Temporal Implications of Database Information Accountability

Kyriacos E. Pavlou and Richard T. Snodgrass

Computer Science Department
The University of Arizona

TIME 2012

The University of Arizona

Motivation

Motivation

Corporate collusion has given rise to regulations for trustworthy long-term data management.

- Code of Federal Regulations of FDA: Clinical trials

Motivation

Corporate collusion has given rise to regulations for trustworthy long-term data management.

- Code of Federal Regulations of FDA: Clinical trials
- Sarbanes-Oxley Act: Financial transactions
- HIPAA – Health Insurance Portability and Accountability Act; Canada's PIPEDA: Disclosure of medical information

Introduction

Introduction

- File systems & DB communities

Introduction

- File systems & DB communities
  - tamper detection / prevention mechanisms

Introduction

- File systems & DB communities
  - tamper detection / prevention mechanisms
- Audit log security & compliant records
  - Creation
  - Storage
  - Access
  - Maintenance / Retention

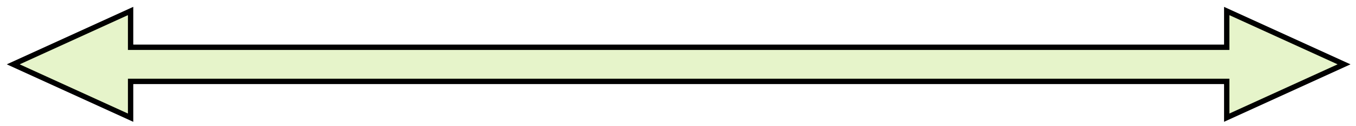
Introduction

- File systems & DB communities
  - tamper detection / prevention mechanisms
- Audit log security & compliant records
  - Creation
  - Storage
  - Access
  - Maintenance / Retention

Governed by laws & regulations

Spectrum of Approaches to Achieve Trustworthiness

Spectrum of Approaches to Achieve Trustworthiness

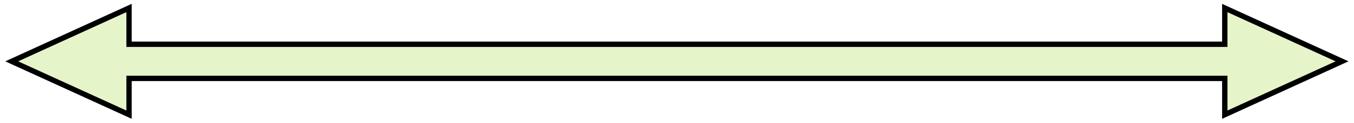


Information Restriction

immutable retained records

access control

Spectrum of Approaches to Achieve Trustworthiness



Information Restriction

immutable retained records

access control

Information Accountability

transparent information

set of rules

easily determine appropriate use

Spectrum of Approaches to Achieve Trustworthiness

Information Restriction

immutable retained records
access control

Information Accountability

transparent information
set of rules
easily determine appropriate use

"[Information] accountability must become a primary means through which society addresses appropriate use." (Weitzner et al., CACM 2008)

Restriction vs Accountability

Restriction vs Accountability

- Home Security
  - Locked doors and windows (restriction)
  - Sweeping front yard, cameras (accountability)

Restriction vs Accountability

- Home Security
  - Locked doors and windows (restriction)
  - Sweeping front yard, cameras (accountability)
- Bank Security
  - The vault is unlocked during business hours.
  - Easy access
  - CCTV cameras everywhere

Information Accountability

Information Accountability

- Tried and tested idea

Information Accountability

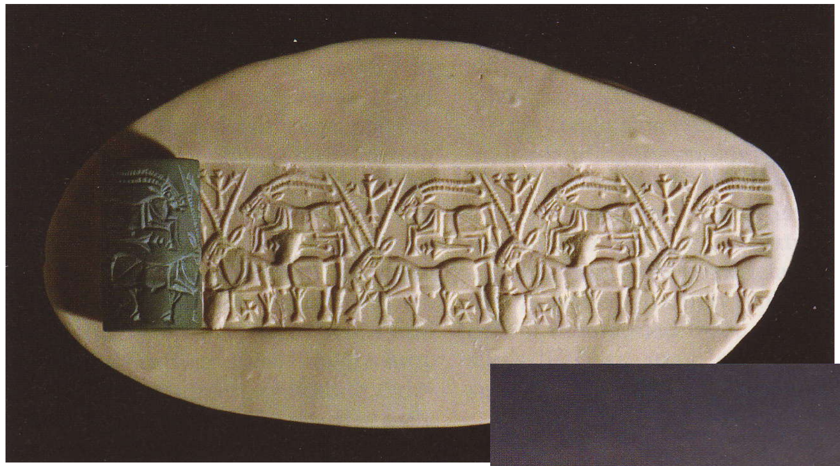
- Tried and tested idea
- Example: Bullae, sigils, seals, etc

Information Accountability

- Tried and tested idea
- Example: Bullae, sigils, seals, etc

Information Accountability

- Tried and tested idea
- Example: Bullae, sigils, seals, etc

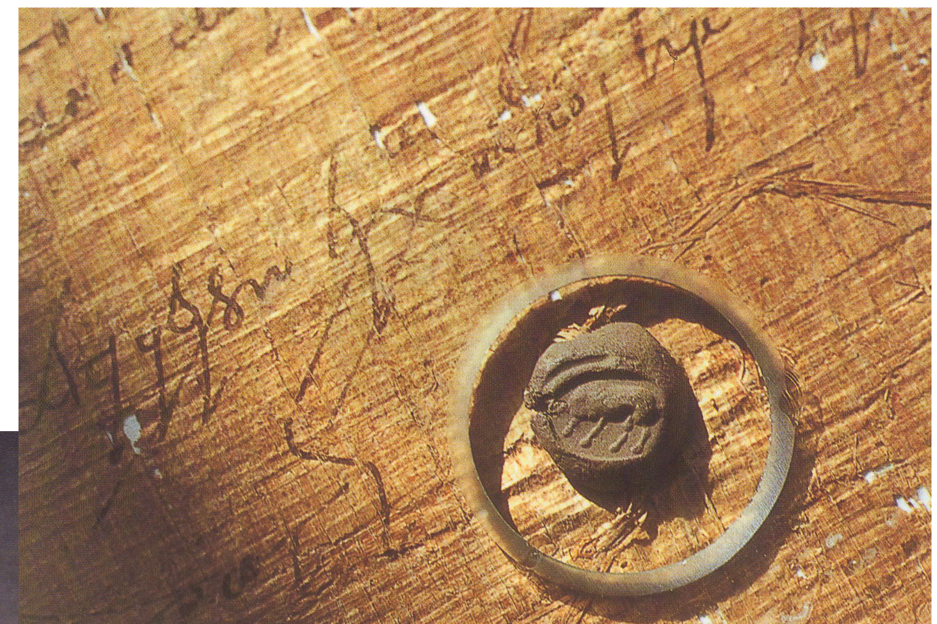


Information Accountability

- Tried and tested idea
- Example: Bullae, sigils, seals, etc

Information Accountability

- Tried and tested idea
- Example: Bullae, sigils, seals, etc

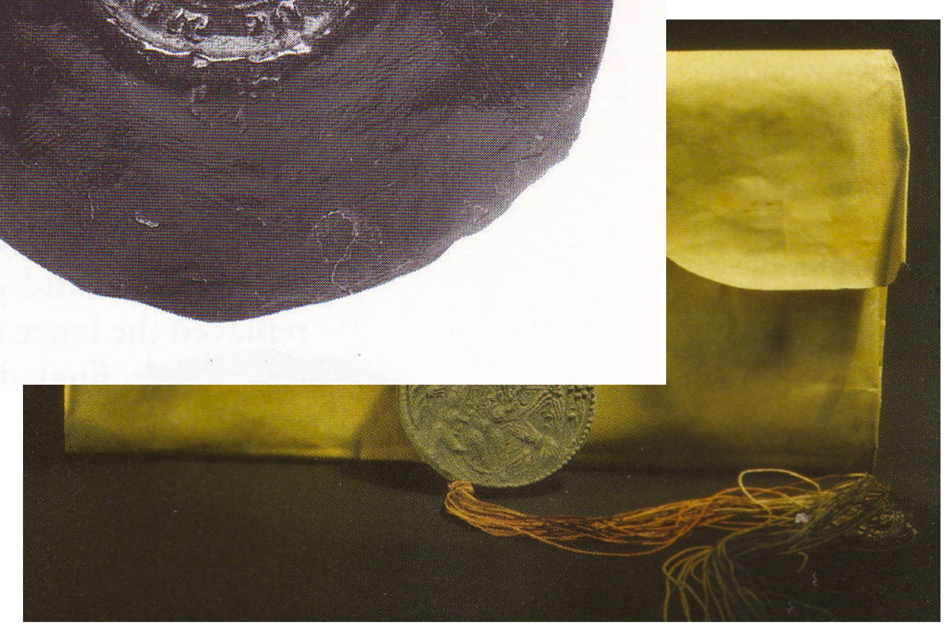


Information Accountability

- Tried and tested idea
- Example: Bullae, sigils, seals, etc

Information Accountability

- Tried and tested idea
- Example: Bullae, sigils, seals, etc



Information Accountability (2)

Information Accountability (2)

- Tried and tested idea

Information Accountability (2)

- Tried and tested idea
- Example: Fair Credit Reporting Act (1970)

No rules on the collection of data and analysis but on their use (credit report).

Information Accountability (2)

- Tried and tested idea
- Example: Fair Credit Reporting Act (1970)

No rules on the collection of data and analysis but on their use (credit report).

The consumers are allowed access to the data.

Information Accountability (2)

- Tried and tested idea
- Example: Fair Credit Reporting Act (1970)

No rules on the collection of data and analysis but on their use (credit report).

The consumers are allowed access to the data.

Agencies using credit reports are accountable for their decisions.

Information Accountability (3)

Information Accountability (3)

- Tried and tested idea

Information Accountability (3)

- Tried and tested idea
- Example: Creative Commons Licensing

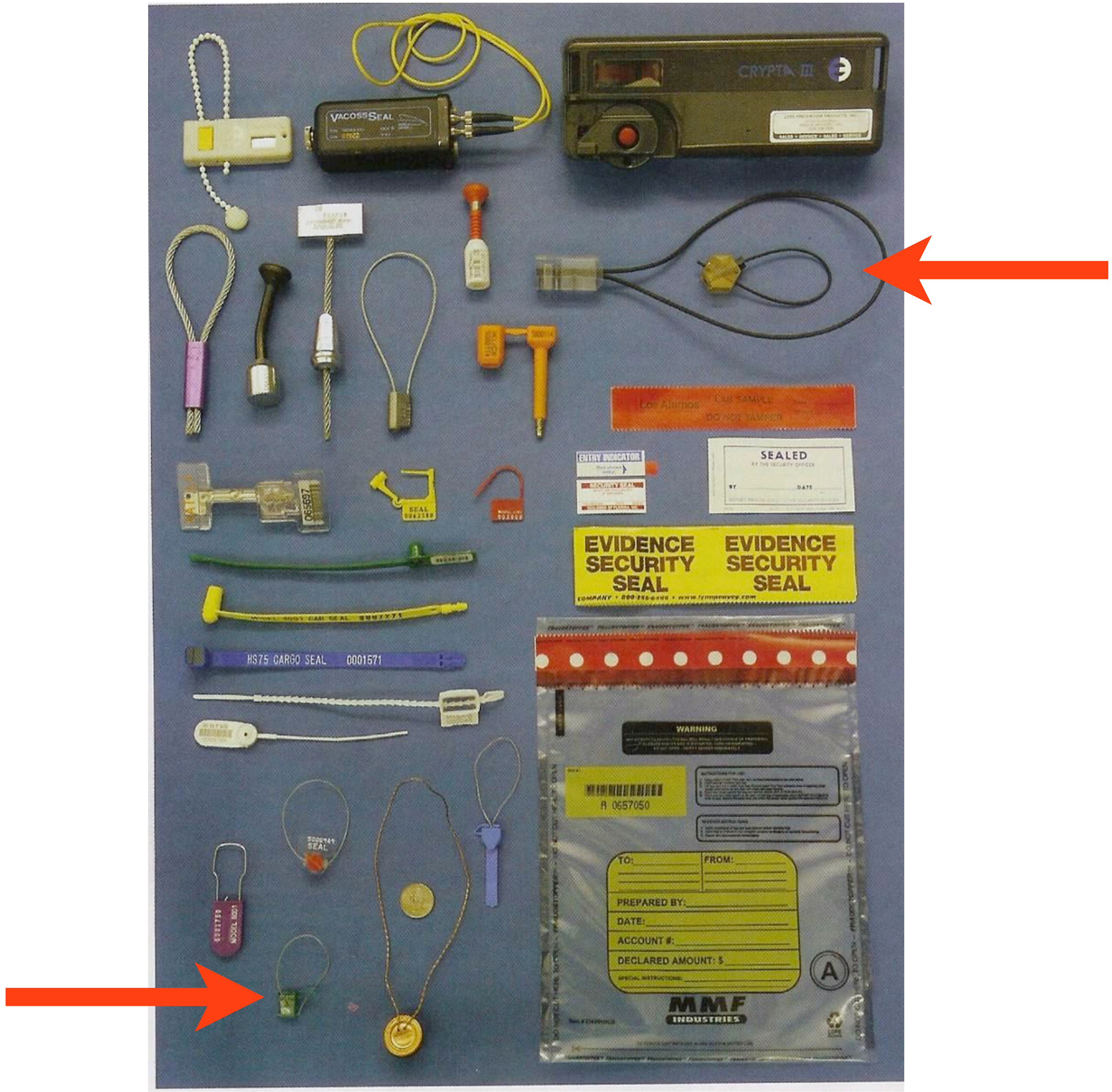
Information Accountability (3)

- Tried and tested idea
- Example: Creative Commons Licensing

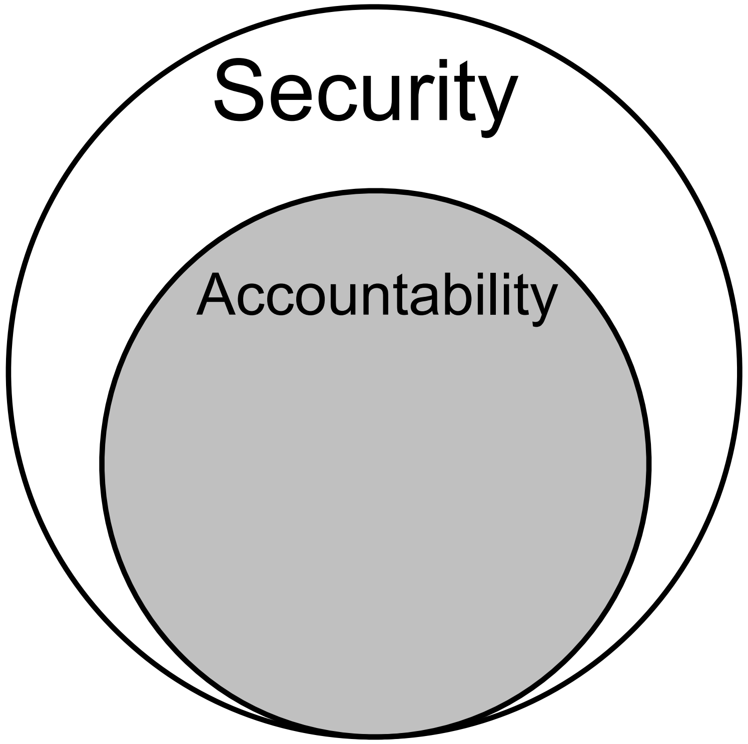
Do not attempt to prevent
the lawful use of works
they protect by using technology,
but rather set forth rules
regulating the use of the works.

Tamper-Indicating Seals for Nuclear Safeguarding

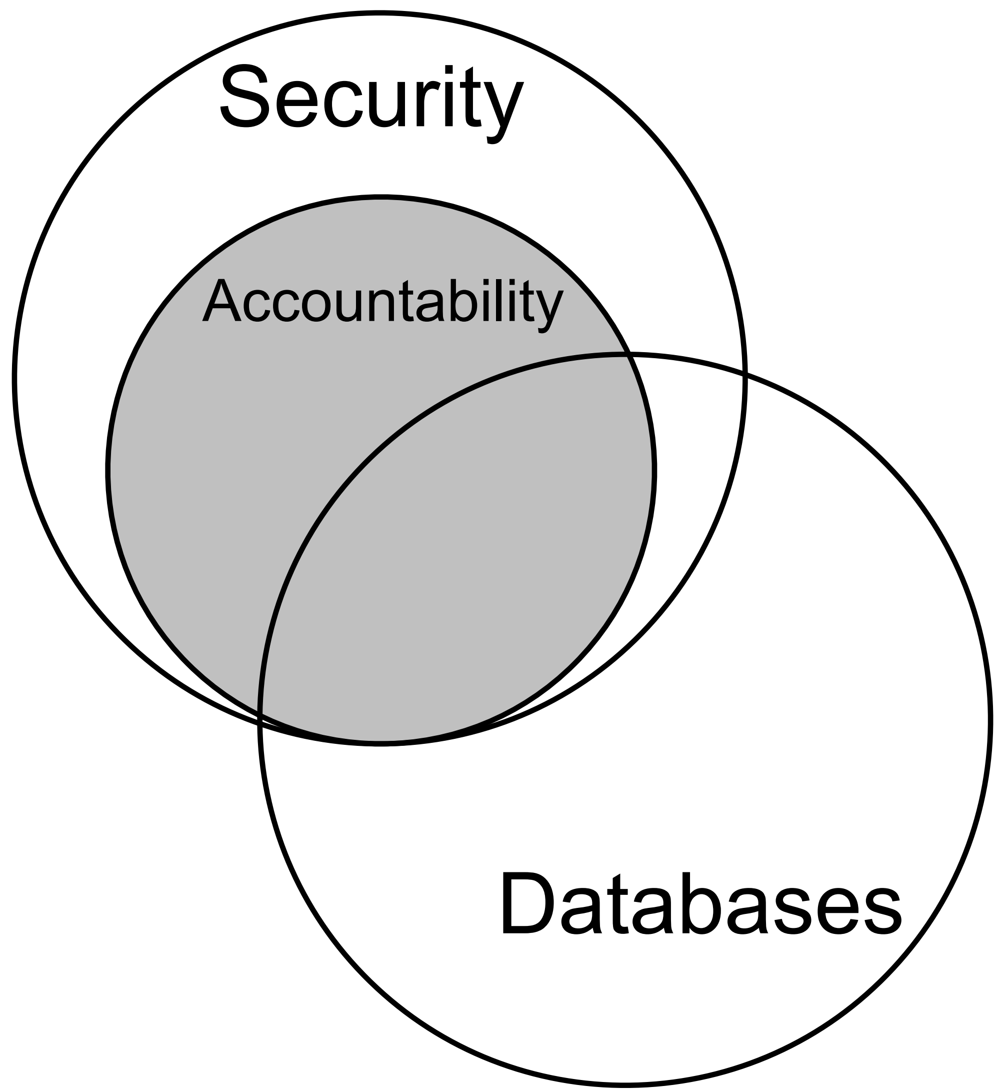
Tamper-Indicating Seals for Nuclear Safeguarding



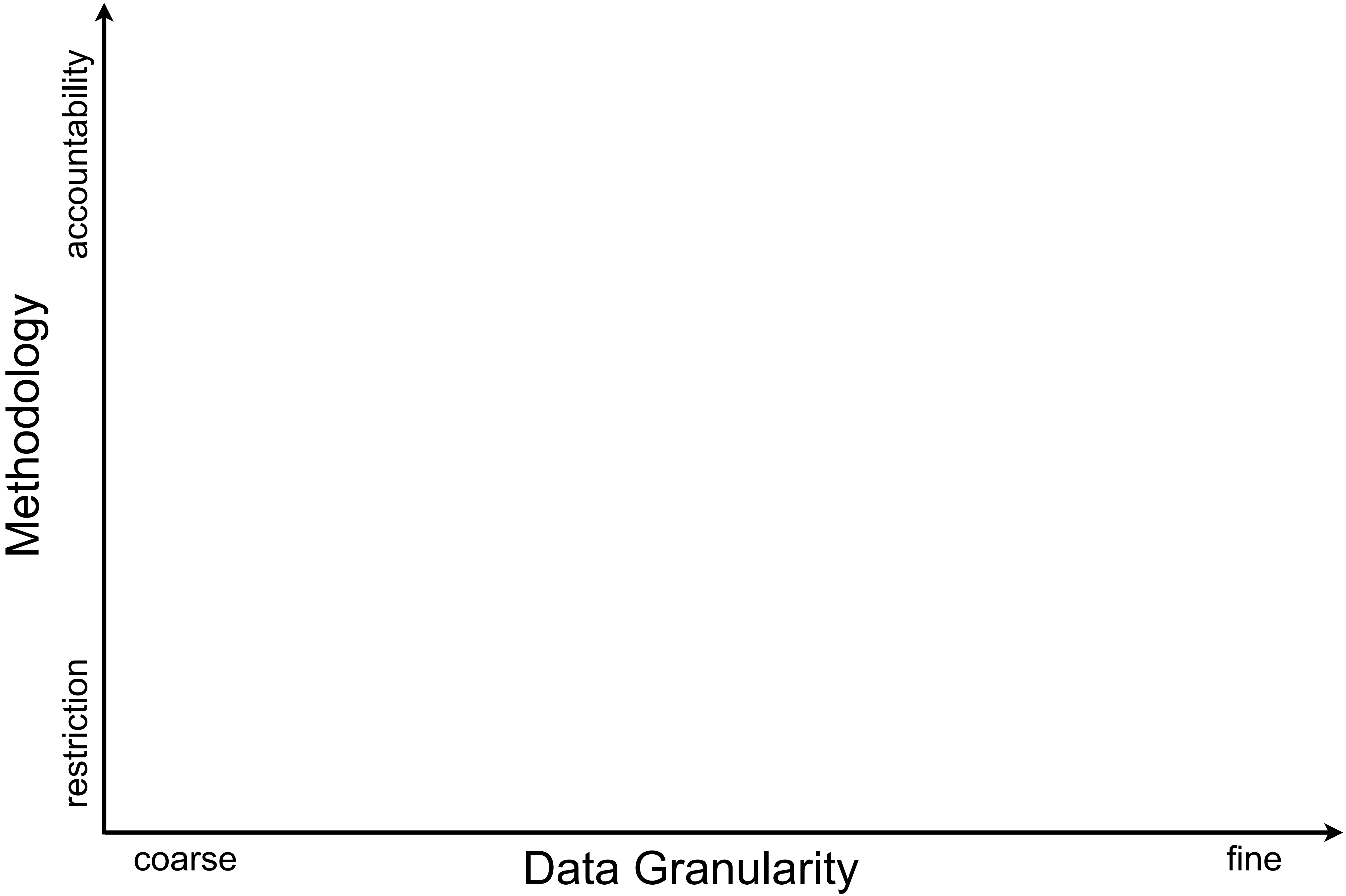
Accountability ∩ Databases



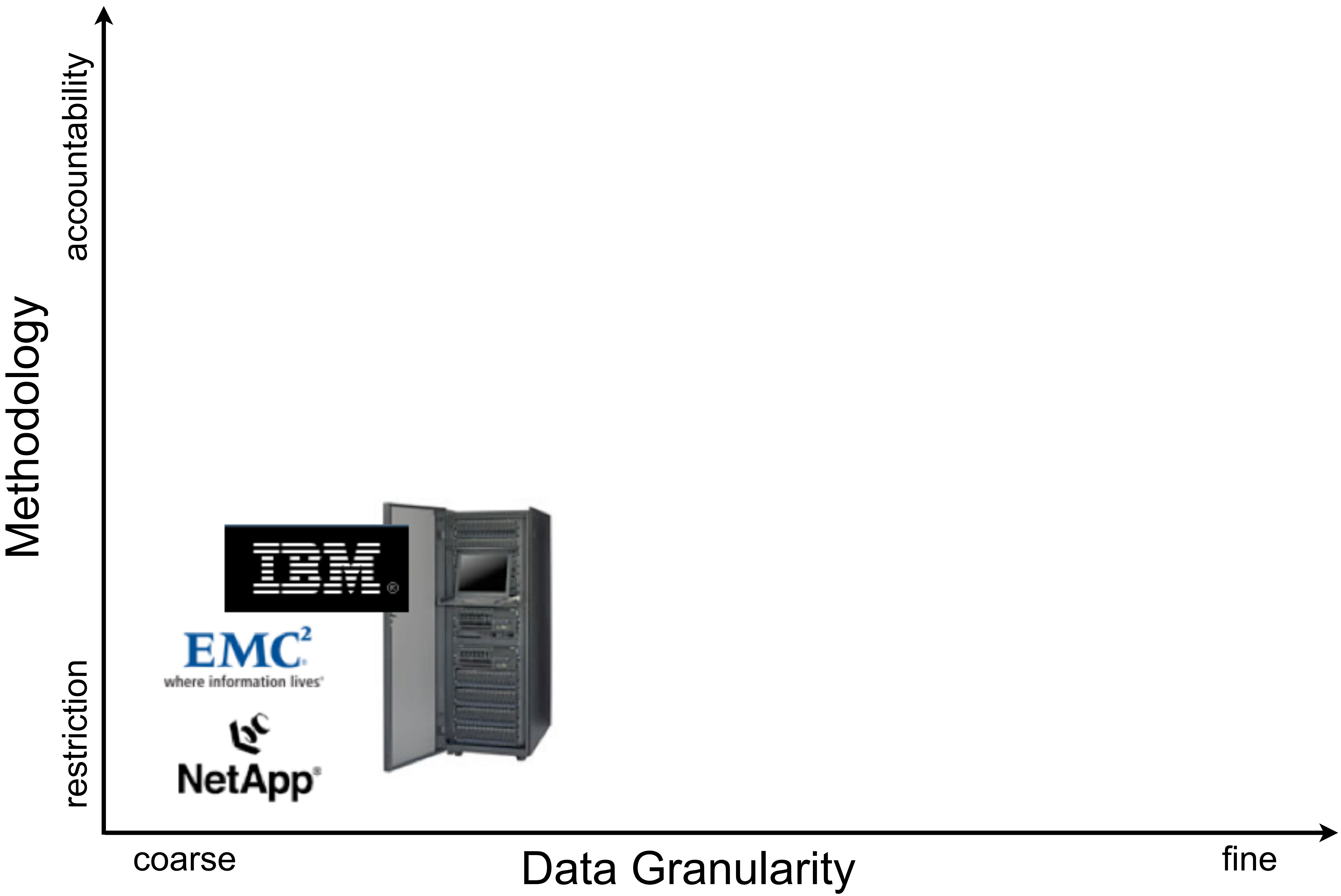
Accountability ∩ Databases



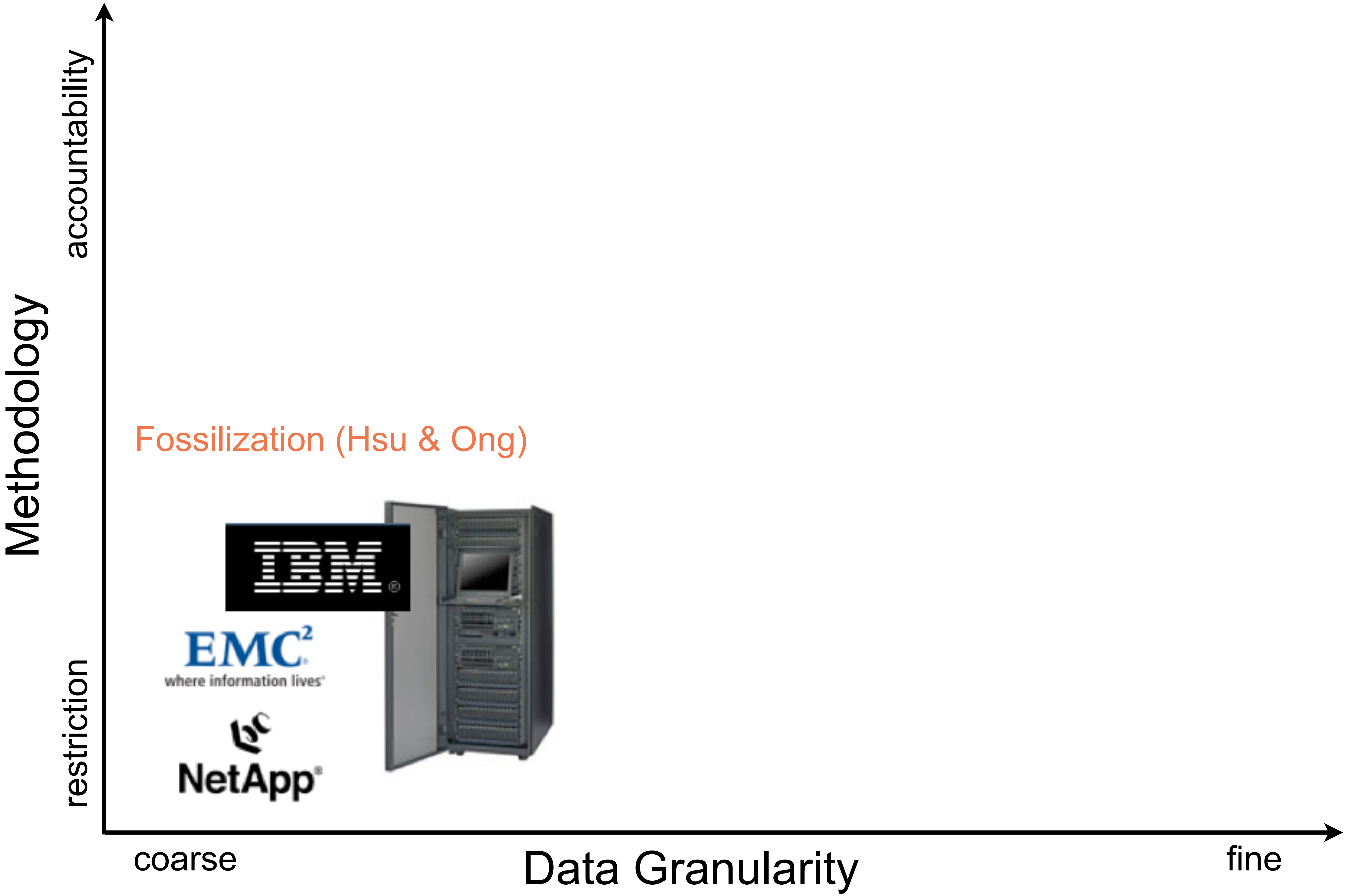
Related Work & Security Spectrum



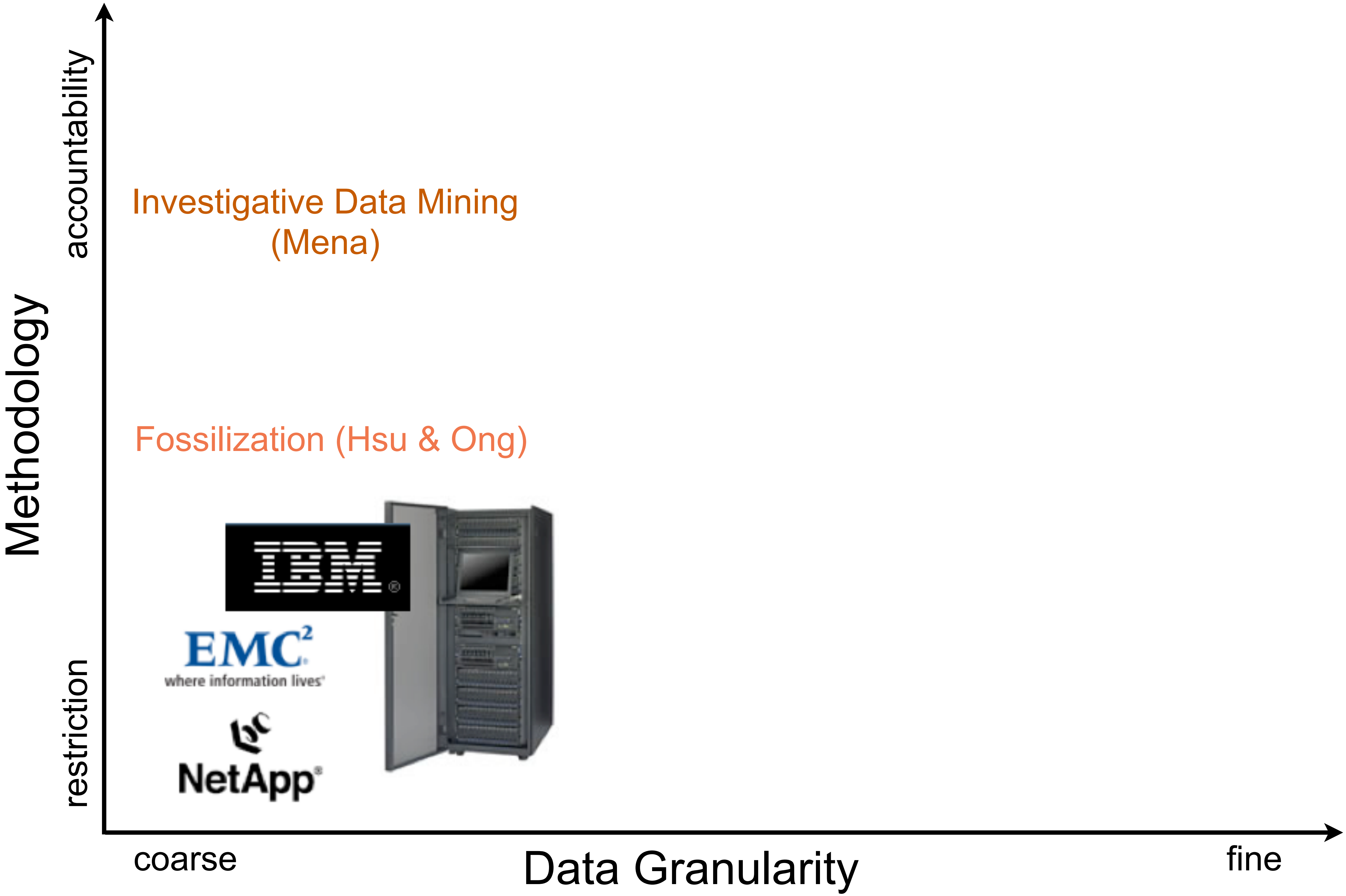
Related Work & Security Spectrum



Related Work & Security Spectrum



Related Work & Security Spectrum



Related Work & Security Spectrum

accountability

Forensic Server Project
(Carvey & Kleiman)

Investigative Data Mining
(Mena)

Methodology

Fossilization (Hsu & Ong)

IBM

EMC²
where information lives

NetApp

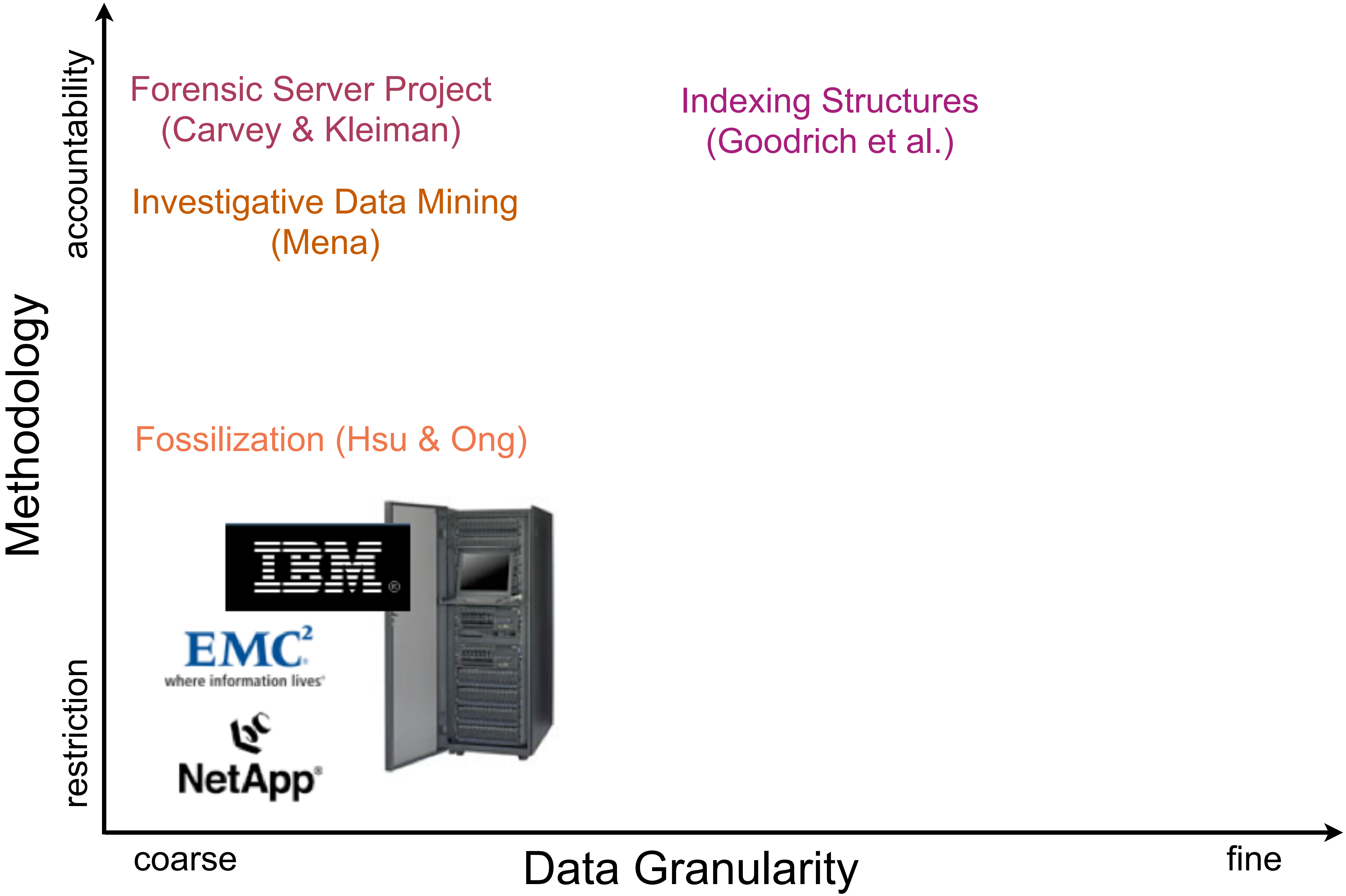
restriction

coarse

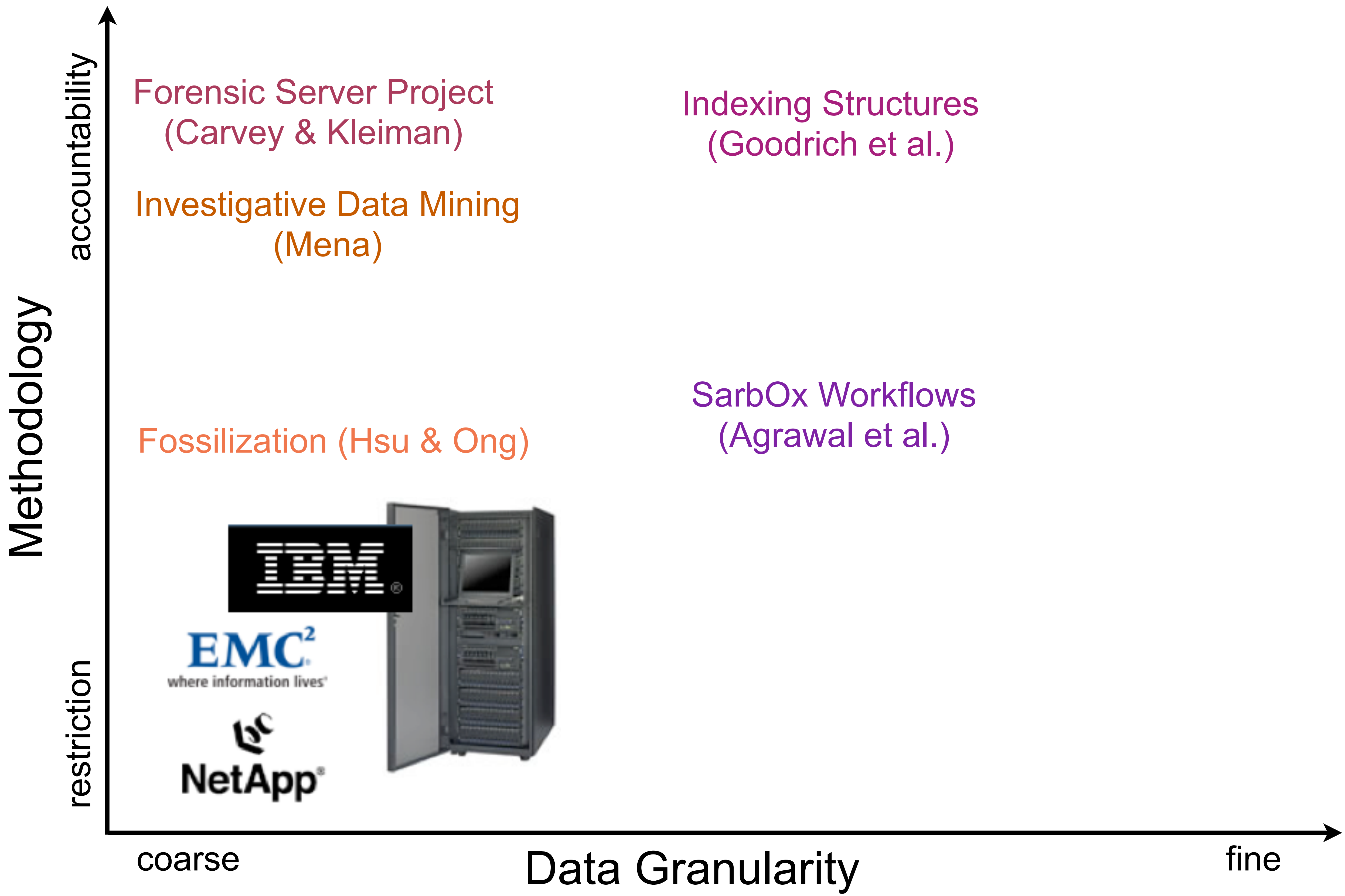
Data Granularity

fine

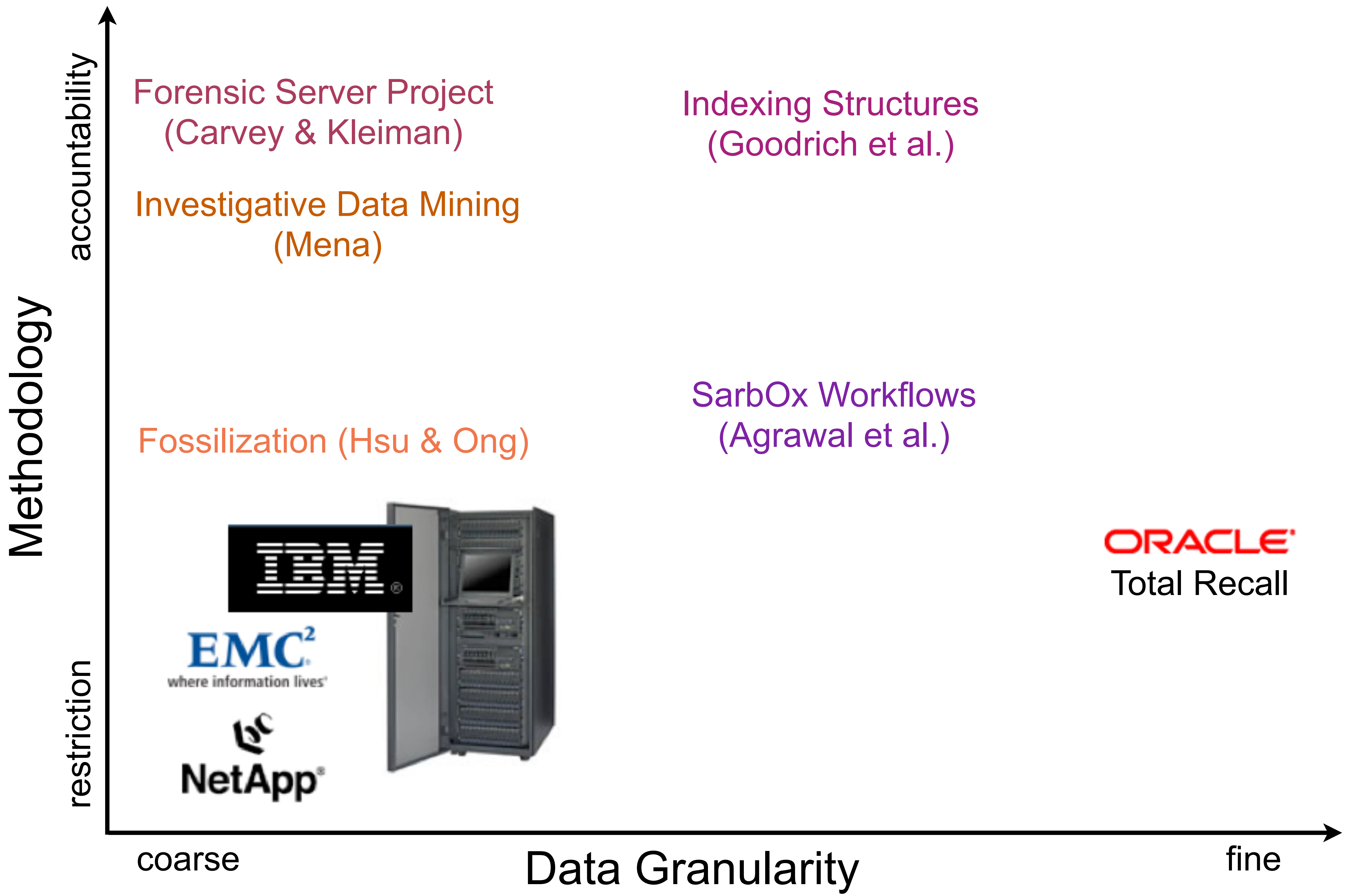
Related Work & Security Spectrum



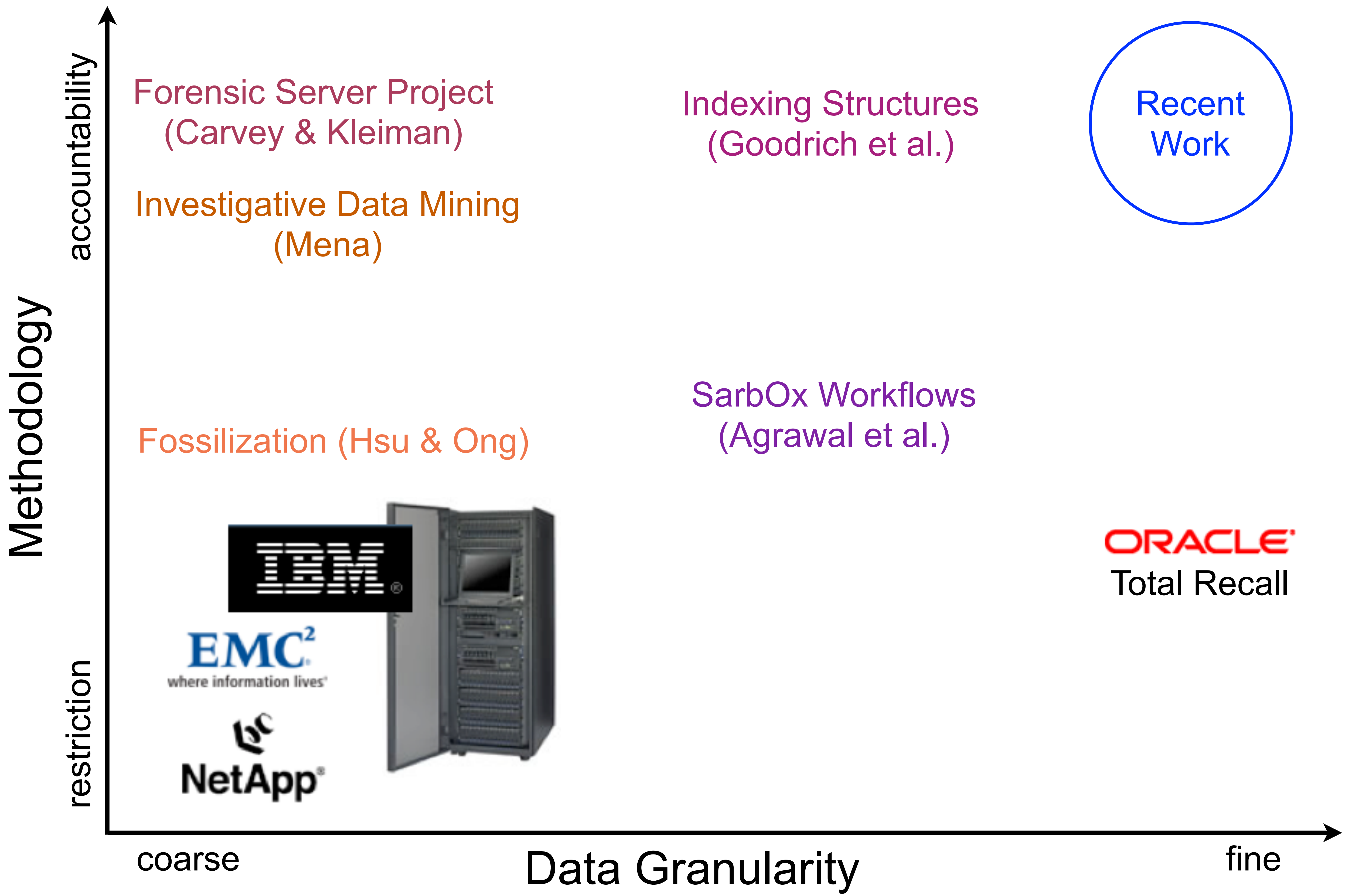
Related Work & Security Spectrum



Related Work & Security Spectrum



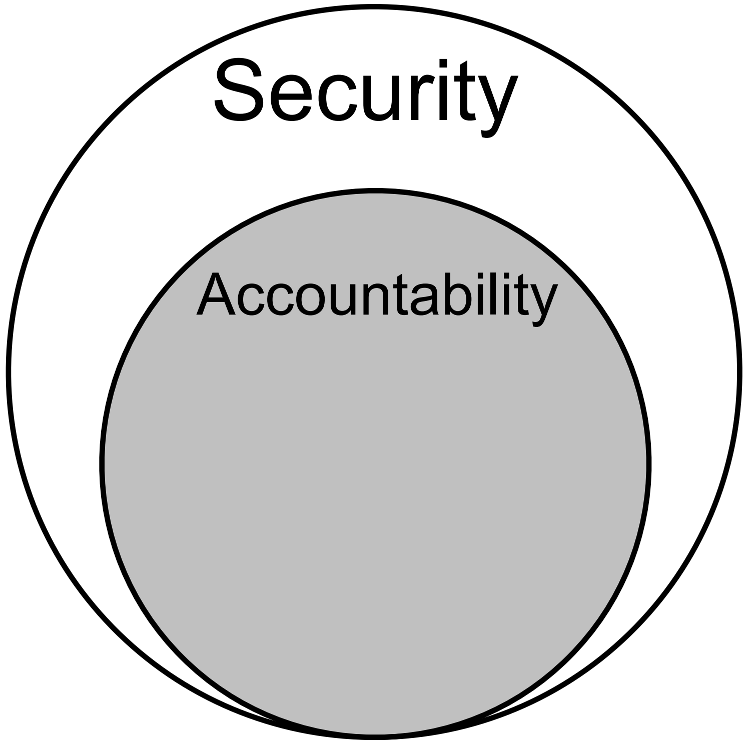
Related Work & Security Spectrum



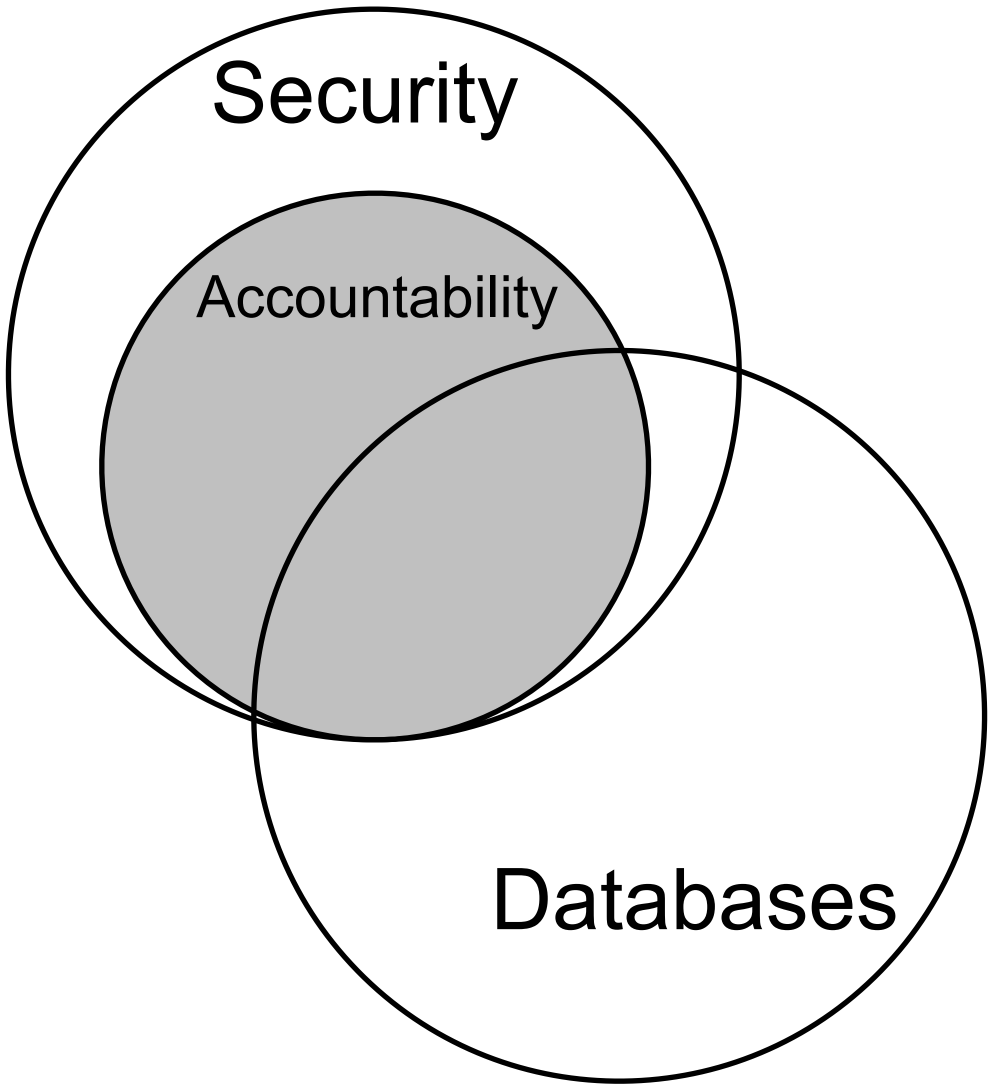
Info Accountability of Fine-Grained Data

- Fragile watermarking scheme for detecting malicious modifications of database relations [Guo, Li, Liu, and Jajodia 2006].
- Efficient audit-based compliance for relational data retention [Hasan, Winslett, and Mitra 2009].
- Tamper detection in audit logs [Snodgrass, Yao, and Collberg 2004].

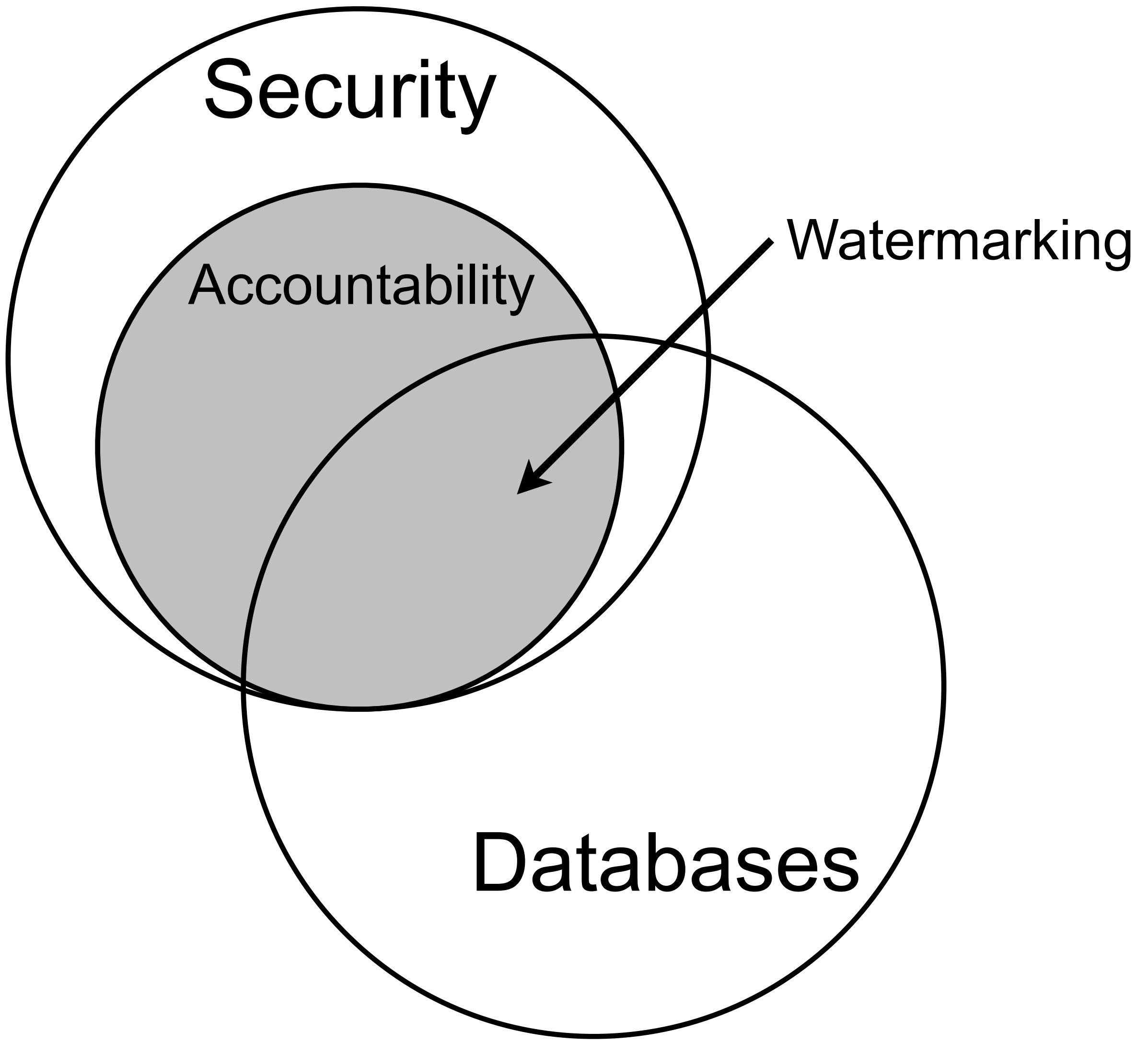
Accountability ∩ Databases ∩ Time



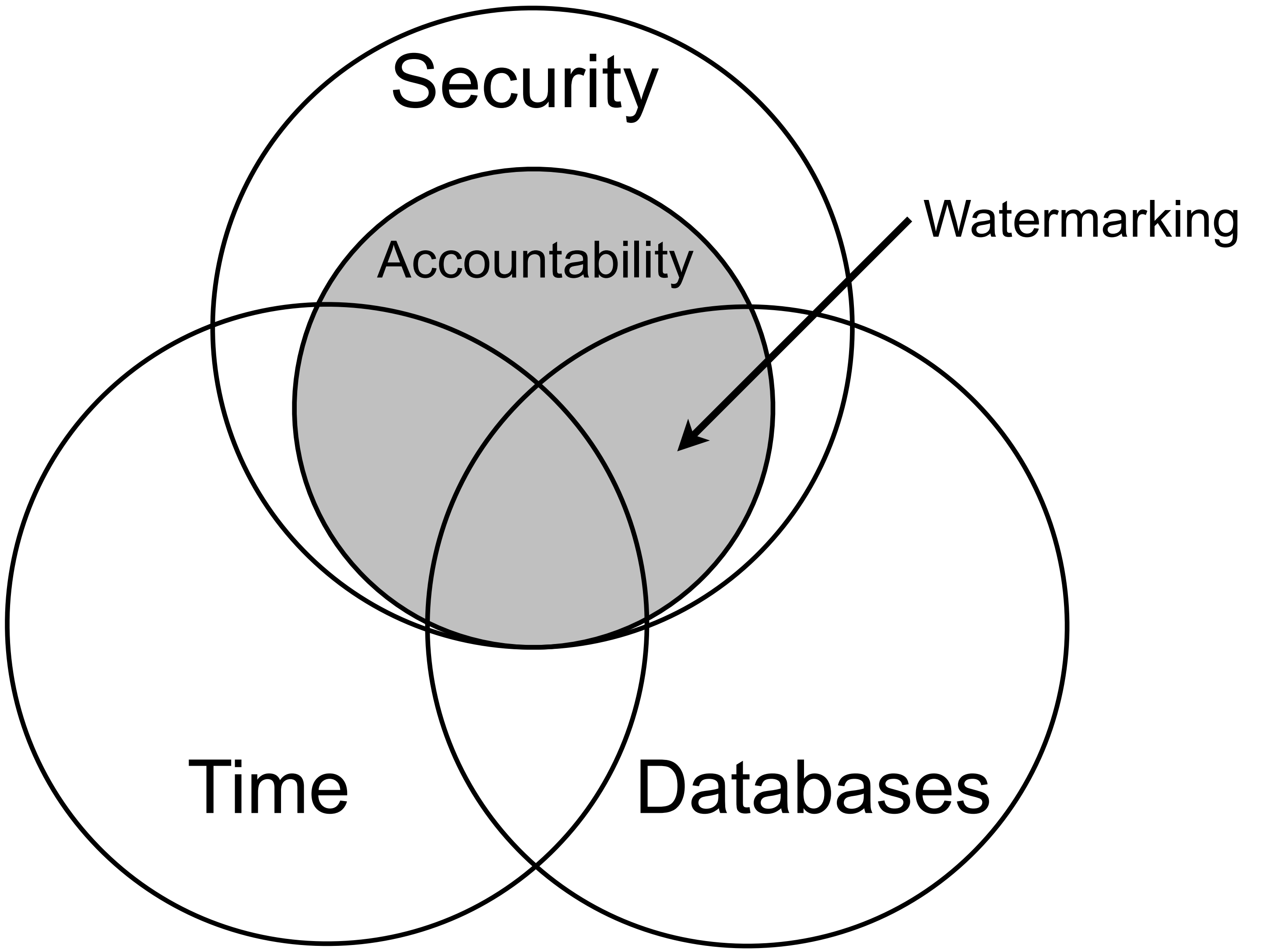
Accountability ∩ Databases ∩ Time



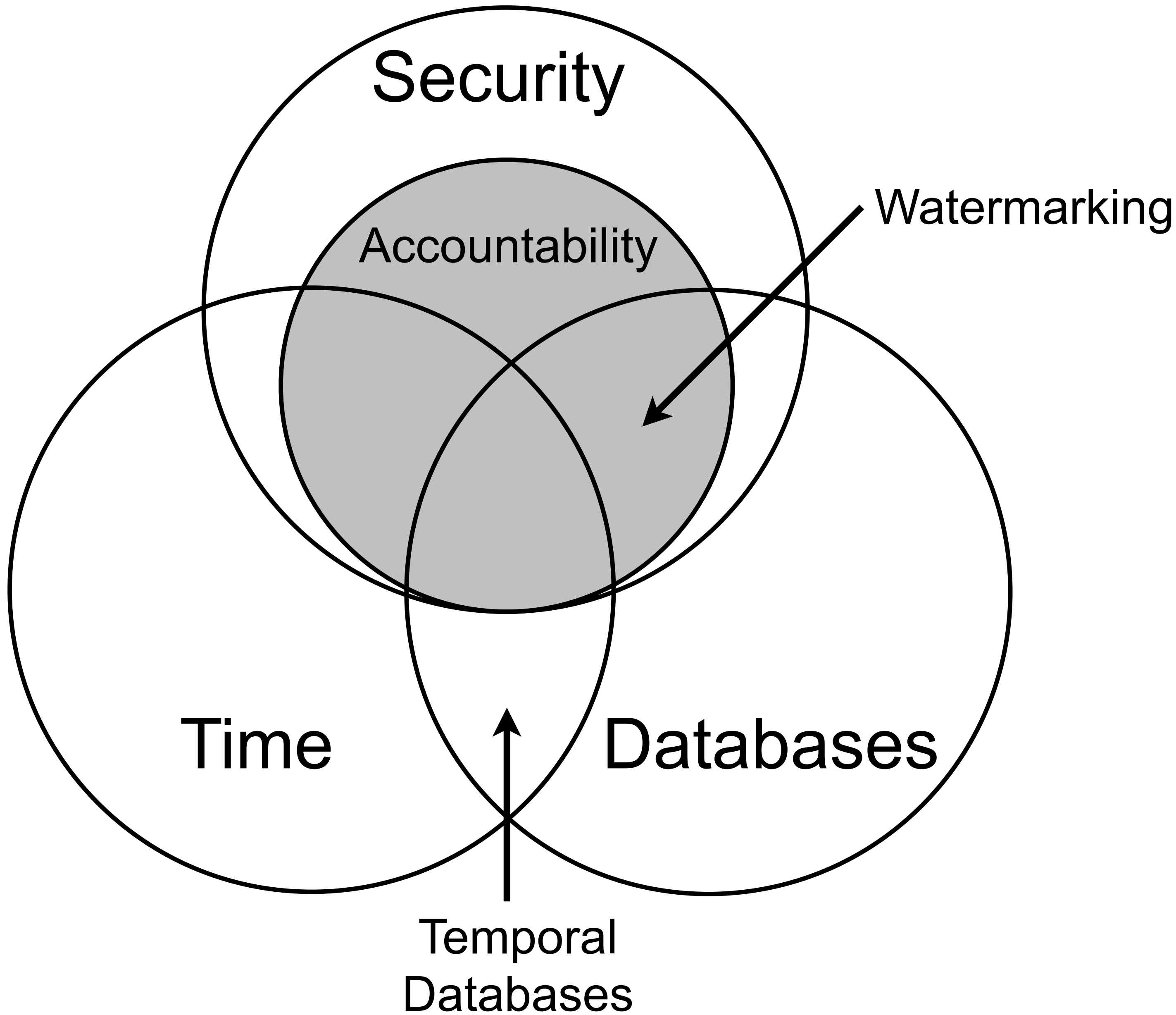
Accountability ∩ Databases ∩ Time



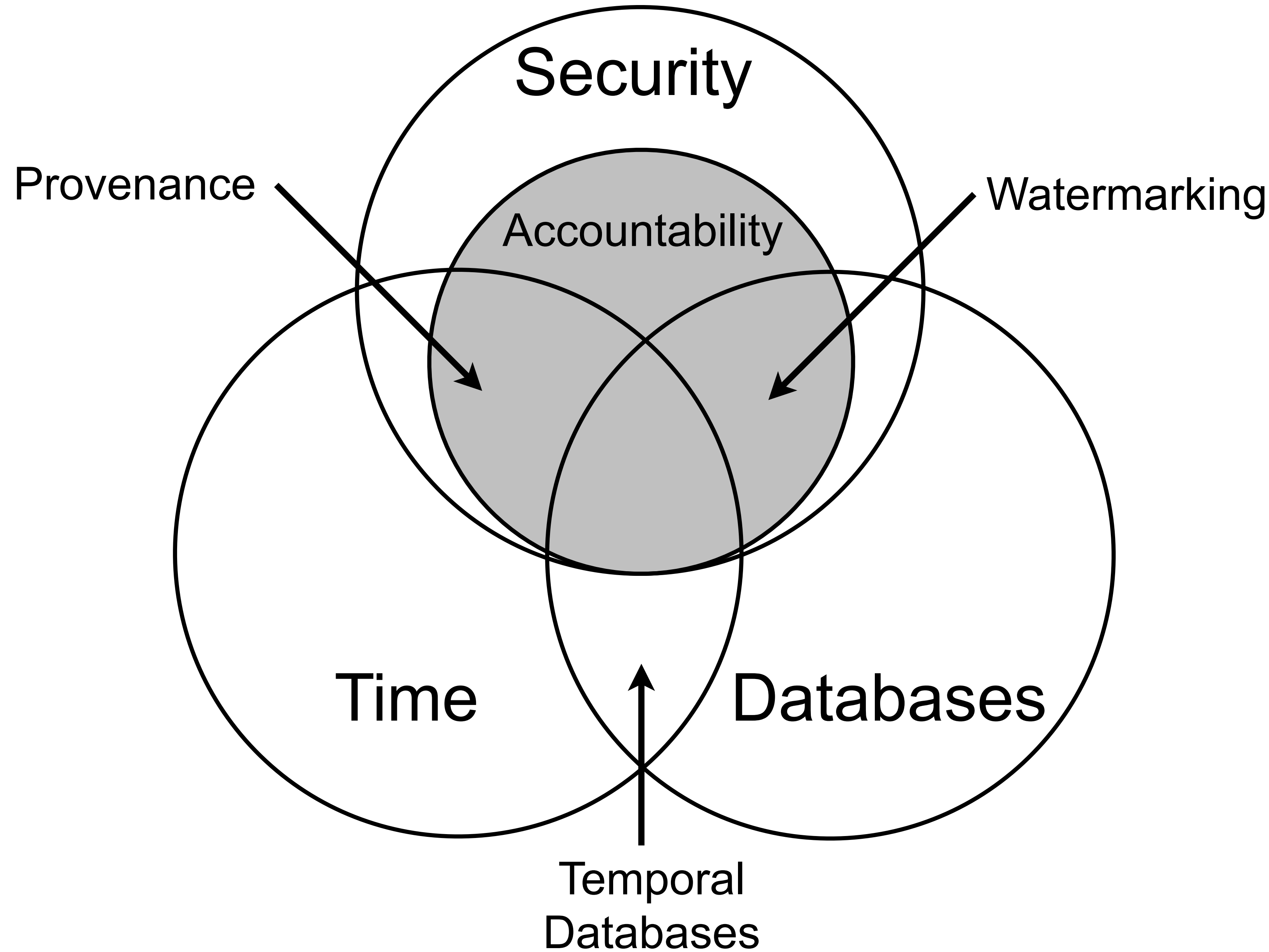
Accountability ∩ Databases ∩ Time



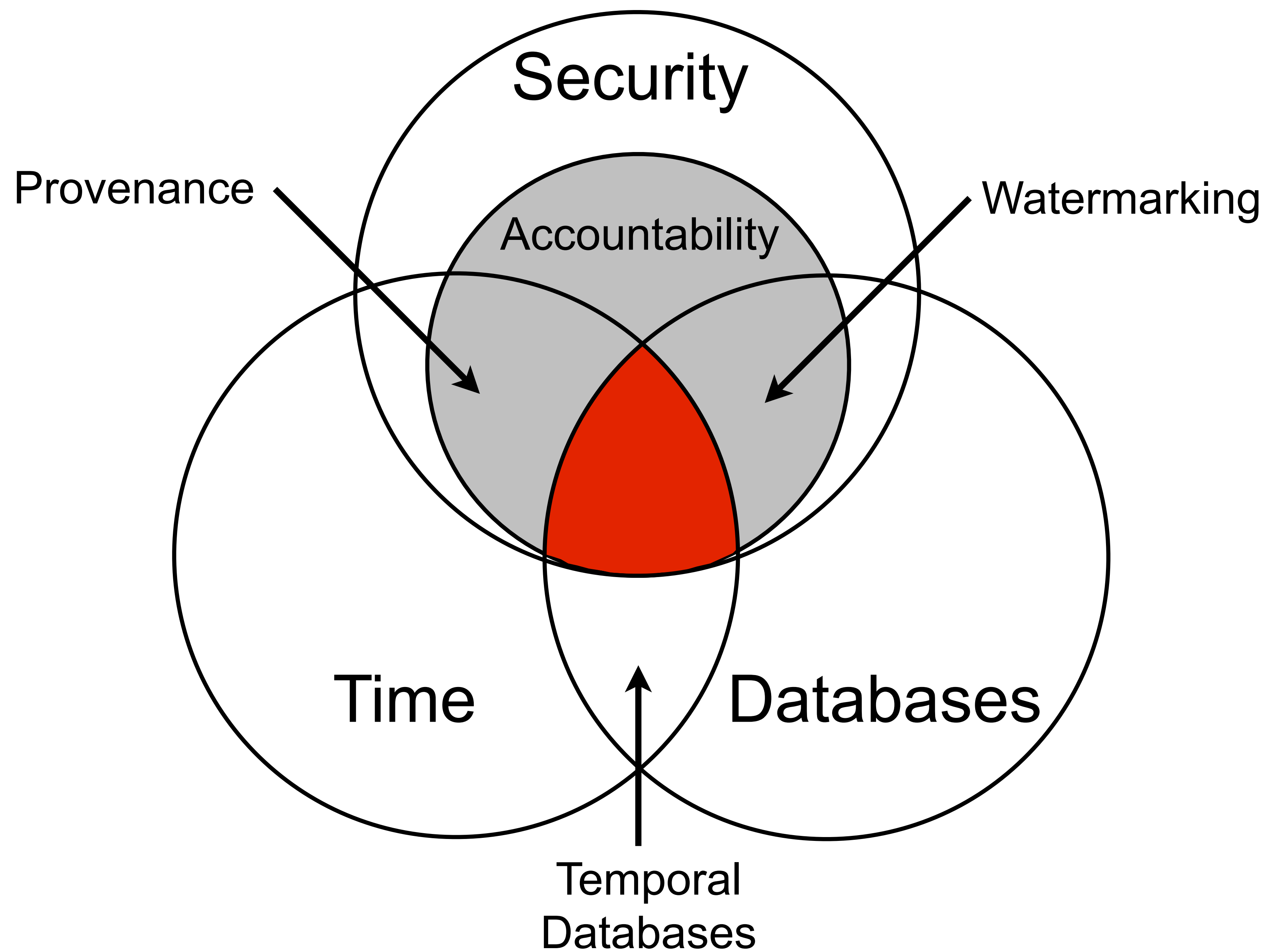
Accountability ∩ Databases ∩ Time



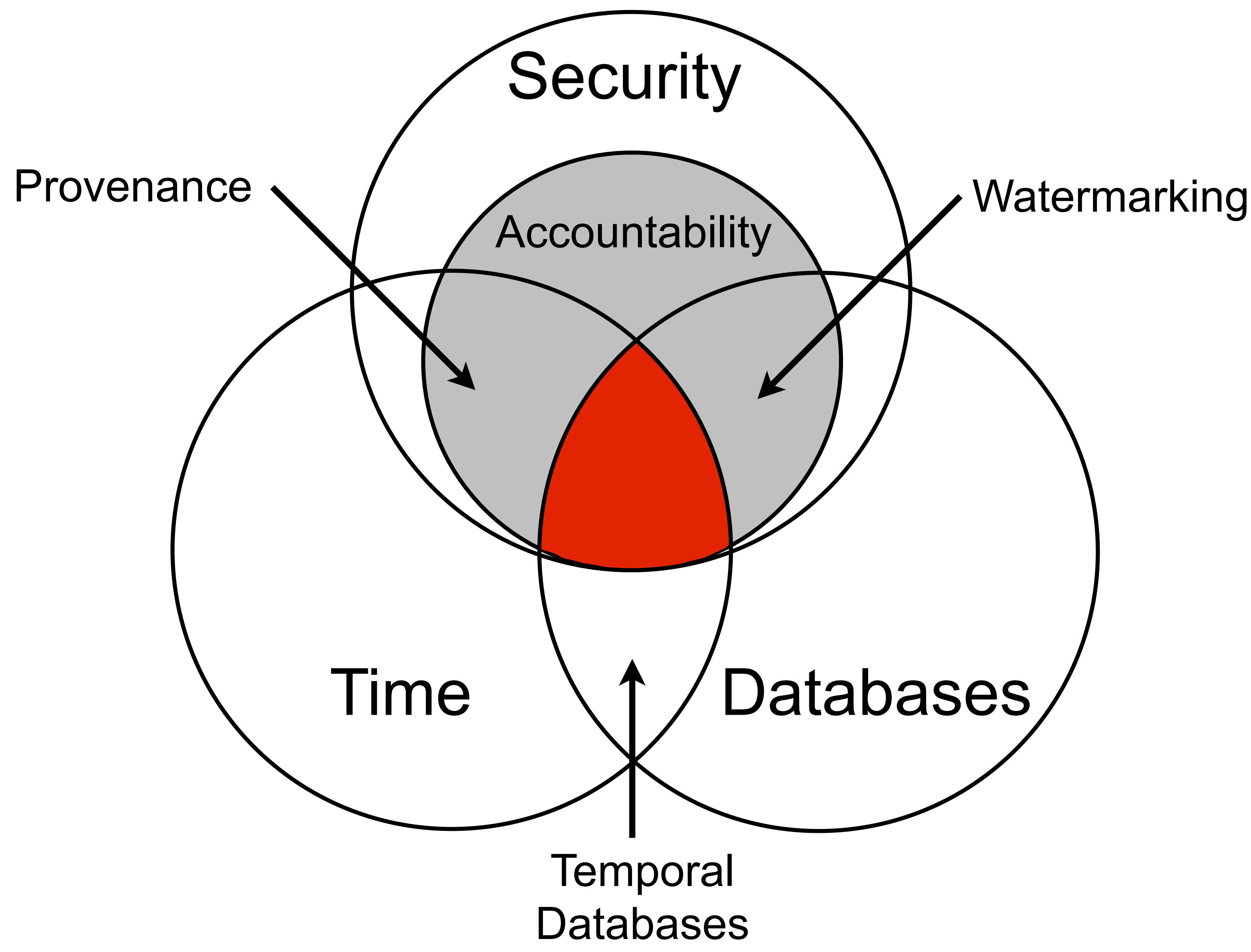
Accountability ∩ Databases ∩ Time



Accountability ∩ Databases ∩ Time



Accountability ∩ Databases ∩ Time



Temporal concepts are found throughout this area of interest.

Outline

- Information Accountability
- Reference Architecture & Execution Phases
- Forensic Analysis
- Refinements
- Enterprise Considerations

Outline

- Information Accountability
- Reference Architecture & Execution Phases
- Forensic Analysis
- Refinements
- Enterprise Considerations

Approach

Approach

- Continuous assurance technology
    - provides technology-enabled auditing
    - produces audit results close to occurrence of relevant events
    - achieves meaningful operationalization of information accountability.

Approach

- Continuous assurance technology
  - provides technology-enabled auditing
  - produces audit results close to occurrence of relevant events
  - achieves meaningful operationalization of information accountability.
- Cryptographic hashing captures state of database as it evolves.

