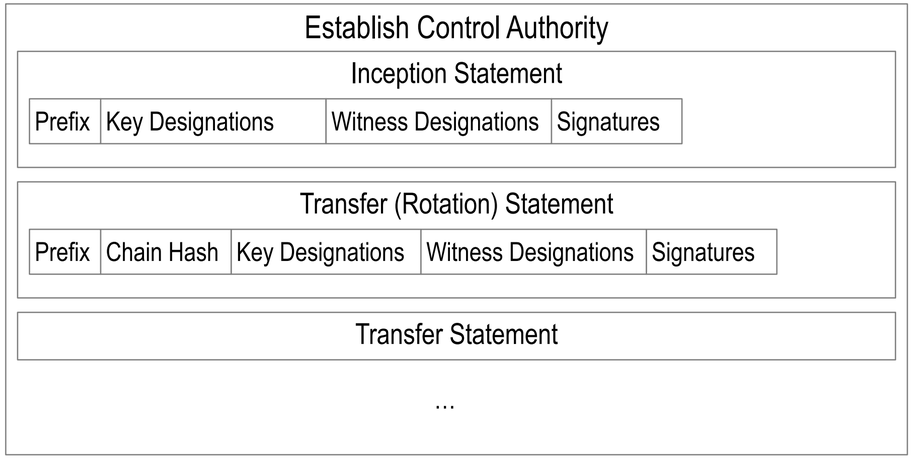
Shared control between controller and validator may be problematic for governance, scalability, and performance.

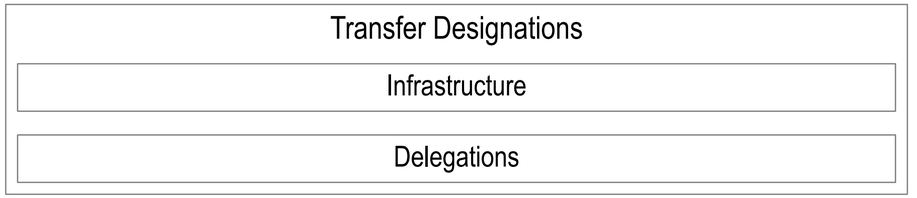
KERI = *separated control* over *shared data*.

Separated control between controller and validator may provide better decentralization, more flexibility, better scalability, lower cost, higher performance, and more privacy at comparable security.

Function Stack

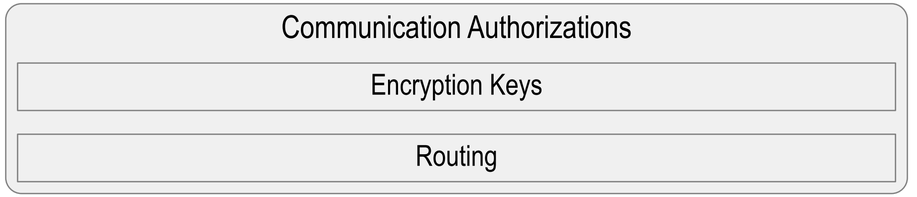
KERI





Authorizations after Establishment

On Top of KERI



Design follows the *Hourglass Model* of a stack of thin layers

CONCLUSION

Q&A

Rotate Prefix vs Rotate Keys

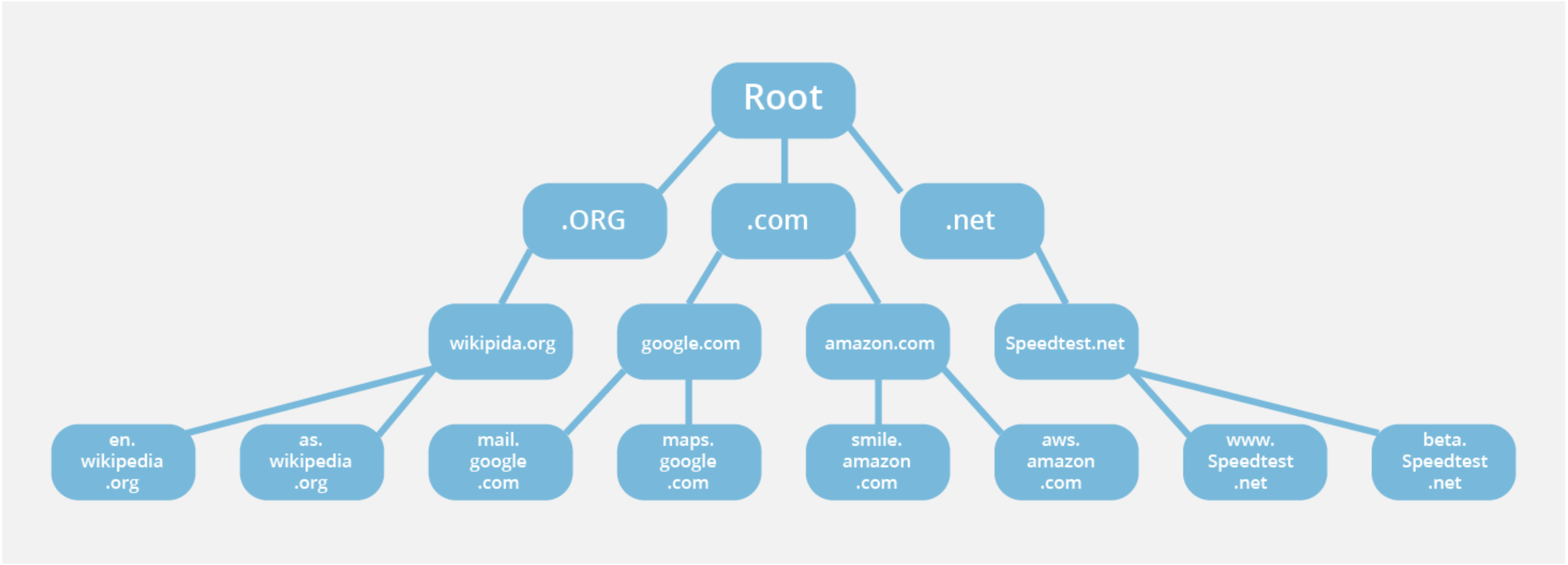
Non-transferable may not rotate keys. May only rotate prefix
Rotate prefix good for bootstrapping. No key event log (KEL) needed.
If prefix has no persistent value outside its function and its function may be marshaled by some other prefix controller then rotating prefix may be preferred.

