

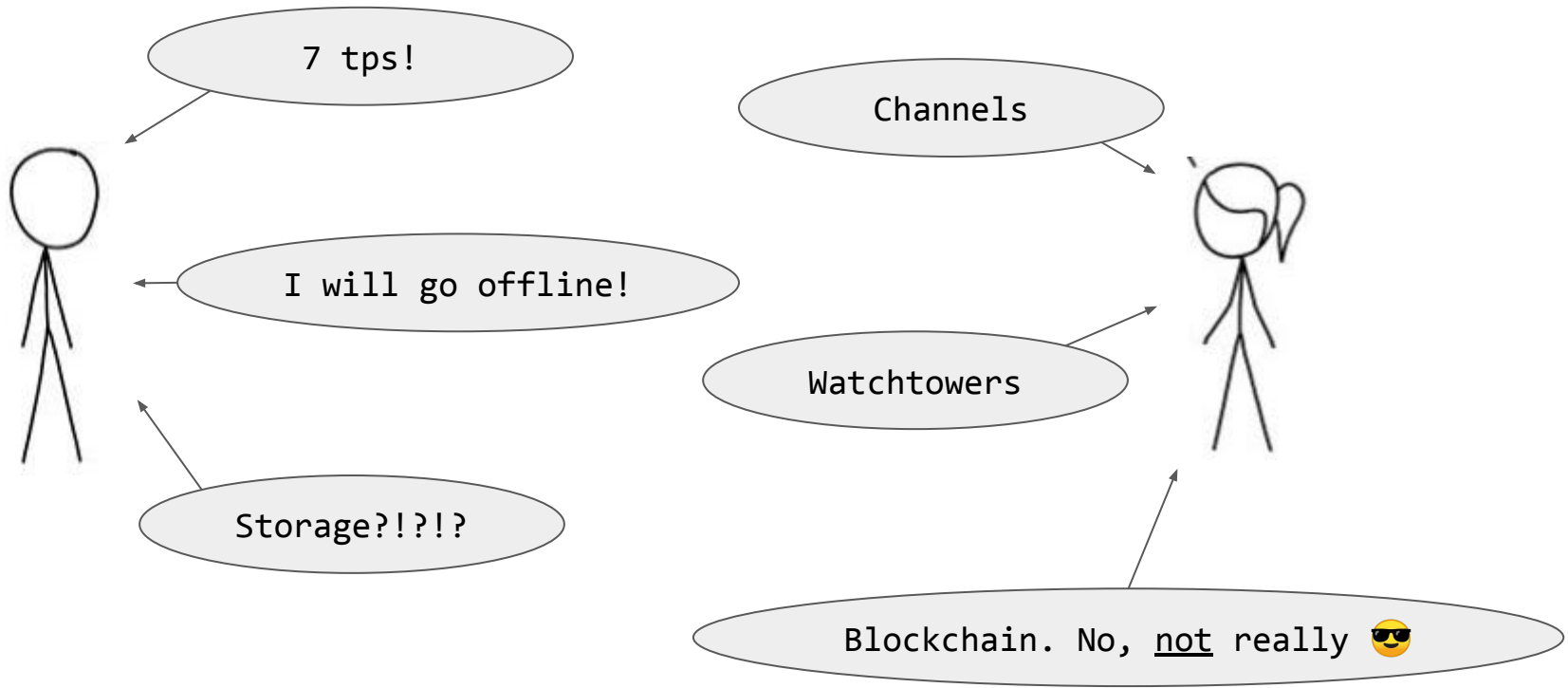
Outpost: A Lightweight Responsive Watchtower