Reference Architecture Threat Model

Reference Architecture Threat Model

- Trusted computing base (TCB)
  - Correctly booted and running hardware, OS and DBMS
  - TCB runs correctly until intrusion
- A trusted external digital notarization service (EDNS)
- The adversary could be
  - Inside/outside intruders who gain full control of the whole TCB and logs
  - Malware such as virus, bugs, power surge
- Regret Interval: minimum time before someone can reverse the change
  - Determined by the specific application

Reference Architecture Threat Model

- Trusted computing base (TCB)
  - Correctly booted and running hardware, OS and DBMS
  - TCB runs correctly until intrusion
- A trusted external digital notarization service (EDNS)
- The adversary could be
  - Inside/outside intruders who gain full control of the whole TCB and logs
  - Malware such as virus, bugs, power surge
- Regret Interval: minimum time before someone can reverse the change
  - Determined by the specific application

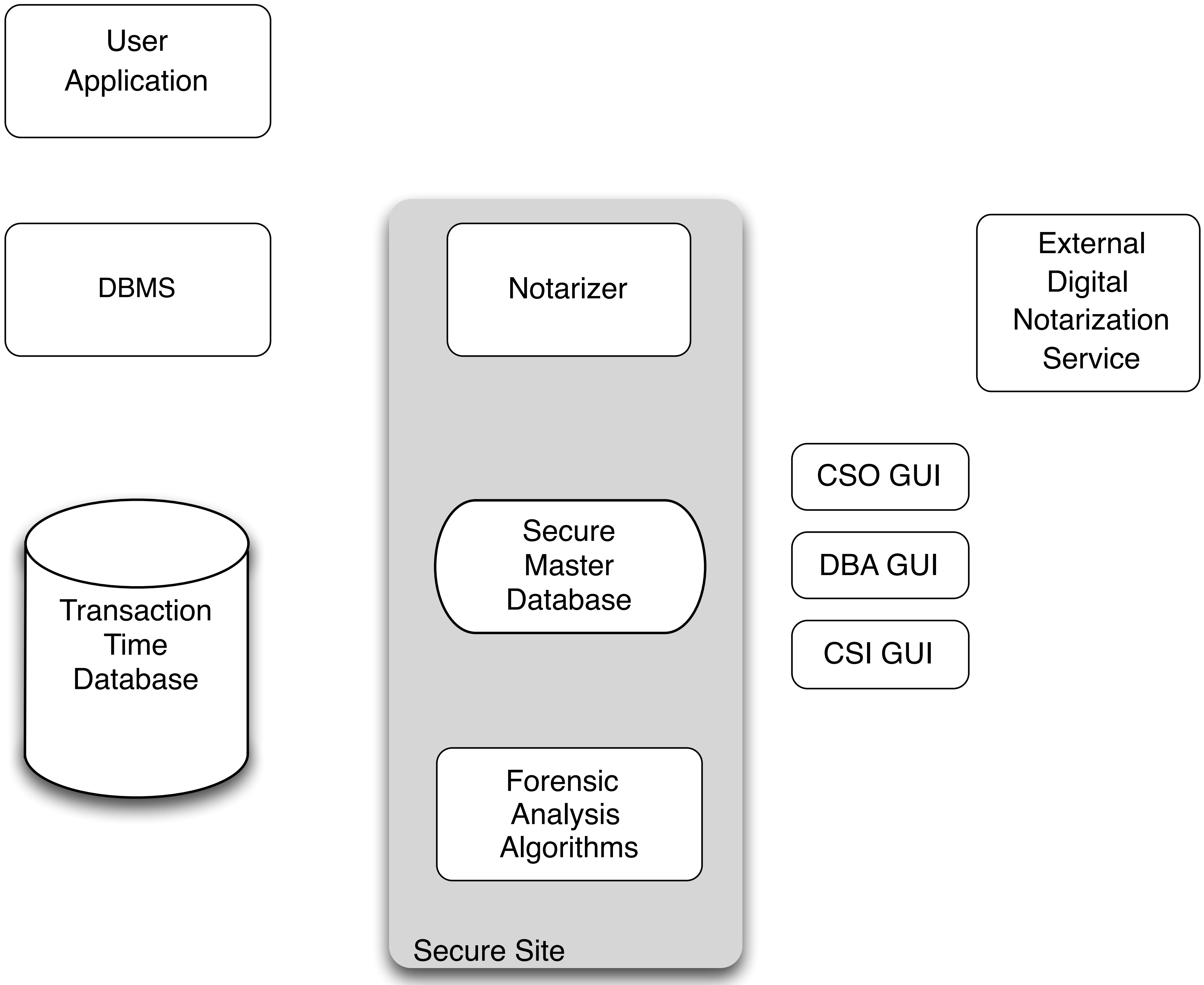
Reference Architecture Threat Model

- Trusted computing base (TCB)
  - Correctly booted and running hardware, OS and DBMS
  - TCB runs correctly until intrusion
- A trusted external digital notarization service (EDNS)
- The adversary could be
  - Inside/outside intruders who gain full control of the whole TCB and logs
  - Malware such as virus, bugs, power surge
- Regret Interval: minimum time before someone can reverse the change
  - Determined by the specific application

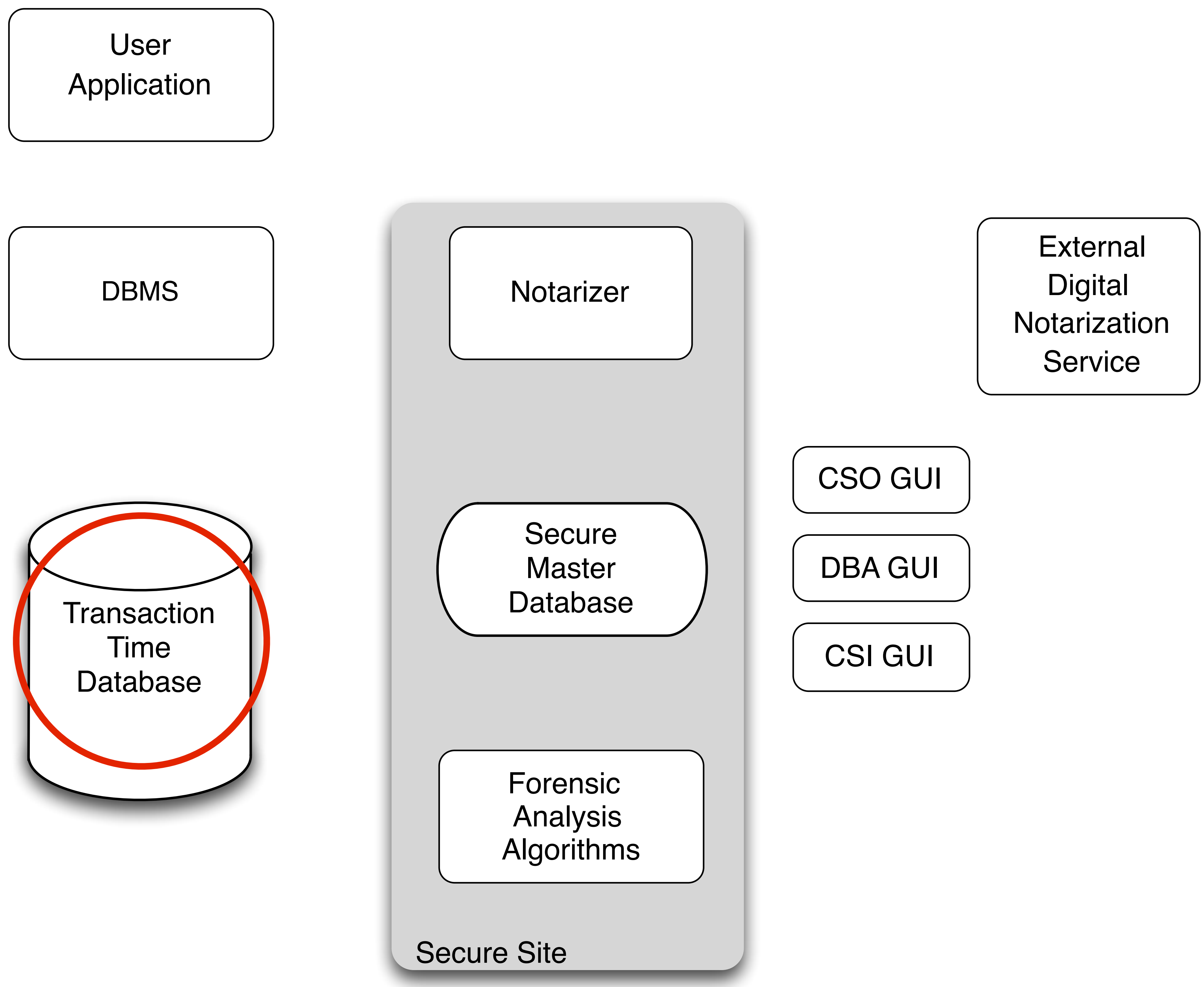
Reference Architecture Threat Model

- Trusted computing base (TCB)
  - Correctly booted and running hardware, OS and DBMS
  - TCB runs correctly until intrusion
- A trusted external digital notarization service (EDNS)
- The adversary could be
  - Inside/outside intruders who gain full control of the whole TCB and logs
  - Malware such as virus, bugs, power surge
- Regret Interval: minimum time before someone can reverse the change
  - Determined by the specific application

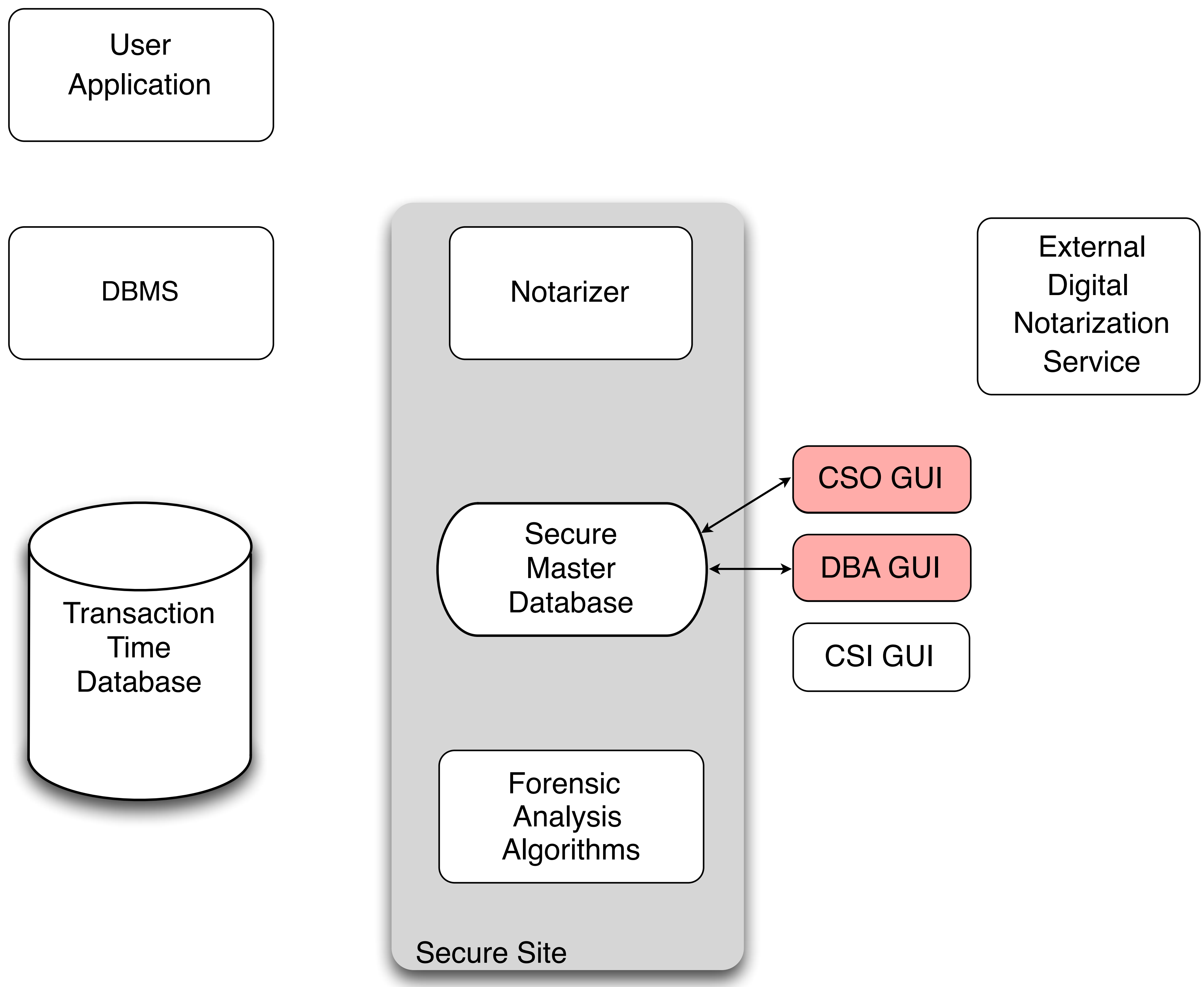
Total Chain Computation Phase



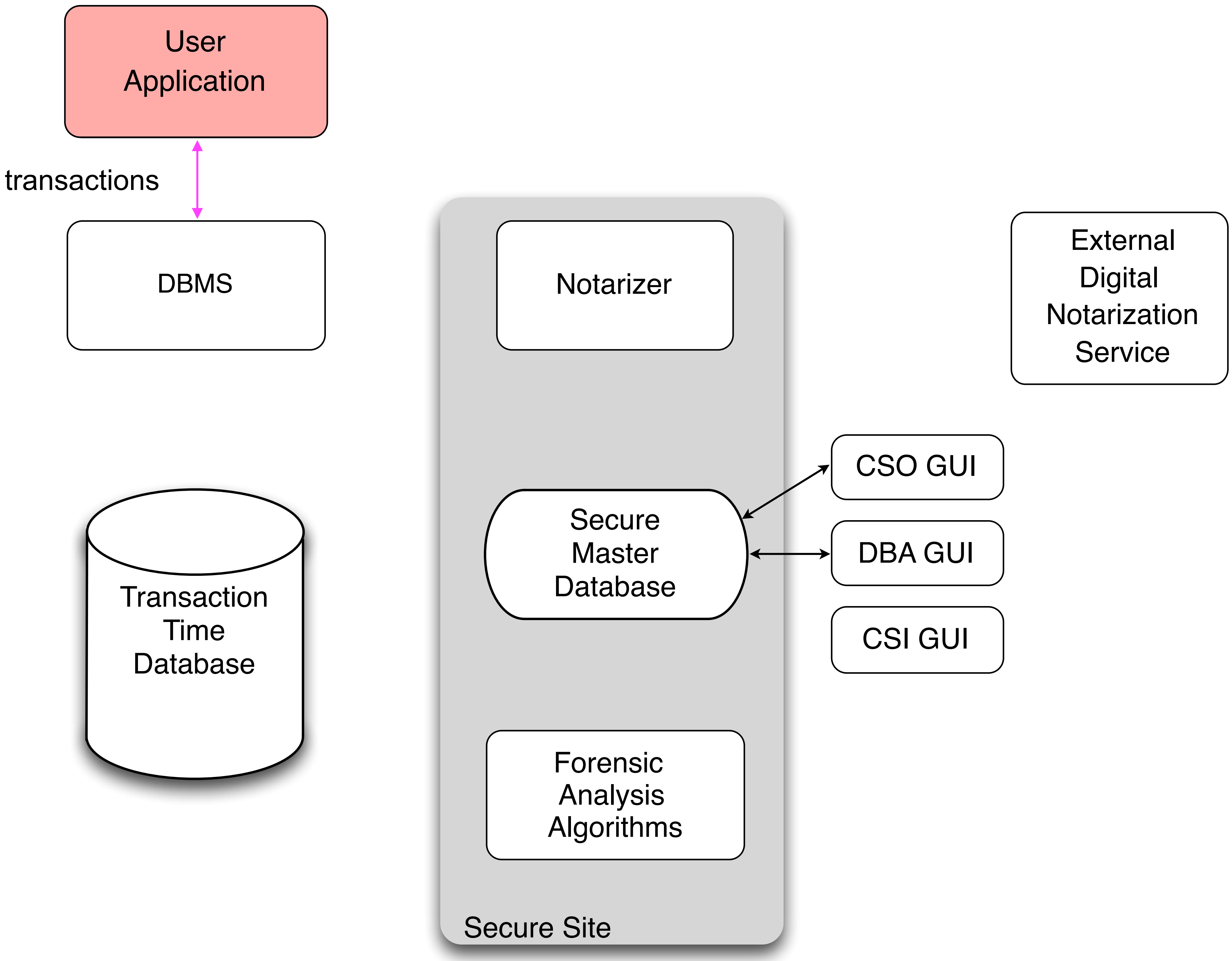
Total Chain Computation Phase



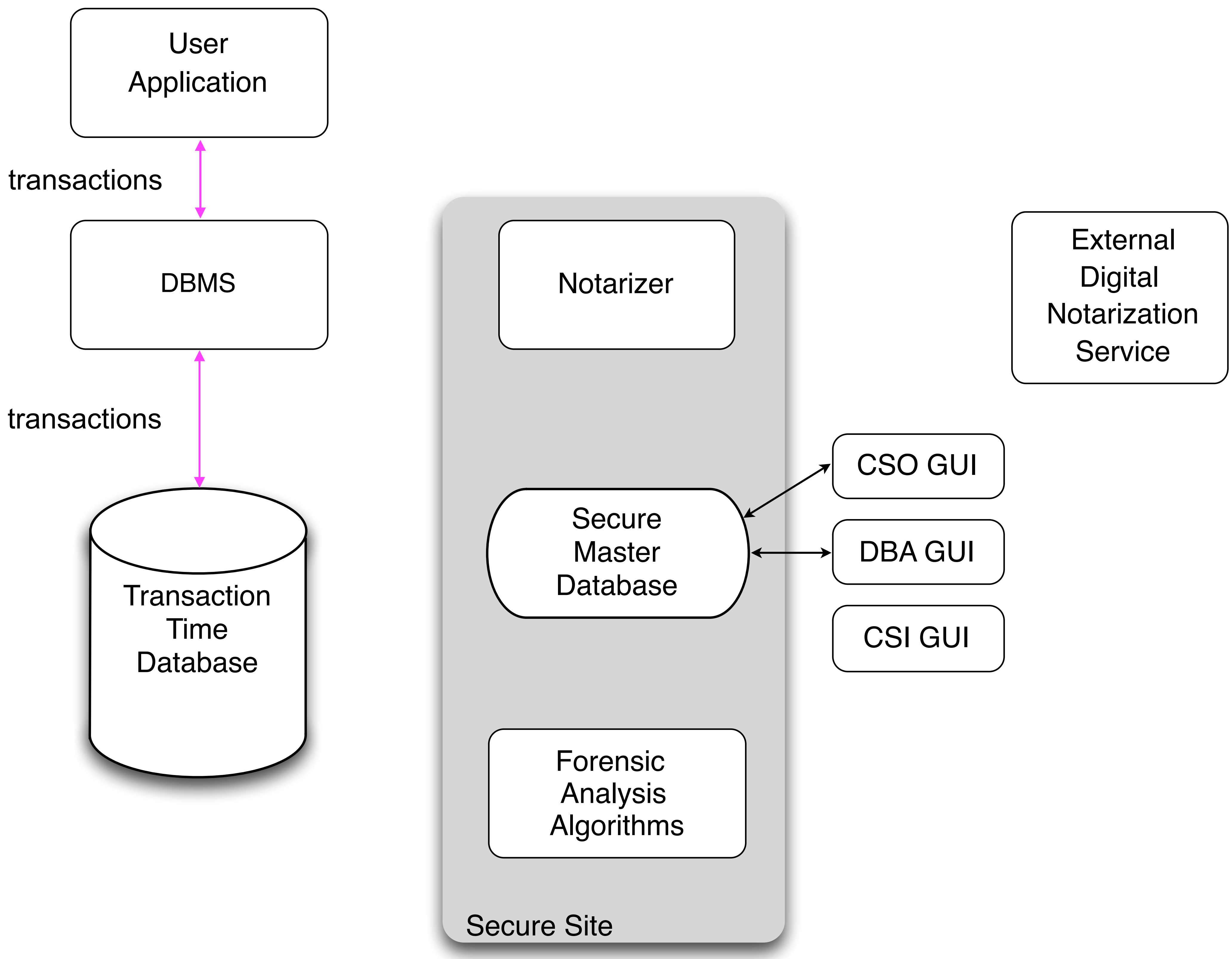
Total Chain Computation Phase



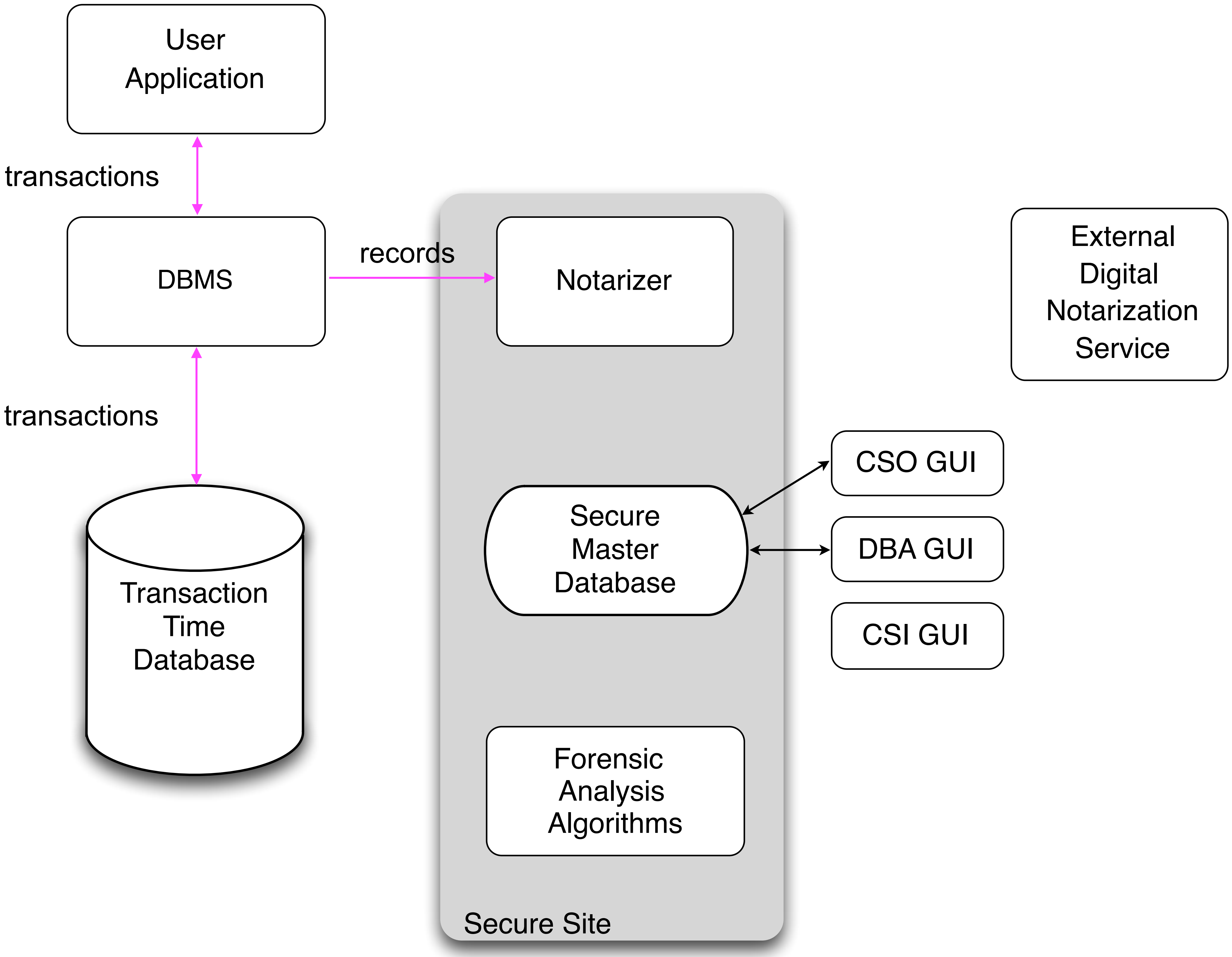
Total Chain Computation Phase



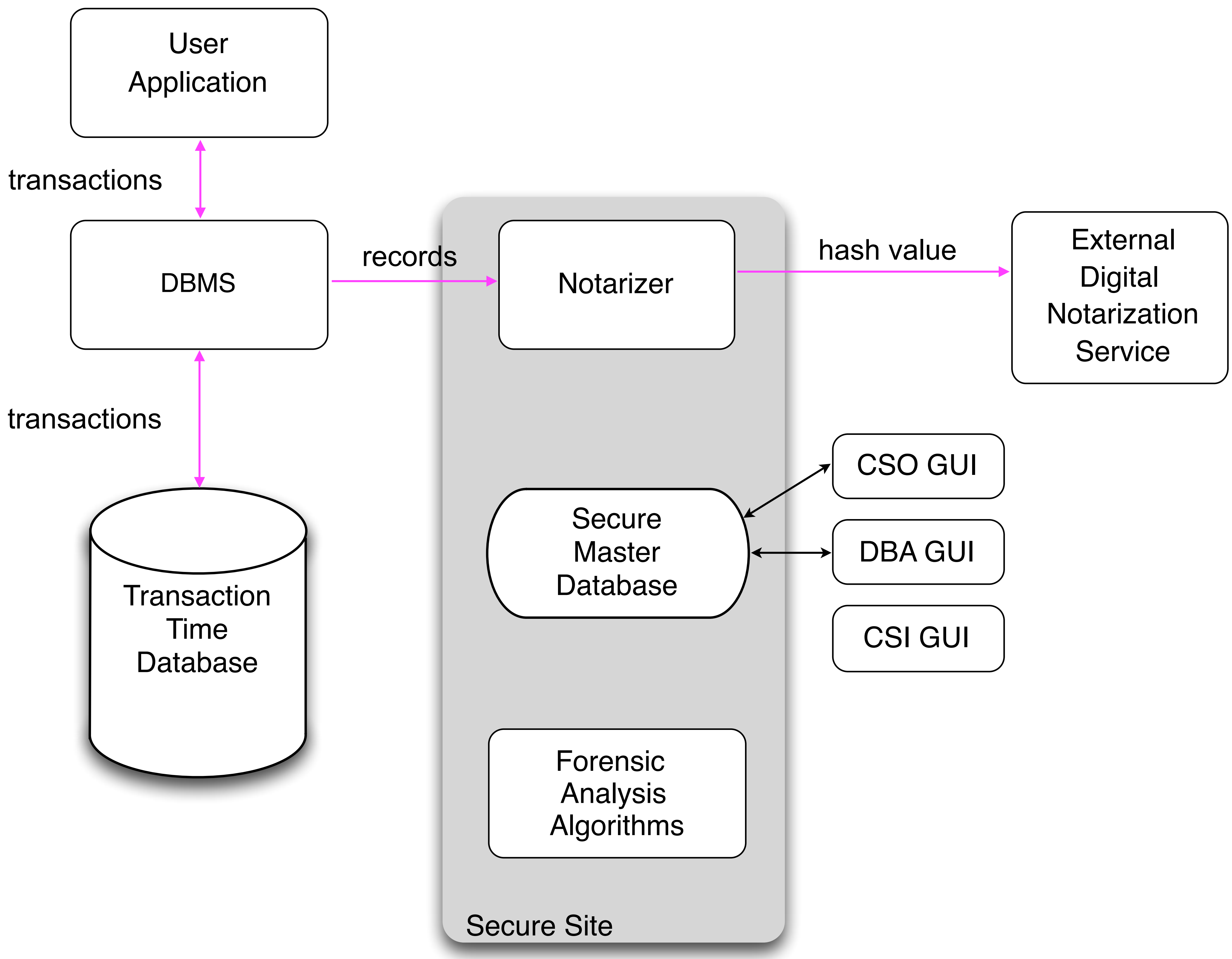
Total Chain Computation Phase



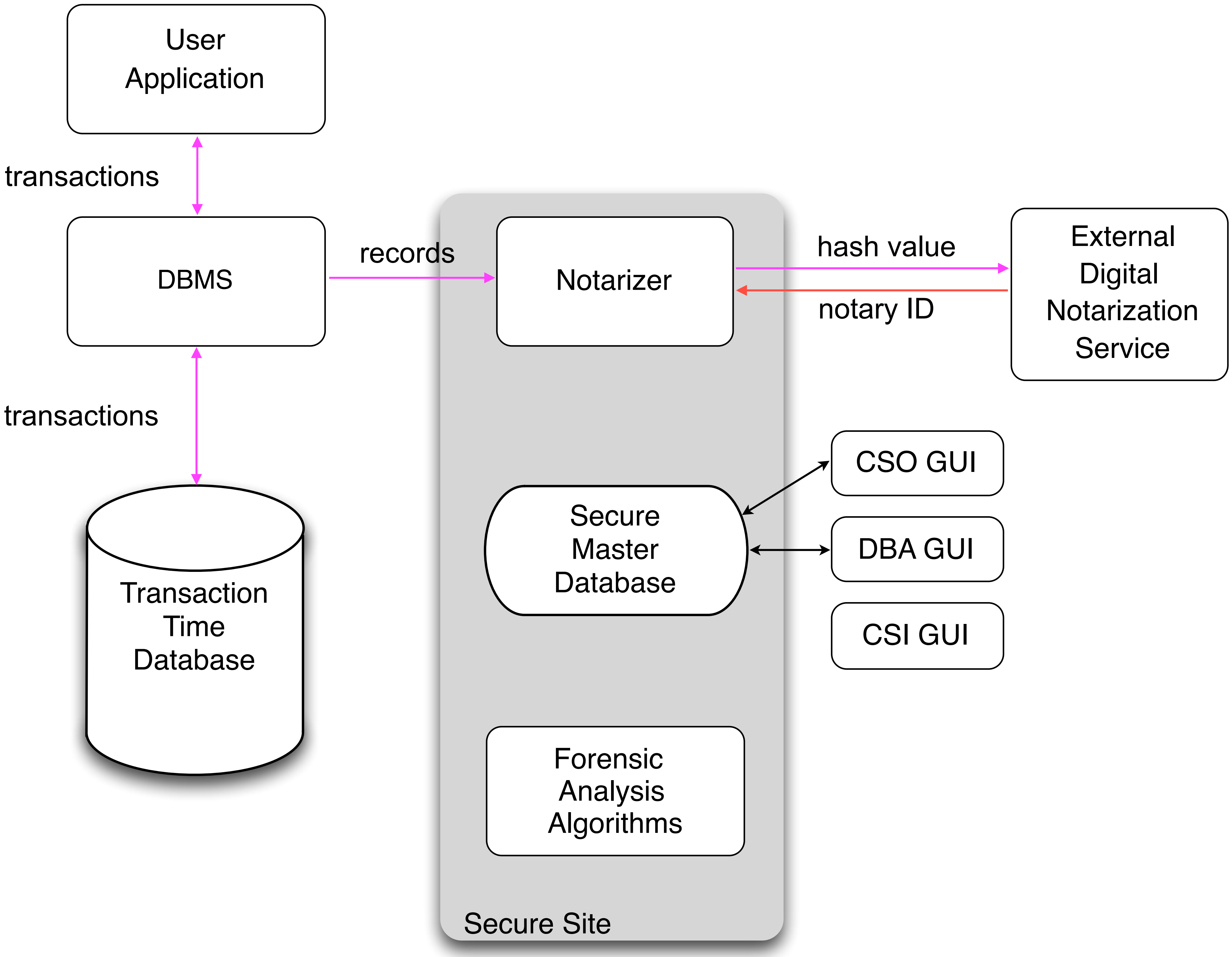
Total Chain Computation Phase



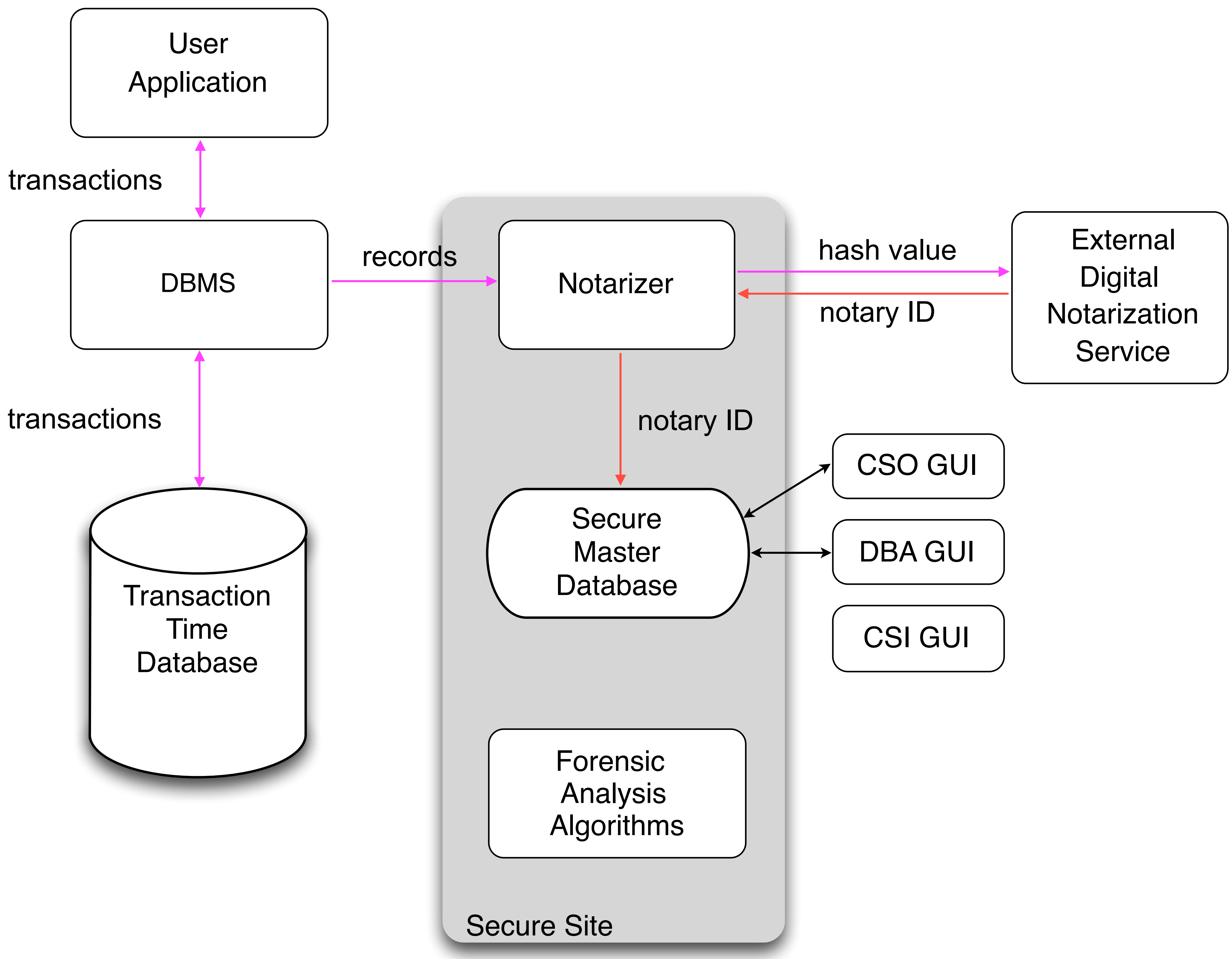
Total Chain Computation Phase



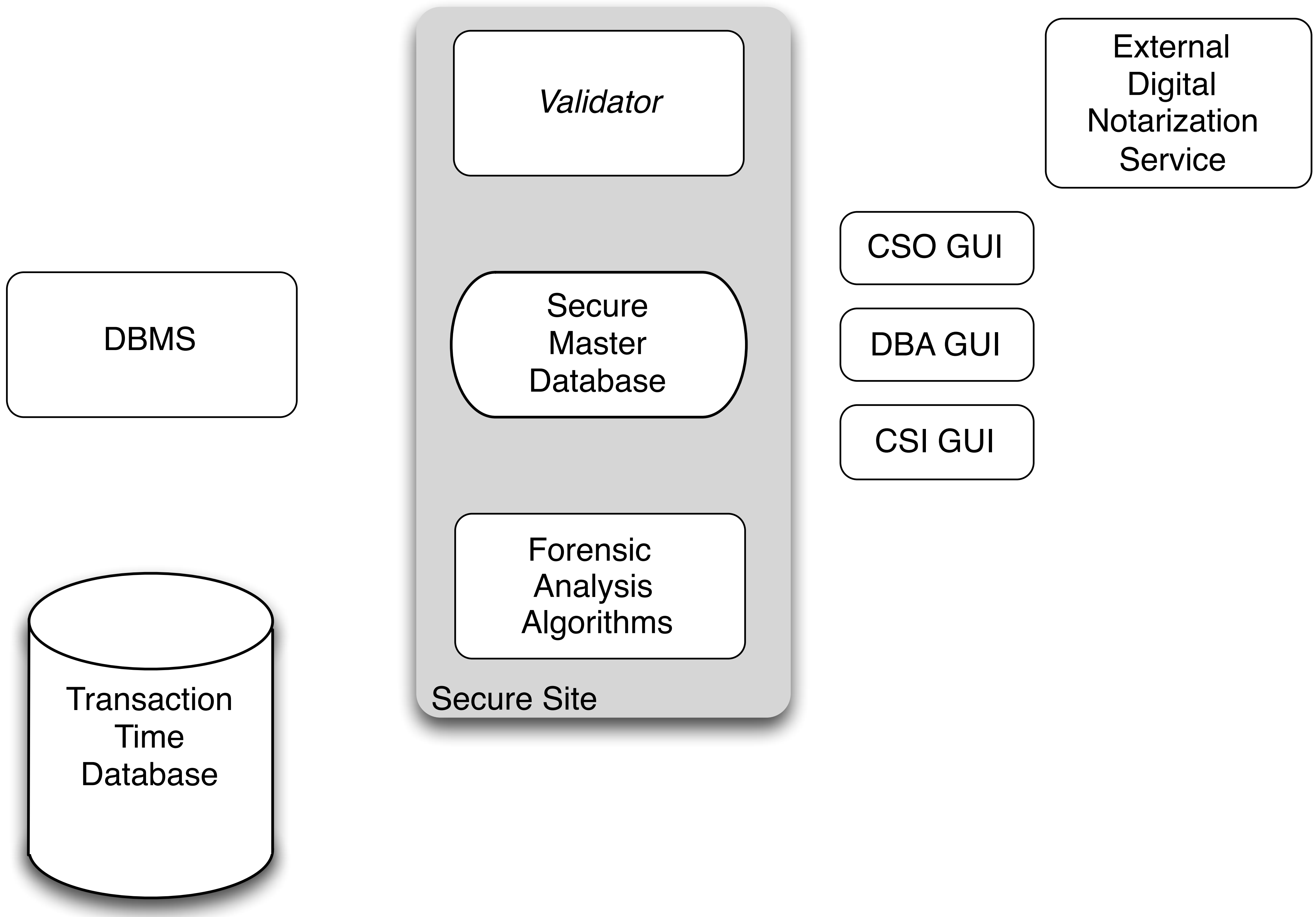
Total Chain Computation Phase



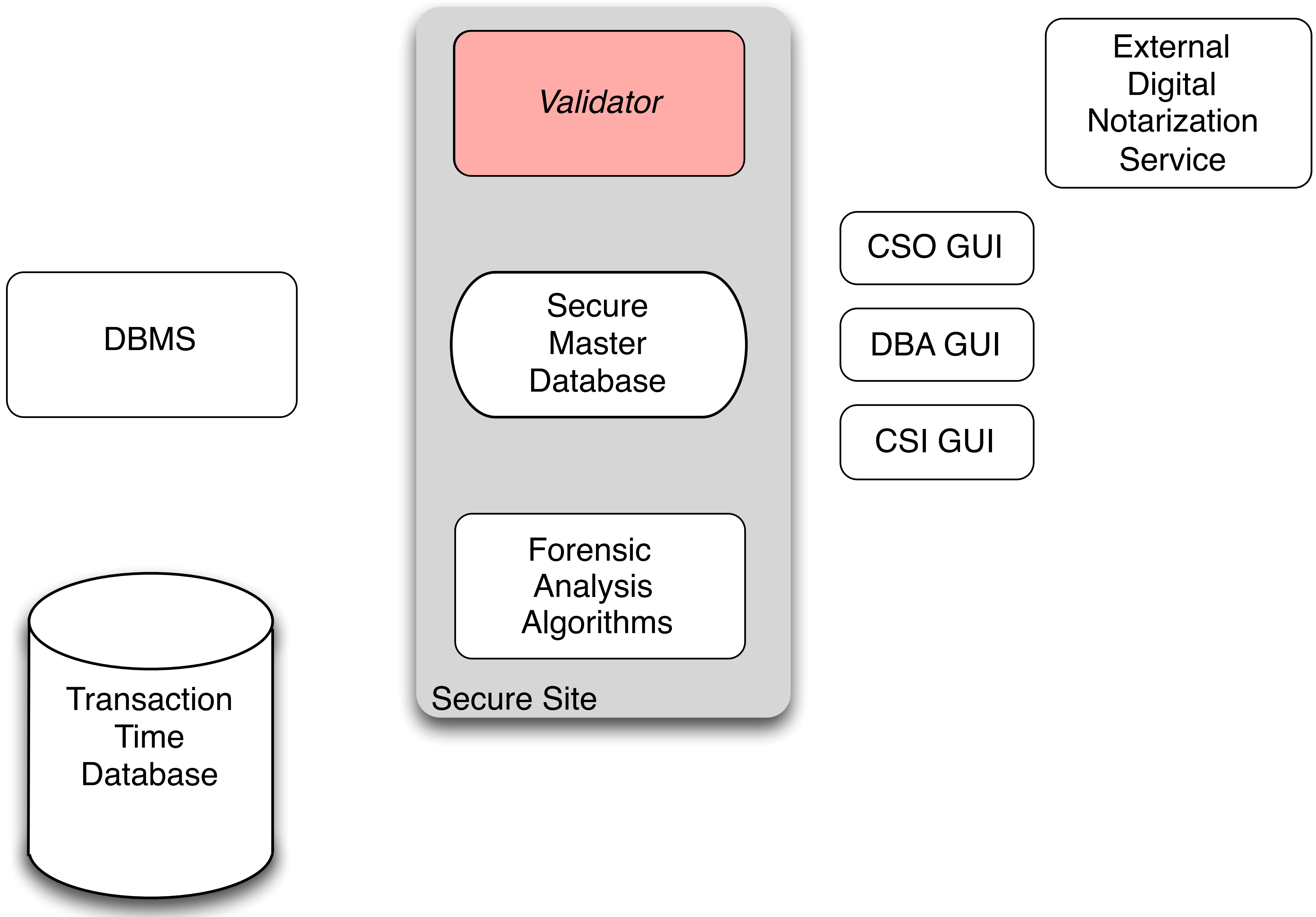
Total Chain Computation Phase



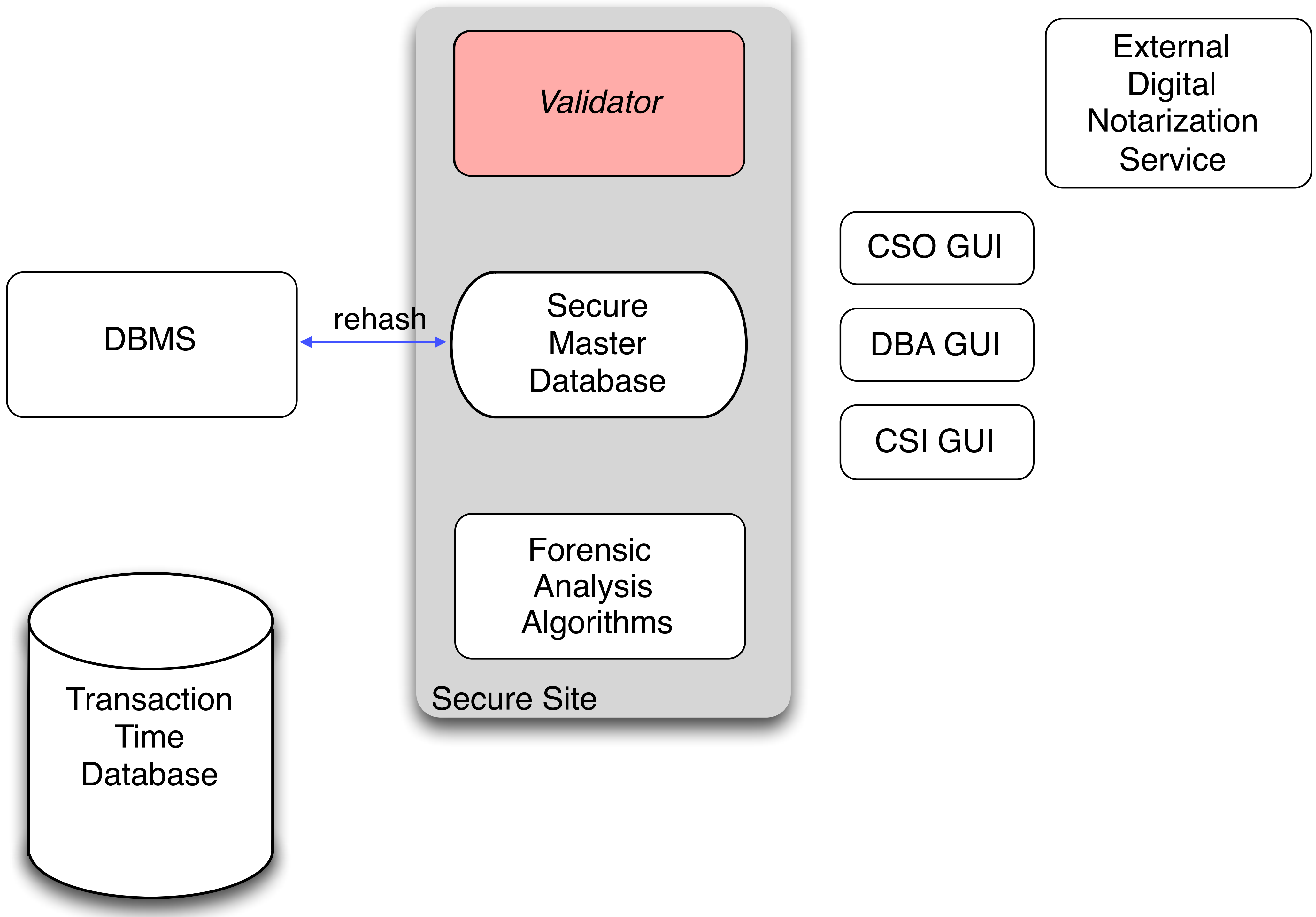
Tamper Detection and Forensic Analysis Phase



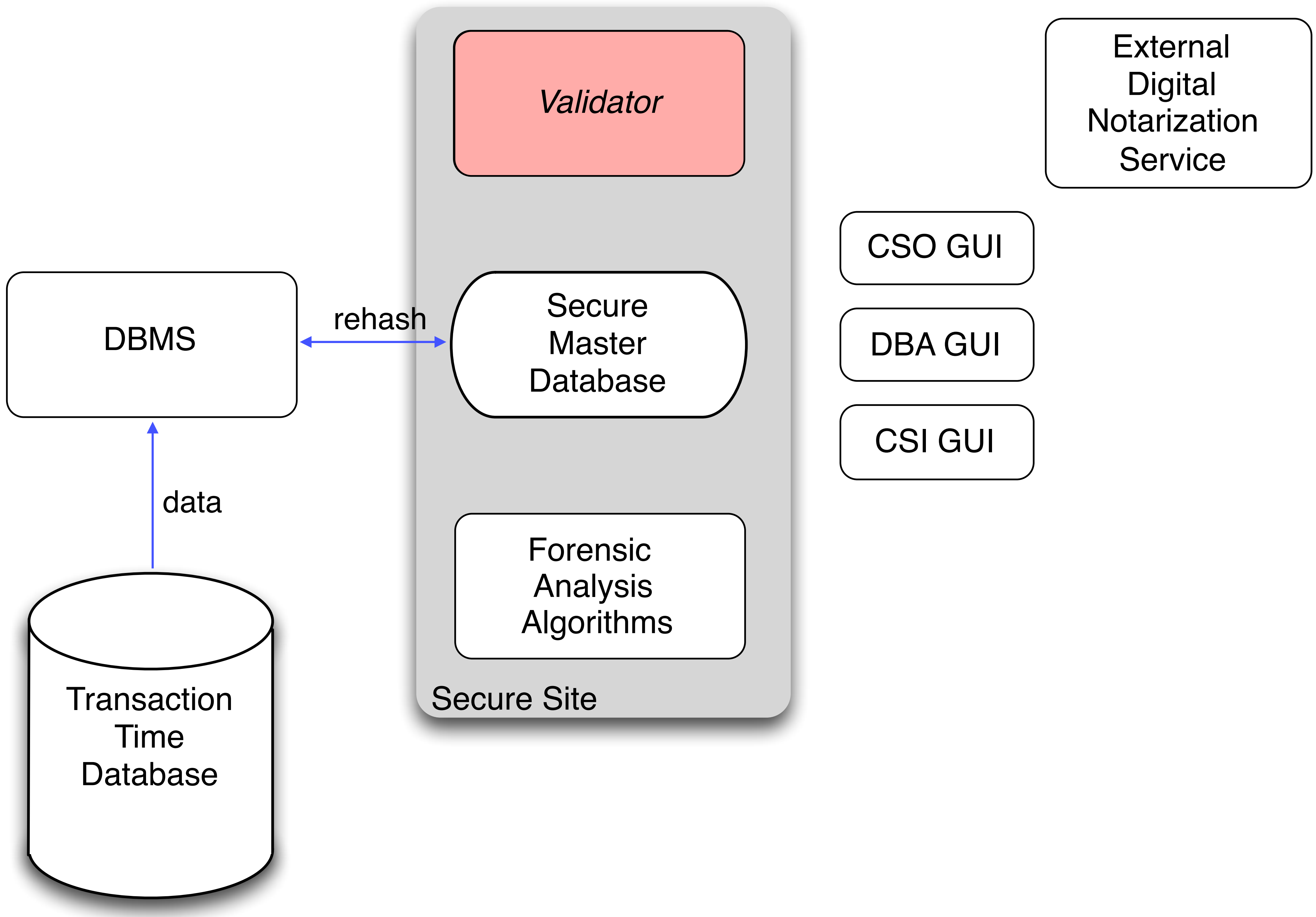
Tamper Detection and Forensic Analysis Phase



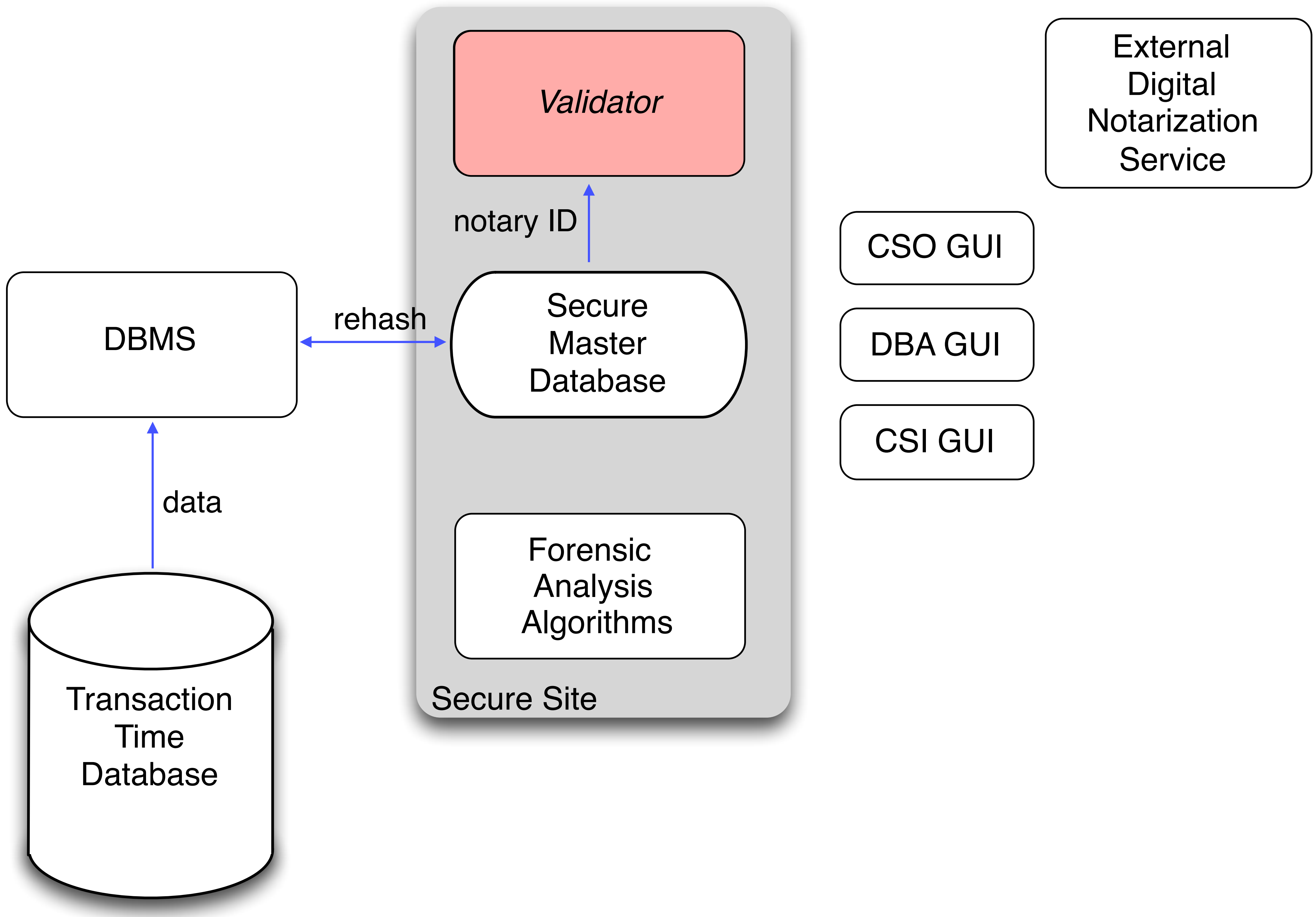
Tamper Detection and Forensic Analysis Phase



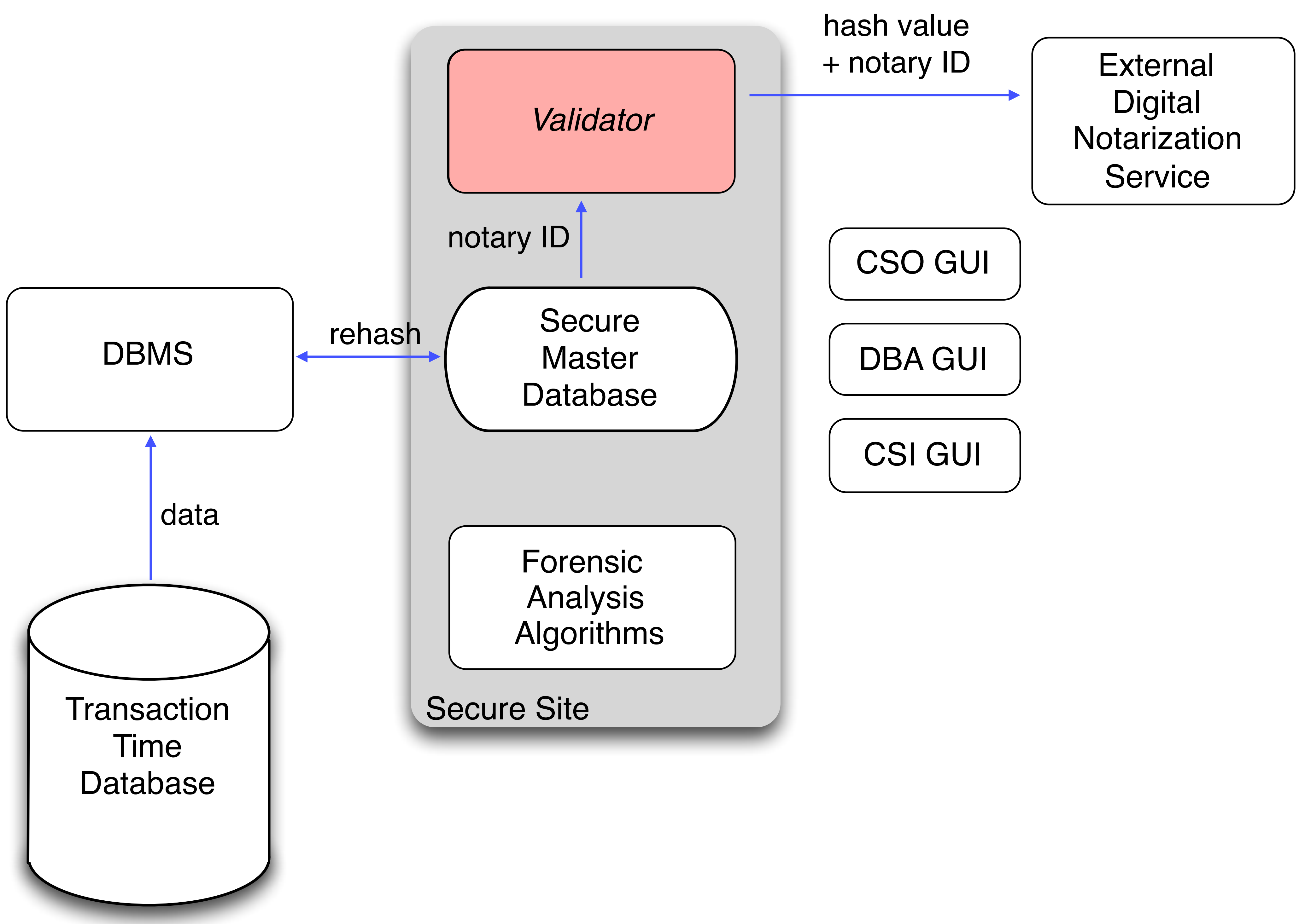
Tamper Detection and Forensic Analysis Phase



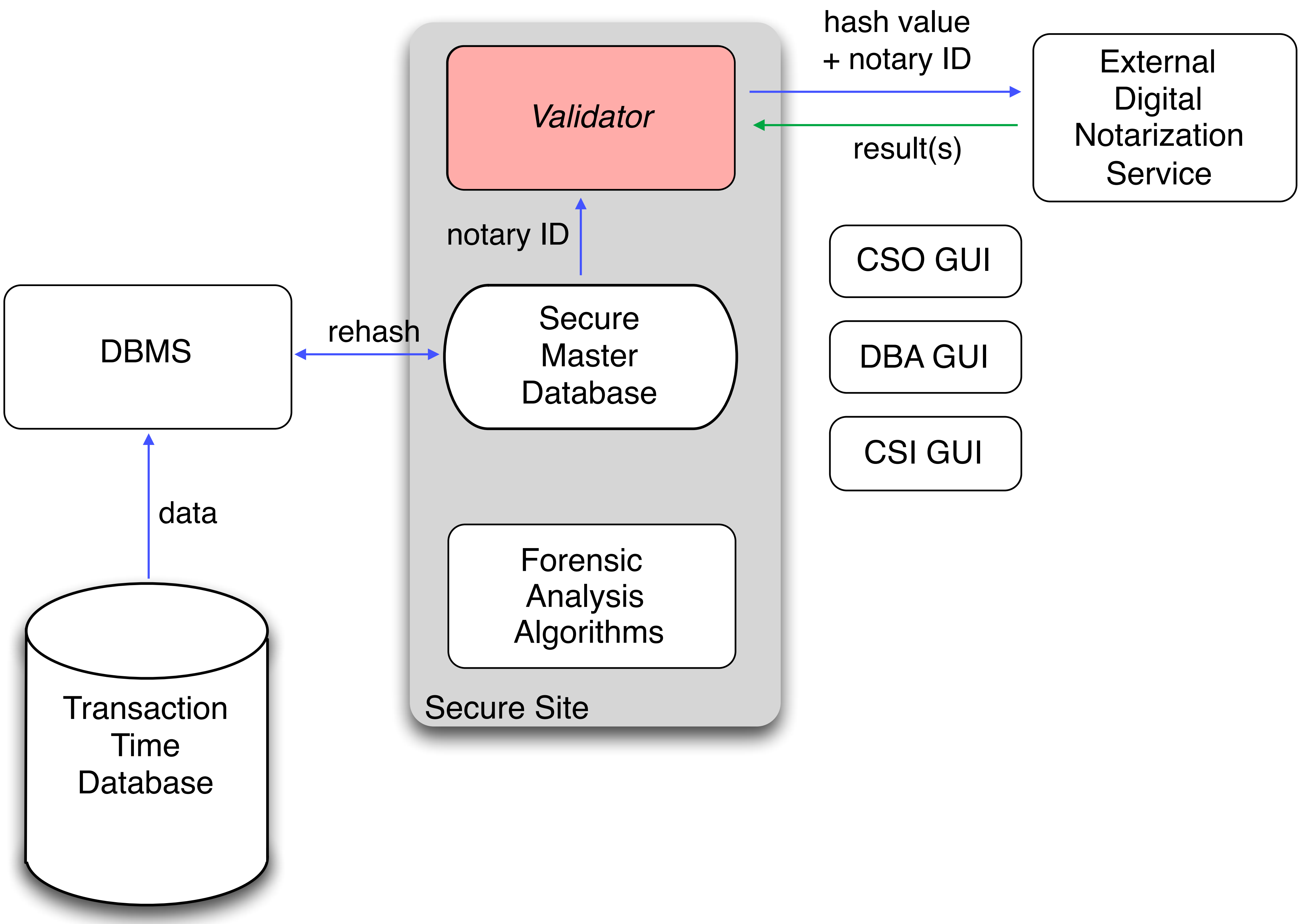
Tamper Detection and Forensic Analysis Phase



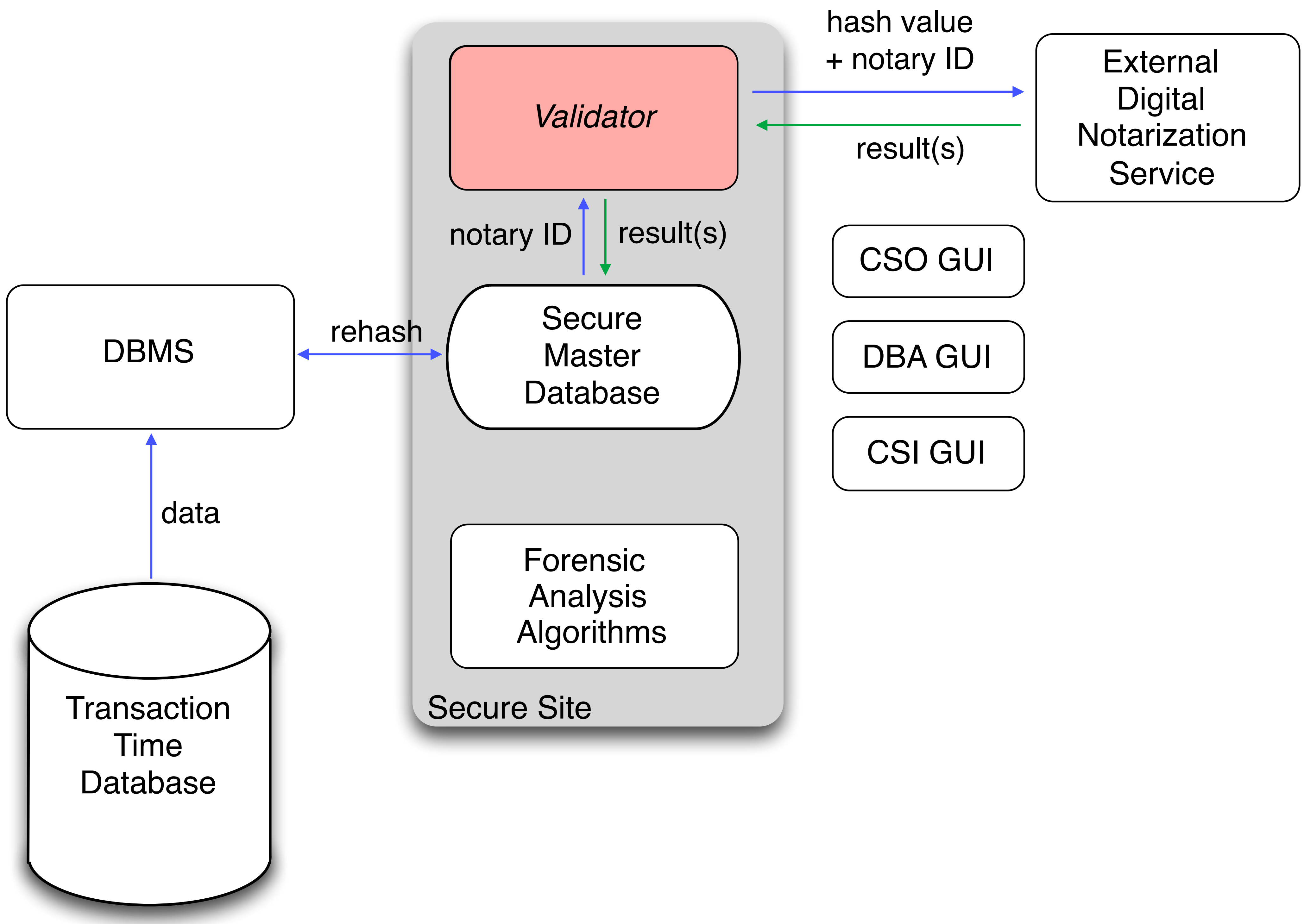
Tamper Detection and Forensic Analysis Phase



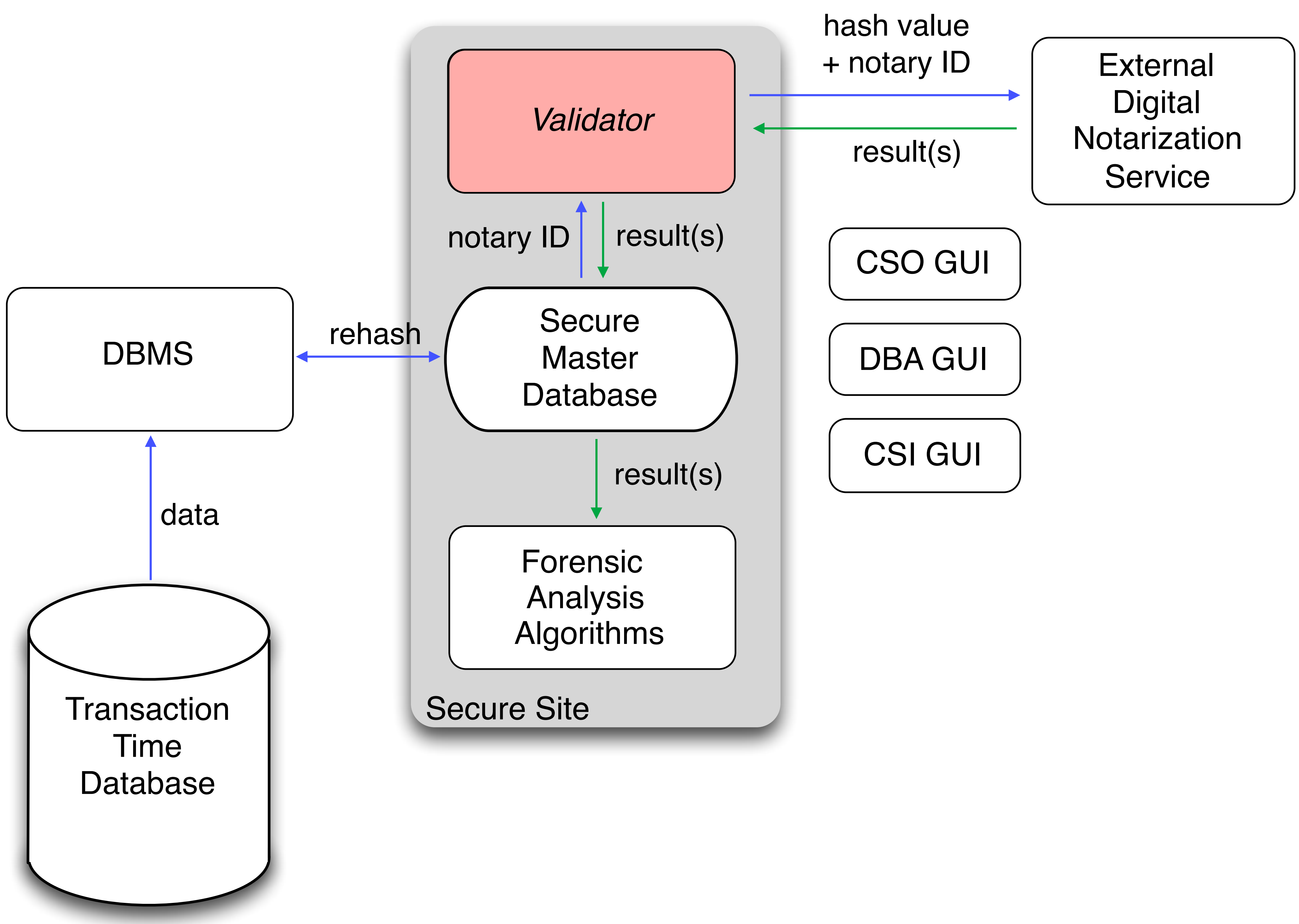
Tamper Detection and Forensic Analysis Phase



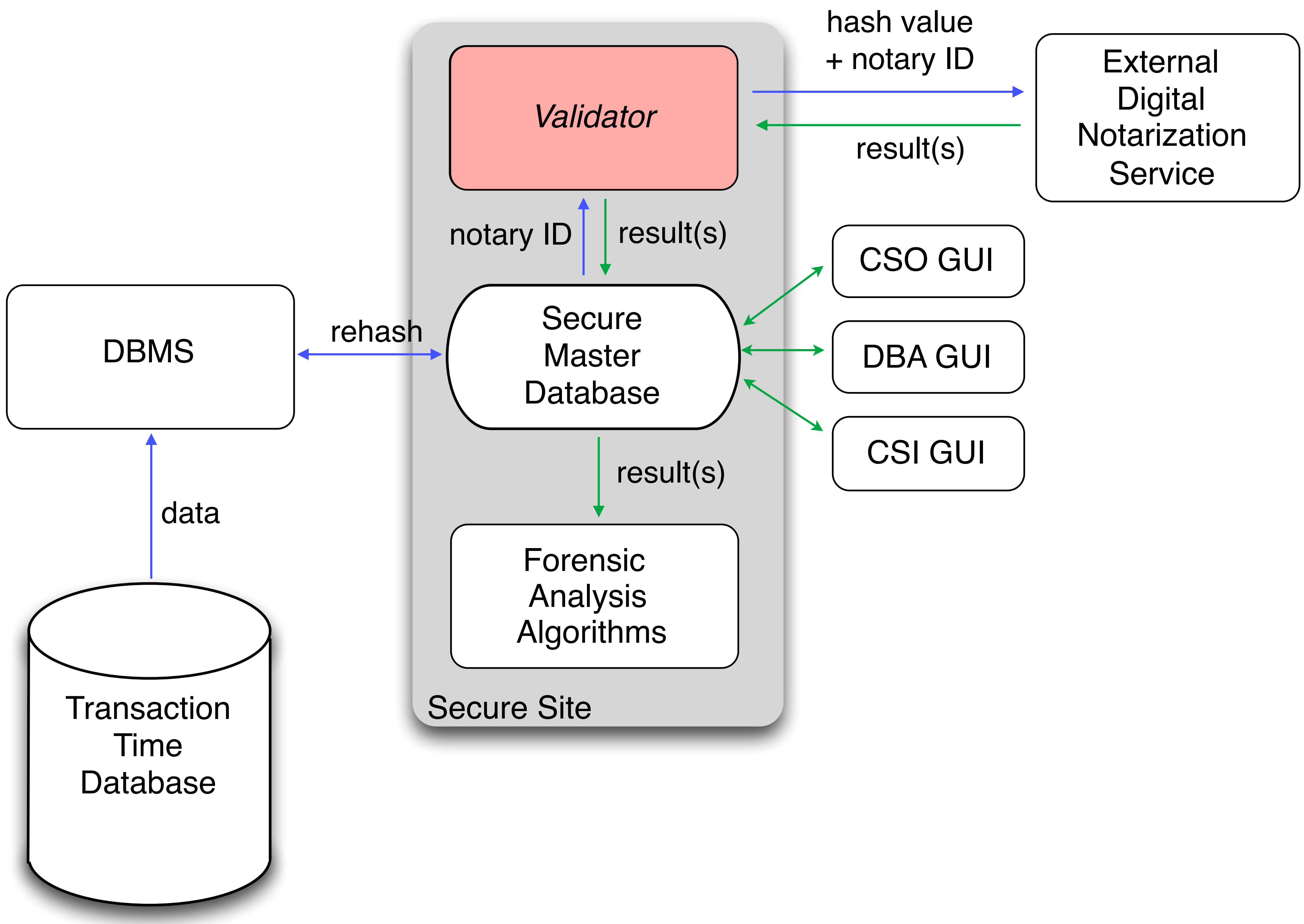
Tamper Detection and Forensic Analysis Phase



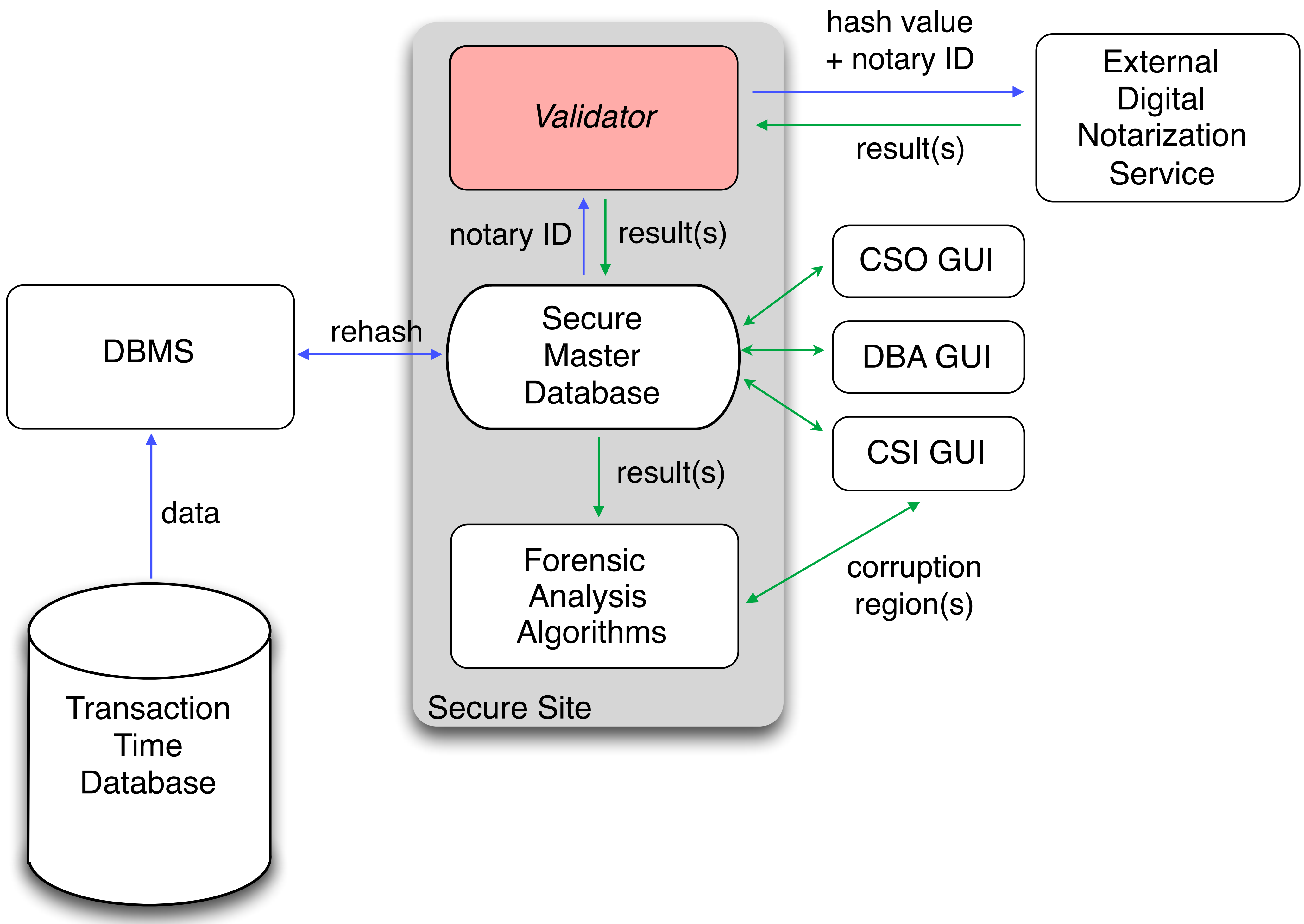
Tamper Detection and Forensic Analysis Phase



Tamper Detection and Forensic Analysis Phase



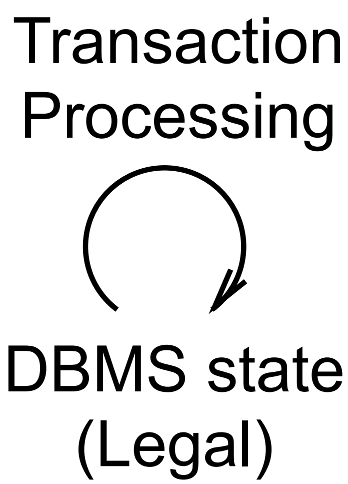
Tamper Detection and Forensic Analysis Phase



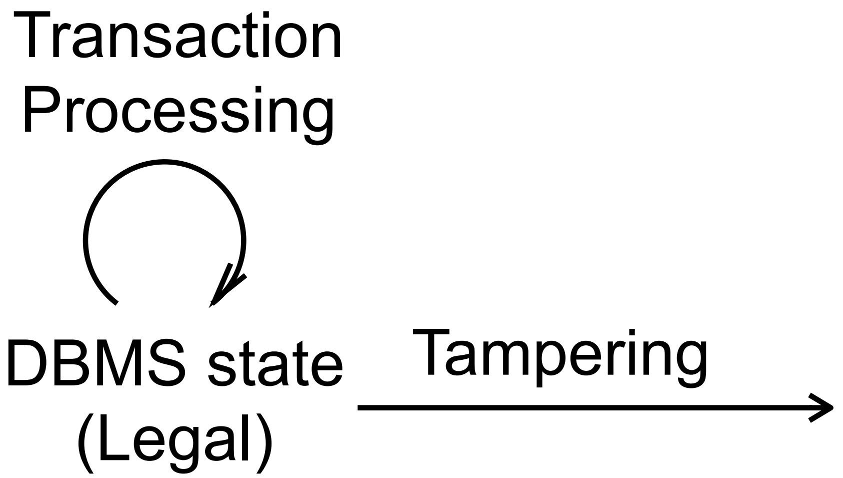
Outline

- Information Accountability
- Reference Architecture & Execution Phases
- Forensic Analysis
- Refinements
- Enterprise Considerations

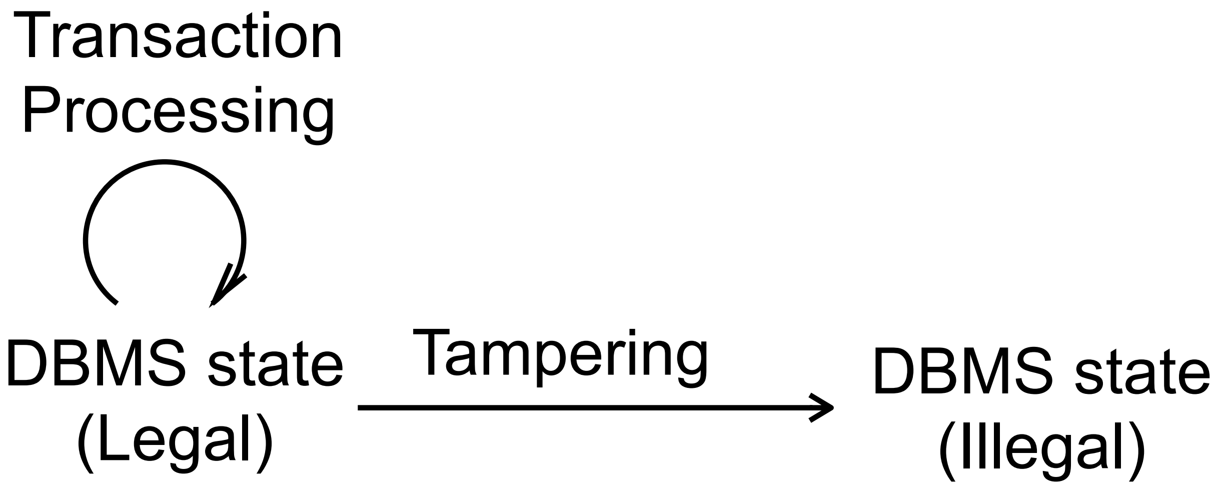
Tampering, Detection and Forensic Analysis



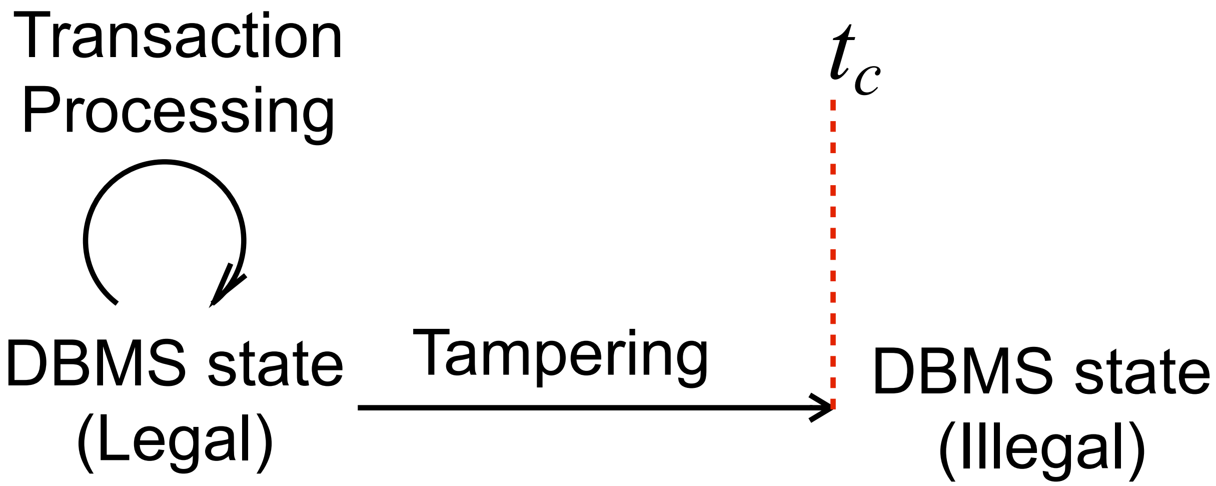
Tampering, Detection and Forensic Analysis



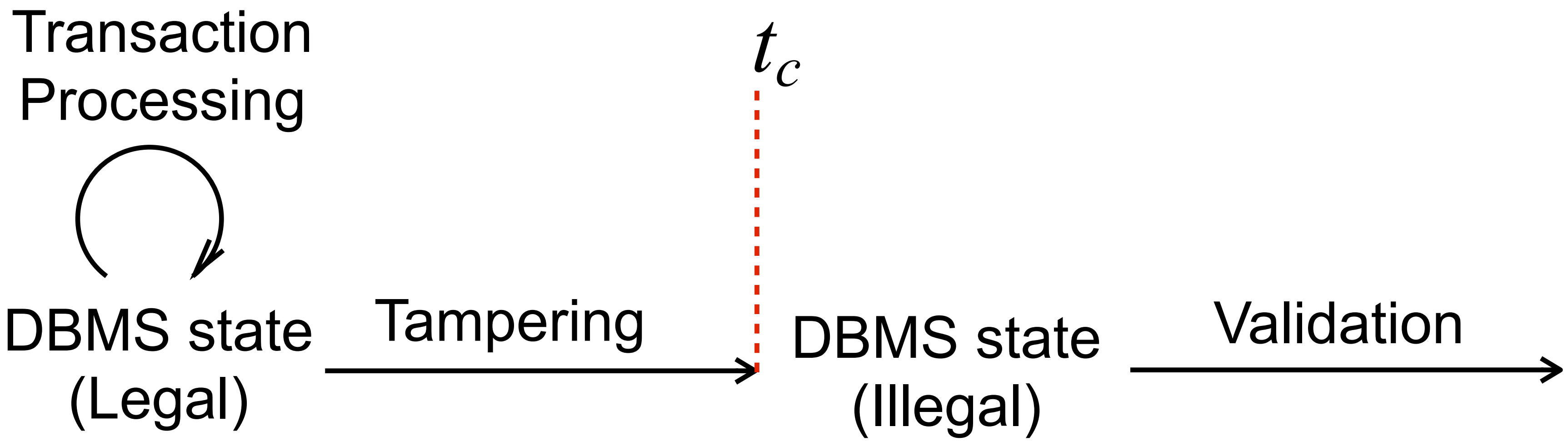
Tampering, Detection and Forensic Analysis



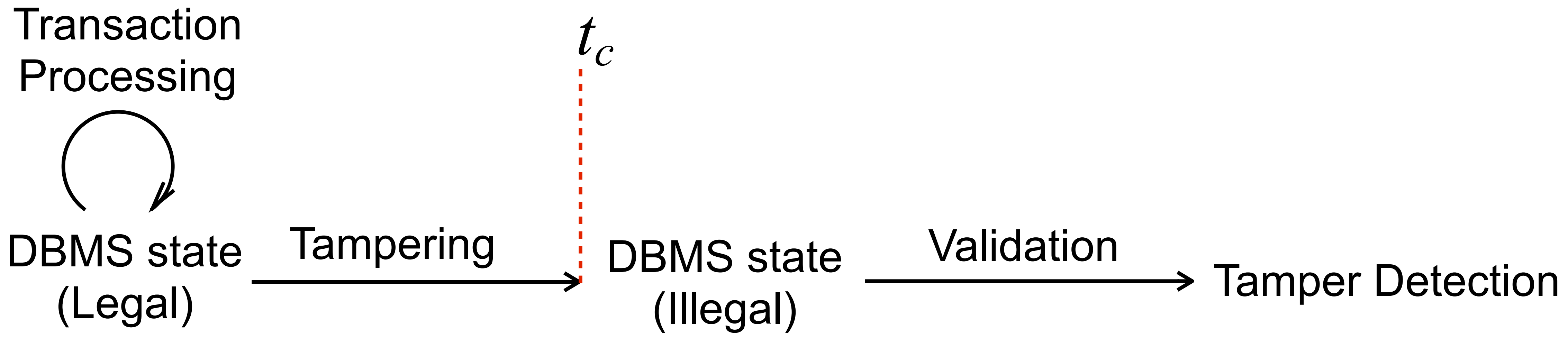
Tampering, Detection and Forensic Analysis



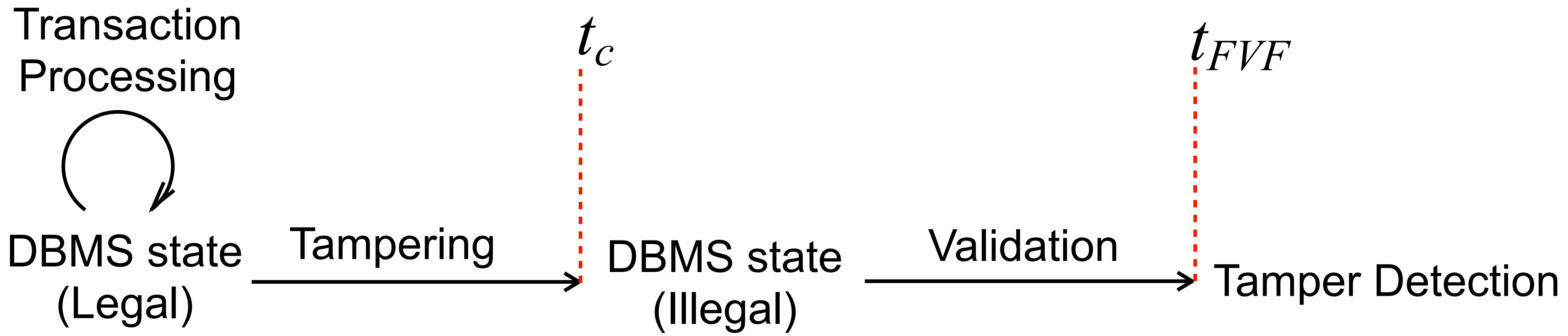
Tampering, Detection and Forensic Analysis



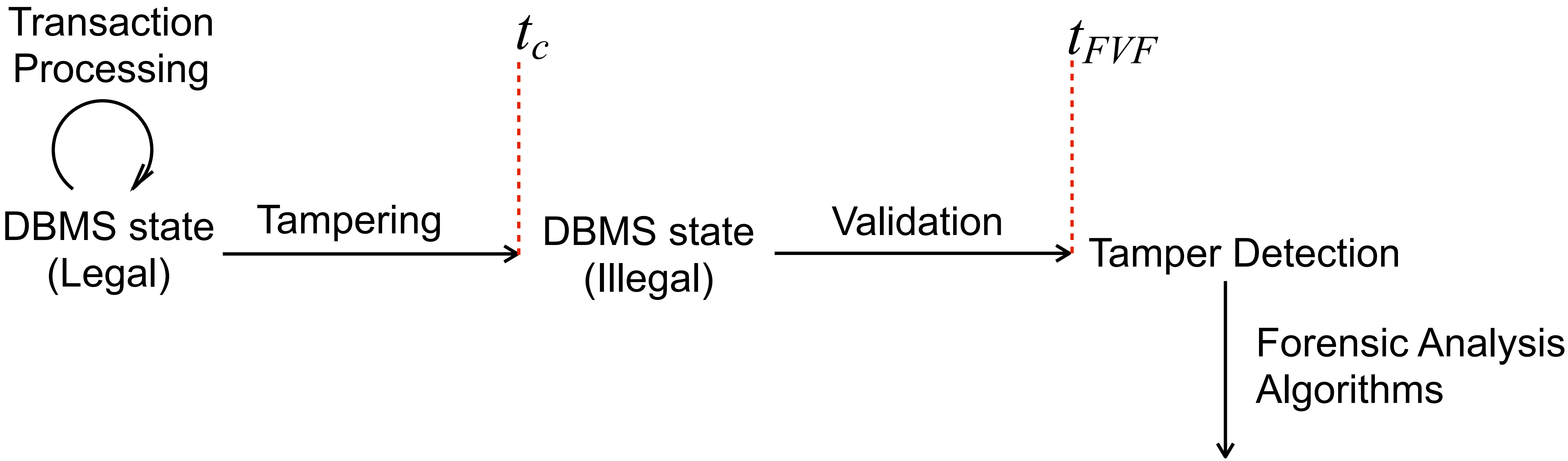
Tampering, Detection and Forensic Analysis



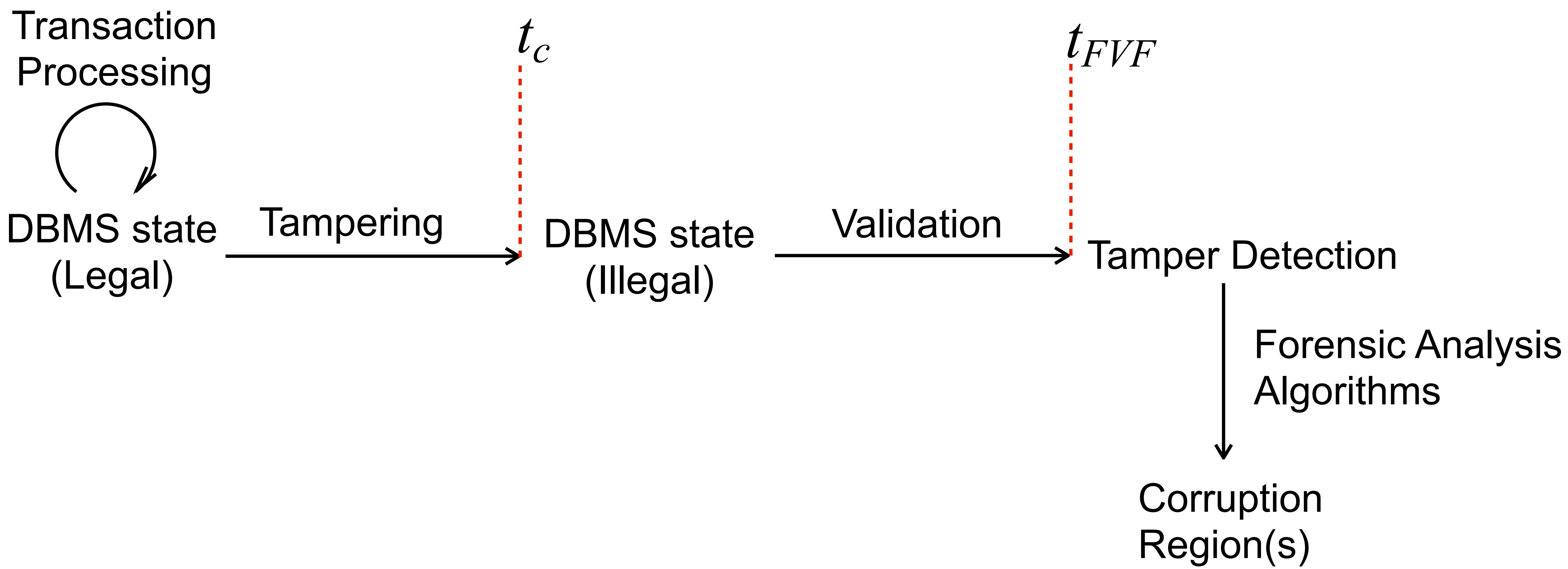
Tampering, Detection and Forensic Analysis



