Blockchains as Kripke models: an Analysis of Atomic Cross-Chain Swap

Yoichi Hirai

Limassol, 2018-11-05

Atomic Cross-Chain Swap vs Chandy-Misra

"Atomic Swap" protocols swap tokens on different blockchains atomically.

No asynchronous communication can create a new piece of common knowledge [Chandy, Misra: How Processes Learn, 1986].

"Atomic Swap" should require some synchrony. What kind of?

Atomic Cross-Chain Swap Uses Hash Lock

To spend the fund in a hash lock,

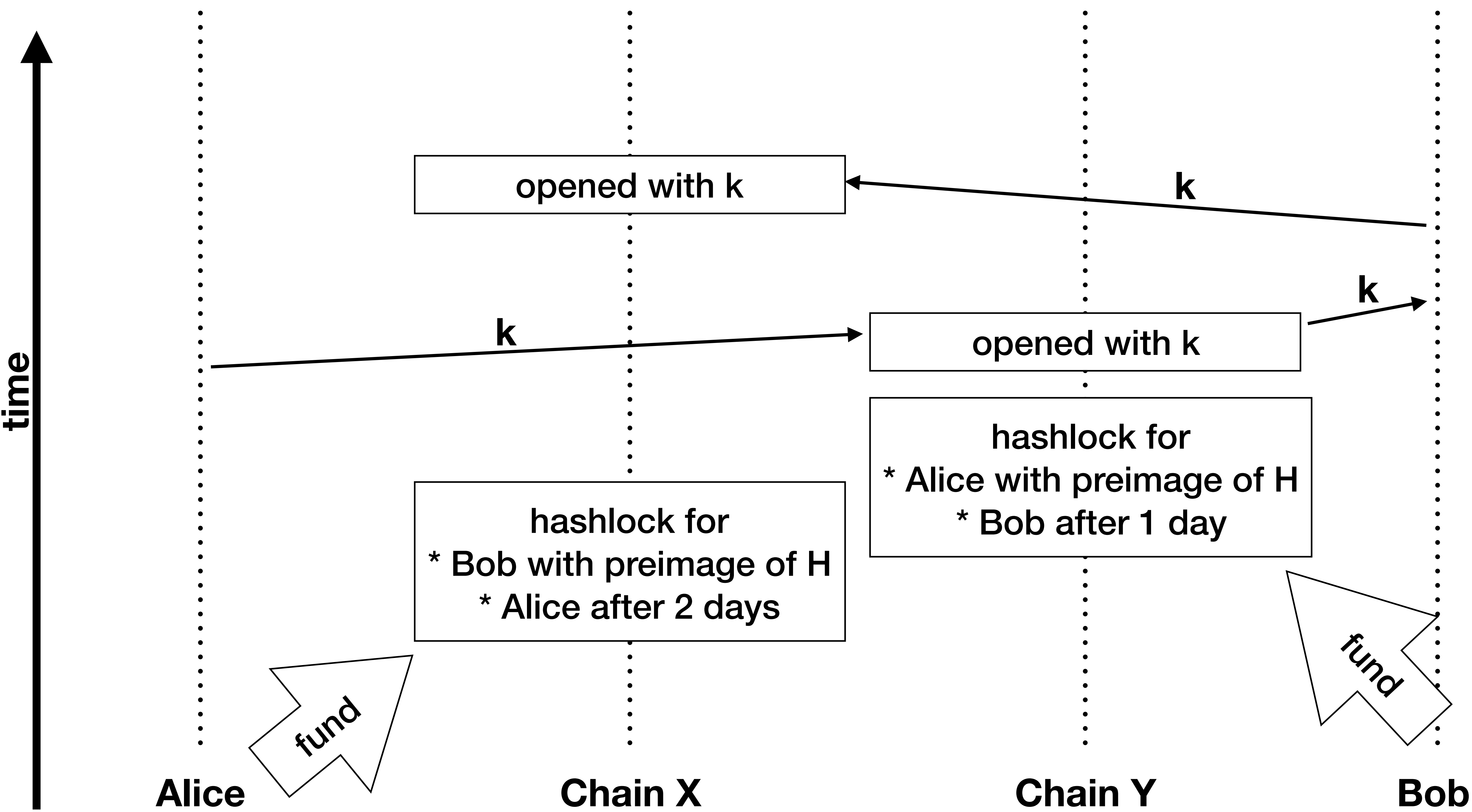
the first way is

1. with Bob's signature
2. with input whose hash is H
3. before the deadline.