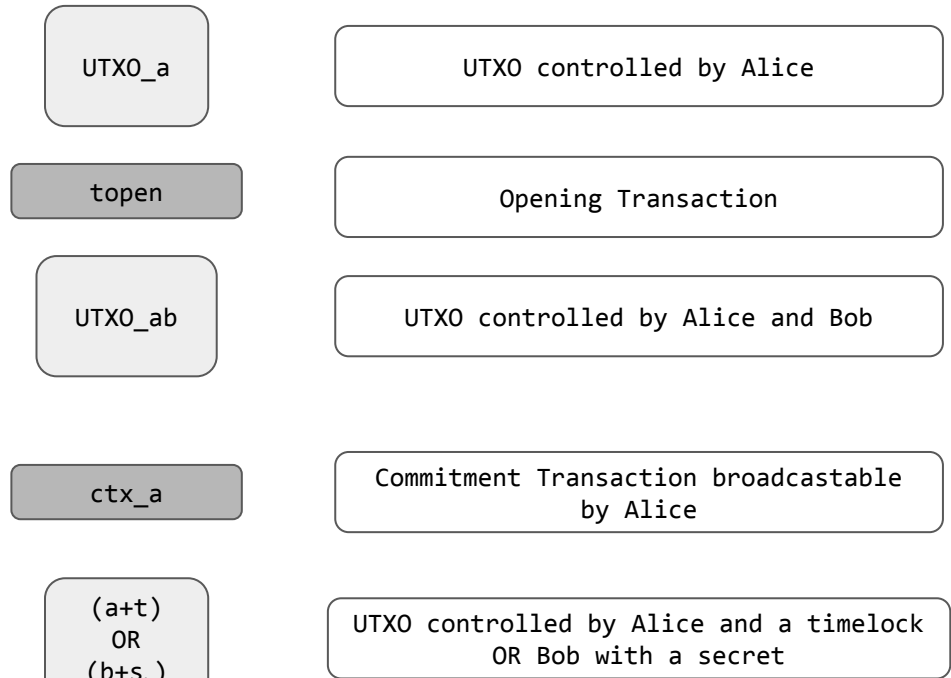
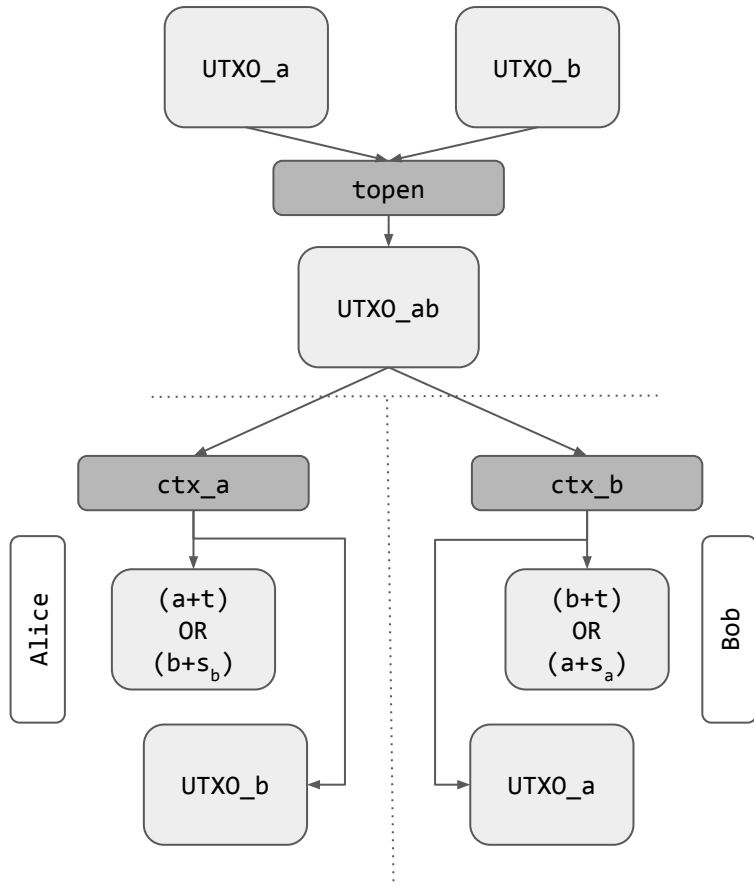
eth = Eidgenössische Technische Hochschule
(Federal Institute of Technology)