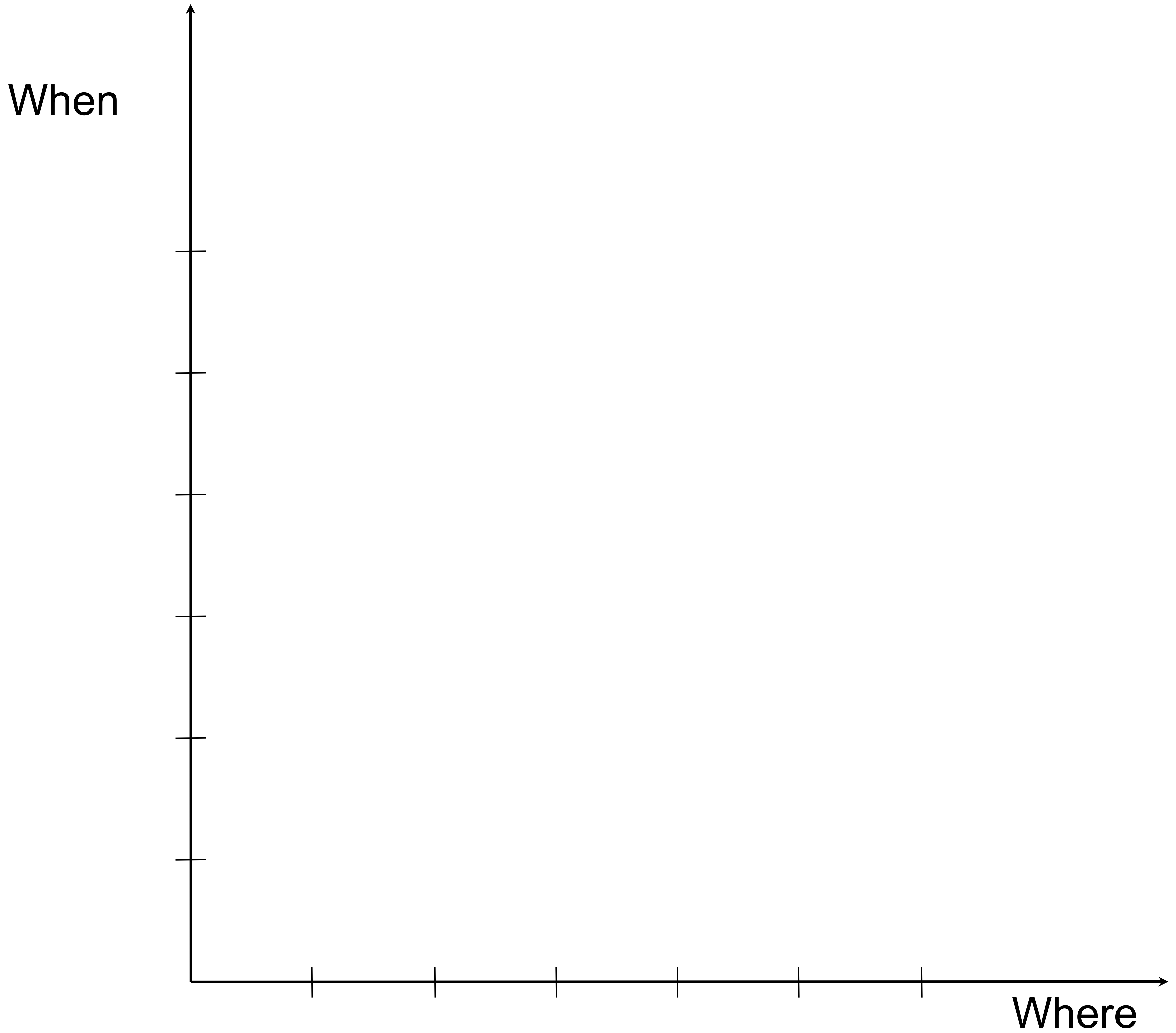
Tampering, Detection and Forensic Analysis



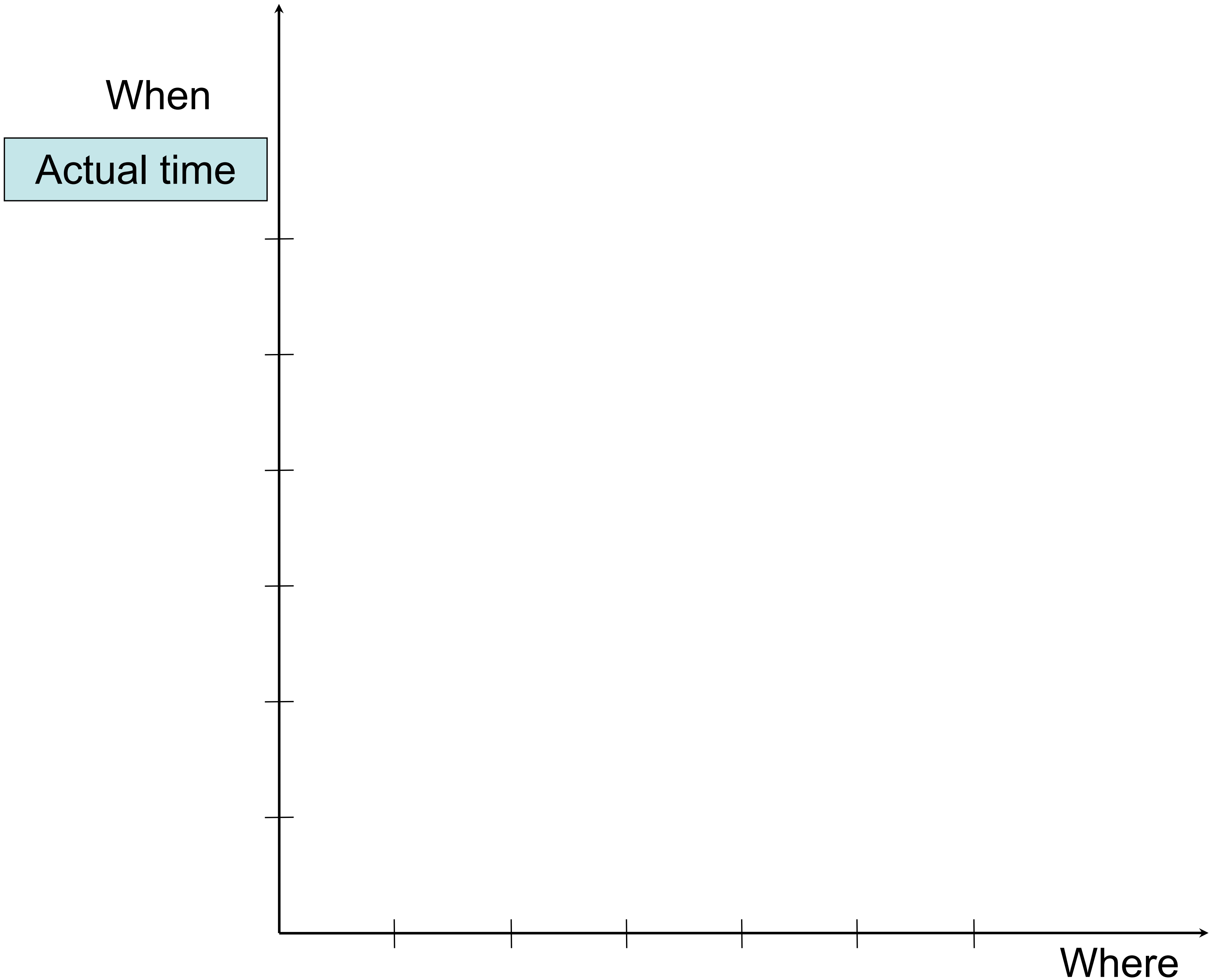
Tampering, Detection and Forensic Analysis