Discovery

Ledger Based

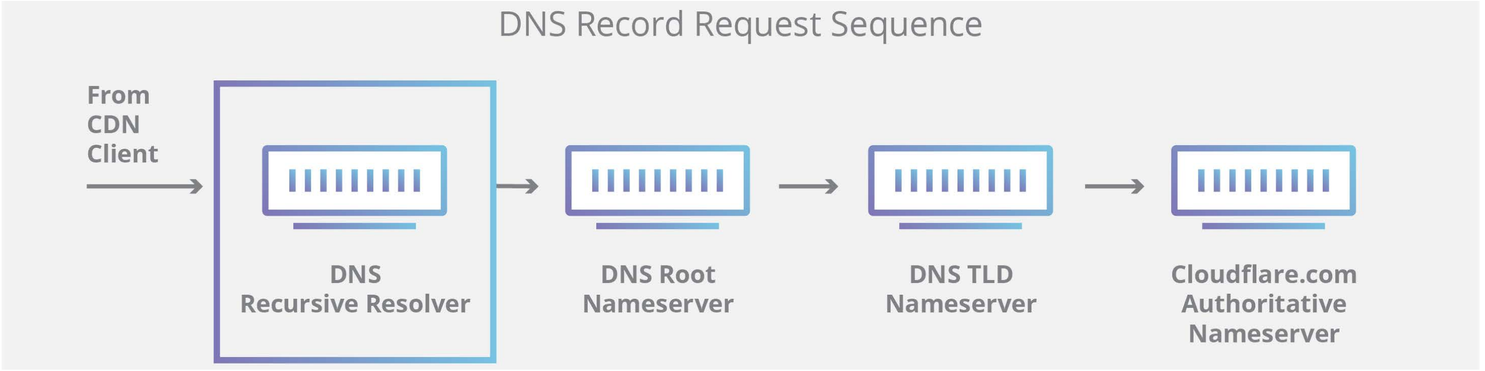
Non-Ledger Based

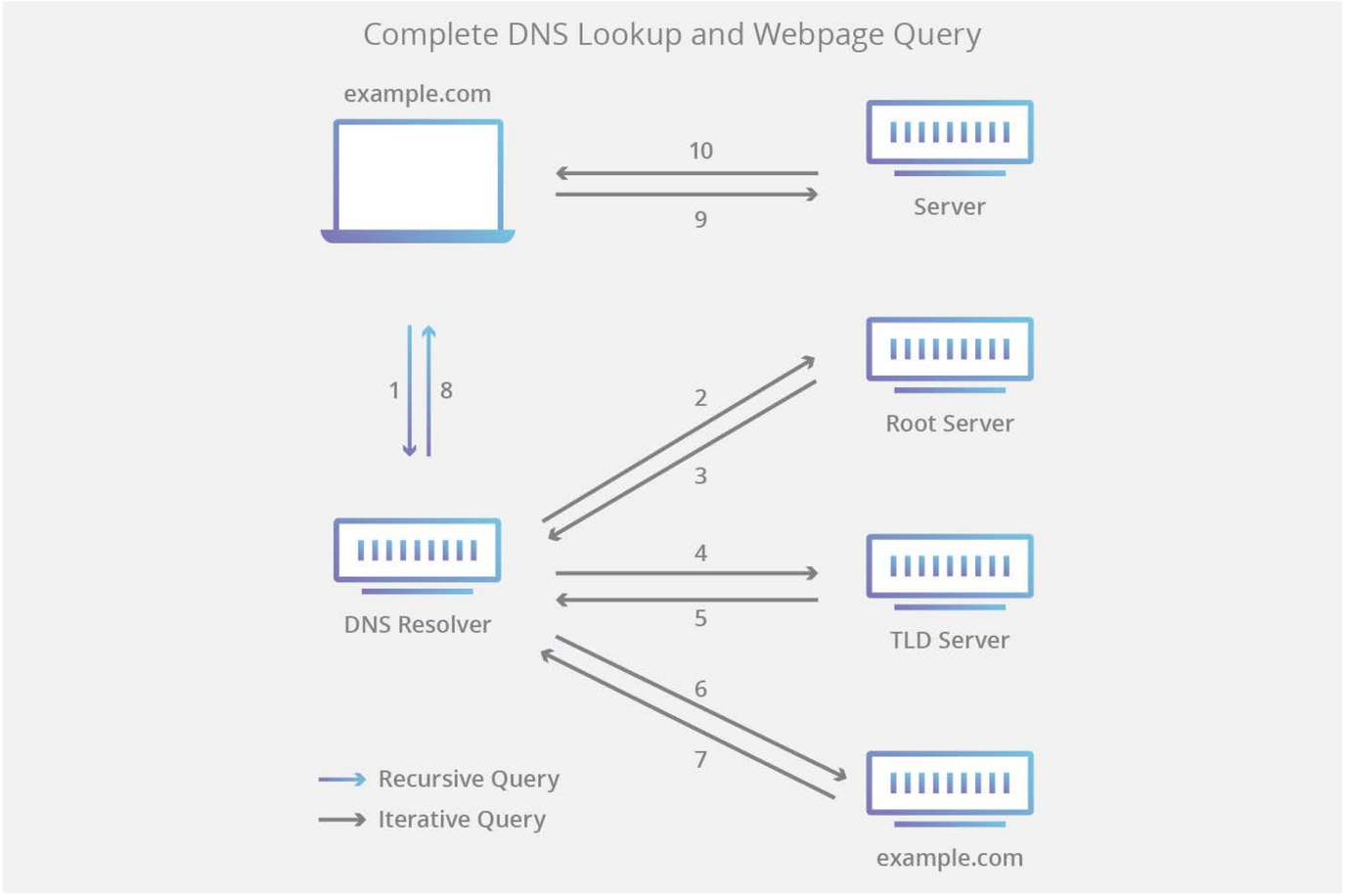
DNS “Hierarchical” Discovery



Diagrams from https://www.cloudflare.com/learning/dns/what-is-dns/

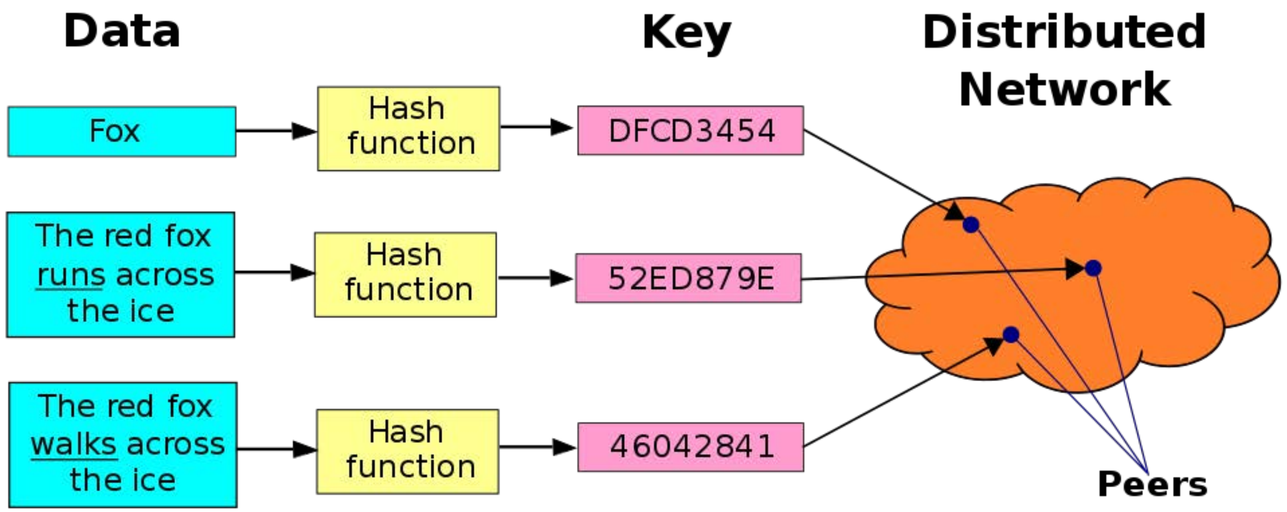
DNS “Hierarchical” Discovery





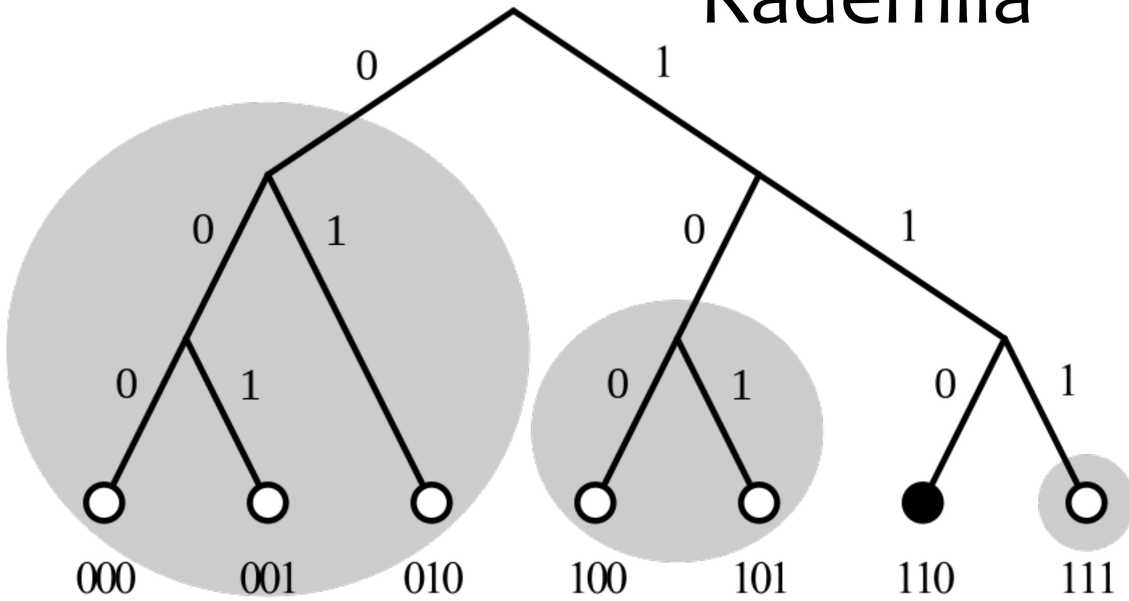

```
$ORIGIN example.com.
                        @               3600 SOA   ns1.p30.oraclecloud.net. (
                        zone-admin.dyndns.com.    ; address of responsible party
                        2016072701              ; serial number
                        3600                    ; refresh period
                        600                     ; retry period
                        604800                  ; expire time
                        1800                    ) ; minimum ttl
                        86400 NS    ns1.p68.dns.oraclecloud.net.
                        86400 NS    ns2.p68.dns.oraclecloud.net.
                        86400 NS    ns3.p68.dns.oraclecloud.net.
                        86400 NS    ns4.p68.dns.oraclecloud.net.
                        3600 MX    10 mail.example.com.
                        3600 MX    20 vpn.example.com.
                        3600 MX    30 mail.example.com.
                        60 A     204.13.248.106
                        3600 TXT   "v=spf1 includespf.oraclecloud.net ~all"
                        mail            14400 A     204.13.248.106
                        vpn               60 A     216.146.45.240
                        webapp            60 A     216.146.46.10
                        webapp            60 A     216.146.46.11
www                     43200 CNAME example.com.
```

DHT “Distributed” Discovery



Diagrams from https://en.wikipedia.org/wiki/Distributed_hash_table

Kademlia



Diagrams from https://en.wikipedia.org/wiki/Kademlia

DHT Discovery for KERI

Resolve Node Prefix to IP Mapping

Prefix to Inception/Latest Rotation Event Caching
-> Extract Witness Prefixes from Event