Tejaswi Nadahalli (*ETH Zürich*)
Majid Khabazzian (*Univ. of Alberta*)
Roger Wattenhofer (*ETH Zürich*)

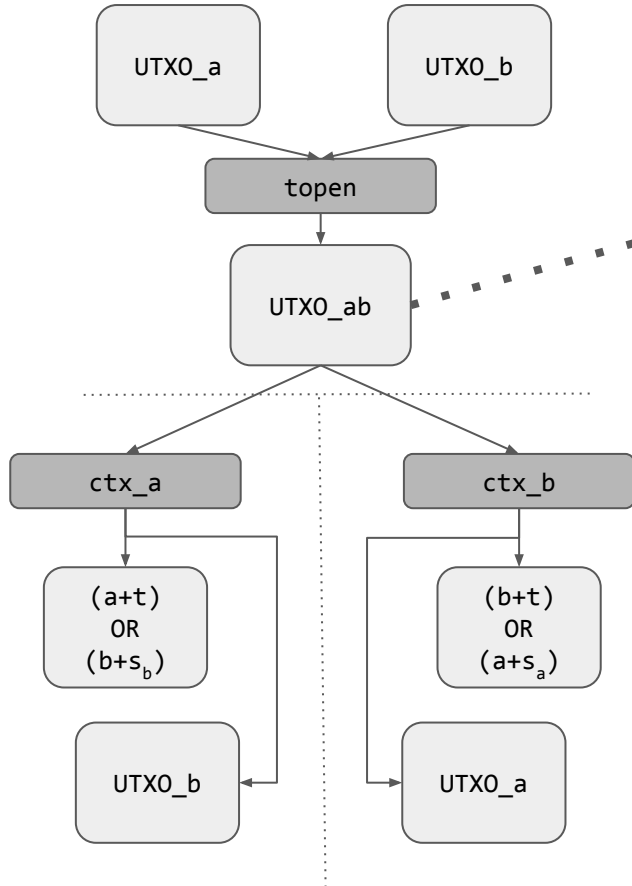
What's happening?