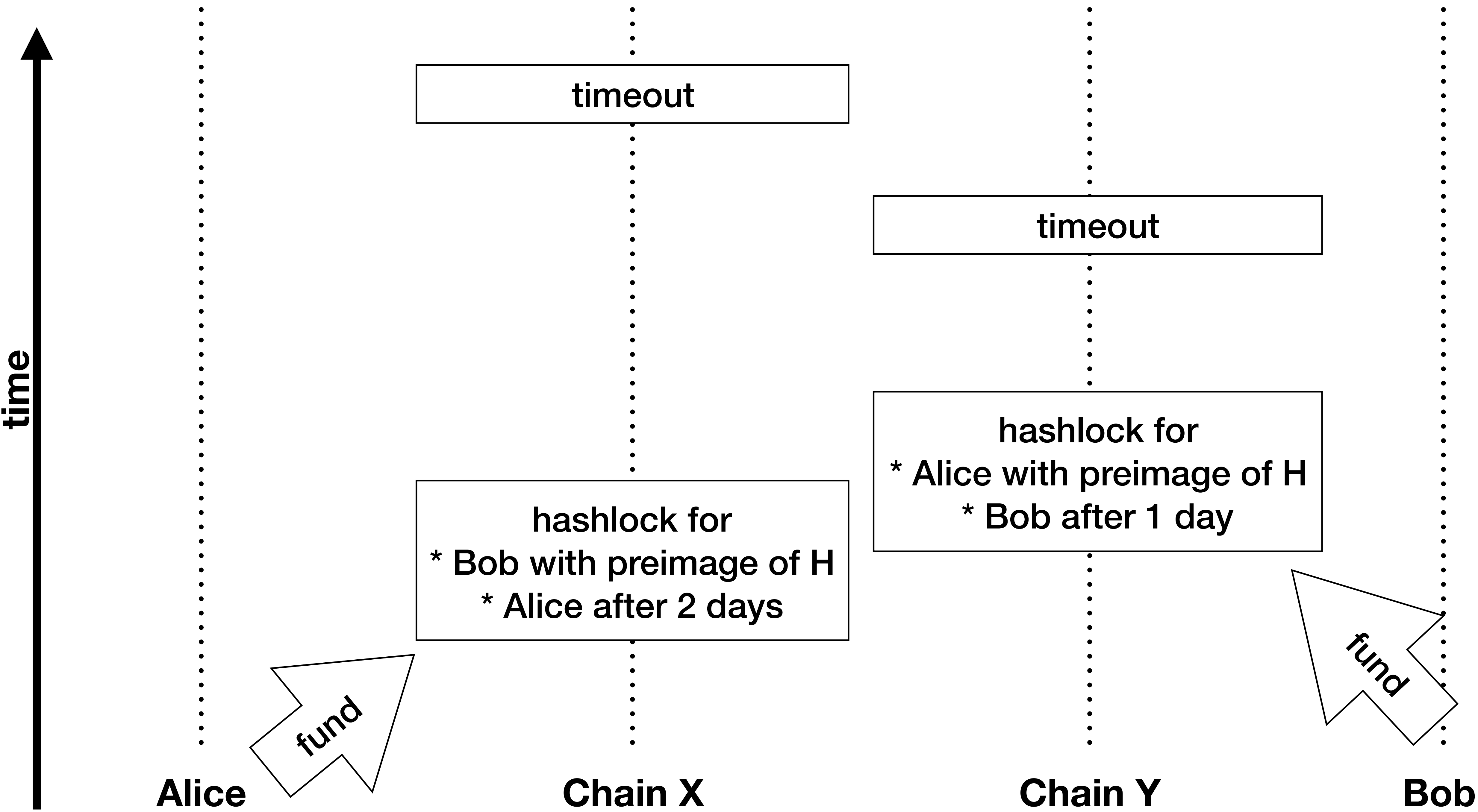
the second way is

1. with Alice's signature
2. after the deadline.

Atomic Cross-Chain Swap
Success Case



Atomic Cross-Chain Swap Failure Case



Observations

Obs. 1 Properties dependent on states.