Witness Prefix to IP Mapping

KERL Query to Witness Node

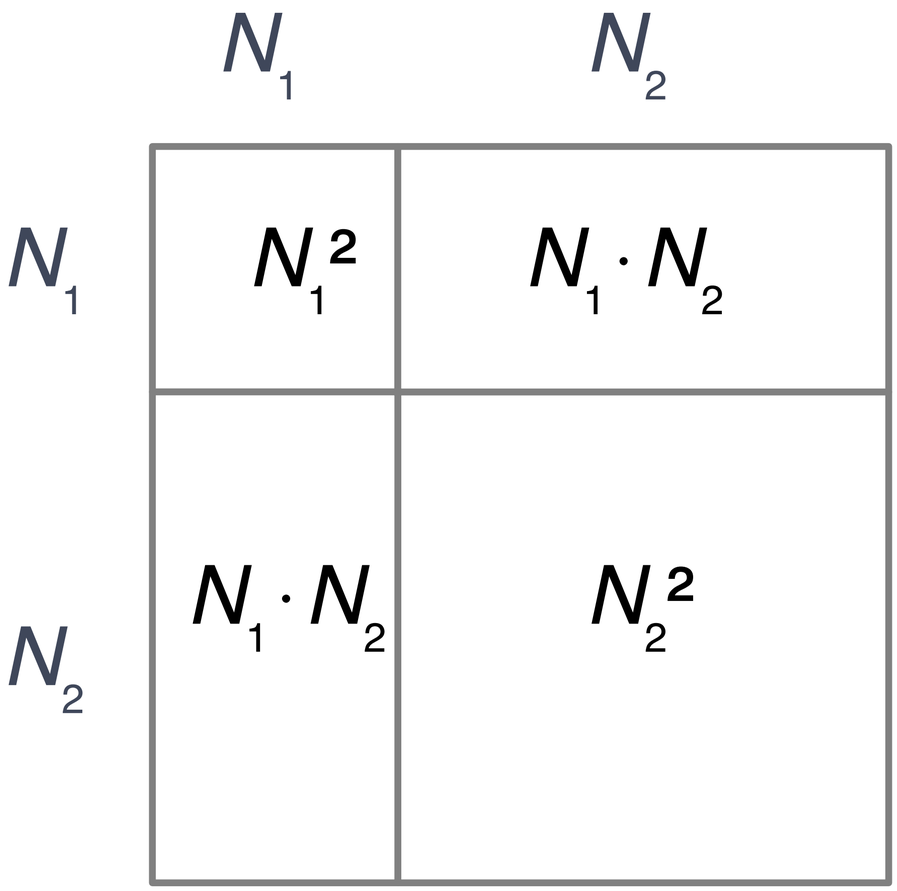
Diagrams from https://en.wikipedia.org/wiki/Distributed_hash_table

Diagrams from https://en.wikipedia.org/wiki/Kademlia

Leverage cooperative network effects

Cooperating Networks

What happens to value when two smaller networks combine?



$$v_1 = v_2 = a \cdot (N_1 + N_2)$$

$$V_1 = a \cdot N_1 \cdot (N_1 + N_2) = a \cdot N_1^2 + a \cdot N_1 \cdot N_2$$

$$V_2 = a \cdot N_2 \cdot (N_1 + N_2) = a \cdot N_2^2 + a \cdot N_1 \cdot N_2$$

$$V = V_1 + V_2 = a \cdot N_1^2 + 2 \cdot a \cdot N_1 \cdot N_2 + a \cdot N_2^2 = a \cdot (N_1 + N_2)^2$$

$$a \cdot N_1 \cdot N_2.$$

Cooperating Network Lifetime Value

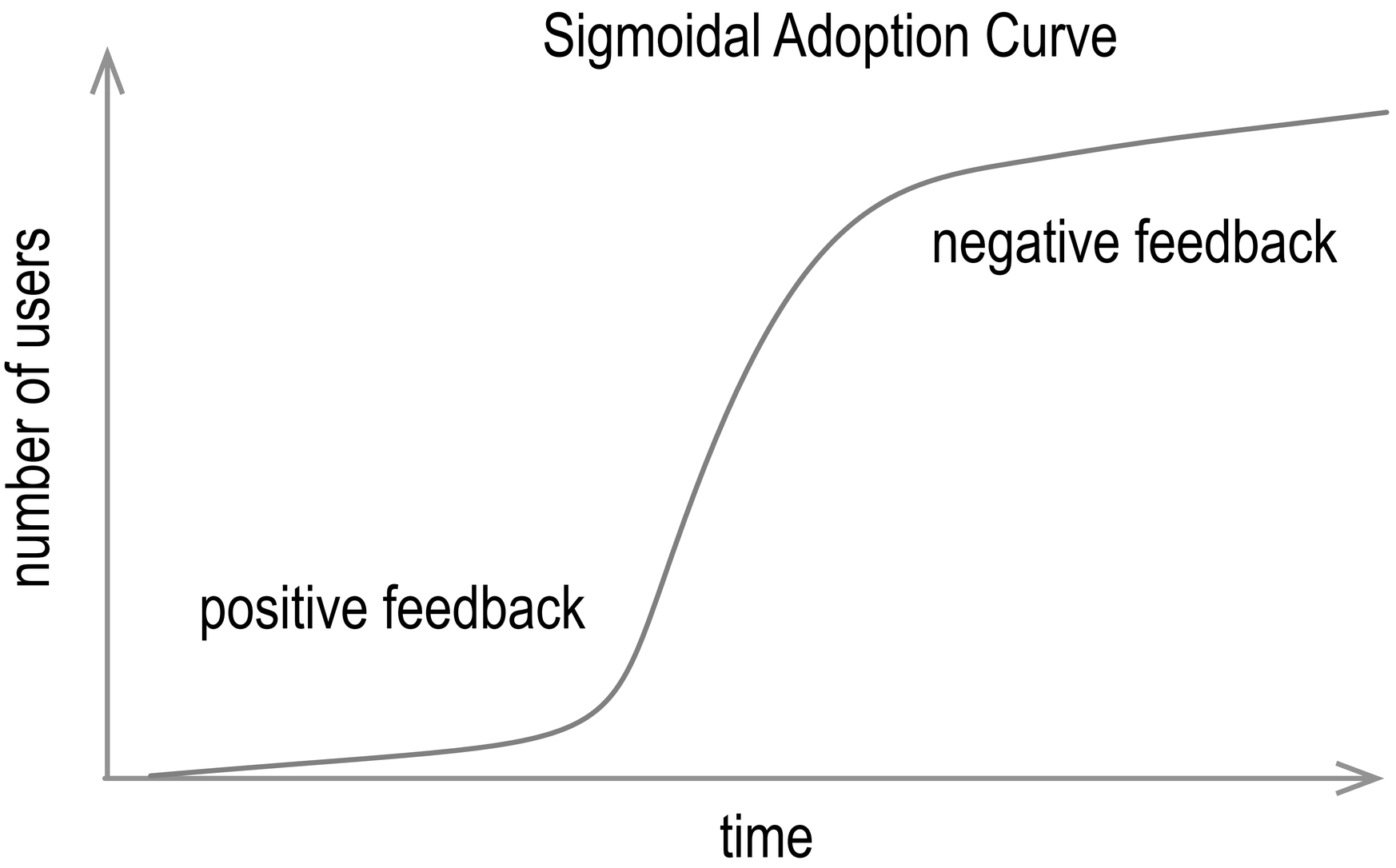
Xie, J. and Sirbu, M., "Price competition and compatibility in the presence of positive demand externalities," *Management science*, vol. 41, no. 5, pp. 909-926, 1995

When the two networks are value symmetric then it is always more profitable for both to combine.