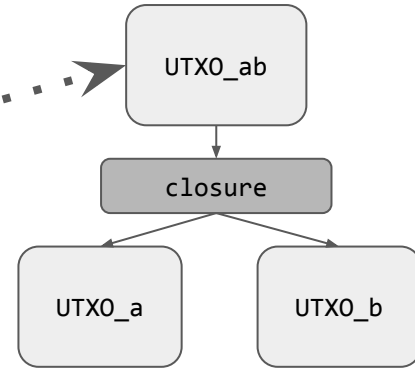
Lightning Channel



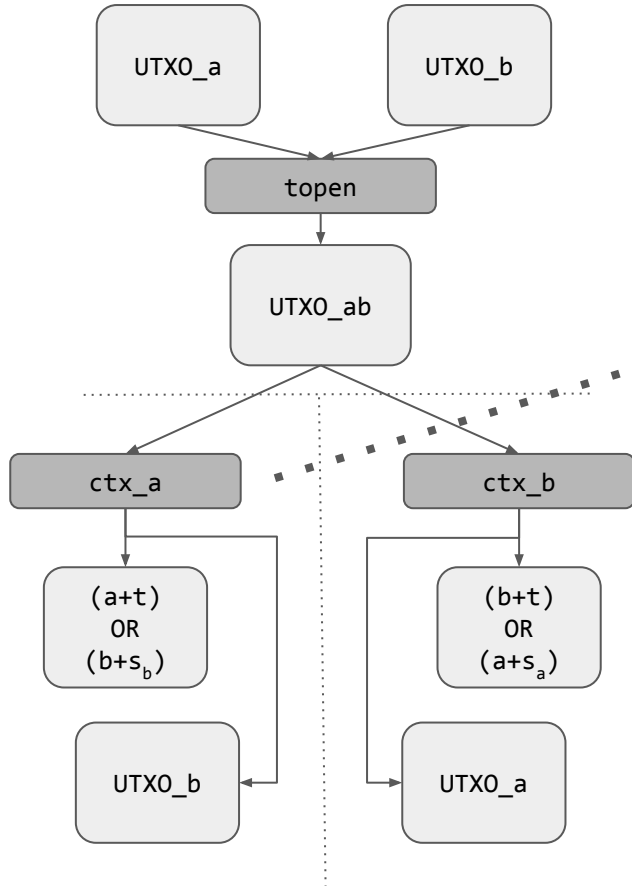
Lightning Channel



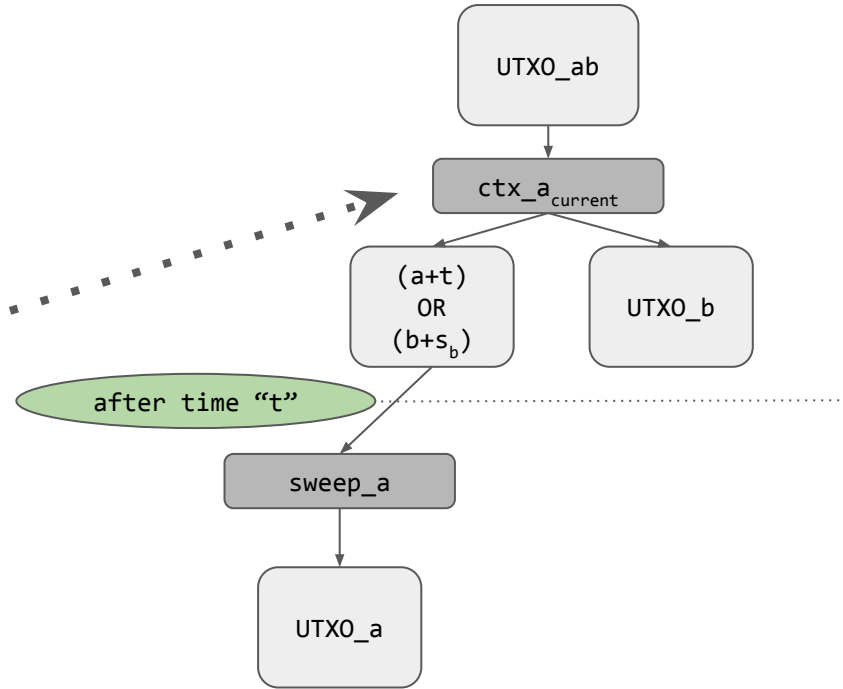
Bilateral Closure



