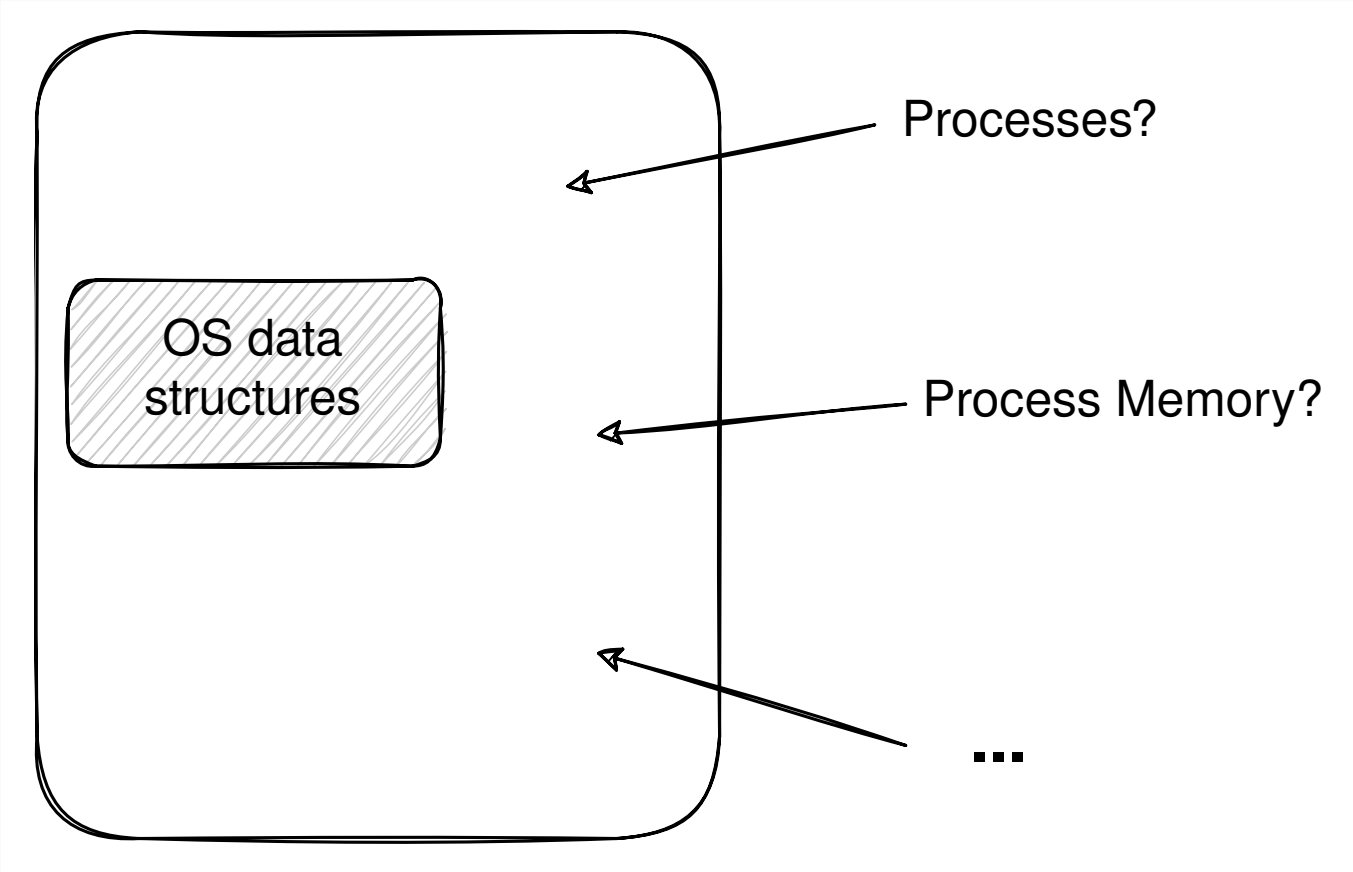
Defining Atomicity (and Integrity) for Snapshots of Storage in Forensic Computing