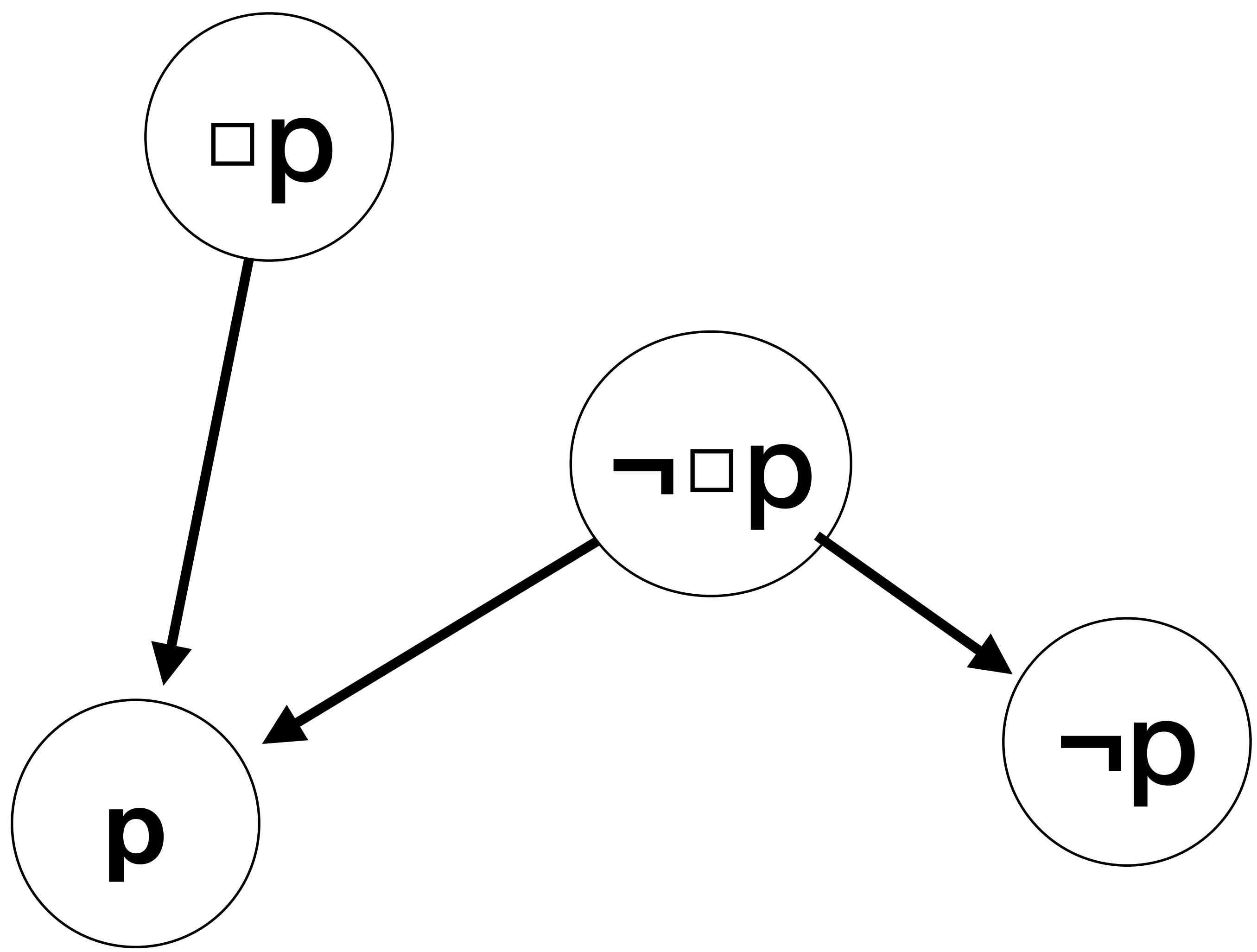
Obs. 2 Most interesting properties are persistent.

e.g.

Once a hashlock is opened, it remains opened.
Once a secret is revealed on a blockchain, it remains revealed.