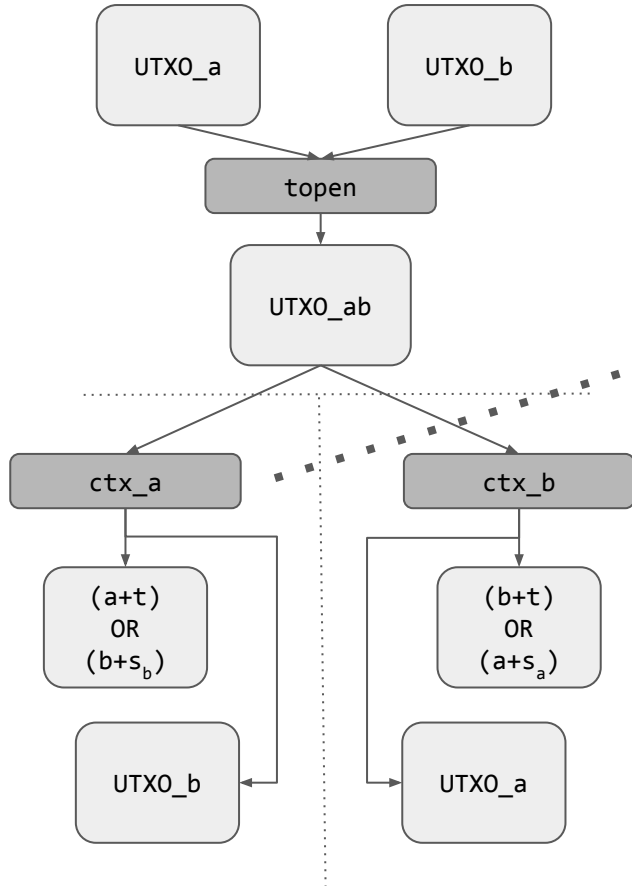
Lightning Channel



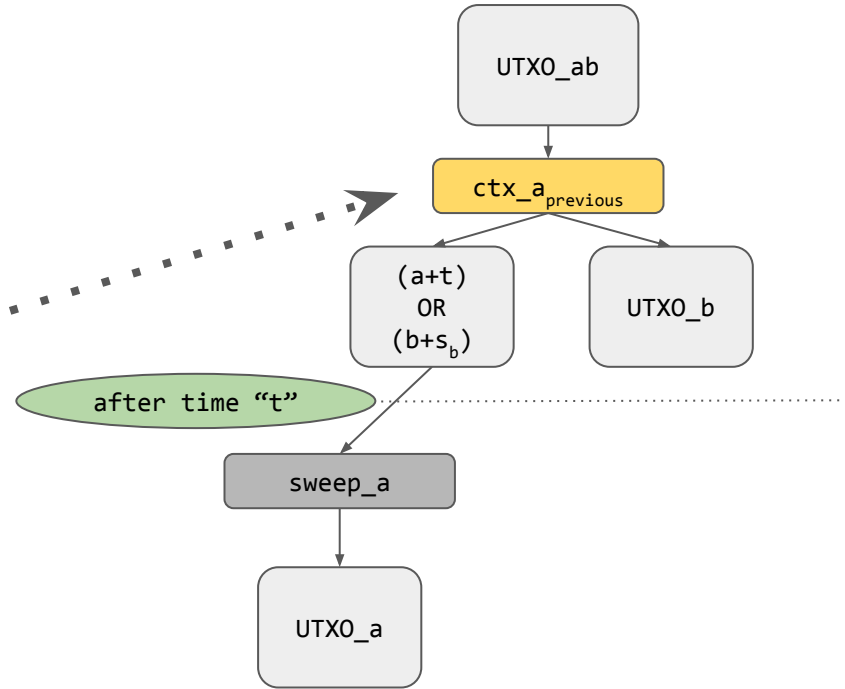
Unilateral Closure



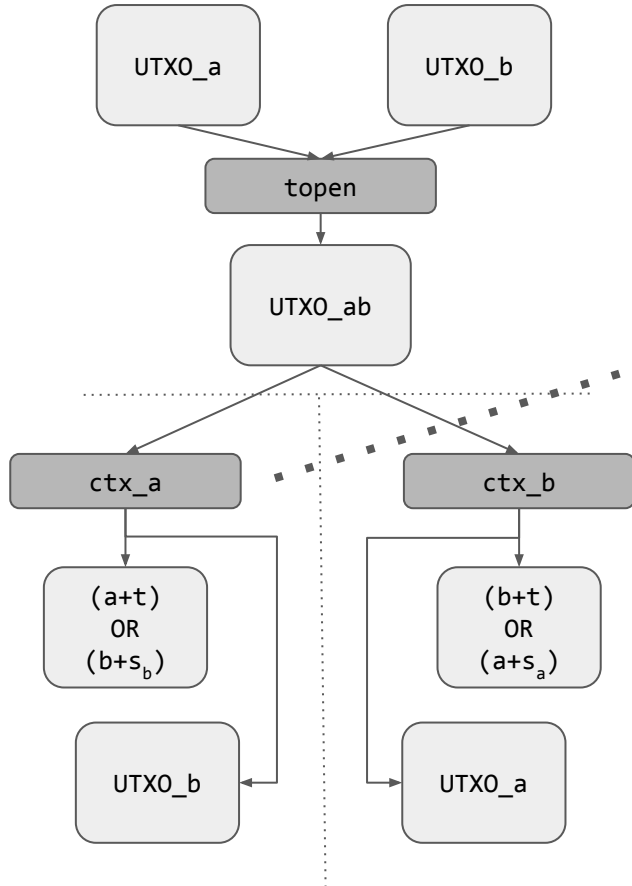
Lightning Channel