Jenny Ottmann, Frank Breitinger, Felix Freiling

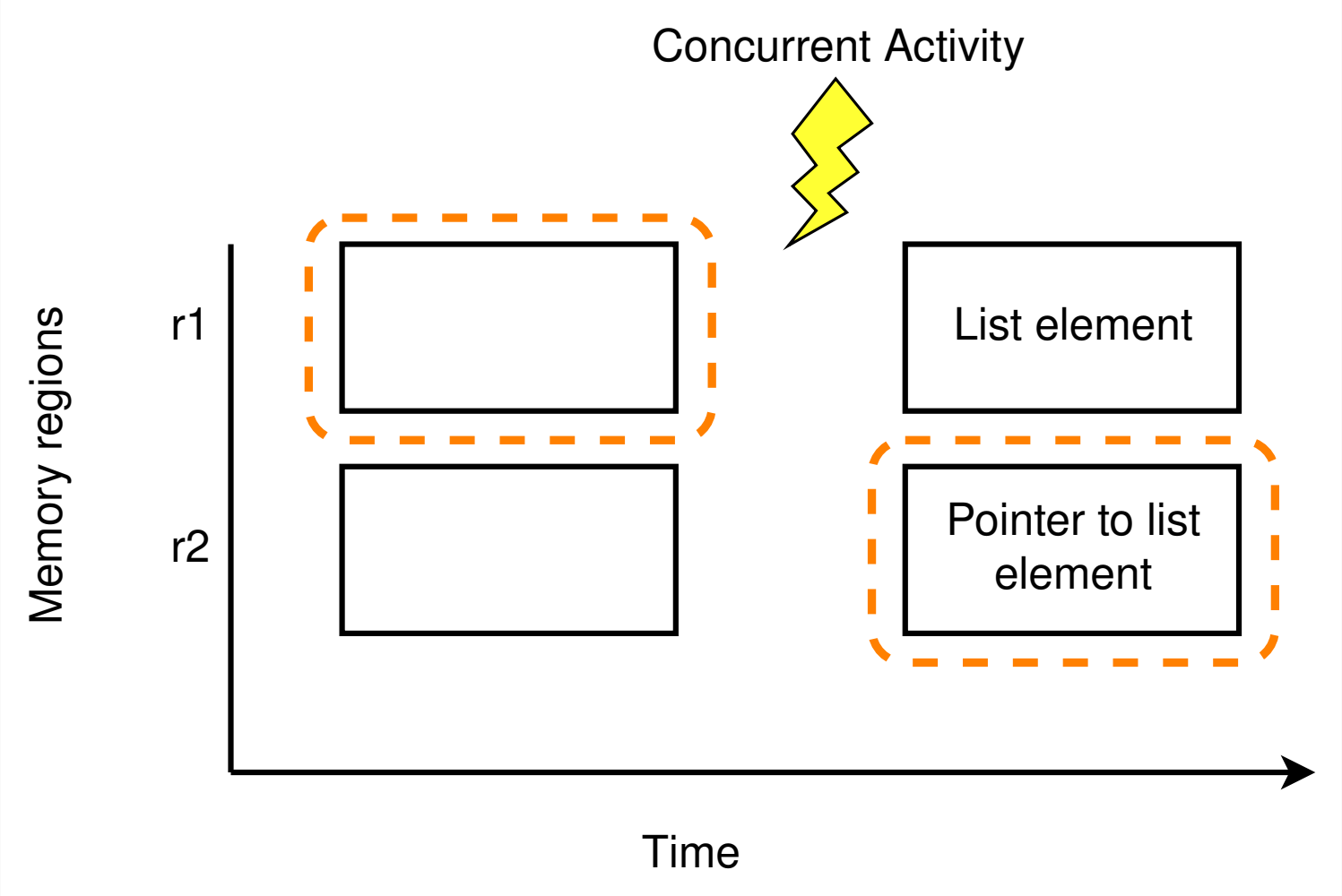
DFRWS EU 2022, Oxford

IT Security Infrastructures Lab
Department of Computer Science
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Main Memory



Inconsistencies



Quality Criteria

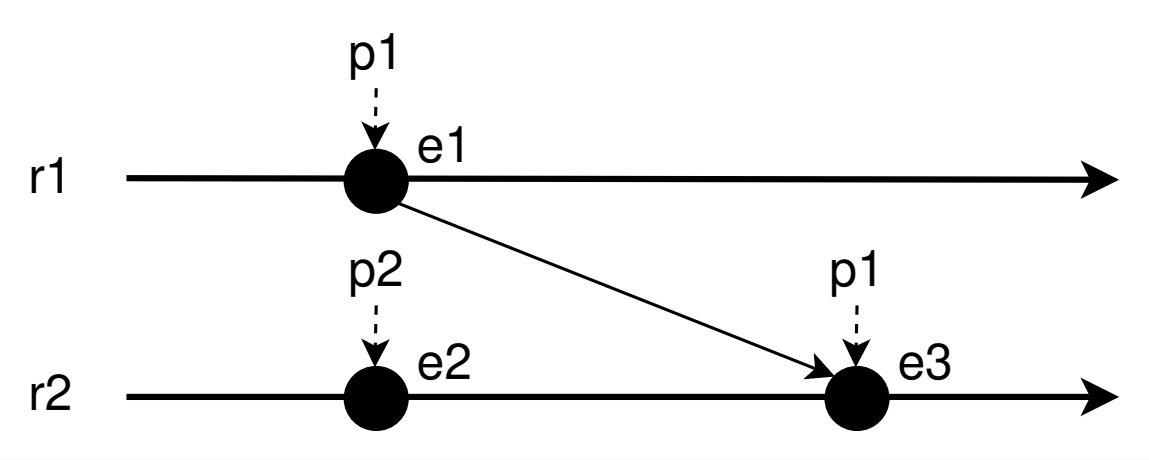
Vömel and Freiling (2012)