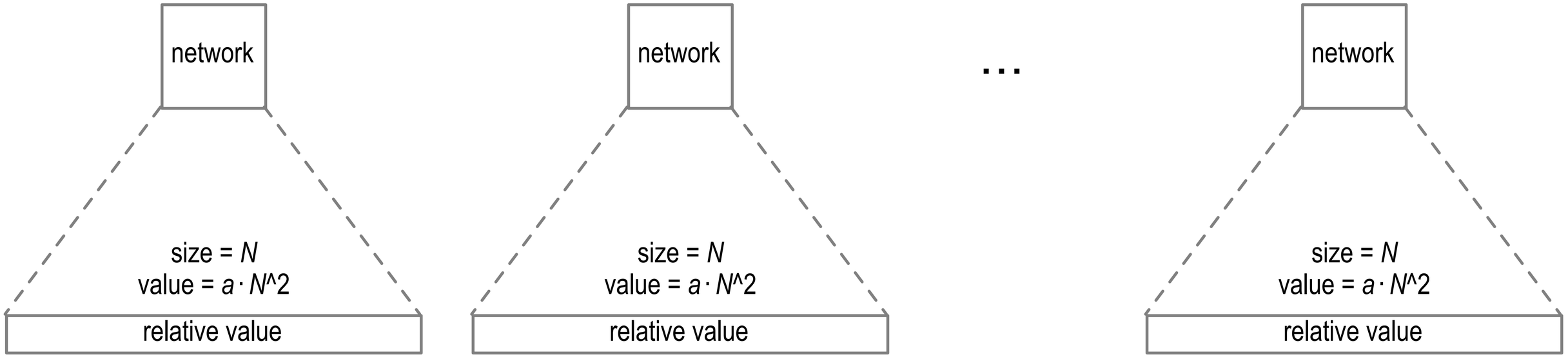
When the two networks are value asymmetric then it is always more profitable for the smaller network to combine.

When the two networks are value asymmetric and when the larger network's size is below a threshold then it is also always more profitable for the larger network to combine.