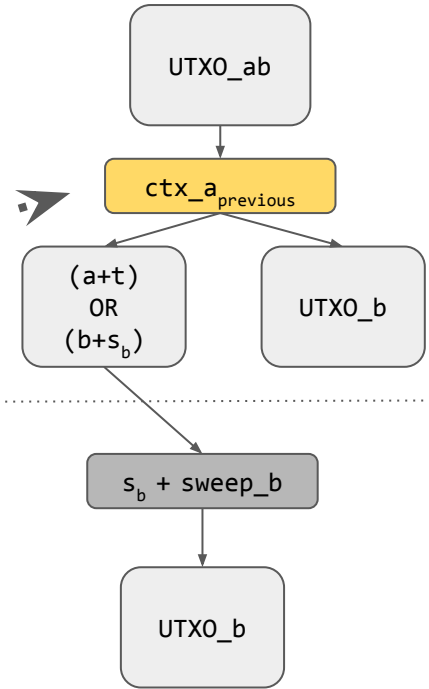
Cheating Closure



Lightning Channel



Justice Transaction

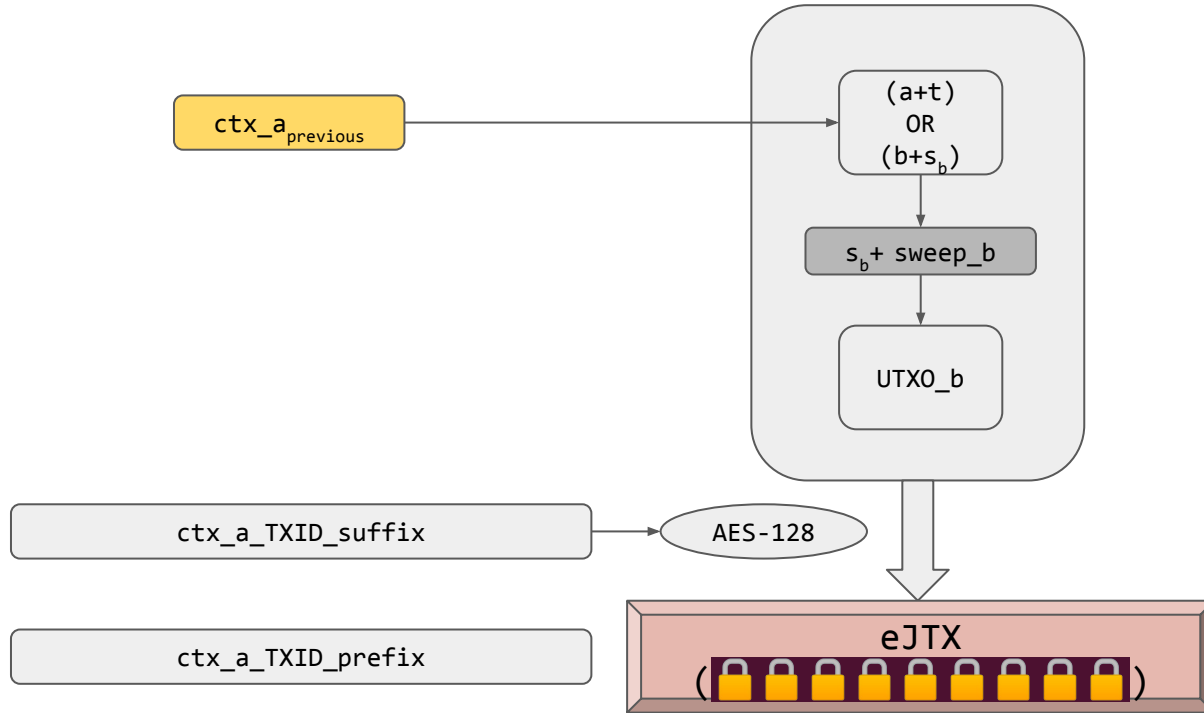


Offline...









Watchtower

Justice Kit



Watchtower