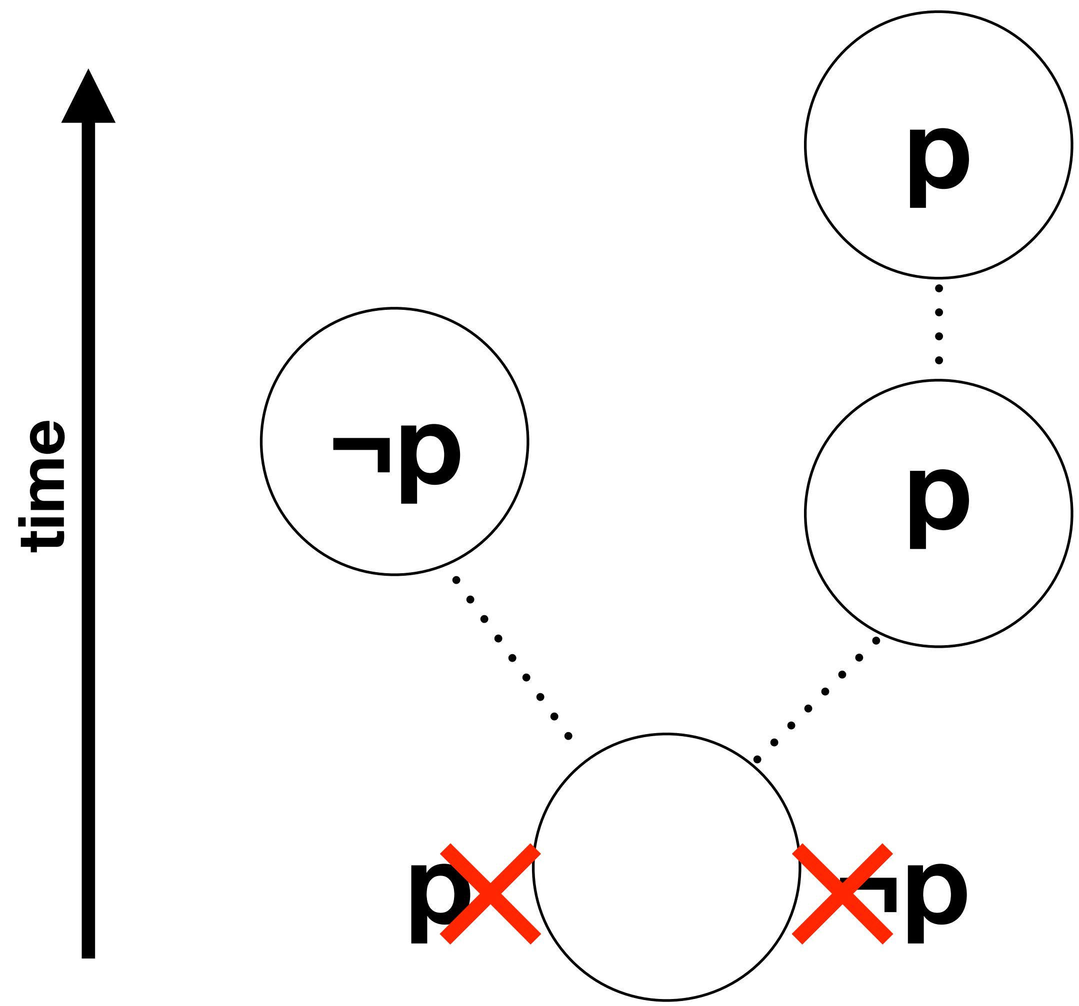
Obs. 3 “Bob knows chain Y has something.”

Obs. 1 Properties dependent on local states.
→ Kripke Models



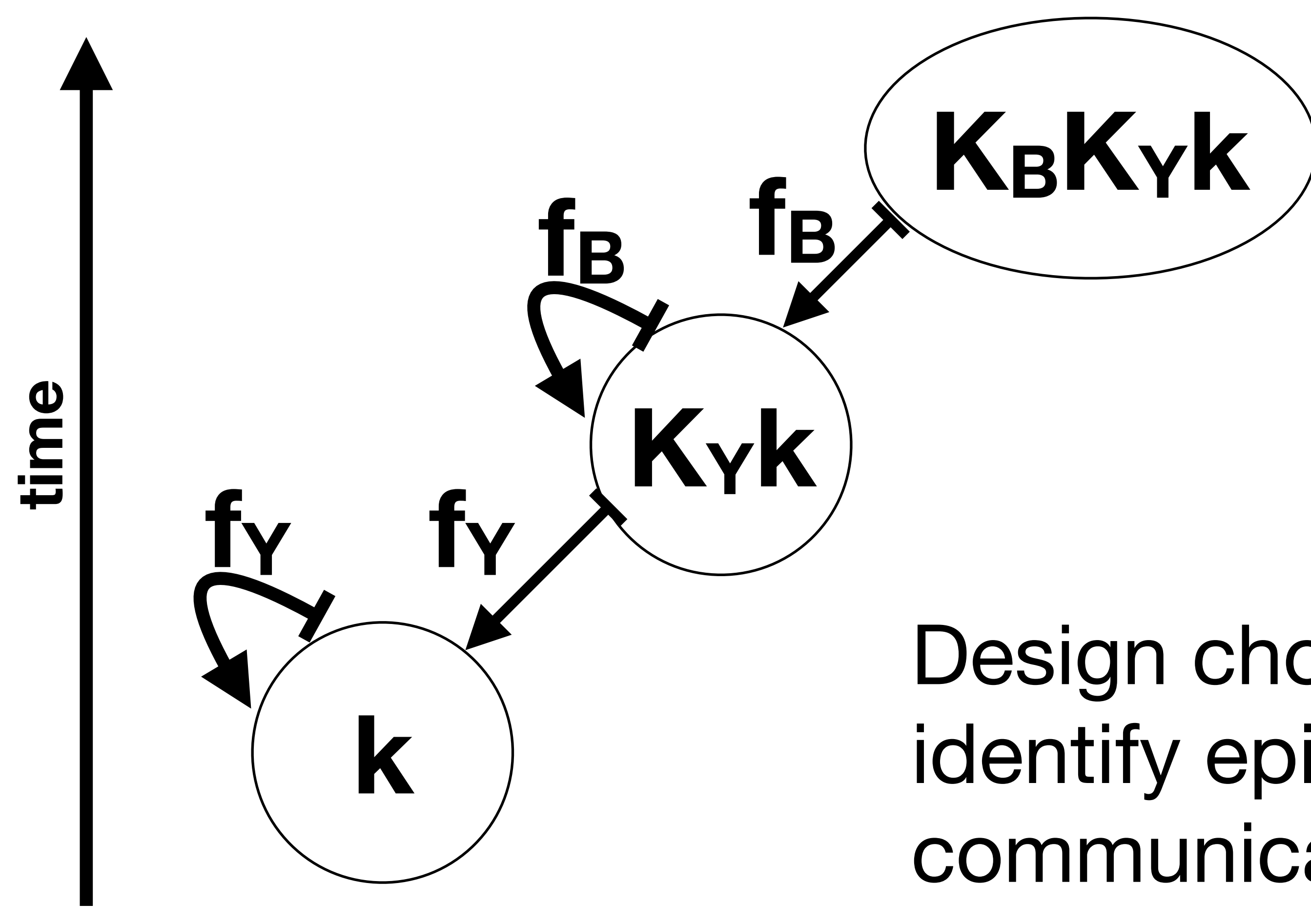
Obs. 2 Most interesting properties are persistent.