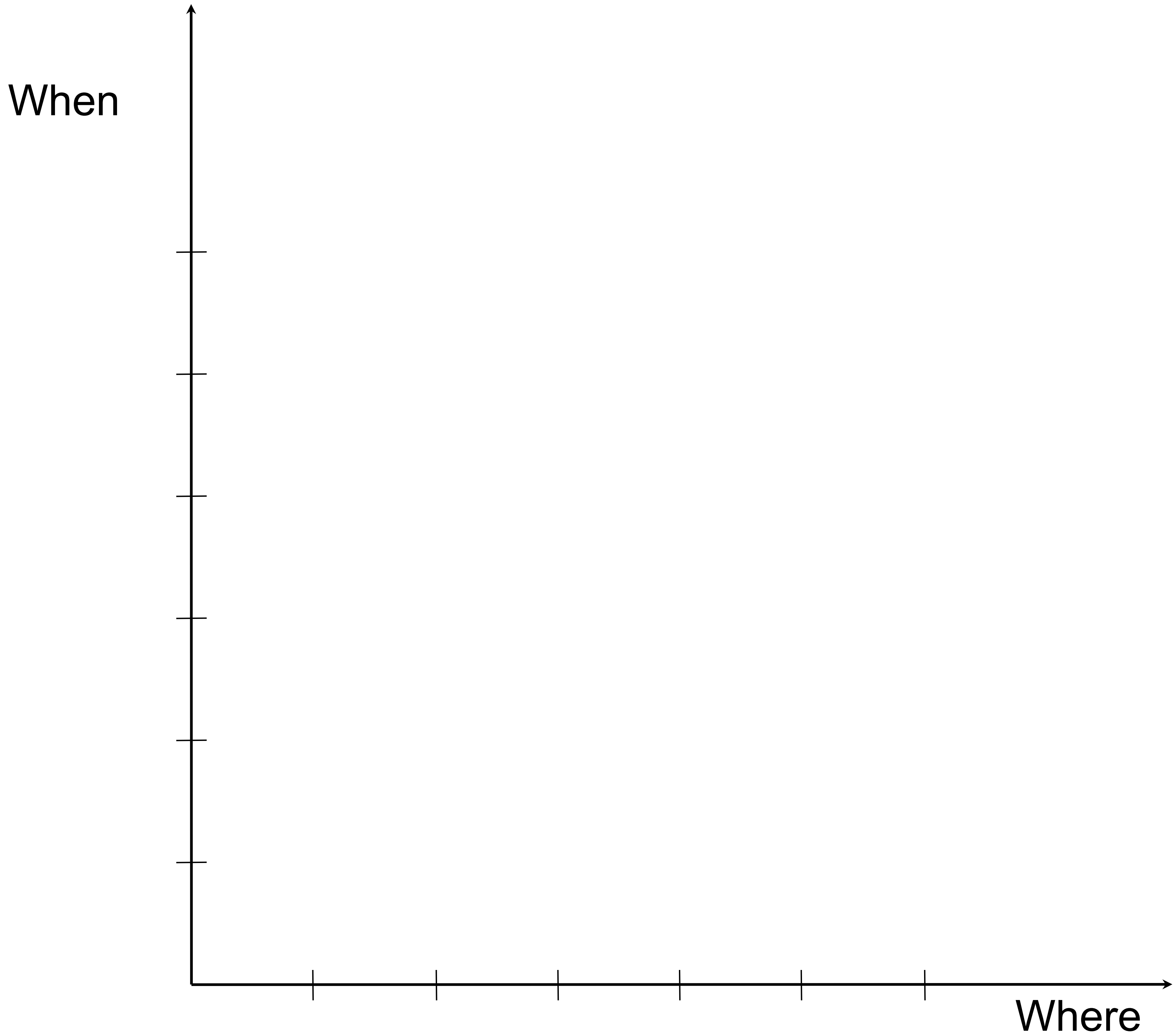
The Corruption Diagram



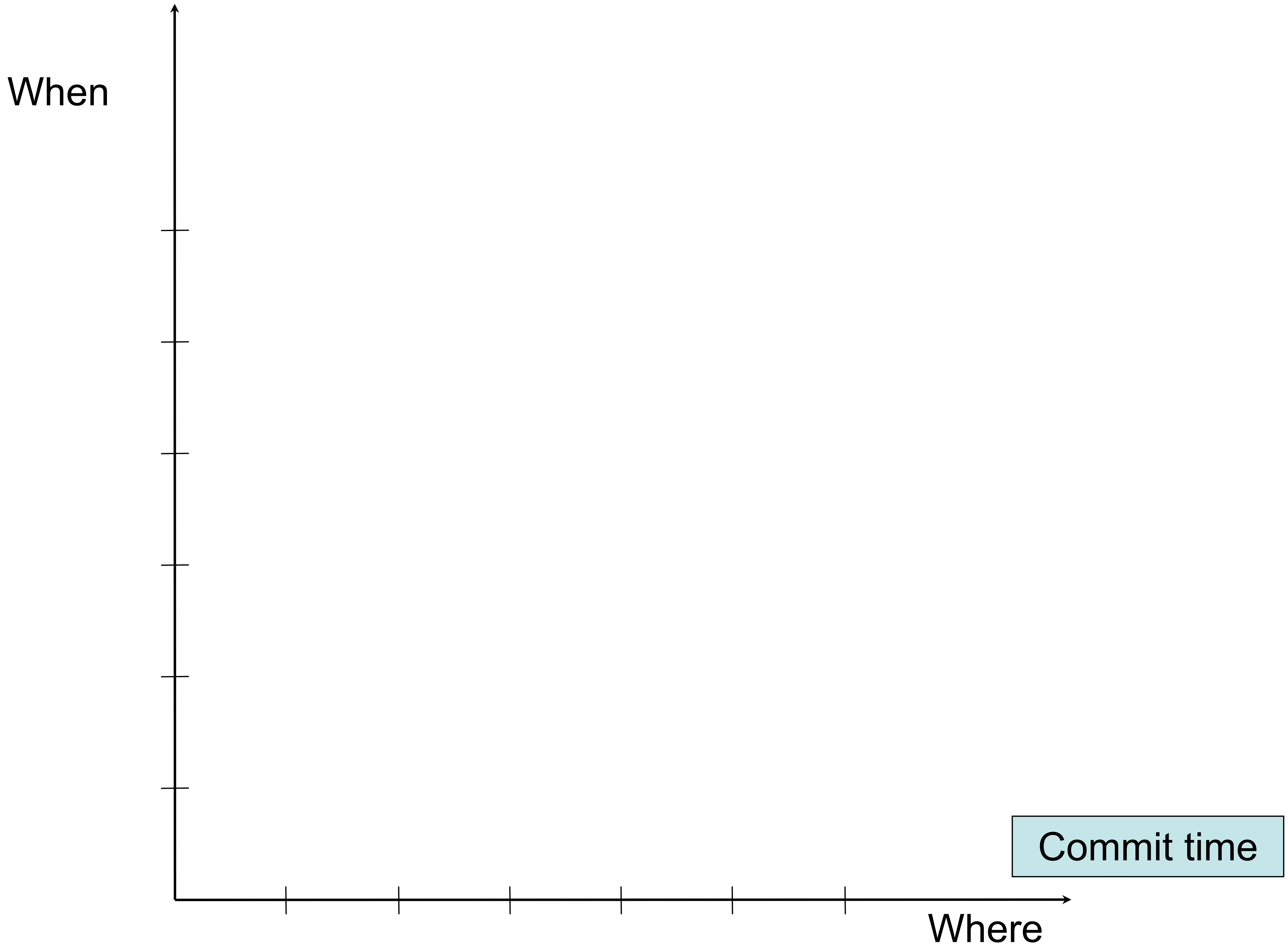
The Corruption Diagram



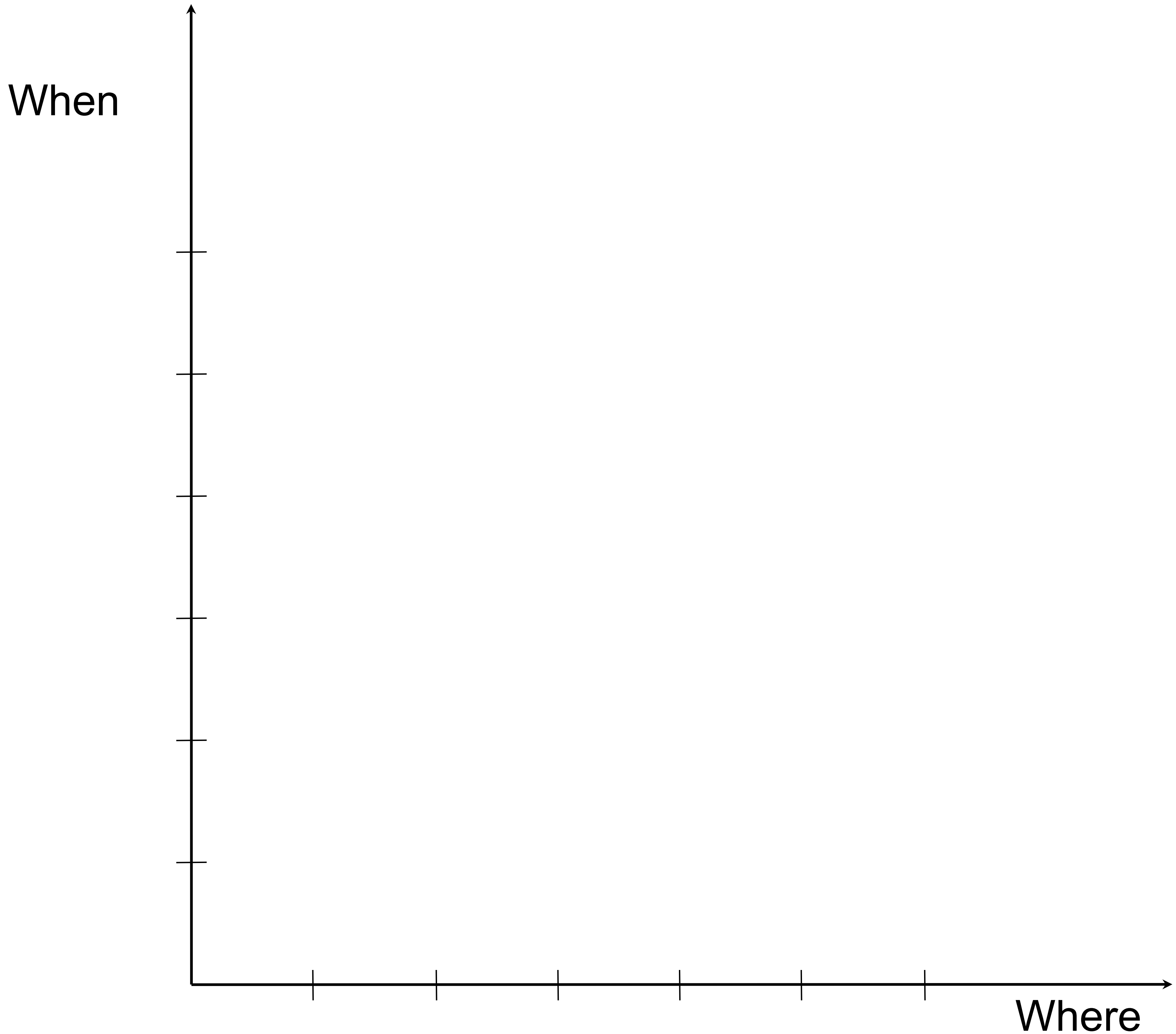
The Corruption Diagram



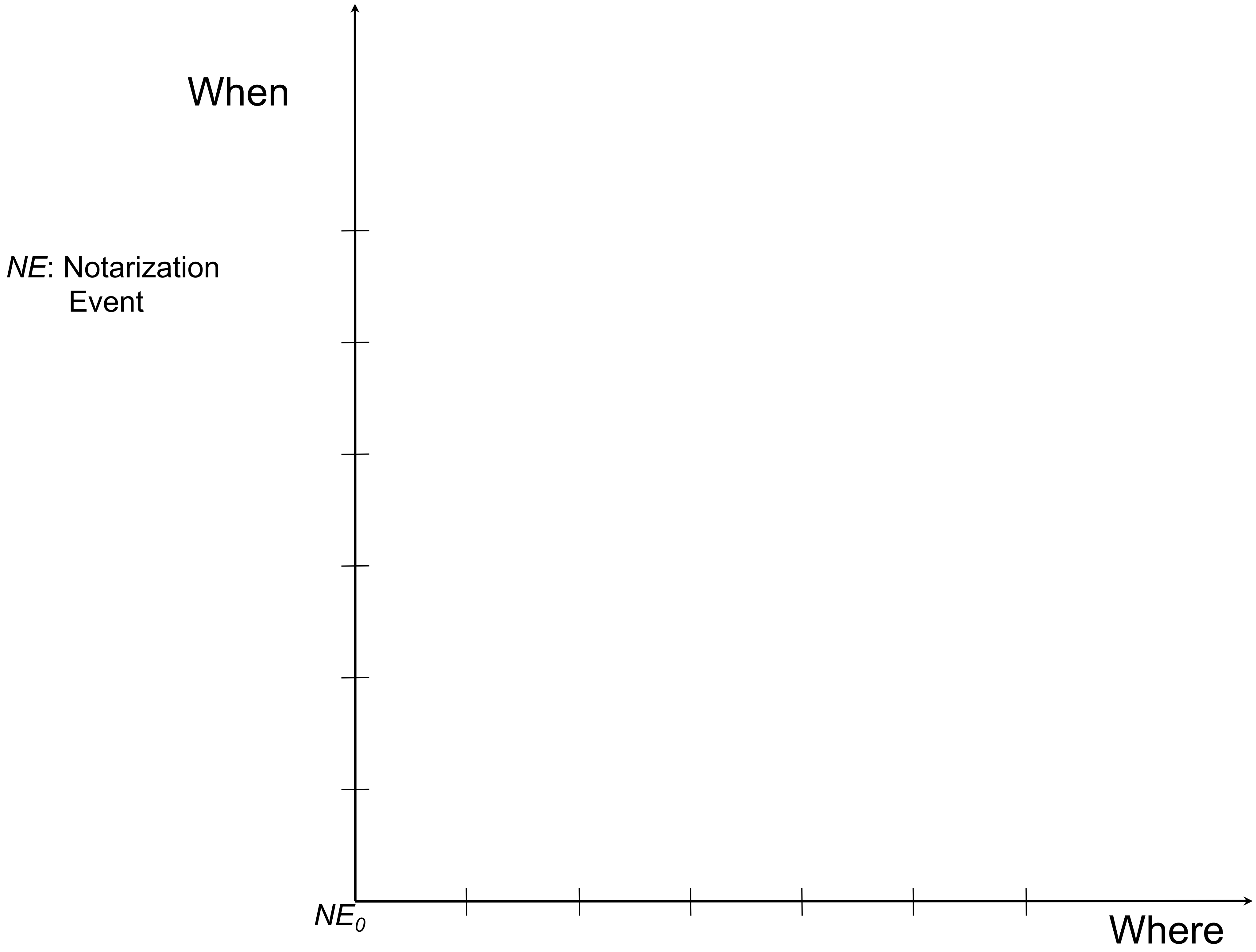
The Corruption Diagram



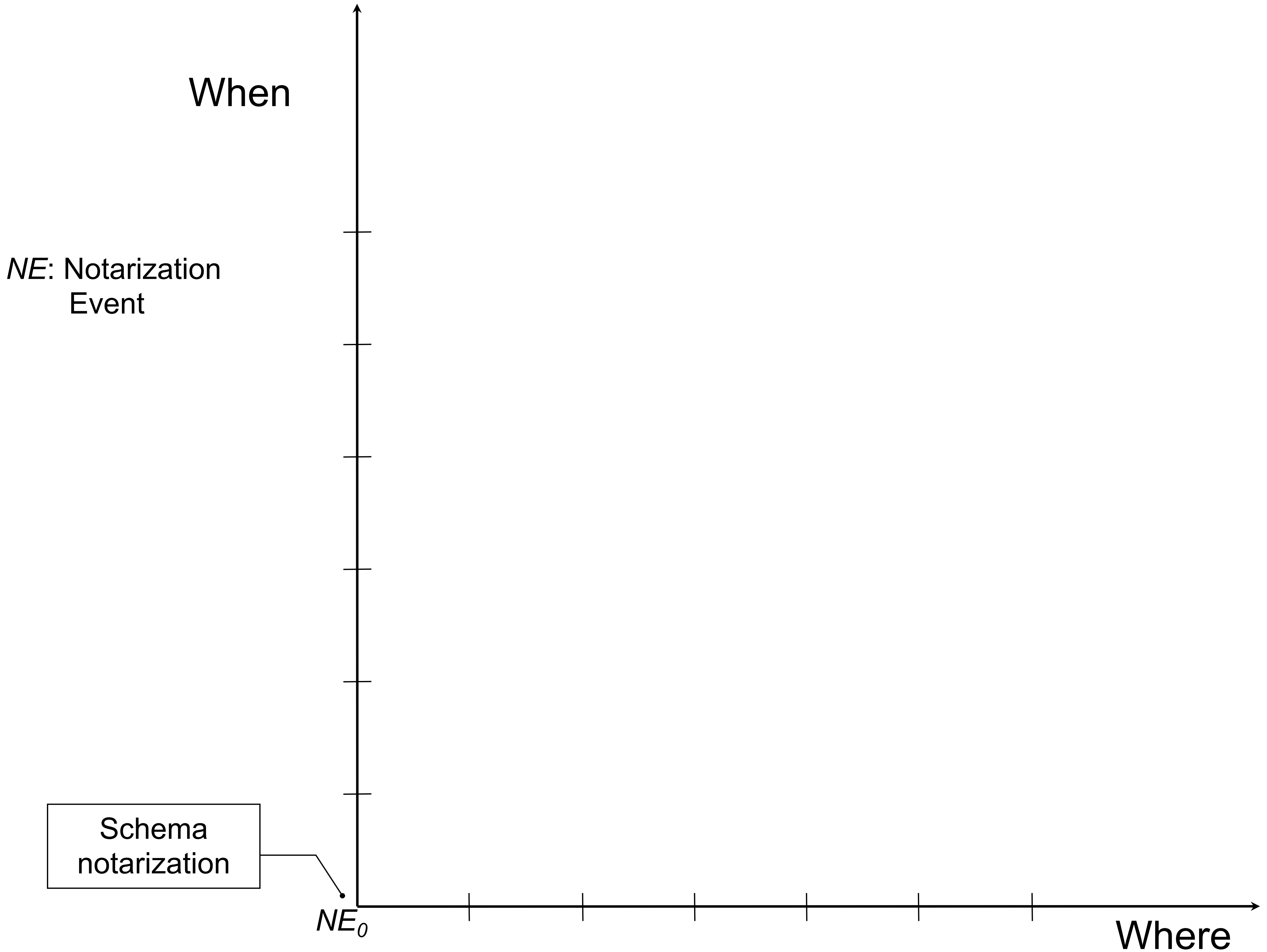
The Corruption Diagram



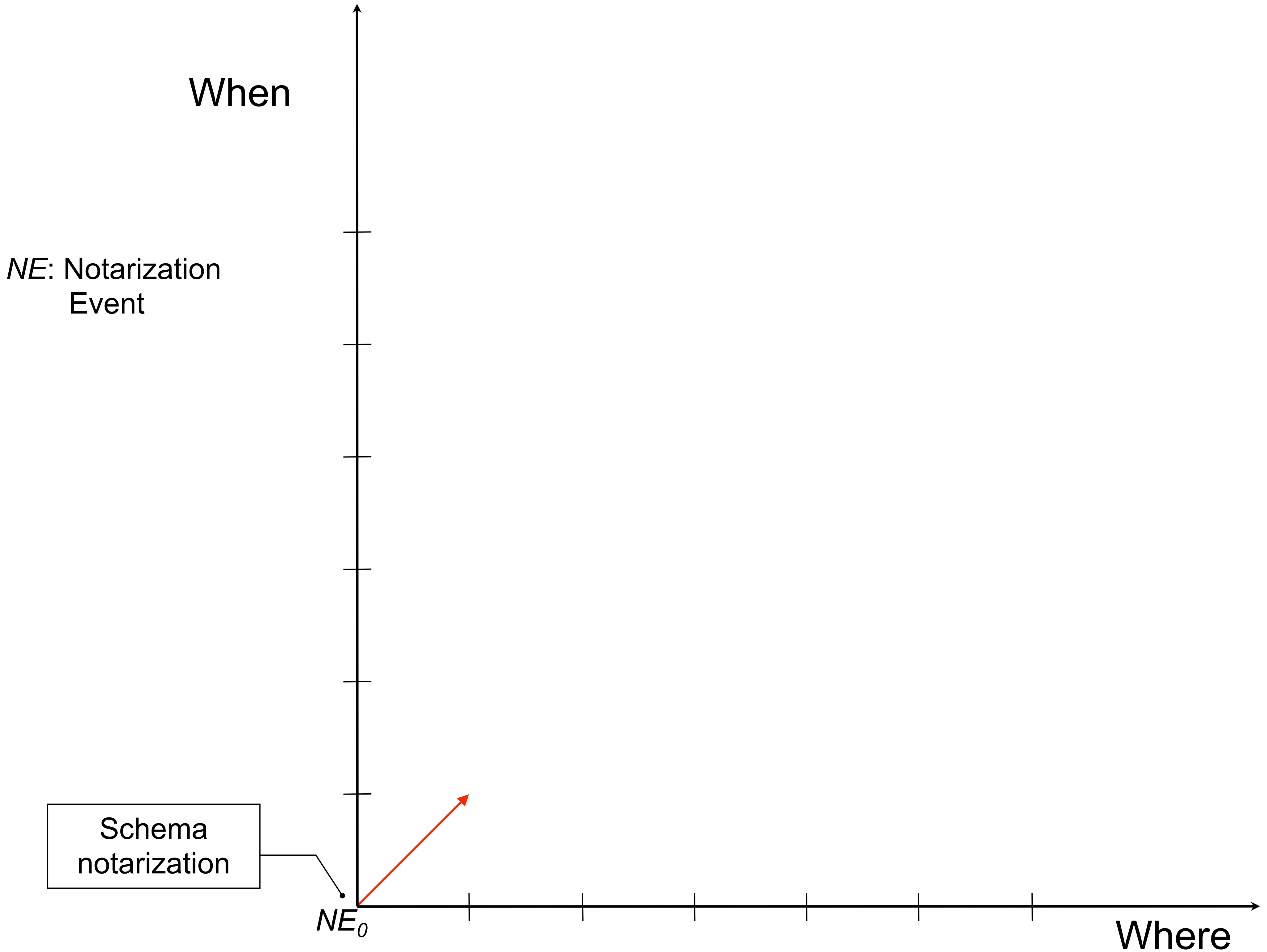
The Corruption Diagram



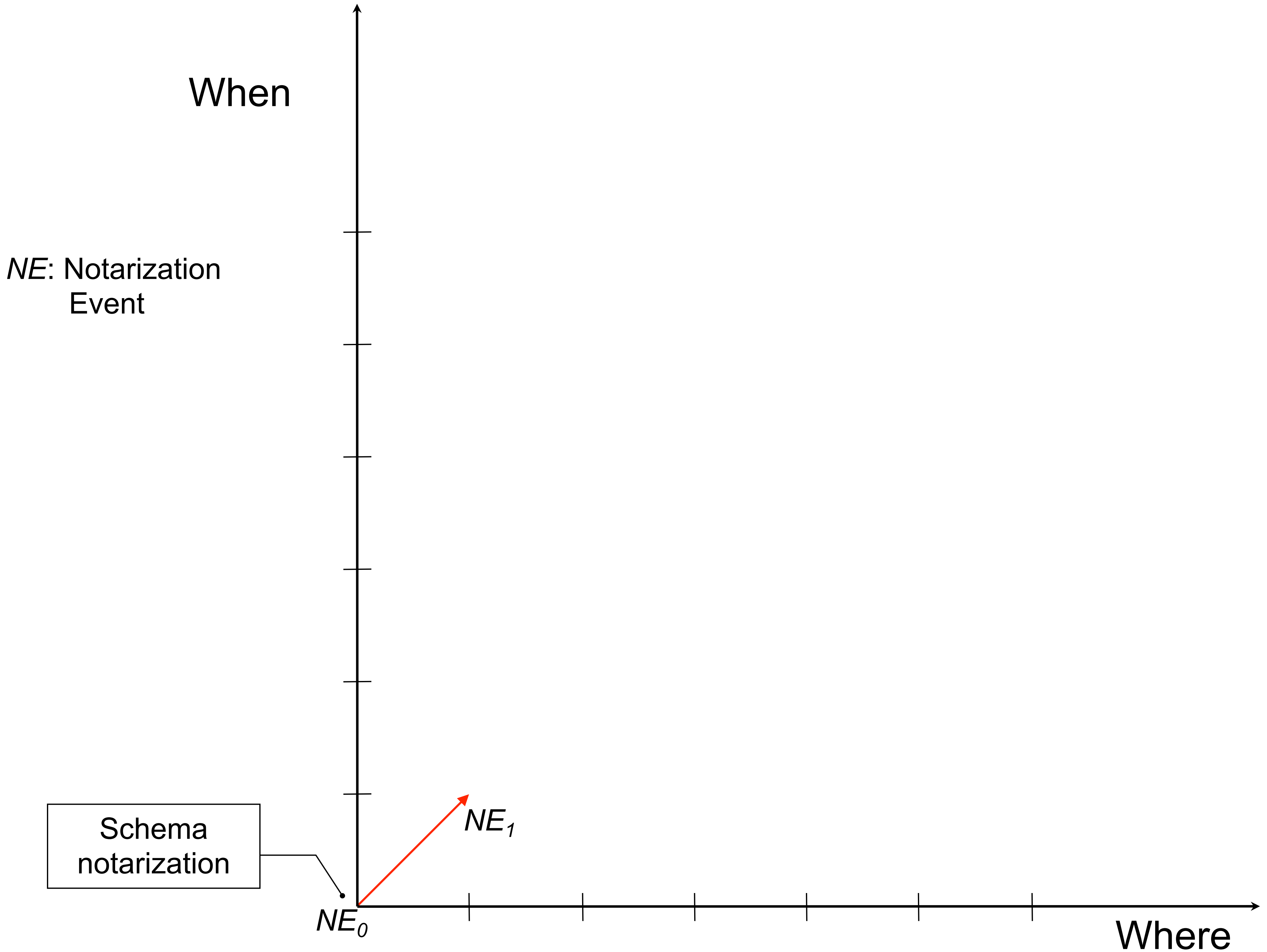
The Corruption Diagram



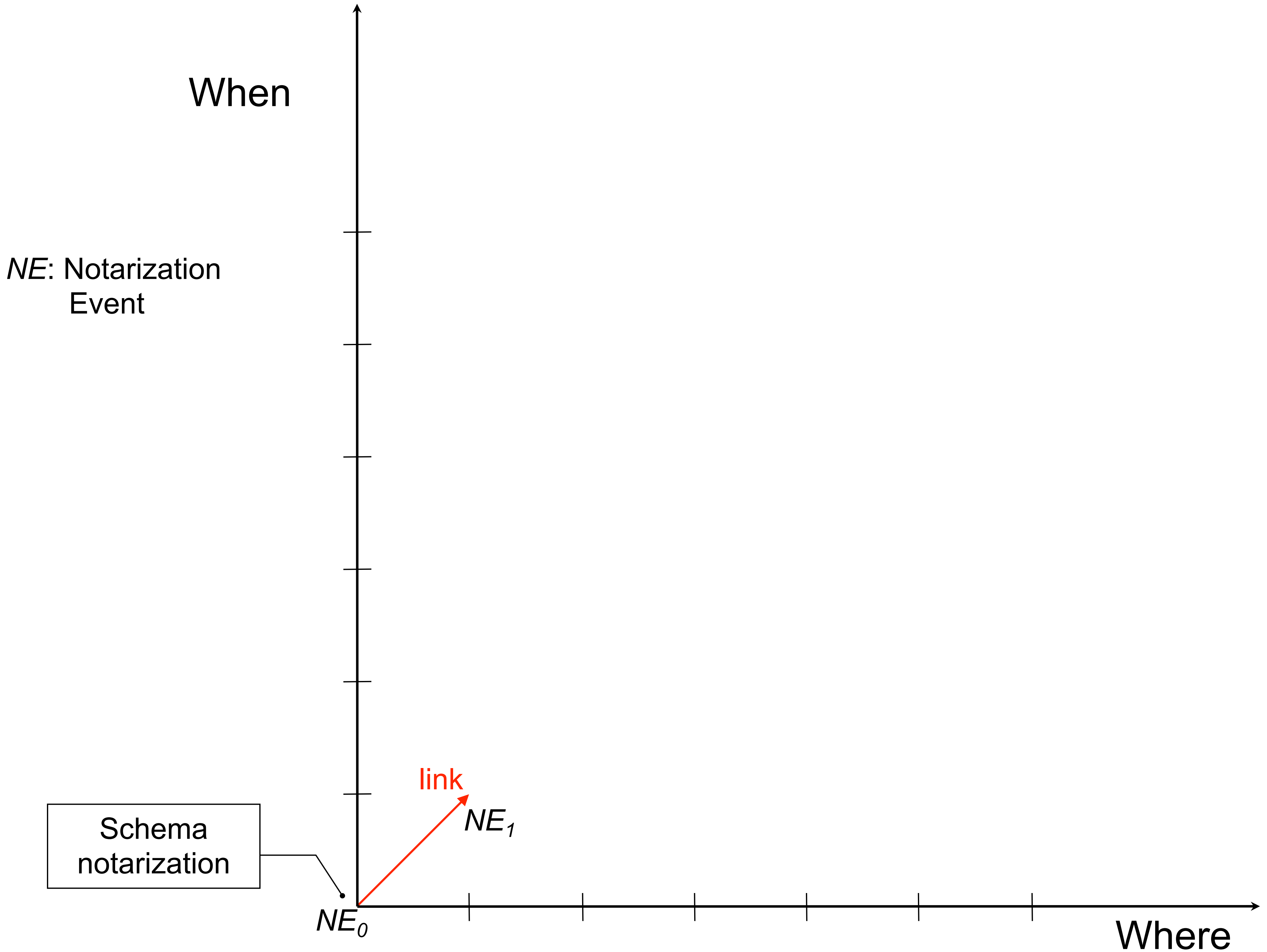
The Corruption Diagram



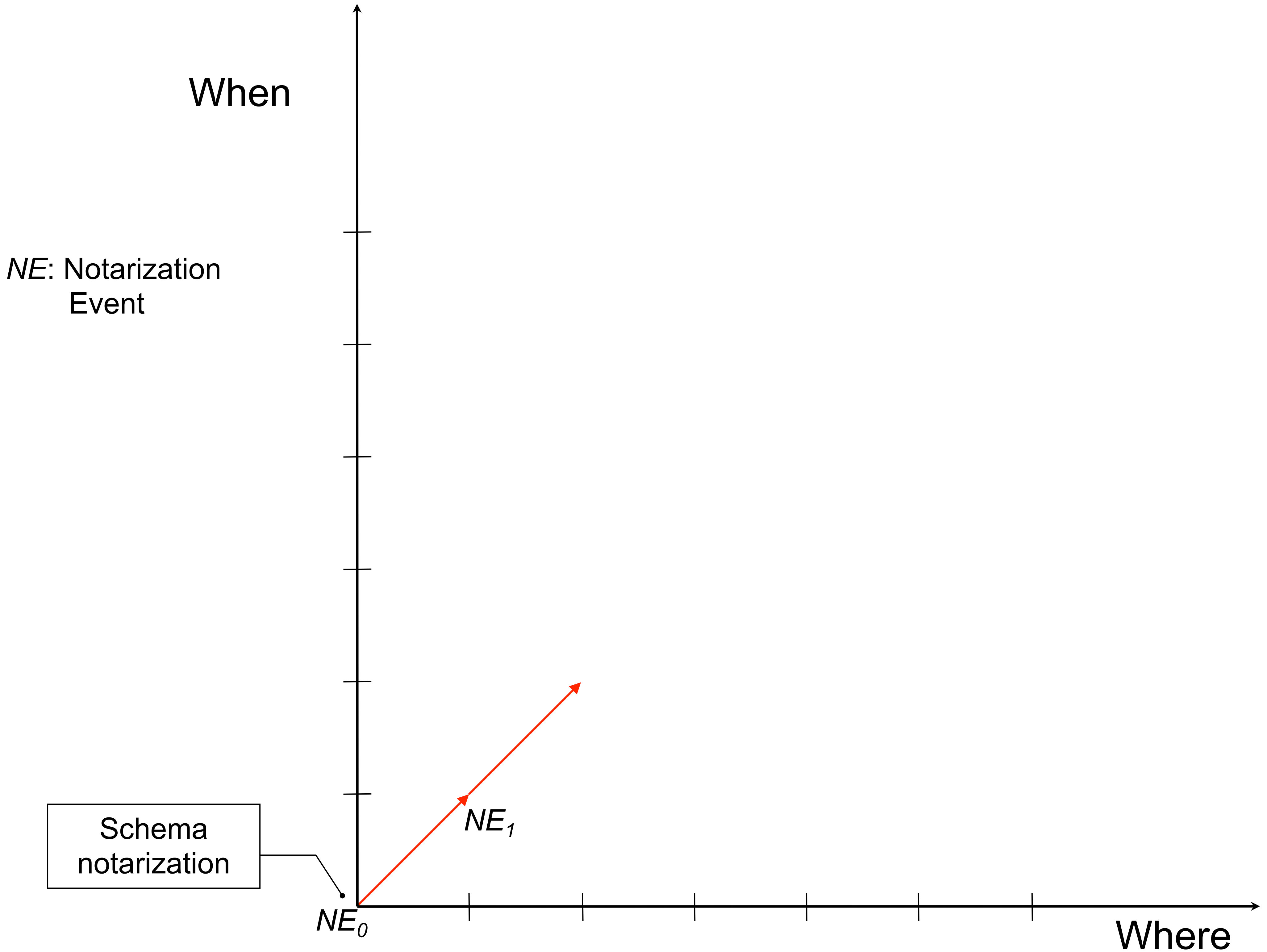
The Corruption Diagram



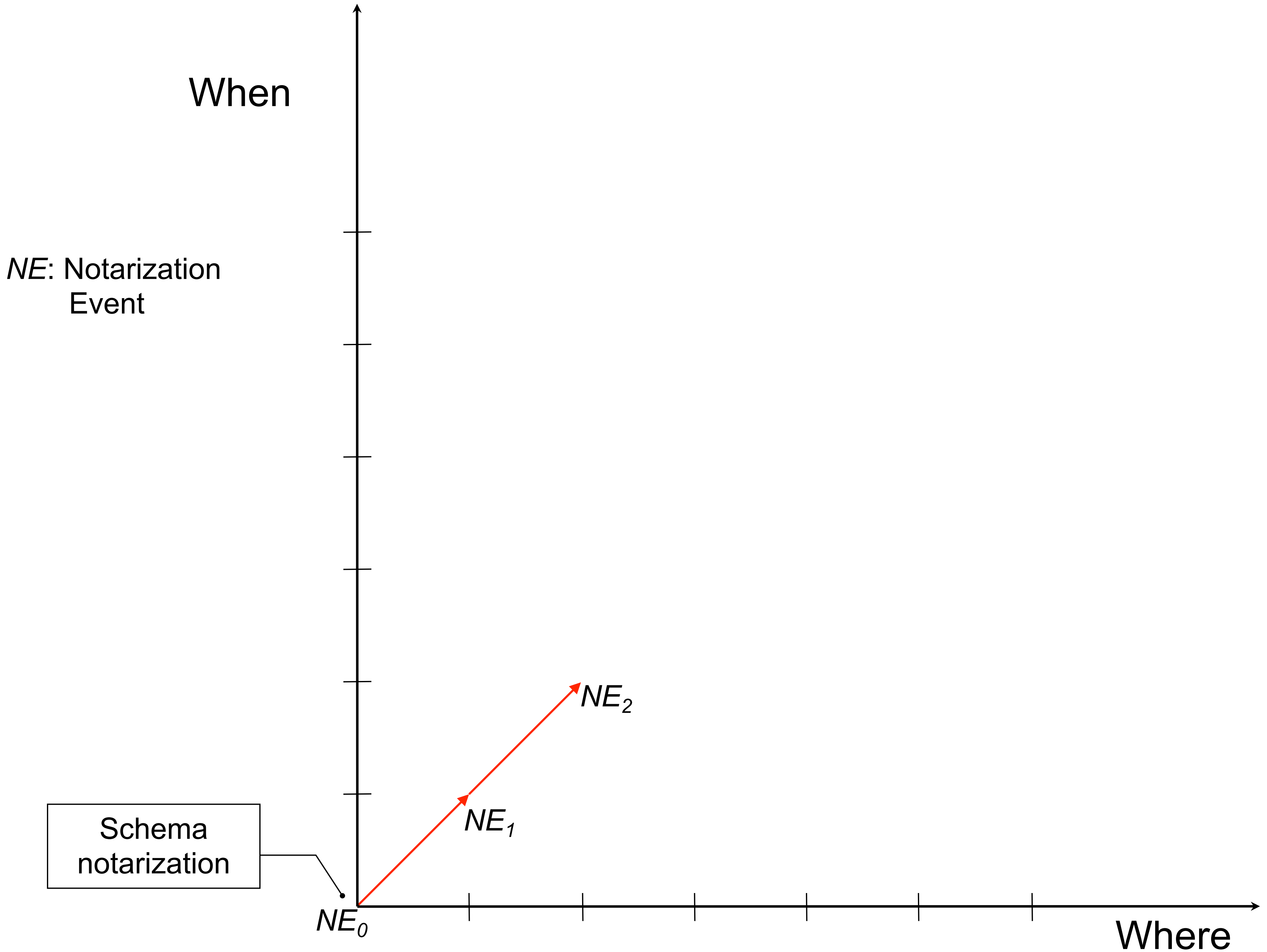
The Corruption Diagram



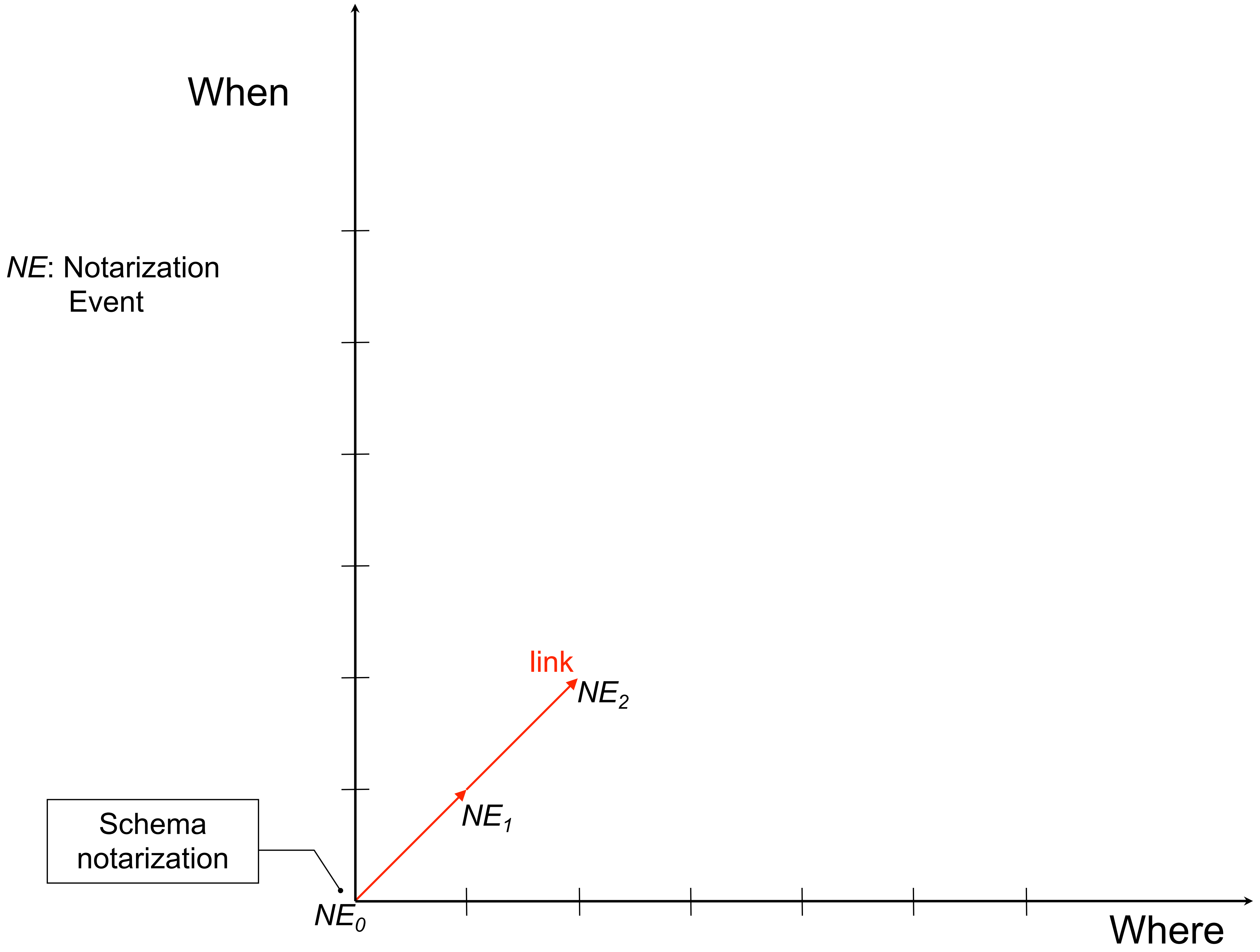
The Corruption Diagram



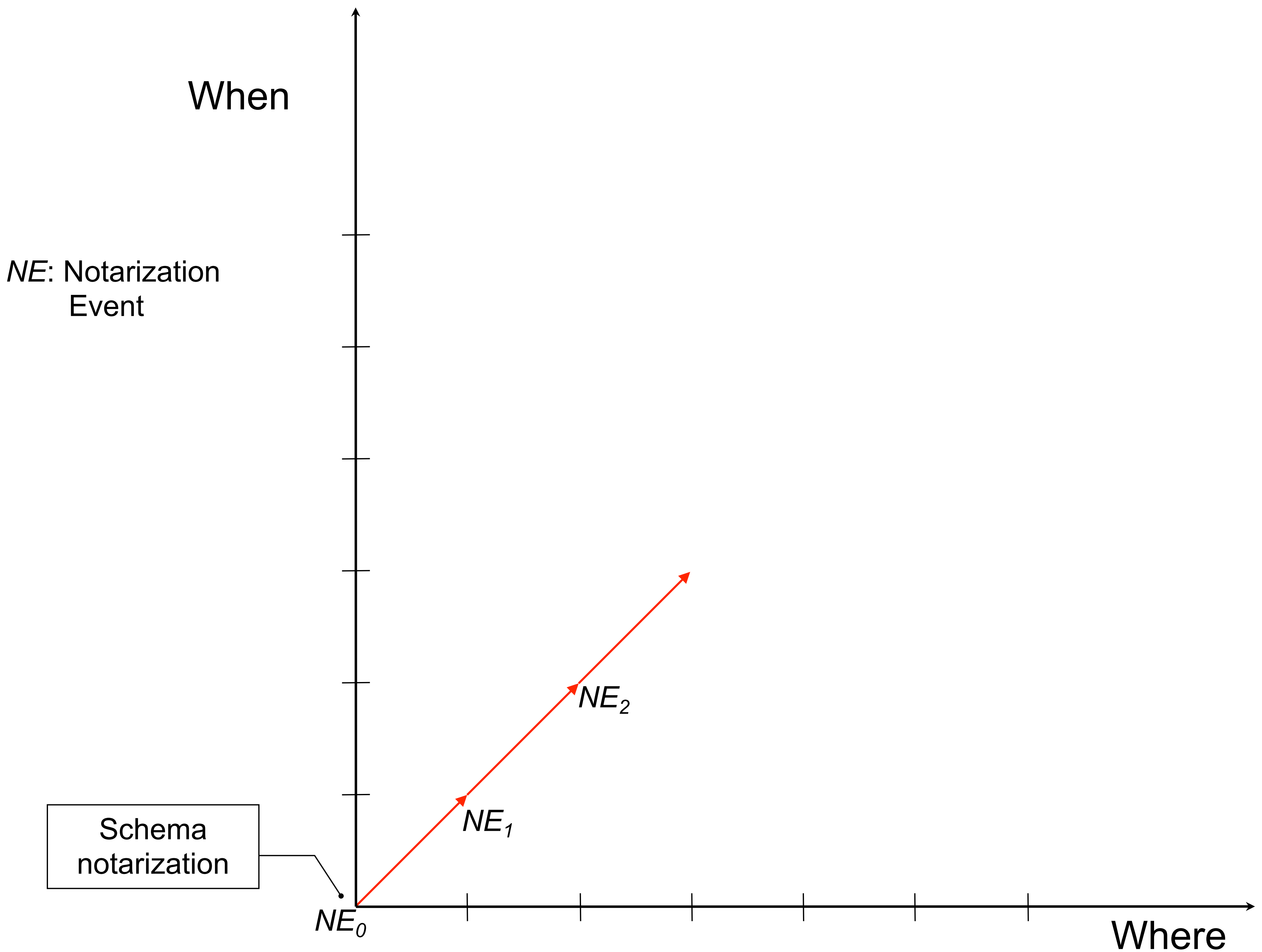
The Corruption Diagram



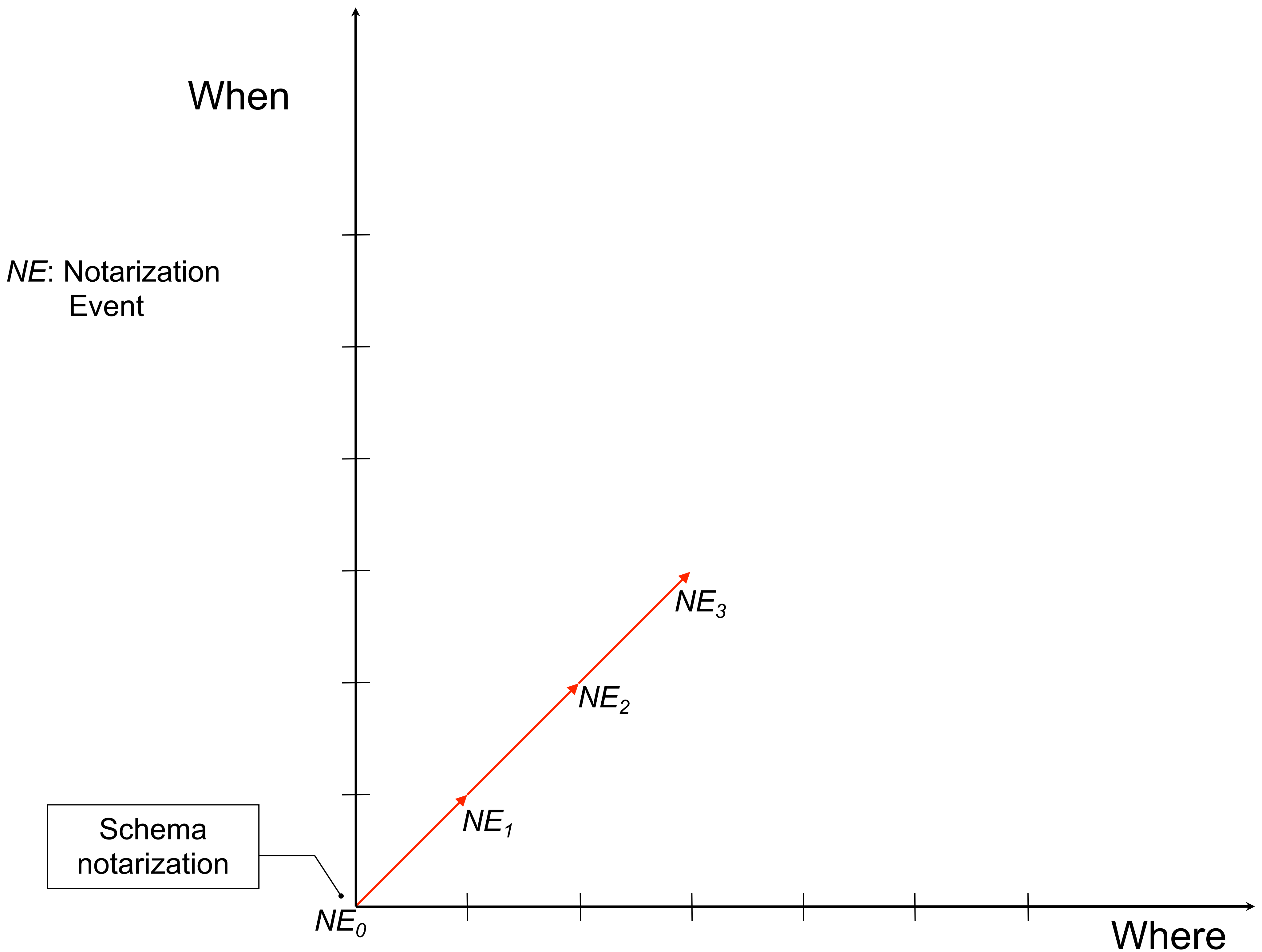
The Corruption Diagram



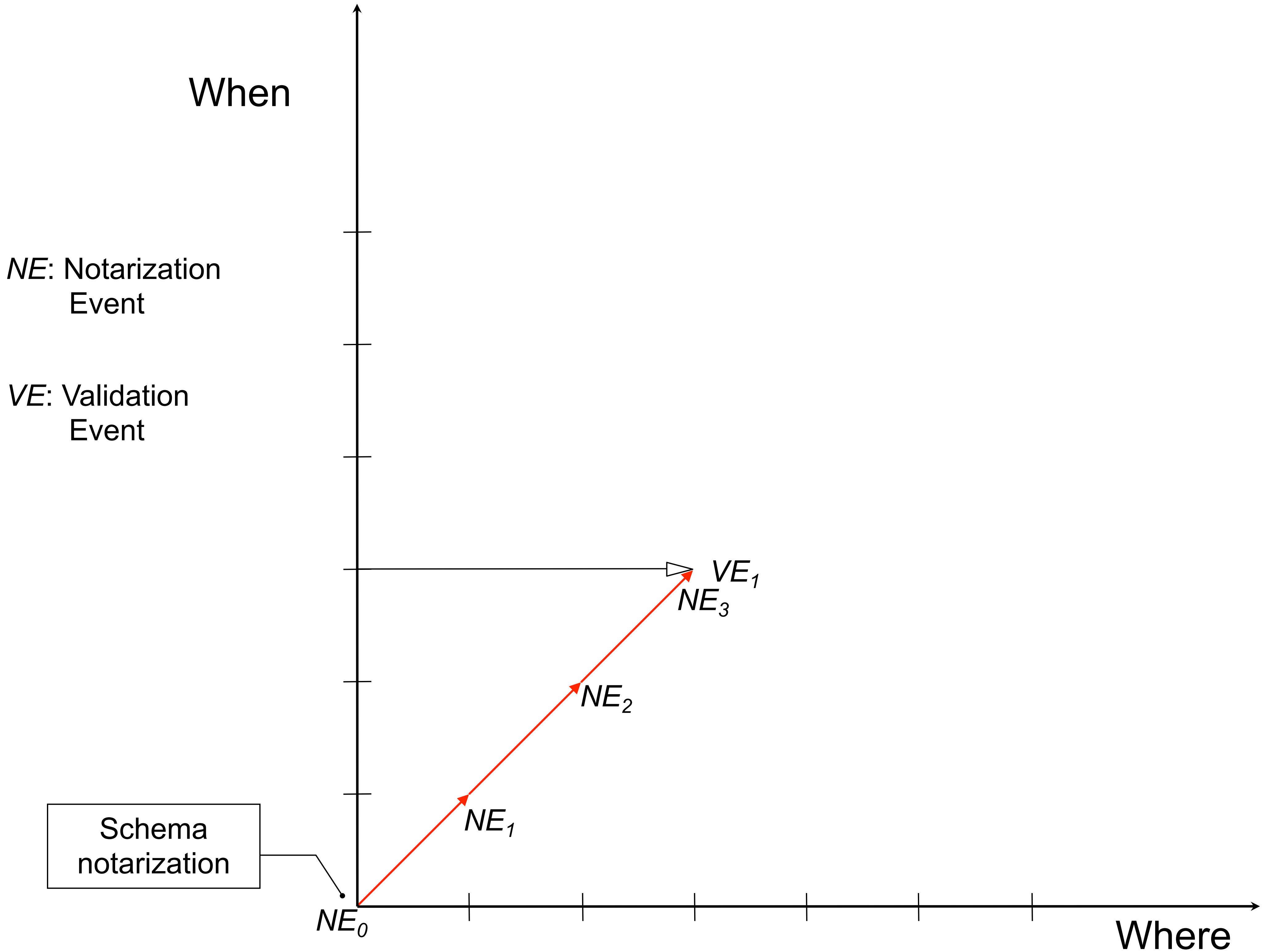
The Corruption Diagram



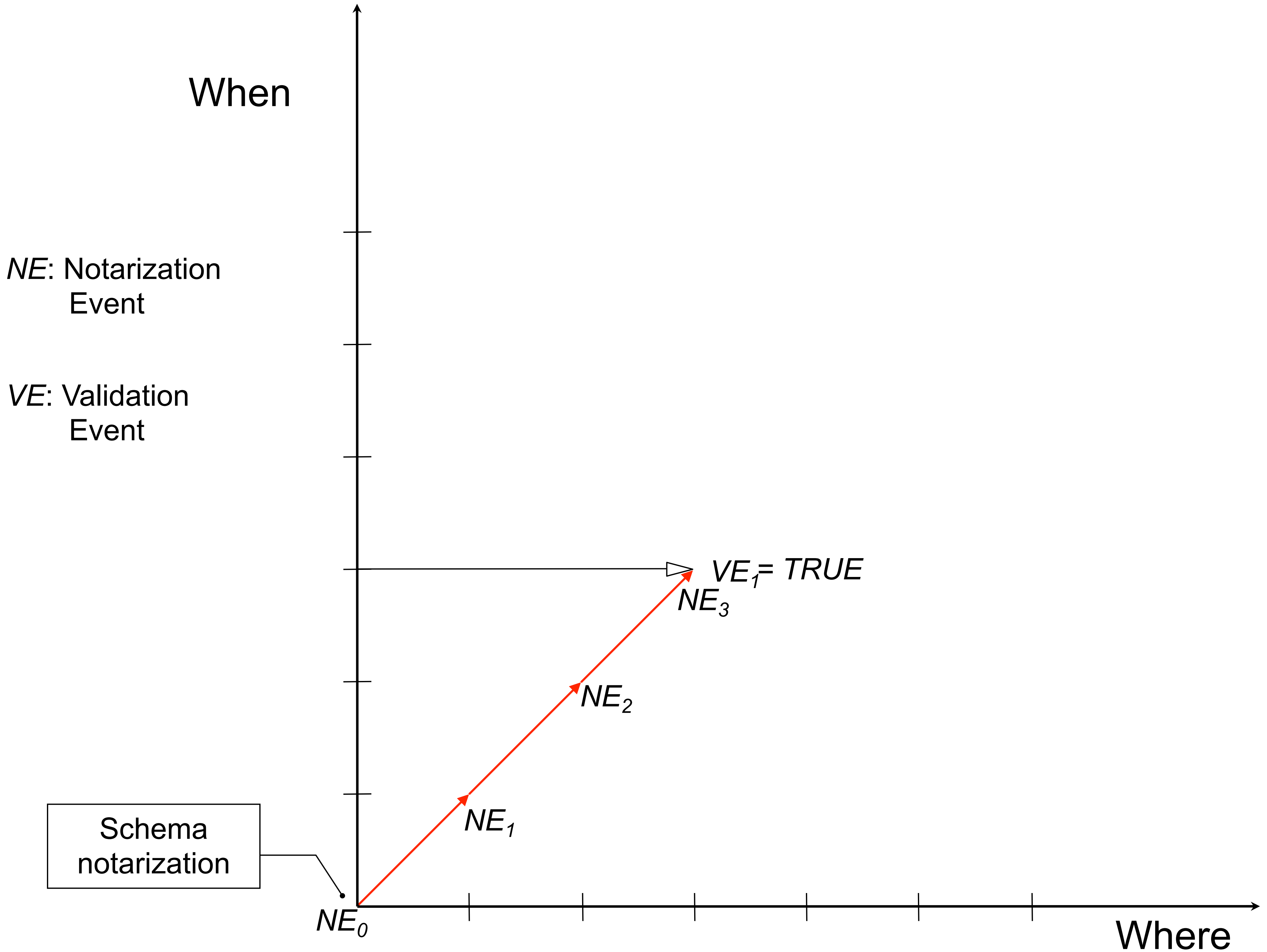
The Corruption Diagram



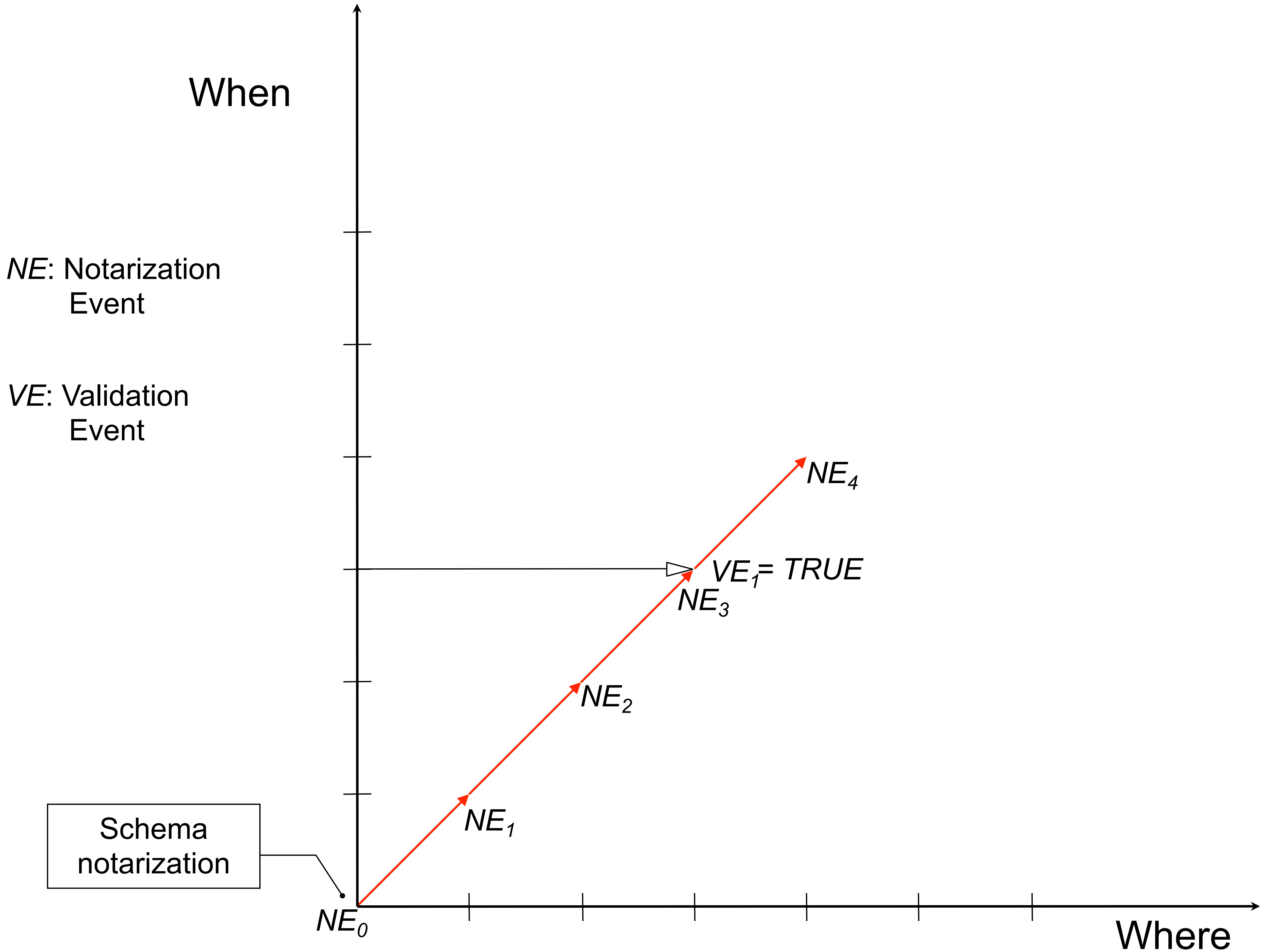
The Corruption Diagram



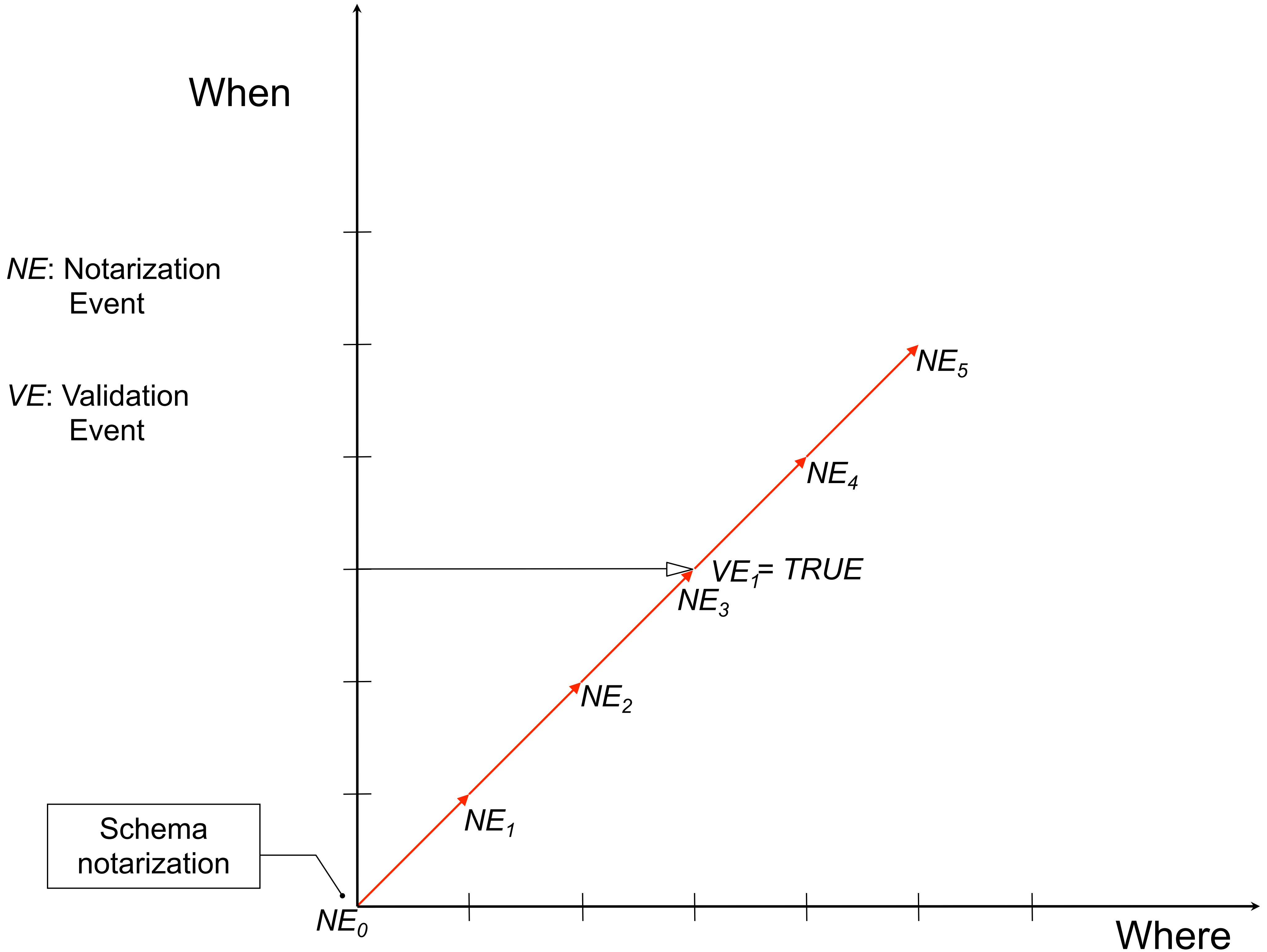
The Corruption Diagram



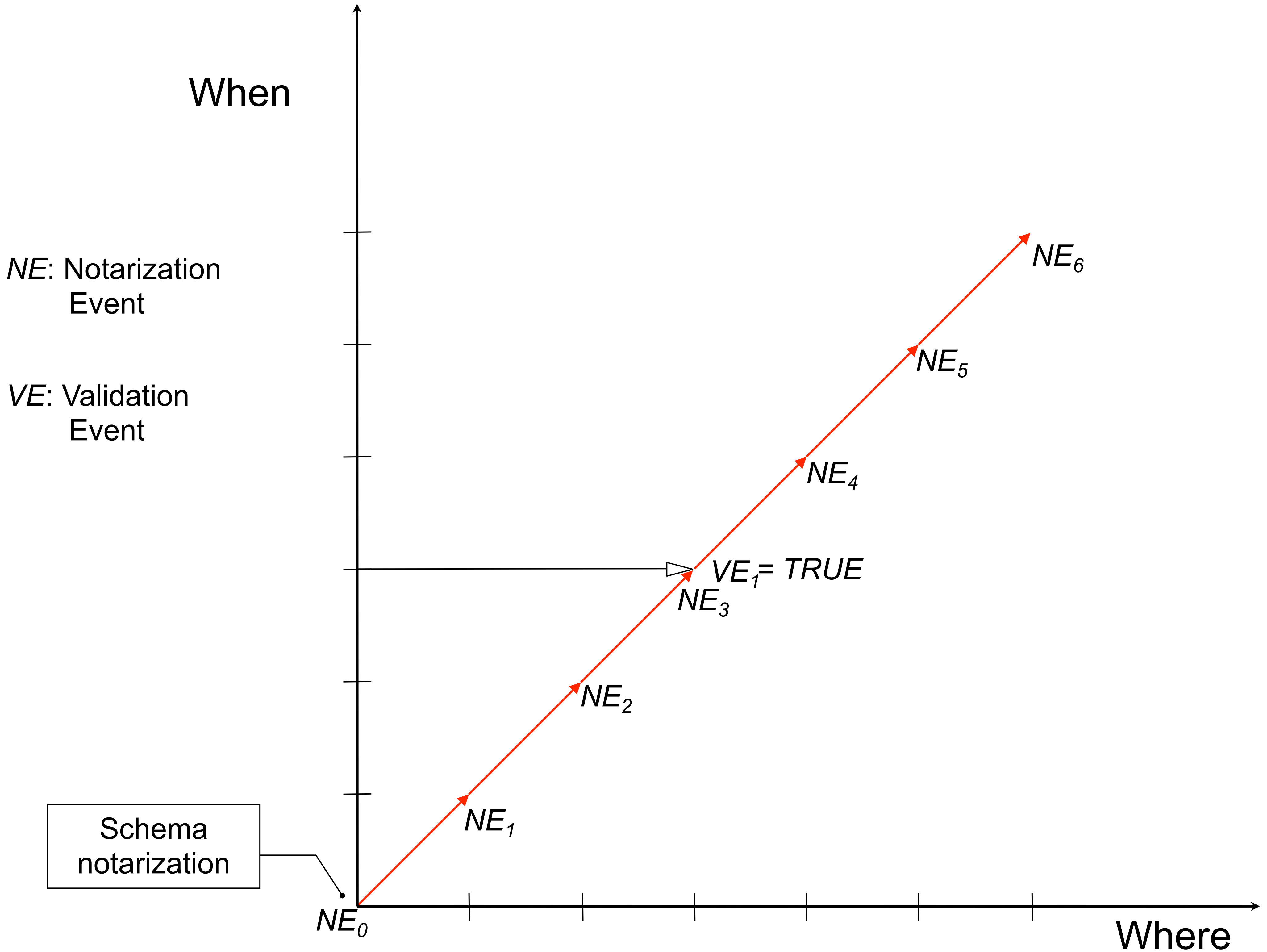
The Corruption Diagram



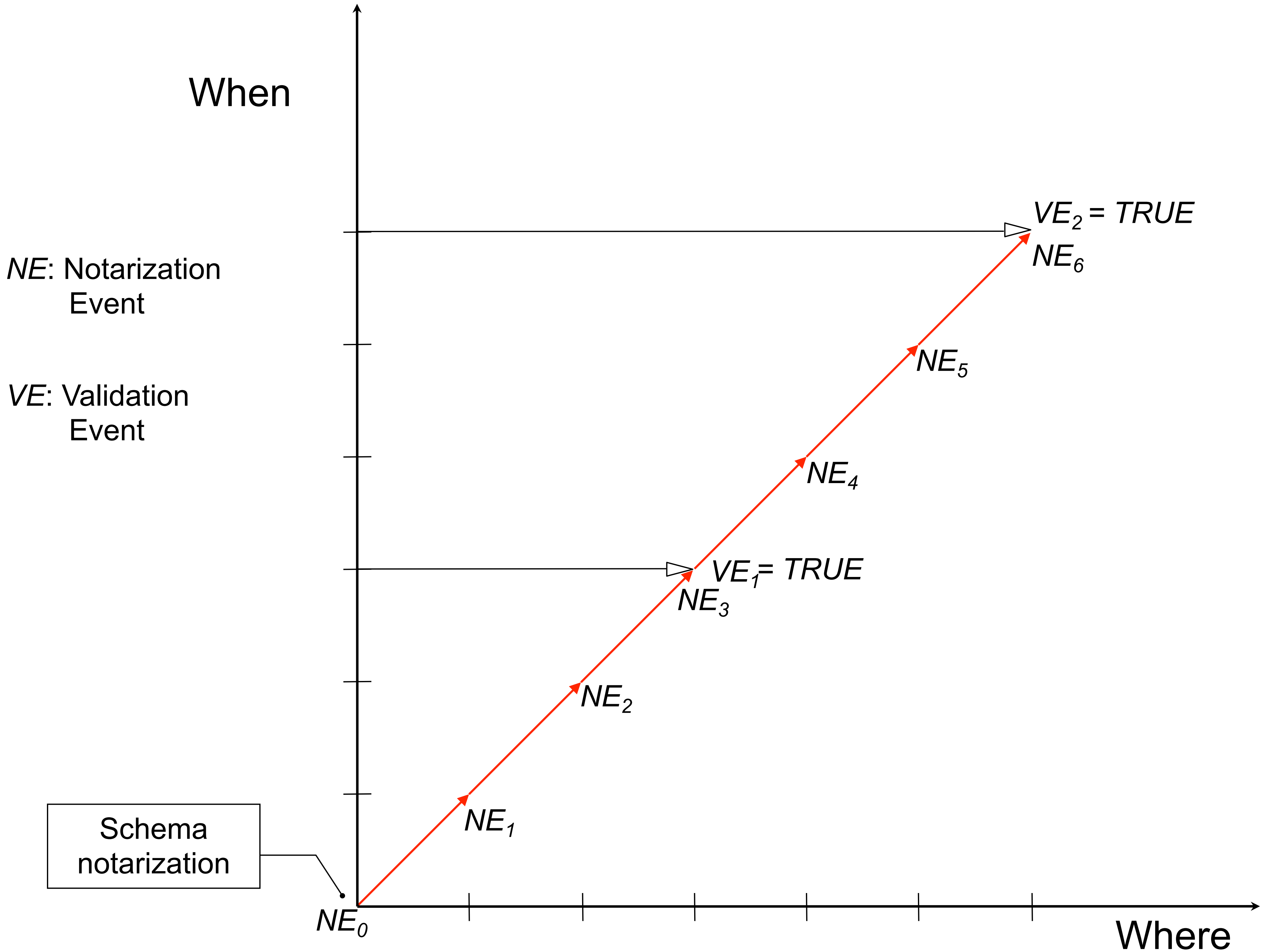
The Corruption Diagram



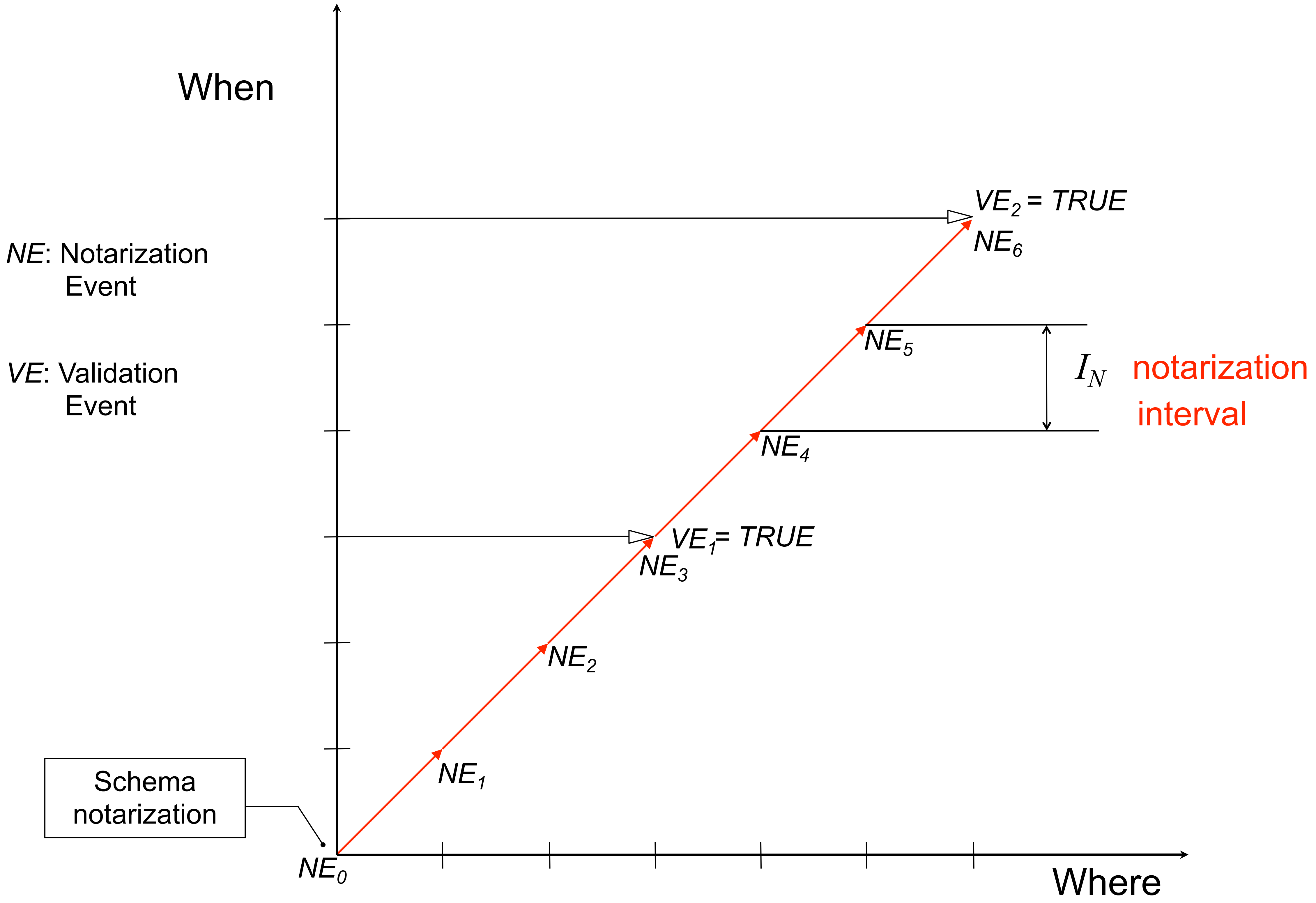
The Corruption Diagram



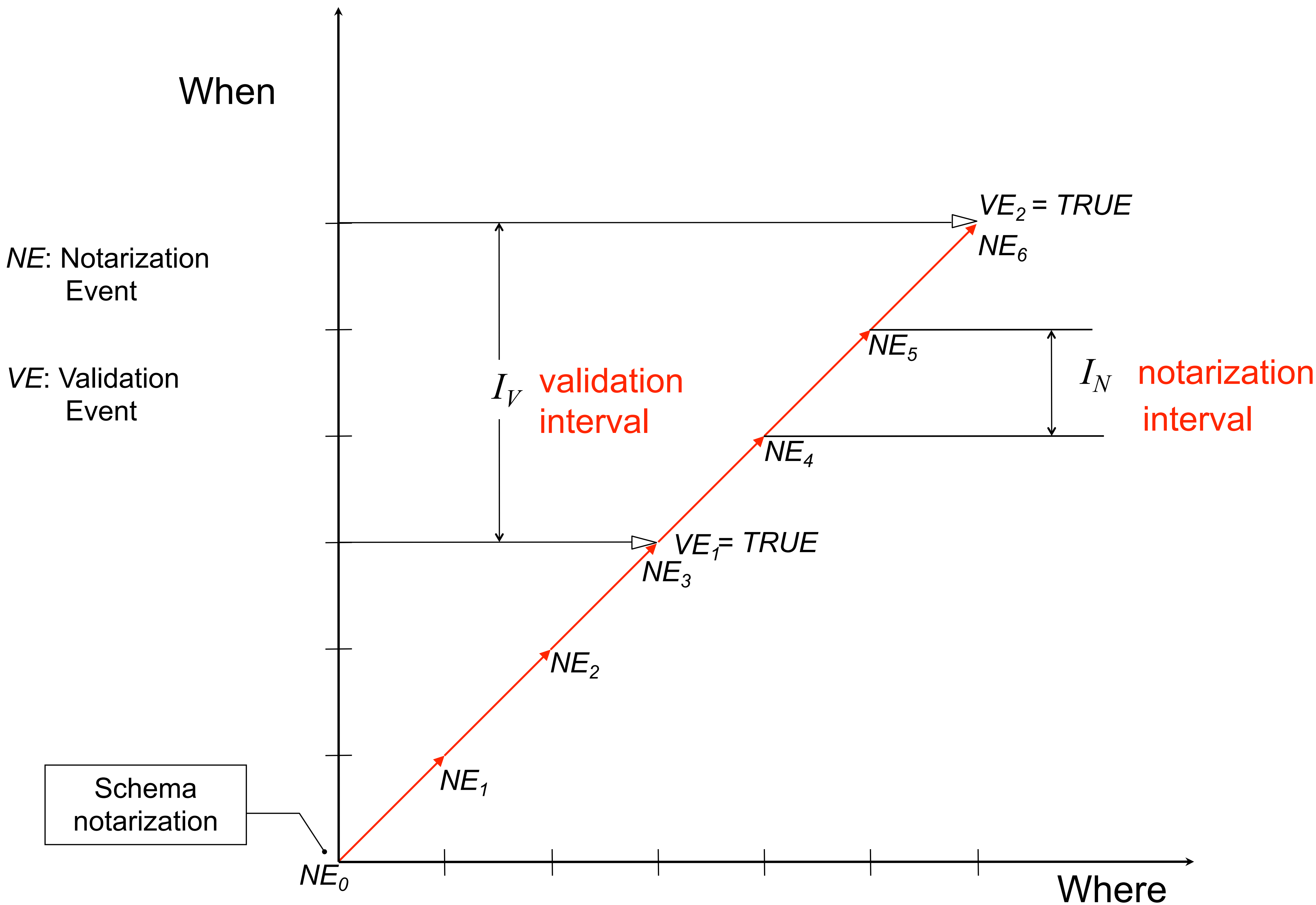
The Corruption Diagram



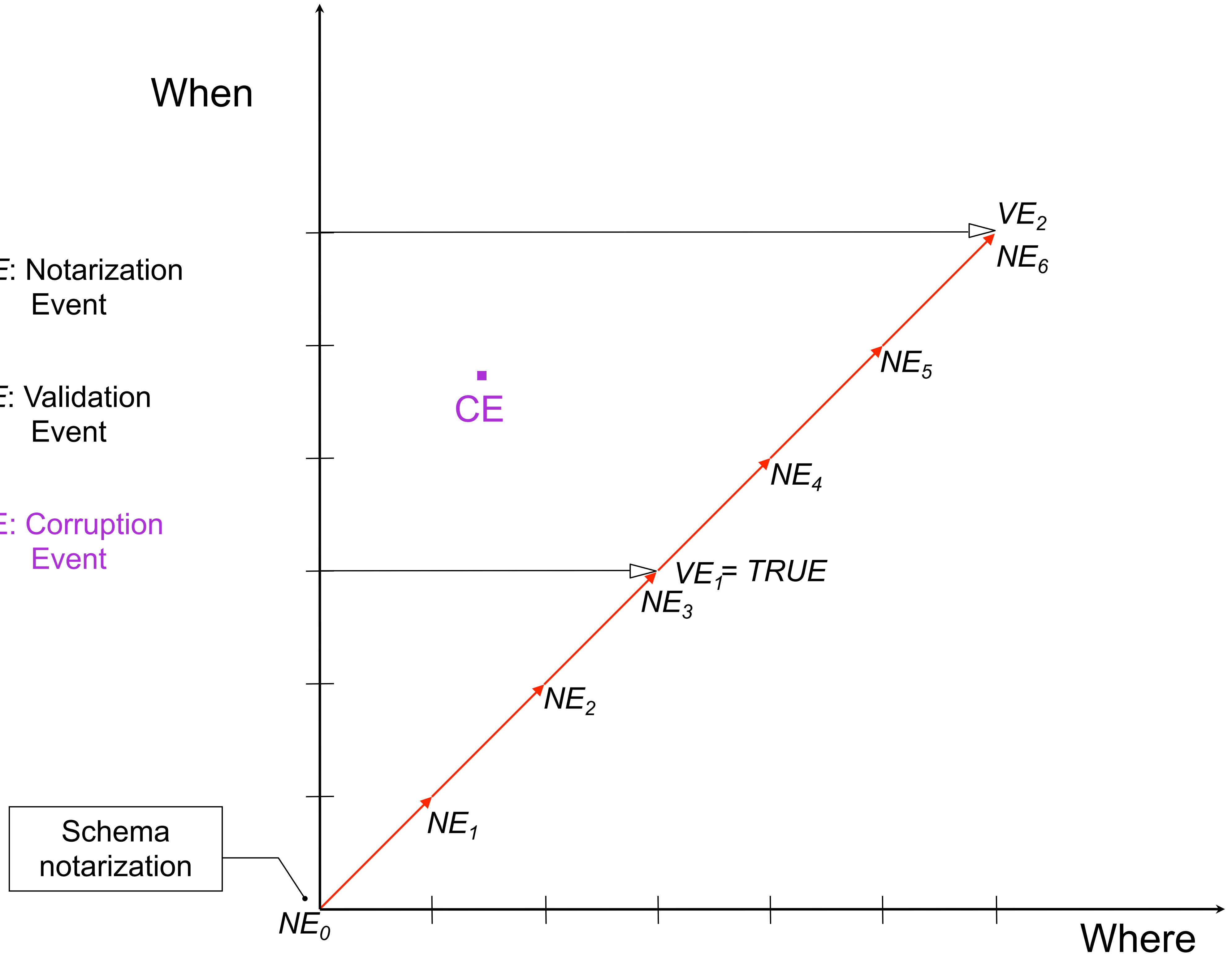
The Corruption Diagram



The Corruption Diagram



The Corruption Diagram

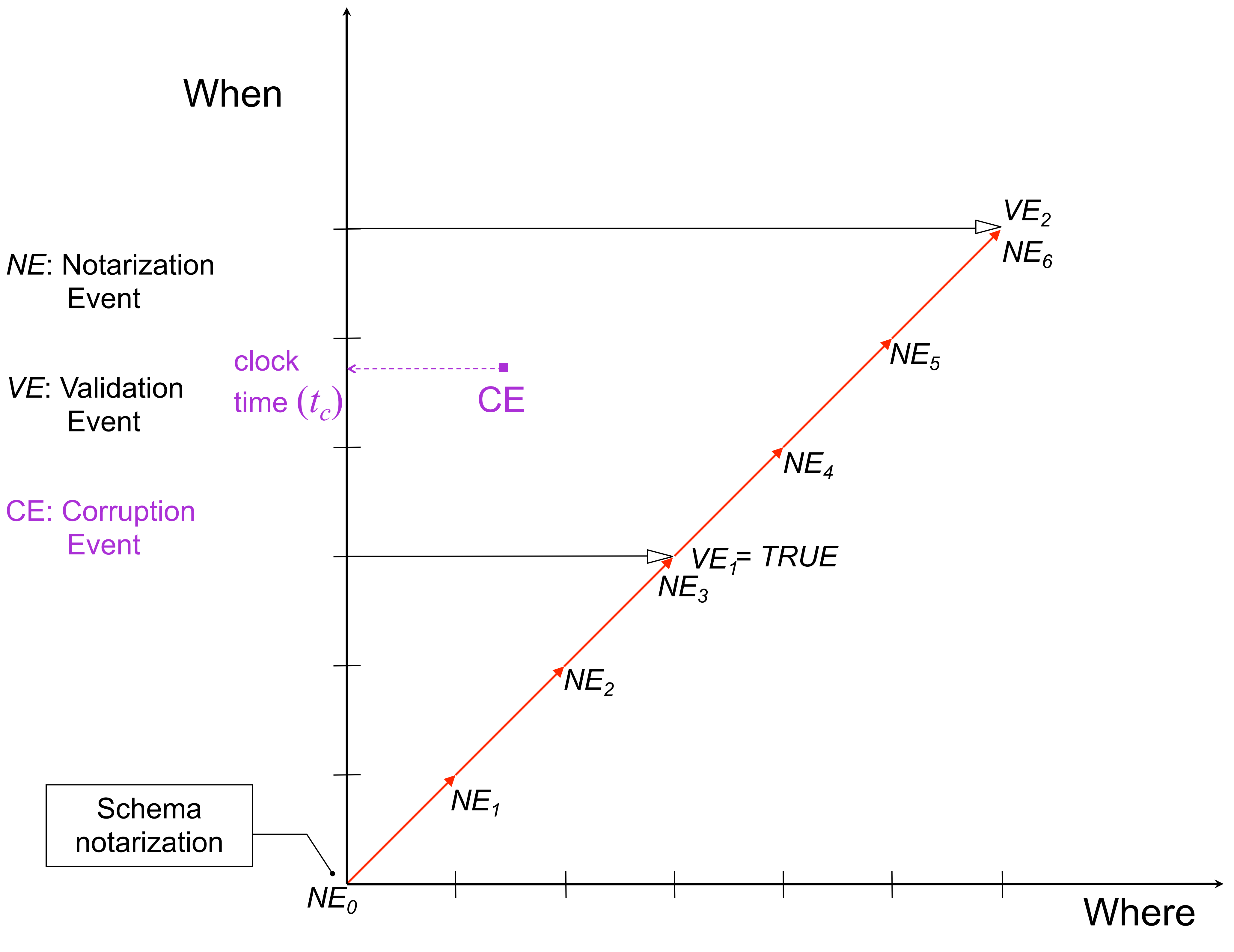


NE: Notarization Event

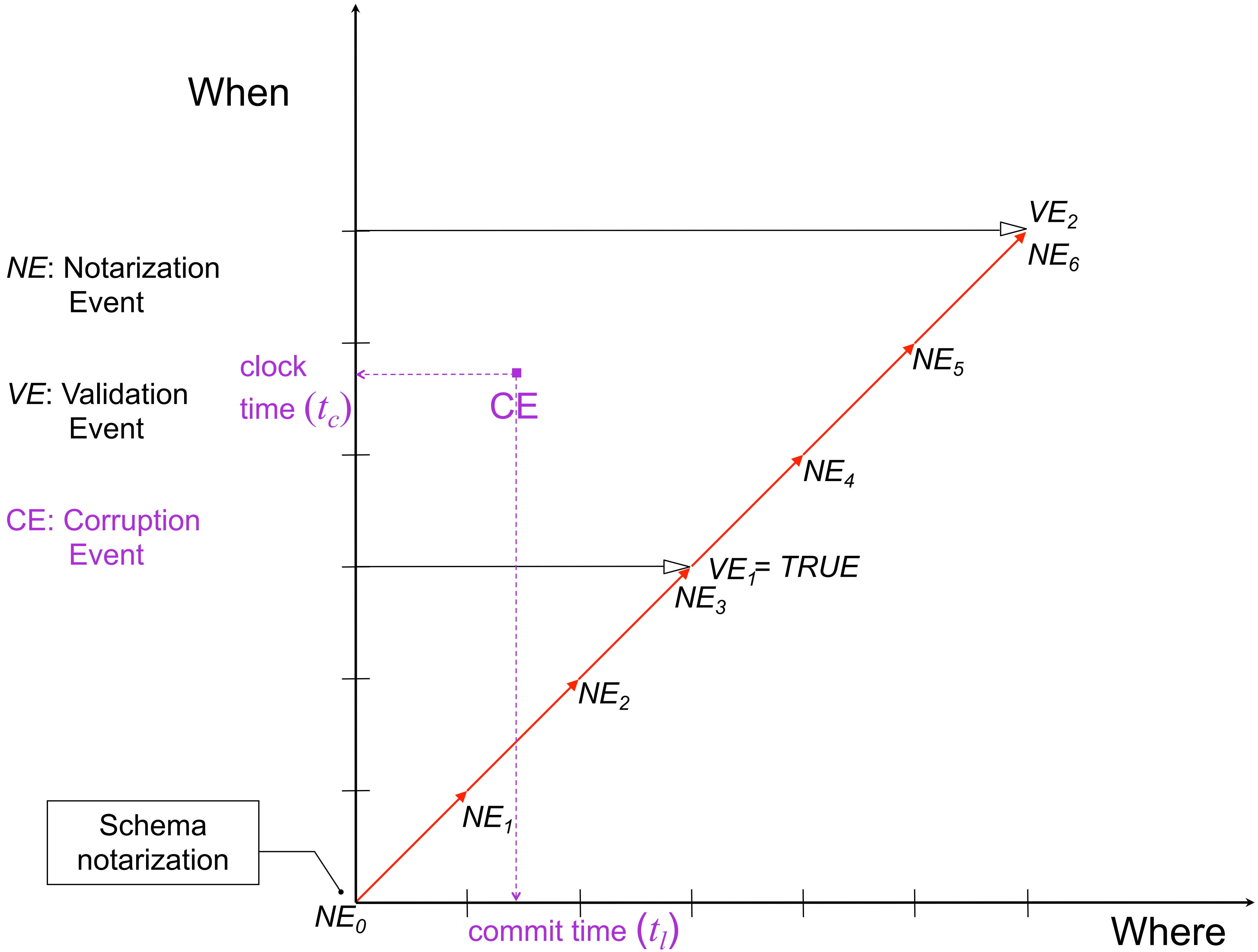
VE: Validation Event

CE: Corruption Event

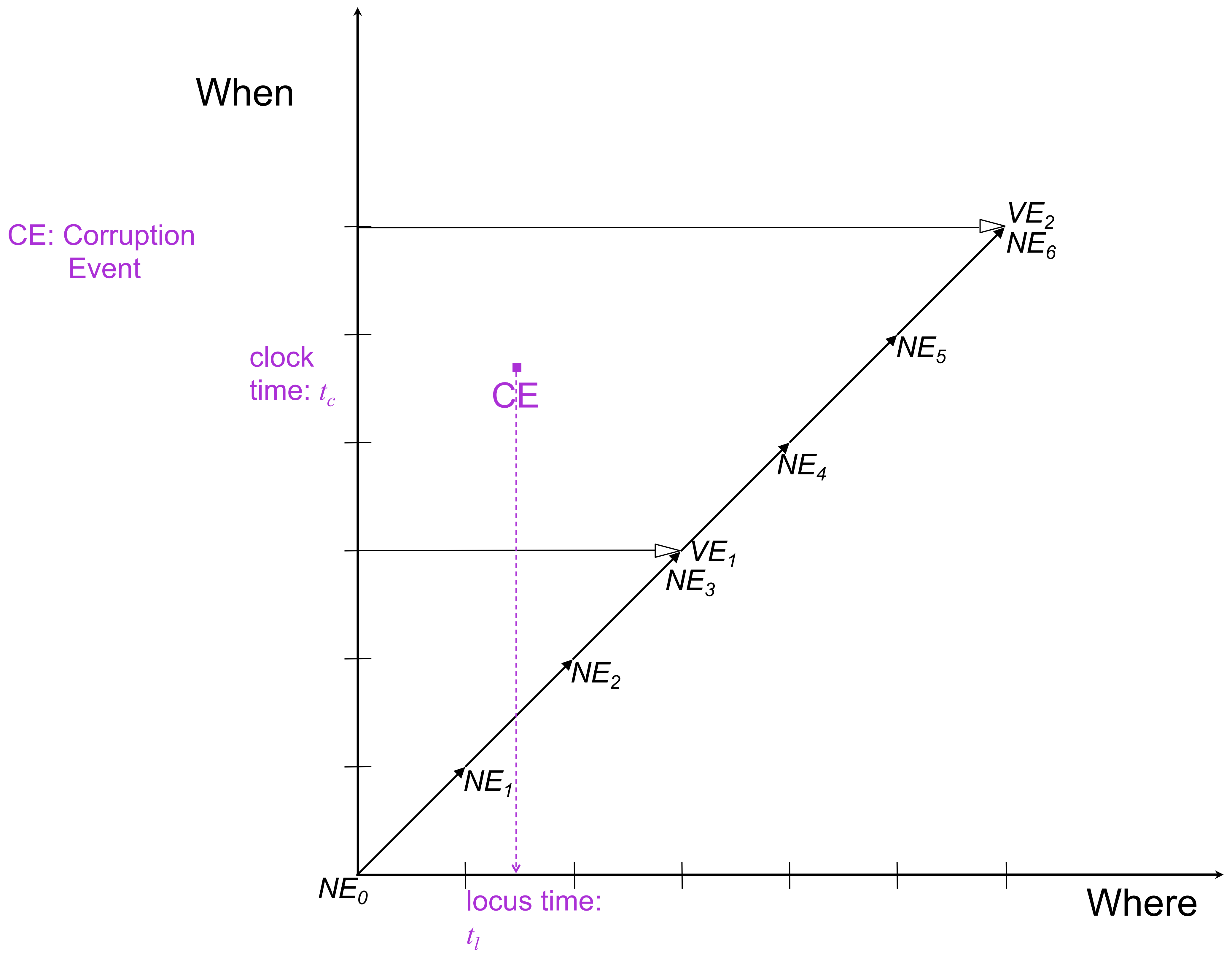
The Corruption Diagram



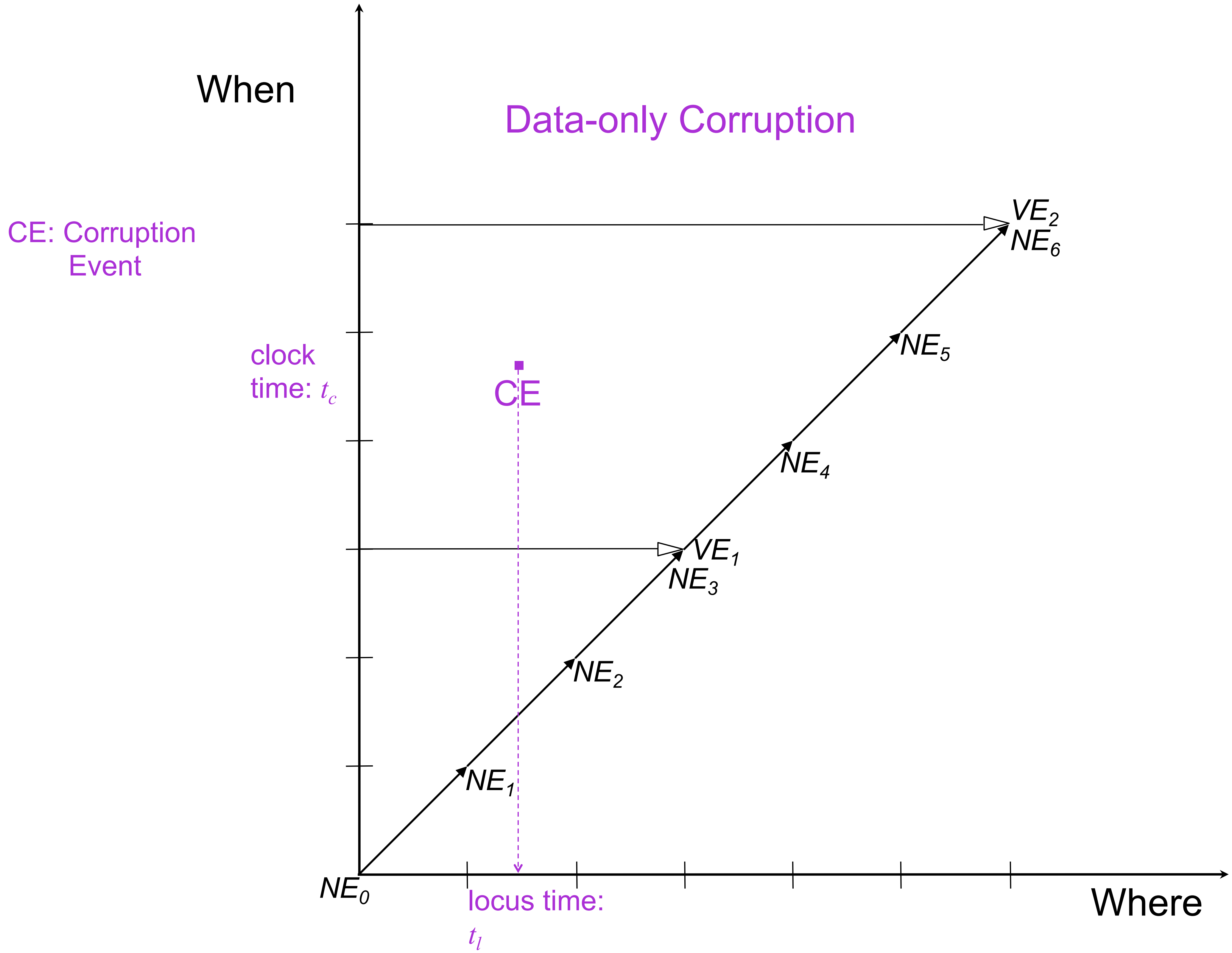
The Corruption Diagram



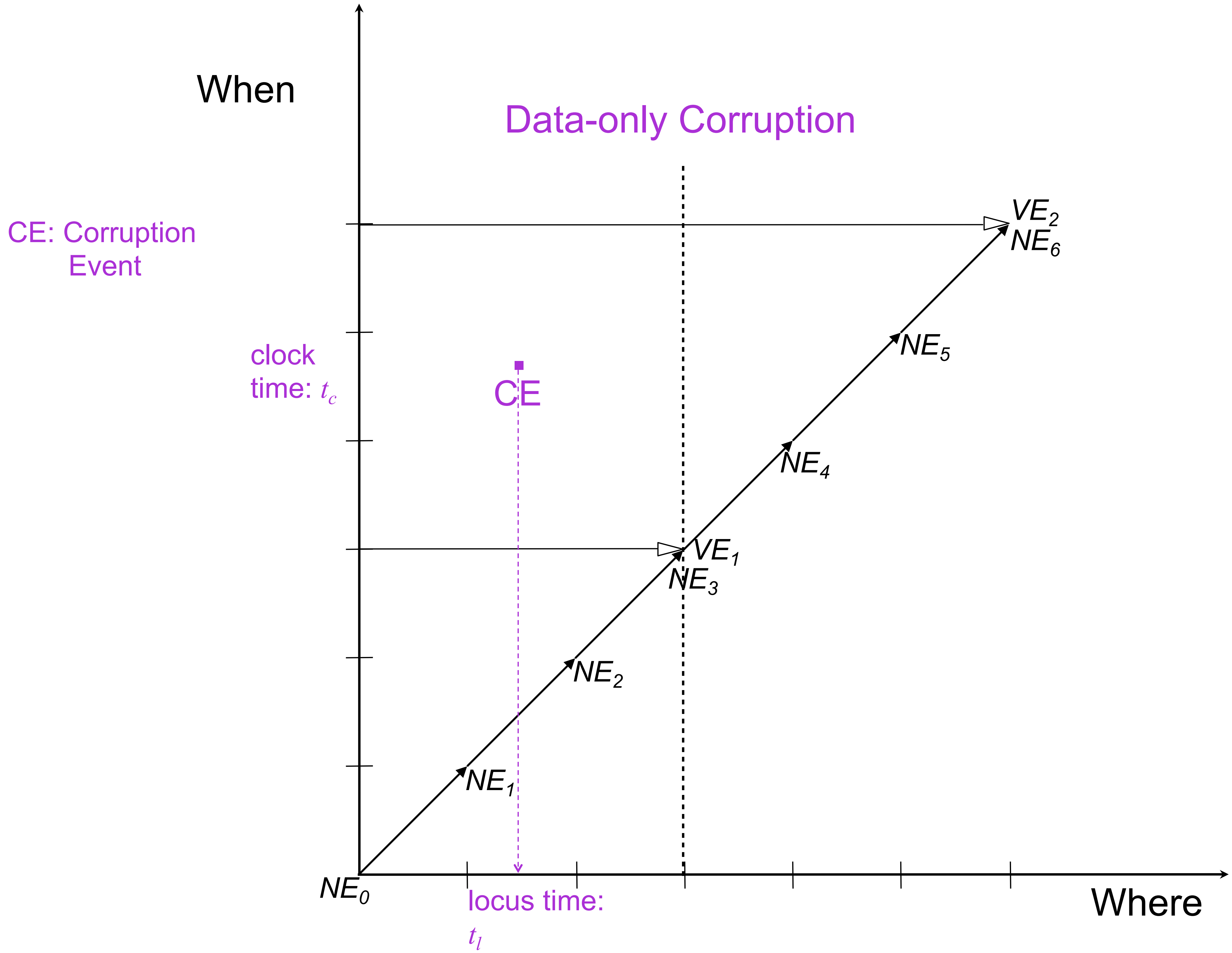
Types of Corruption Events



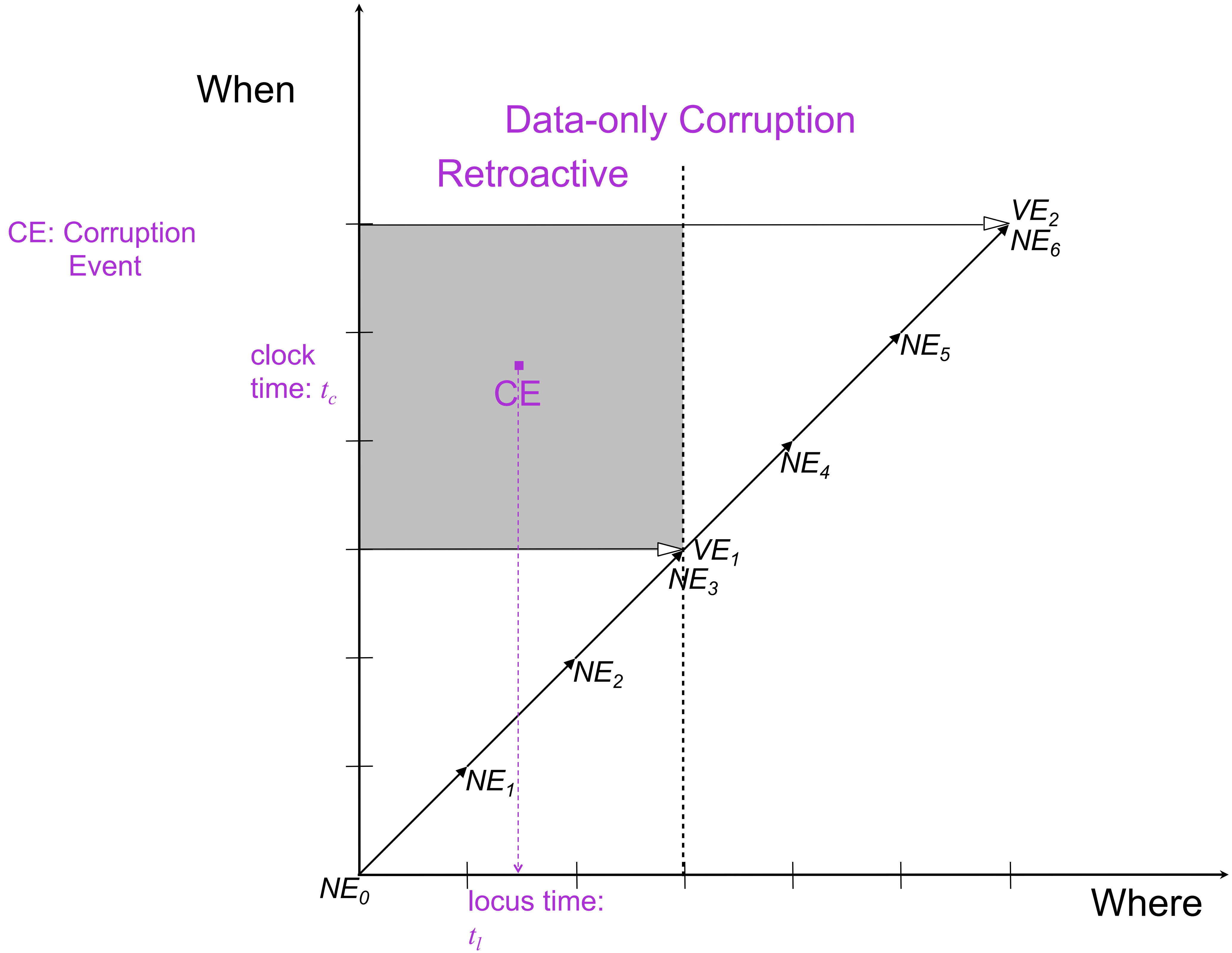
Types of Corruption Events



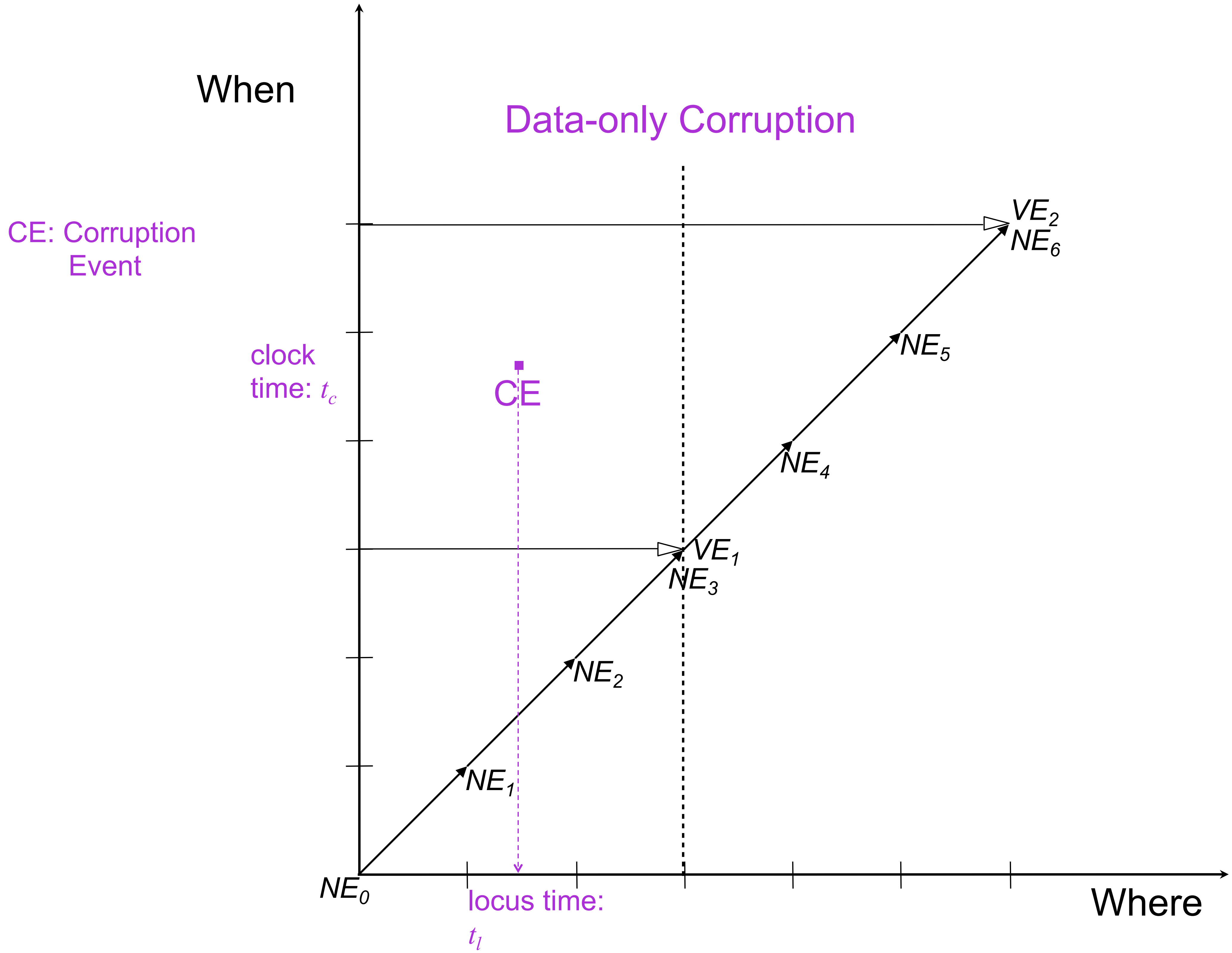
Types of Corruption Events



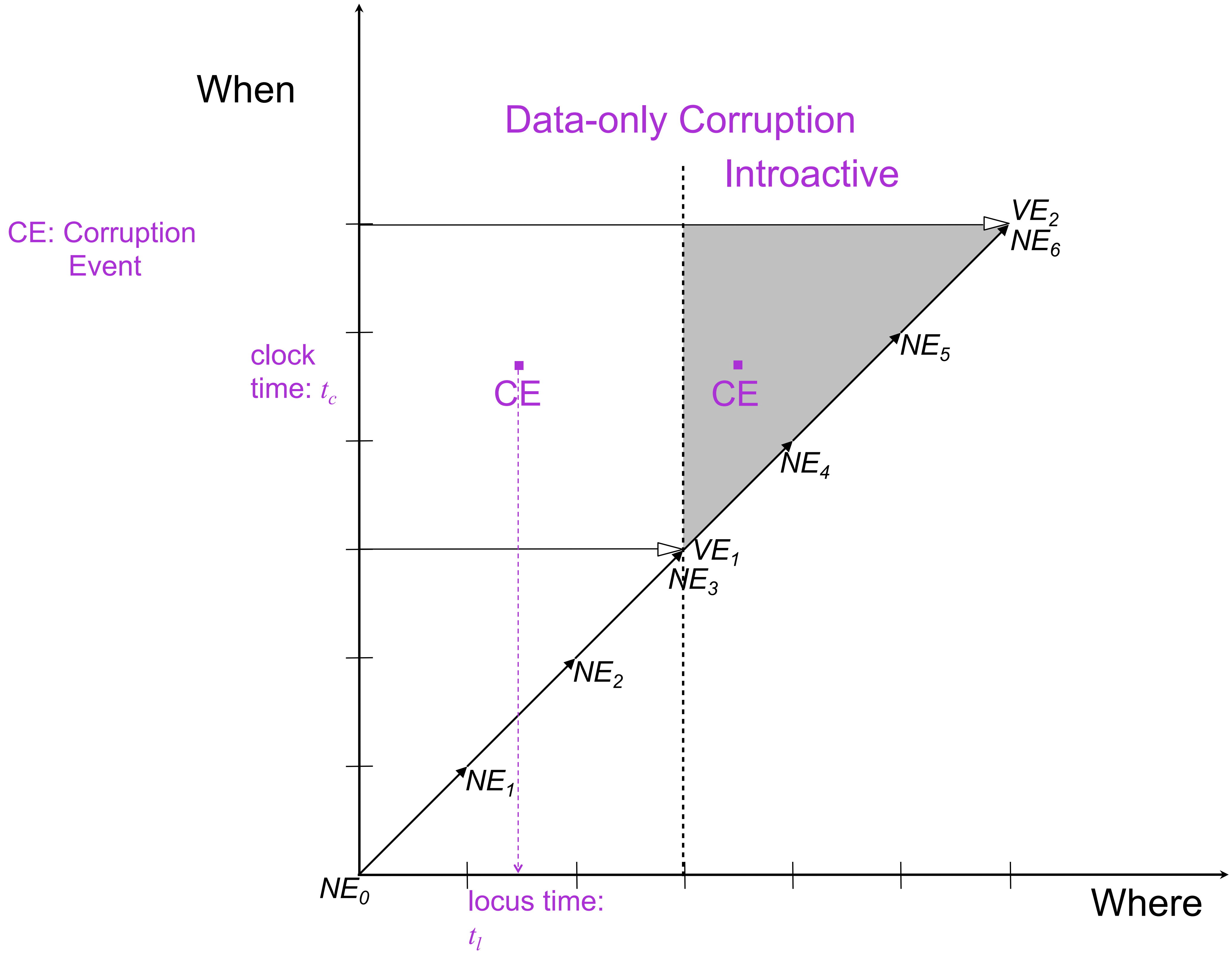
Types of Corruption Events



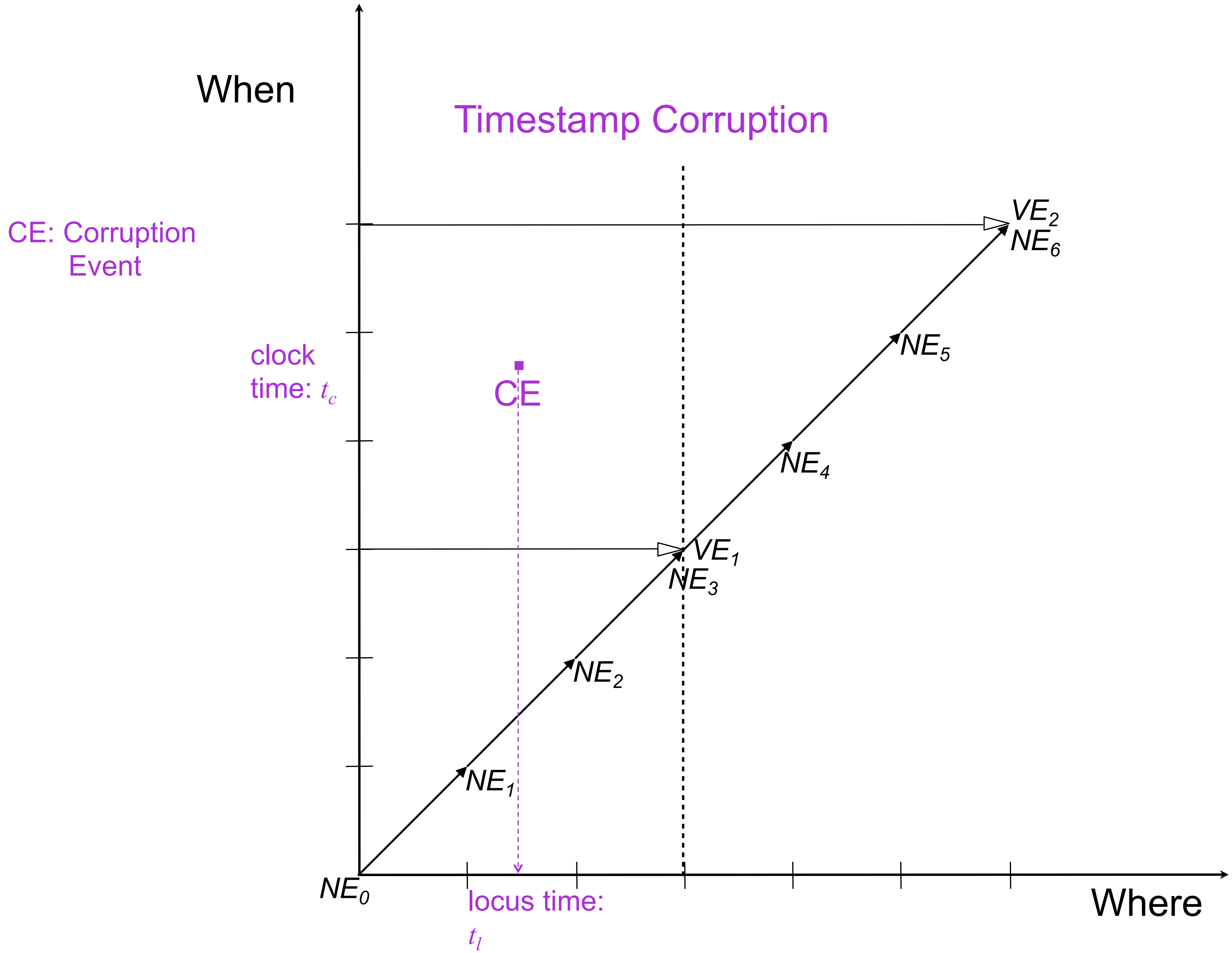
Types of Corruption Events



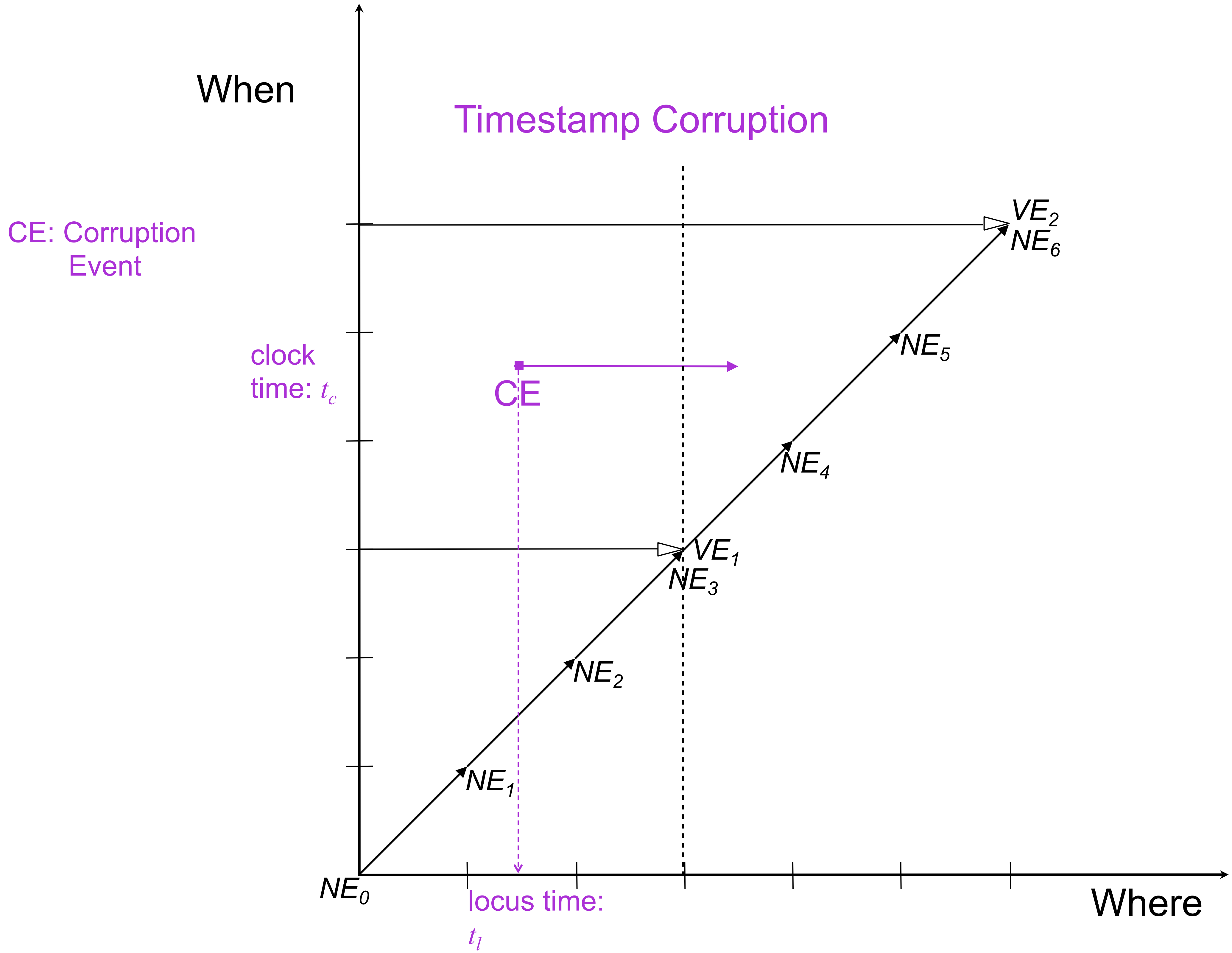
Types of Corruption Events



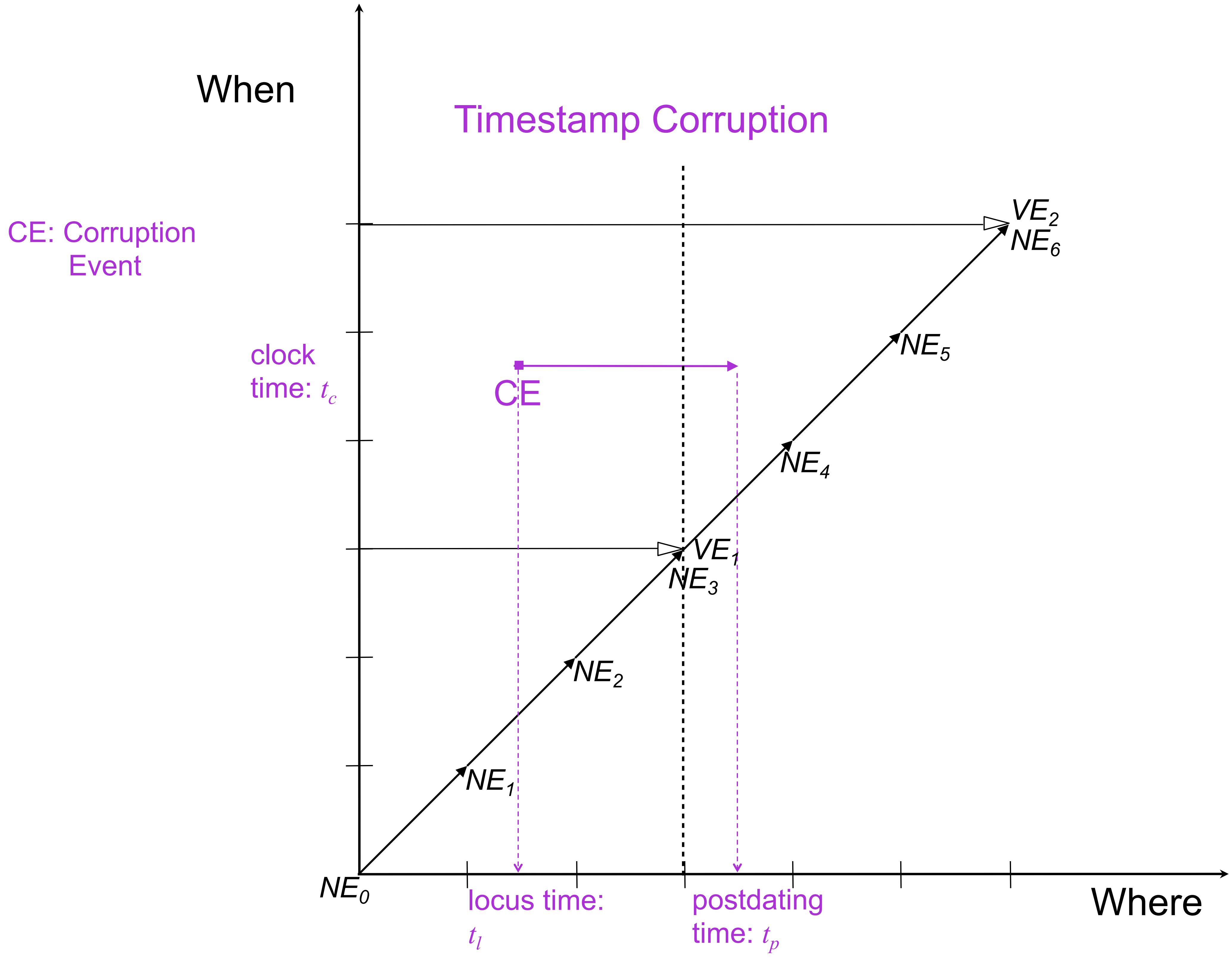
Types of Corruption Events



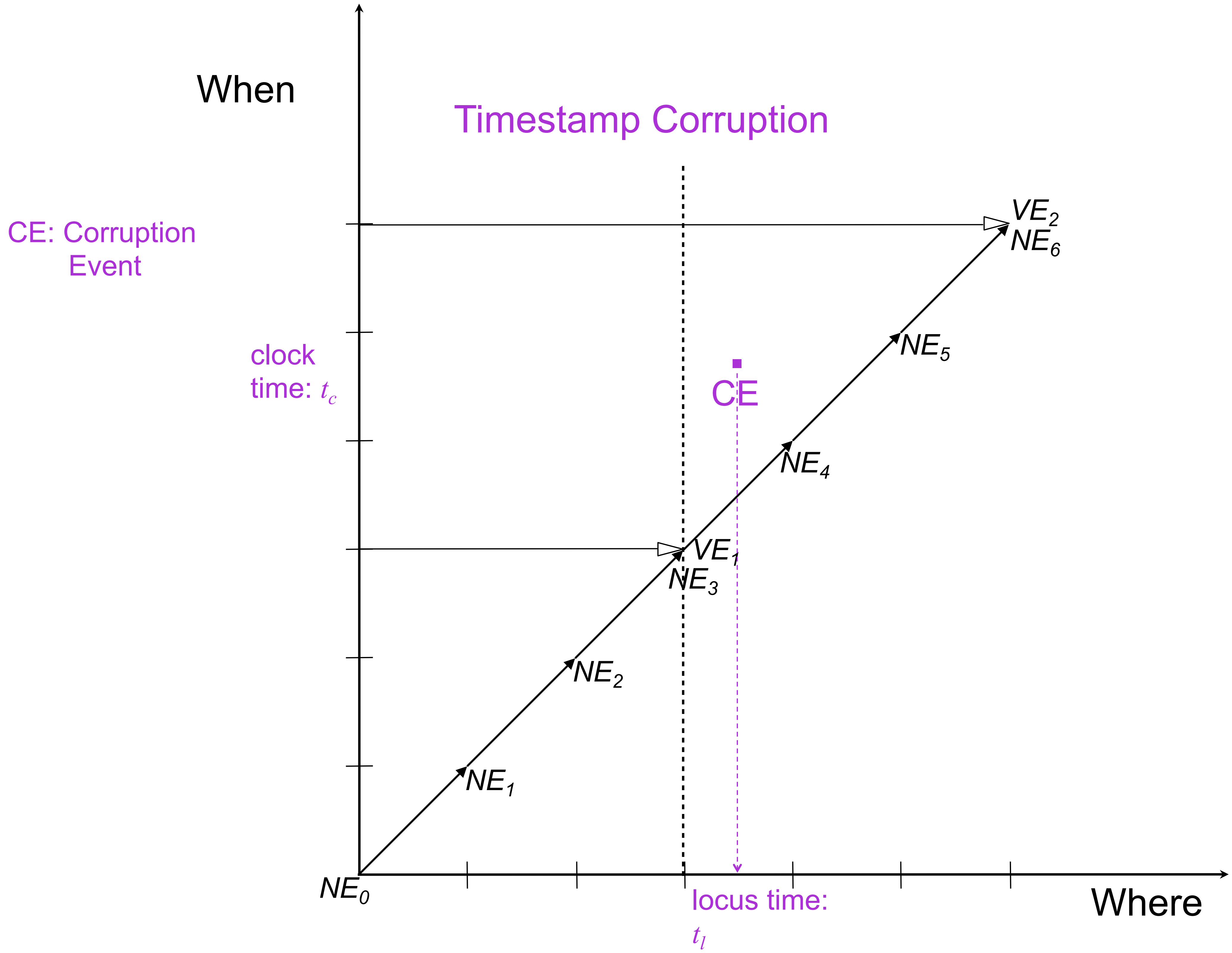
Types of Corruption Events



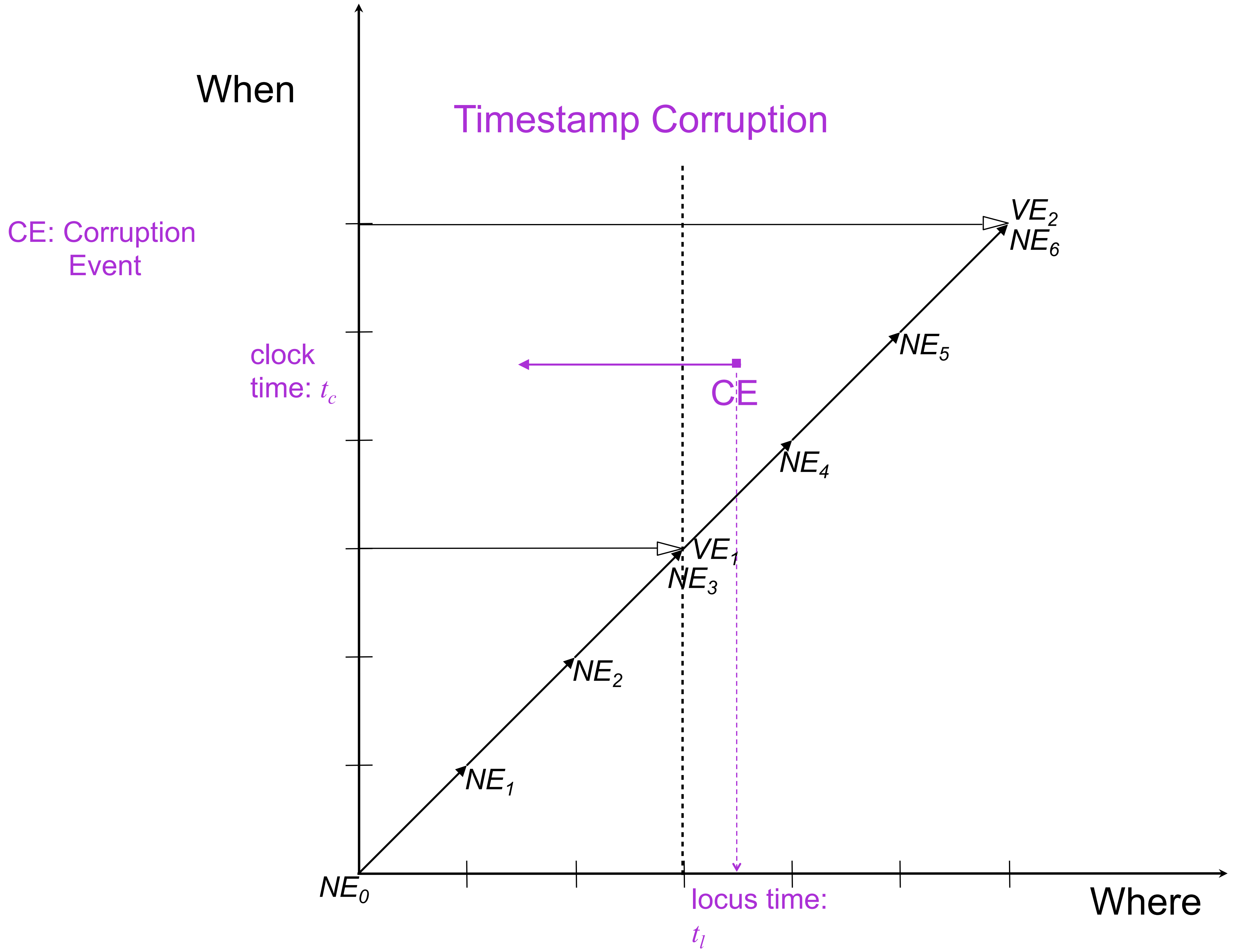
Types of Corruption Events



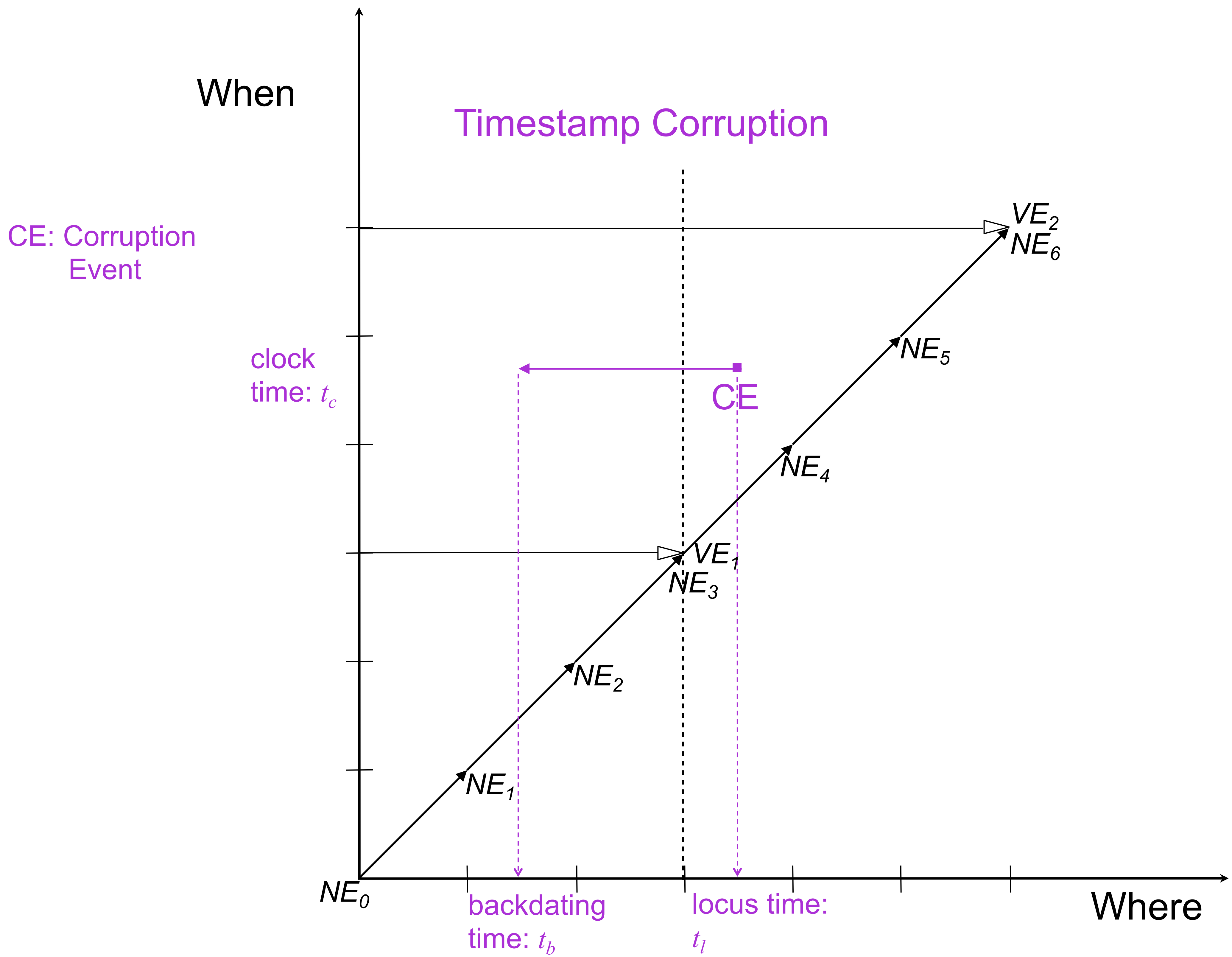
Types of Corruption Events



Types of Corruption Events



Types of Corruption Events



Forensic Analysis

Forensic Analysis

- If a corruption is detected, then the forensic analysis phase begins.

Forensic Analysis

- If a corruption is detected, then the forensic analysis phase begins.
- A *forensic analysis algorithm* is run as directed by the Database Administrator.

Forensic Analysis

- If a corruption is detected, then the forensic analysis phase begins.

- A *forensic analysis algorithm* is run as directed by the Database Administrator.

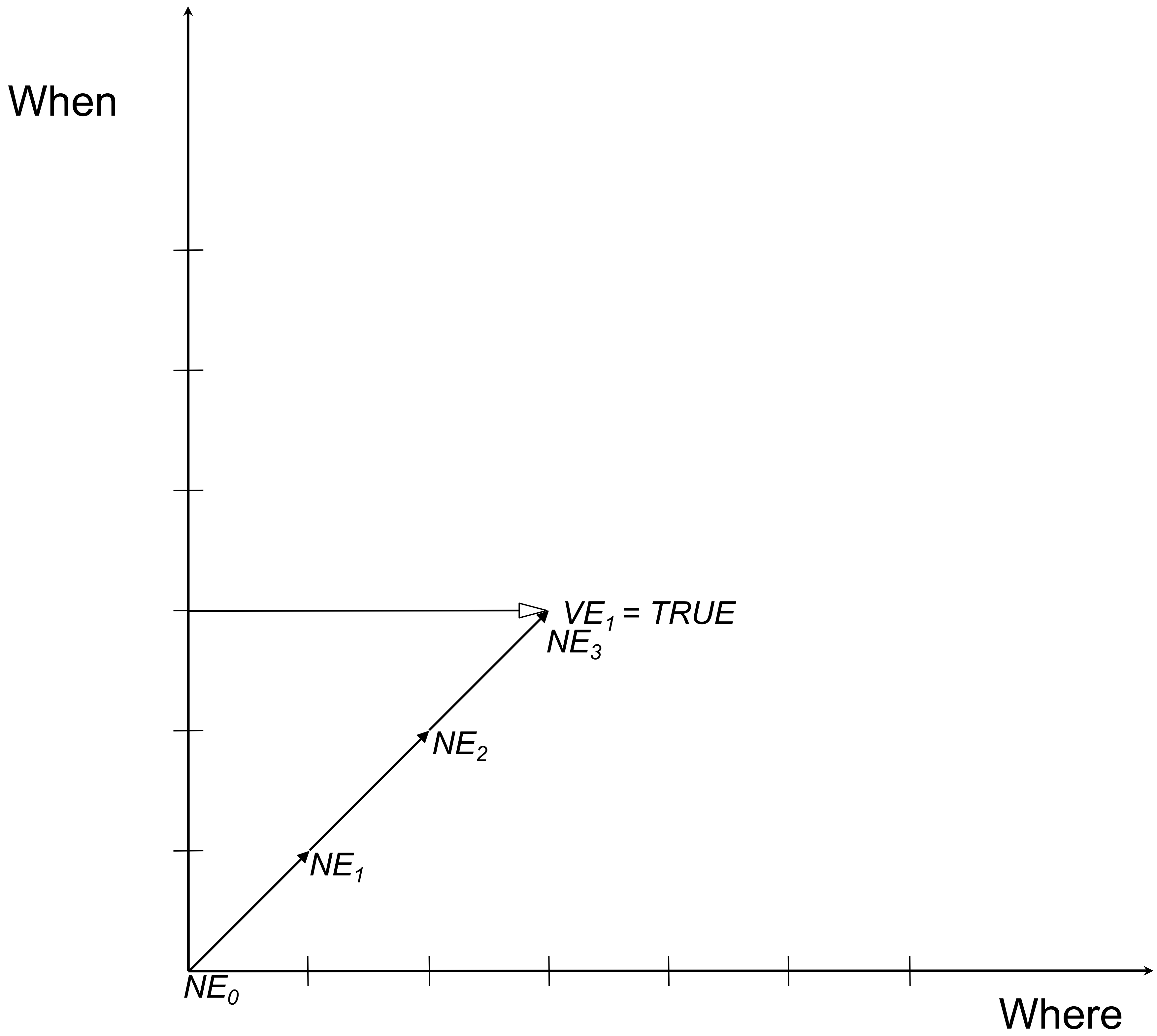
- Attempt to ascertain a *corruption region*: the bounds on the uncertainty of the “where” and “when” of the corruption.

Detection Resolution

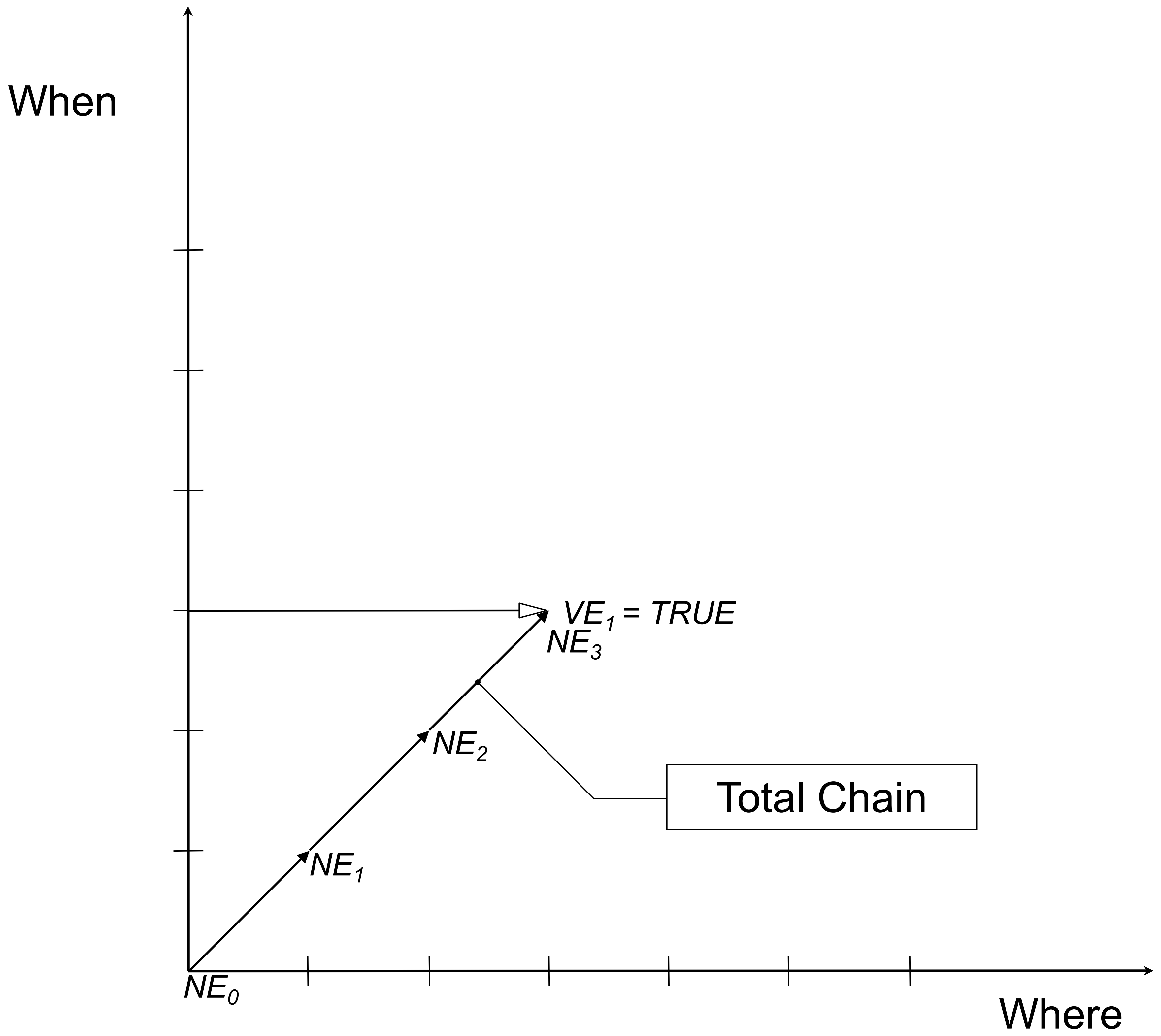
- Temporal Detection Resolution (R_t): the finest granularity of temporal bounds uncertainty of a CE.

- Spatial Detection Resolution (R_s): the finest granularity of spatial bounds uncertainty of a CE.