- Atomicity
- Correctness
- Integrity

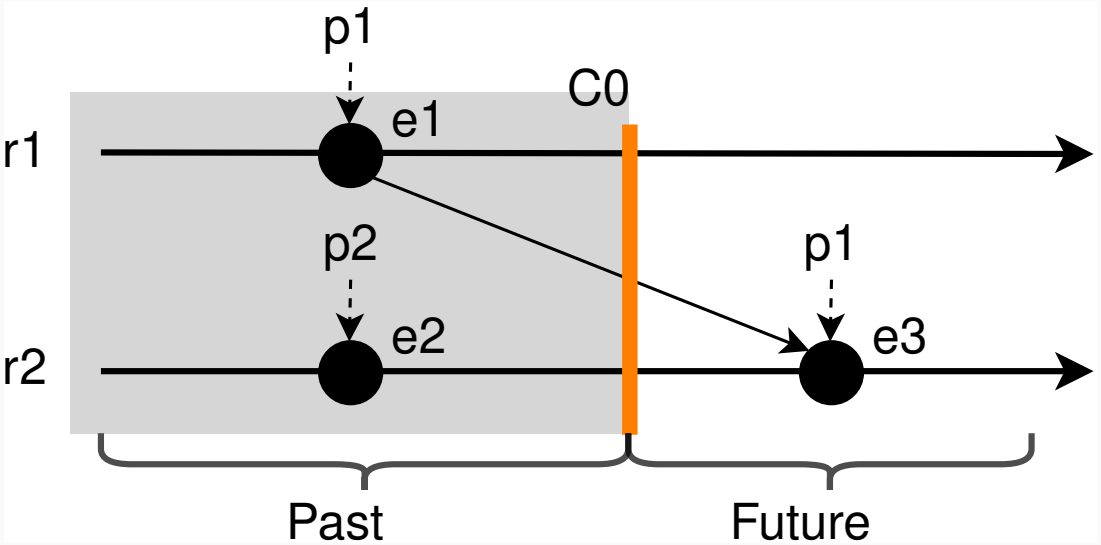
Pagani et al. (2019)