Kripke models with persistent properties ~ model of intuitionistic logic



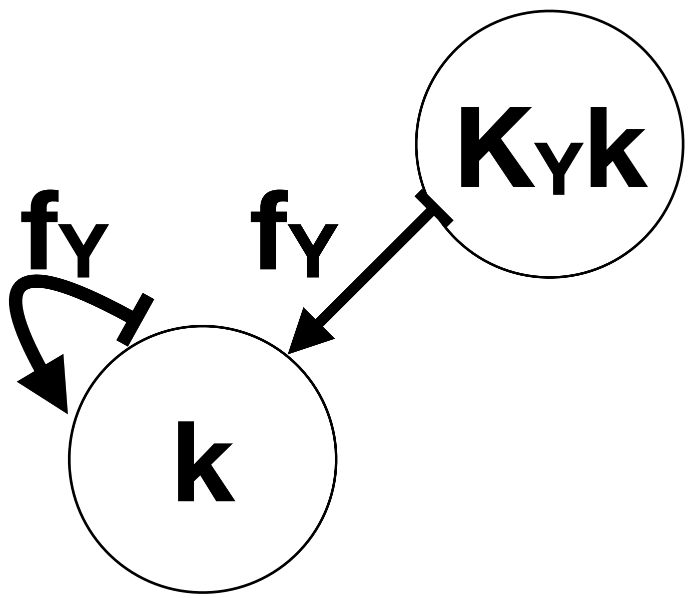
Obs. 3 “Bob knows chain Y has something.”

The logic needs epistemic modality.



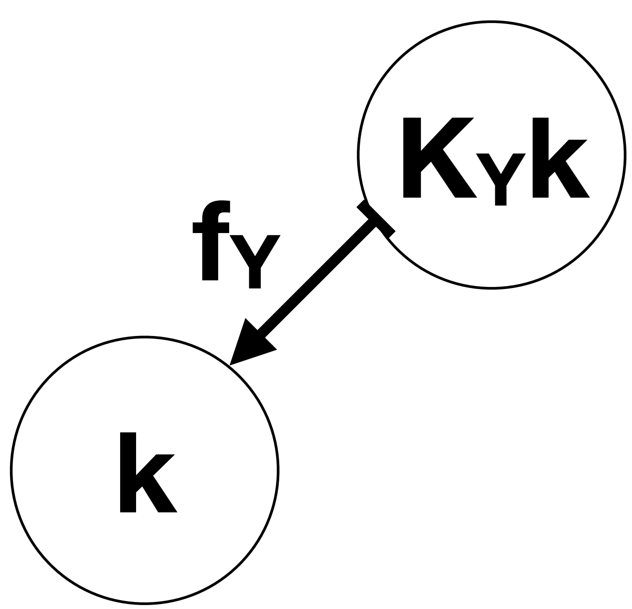
Design choice [Hirai, LPAR-16]: identify epistemic modality with communication