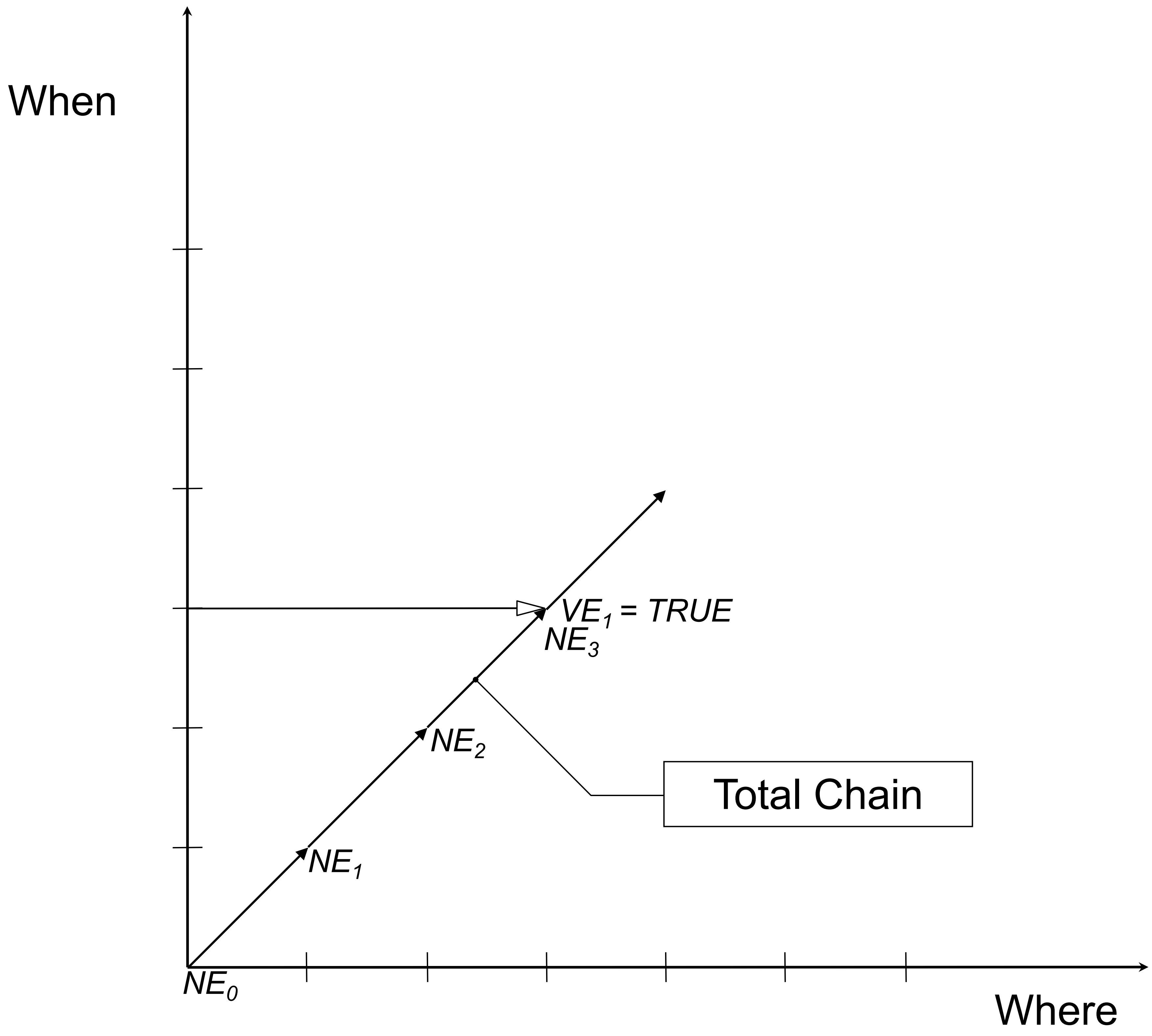
Monochromatic Algorithm



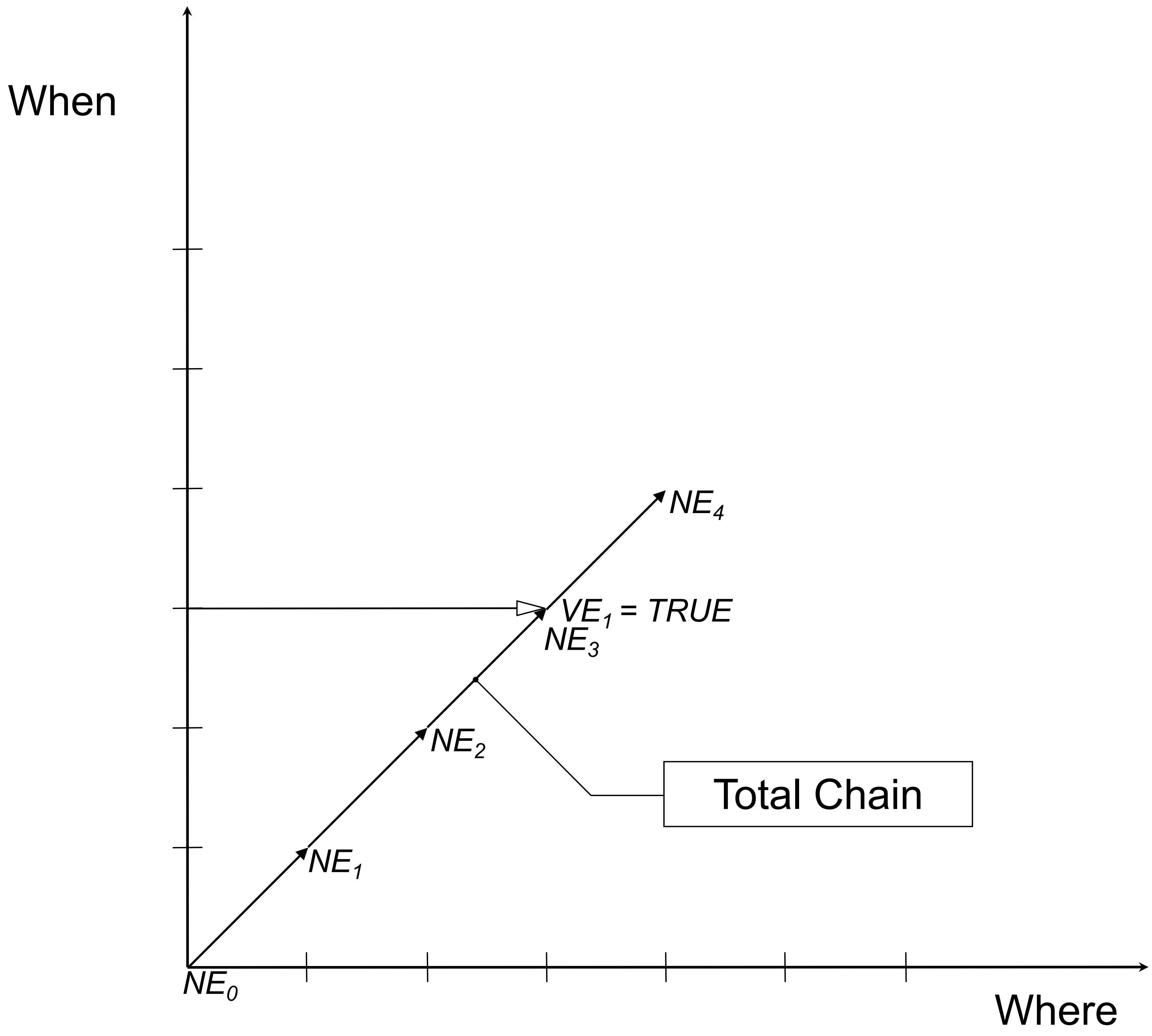
Monochromatic Algorithm



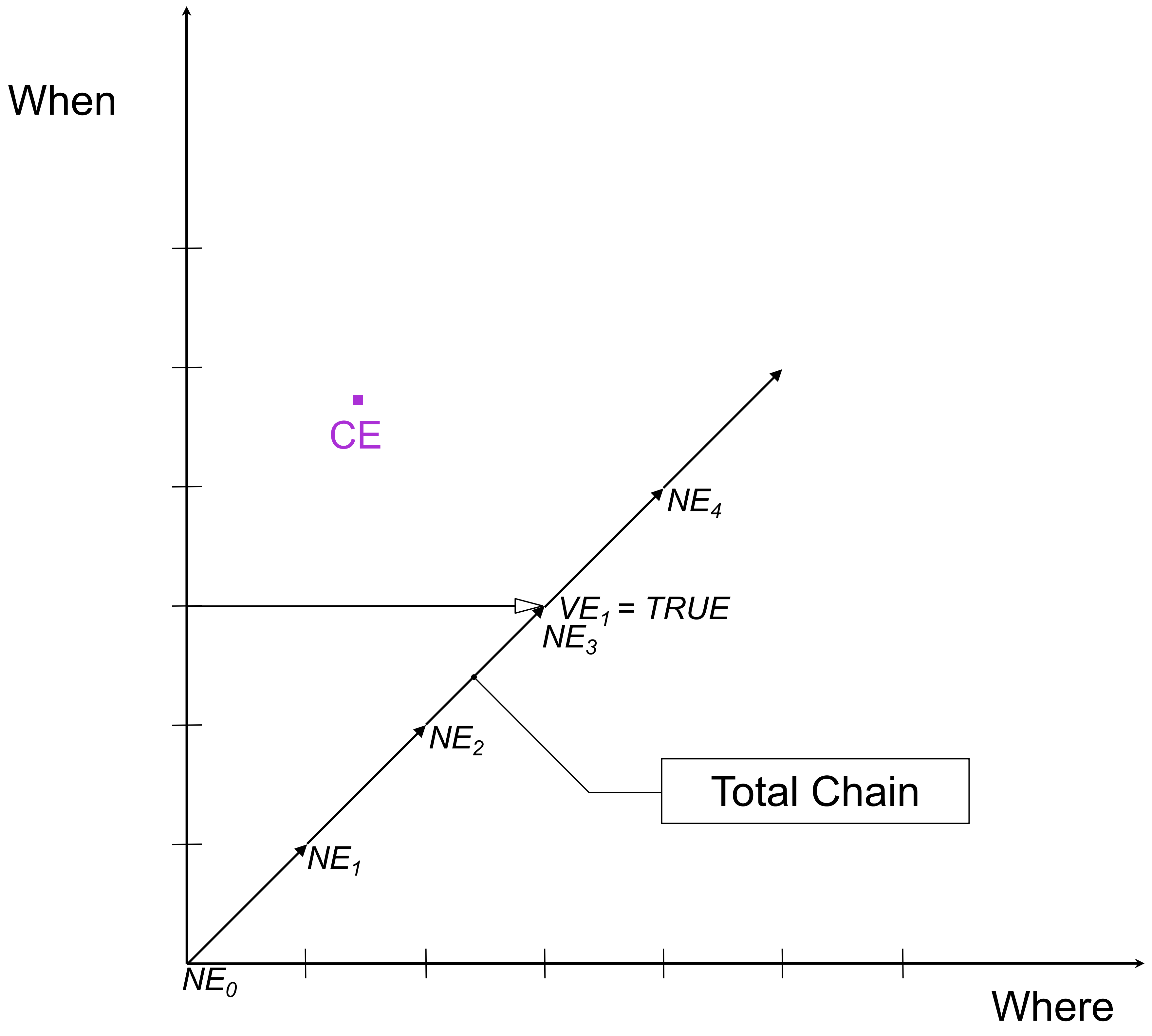
Monochromatic Algorithm



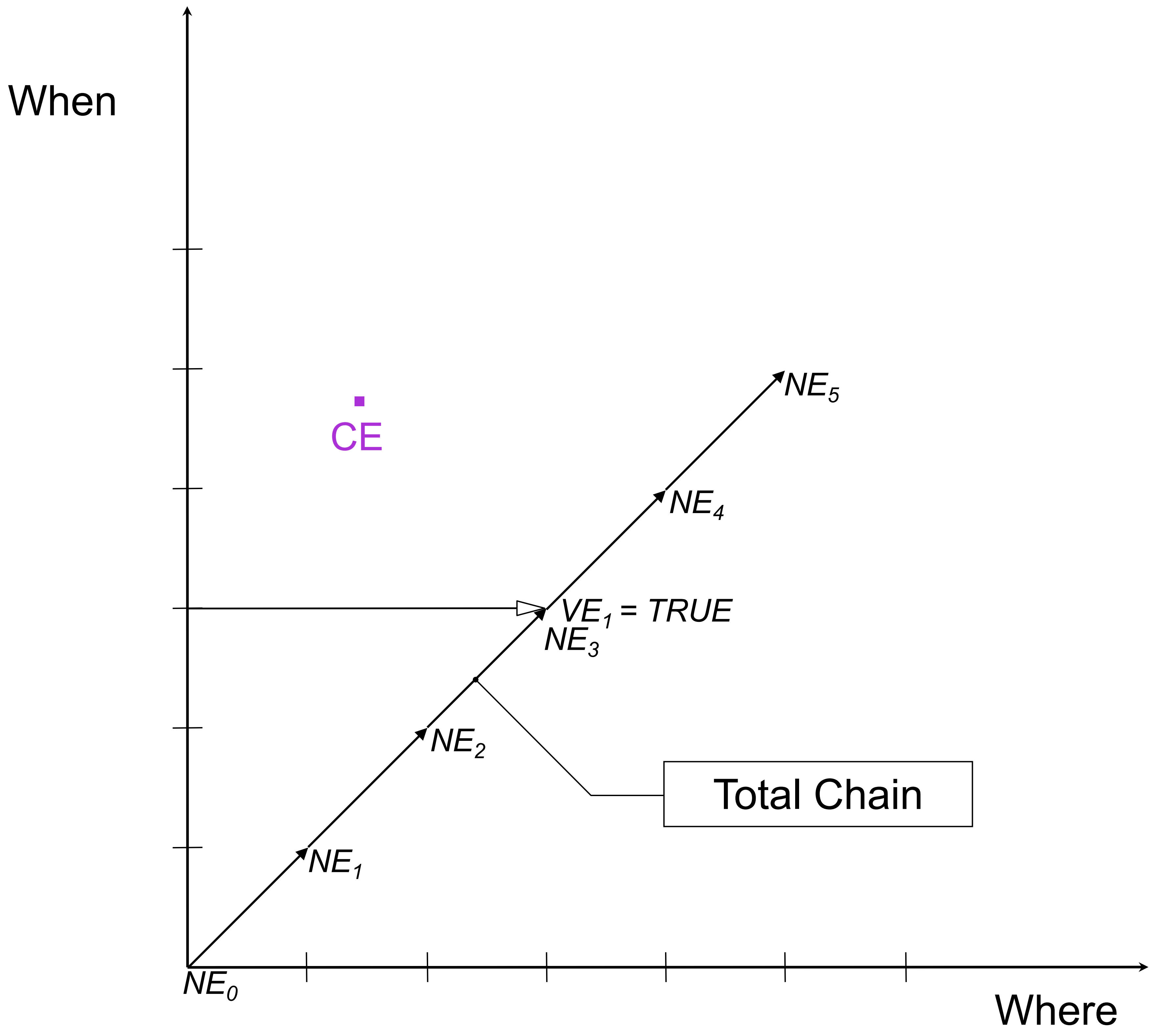
Monochromatic Algorithm



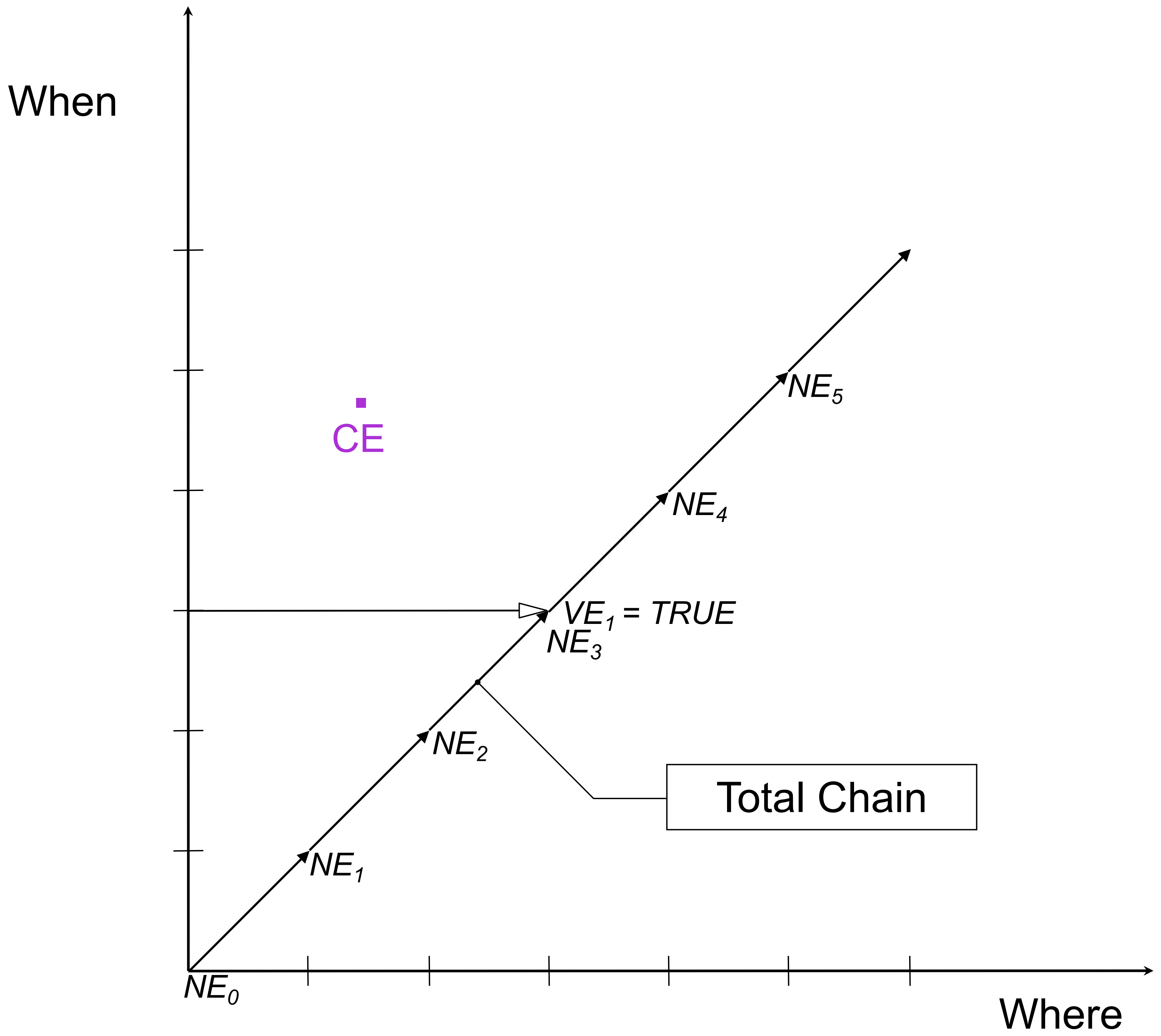
Monochromatic Algorithm



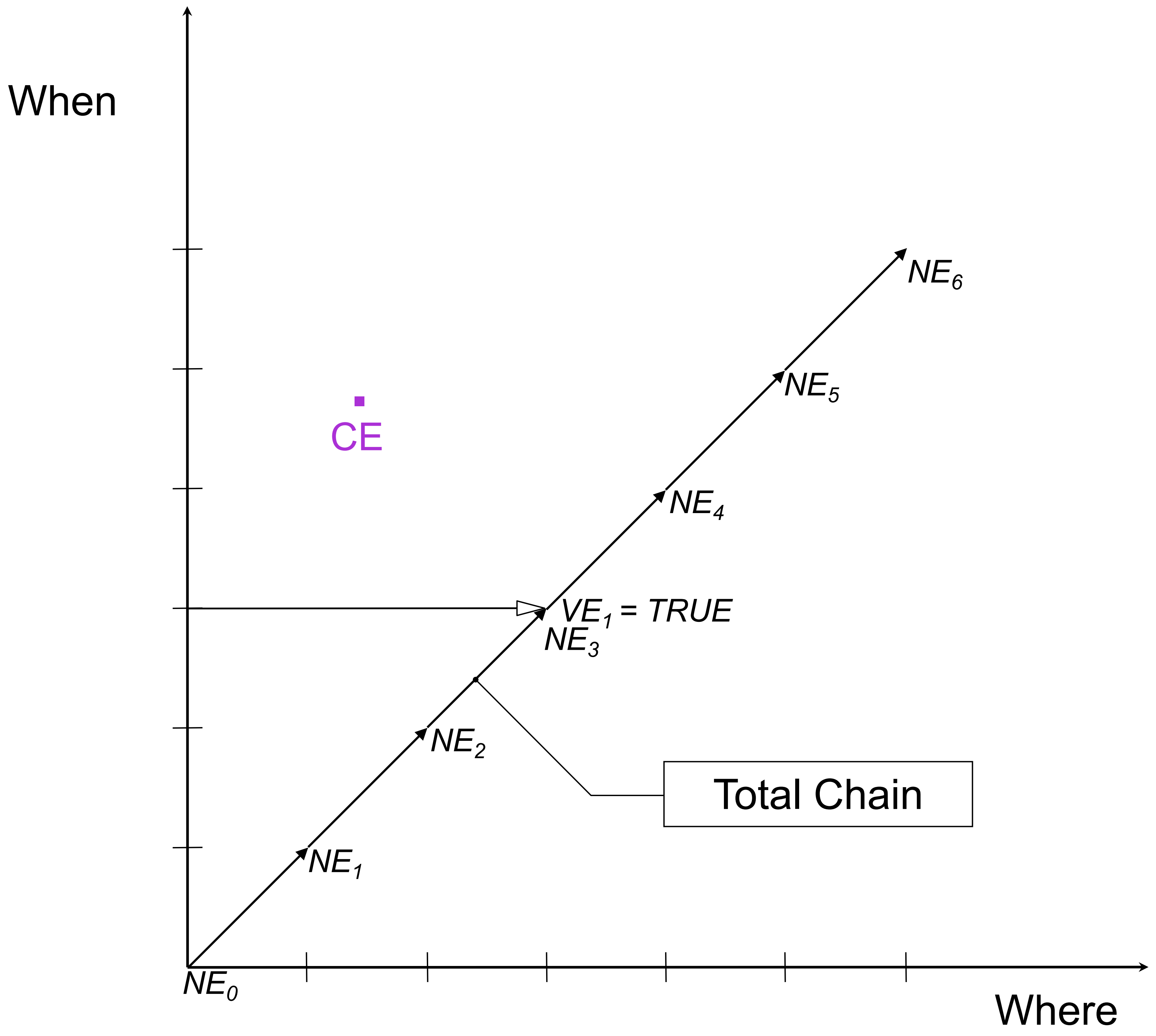
Monochromatic Algorithm



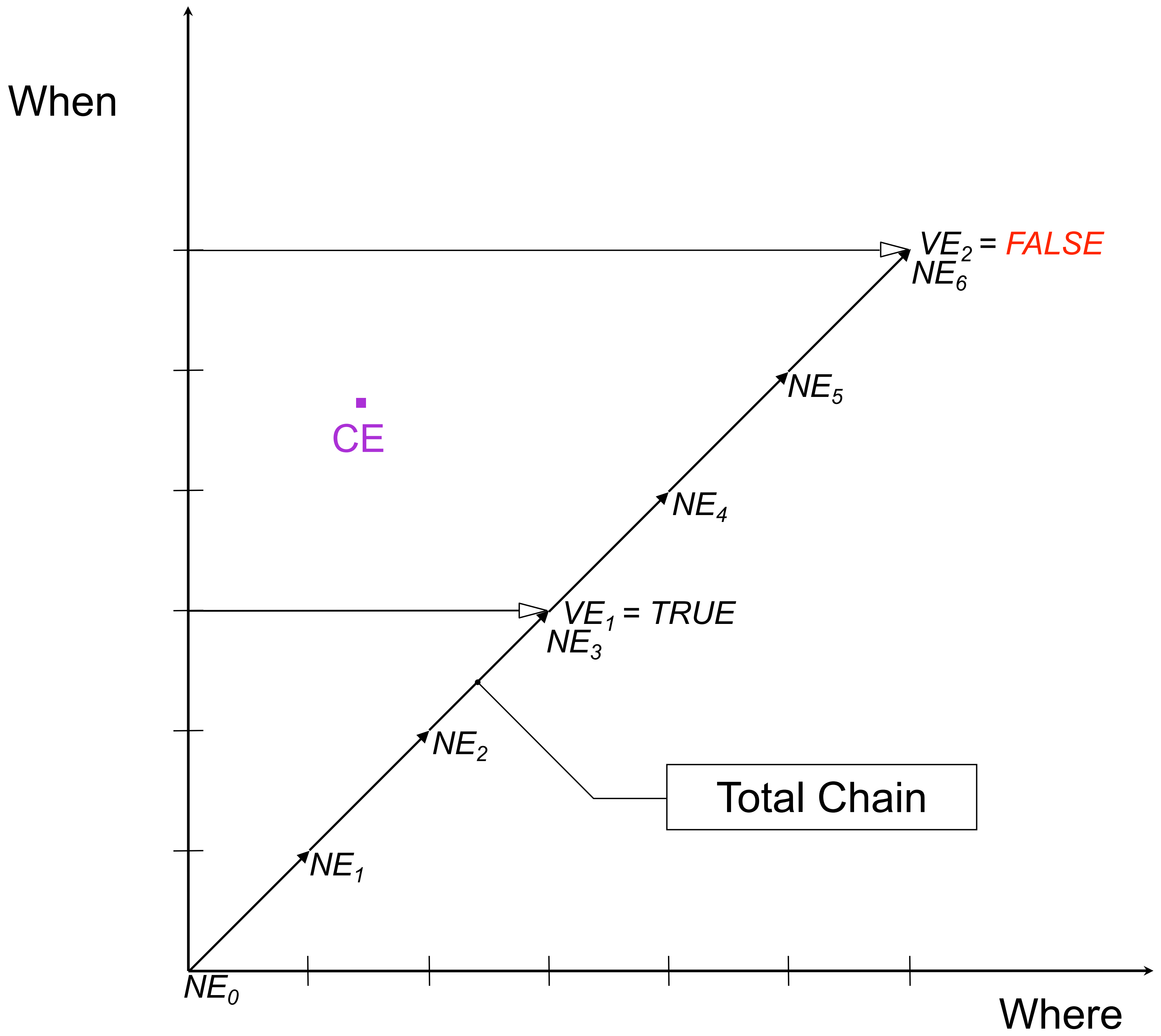
Monochromatic Algorithm



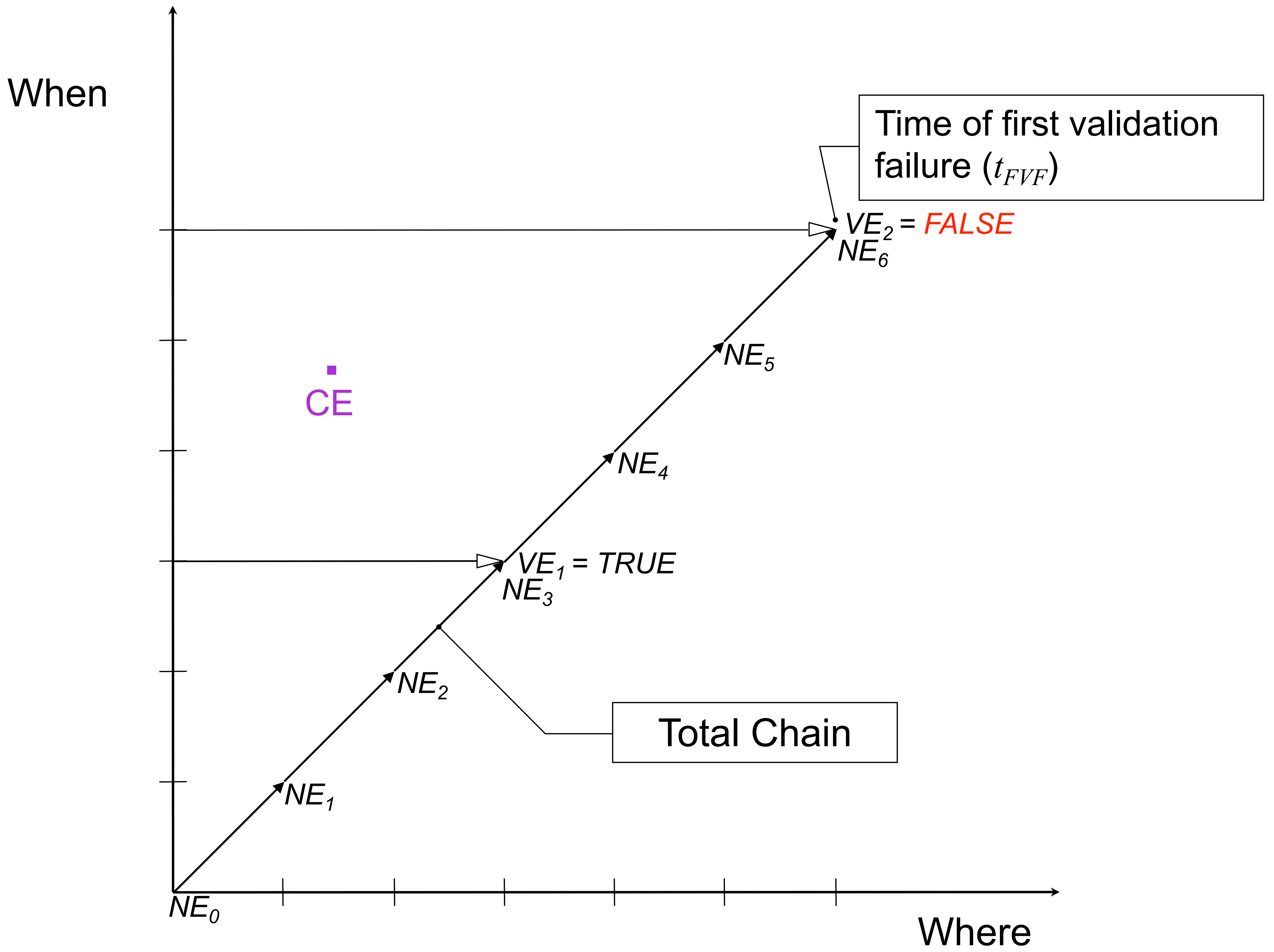
Monochromatic Algorithm



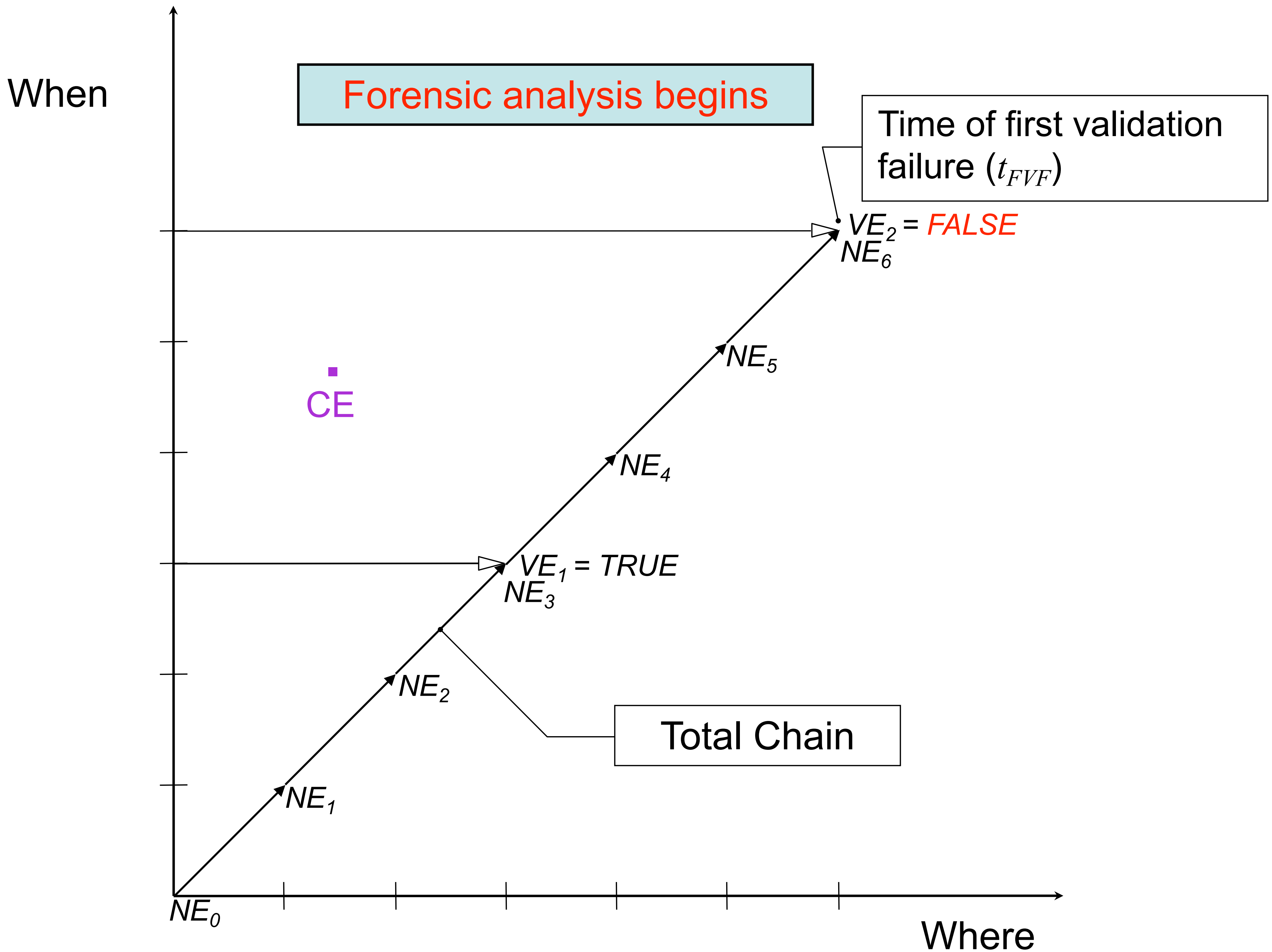
Monochromatic Algorithm



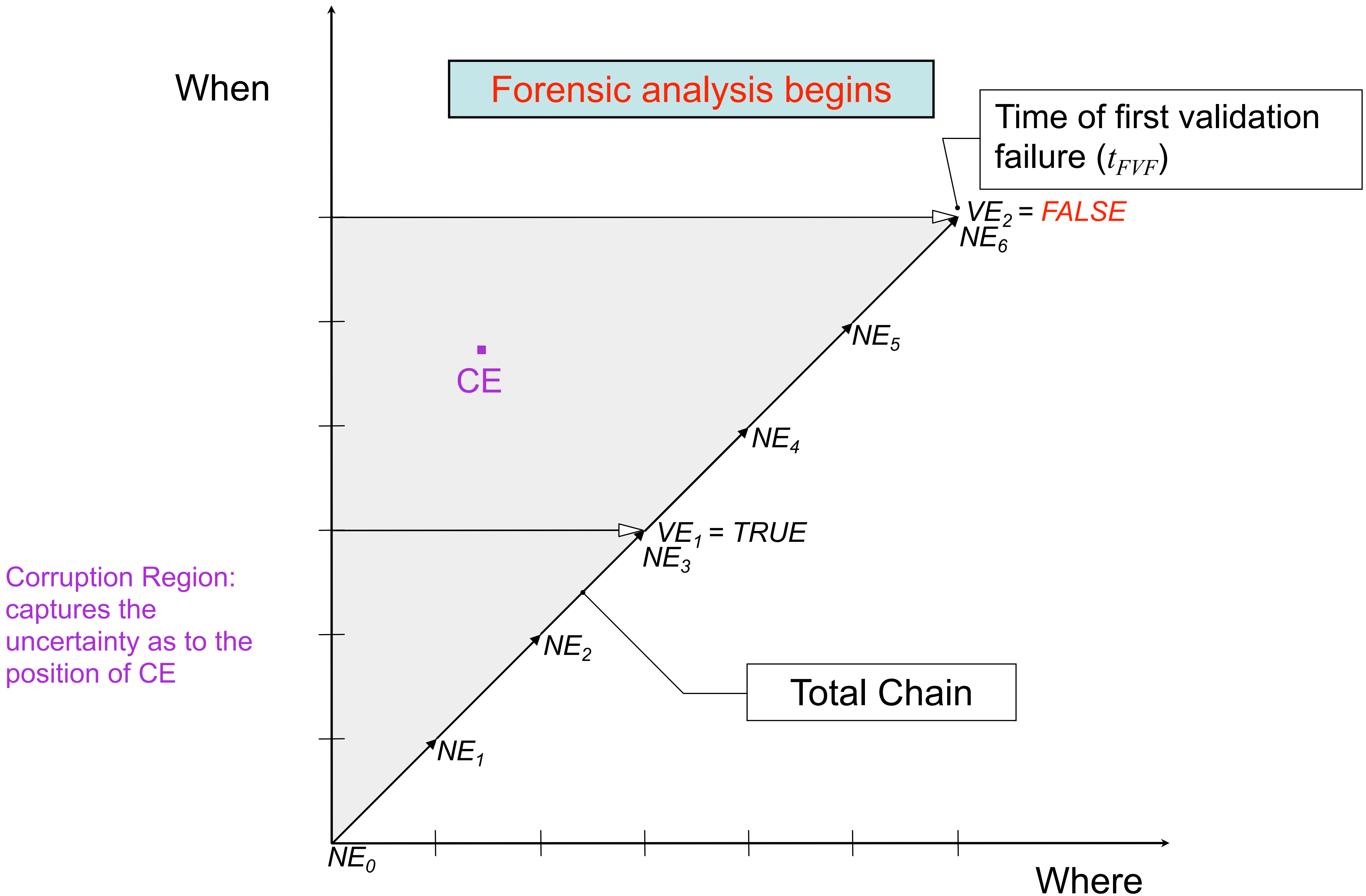
Monochromatic Algorithm



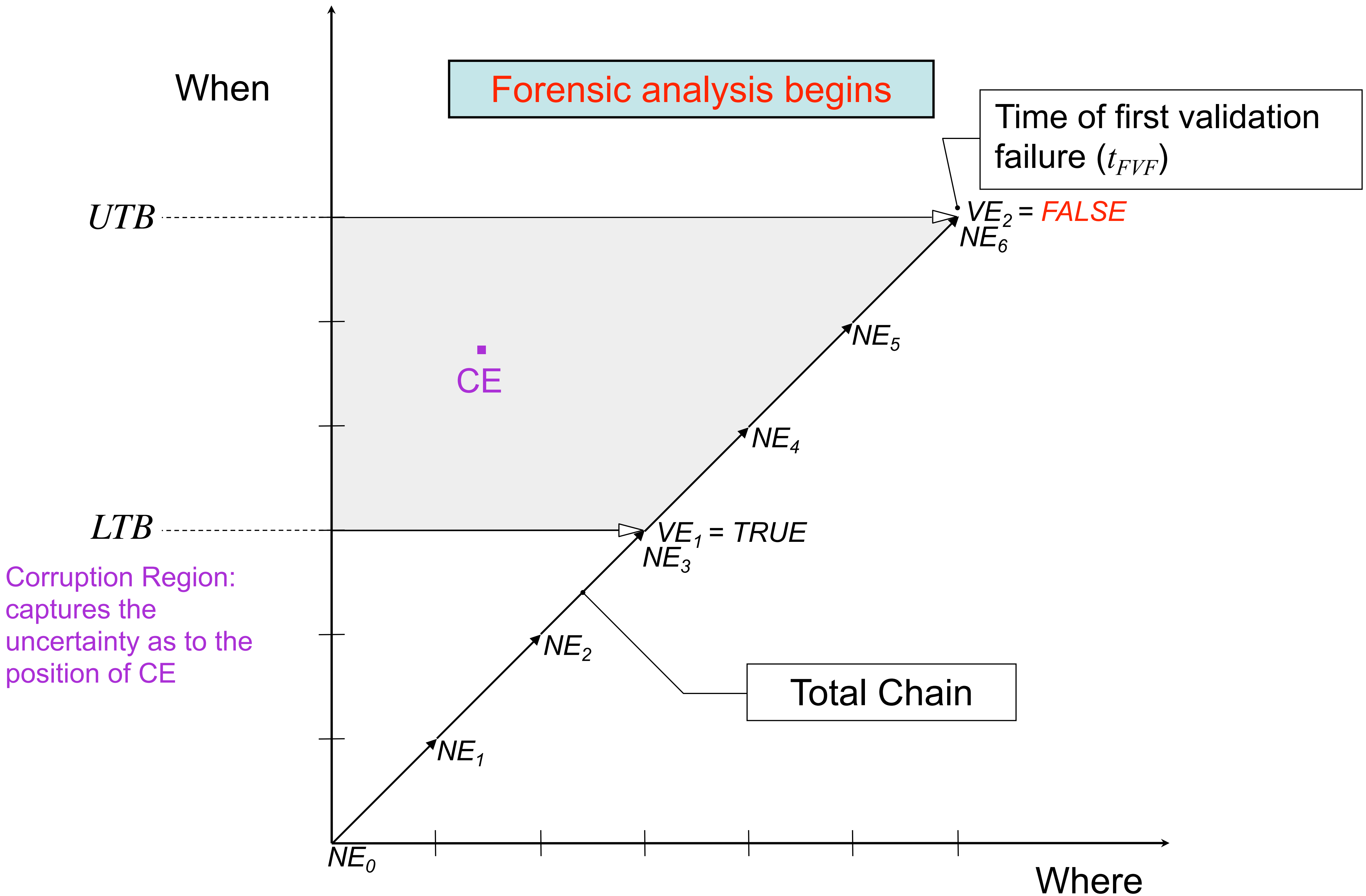
Monochromatic Algorithm



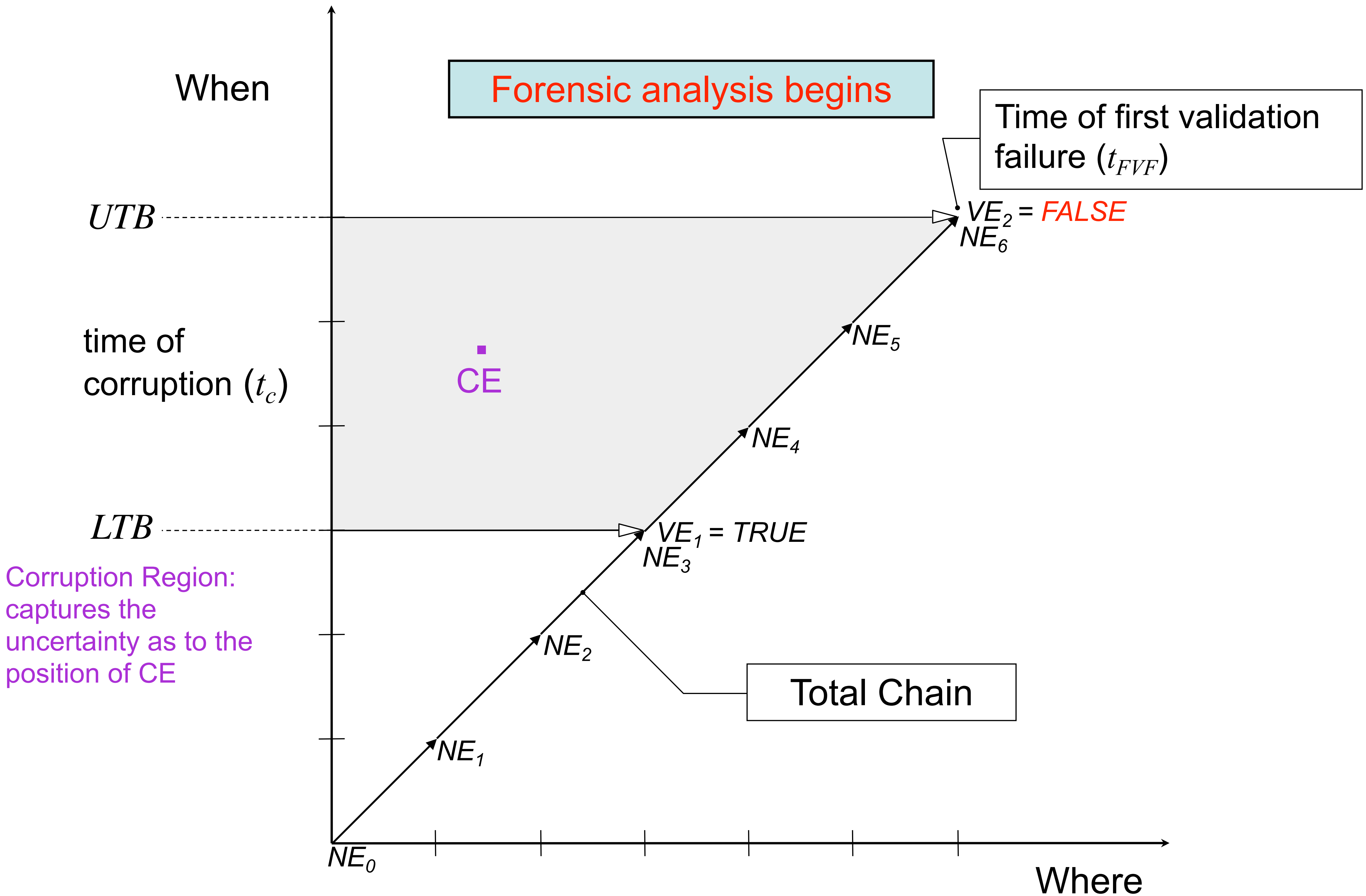
Monochromatic Algorithm



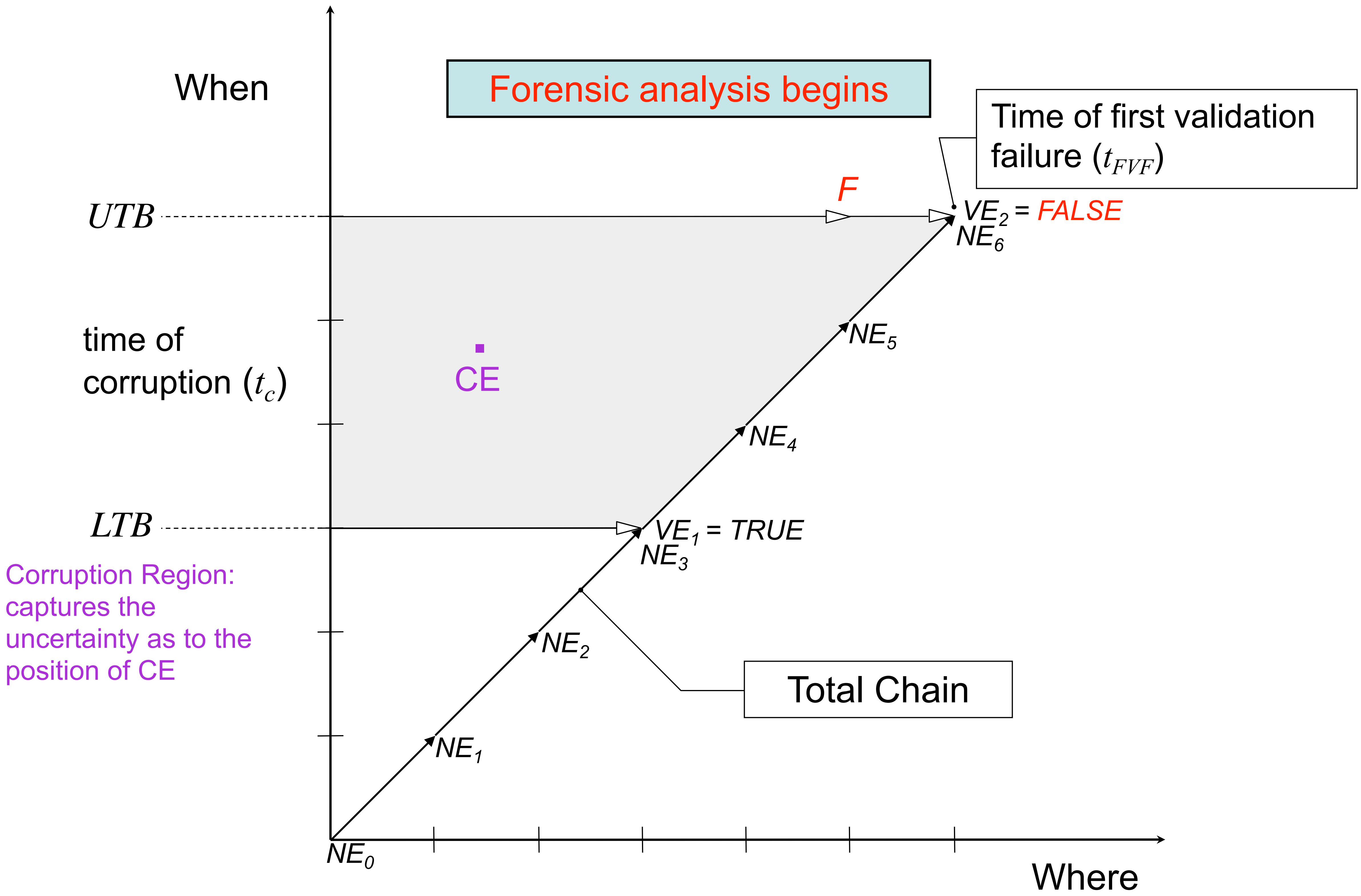
Monochromatic Algorithm



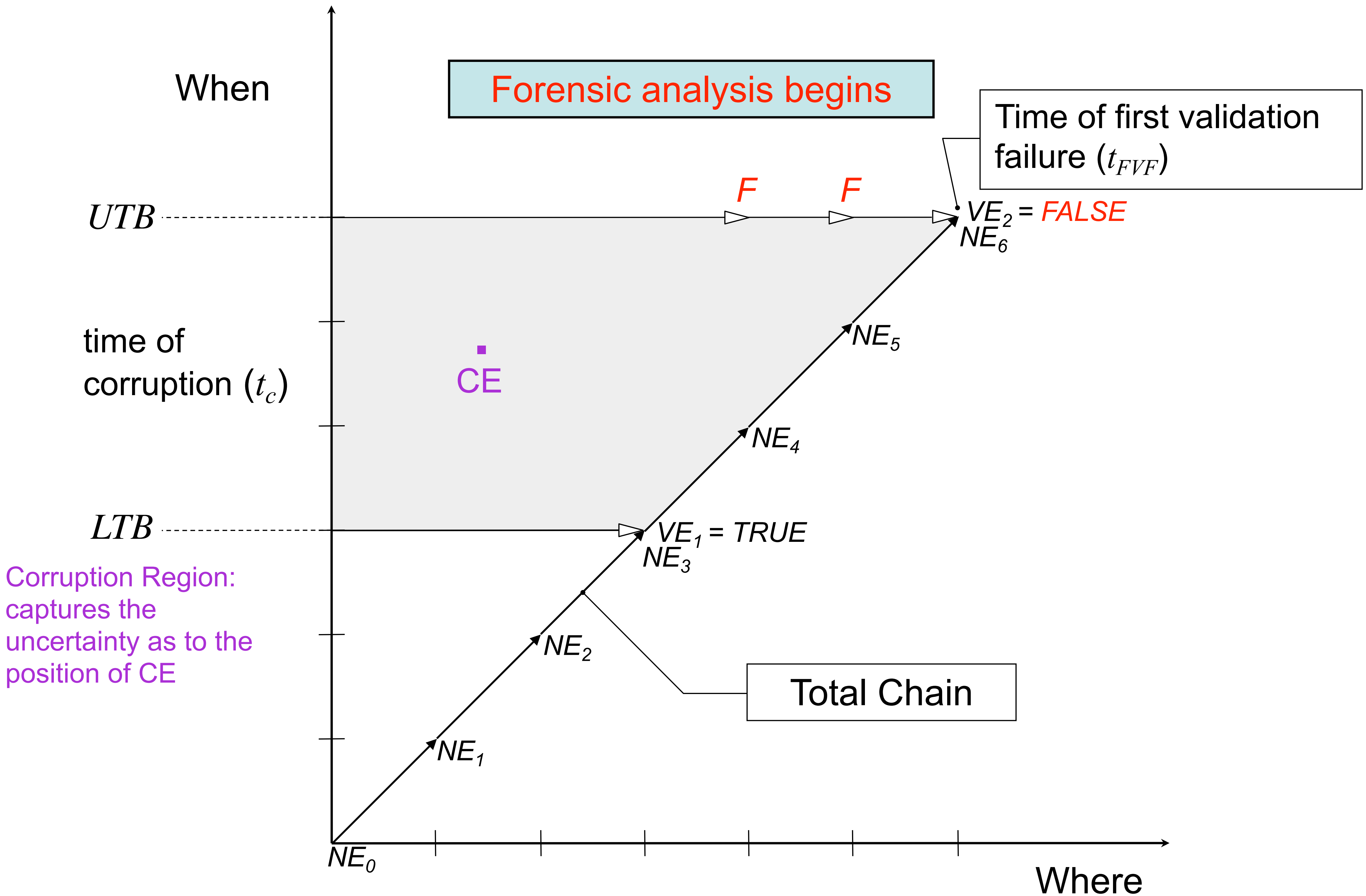
Monochromatic Algorithm



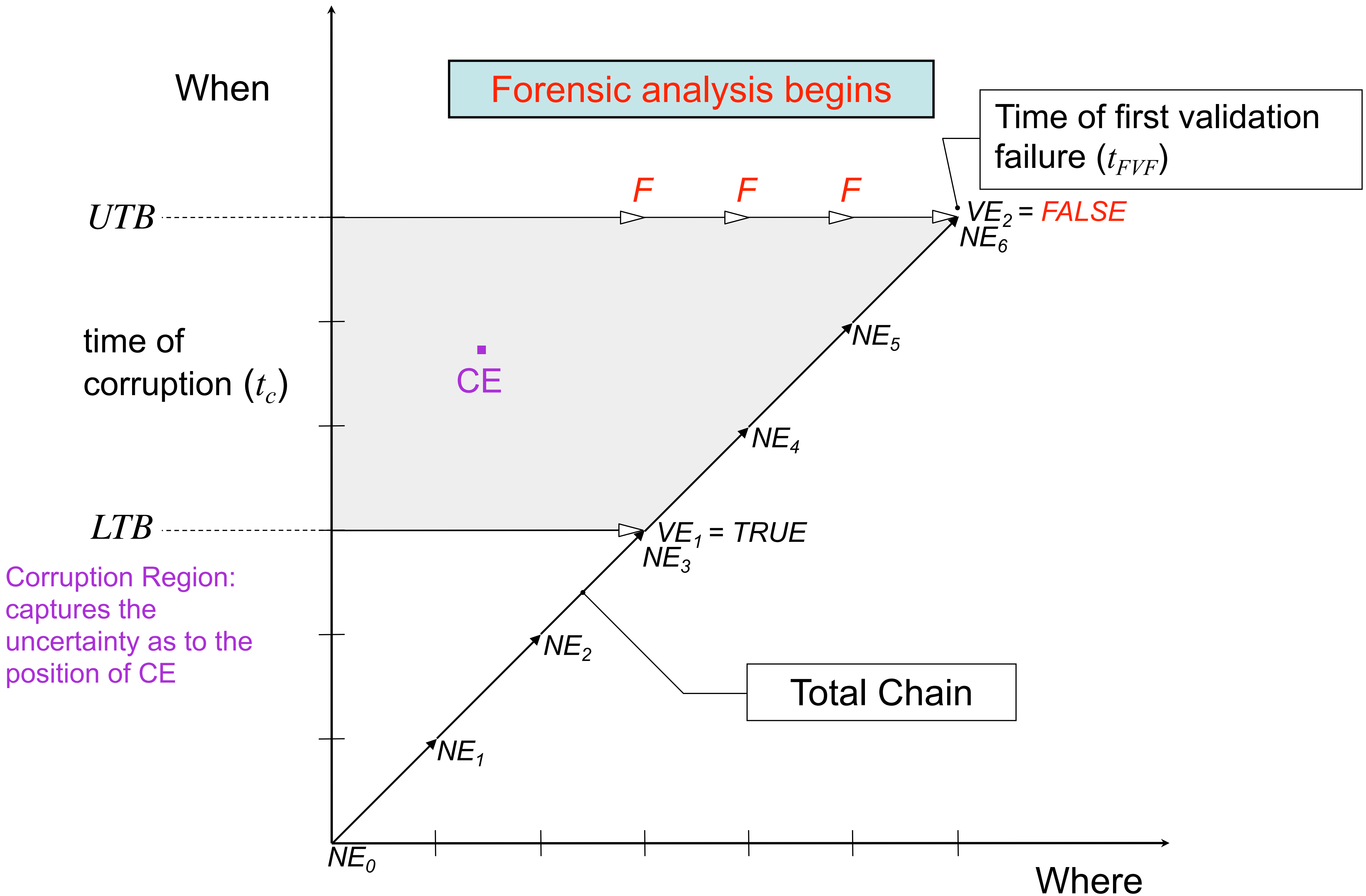
Monochromatic Algorithm



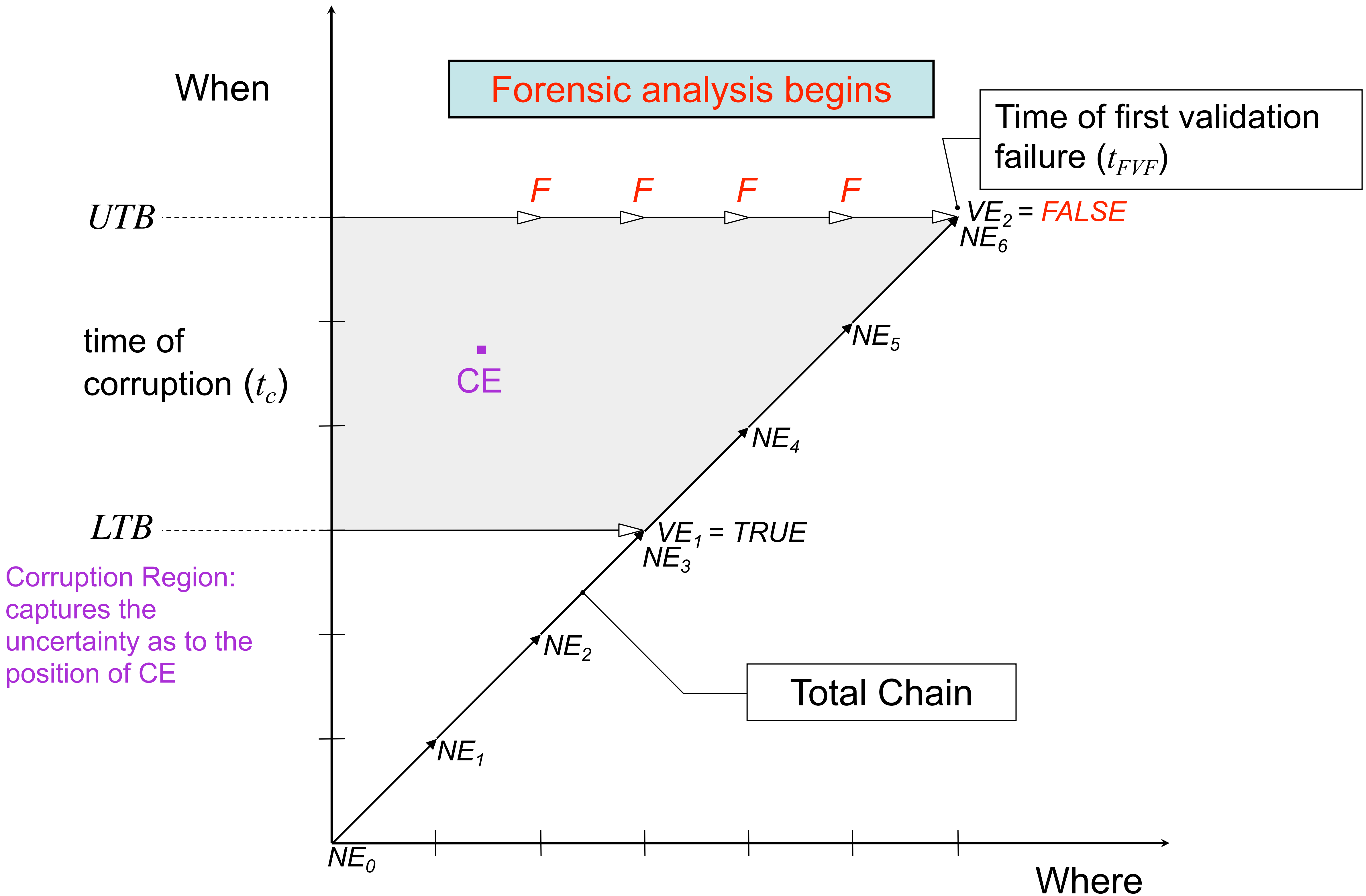
Monochromatic Algorithm



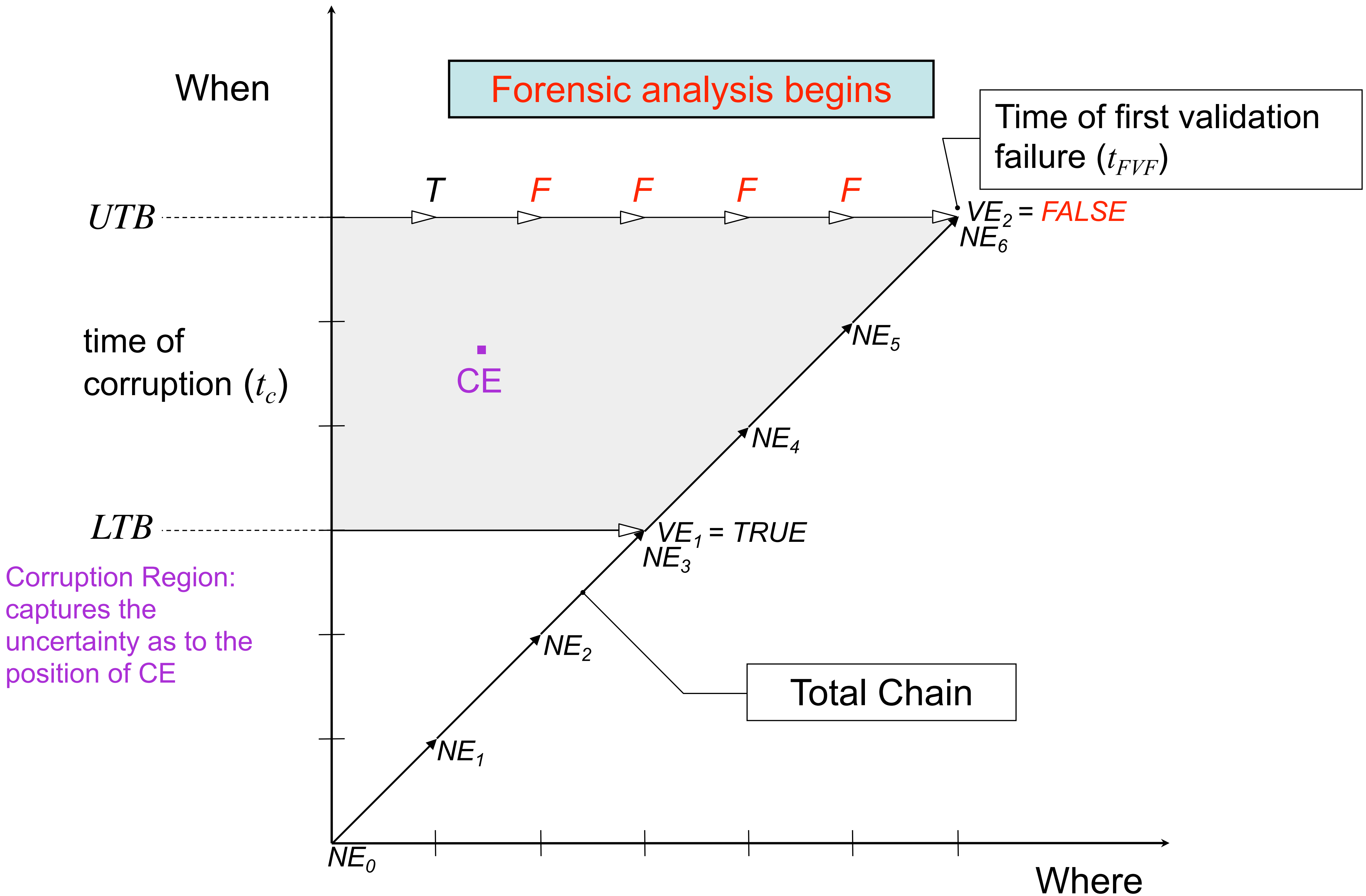
Monochromatic Algorithm



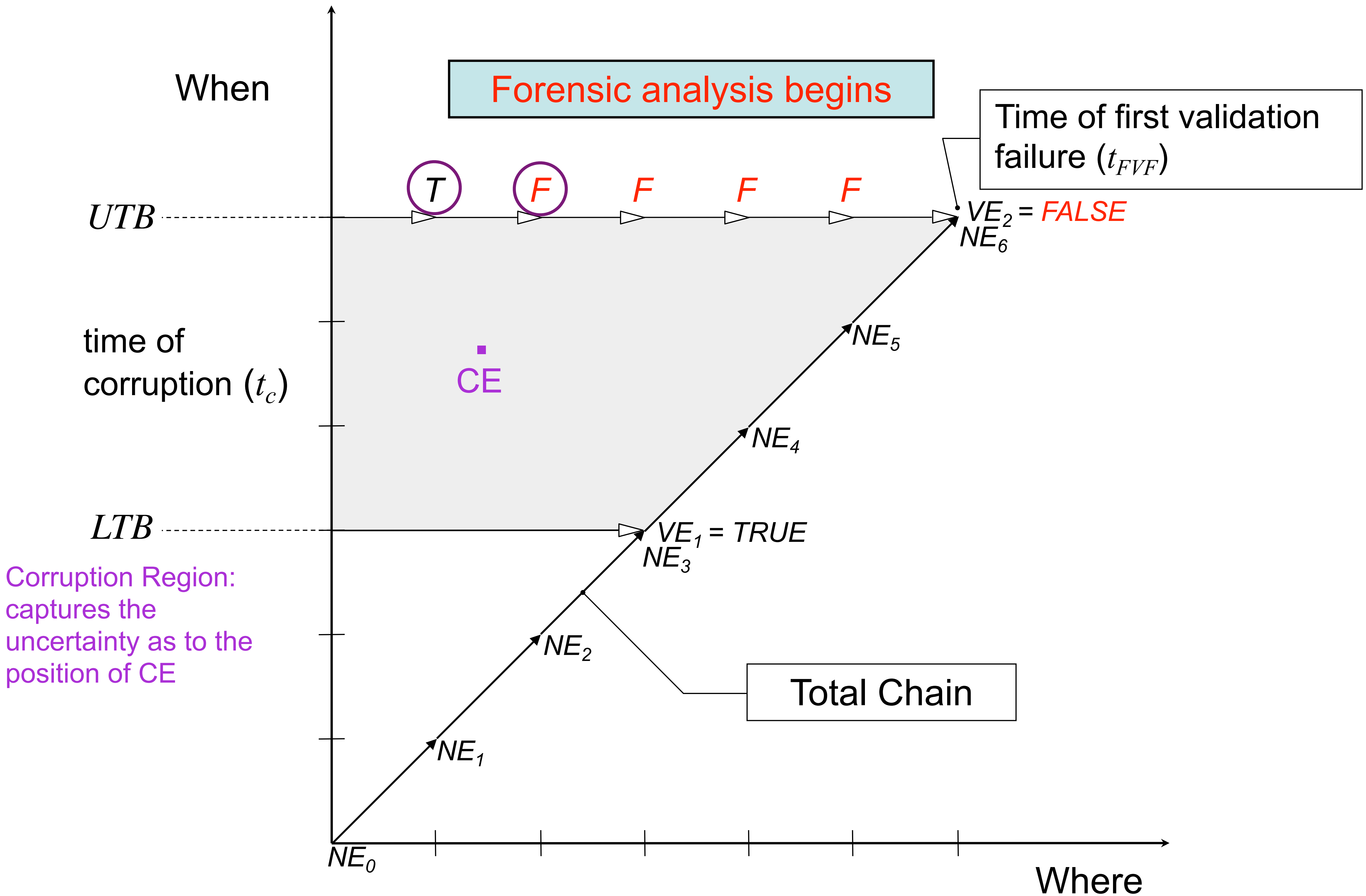
Monochromatic Algorithm



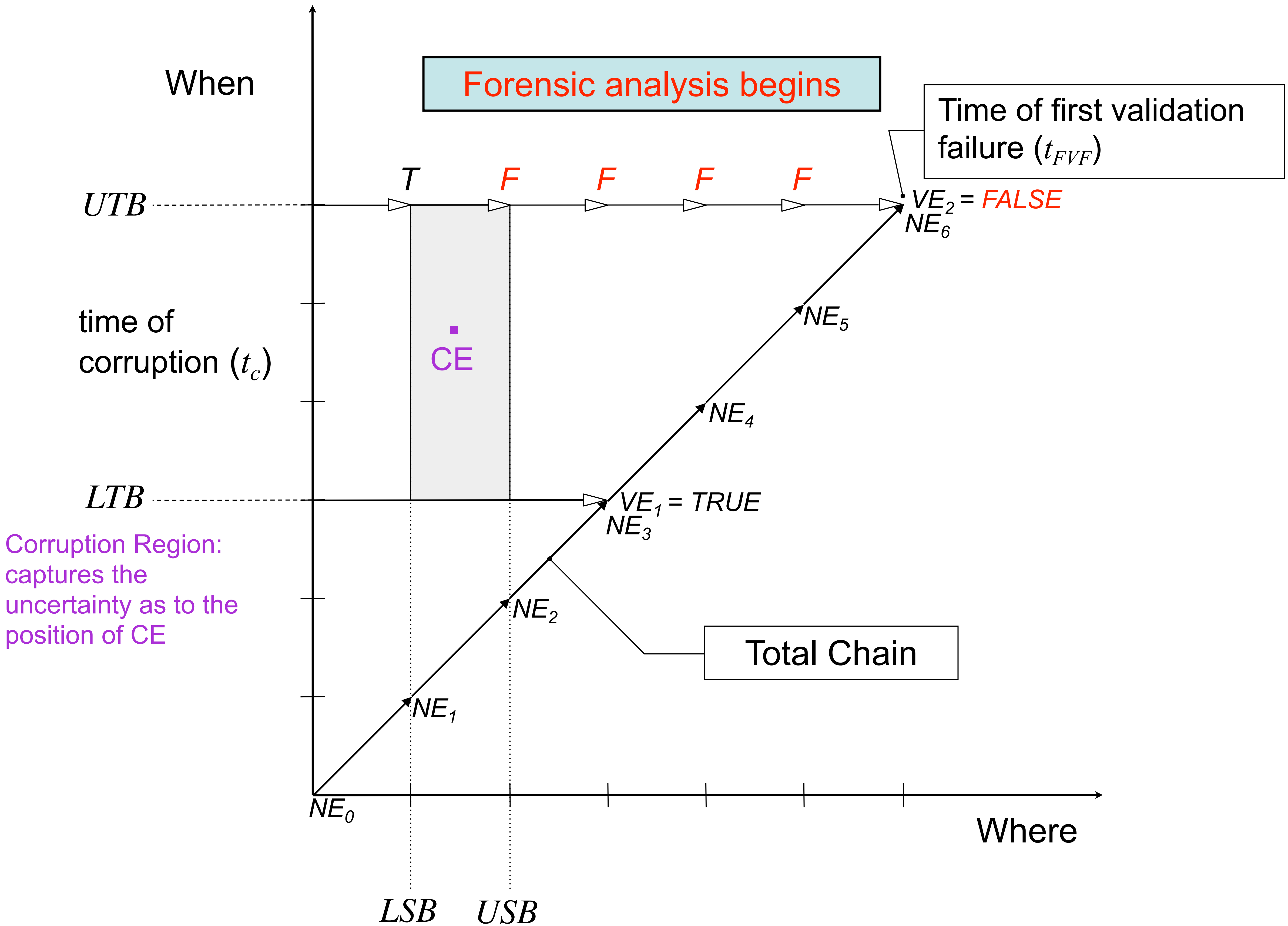
Monochromatic Algorithm



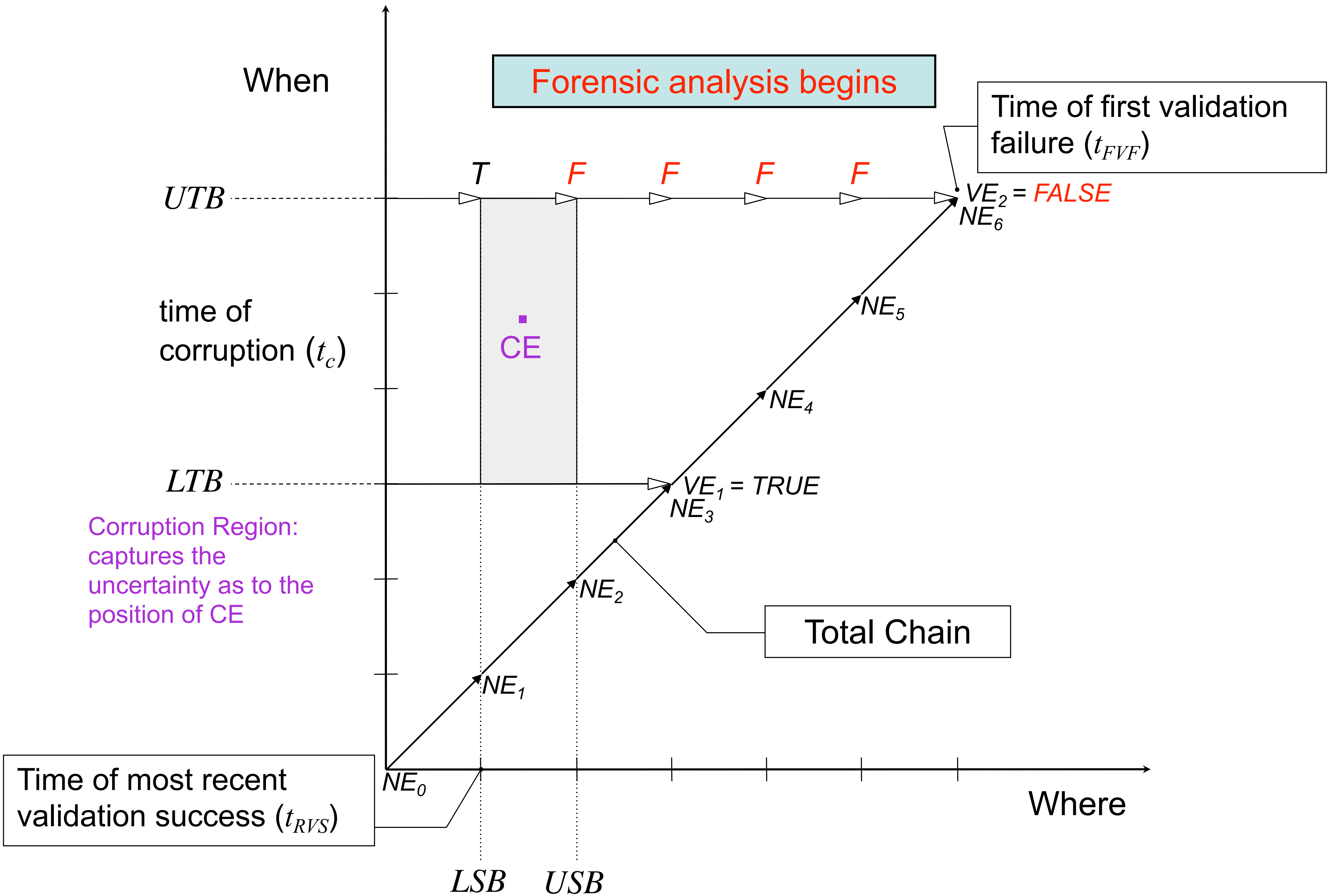
Monochromatic Algorithm



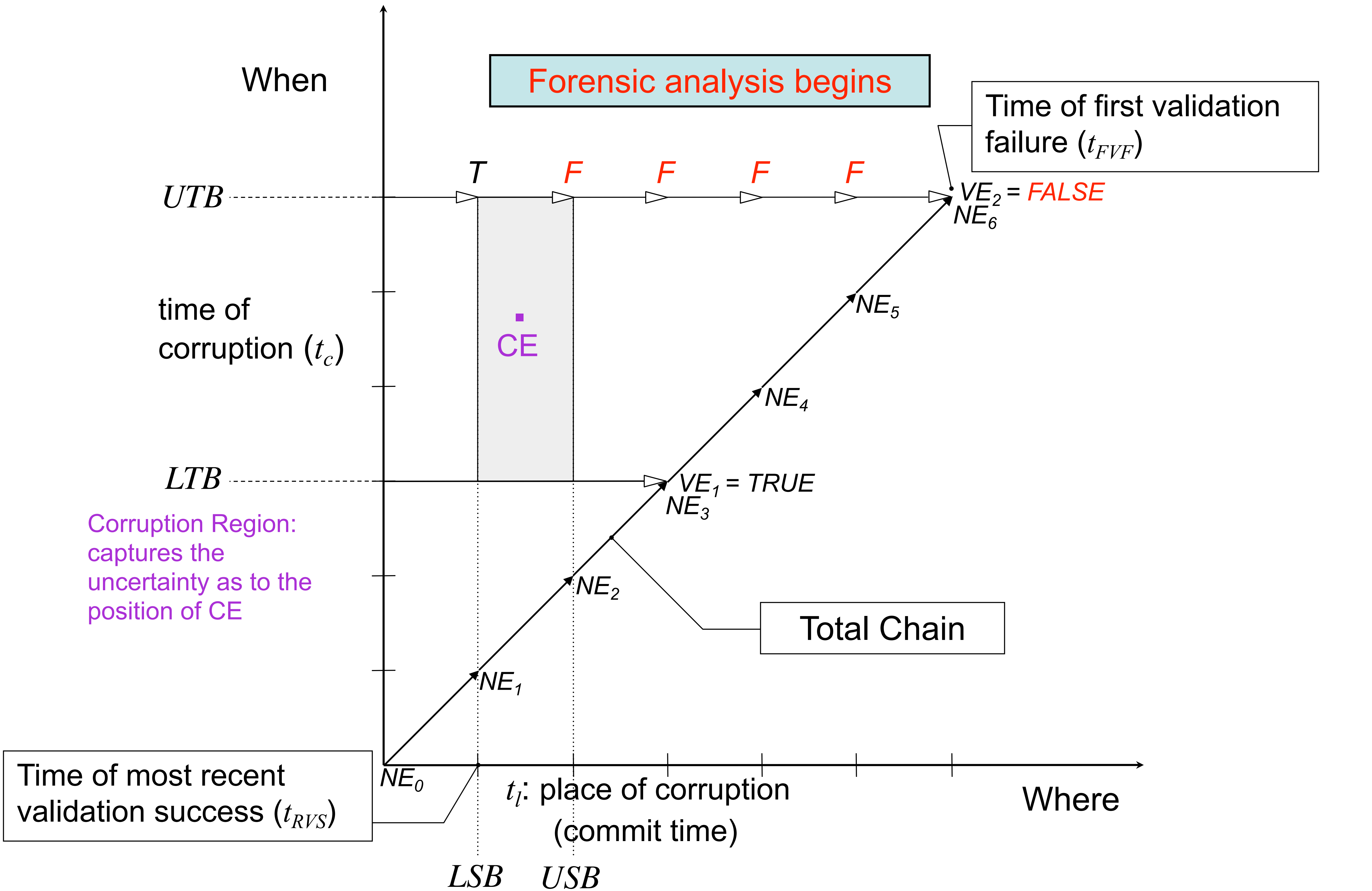
Monochromatic Algorithm



Monochromatic Algorithm



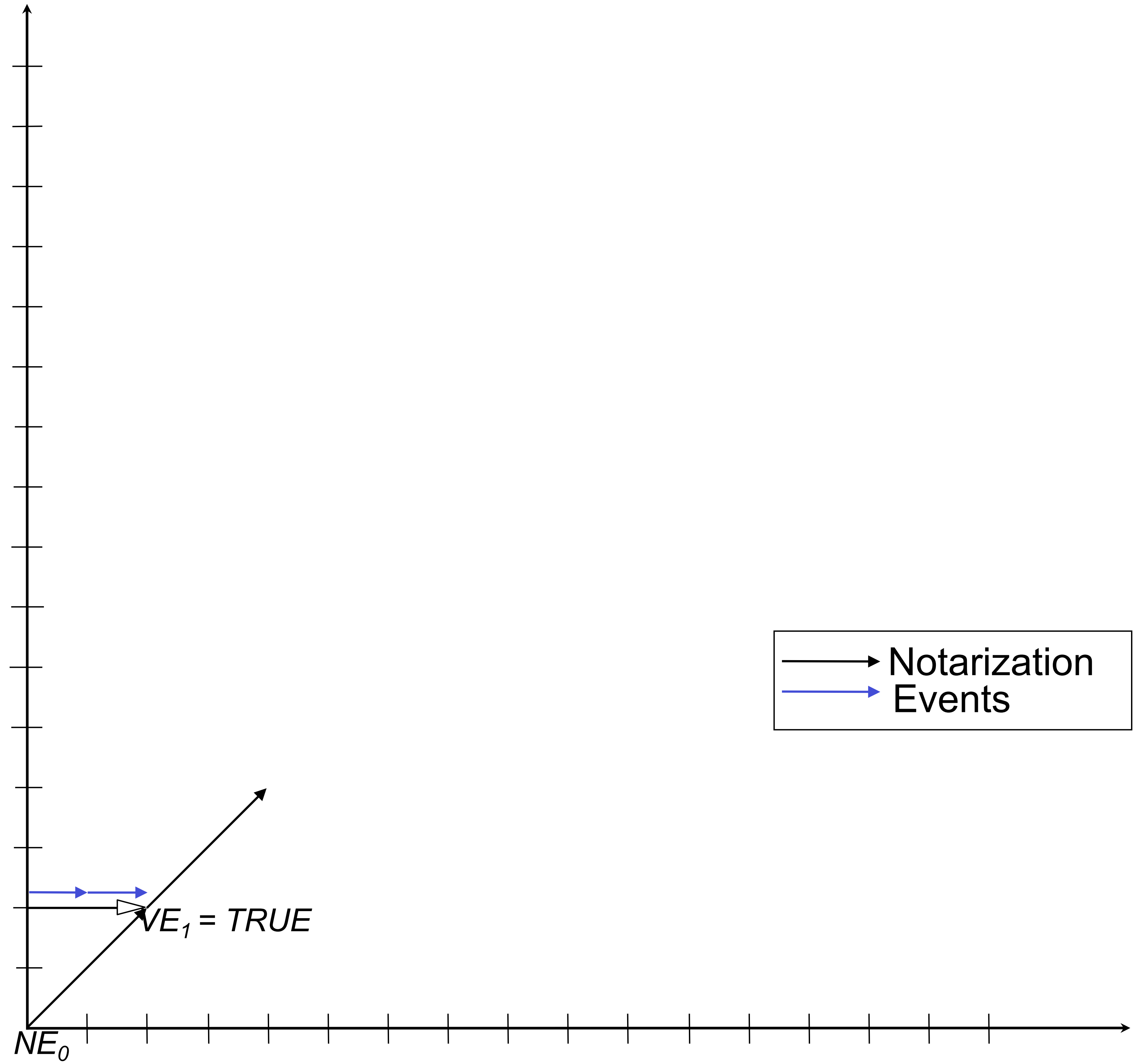
Monochromatic Algorithm



The a3D Algorithm

When

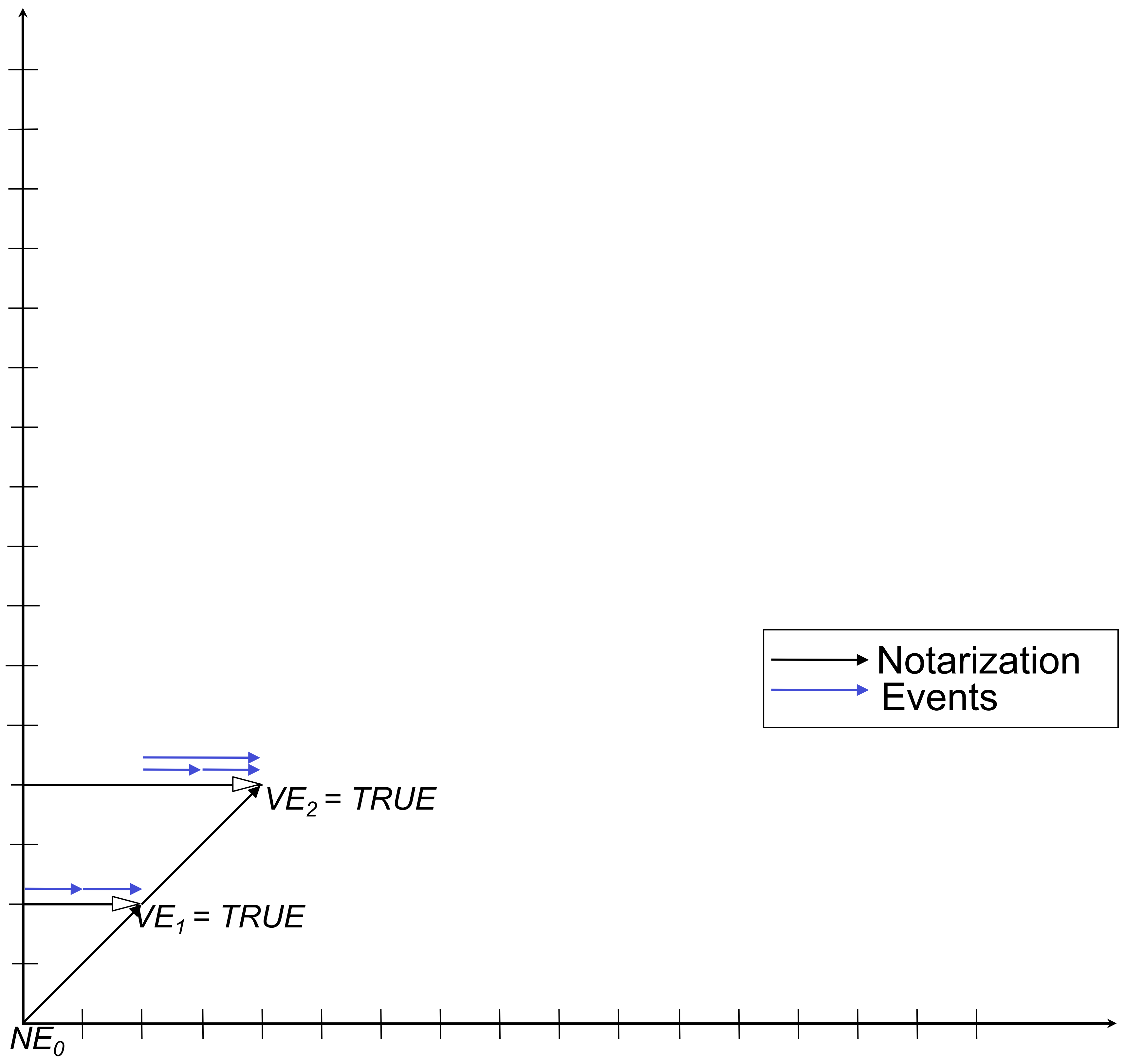
R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



The a3D Algorithm

When

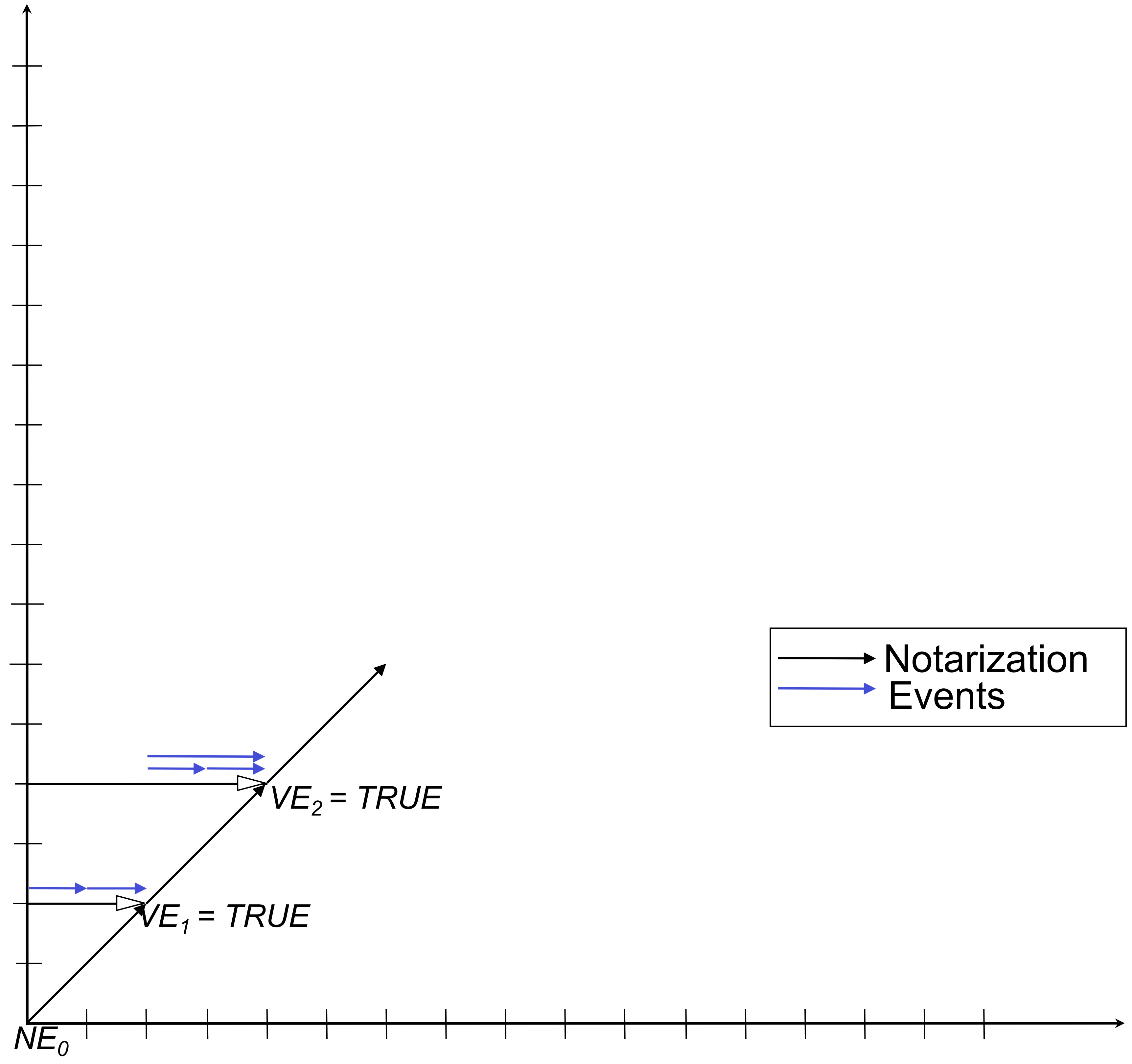
R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



The a3D Algorithm

When

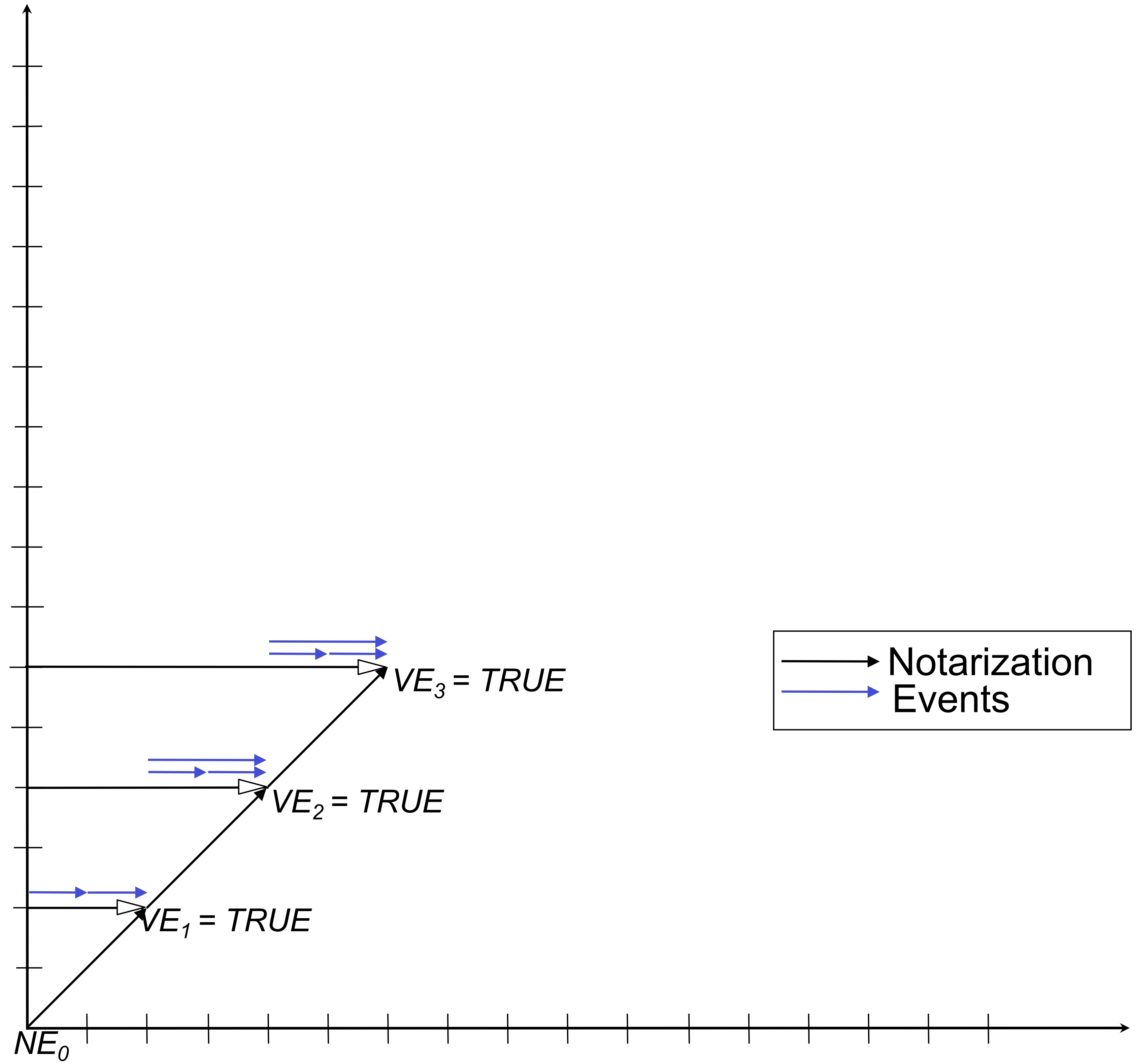
R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



The a3D Algorithm

When

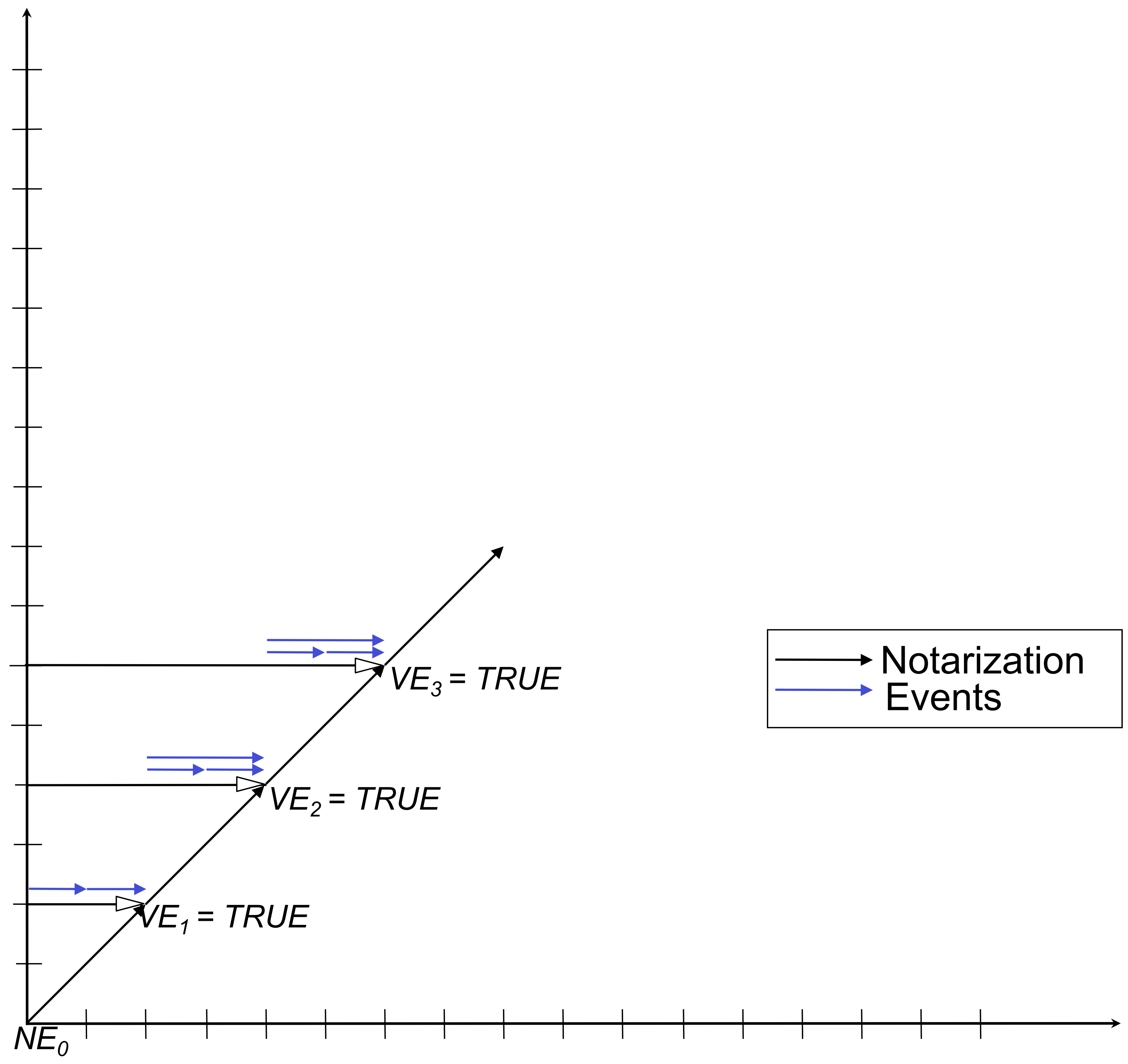
R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



The a3D Algorithm

When

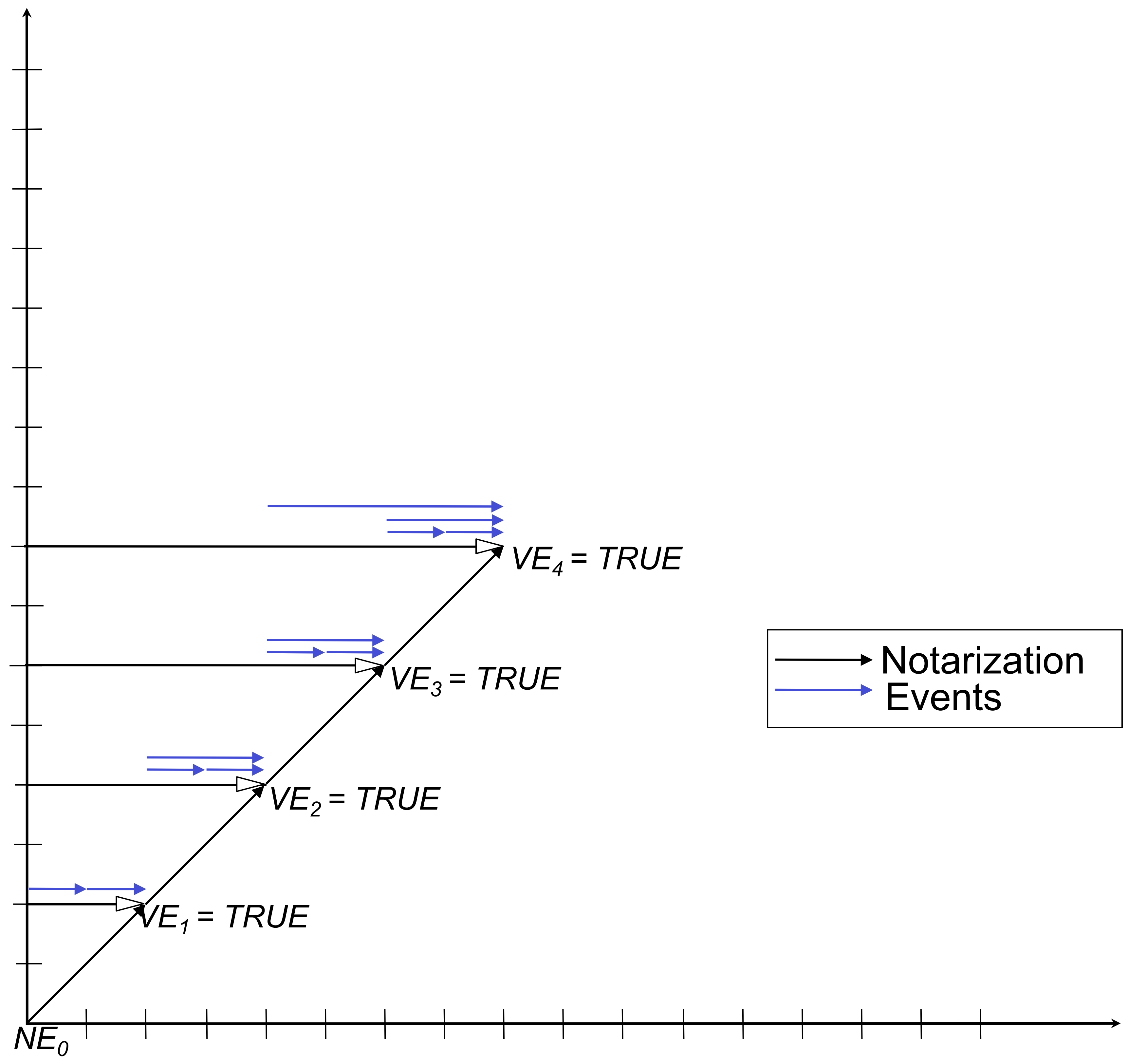
R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



The a3D Algorithm

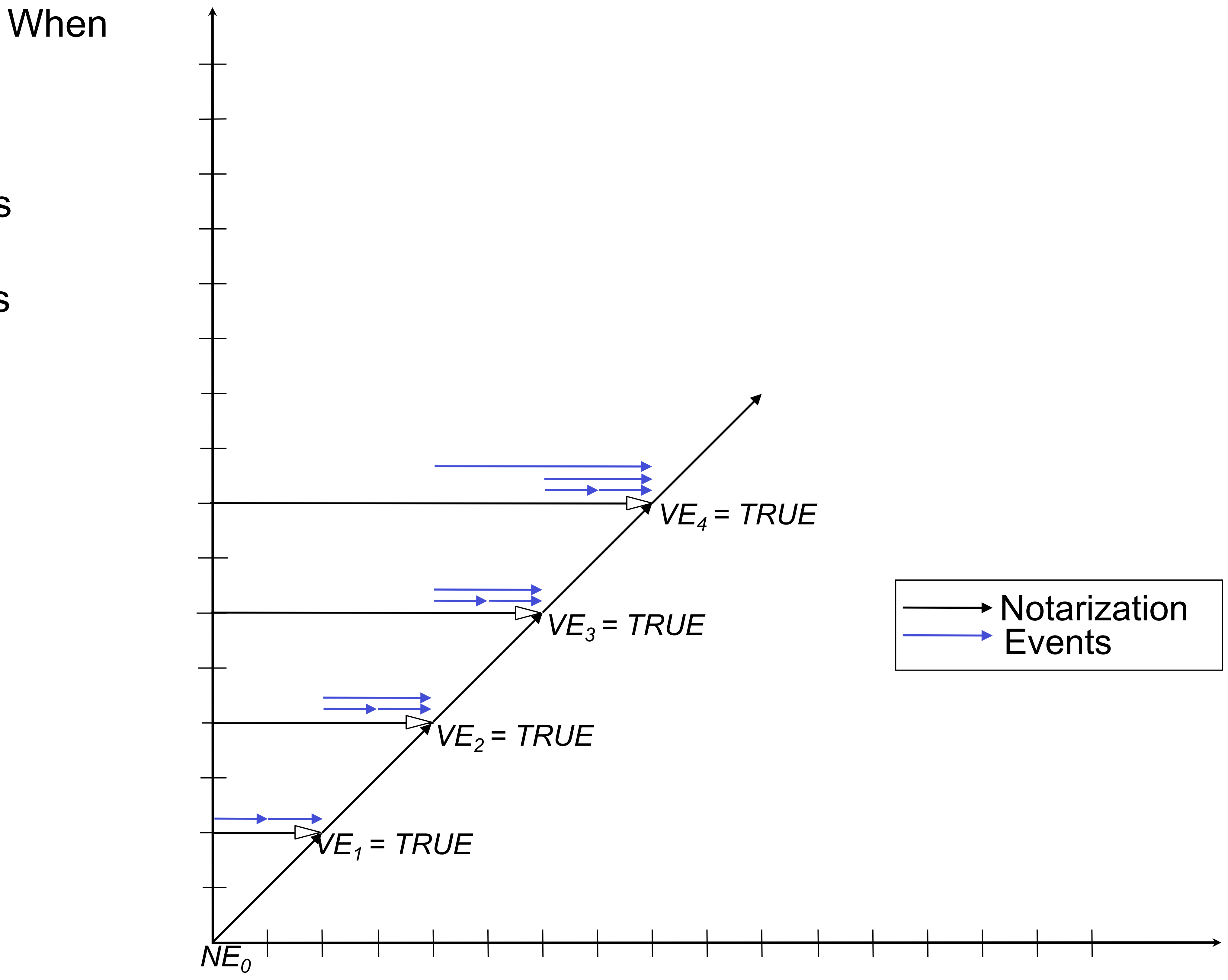
When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