Time consistency

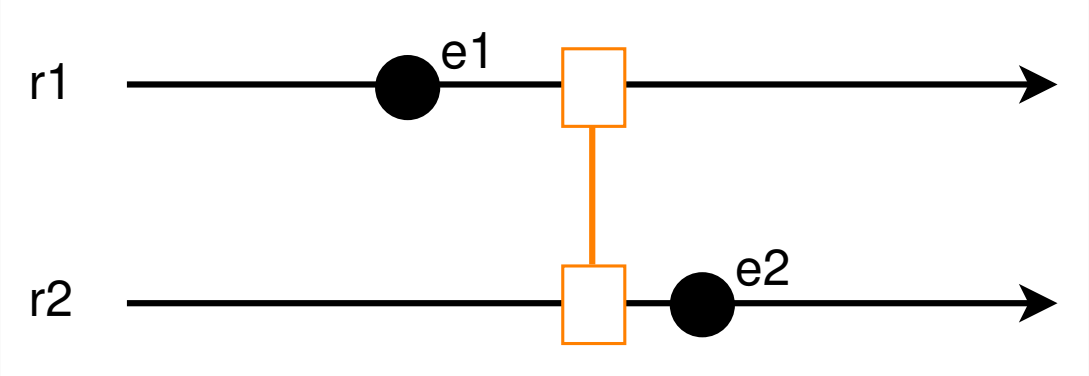
Memory



Memory Snapshot

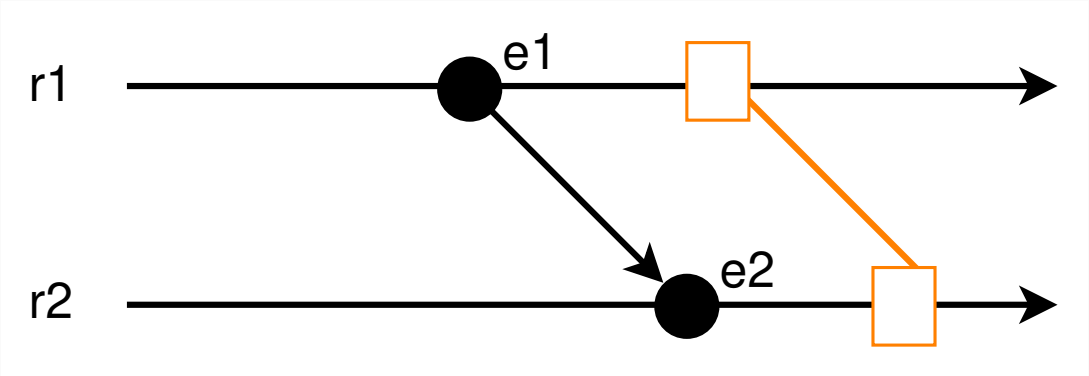


Instantaneous Consistency



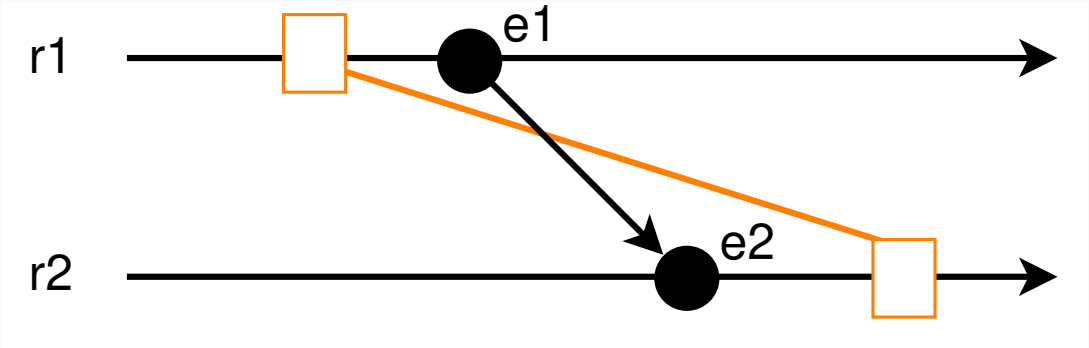
Causal Consistency

Atomic

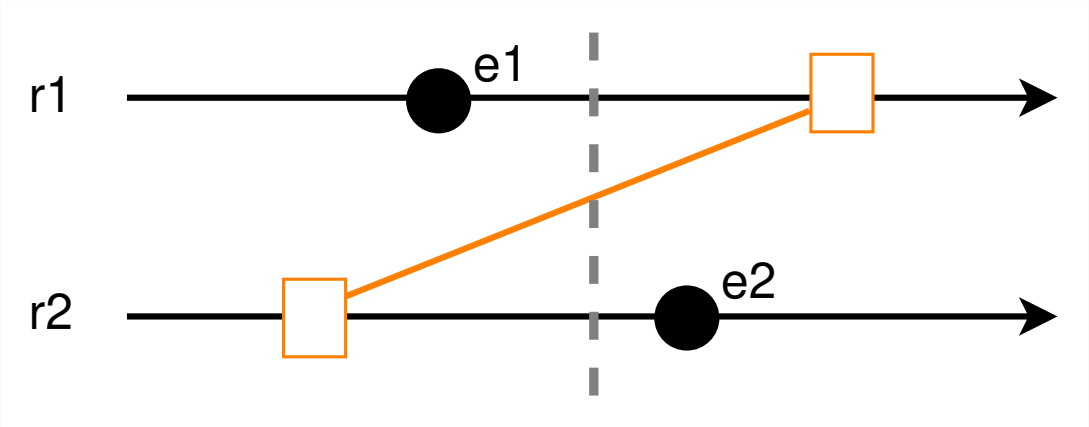


Causal Consistency

Not atomic

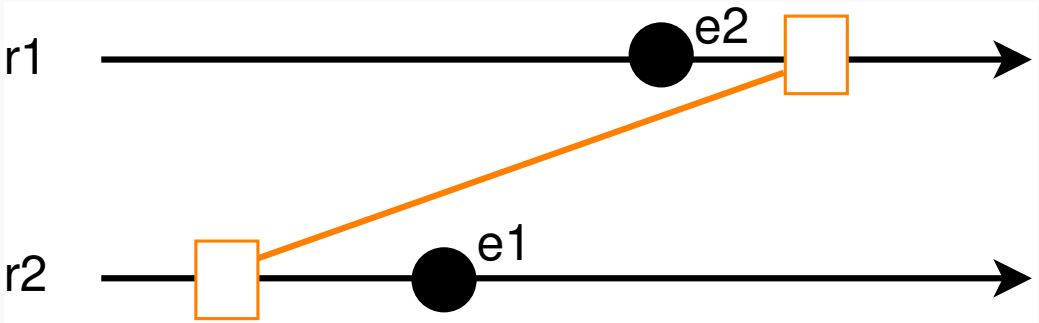


Quasi-instantaneous Consistency