Some valid formulas



$K_Y k \supset K_Y K_Y k$

only consider models where f_Y is idempotent



$K_Y k \supset k$

only consider models where f_Y points to the past
(and all formulas are persistent)

Features of a hash lock

D_2 **two days have passed** $\mathtt{k}$ **secret**

B_X **Bob has opened the hashlock on chain X**

$\neg\mathrm{B}_\mathrm{X}$ **Bob never opens the hashlock on chain X**

$$K_\mathrm{X}(\mathrm{D}_2 \supset ((\mathrm{B}_\mathrm{X} \wedge \mathtt{k}) \vee \neg\mathrm{B}_\mathrm{X})). \qquad \text{(X-live1)}$$

$$K_\mathrm{X}(\mathrm{D}_2 \vee (K_\mathrm{Bob}\mathtt{k} \supset \mathrm{B}_\mathrm{X})). \qquad \text{(X-live2)}$$

$$\mathrm{B}_\mathrm{X} \supset K_\mathrm{X} K_\mathrm{Bob}\mathtt{k}. \qquad \text{(X-safe)}$$

Another hashlock

$$K_{\mathrm{Y}}(\mathrm{D}_1 \supset ((\mathrm{A}_{\mathrm{Y}} \wedge \mathtt{k}) \vee \neg \mathrm{A}_{\mathrm{Y}})). \qquad \text{(Y-live1)}$$

$$K_{\mathrm{Y}}(\mathrm{D}_1 \vee (K_{\mathrm{Alice}}\mathtt{k} \supset \mathrm{A}_{\mathrm{Y}})). \qquad \text{(Y-live2)}$$

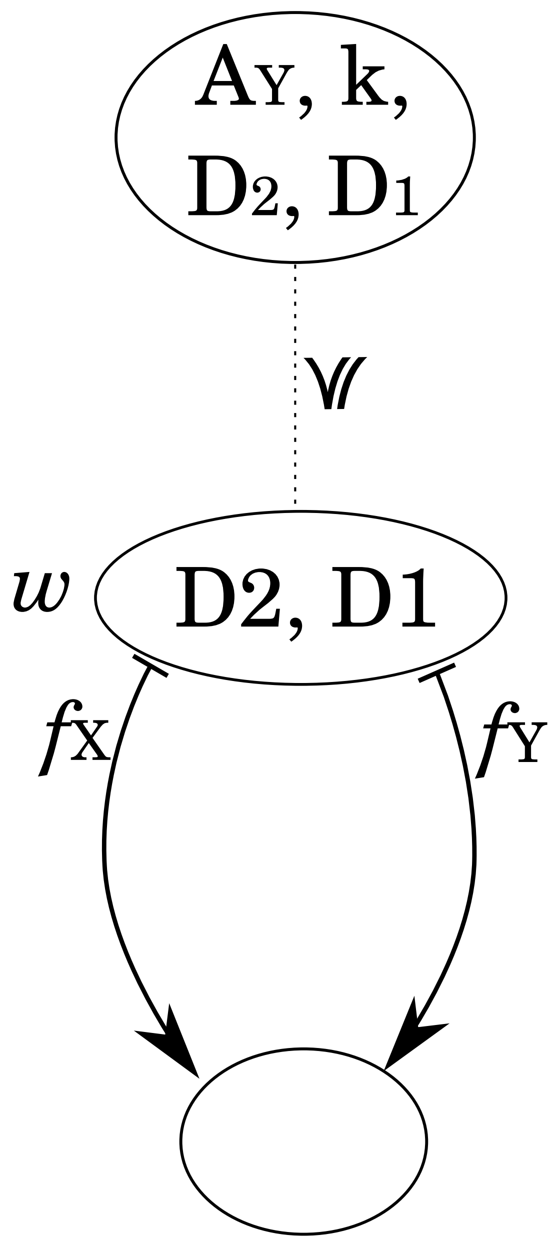
$$\mathrm{A}_{\mathrm{Y}} \supset K_{\mathrm{Y}}\mathtt{k}. \qquad \text{(Y-safe)}$$

and a timing constraint

$$\mathrm{D}_2 \supset \mathrm{D}_1. \qquad \text{(Days)}$$

These don't imply binary outcomes.