The a3D Algorithm

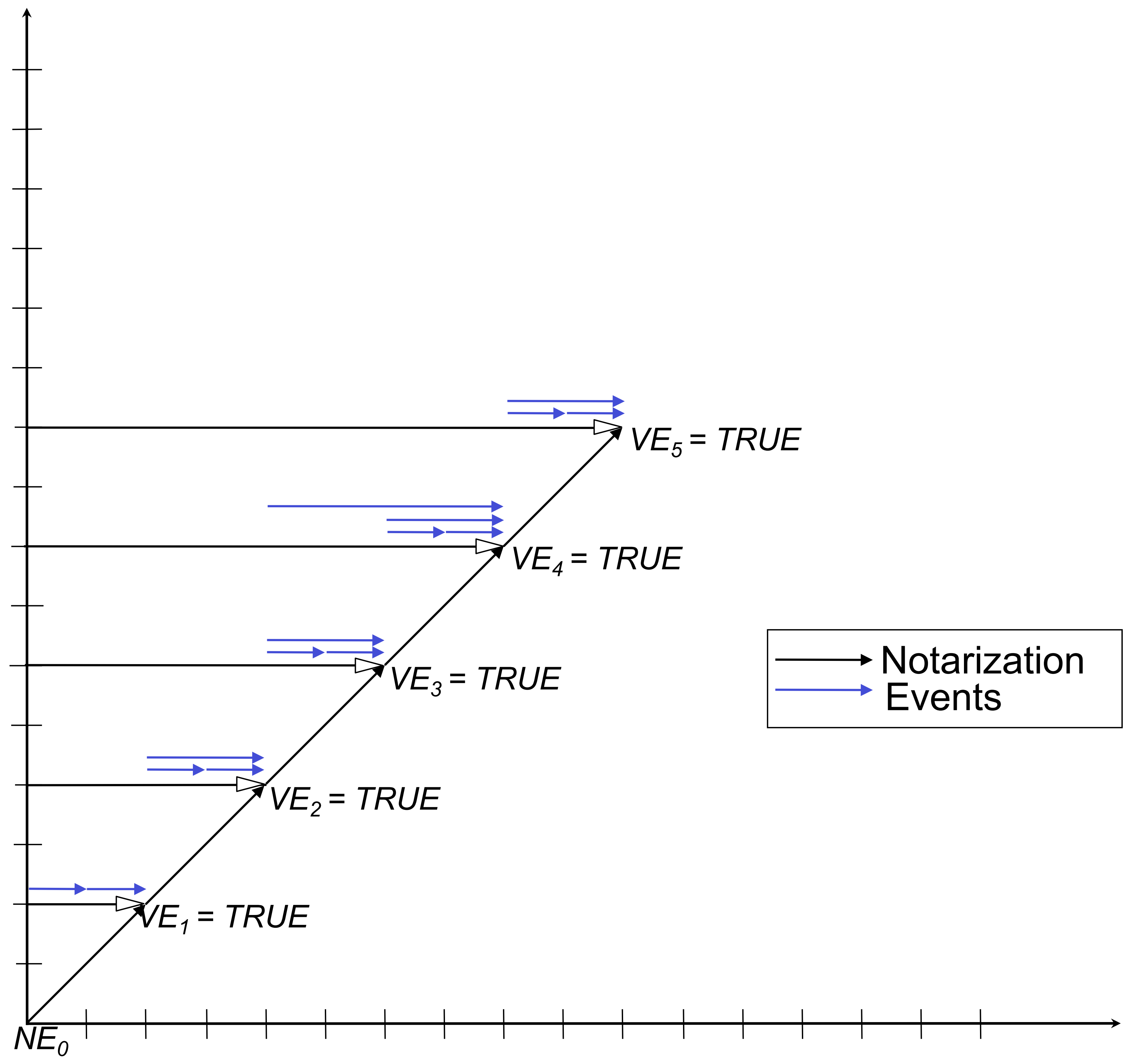
R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



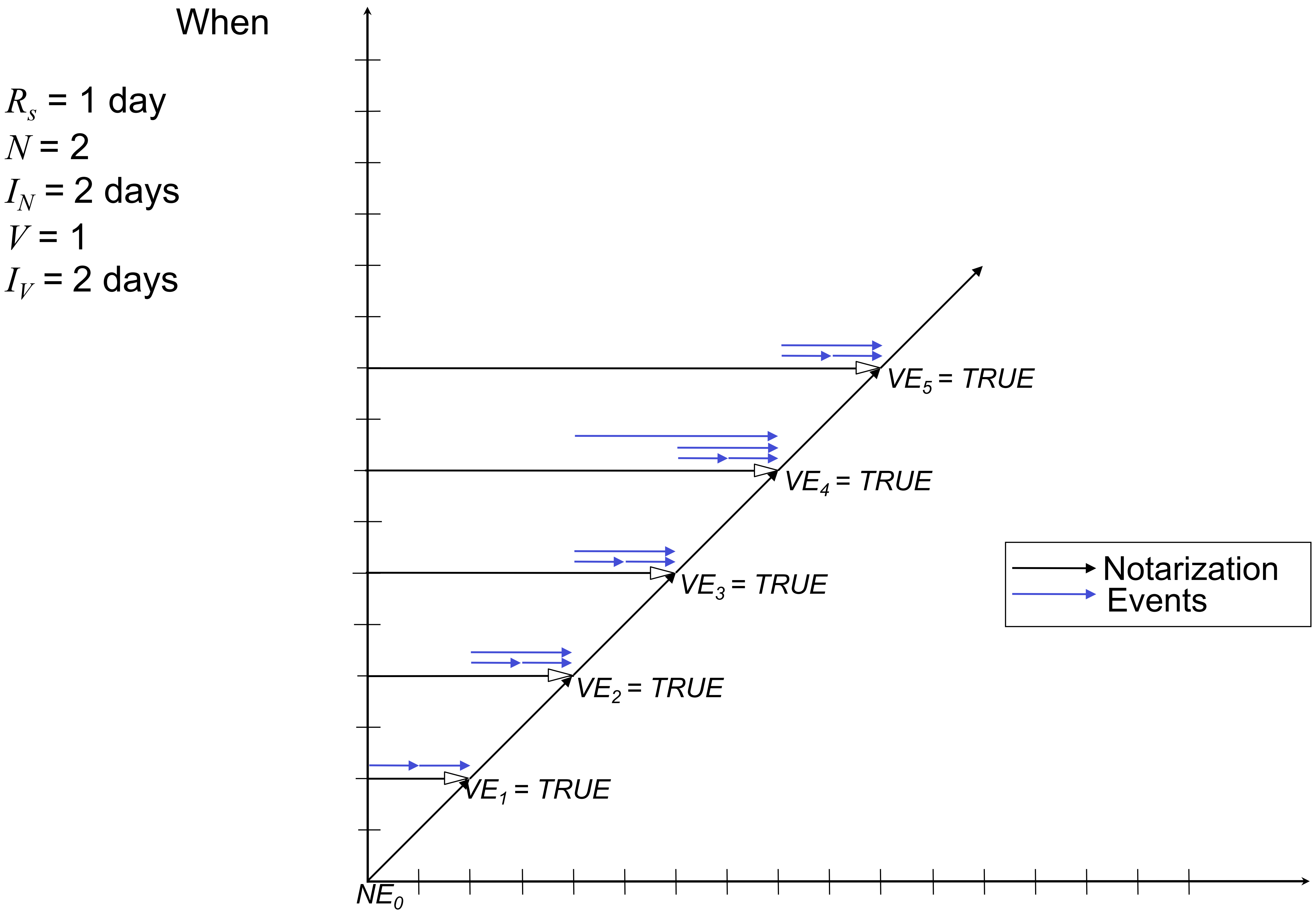
The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



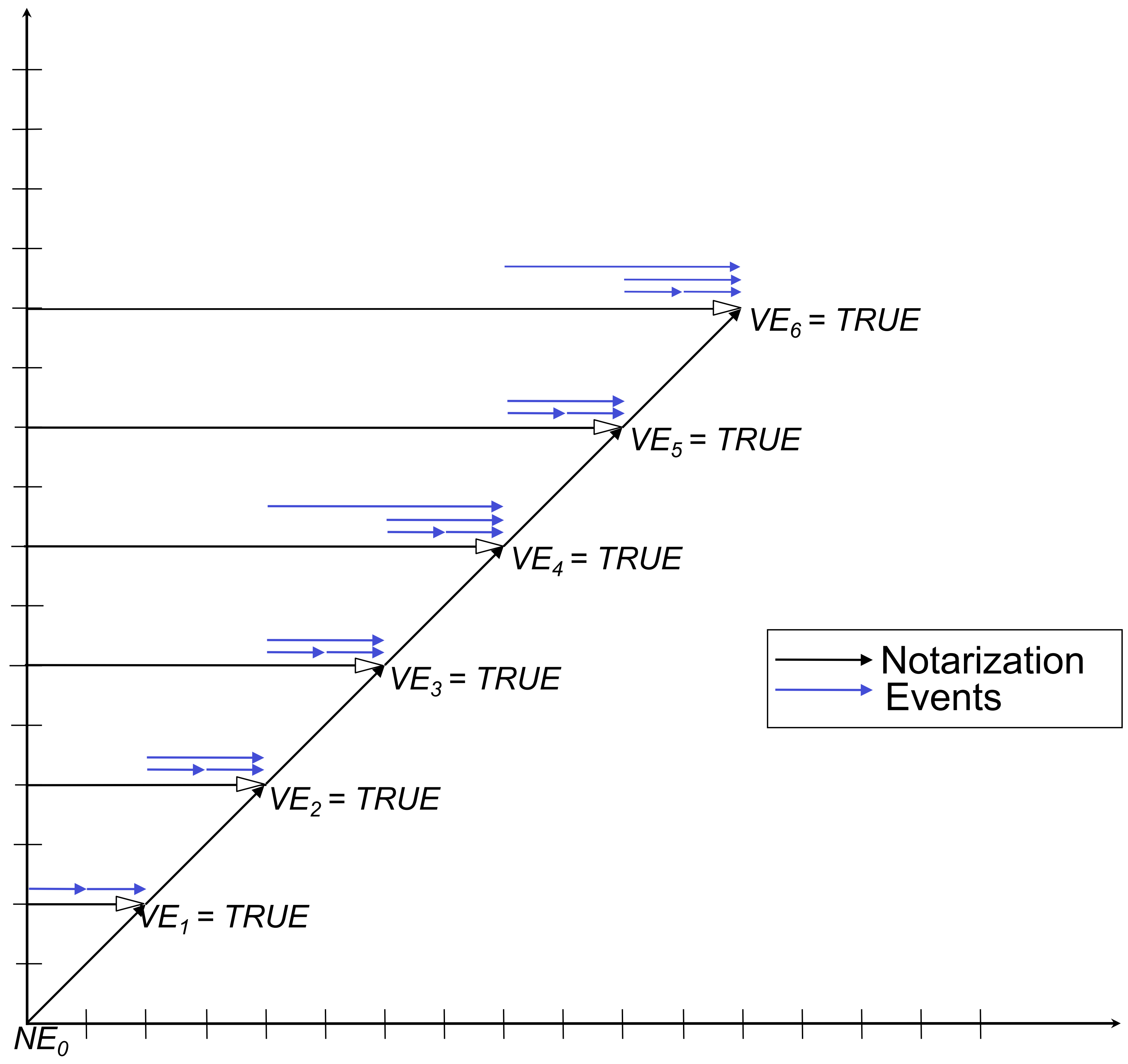
The a3D Algorithm



The a3D Algorithm

When

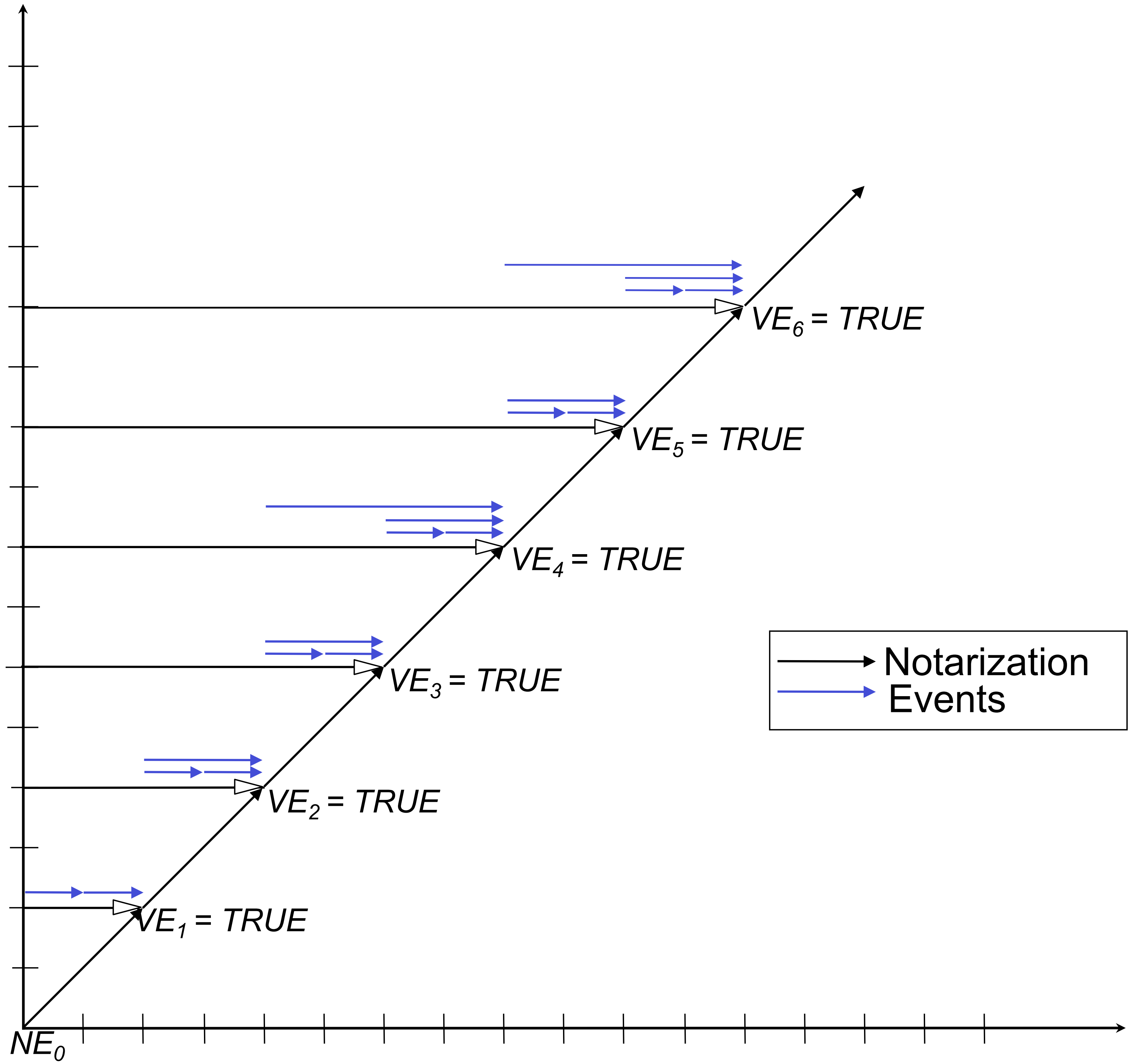
R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



The a3D Algorithm

When

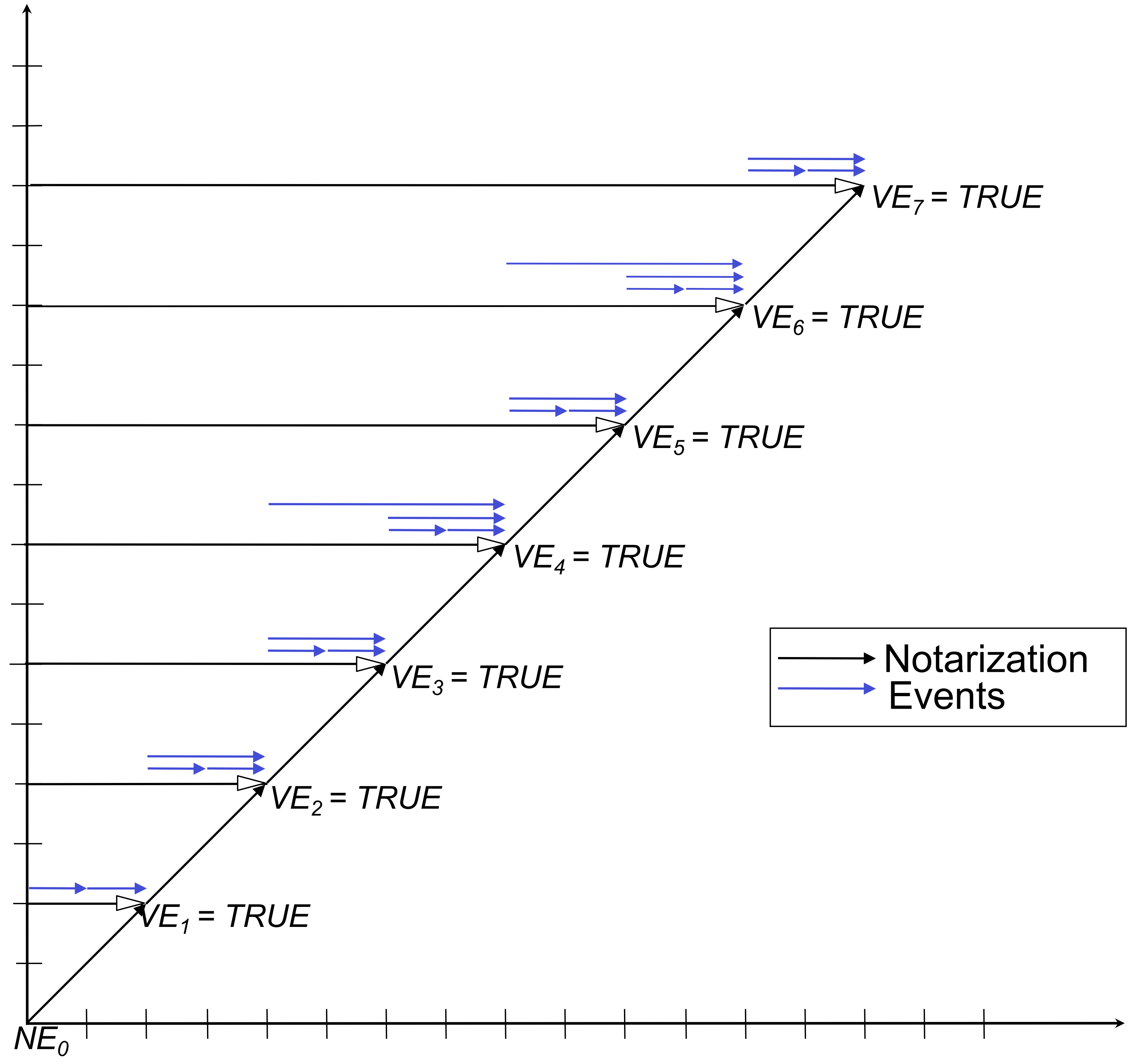
R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

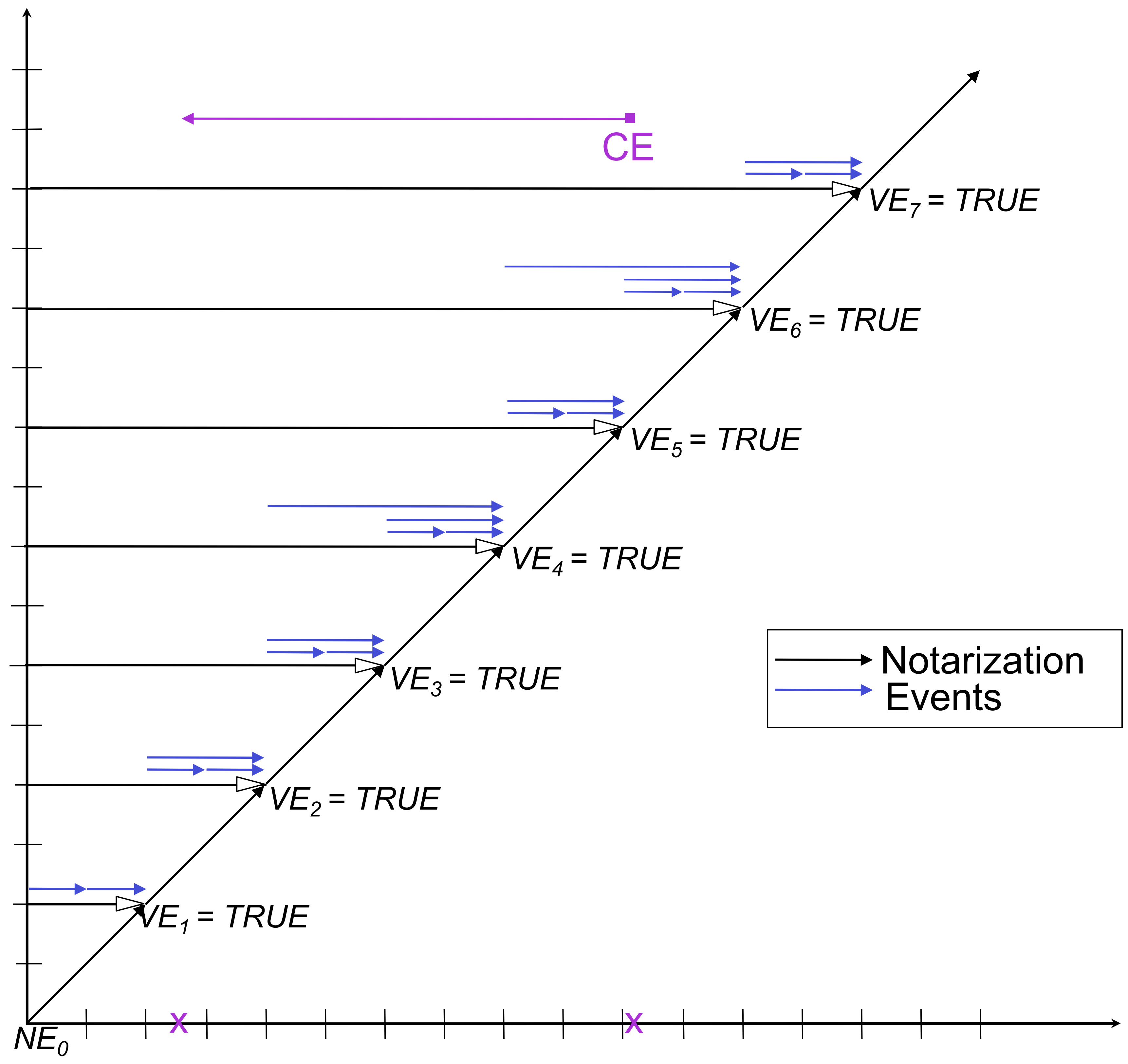


The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

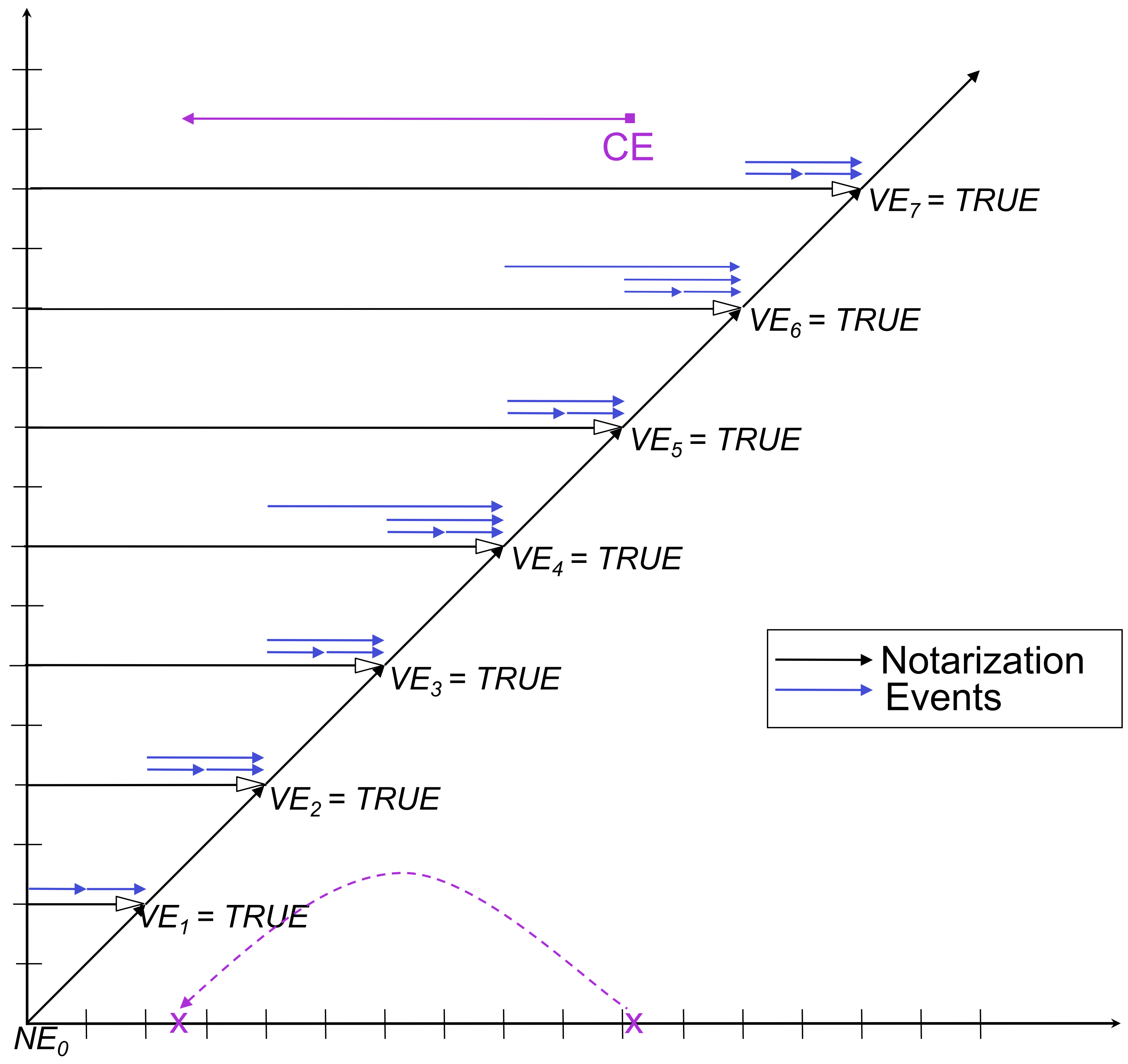


The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

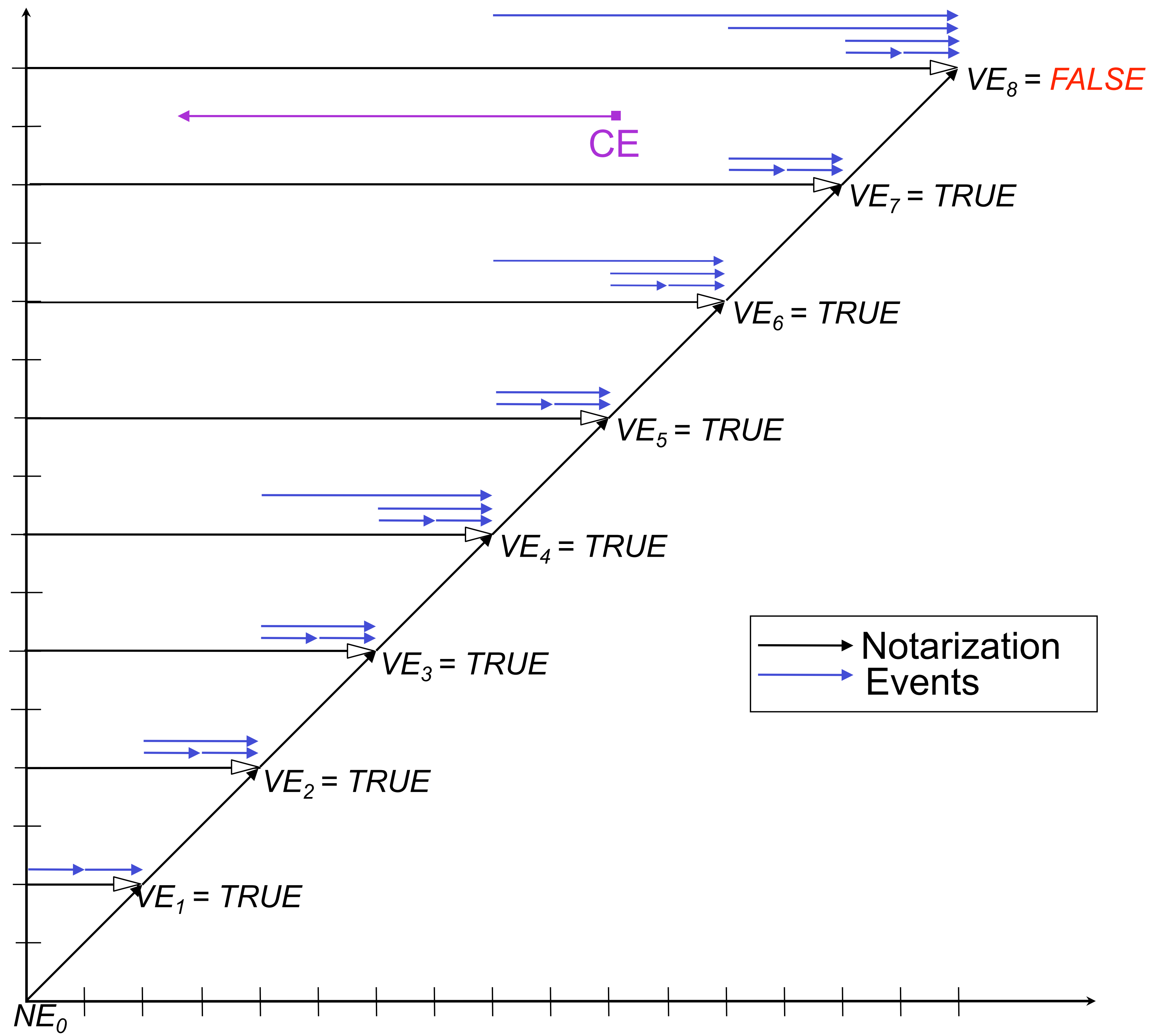


The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

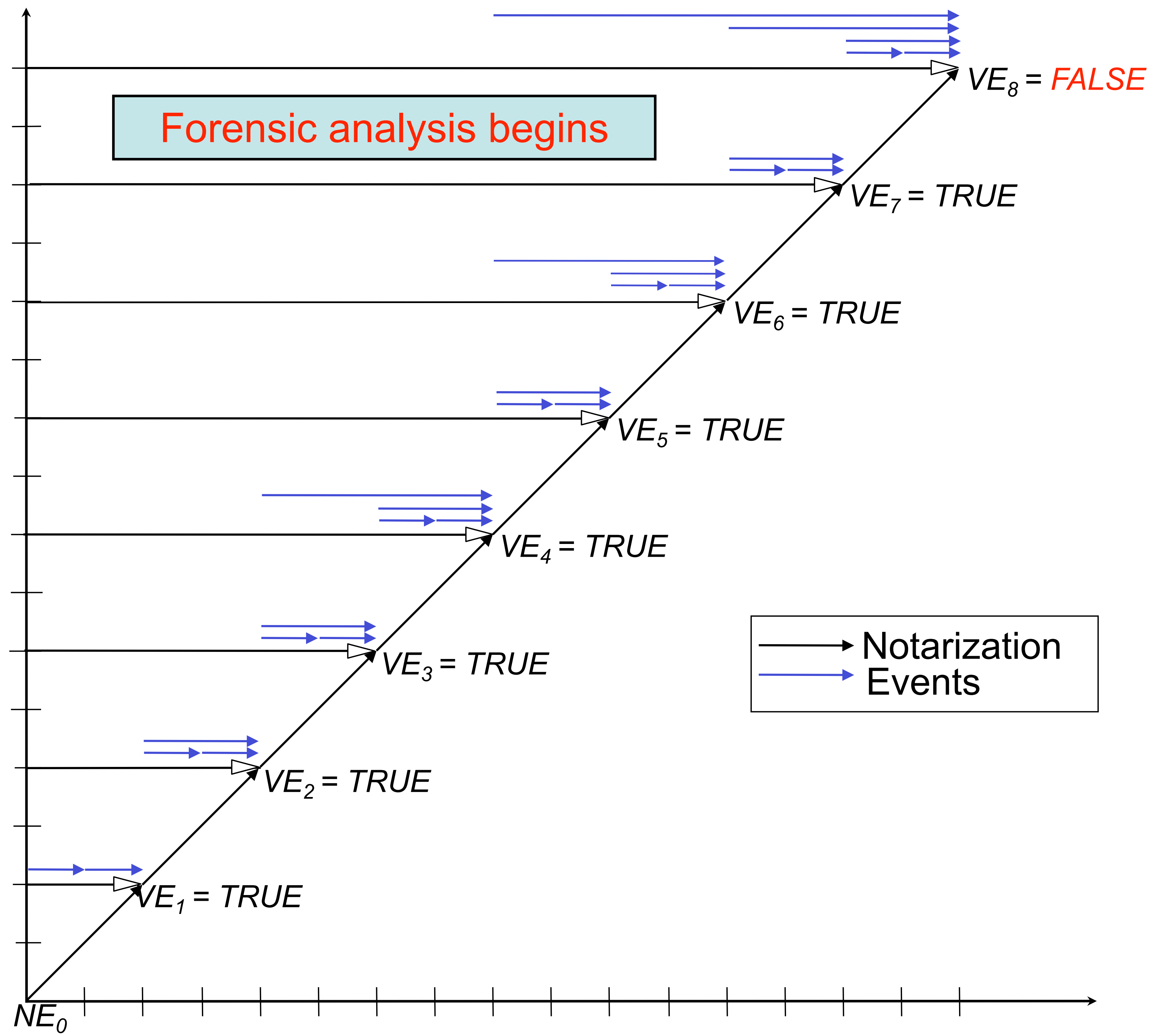


The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

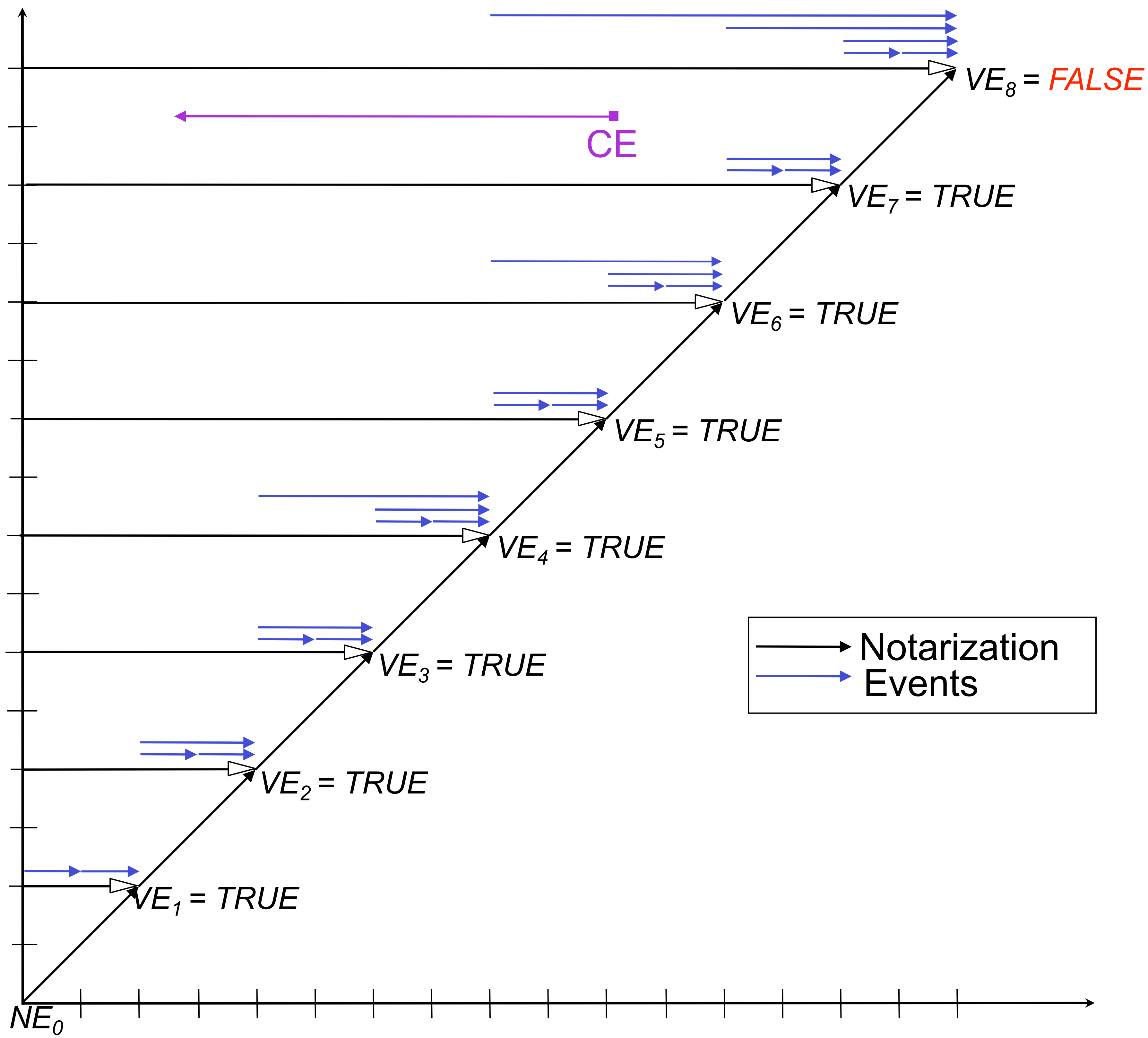


The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

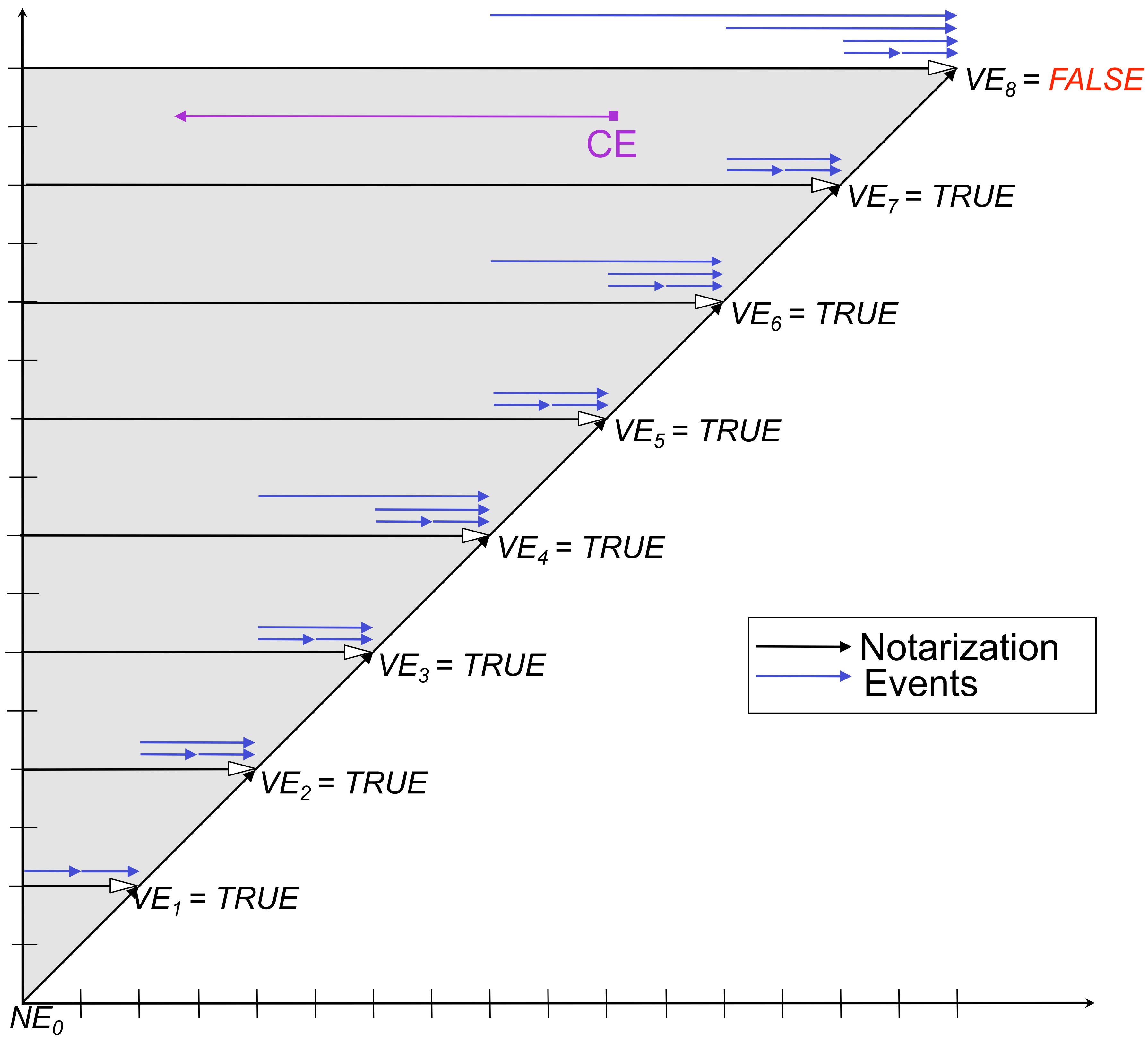


The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

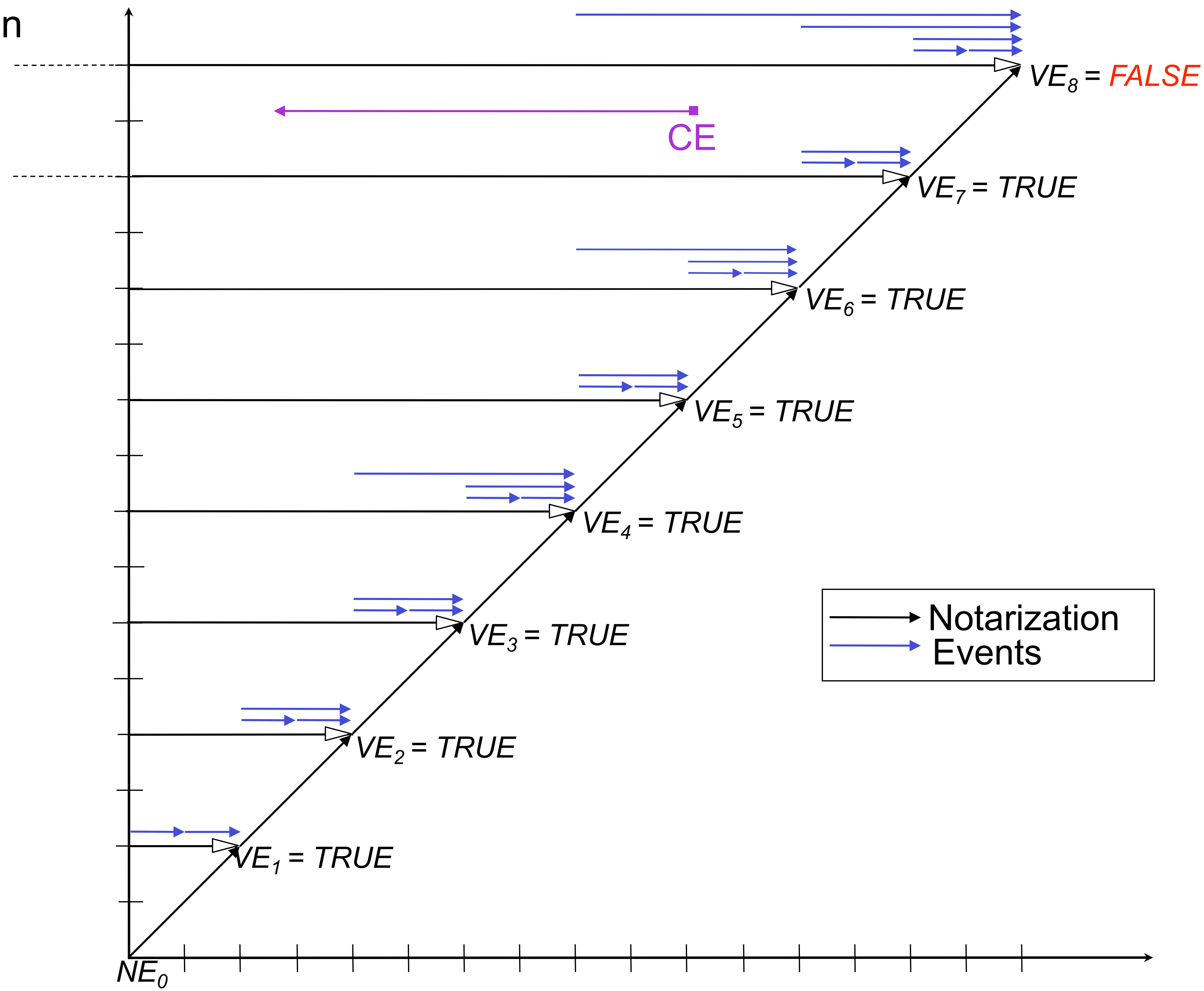
Backdating CE



The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

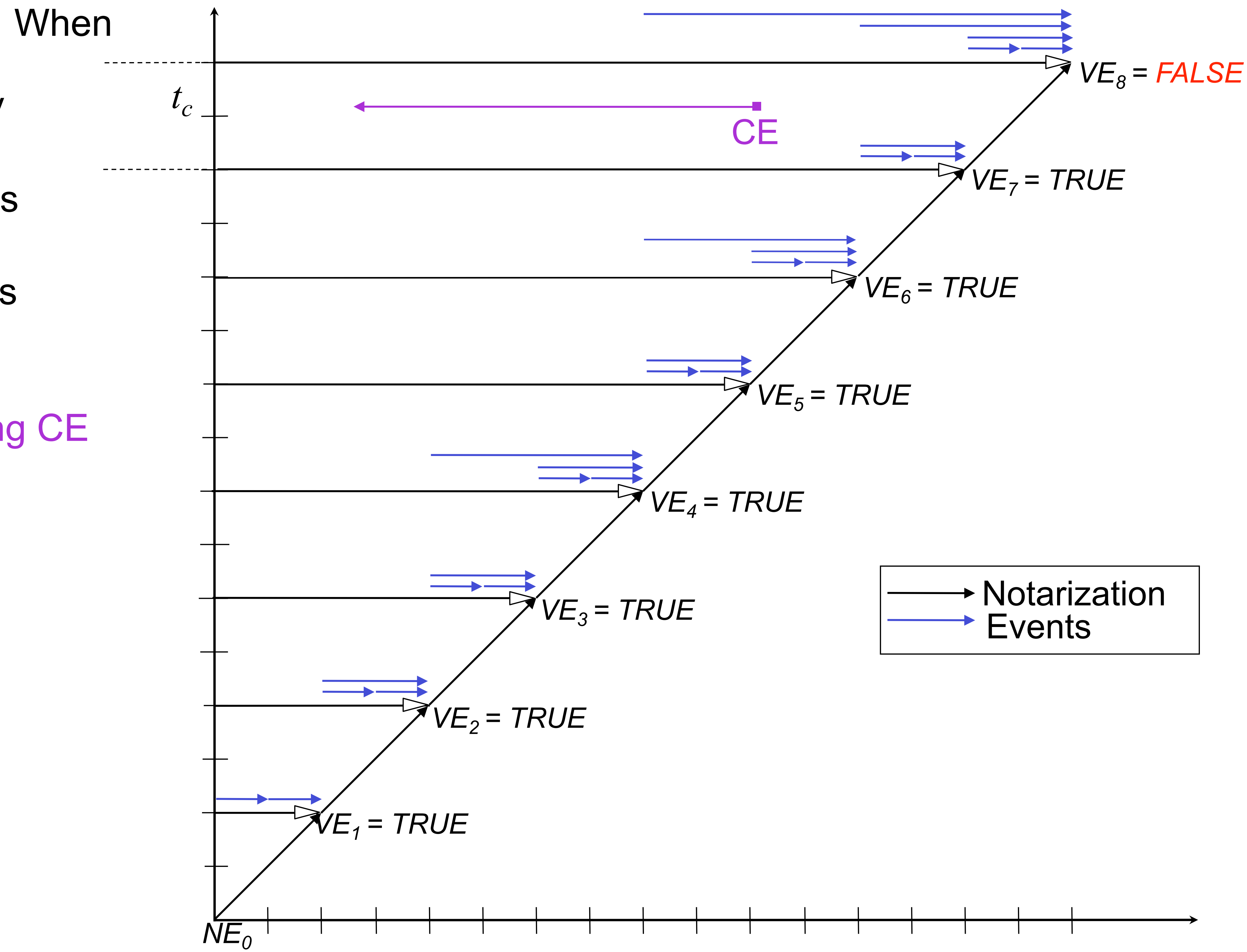
Backdating CE



The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

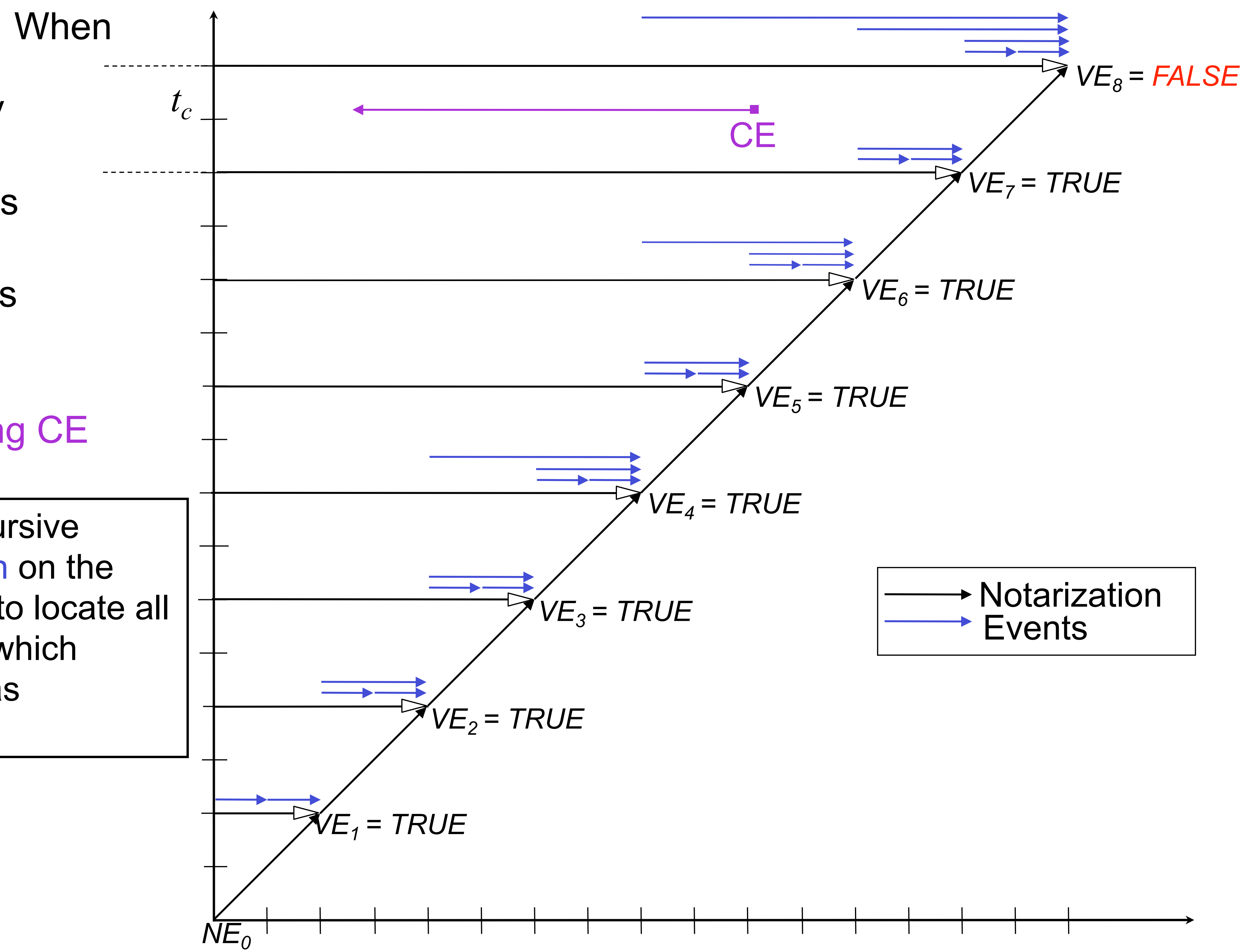


The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

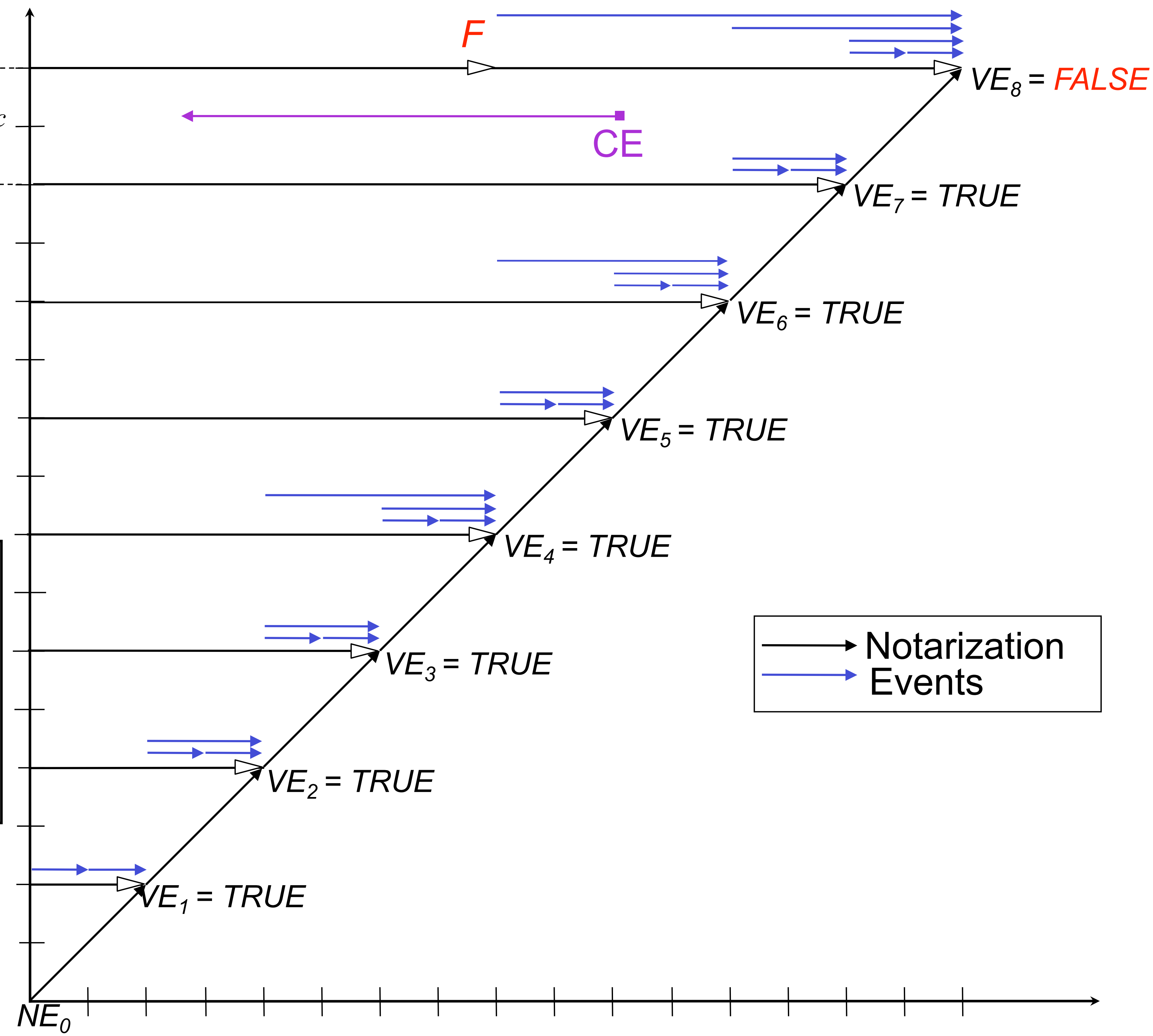


The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

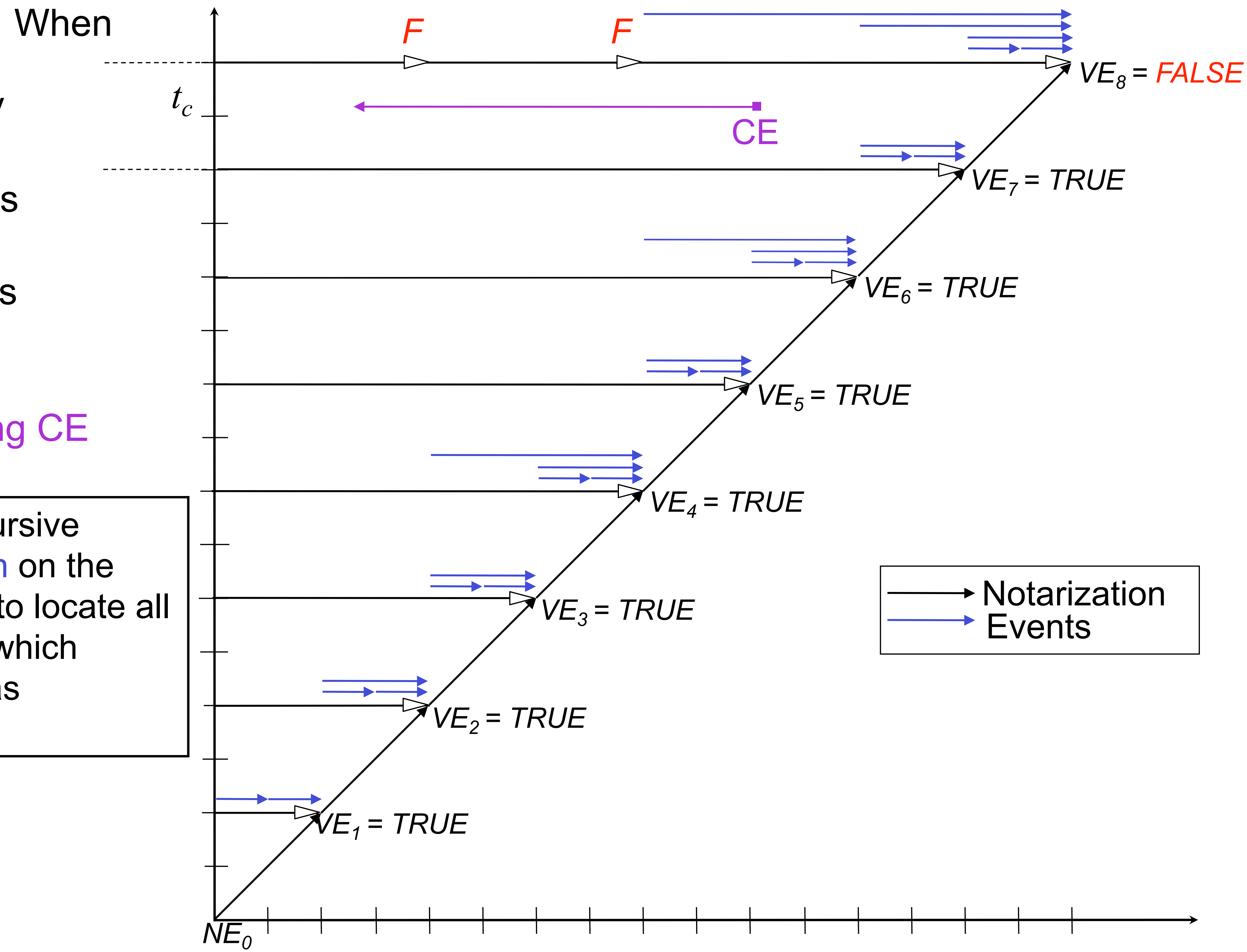


The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

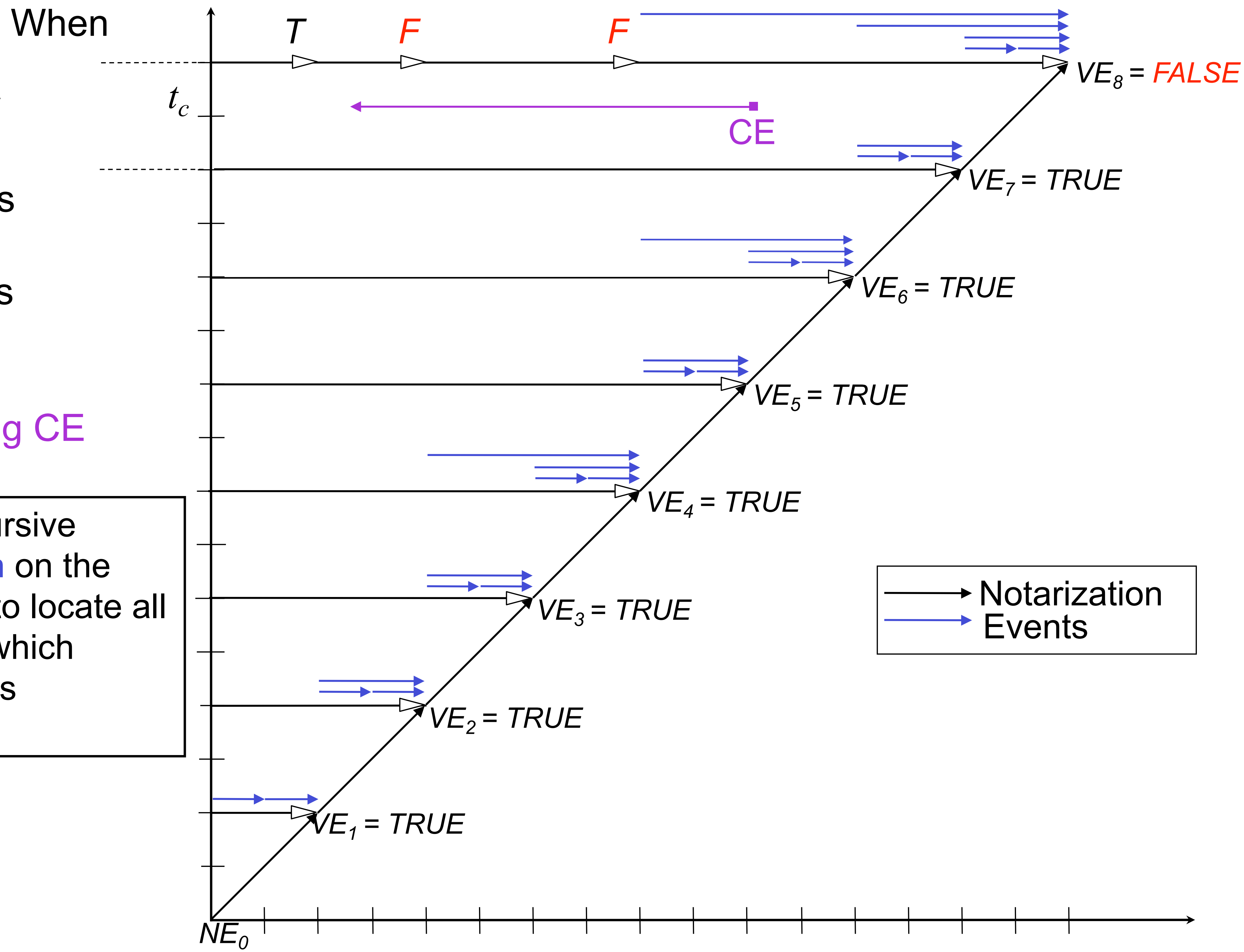
Backdating CE

Can use recursive binary search on the the hash chains to locate all days during which tampering has occurred.



The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



Backdating CE

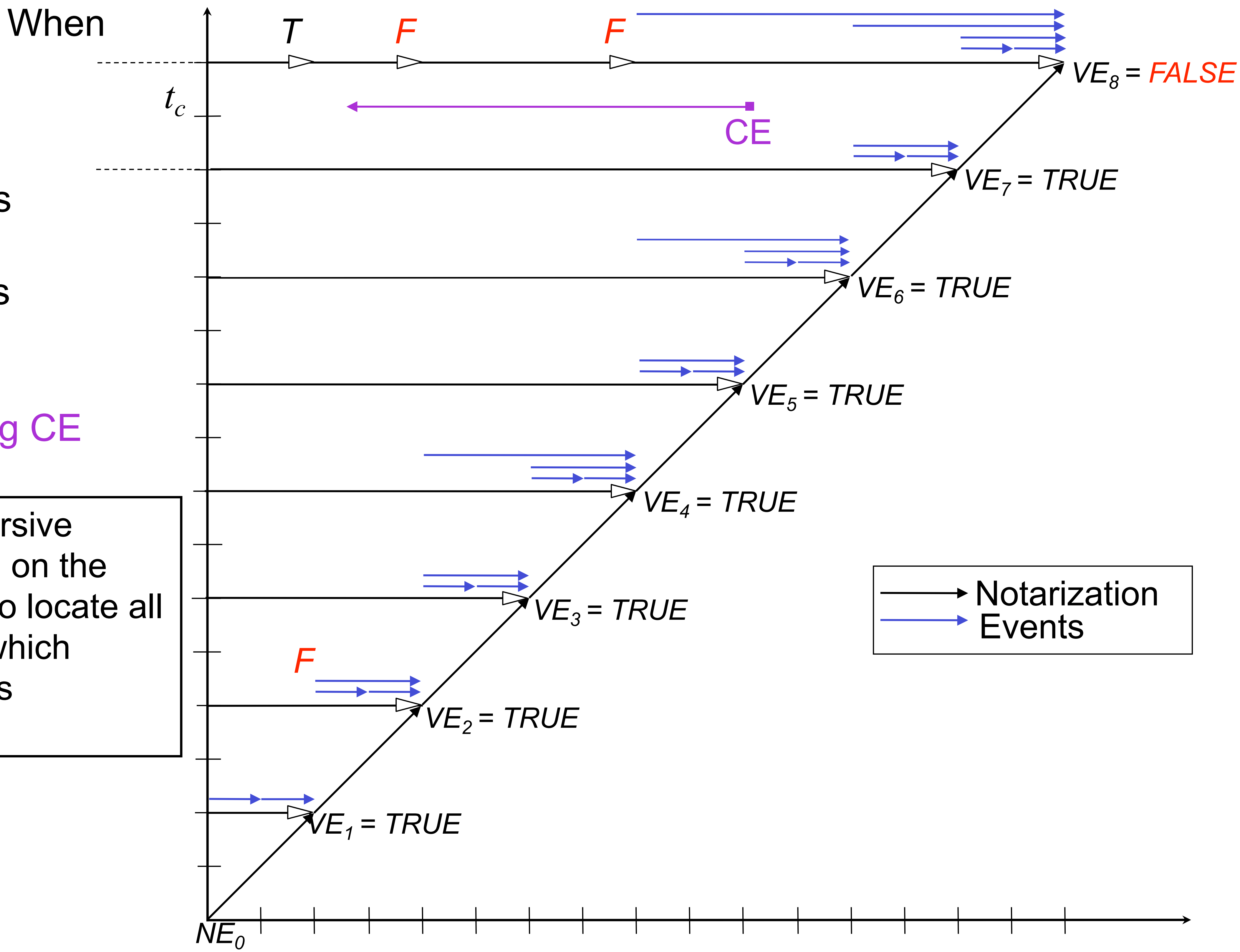
Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

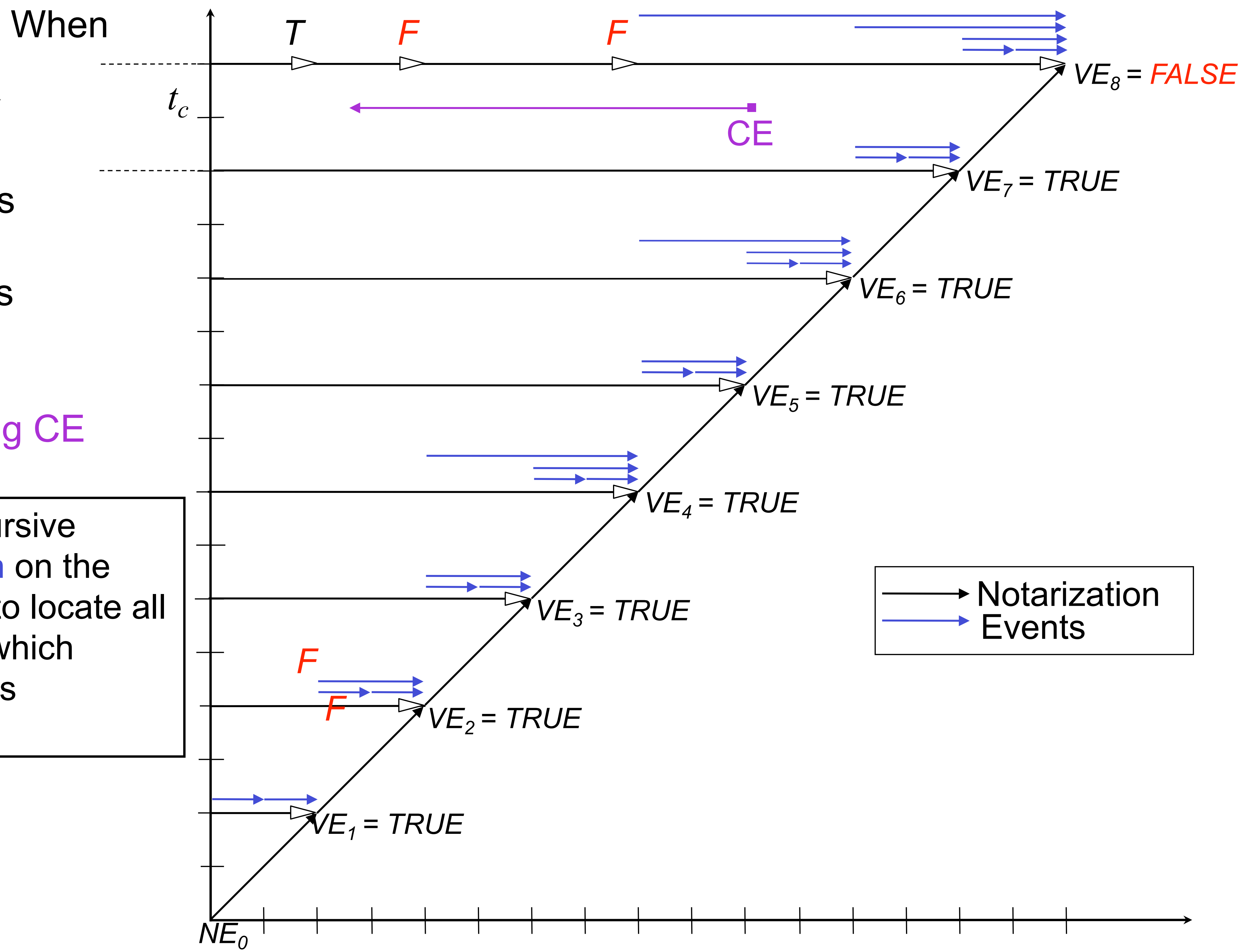
Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.



The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

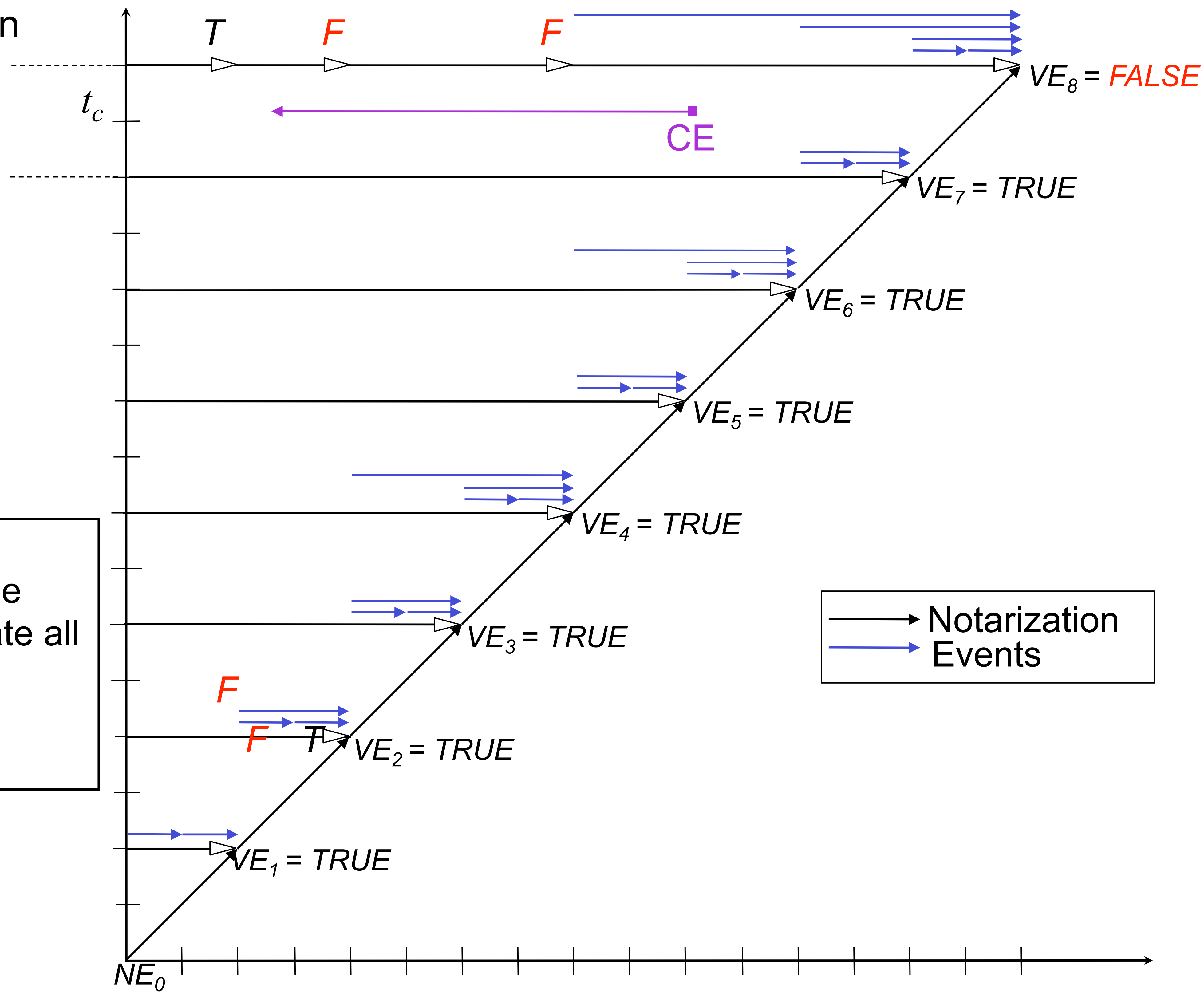


Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



Backdating CE

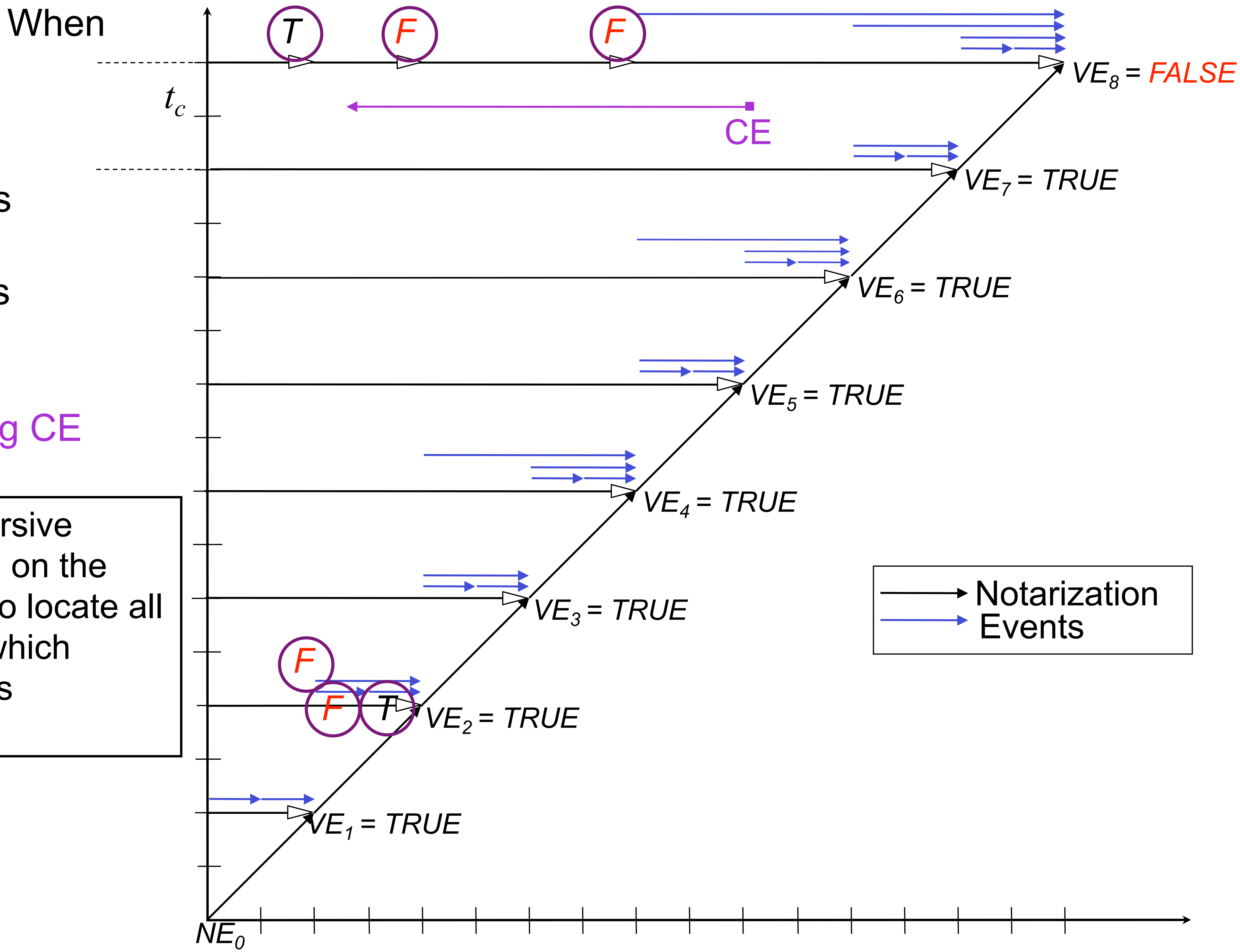
Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

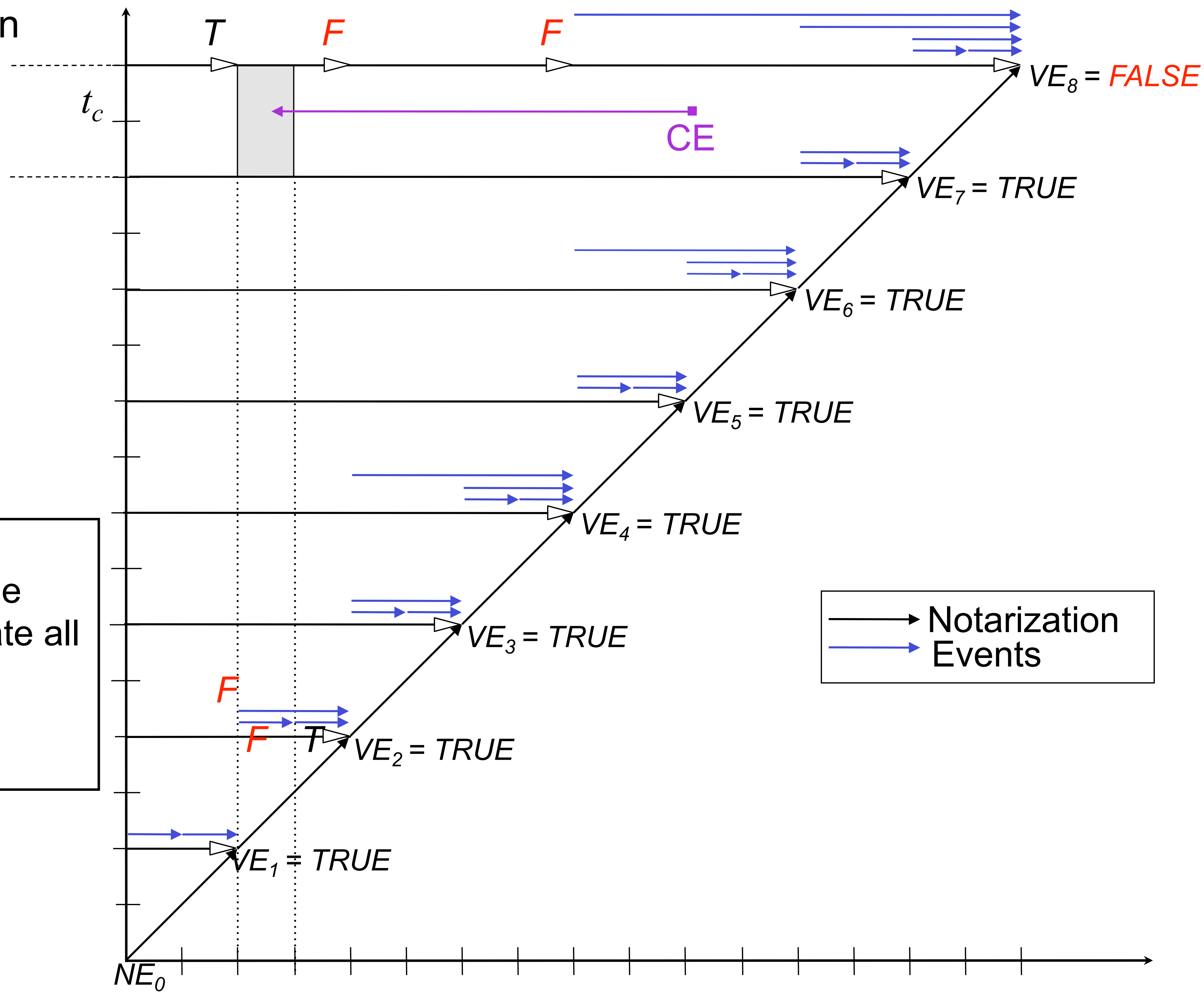


The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.