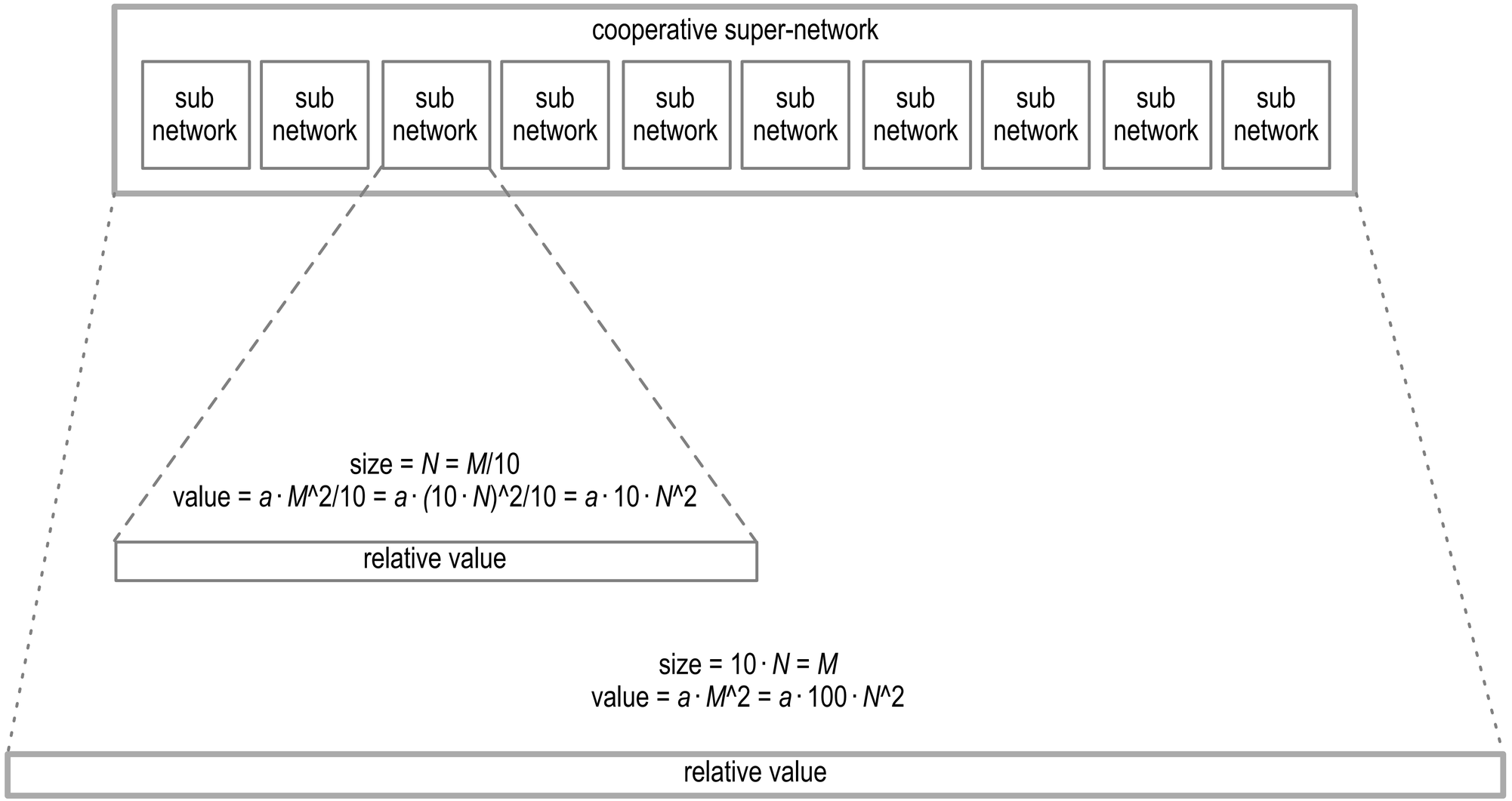
Feedback and Adoption Growth Rate



Competing Small Networks



Super-Network of Cooperating Small Networks



Cooperative Network of Networks Effect

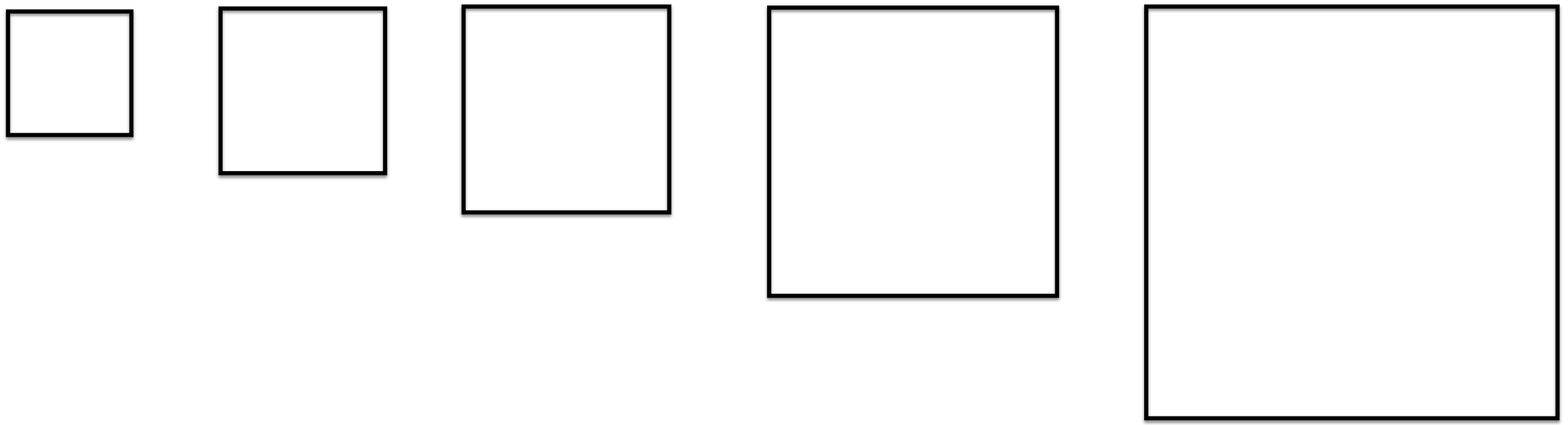
$$V(N{:}M)/V(N) = ((N/M)\cdot a\cdot M^2)/(a\cdot N^2) = M/N$$

$$V(N{:}M) = (M/N)\cdot V(N)$$

The network effect resulting from sub-network joining a cooperating super-network is that the sub-network's value is increased by the ratio of super-network to sub-network size.

Cooperation Advantage

Small Network Strategy



Cooperative Network Cascade

How to remove primary barrier to cooperation?

Different value contexts = not directly competitive.

Find value that is transferrable between contexts.

Trans-contextual value creation and capture.

Use *trans-contextual* value creation and capture to *fuel cooperative* network effects.

Participant controlled

trans-contextual value creation and capture

= *virtual* participant centric network

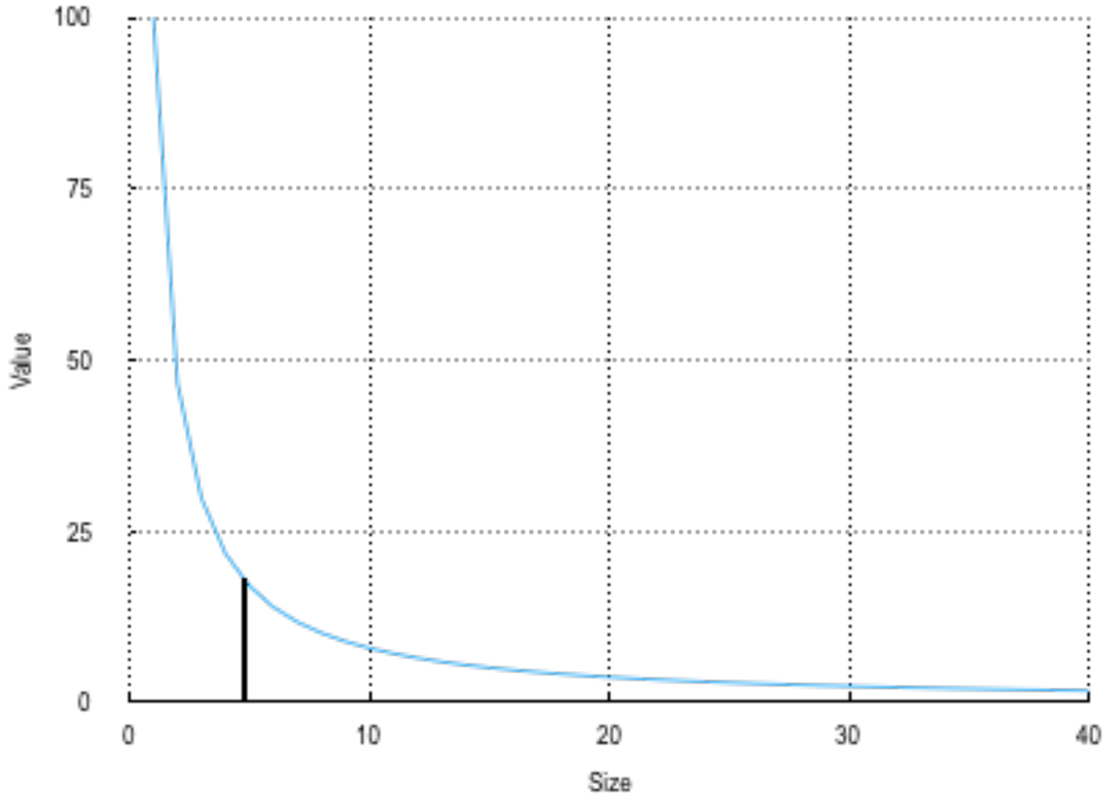
Enables participant to *amplify* own value

across multiple contexts

= maximum adoption *pull*

= fastest spin-up of *cooperative* network effects.

Cooperative long-tail network effects



Treat long-tail as effective set of different contexts

Q: Where to find trans-contextual value?

A: Transaction Costs?

Triangulation: Connection, Find, Filter, Match

Transfer: Facilitation,Transport, Delivery, Payment

Trust: Security, Competency, Reliability, Privacy, Liability

Platforms/Networks sell reductions in transaction costs.

To a consumer, all costs look like transaction costs.

Principal super aggregator pull is reduced trust transaction costs.

Trust may be highly transferable between contexts!

Reduction of trust transaction costs

is a

primary network effect value from cooperation.