e3b0c44298...	
6e340b9cff...	
96a296d224...	
709e80c884...	
df3f619804...	
8855508aad...	
...	...
...	...

Observations

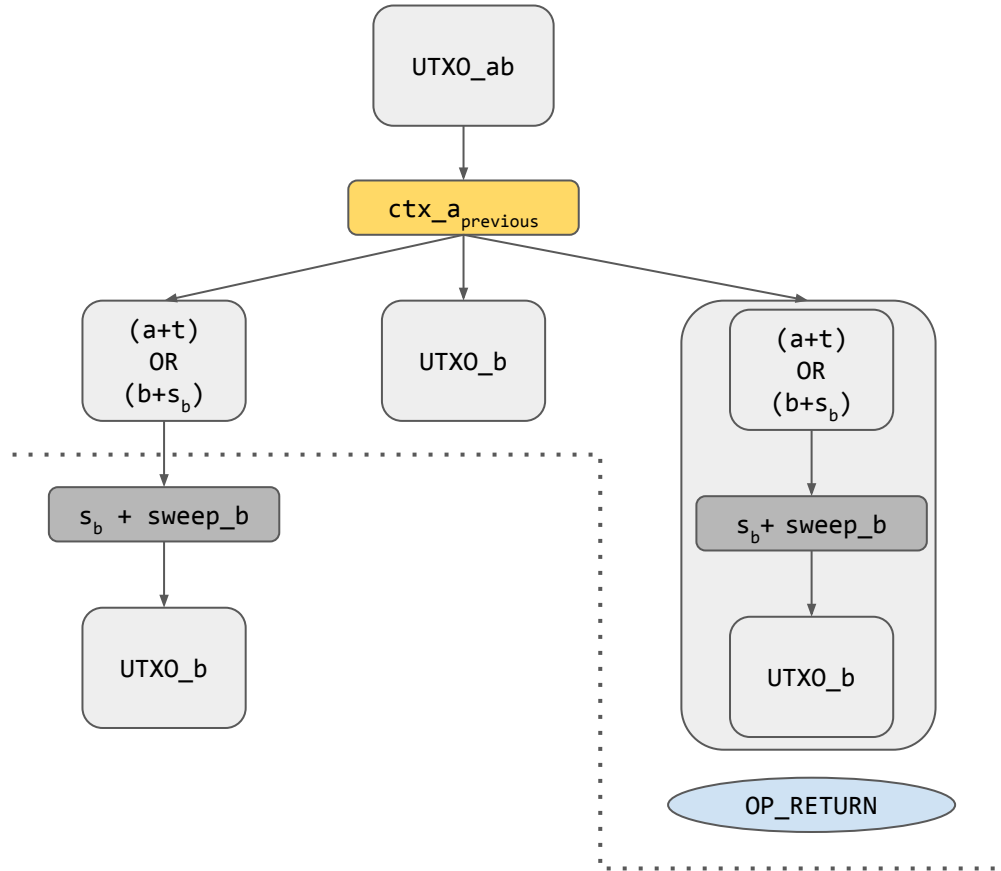
Cheater has to store cheating CTX(s)