The a3D Algorithm

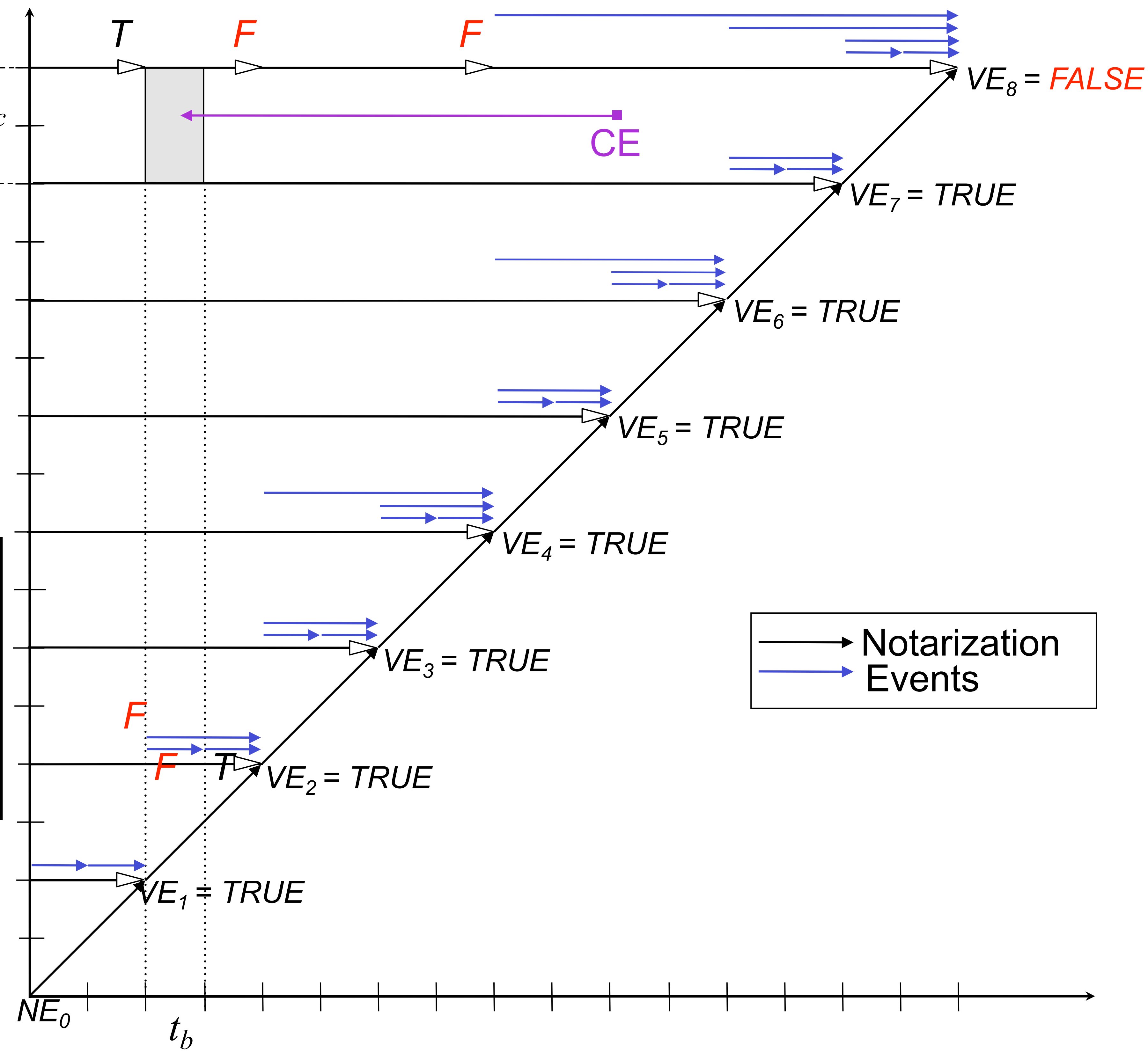
When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



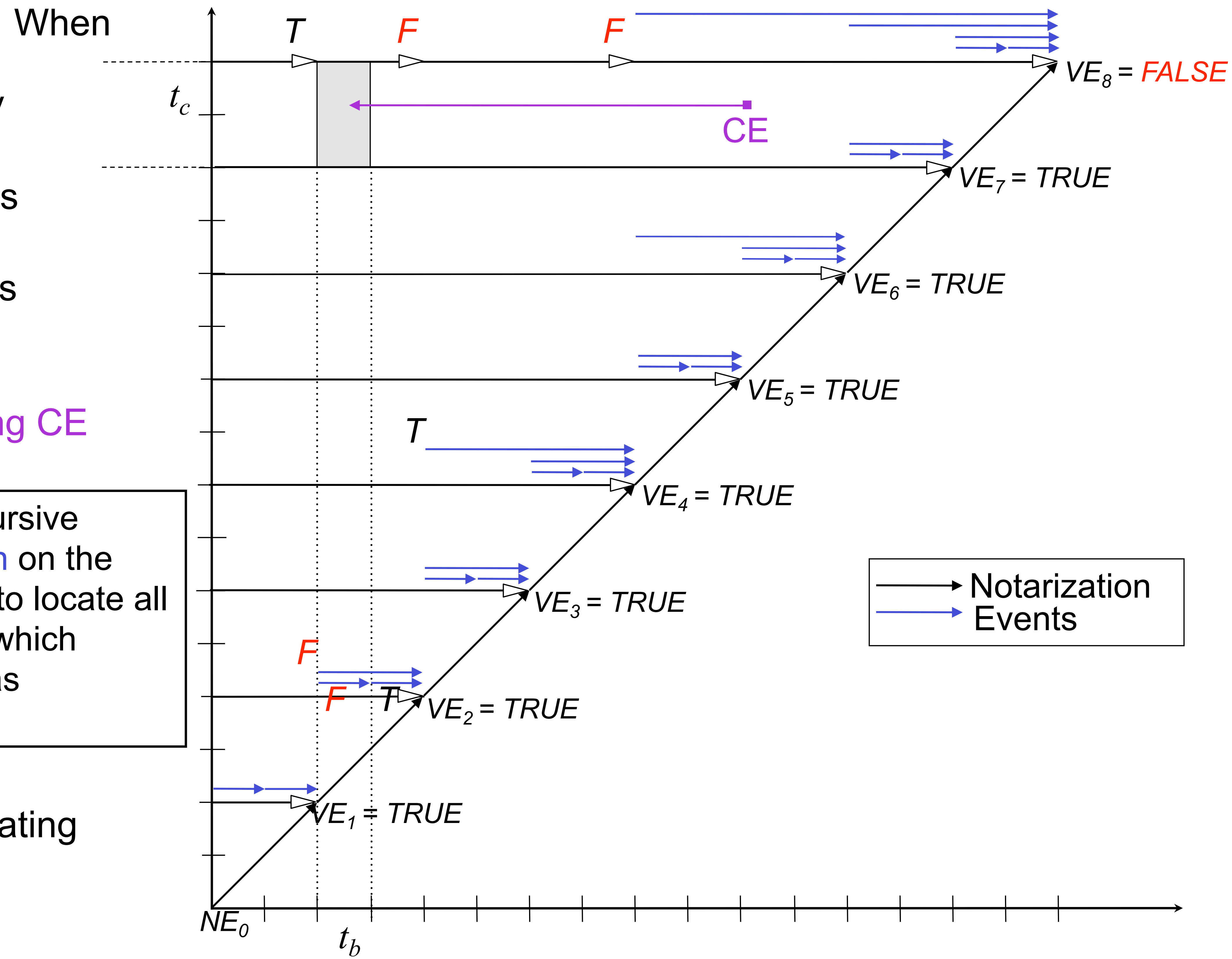
The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



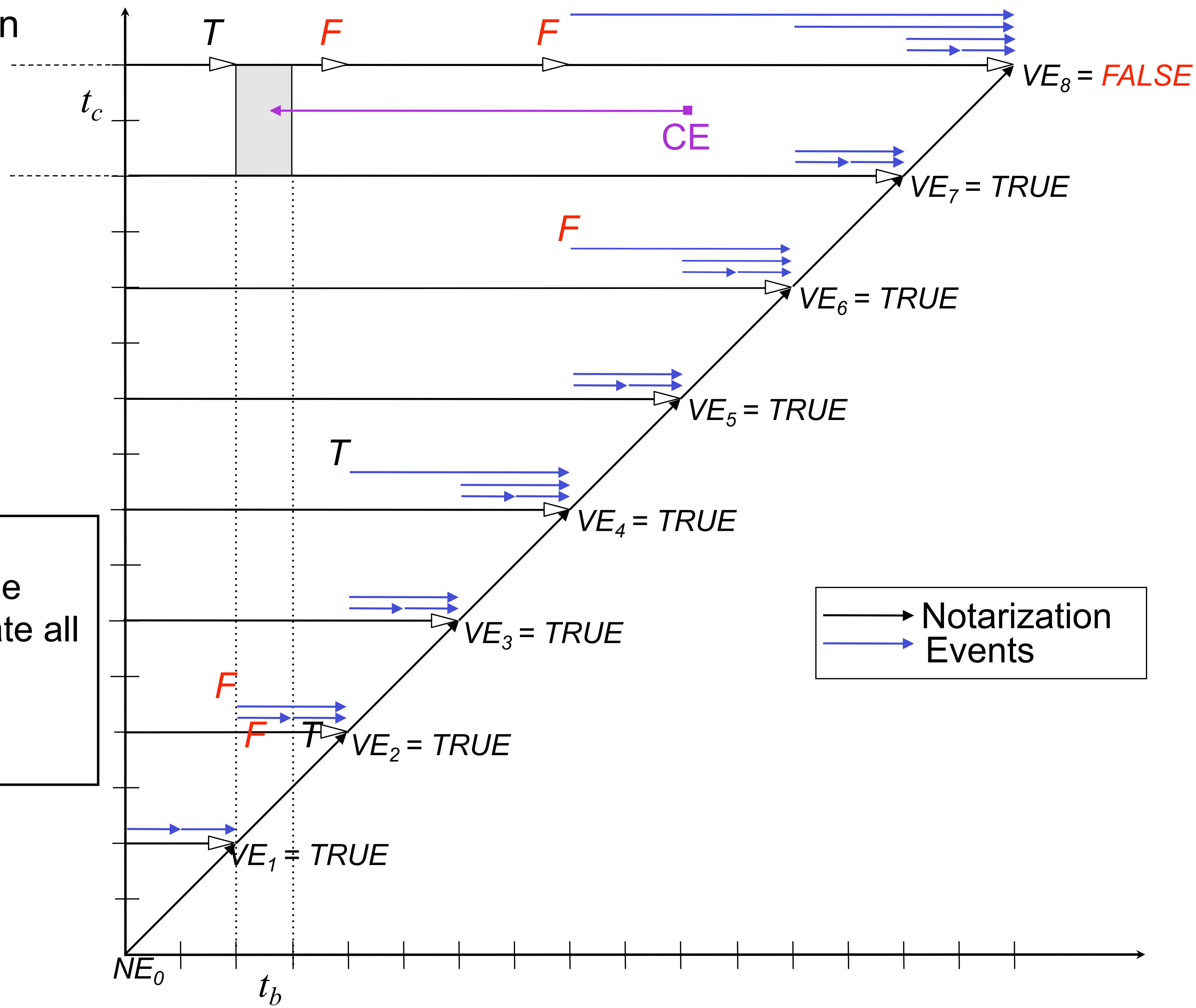
The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

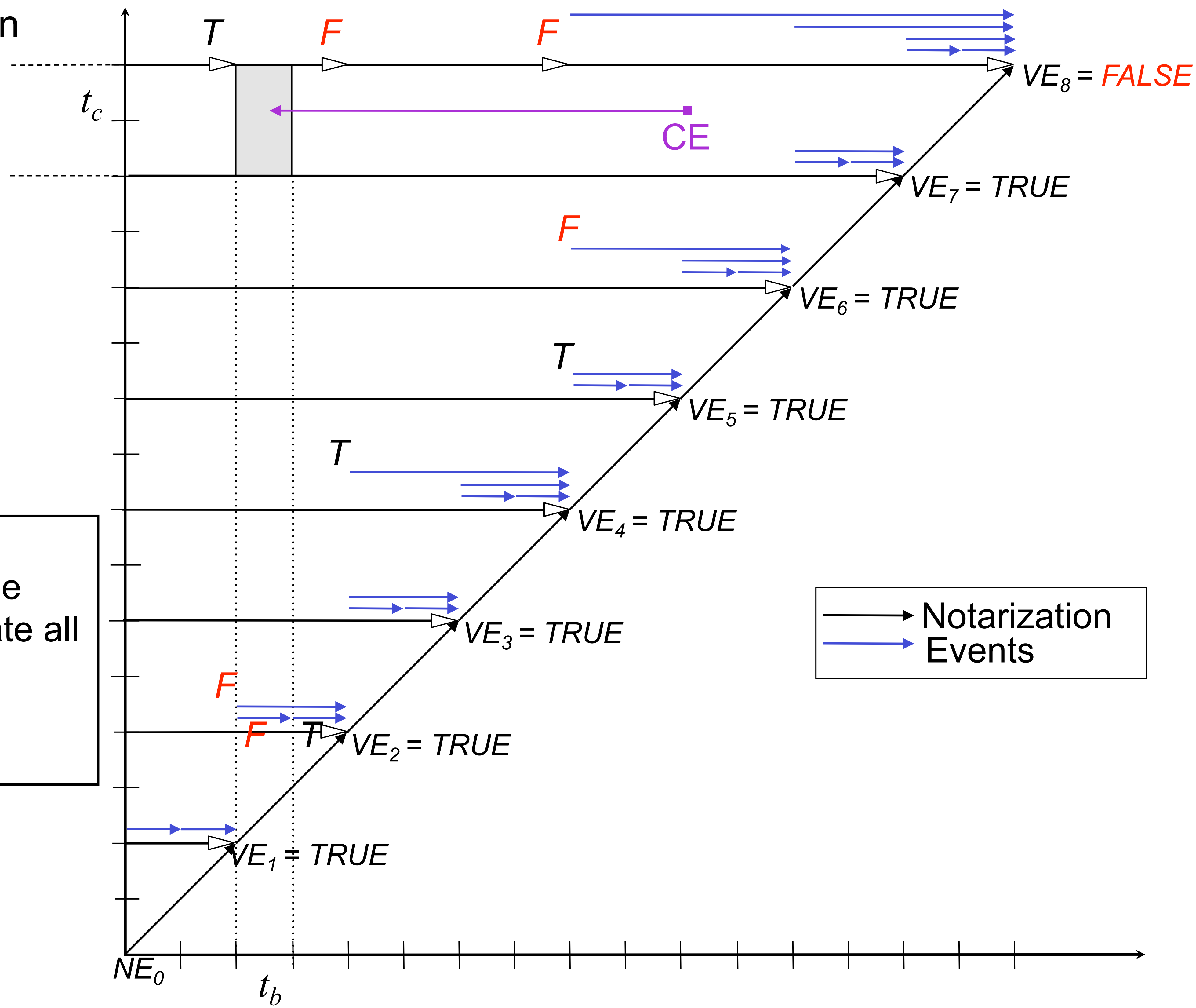
t_b: backdating time



The a3D Algorithm

When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days



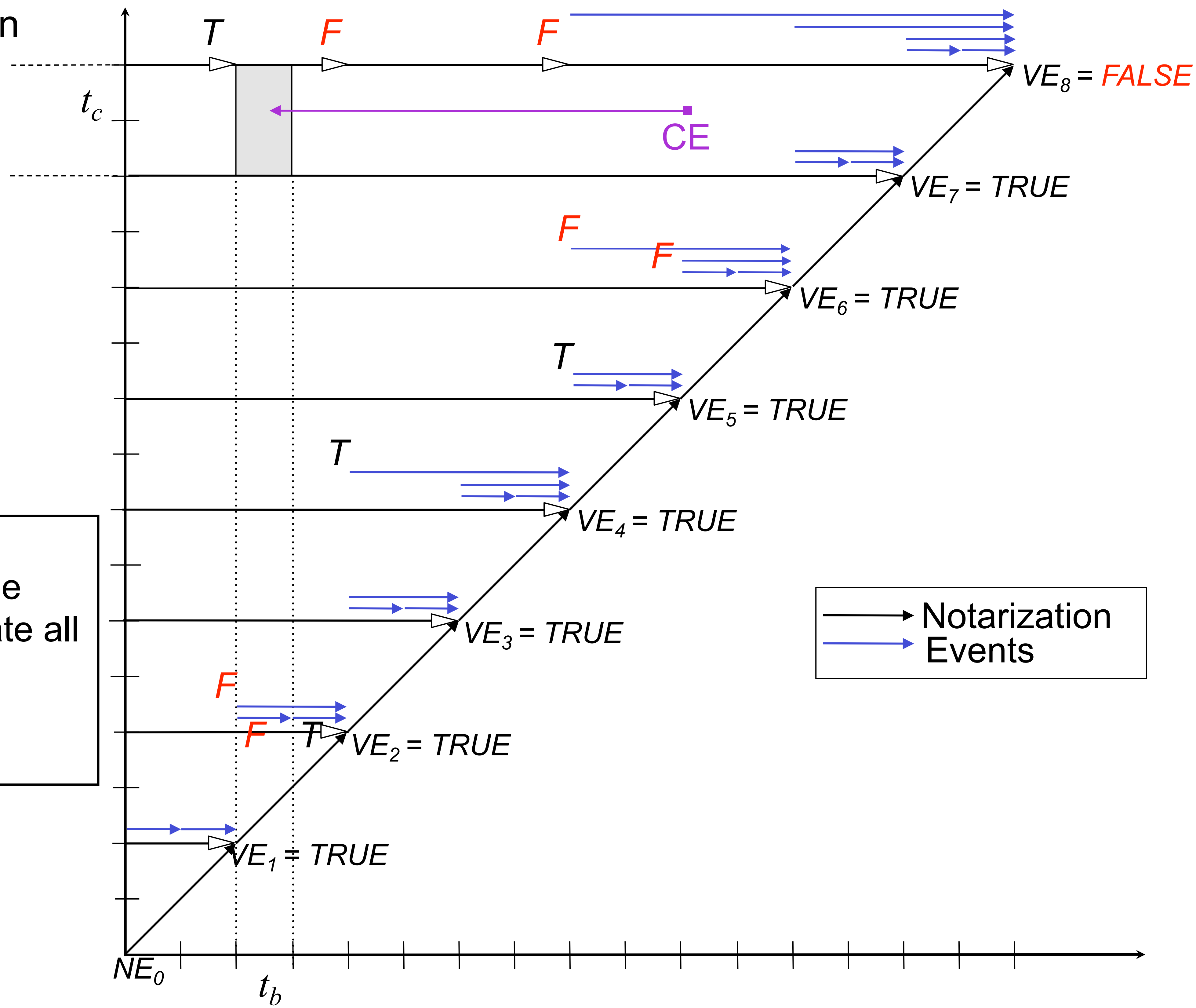
Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time

The a3D Algorithm

When



R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time

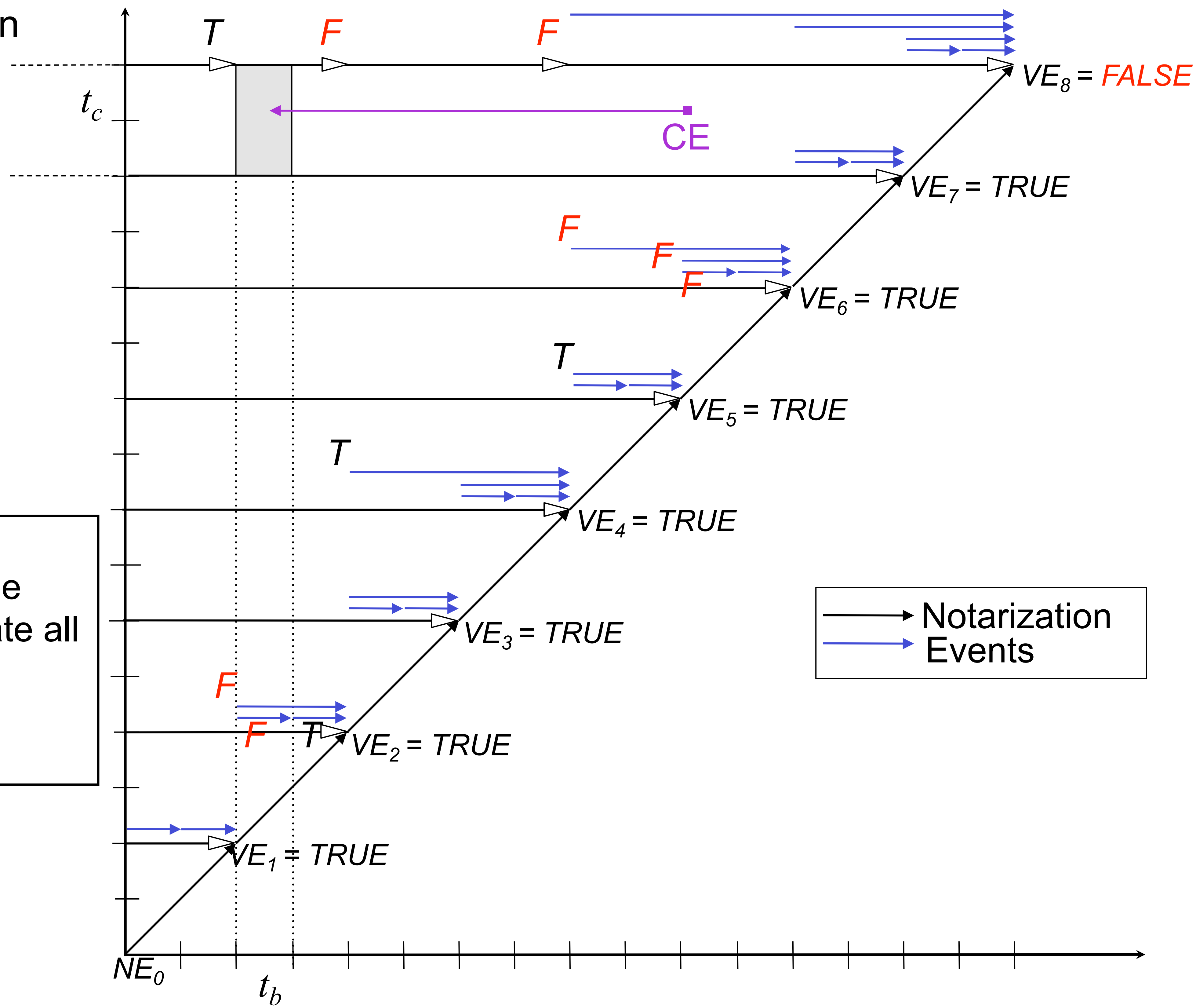
The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



The a3D Algorithm

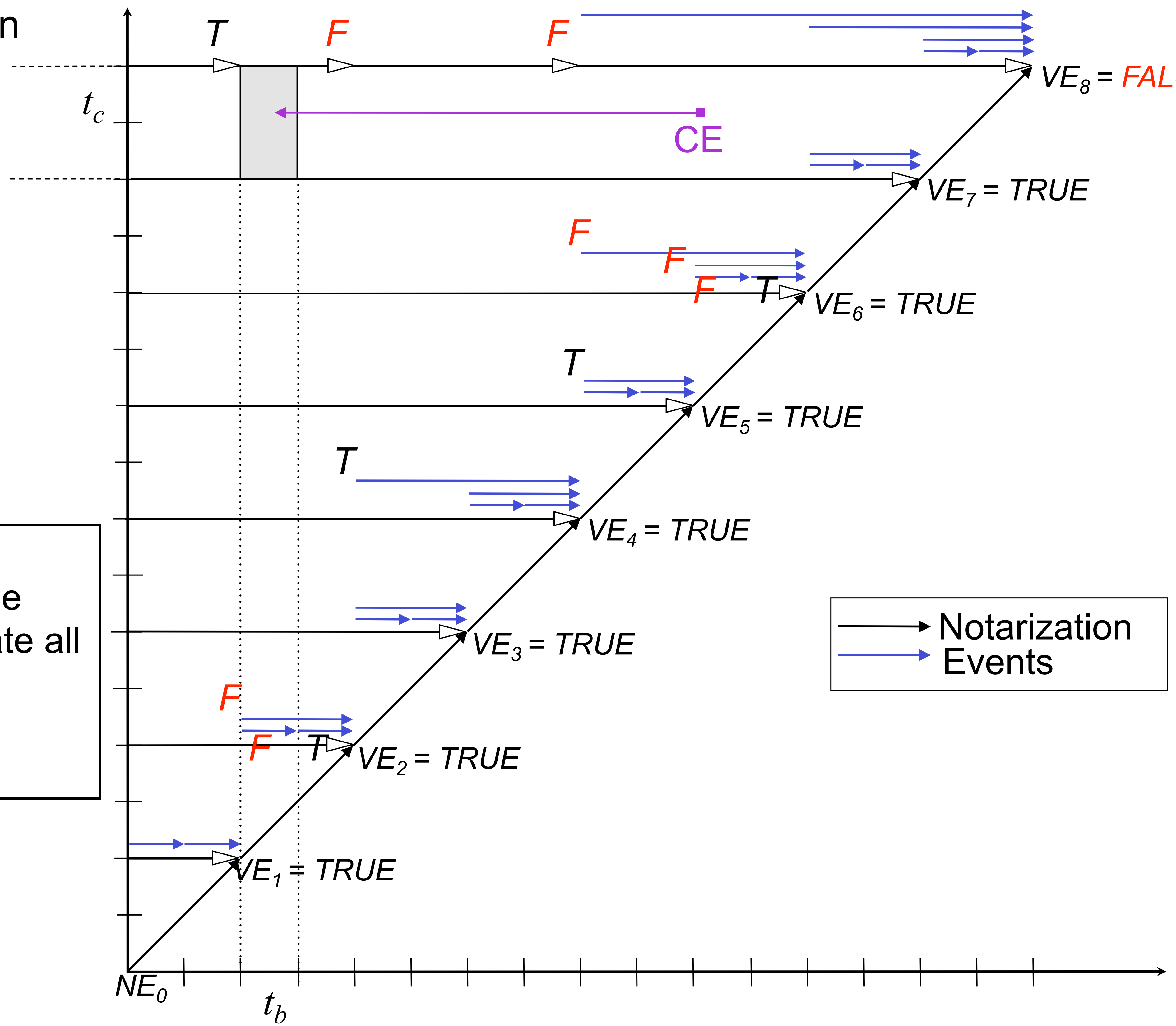
When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



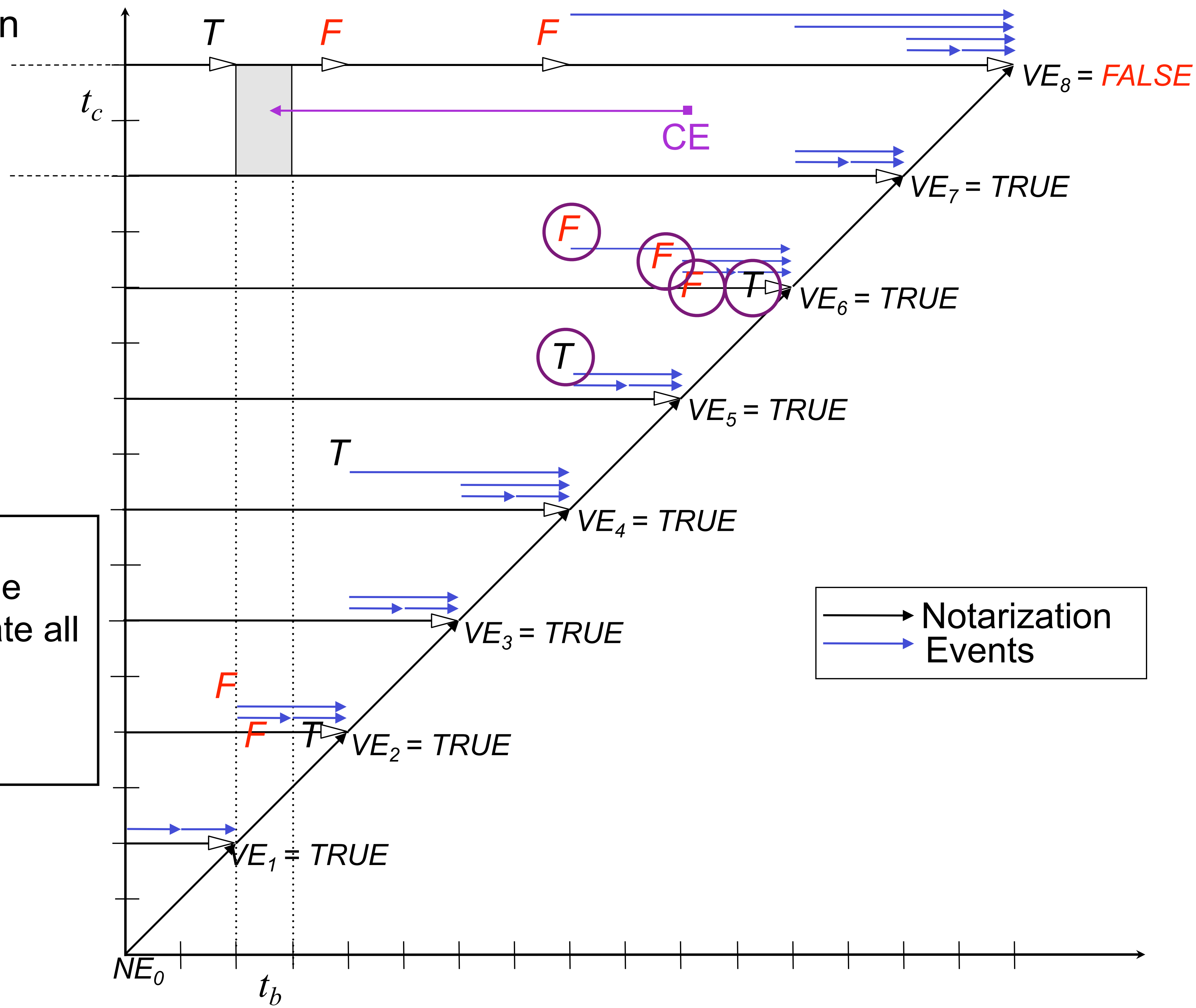
The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



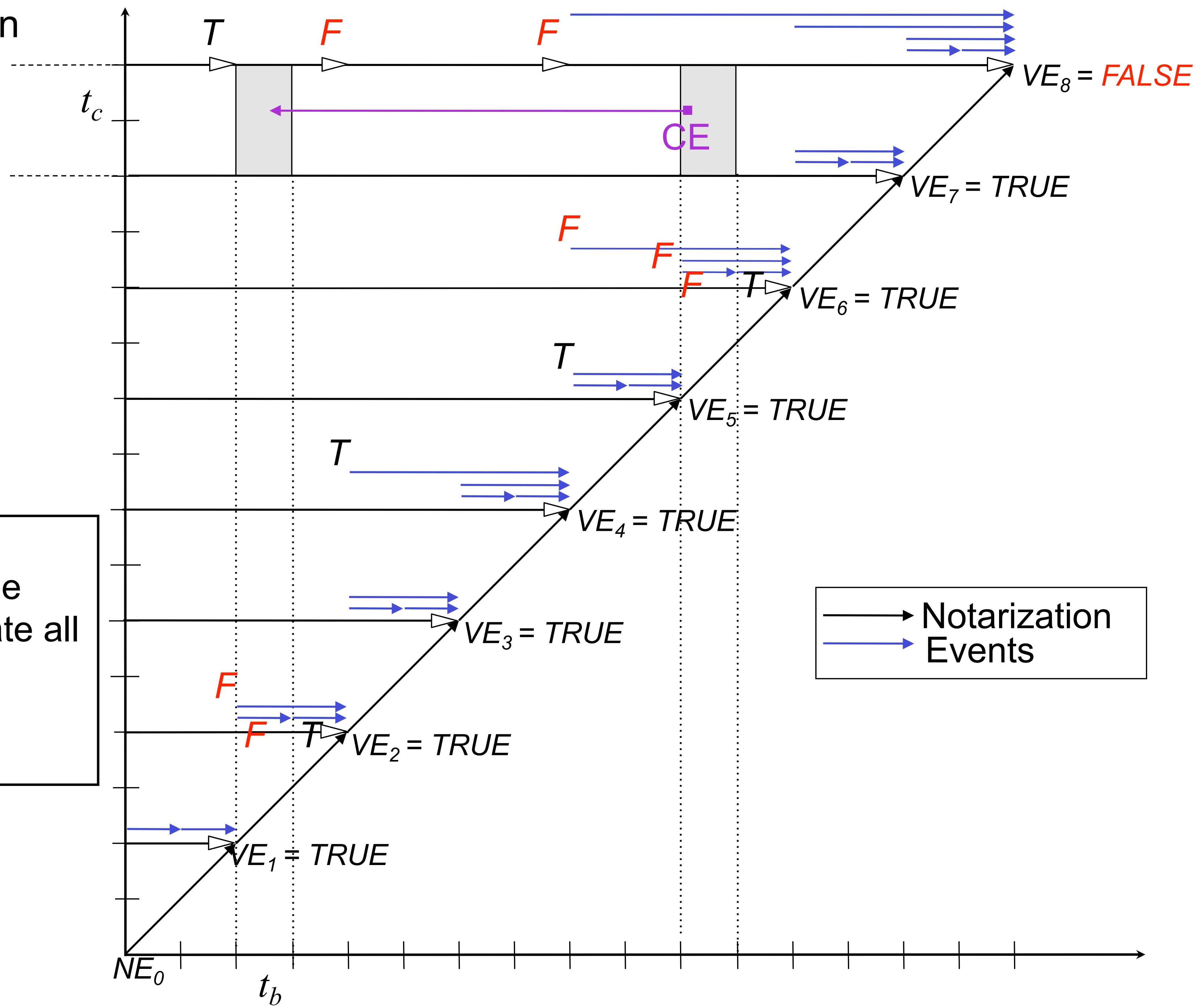
The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



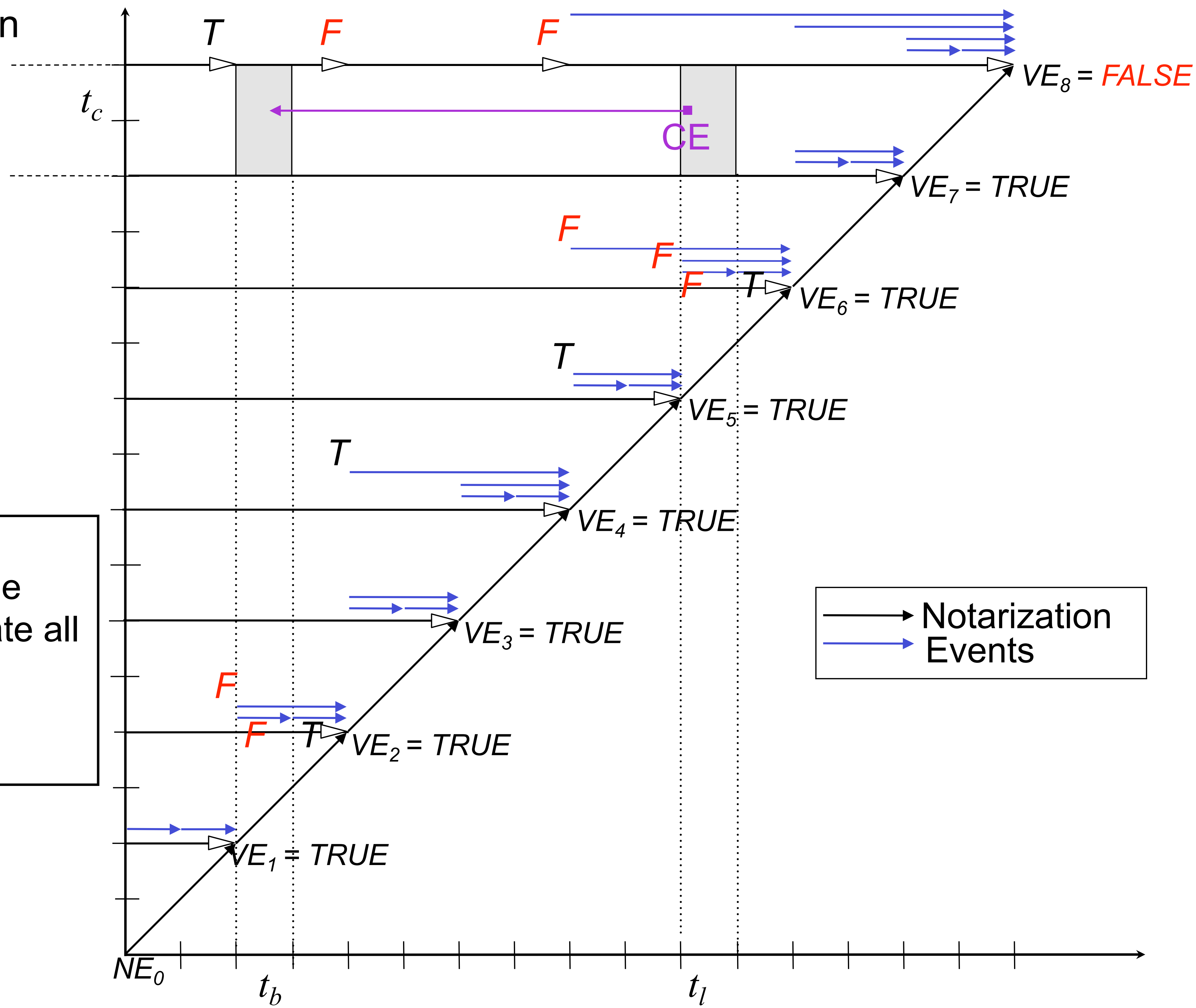
The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



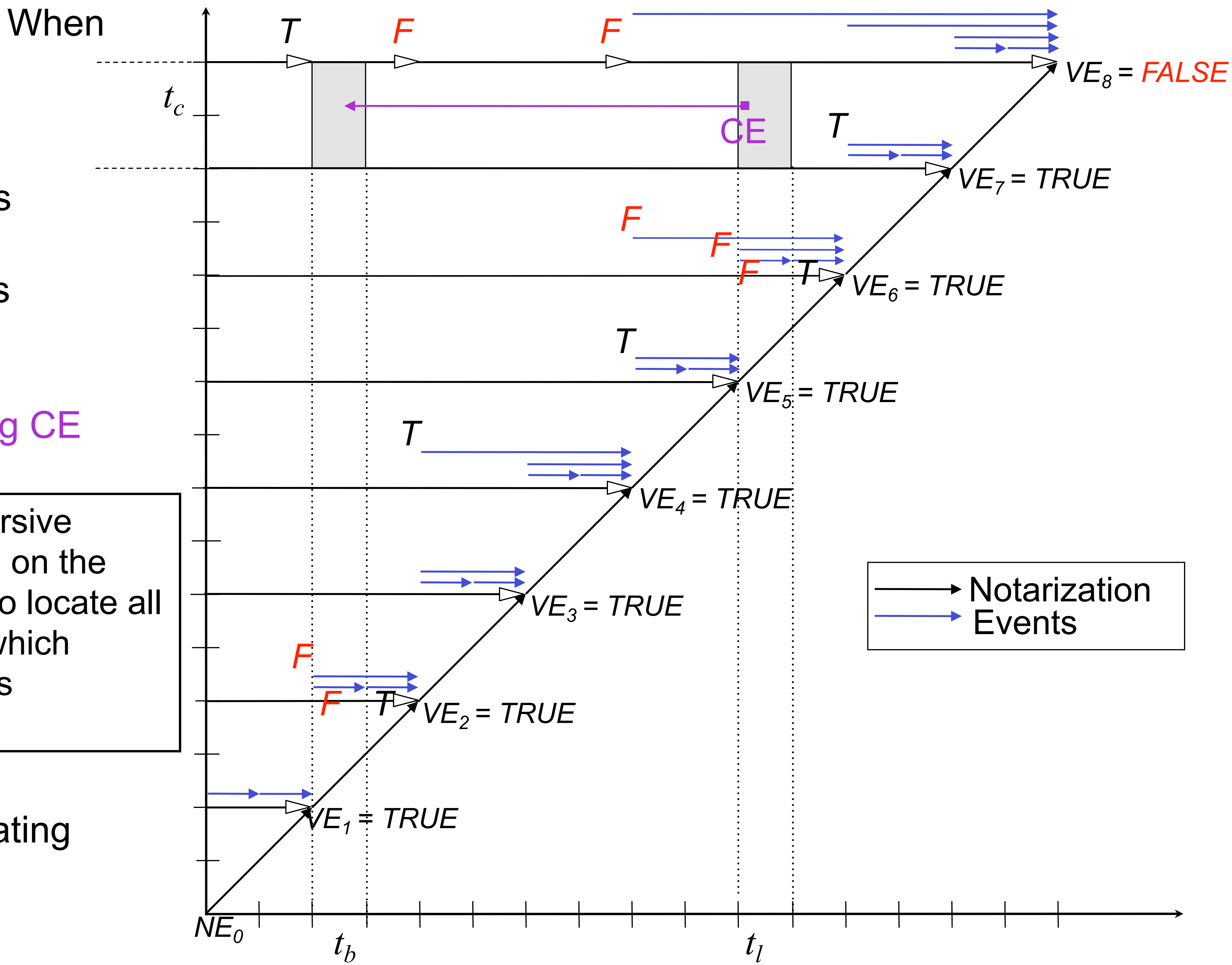
The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



The a3D Algorithm

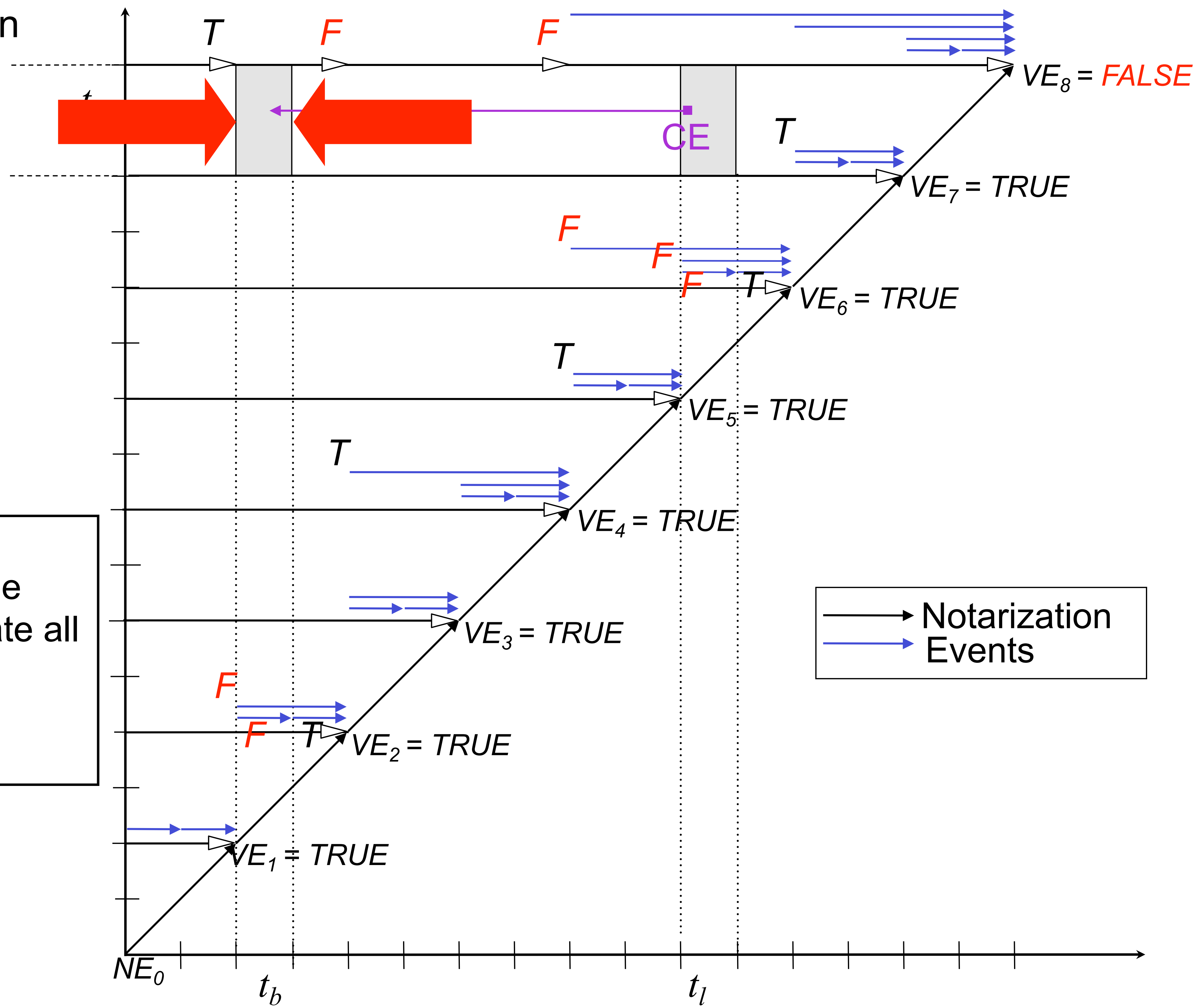
When

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

t_b: backdating time



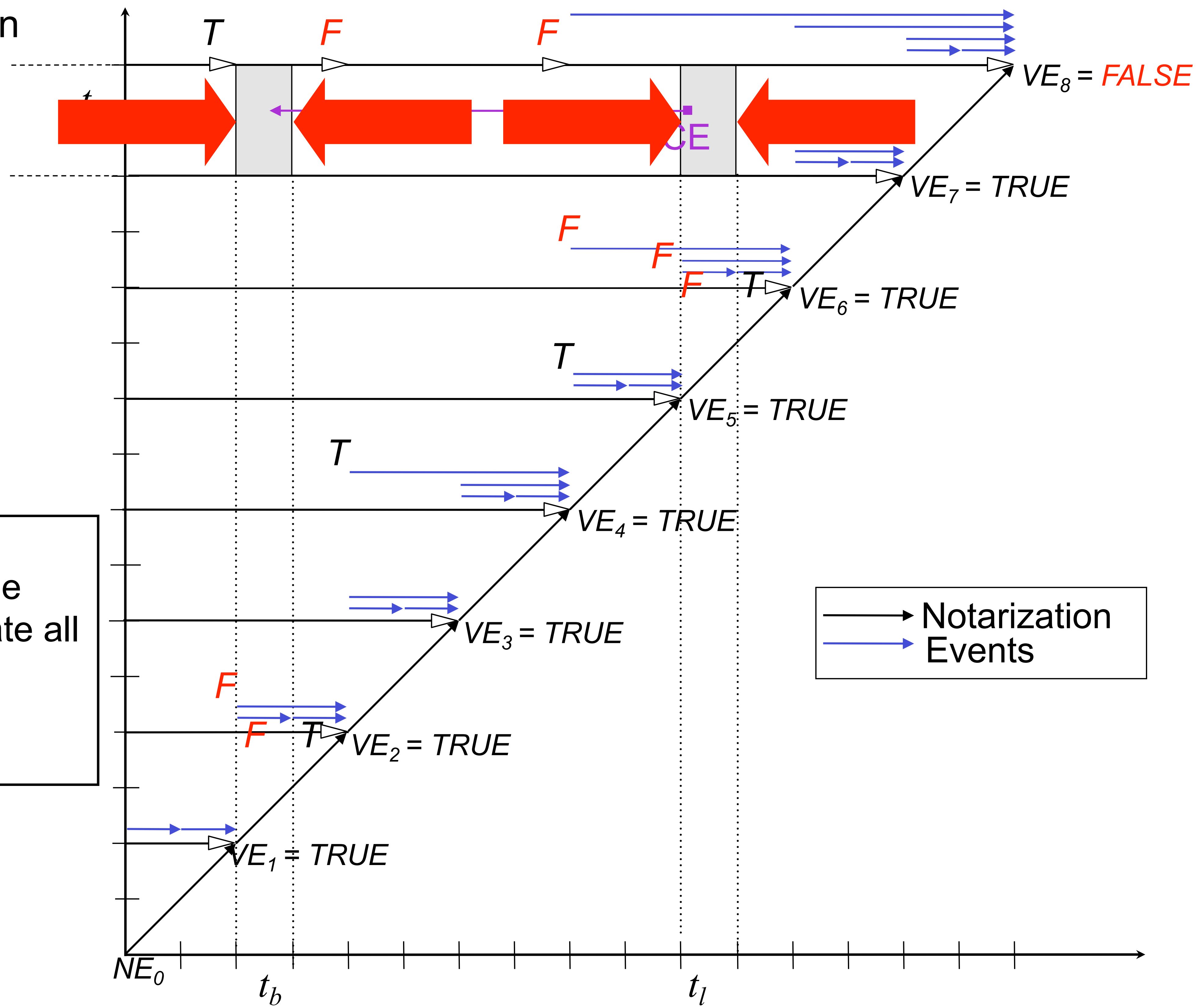
The a3D Algorithm

R_s = 1 day
N = 2
I_N = 2 days
V = 1
I_V = 2 days

Backdating CE

Can use recursive binary search on the hash chains to locate all days during which tampering has occurred.

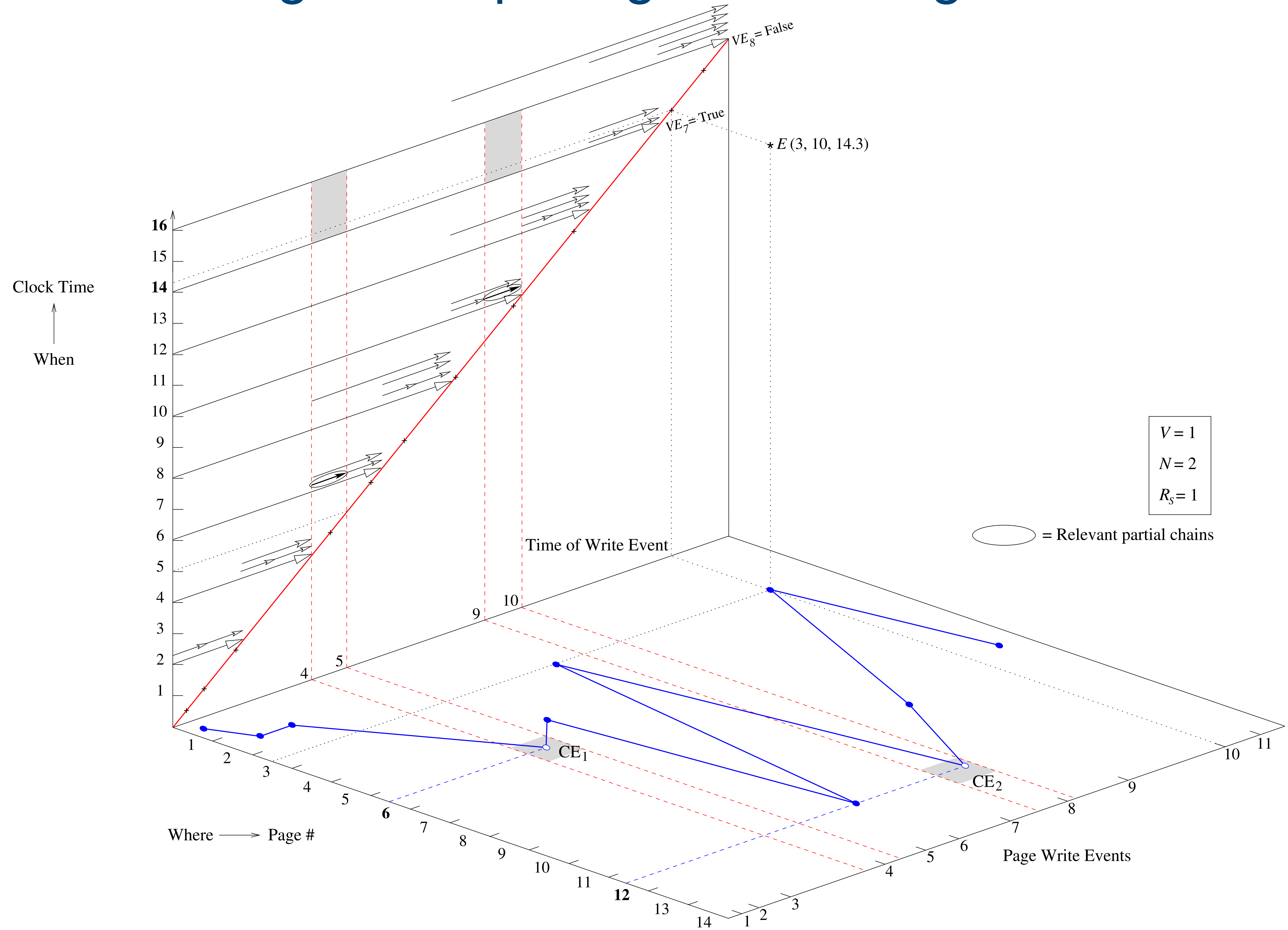
t_b: backdating time



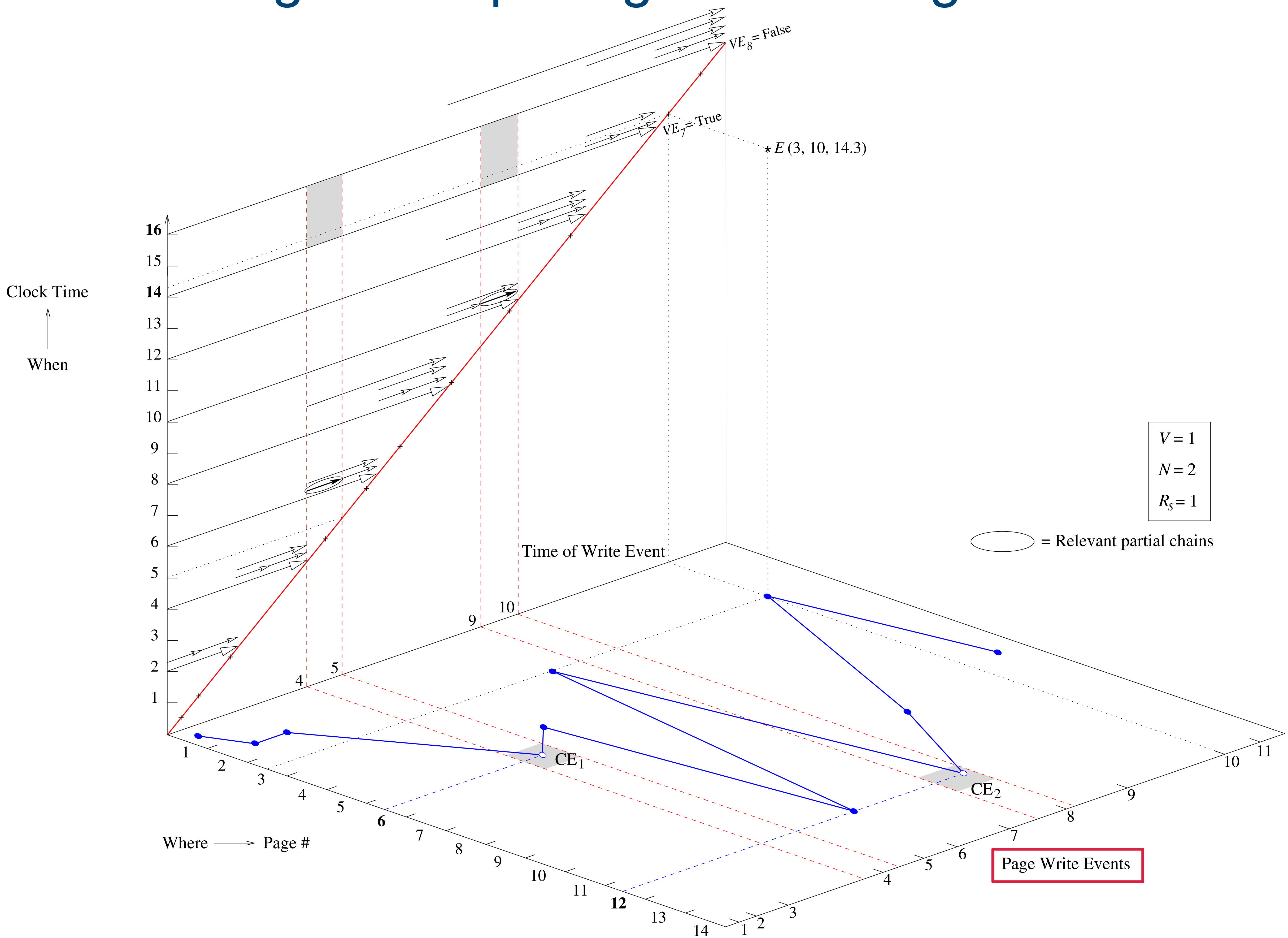
Comparison of Forensic Algorithms

	Partitioning		
	Commit-Time-Based	**Page-Based**	**Attribute-Based**
Tables Affected	Any number	Any number	One or several of those containing the designated attribute
R_s	Time interval	Time interval	Time interval
R_d	N/A	N/A	Number of subsets of domain values
Segment	One of the contiguous *periods* induced by R_s, starting from a particular anchor. Contiguous periods form a chronologically ordered partition.	One of the contiguous *periods* induced by R_s, starting from a particular anchor. Contiguous periods form a chronologically ordered partition.	One of the contiguous *periods* induced by R_s, starting from a particular anchor. Contiguous periods form a chronologically ordered partition.
Granule	Encompasses all tuples with *commit times* within the associated segment (one granule has tuples from many transactions committing in that segment).	Encompasses all tuples whose *physical location* is in a page mentioned within the associated segment.	Encompasses all tuples with *commit times* within the associated segment (one granule has tuples from many transactions committing in that segment).
Hashing order	Transactions hashed in order of increasing *commit time*.	Granules hashed in chronological *order of* "page write" *event* of the page. Granules not hashed in order of page number.	Transactions hashed in order of increasing *commit time*.
Segment Completion Event	When the last *tuple* in the granule associated with that segment commits	When the last *page* write event in the segment occurs.	When the last *tuple* in the granule associated with that segment commits
Notarization Factor (N)	Specified by DBA	Specified by DBA	Specified by DBA
Validation Factor (V)	Specified by DBA	Specified by DBA	Specified by DBA
I_N	$N \times R_s$	$N \times R_s$	$N \times R_s$
I_V	$V \times I_N$	$V \times I_N$	$V \times I_N$
Notarization	Occurs *as soon as* N granules are hashed.	Occurs *as soon as* N granules are hashed.	Occurs *as soon as* N granules are hashed.
Validation	Occurs as soon as V notarizations have occurred.	Occurs as soon as V notarizations have occurred.	Occurs as soon as V notarizations have occurred.

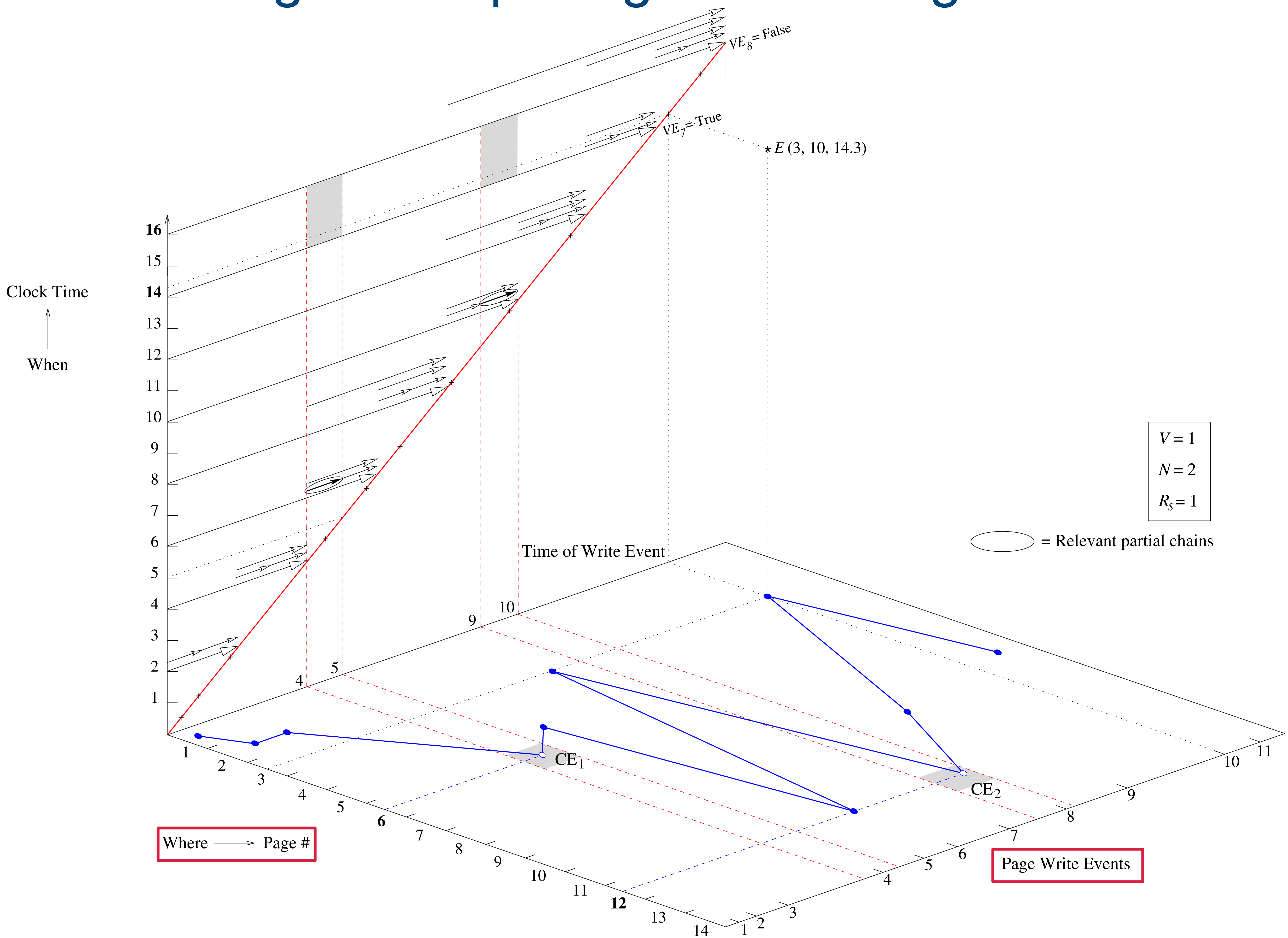
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



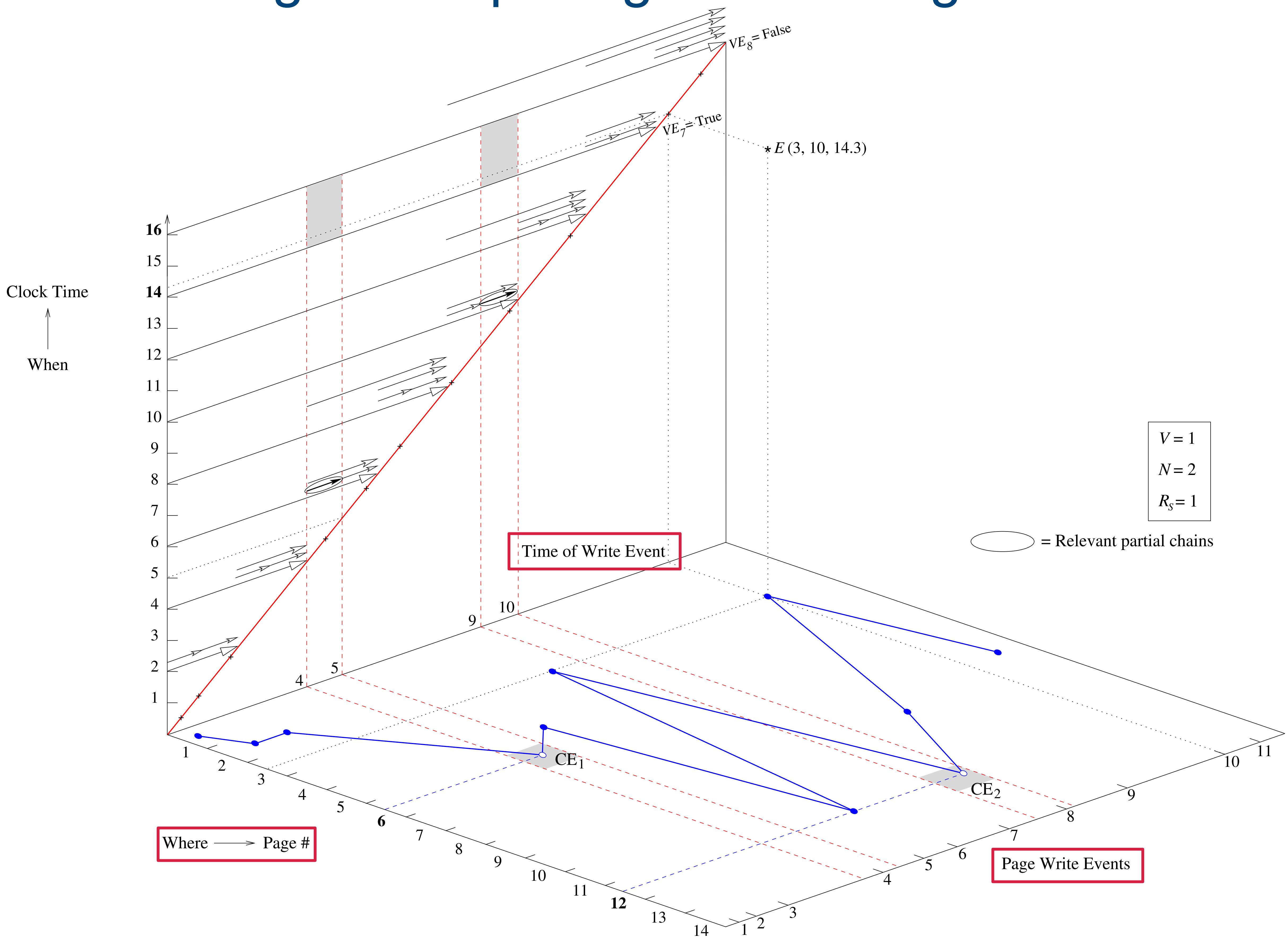
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



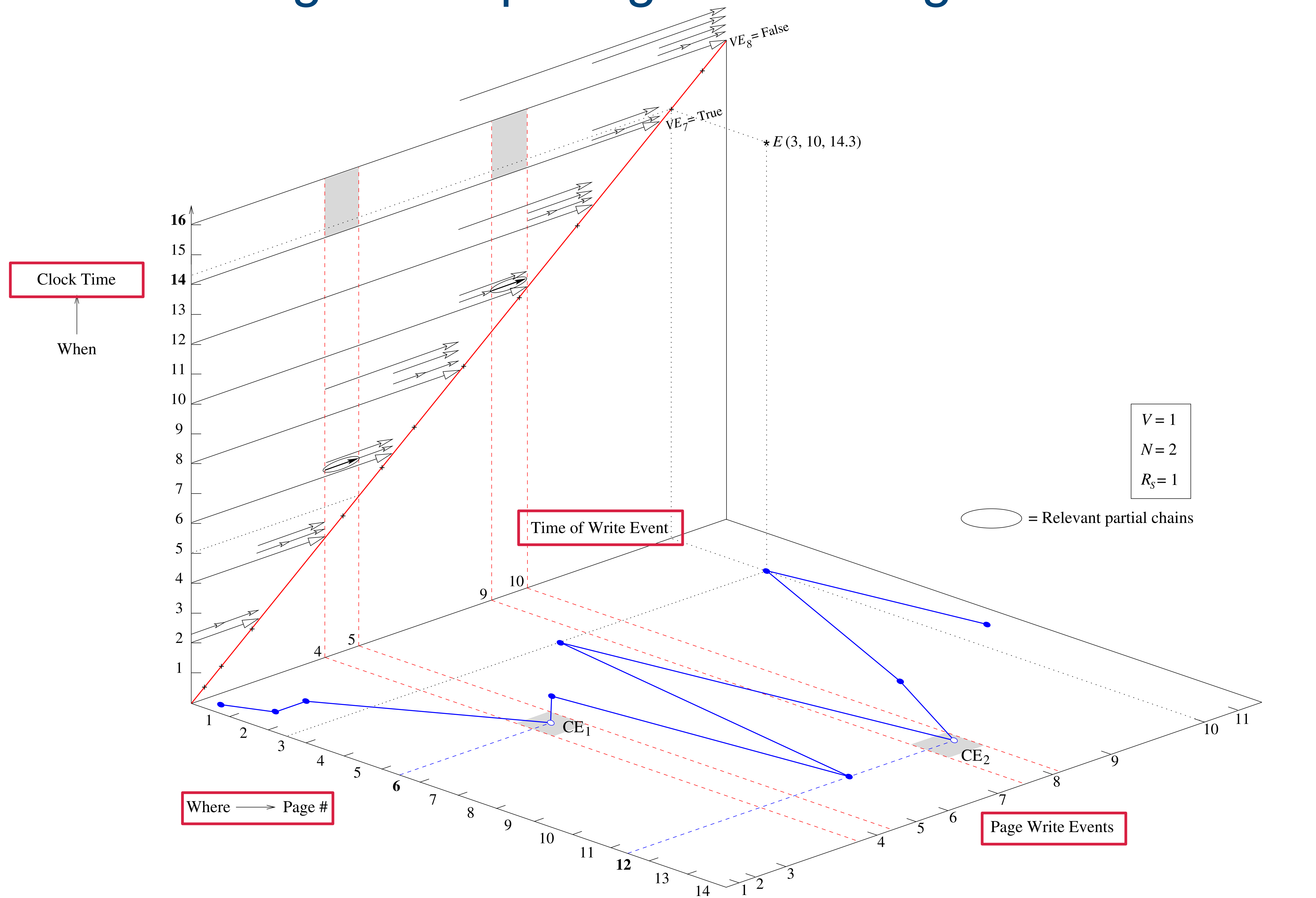
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



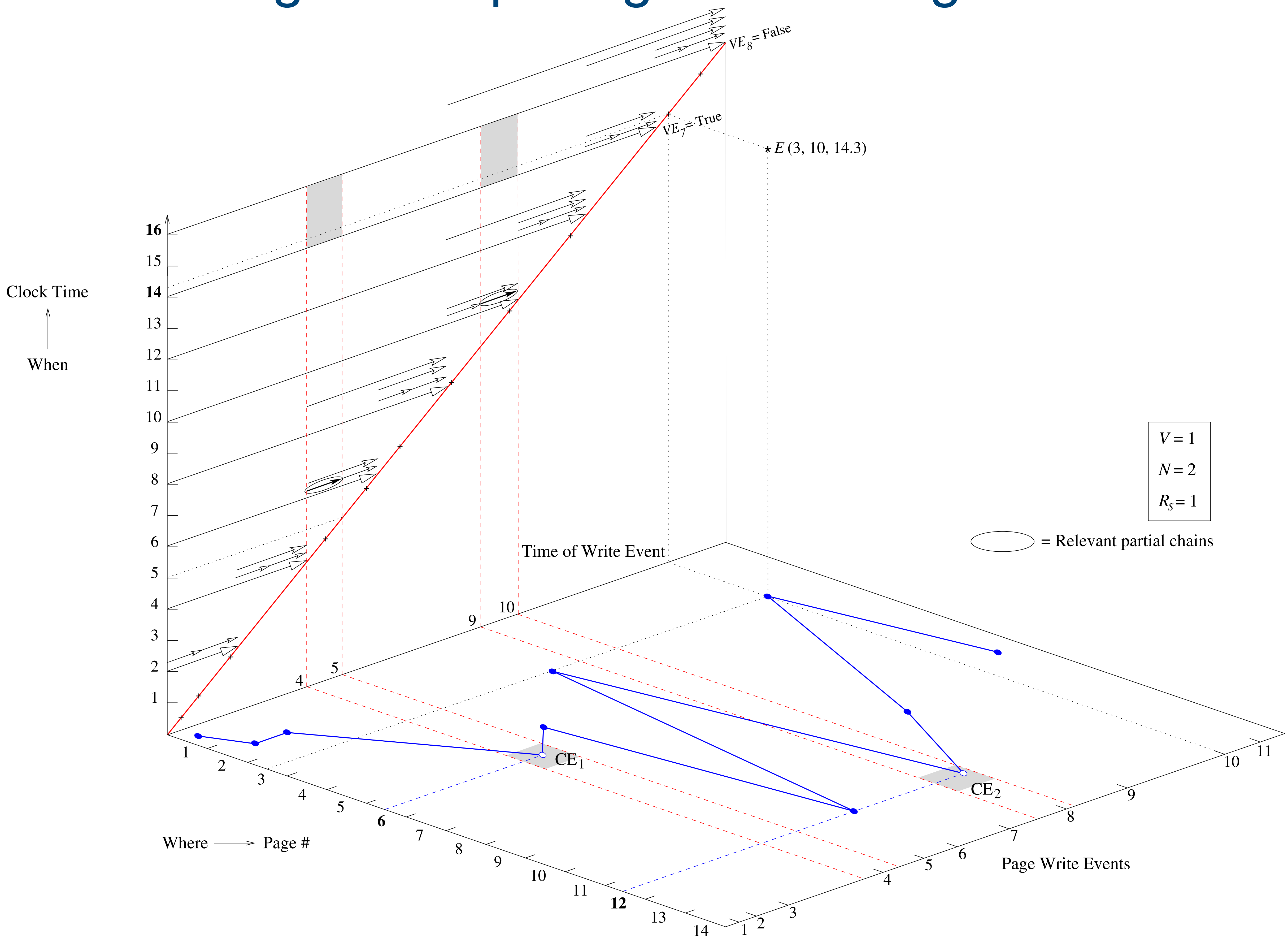
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



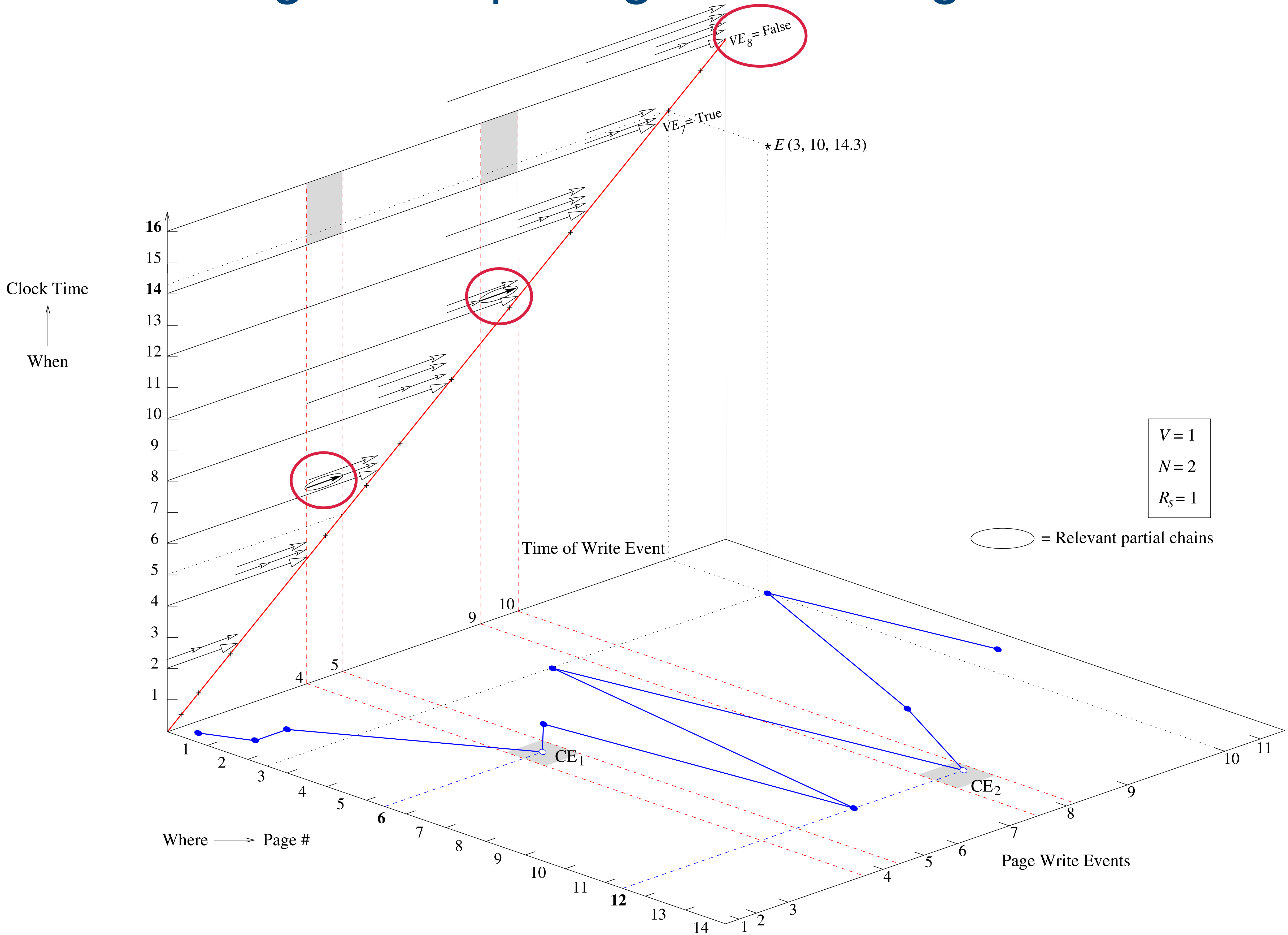
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



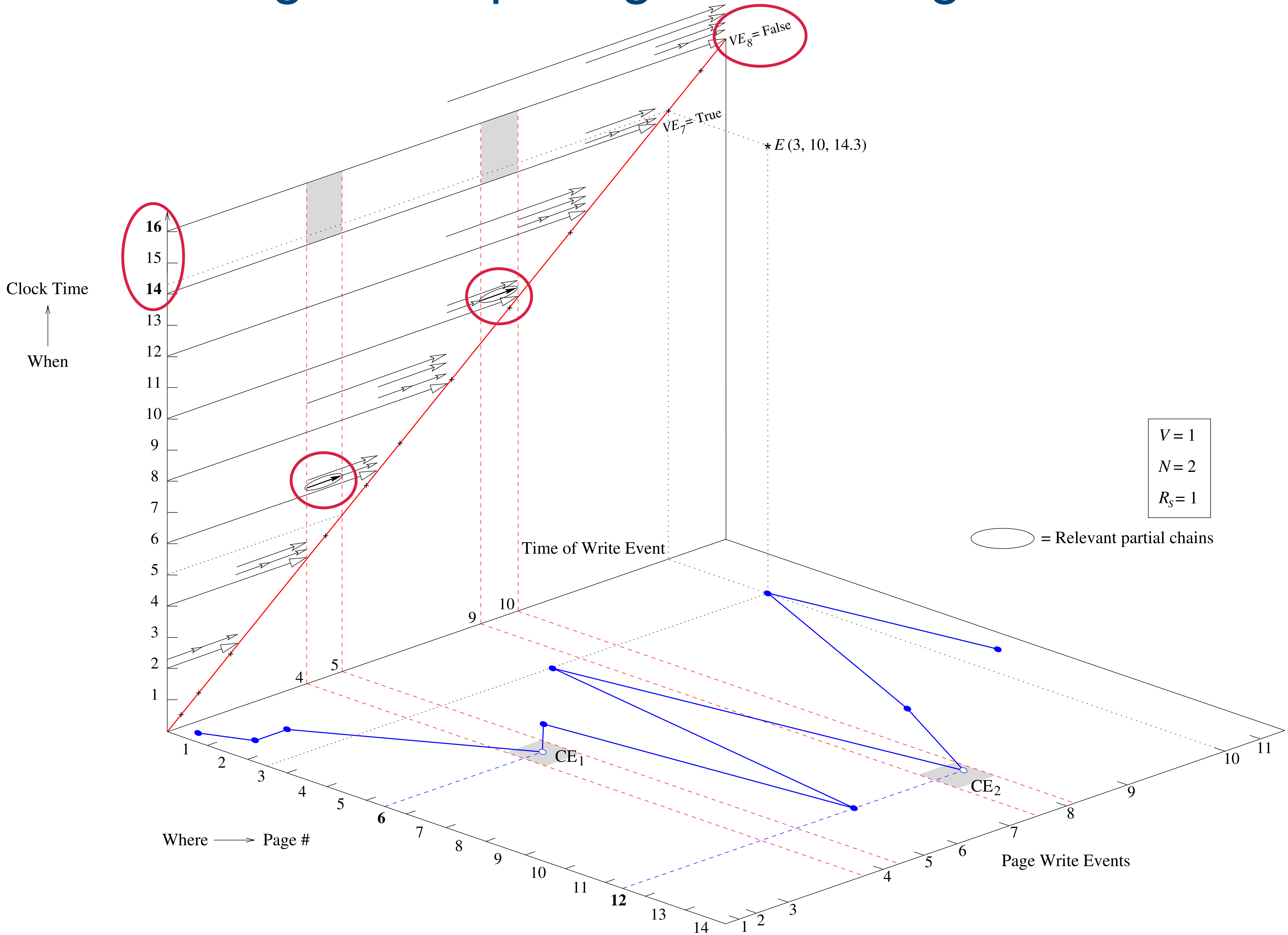
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



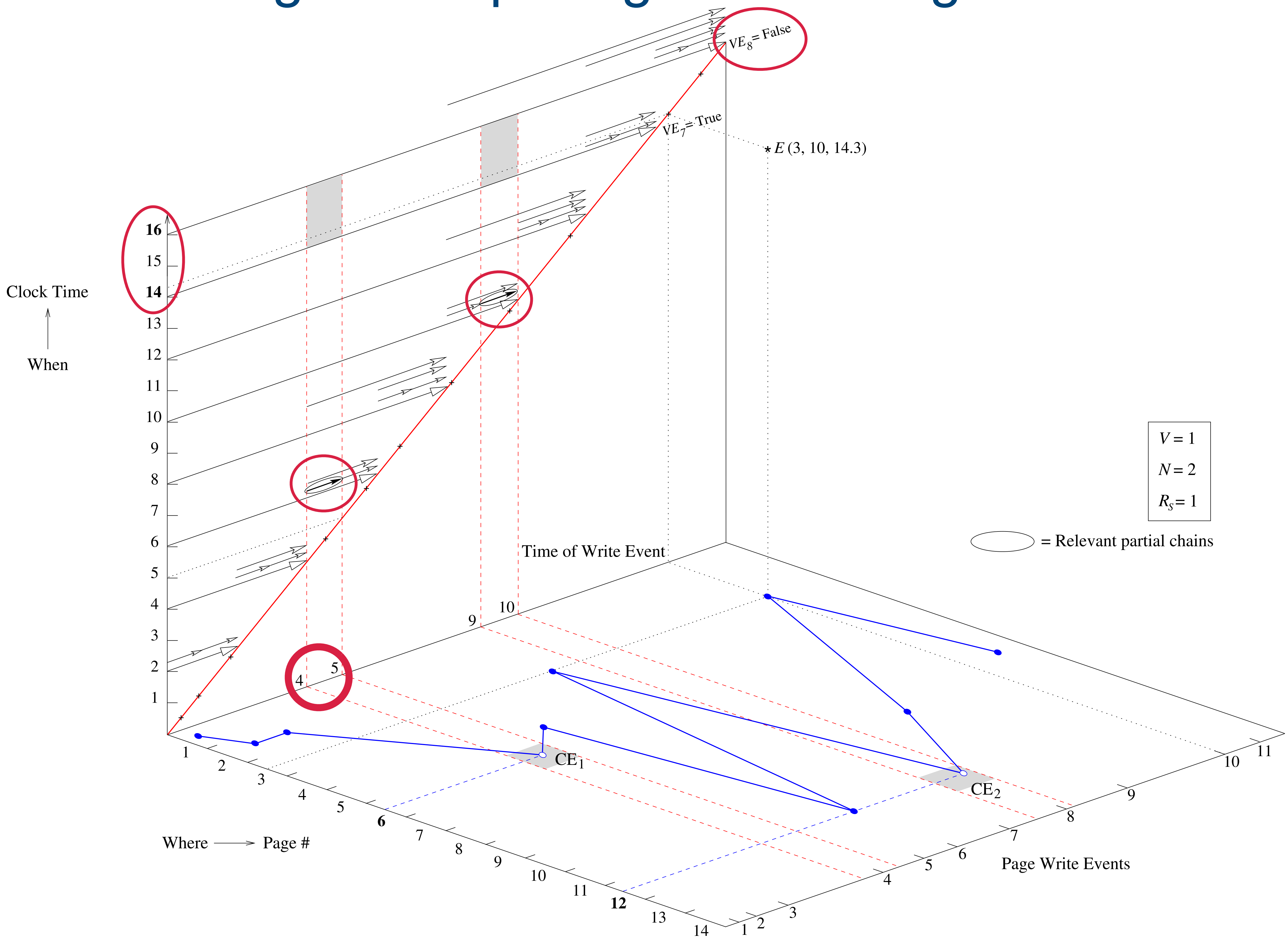
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



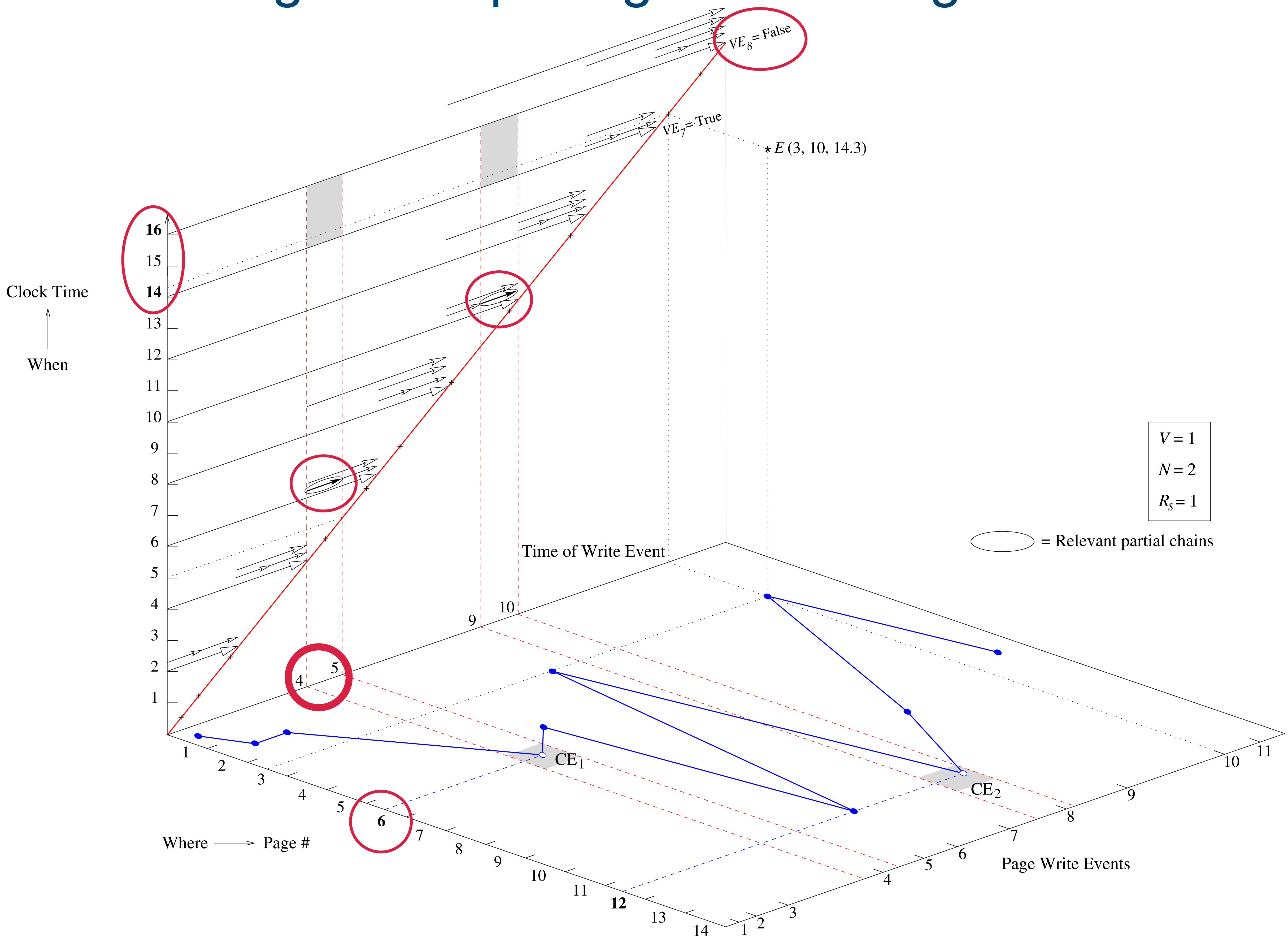
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



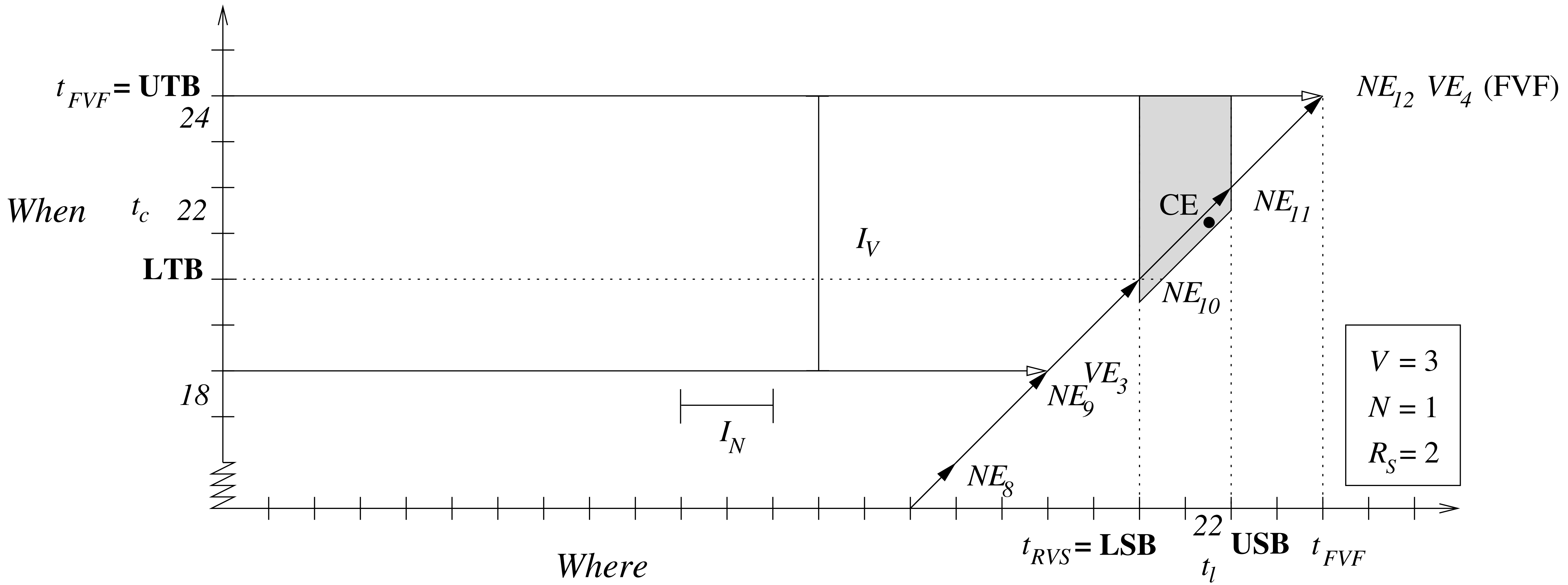
The Correlated Page-Based Corruption Diagram Depicting the a3D Algorithm



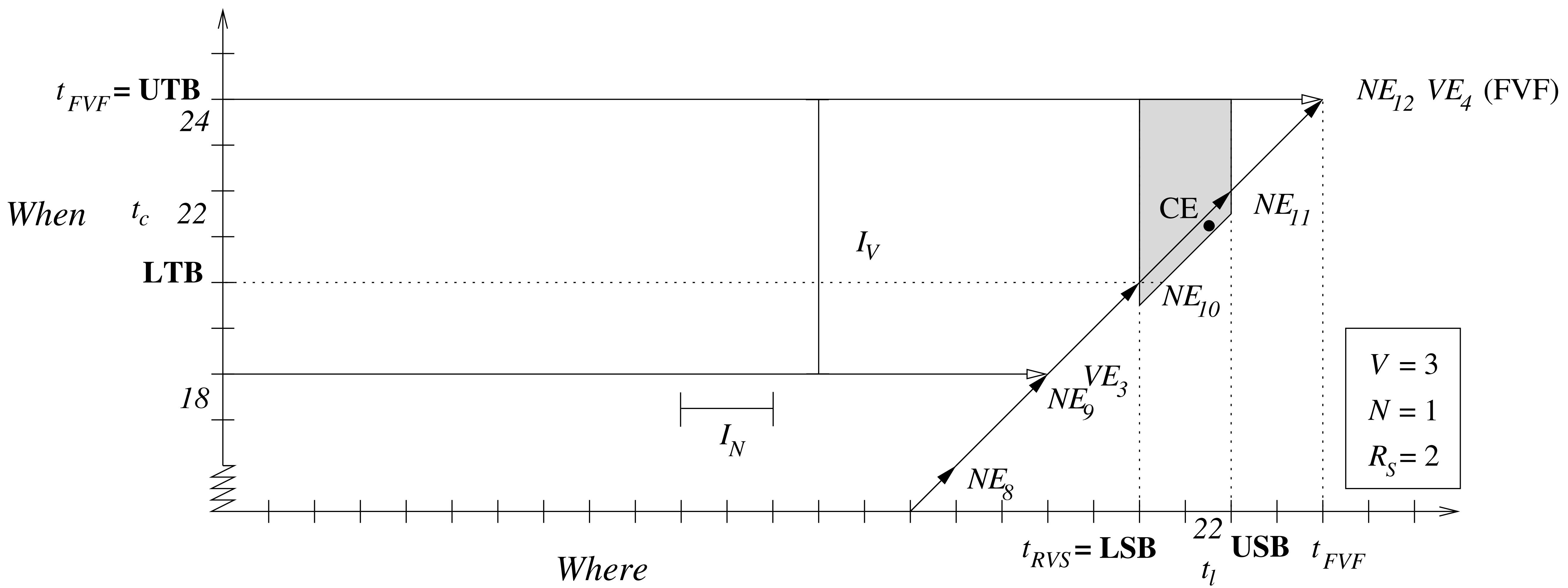
Outline

- Information Accountability
- Reference Architecture & Execution Phases
- Forensic Analysis
- Refinements
- Enterprise Considerations

Very Recent Corruptions

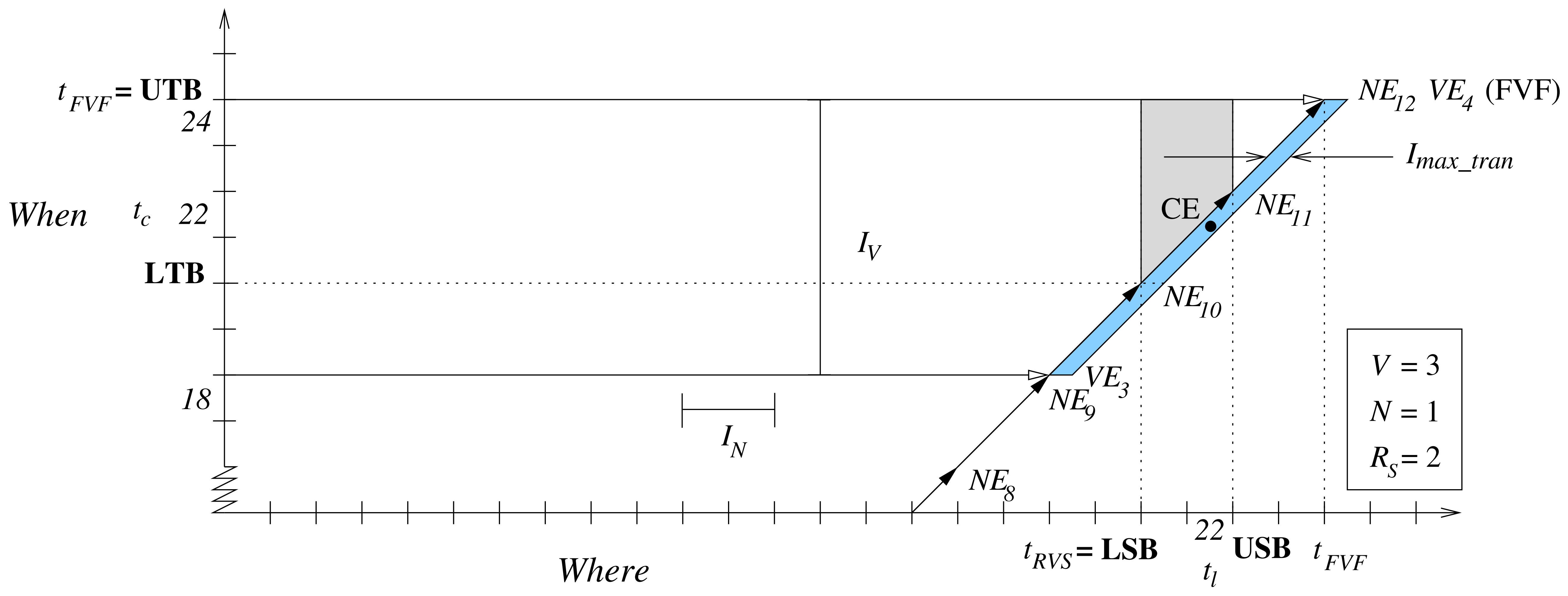


Very Recent Corruptions



- In general $t_c > t_l$
- Exception: corruption affects currently executing transaction

Very Recent Corruptions



- In general $t_c > t_l$
- Exception: corruption affects currently executing transaction
- Introduce "envelope" of width I_{max_tran}

Very Recent Corruptions (2)

Very Recent Corruptions (2)

- Different solution: Exploit the Regret Interval

Very Recent Corruptions (2)

- Different solution: Exploit the Regret Interval
- The regret interval (I_R) is the minimum time interval before any adversary can reverse the change they made.