Transitive Value Virtual Network Scaling Law

Set of trans-contextual cooperating networks **n**.

average transitivity factor, *t*,

$0 \le t \le 1$.

$$\mathbf{s} = \begin{bmatrix} a_1 N & a_2 N_2 & \dots & a_m N_m \end{bmatrix}$$

$$\mathbf{T} = \begin{bmatrix} t_{11} & t_{12} & \dots & t_{1m} \\ t_{21} & t_{22} & \dots & t_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ t_{m1} & t_{m2} & \dots & t_{mm} \end{bmatrix} \qquad t_{ij} = 1 \Big|_{i=j}$$

$$\mathbf{v} = \begin{bmatrix} v_1 & v_2 & \dots & v_m \end{bmatrix}$$

$$\mathbf{v}^{\mathrm{T}} = \mathbf{T} \cdot \mathbf{s}^{\mathrm{T}}$$

$$\mathbf{n} = \begin{bmatrix} N_1 & N_2 & \dots & N_m \end{bmatrix}$$

$$V = \mathbf{n} \cdot \mathbf{v}^{\mathrm{T}} = \mathbf{n} \cdot \mathbf{T} \cdot \mathbf{s}^{\mathrm{T}}$$

https://medium.com/selfrule/meta-platforms-and-cooperative-network-of-networks-effects-6e61eb15c586

https://medium.com/selfrule/meta-platforms-and-cooperative-network-of-networks-effects-6e61eb15c586

GitHub

SmithSamuelM

Papers

Metcalfe's Law Validation

Madureira A., F. den Hartog, H. Bouwman *et al.*, "Empirical validation of Metcalfe's law: How Internet usage patterns have changed over time," *Information Economics and Policy*, vol. 25, no. 4, pp. 246–256, 2013

Metcalfe B., "Metcalfe's law after 40 years of ethernet," *Computer*, vol. 46, no. 12, pp. 26–31, 2013

Van Hove L., "Testing Metcalfe's law: pitfalls and possibilities," *ES-Working Paper*, 2016/08/01 http://research.vub.ac.be/sites/default/files/uploads/BUTO/Working-Papers/es_working_paper_6_-_van_hove_l._2016_testing_metcalfes_law._pitfalls_and_possibilities.pdf

Van Hove L., "Metcalfe's law: not so wrong after all," *NETNOMICS: Economic Research and Electronic Networking*, vol. 15, no. 1, pp. 1–8, 2014

Van Hove L., "Metcalfe's Law and Network Quality: An Extension of Zhang et al.," *Journal of Computer Science and Technology*, vol. 31, no. 1, pp. 117–123, 2016

Van Hove L., "Testing Metcalfe's law: Pitfalls and possibilities," *Information Economics and Policy*, vol. 37, pp. 67–76, 2016

Zhang X.-Z., J.-J. Liu and Z.-W. Xu, "Tencent an dFacebook Data Validate Metcalfe's Law," *Journal of Computer Science and Technology*, vol. 30, no. 2, pp. 246–251, March 2015

Xie, J. and Sirbu, M., "Price competition and compatibility in the presence of positive demand externalities," *Management science*, vol. 41, no. 5, pp. 909-926, 1995

Reading List 1

Anderson C., “The Long Tail,” *Wired*, 2004/10/01 https://www.wired.com/2004/10/tail/
Anderson C. , “The Long Tail: Why the Future of Business Is Selling Less of More,” Random House, 2006/07/11.
Bennet J. , “Sarnoff’s Law,” *Protocoldigital.com*, 2013/12/03 http://protocoldigital.com/blog/sarnoffs-law/
Briscoe B., A. Odlyzko and B. Tilly, “Metcalfe’s law is wrong-communications networks increase in value as they add members-but by how much,” *IEEE Spectrum*, vol. 43, no. 7, pp. 34–39, 2006
Conway S., A. H., M. Ma *et al.*, “A DID for Everything,” *RWOT Fall 2018*, 2018/09/26 https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/A_DID_for_everything.pdf
Currier J., “The NFX Archives: Foundations for Mastering Network Effects,” *NFX.com*, https://www.nfx.com/post/network-effects-archives
“Decentralized Identifiers (DIDs),” *W3C Draft Community Group Report 23 August 2018*, https://w3c-ccg.github.io/did-spec/
DIF “Join us in building an open source decentralized identity ecosystem for people, organizations, apps, and devices.,” *Decentralized Identity Foundation (DIF)*, http://identity.foundation
Erickson K. J., “The Future Of Network Effects: Tokenization and the End of Extraction,” *Medium.com*, 2018/07/17 https://medium.com/public-market/the-future-of-network-effects-tokenization-and-the-end-of-extraction-a0f895639ffb
Ferguson N., “The square and the tower: Networks and power, from the freemasons to Facebook,” Penguin Books, 2019.
Griffen T., “A Dozen Things I’ve Learned from Nassim Taleb about Optionality/Investing,” *25IQ*, 2013/10/13 https://25iq.com/2013/10/13/a-dozen-things-ive-learned-from-nassim-taleb-about-optionalityinvesting/
Kilkki K. and M. Kalervo, “KK-law for group forming services,” vol. XVth International Symposium on Services and Local Access, pp. 21–26, 2004
Madureira A., F. den Hartog, H. Bouwman *et al.*, “Empirical validation of Metcalfe’s law: How Internet usage patterns have changed over time,” *Information Economics and Policy*, vol. 25, no. 4, pp. 246–256, 2013
Metcalfe’s Law, *Wikipedia*, https://en.wikipedia.org/wiki/Metcalfe%27s_law
Metcalfe B., “Metcalfe’s law after 40 years of ethernet,” *Computer*, vol. 46, no. 12, pp. 26–31, 2013
Metcalfe B., “Metcalfe’s Law Recurses Down the Long Tail of Social Networking,” *VCMikes’s Blog*, 2006/08/16 https://vcmike.wordpress.com/2006/08/18/metcalfe-social-networks/
Munger M. C., “Tomorrow 3.0: Transaction costs and the sharing economy,” Cambridge University Press, 2018.
Odlyzko A. and B. Tilly, “A refutation of Metcalfe’s Law and a better estimate for the value of networks and network interconnections,” *Manuscript, March*, vol. 2, pp. 2005, 2005

Reading List 2

Pearson T., “Markets Are Eating The World,” *RibbonFarm*, 2019/02/18 https://www.ribbonfarm.com/2019/02/28/markets-are-eating-the-world/

Parker G. G., M. W. Van Alstyne and S. P. Choudary, “Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You,” WW Norton & Company, 2016.

Rajan R. G. and L. Zingales, “Saving capitalism from the capitalists: Unleashing the power of financial markets to create wealth and spread opportunity,” Princeton University Press, 2004.