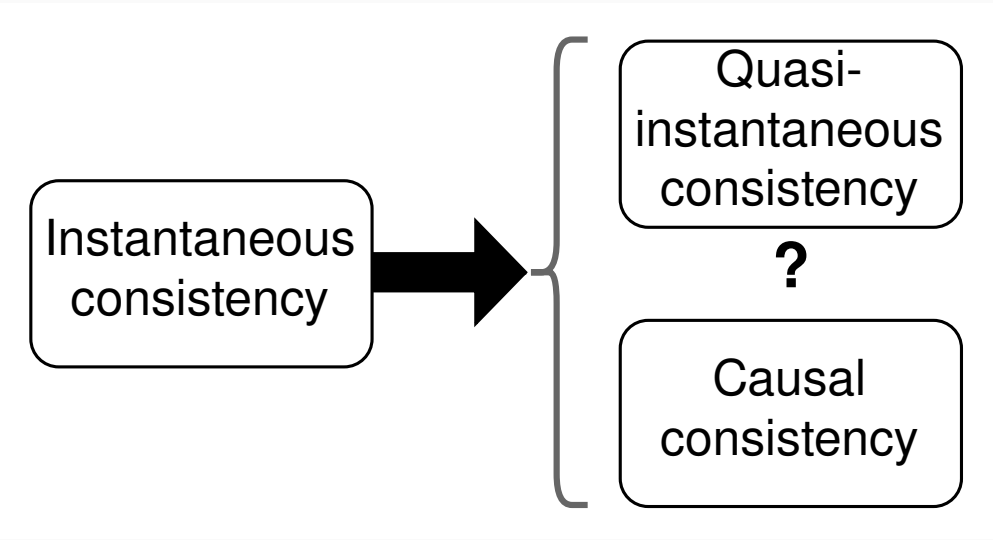


Quasi-instantaneous Consistency

Consistency violation

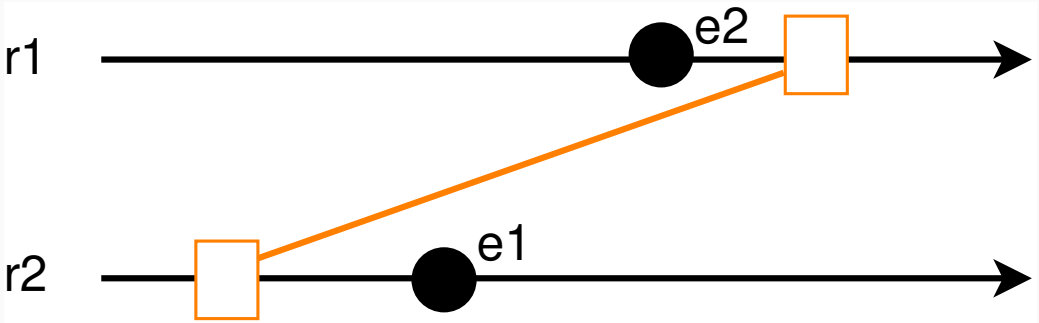


Consistency Implications

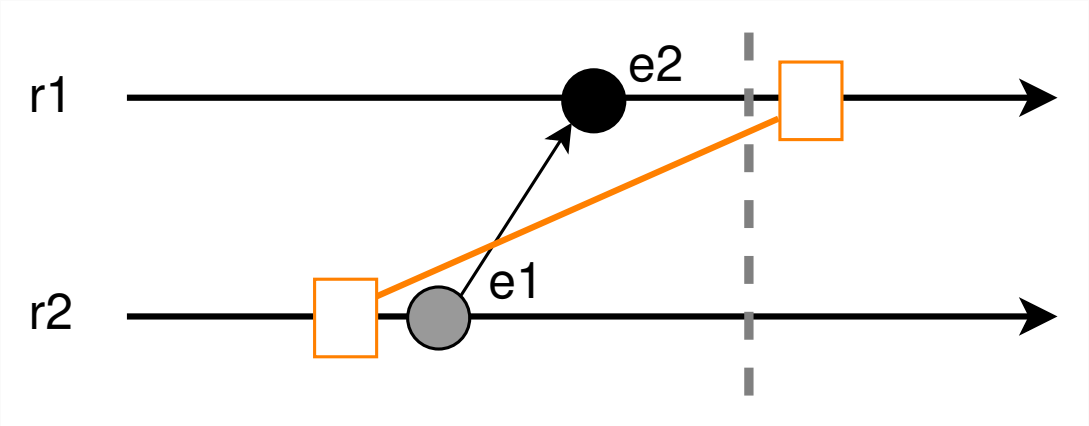


Consistency Implications

Atomic but not quasi-instantaneous



Consistency Implications



Integrity

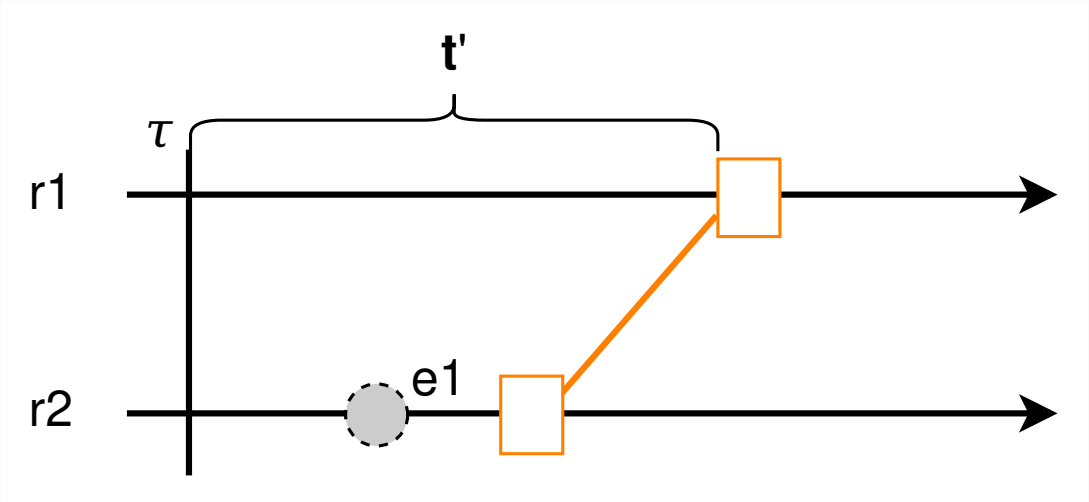
Focus so far:

Influence of concurrent activity on snapshot contents.

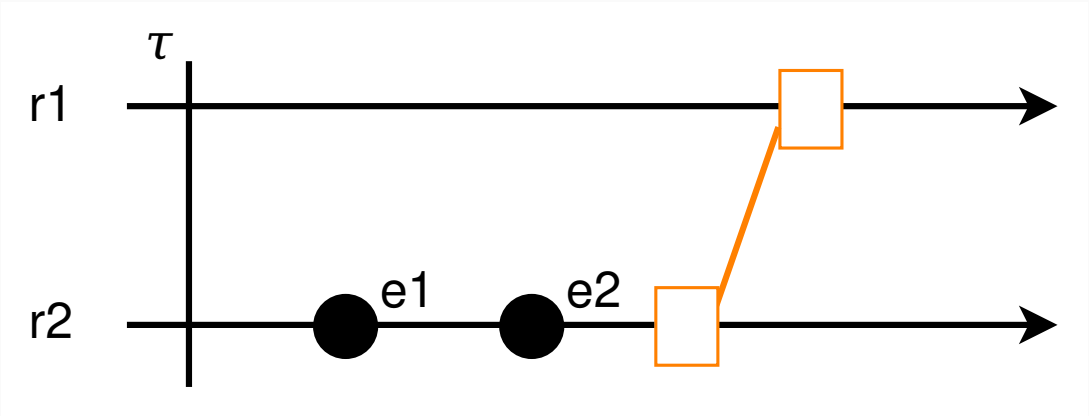
Focus now:

Influence of the acquisition program on memory contents.