$$\mathrm{D}_2 \supset ((\mathrm{A}_\mathrm{Y} \wedge \mathrm{B}_\mathrm{X}) \vee ((\neg \mathrm{A}_\mathrm{Y}) \wedge (\neg \mathrm{B}_\mathrm{X}))). \qquad \text{(Binary-Outcome)}$$



$$K_\mathrm{X}(\mathrm{D}_2 \supset ((\mathrm{B}_\mathrm{X} \wedge \mathtt{k}) \vee \neg \mathrm{B}_\mathrm{X})).$$

$$K_\mathrm{X}(\mathrm{D}_2 \vee (K_\mathrm{Bob}\mathtt{k} \supset \mathrm{B}_\mathrm{X})).$$

$$\mathrm{B}_\mathrm{X} \supset K_\mathrm{X} K_\mathrm{Bob}\mathtt{k}.$$

$$K_\mathrm{Y}(\mathrm{D}_1 \supset ((\mathrm{A}_\mathrm{Y} \wedge \mathtt{k}) \vee \neg \mathrm{A}_\mathrm{Y})).$$

$$K_\mathrm{Y}(\mathrm{D}_1 \vee (K_\mathrm{Alice}\mathtt{k} \supset \mathrm{A}_\mathrm{Y})).$$

$$\mathrm{A}_\mathrm{Y} \supset K_\mathrm{Y}\mathtt{k}.$$

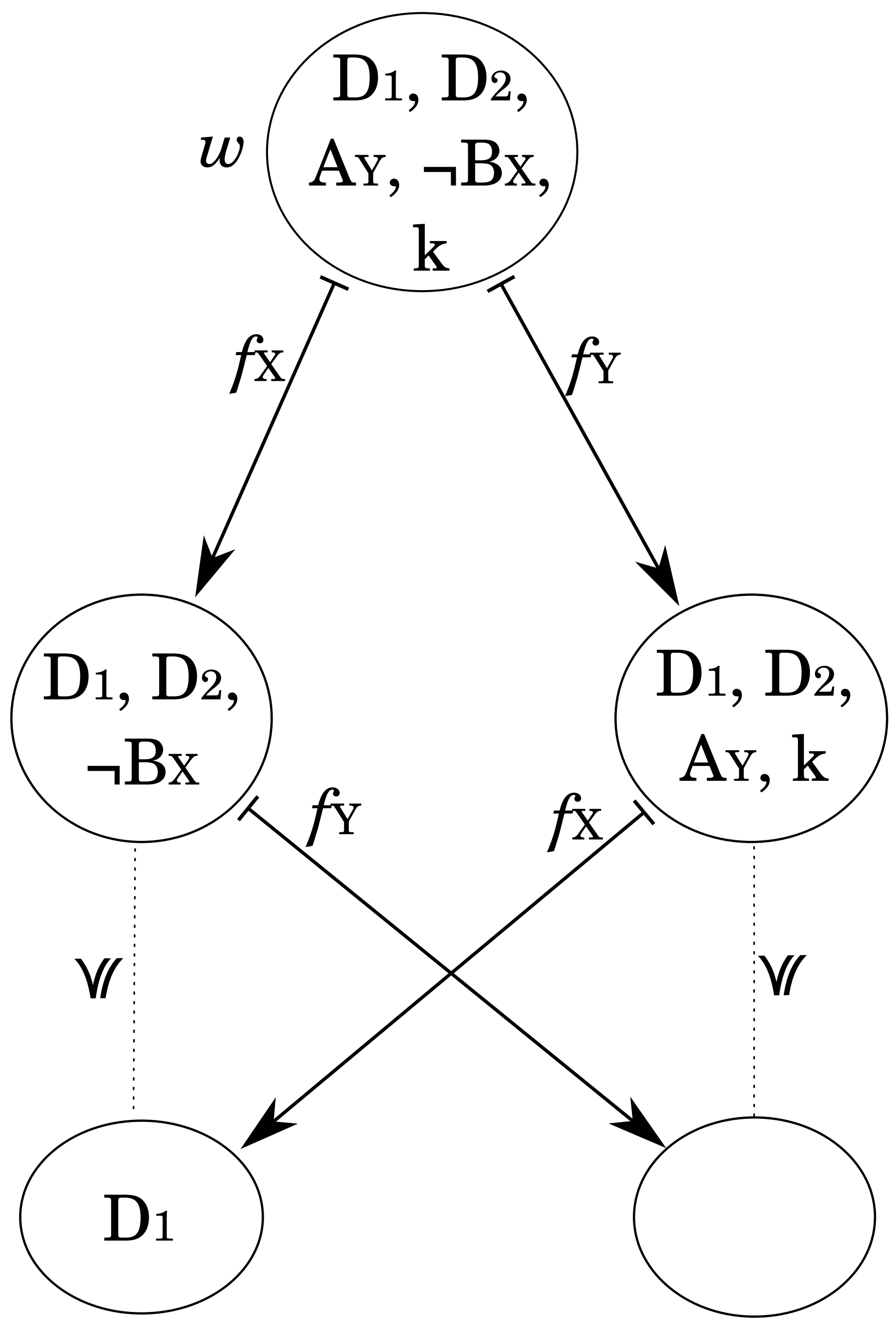
$$\mathrm{D}_2 \supset \mathrm{D}_1.$$

Each function f_a is identity whenever not explicitly shown.