Reed D. P., “The law of the pack.,” *Harvard business review*, vol. 79, no. 2, pp. 23, 2001

“Reed’s Law,” *Wikipedia*, https://en.wikipedia.org/wiki/Reed%27s_law

Reed D. P., “That Sneaky Exponential—Beyond Metcalfe’s Law to the Power of Community Building https://www.deepplum.com/dpr/locus/gfn/reedslaw.html

Reed, D.P. Beyond Metcalfe’s Law to the Power of Community Building,” 1999 https://www.deepplum.com/dpr/locus/gfn/reedslaw.html

Smith S. M., “Open Reputation Framework,” vol. Version 1.2, 2015/05/13 https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/open-reputation-low-level-whitepaper.pdf

Smith S. M., “Decentralized Autonomic Data (DAD) and the three R’s of Key Management,” Spring 2018 https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-spring2018/blob/master/final-documents/DecentralizedAutonomicData.pdf

S. M. Smith and D. Khovratovich, “Identity System Essentials,” 2016/03/29 https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/Identity-System-Essentials.pdf

Smith S. M.. https://medium.com/selfrule/is-it-real-or-is-it-virtual-currency-8f86665b6c04

Taleb N., “Antifragile: Things That Gain from Disorder,” Random House, 2012.

Taleb N., “Convexity Science,” *FooledByRandomness.com*, 2012 http://www.fooledbyrandomness.com/ConvexityScience.pdf

Van Hove L., “Testing Metcalfe’s law: pitfalls and possibilities,” *ES-Working Paper*, 2016/08/01 http://research.vub.ac.be/sites/default/files/uploads/BUTO/Working-Papers/es_working_paper_6_-_van_hove_l._2016_testing_metcalfes_law._pitfalls_and_possibilities.pdf

Van Hove L., “Metcalfe’s law: not so wrong after all,” *NETNOMICS: Economic Research and Electronic Networking*, vol. 15, no. 1, pp. 1–8, 2014

Van Hove L., “Metcalfe’s Law and Network Quality: An Extension of Zhang et al.,” *Journal of Computer Science and Technology*, vol. 31, no. 1, pp. 117–123, 2016

Van Hove L., “Testing Metcalfe’s law: Pitfalls and possibilities,” *Information Economics and Policy*, vol. 37, pp. 67–76, 2016

Wu, T. “The Master Switch: The Rise and Fall of Information Empires” Random House, 2010. https://www.amazon.com/Master-Switch-Rise-Information-Empires-ebook/dp/B003F3PKTK/ref=sr_1_1?keywords=The+master+switch&qid=1553973768&s=digital-text&sr=1-1

Xie, J. and Sirbu, M., “Price competition and compatibility in the presence of positive demand externalities,” *Management science*, vol. 41, no. 5, pp. 909-926, 1995

Zhang X.-Z., J.-J. Liu and Z.-W. Xu, “Tencent an dFacebook Data Validate Metcalfe’s Law,” *Journal of Computer Science and Technology*, vol. 30, no. 2, pp. 246–251, March 2015

Resources

sam@prosapien.com

https://arxiv.org/abs/1907.02143
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf
https://github.com/SmithSamuelM/Papers/blob/master/presentations/KERI2_Overview.web.pdf
https://github.com/SmithSamuelM/Papers/blob/master/presentations/DuplicityGame_IIW_2020_A.pdf
https://github.com/SmithSamuelM/keri
https://github.com/SmithSamuelM/keripy

DIF
Identity and Discovery WG
https://github.com/decentralized-identity/keri
https://github.com/decentralized-identity/keripy

SSI Meetup
https://ssimeetup.org/key-event-receipt-infrastructure-keri-secure-identifier-overlay-internet-sam-smith-webinar-58/

Background References

Self-Certifying Identifiers:

Girault, M., "Self-certified public keys," EUROCRYPT 1991: Advances in Cryptology, pp. 490-497, 1991
https://link.springer.com/content/pdf/10.1007%2F3-540-46416-6_42.pdf

Mazieres, D. and Kaashoek, M. F., "Escaping the Evils of Centralized Control with self-certifying pathnames," MIT Laboratory for Computer Science,
http://www.sigops.org/ew-history/1998/papers/mazieres.ps

Kaminsky, M. and Banks, E., "SFS-HTTP: Securing the Web with Self-Certifying URLs," MIT, 1999
https://pdos.csail.mit.edu/~kaminsky/sfs-http.ps

Mazieres, D., "Self-certifying File System," MIT Ph.D. Dissertation, 2000/06/01
https://pdos.csail.mit.edu/~ericp/doc/sfs-thesis.ps

TCG, "Implicit Identity Based Device Attestation," Trusted Computing Group, vol. Version 1.0, 2018/03/05
https://trustedcomputinggroup.org/wp-content/uploads/TCG-DICE-Arch-Implicit-Identity-Based-Device-Attestation-v1-rev93.pdf

Autonomic Identifiers:

Smith, S. M., "Open Reputation Framework," vol. Version 1.2, 2015/05/13
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/open-reputation-low-level-whitepaper.pdf

Smith, S. M. and Khovratovich, D., "Identity System Essentials," 2016/03/29
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/Identity-System-Essentials.pdf

Smith, S. M., "Decentralized Autonomic Data (DAD) and the three R's of Key Management," Rebooting the Web of Trust RWOT 6, Spring 2018
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/DecentralizedAutonomicData.pdf

Smith, S. M., "Key Event Receipt Infrastructure (KERI) Design and Build", arXiv, 2019/07/03 revised 2020/04/23
https://arxiv.org/abs/1907.02143

Smith, S. M., "Key Event Receipt Infrastructure (KERI) Design", 2020/04/22
https://github.com/SmithSamuelM/Papers/blob/master/whitepapers/KERI_WP_2.x.web.pdf

Stocker, C., Smith, S. and Caballero, J., "Quantum Secure DIDs," RWOT10, 2020/07/09
https://github.com/WebOfTrustInfo/rwot10-buenosaires/blob/master/final-documents/quantum-secure-dids.pdf

Certificate Transparency:

Laurie, B., "Certificate Transparency: Public, verifiable, append-only logs," ACMQueue, vol. Vol 12, Issue 9, 2014/09/08
https://queue.acm.org/detail.cfm?id=2668154

Google, "Certificate Transparency,"
http://www.certificate-transparency.org/home

Laurie, B. and Kasper, E., "Revocation Transparency,"
https://www.links.org/files/RevocationTransparency.pdf