Very Recent Corruptions (2)

- Different solution: Exploit the Regret Interval
- The regret interval (I_R) is the minimum time interval before any adversary can reverse the change they made.
- I_R is intrinsic to the semantics and social use of application. We have no control over it.

Very Recent Corruptions (2)

- Different solution: Exploit the Regret Interval
- The regret interval (I_R) is the minimum time interval before any adversary can reverse the change they made.
- I_R is intrinsic to the semantics and social use of application. We have no control over it.
- We use an estimate $I_R^* \leq I_R$

Very Recent Corruptions (2)

- Different solution: Exploit the Regret Interval
- The regret interval (I_R) is the minimum time interval before any adversary can reverse the change they made.
- I_R is intrinsic to the semantics and social use of application. We have no control over it.
- We use an estimate $I_R^* \leq I_R$
- No introactive corruptions: $0 < I_N \leq I_V < I_R^* \leq I_R$

Shredding

Shredding

- Transaction time semantics require that data are never physically deleted.
  - Performance overhead
  - Privacy and liability threat

Shredding

- Transaction time semantics require that data are never physically deleted.
  - Performance overhead
  - Privacy and liability threat

- Retention period: a sliding time frame I_{RP}
  - Determined by regulations & company policy
  - Record physically deleted after exiting $now - I_{RP}$

Shredding

- Transaction time semantics require that data are never physically deleted.
  - Performance overhead
  - Privacy and liability threat

- Retention period: a sliding time frame I_{RP}
  - Determined by regulations & company policy
  - Record physically deleted after exiting $now - I_{RP}$

- Shredding ensures information restriction.
  - Breaks semantics of information accountability
  - Reconcile shredding with tamper detection and forensic analysis?

Litigation Holds

Litigation Holds

- Litigation holds can be issued on the data for a duration of time as specified by a court.

Litigation Holds

- Litigation holds can be issued on the data for a duration of time as specified by a court.
- Override retention period regulations

Litigation Holds

- Litigation holds can be issued on the data for a duration of time as specified by a court.
- Override retention period regulations
- Litigation holds “restore” info accountability.

Litigation Holds

- Litigation holds can be issued on the data for a duration of time as specified by a court.
- Override retention period regulations
- Litigation holds “restore” info accountability.
- The capability to impose litigation holds prevents indiscriminate shredding and ensures accountability.

Outline

- Information Accountability
- Reference Architecture & Execution Phases
- Forensic Analysis
- Refinements
- Enterprise Considerations

Enterprise Architecture GUIs

Enterprise Architecture GUIs

- There are three GUIs:
  - Chief Security Office (CSO)
  - Database Administrator (DBA)
  - Crime Scene Investigator (CSI)

Enterprise Architecture GUIs

- There are three GUIs:
  - Chief Security Office (CSO)
  - Database Administrator (DBA)
  - Crime Scene Investigator (CSI)

- Configure the security policies by
  - selecting a database to be monitored
  - setting the security parameters, e.g., R_s, N, V, I_N

Enterprise Architecture GUIs

- There are three GUIs:
  - Chief Security Office (CSO)
  - Database Administrator (DBA)
  - Crime Scene Investigator (CSI)

- Configure the security policies by
  - selecting a database to be monitored
  - setting the security parameters, e.g., R_s, N, V, I_N

- Calculate the forensic cost for normal processing and forensic analysis

Enterprise Architecture GUIs

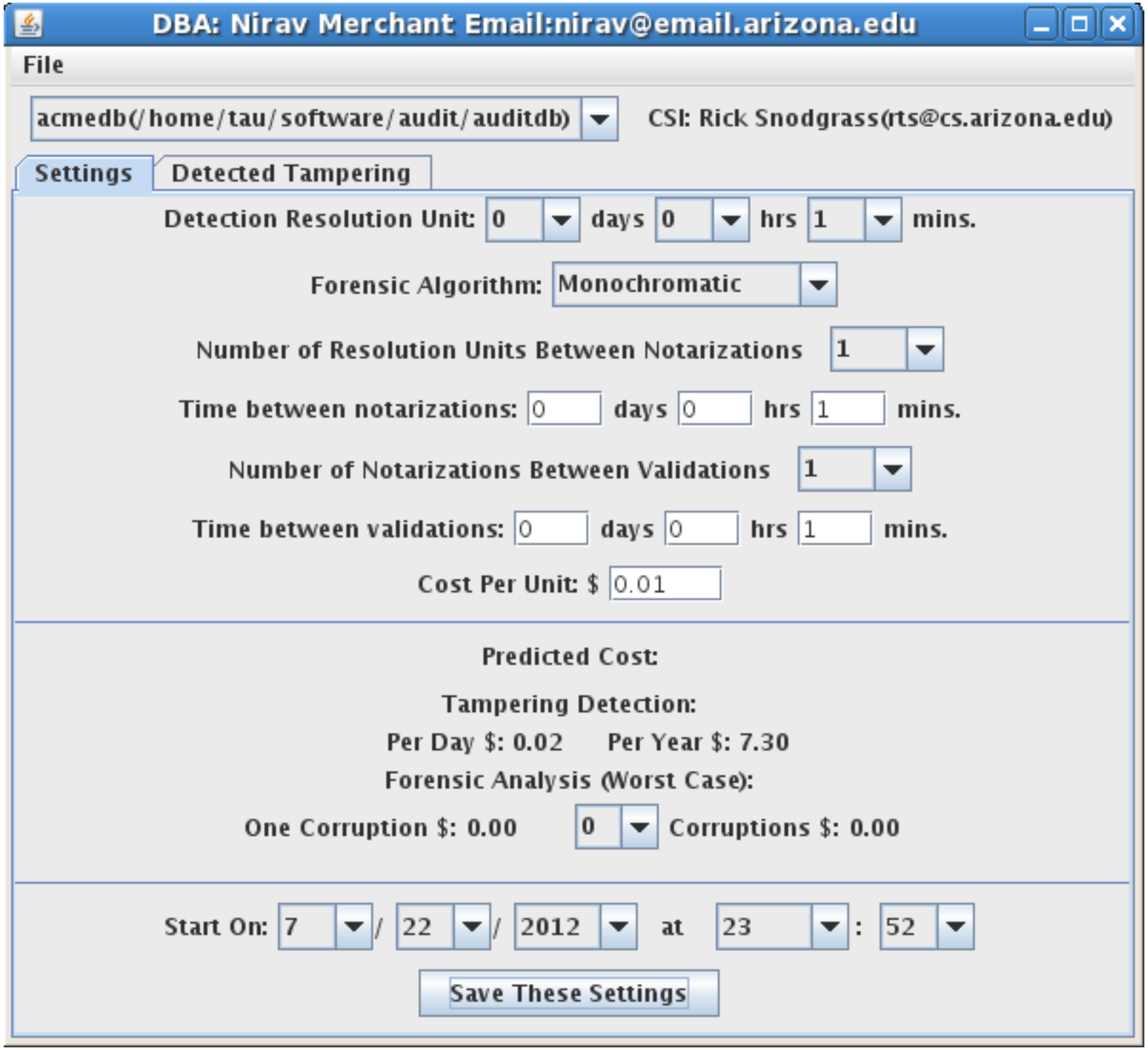
- There are three GUIs:
  - Chief Security Office (CSO)
  - Database Administrator (DBA)
  - Crime Scene Investigator (CSI)

- Configure the security policies by
  - selecting a database to be monitored
  - setting the security parameters, e.g., R_s, N, V, I_N

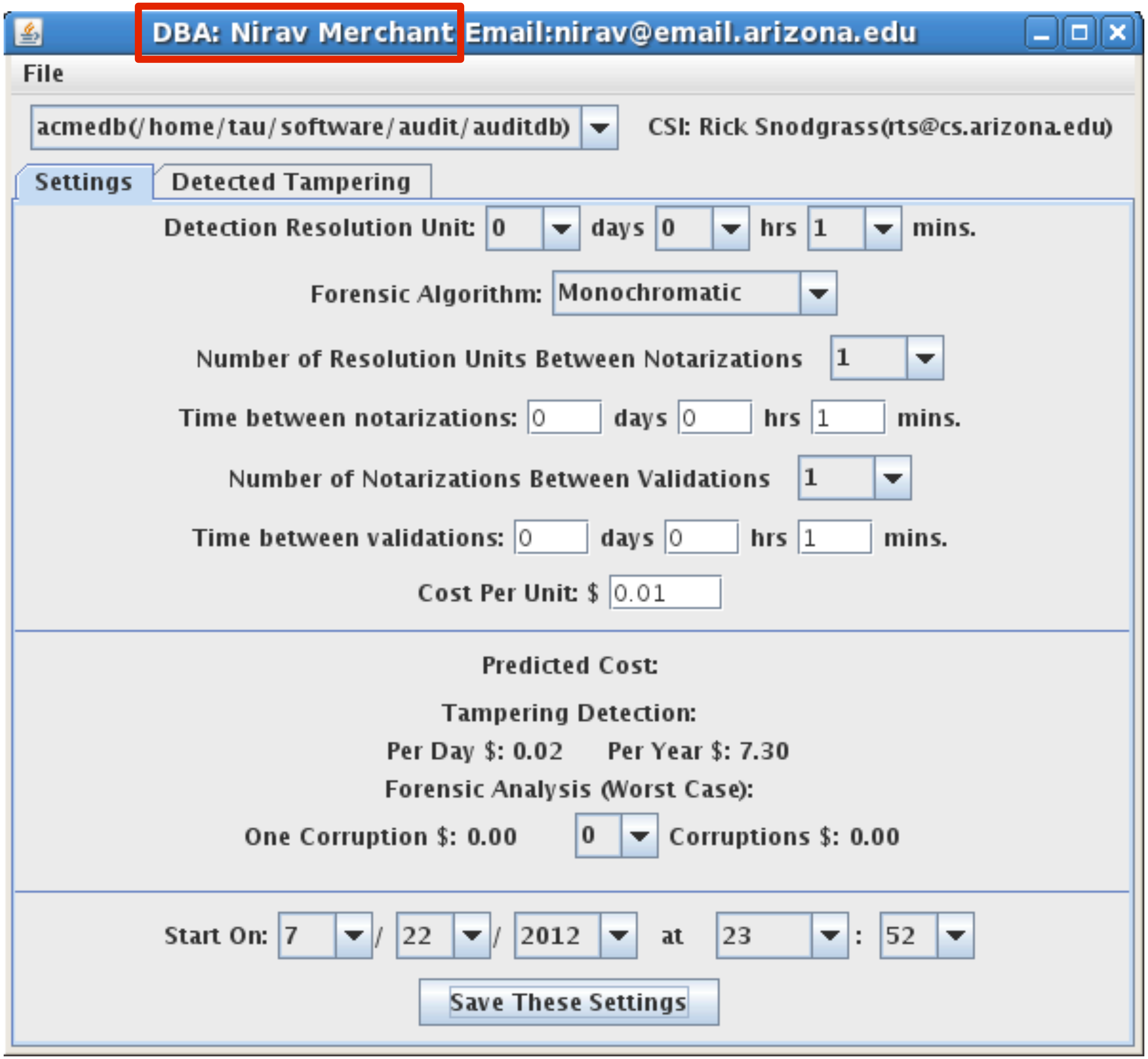
- Calculate the forensic cost for normal processing and forensic analysis

- Create corruption diagrams

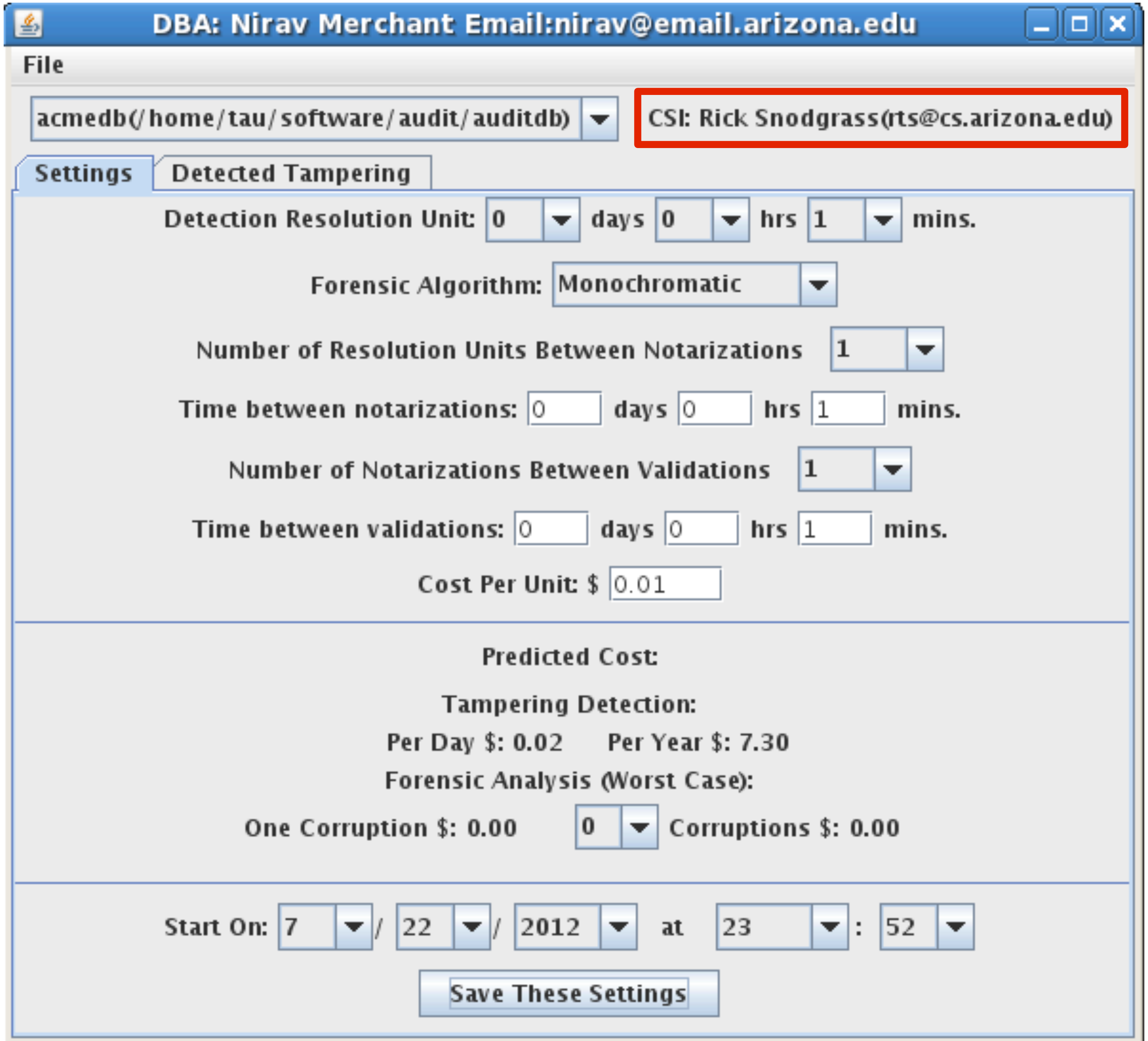
DBA: Database-Specific Settings



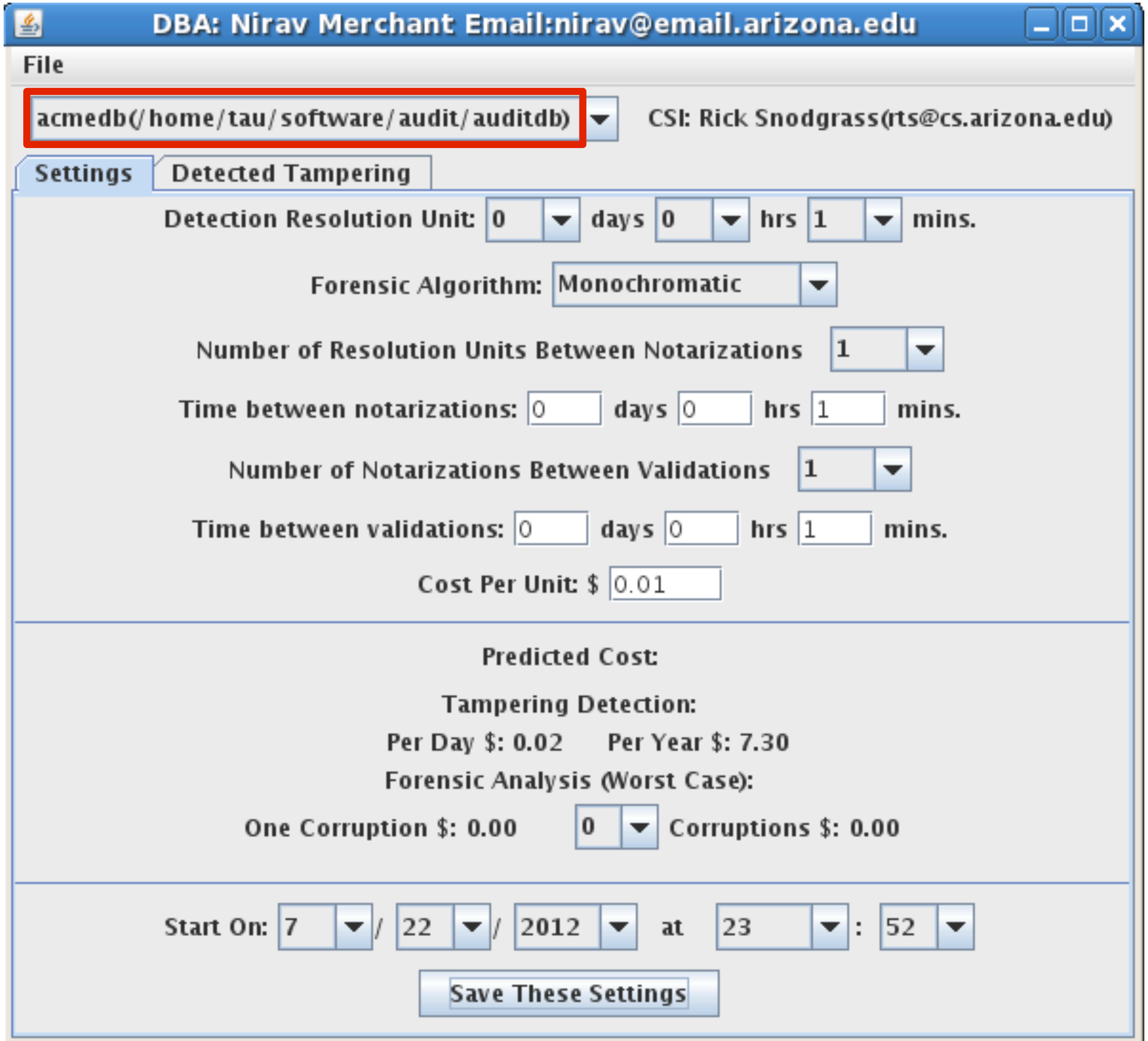
DBA: Database-Specific Settings



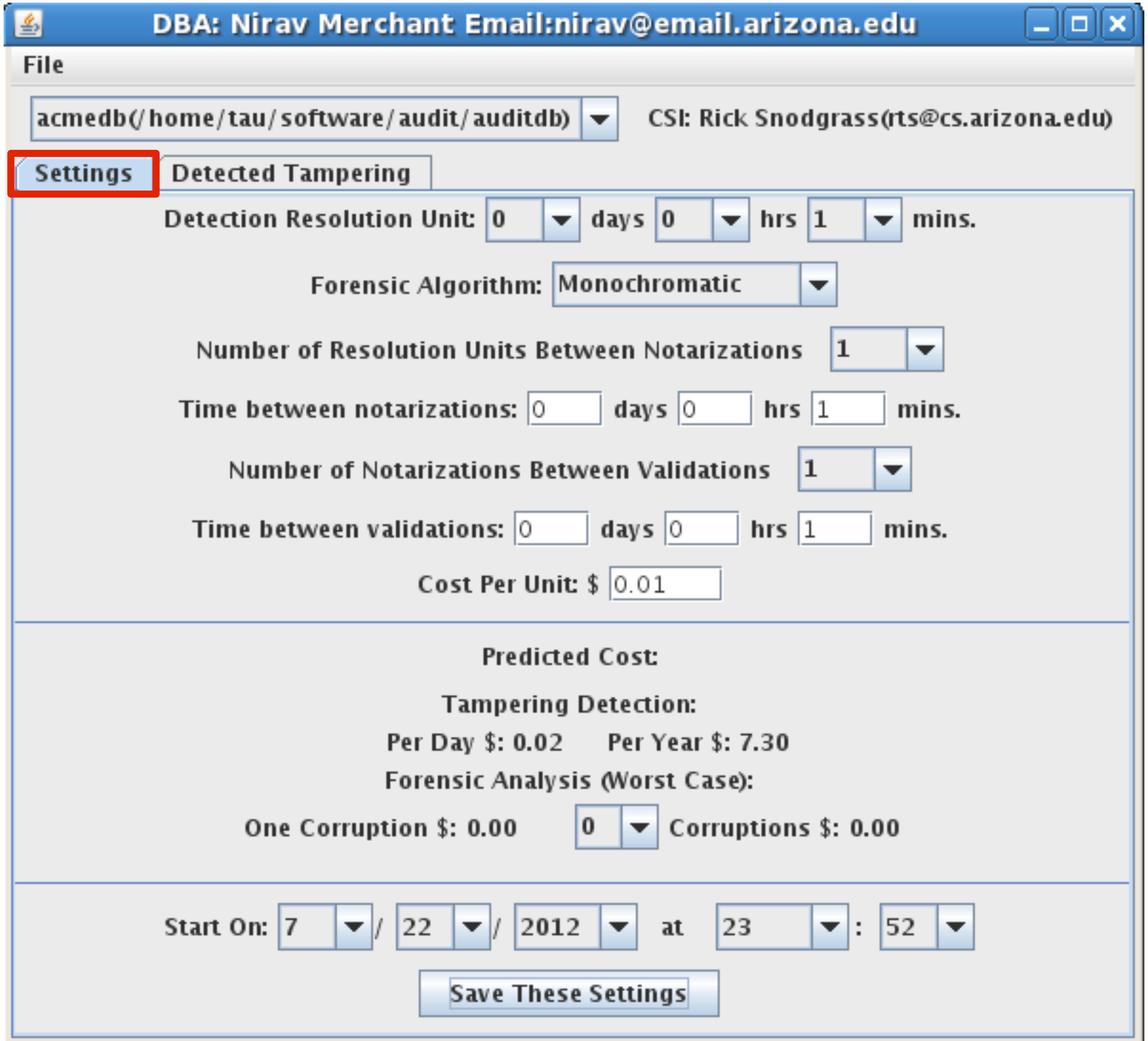
DBA: Database-Specific Settings



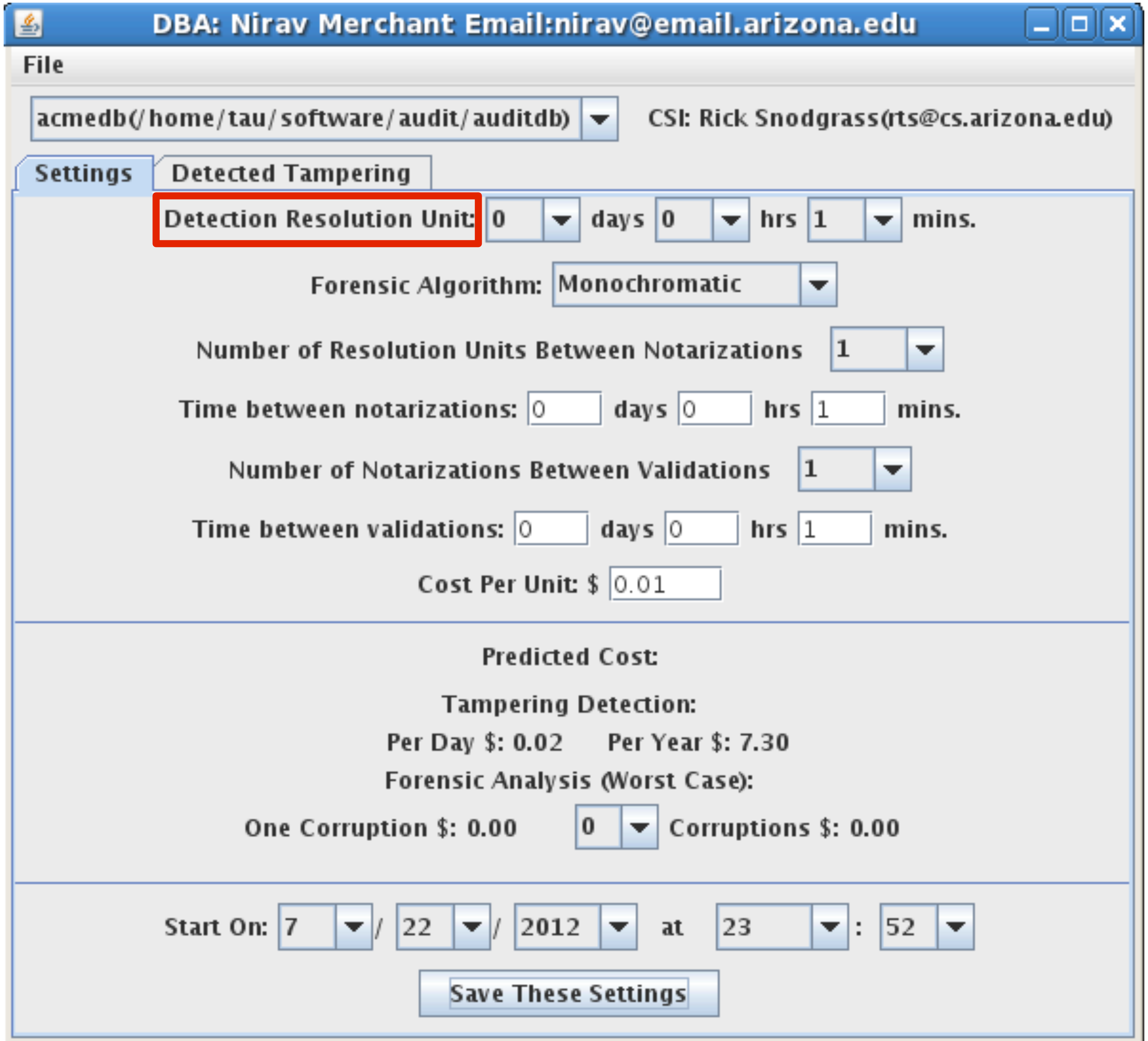
DBA: Database-Specific Settings



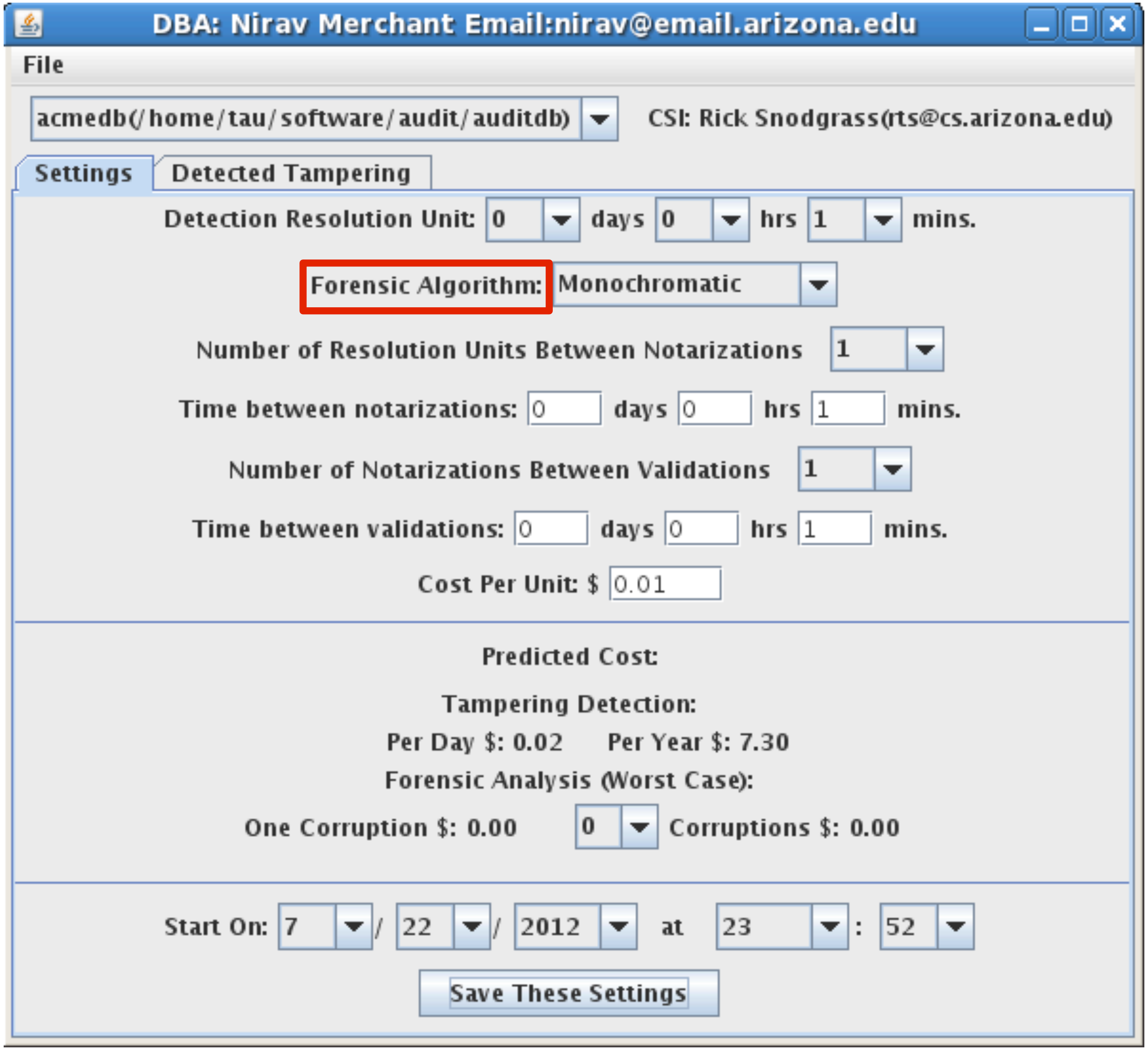
DBA: Database-Specific Settings



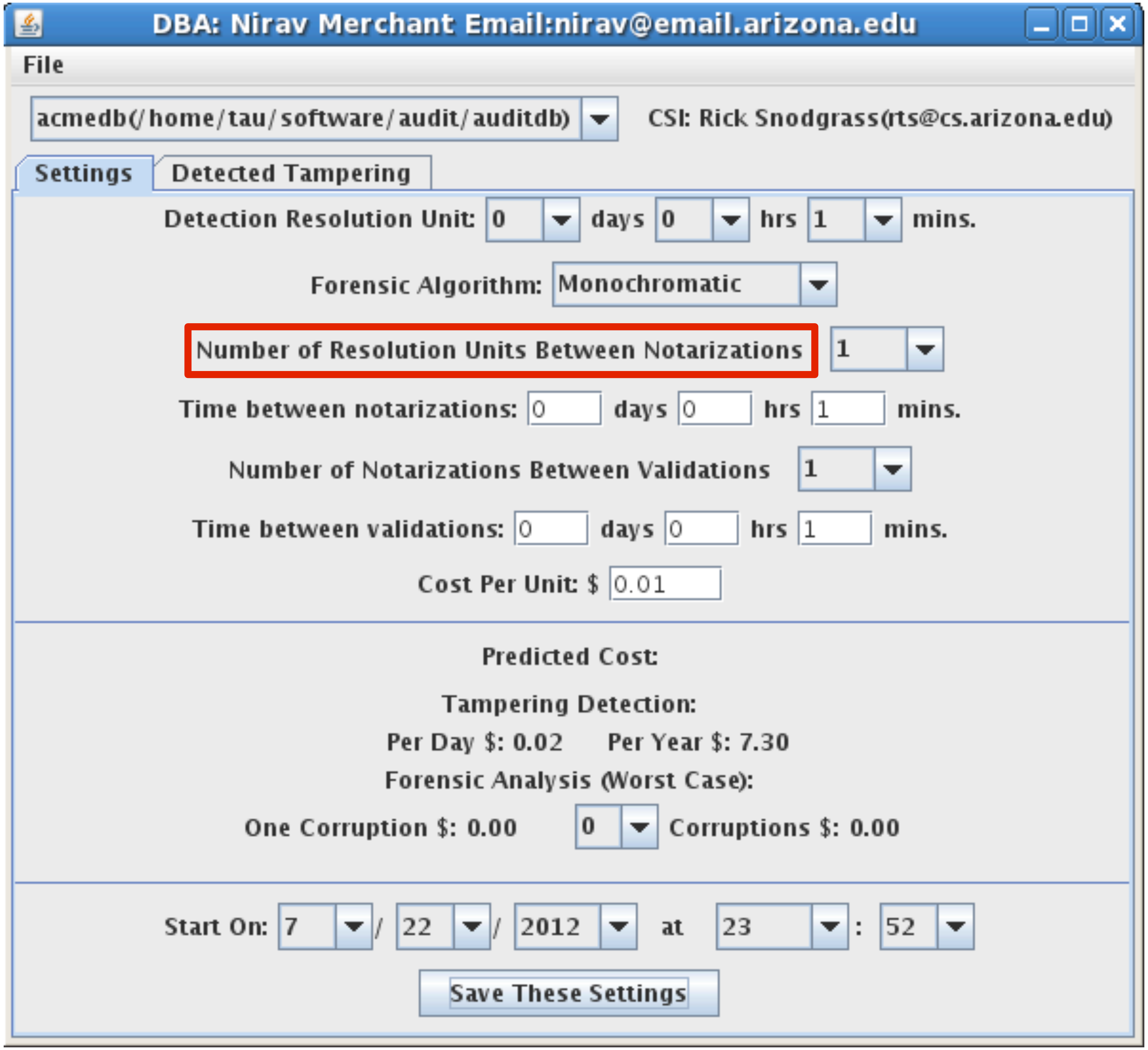
DBA: Database-Specific Settings



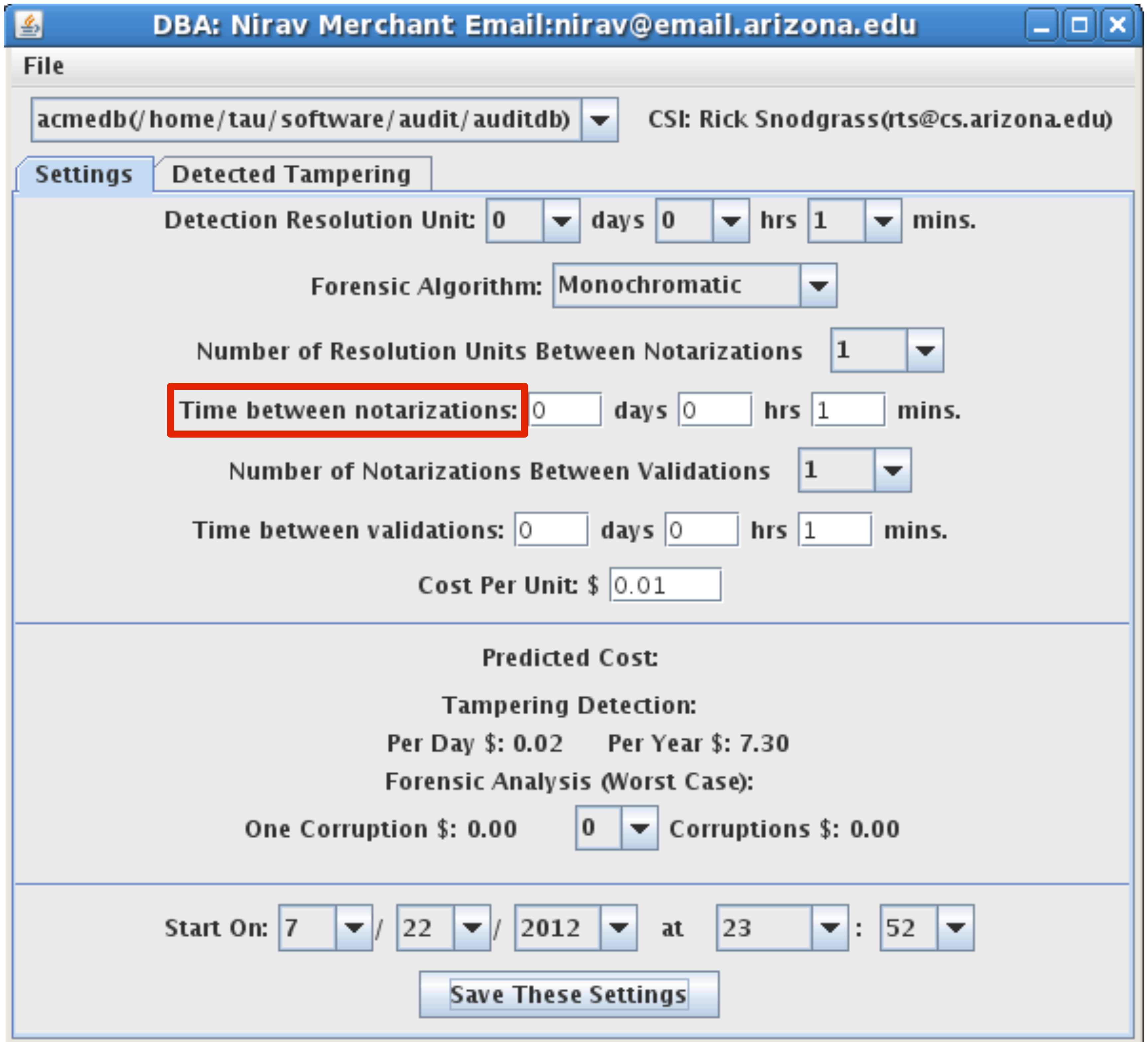
DBA: Database-Specific Settings



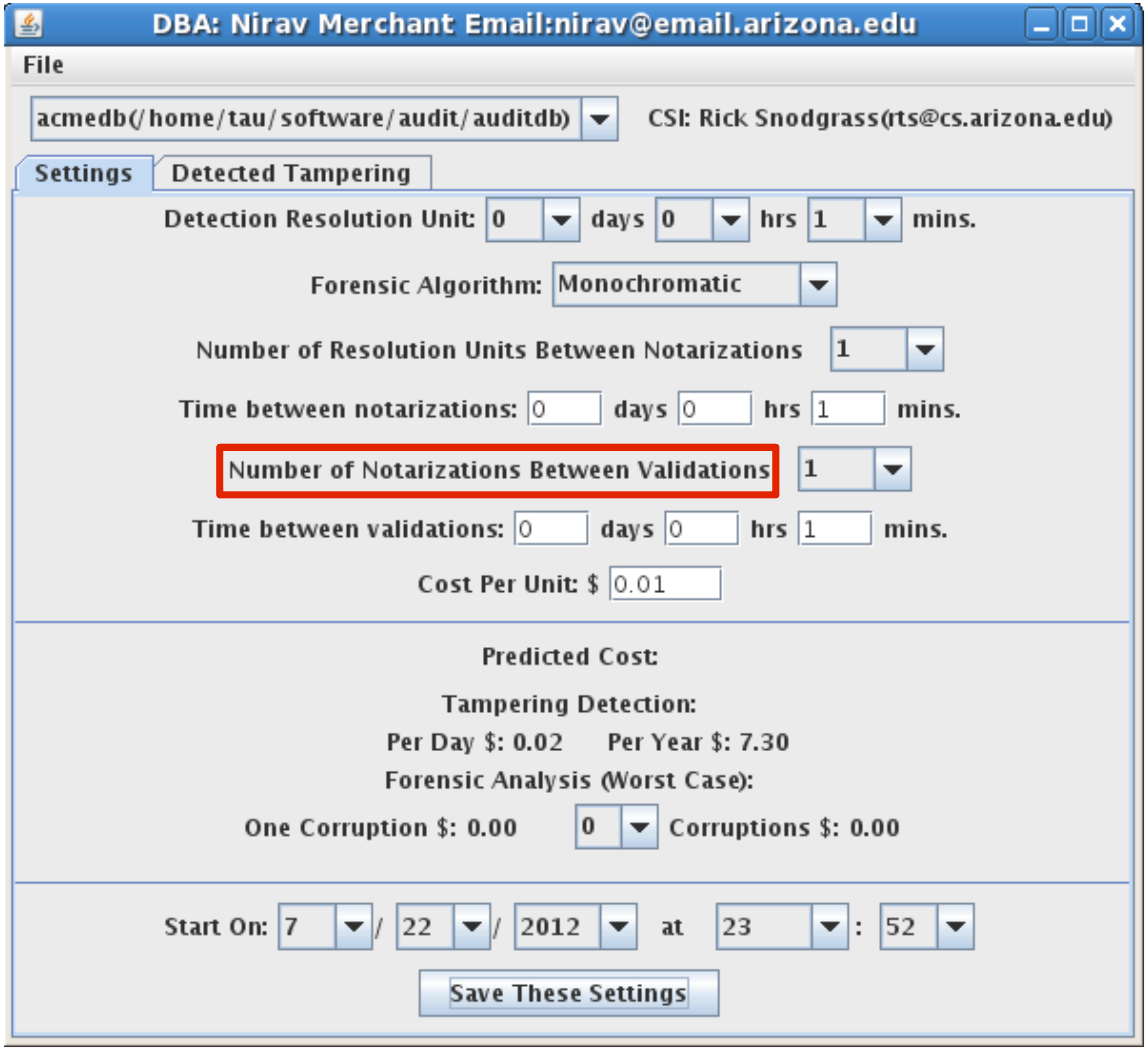
DBA: Database-Specific Settings



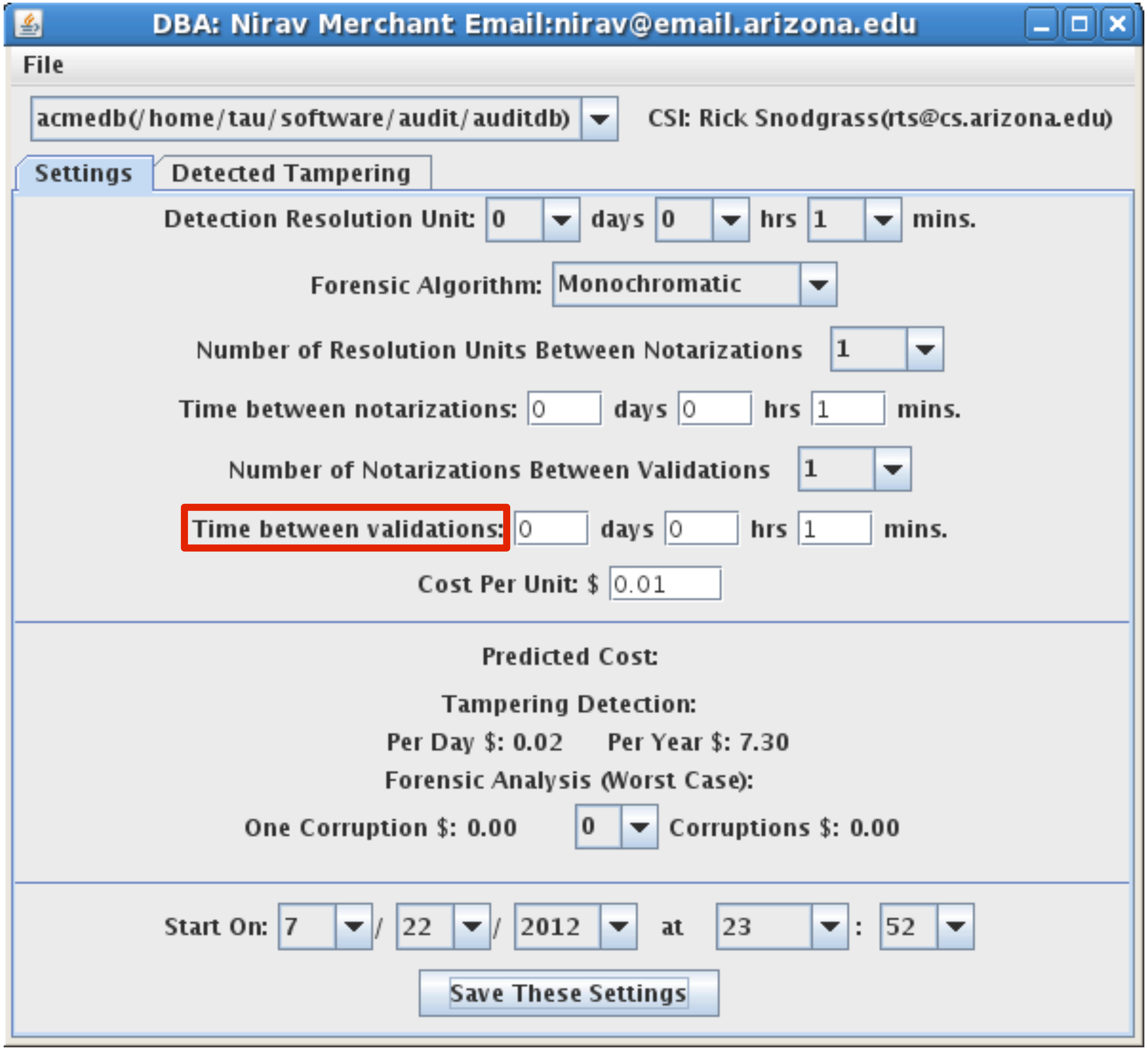
DBA: Database-Specific Settings



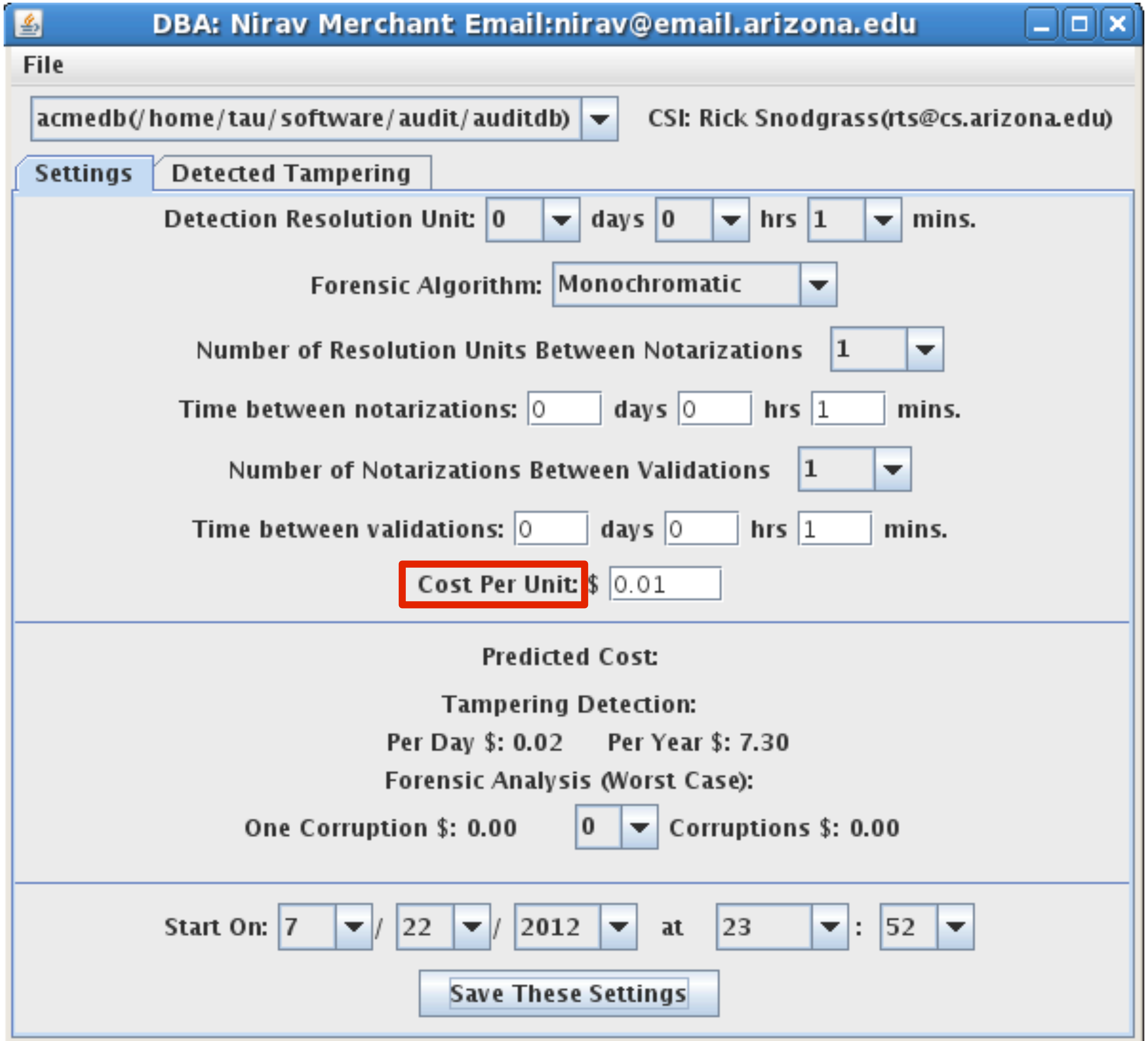
DBA: Database-Specific Settings



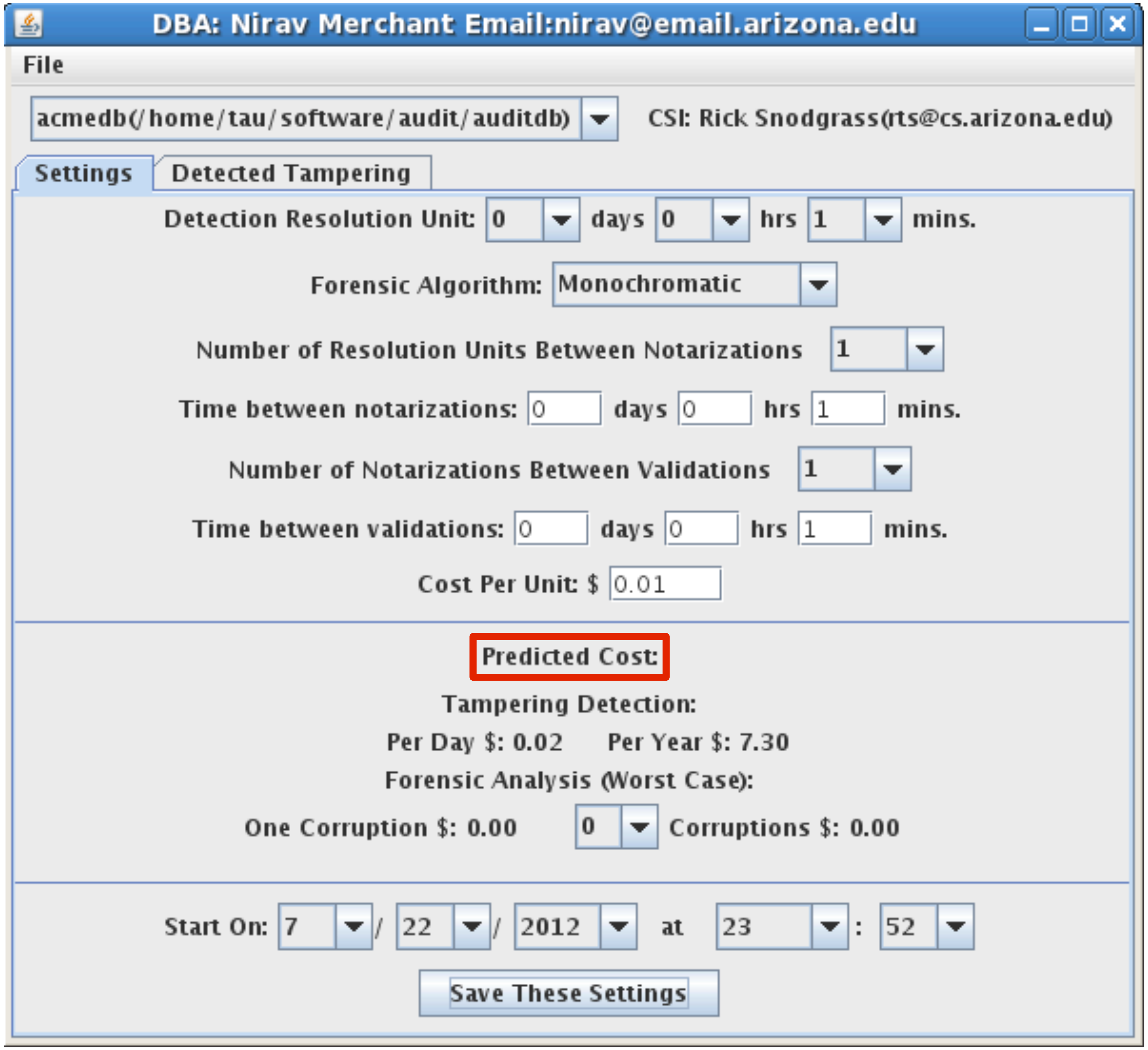
DBA: Database-Specific Settings



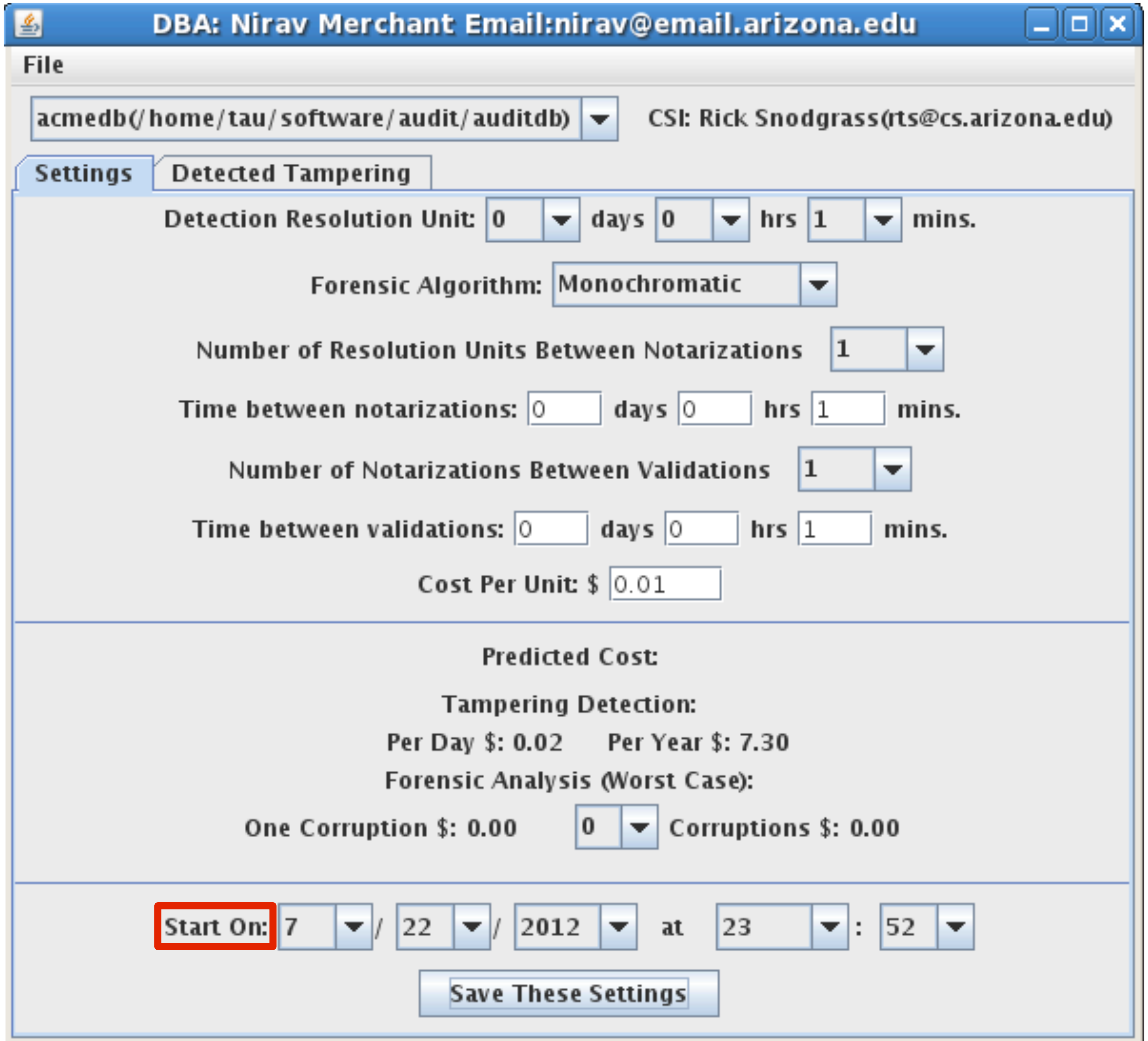
DBA: Database-Specific Settings



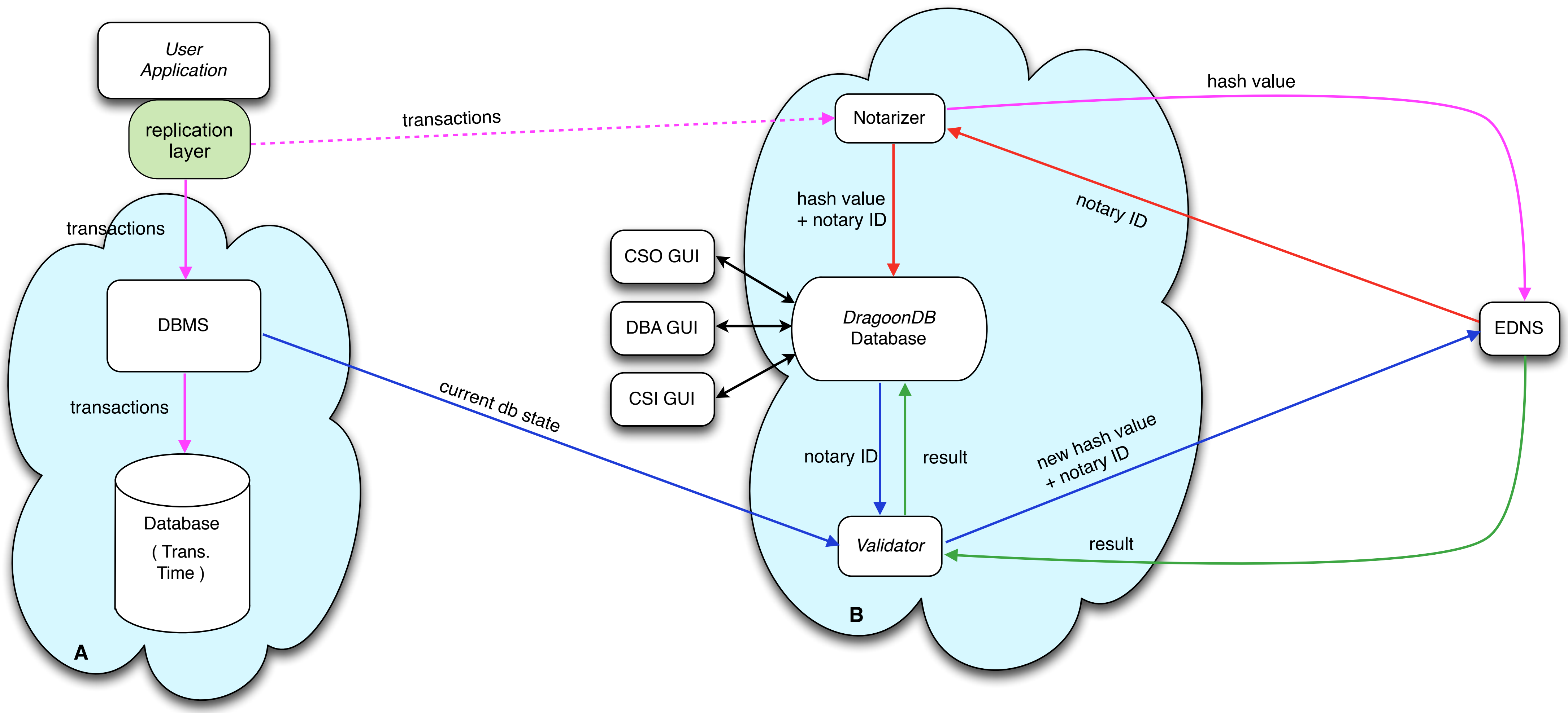
DBA: Database-Specific Settings



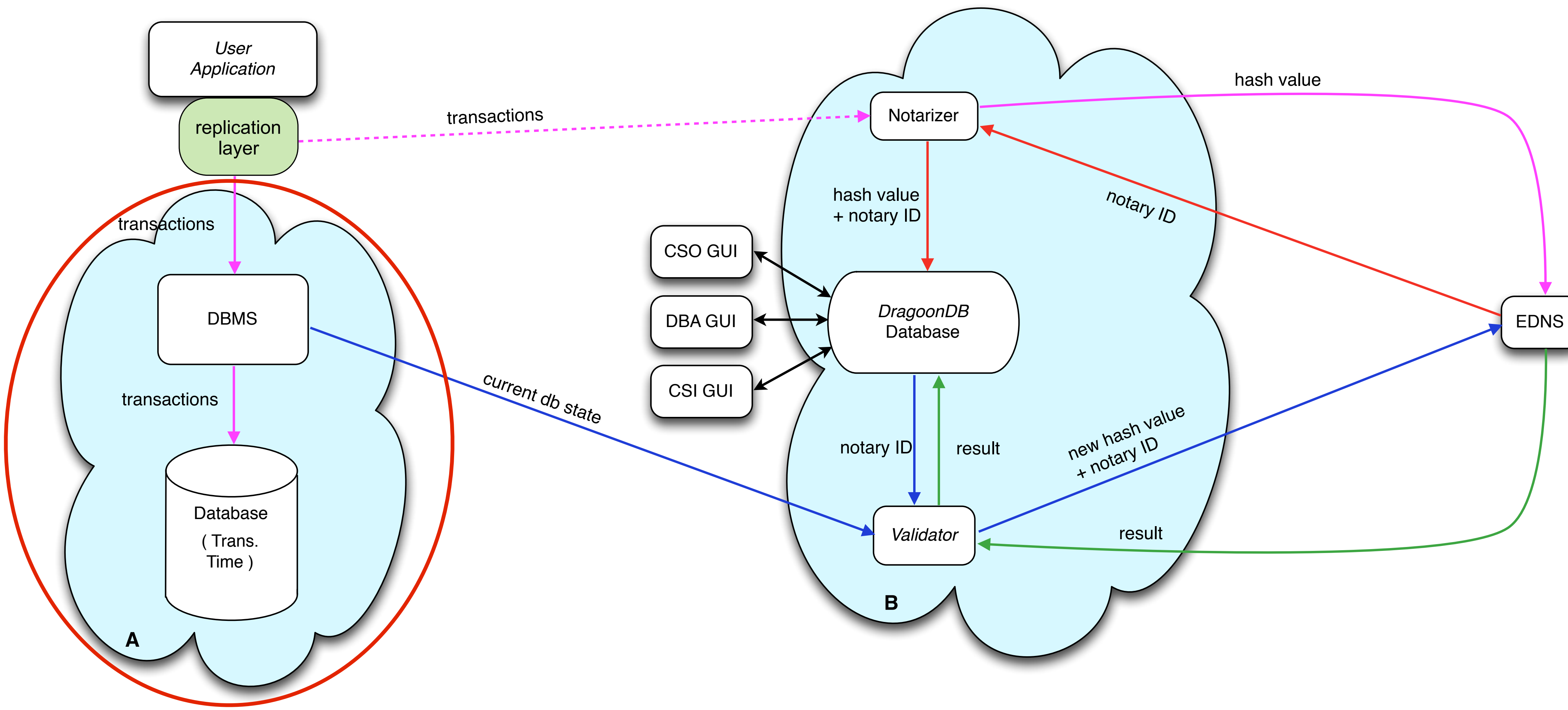
DBA: Database-Specific Settings



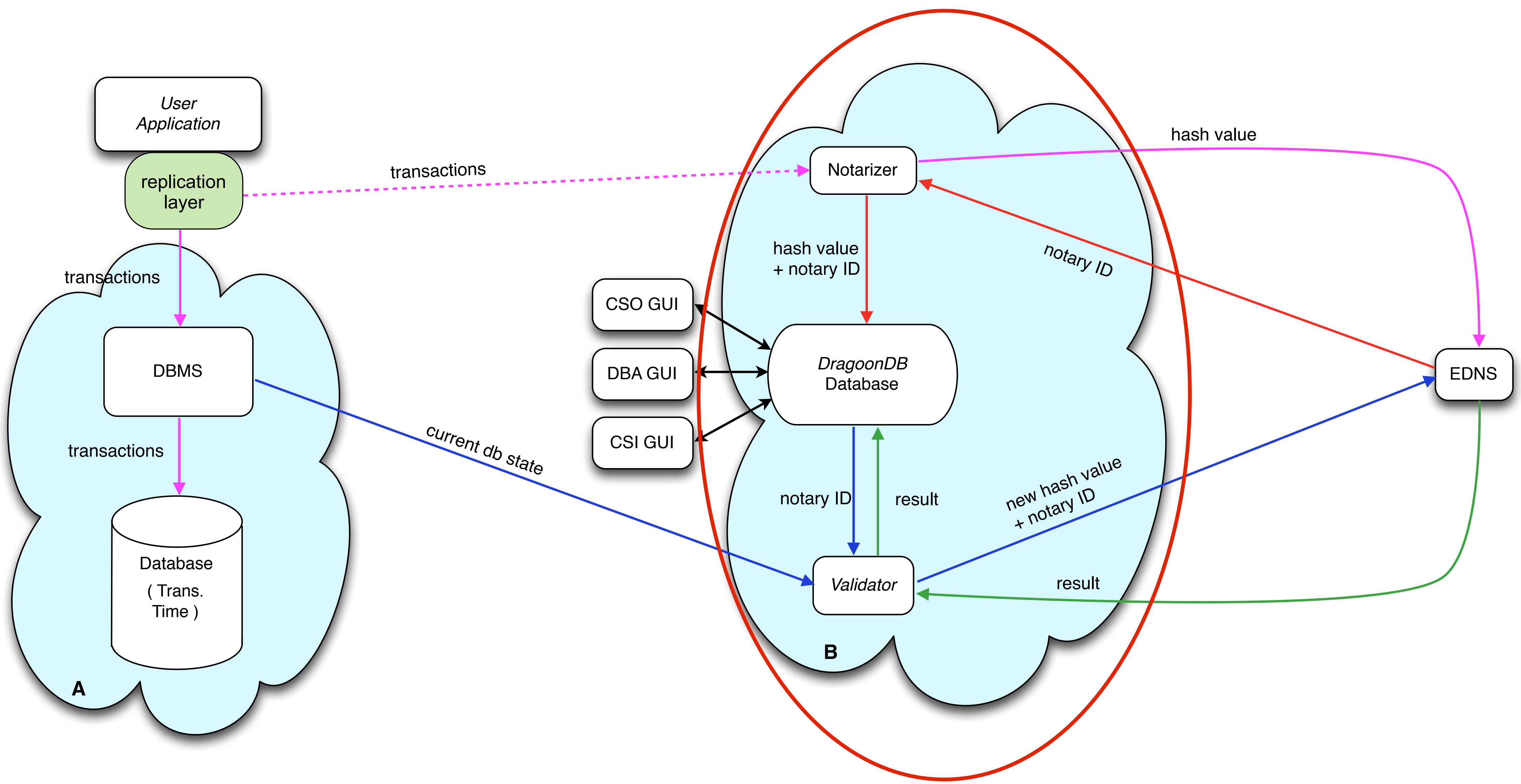
Information Accountability in the Cloud



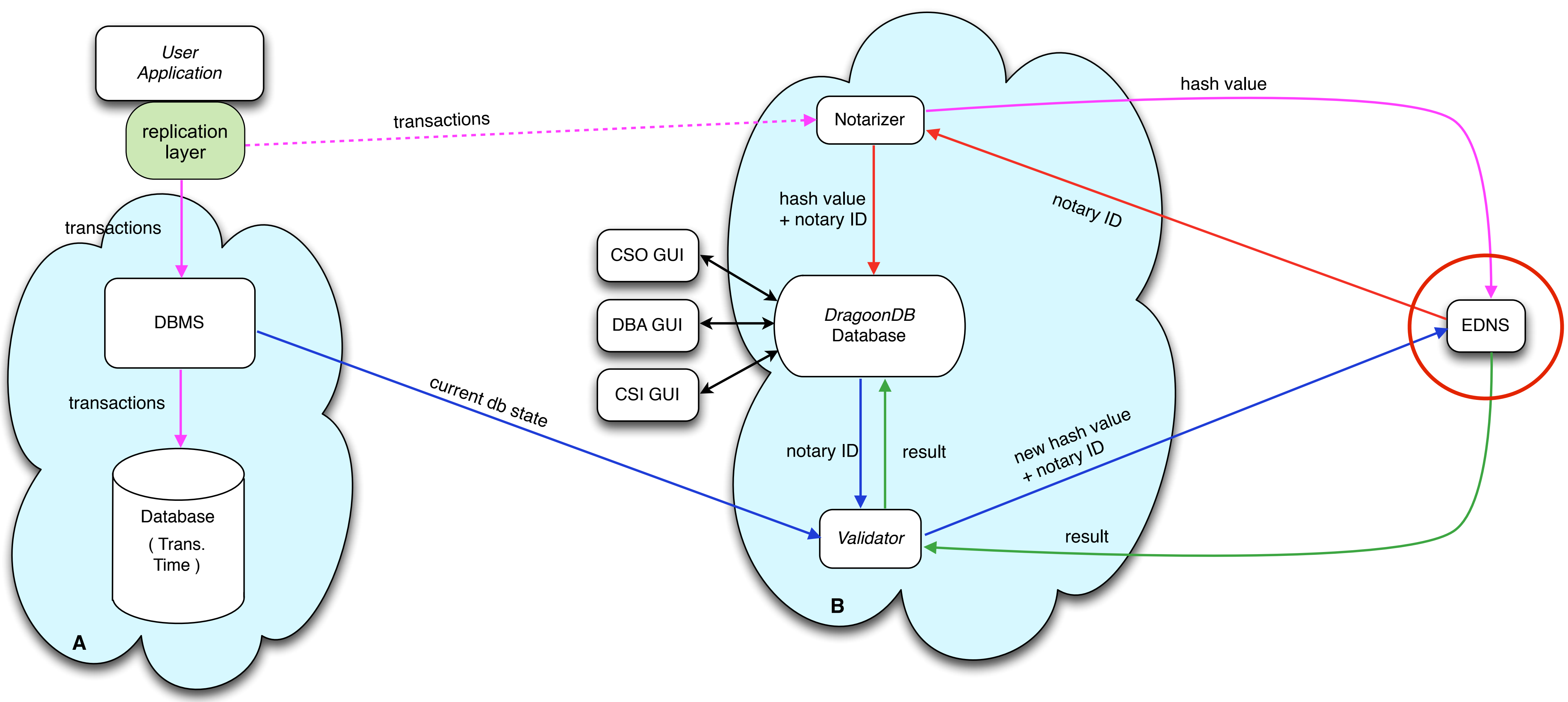
Information Accountability in the Cloud



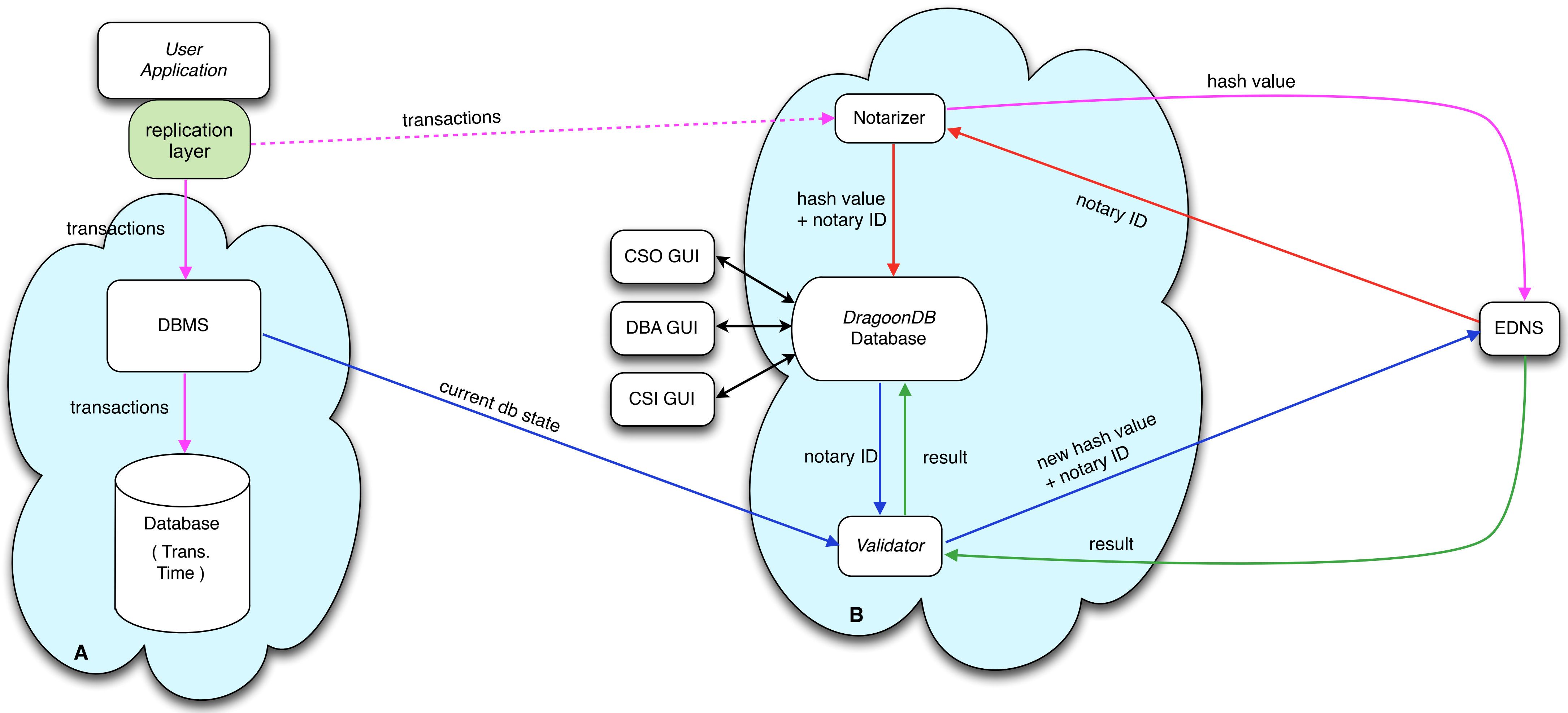
Information Accountability in the Cloud



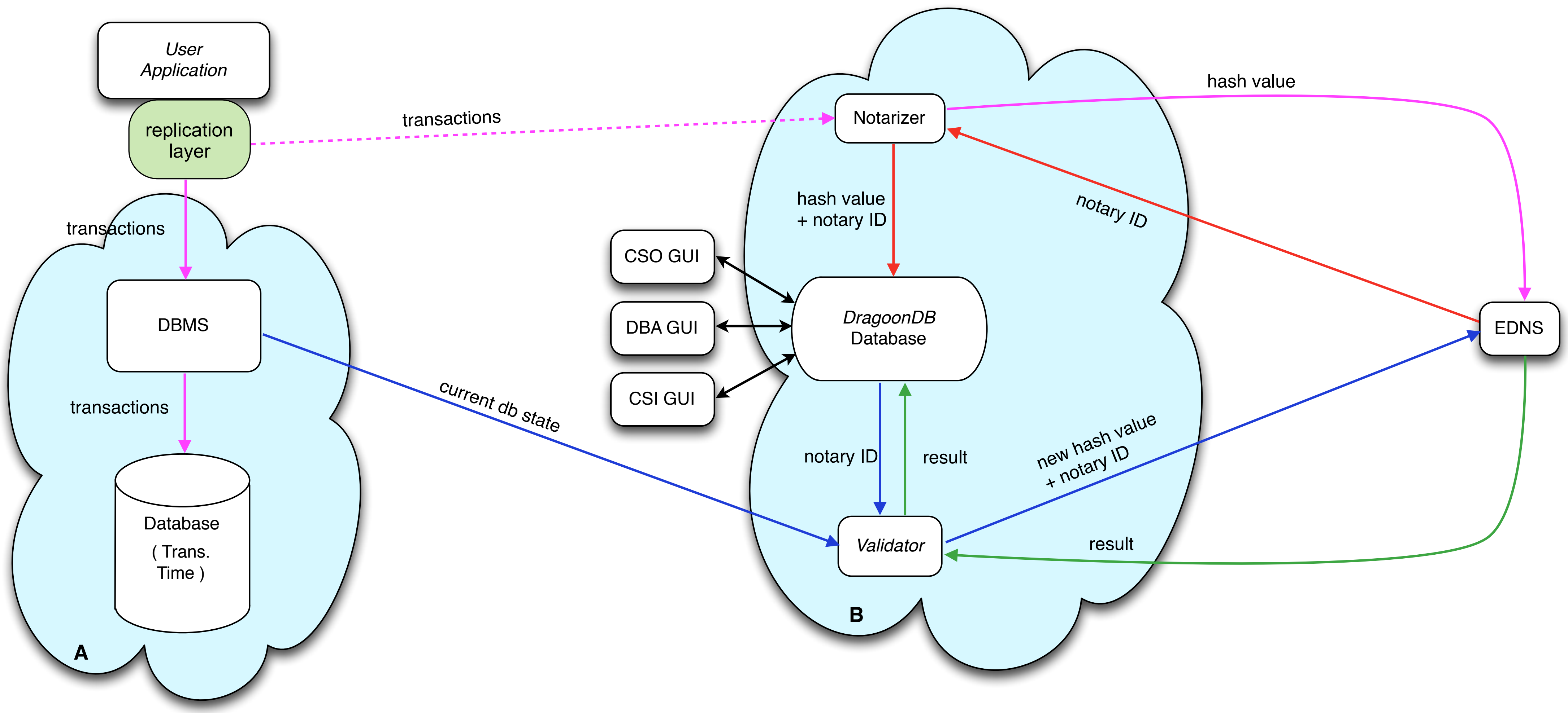
Information Accountability in the Cloud



Information Accountability in the Cloud



Information Accountability in the Cloud



The new threat model may give rise to other temporal concepts.

Also holds for concurrency, replication, and distribution.

Summary

- Information Accountability
- Reference Architecture & Execution Phases
- Forensic Analysis
- Refinements
- Enterprise Considerations

Summary (2)

- Need to be able to capture history.
- Need to be able to revisit history.
- Need a trusted witness or at least consensus opinion to provide continuous assurance over time.

The Challenge

The Challenge

As we have seen time arises naturally in many aspects of database information accountability (and in many guises).

The Challenge

As we have seen time arises naturally in many aspects of database information accountability (and in many guises).

What is the deeper structure of the fundamental connection between temporal databases and information security?

Thank You!

Questions?