Then Require Blocks on Both Chains after Day 2

$$K_X D_2 \supset (K_Y D_2 \supset ((A_Y \wedge B_X) \vee ((\neg A_Y) \wedge \neg B_X))). \quad \text{(Weak-Binary-Outcome)}$$

X timed out



though transfer occurred on Y

X after two days knows nothing about Y after one day.

What makes it work?

Anything that reaches blockchain Y by 1 + 1/4 days also reaches Bob, and chain X by 1 + 1/2 days.

$$(K_{\mathrm{Y}} K_{1\frac{1}{4}} \varphi) \supset K_{\mathrm{X}} K_{1\frac{1}{2}} K_{\mathrm{Bob}} K_{\mathrm{Y}} K_{1\frac{1}{4}} \varphi. \qquad \text{(Bob-has-chance)}$$

By 2 days, blockchain Y sees, the hashlock on Y has been open or timeout since 1 + 1/4 days.

$$K_{\mathrm{Y}}(\mathrm{D}_2 \supset K_{1\frac{1}{4}}((\mathrm{A}_{\mathrm{Y}} \wedge \mathtt{k}) \vee (\neg \mathrm{A}_{\mathrm{Y}}))). \qquad \text{(Y-timed1)}$$

By the time Bob gets the secret, Alice has opened the hashlock on Y.

$$K_{\mathrm{Bob}} \mathtt{k} \supset \mathrm{A}_{\mathrm{Y}}. \qquad \text{(Alice-opsec)}$$

If chain X sees the secret signed by Bob by 1 + 1/2 days, the hash lock opens on X.

$$K_{\mathrm{X}} K_{1\frac{1}{2}}((K_{\mathrm{Bob}} \mathtt{k}) \supset \mathrm{B}_{\mathrm{X}}). \qquad \text{(X-live}1\tfrac{1}{2}\text{)}$$

Then it works somehow.

If a model satisfies (X-live2), (Y-timed1), (Alice-opsec), (Bob-has-chance), (X-live 1+1/2) at every state,

the model also satisfies (Weak-Binary-Outcome) at every state.

Proof: reasoning on the models or deductions?

I chose to reason about Kripke models directly

rather than using

$$\text{(}{\supset}\text{-I)}\;\dfrac{\text{(nec)}\;\dfrac{\text{(}{\supset}\text{-E)}\;\dfrac{\text{(ax)}\;\dfrac{}{K_{\mathsf{m}} K_a \varphi \vdash_{\mathrm{sc}} K_{\mathsf{m}} K_a \varphi} \qquad \text{(ax)}\;\dfrac{}{K_{\mathsf{m}} K_a \varphi \supset K_{\mathsf{m}} K_b \psi \vdash_{\mathrm{sc}} K_{\mathsf{m}} K_a \varphi \supset K_{\mathsf{m}} K_b \psi}}{K_{\mathsf{m}} K_a \varphi,\ K_{\mathsf{m}} K_a \varphi \supset K_{\mathsf{m}} K_b \psi \vdash_{\mathrm{sc}} K_{\mathsf{m}} K_b \psi}}{K_a K_{\mathsf{m}} K_a \varphi,\ K_a (K_{\mathsf{m}} K_a \varphi \supset K_{\mathsf{m}} K_b \psi) \vdash_{\mathrm{sc}} K_a K_{\mathsf{m}} K_b \psi}}{K_a K_{\mathsf{m}} K_a \varphi \vdash_{\mathrm{sc}} K_a (K_{\mathsf{m}} K_a \varphi \supset K_{\mathsf{m}} K_b \psi) \supset K_a K_{\mathsf{m}} K_b \psi}$$

because, defining a deduction system takes space.
and the formal proof is not smaller than the English proof on models.

Discussion

"1 + 1/2 days" and "1 + 1/4 days" are arbitrary.

Failed to capture probabilistic aspects.

Finality of blockchains are hidden in "$K_{\mathrm{Bob}} K_{\mathrm{Y}}$ …" being persistent.

Moreover, Bob never mistakenly believes finality.

Players' strategies are missing.