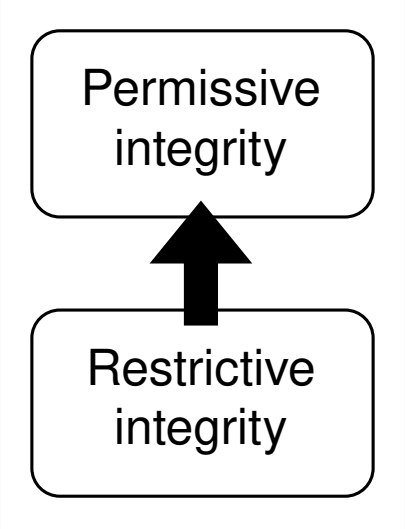
Restrictive Integrity



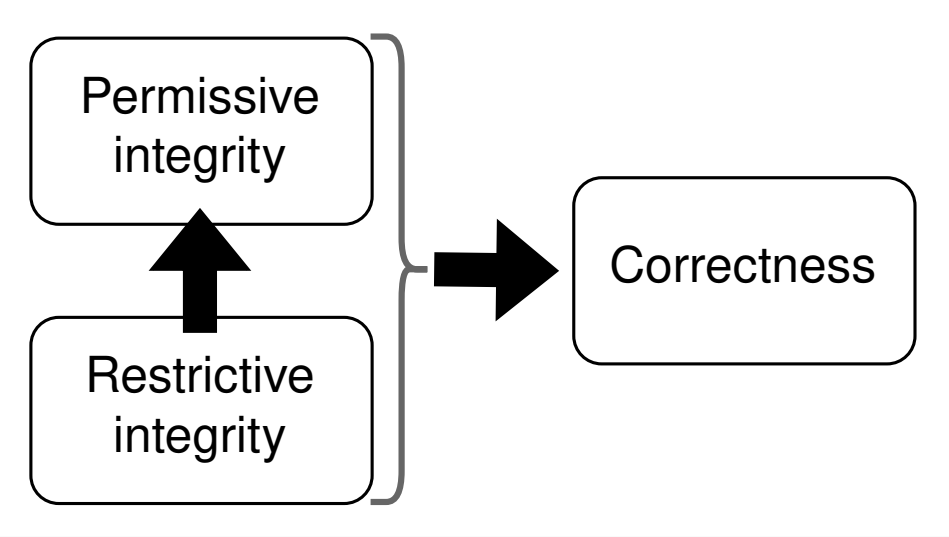
Permissive Integrity



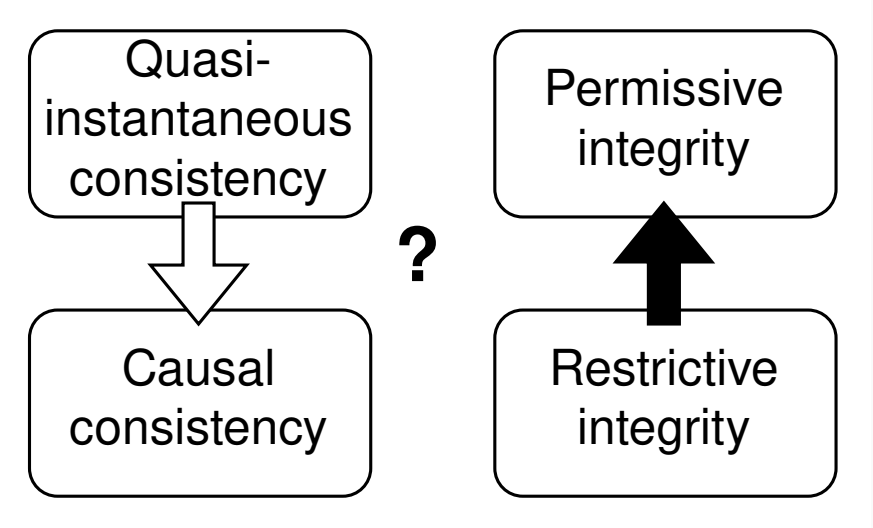
Integrity Implications



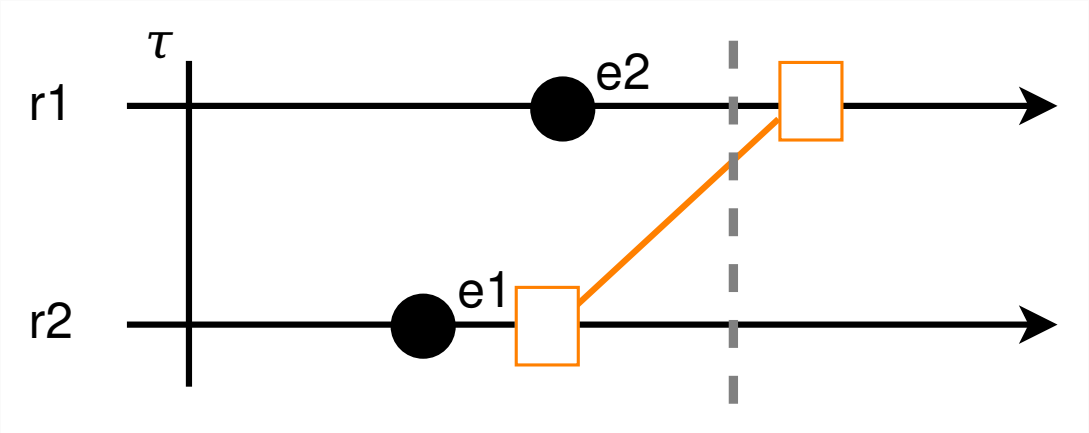
Integrity and Correctness



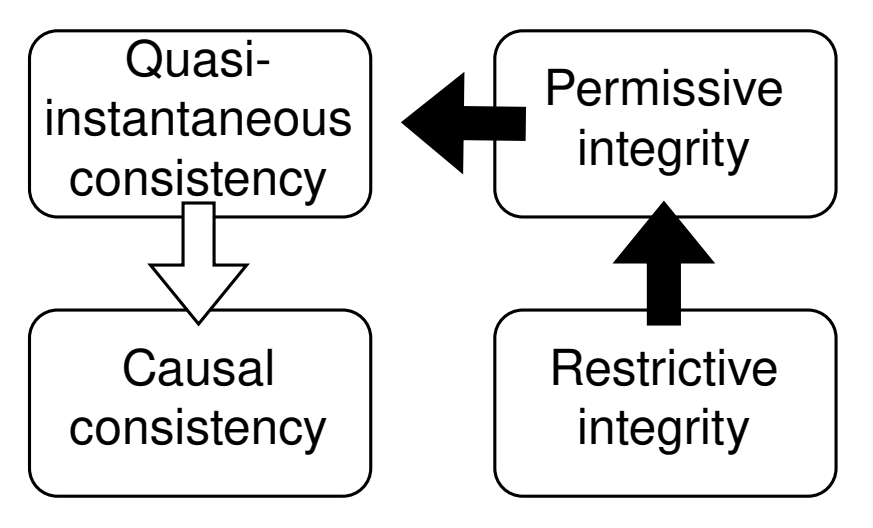
Integrity and Consistency



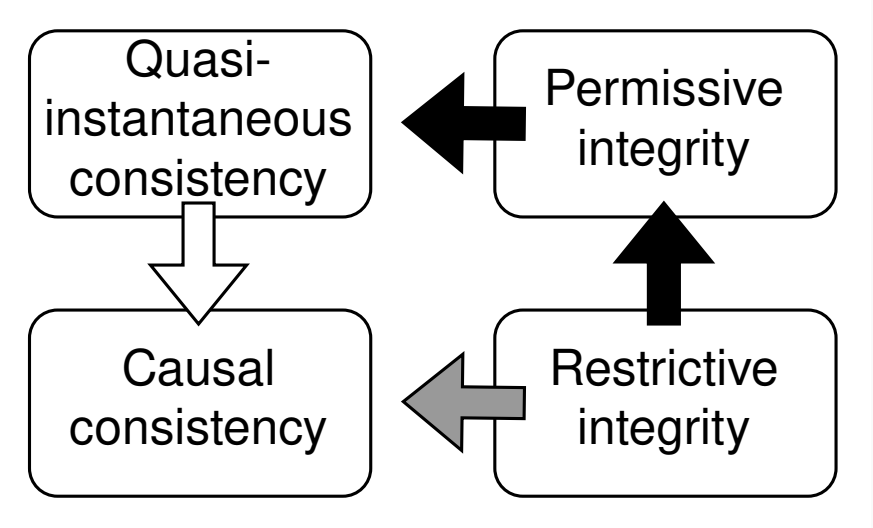
Integrity and Consistency



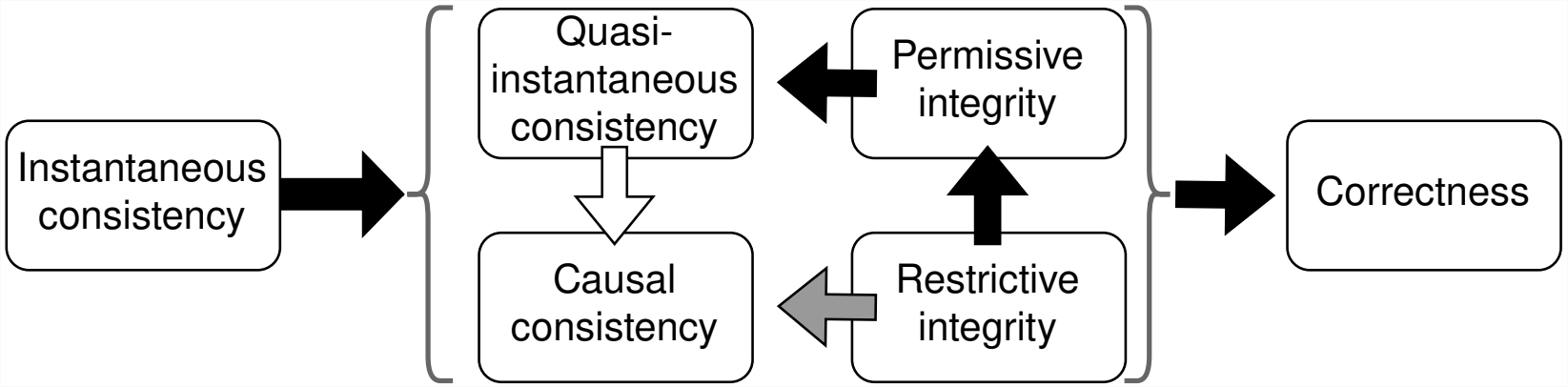
Integrity and Consistency



Integrity and Consistency



Big Picture


Instantaneous consistency
Quasi-instantaneous consistency
Causal consistency
Permissive integrity
Restrictive integrity
Correctness

What's Next?

Practical tool evaluation

- Causal consistency
- Quasi-instantaneous consistency
- Integrity?

Thank you for your attention.

References i


Pagani, Fabio, Fedorov, Oleksii and Balzarotti, Davide. "Introducing the temporal dimension to memory forensics". In: *ACM Transactions on Privacy and Security (TOPS)* 22.2 (2019), pp. 1–21.


Vömel, Stefan and Freiling, Felix C. "Correctness, atomicity, and integrity: defining criteria for forensically-sound memory acquisition". In: *Digital Investigation* 9.2 (2012), pp. 125–137.

Memory and Snapshots

- R: Set of all addressable memory regions
- T: Set of all timestamps
- V: Set of all possible values of a memory region
- Function m returns the value of a memory region for a specific point in time: $m : R \times T \to V$
- Snapshot: $s : R \to V \times T$
- s(r) = (s(r).v, s(r).t)

Consistency

Instantaneous consistency

$$\forall r, r' \in R : s(r).t = s(r').t$$

Quasi-instantaneous consistency

$$\exists s' : (\forall r, r' \in R : s'(r).t = s'(r').t) \wedge$$
$$\forall r \in R : s'(r).v = s(r).v$$

Integrity

Restrictive integrity

$$\forall r \in R : \tau \leq s(r).t \implies \forall t' \in T : \\ \tau \leq t' \leq s(r).t : s(r).v = m(r, t')$$

Permissive integrity

$$\forall r \in R : \tau \leq s(r).t \implies s(r).v = m(r, \tau)$$