

Axiomatische Gesamtformel (Frames Axiomatics) — Reine Mathematik

$$\boxed{\mathcal{F} = \langle \mathbf{F}^* \rangle, \tau, \mathrm{enc}, \mathrm{enc}_{\tau}, H, A, \mu, \mathsf{V} \rangle \text{ mit Invariante} \quad \mathsf{I}(\mathcal{F}) = \Big(h_0 = H(\epsilon) \wedge \forall i \geq 1: h_i = H(\bigvee_{f_i} \tau(f_i)) \wedge \bigvee_{f_i} \mathrm{enc}(f_i) \Big) \wedge \Big(\forall k < \ell: S_k = \mathrm{prefix}_k(S_{\ell}) \Big)}$$

Kurzbeschreibung (formal):

$\mathbf{F}^* = (f_i)_{i \geq 1}$ ist eine Framefolge;
 $S_k := (f_1, \dots, f_k)$.

Die Integrität ist durch die Hashkette (h_i) gegeben.

Append-only ist die Präfix-Invariante $S_k = \mathrm{prefix}_k(S_{\ell})$ für $k < \ell$.