Every CTX has a corresponding JTX

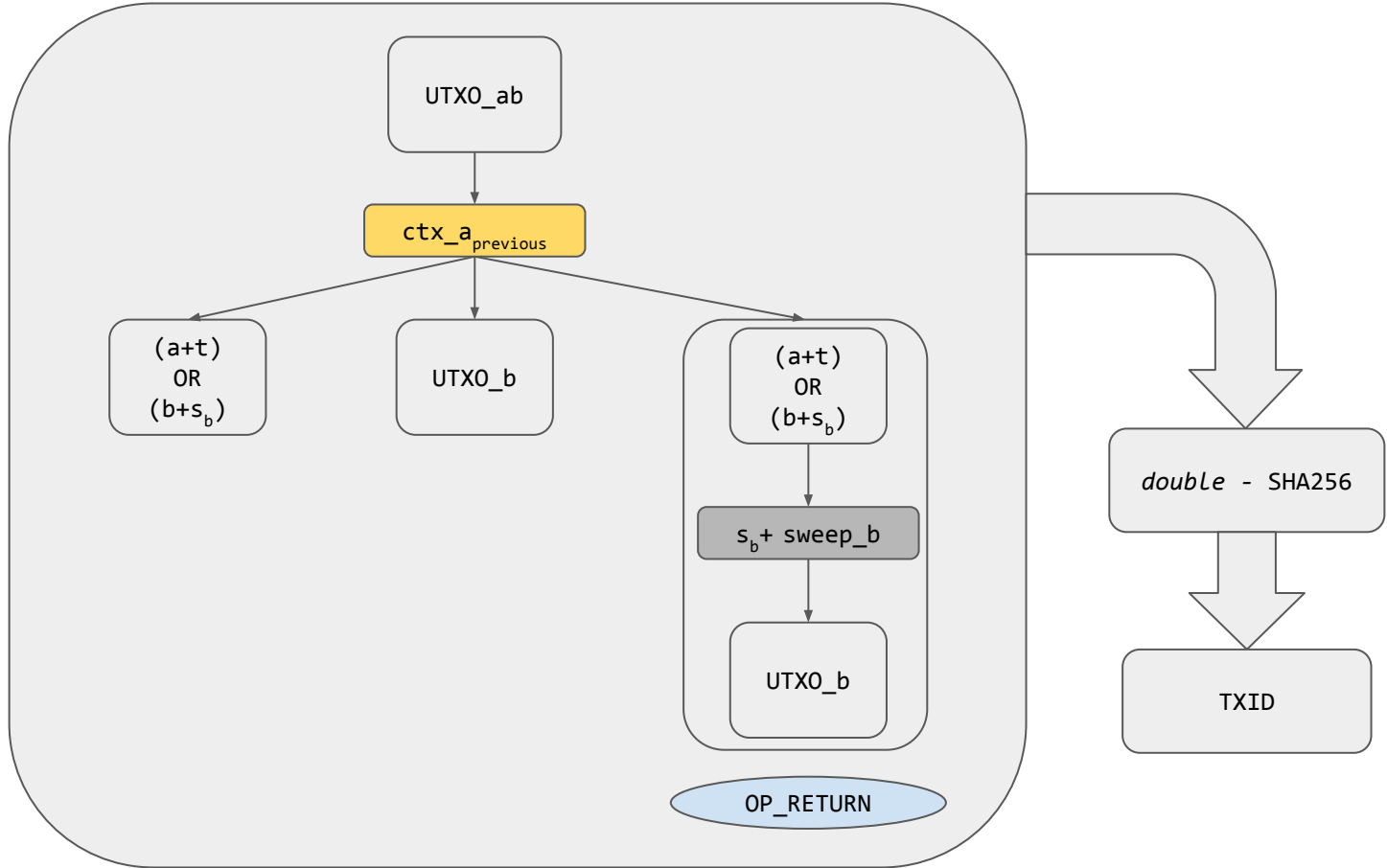
CTX has to be published on the blockchain

Store the corresponding JTX inside this CTX?

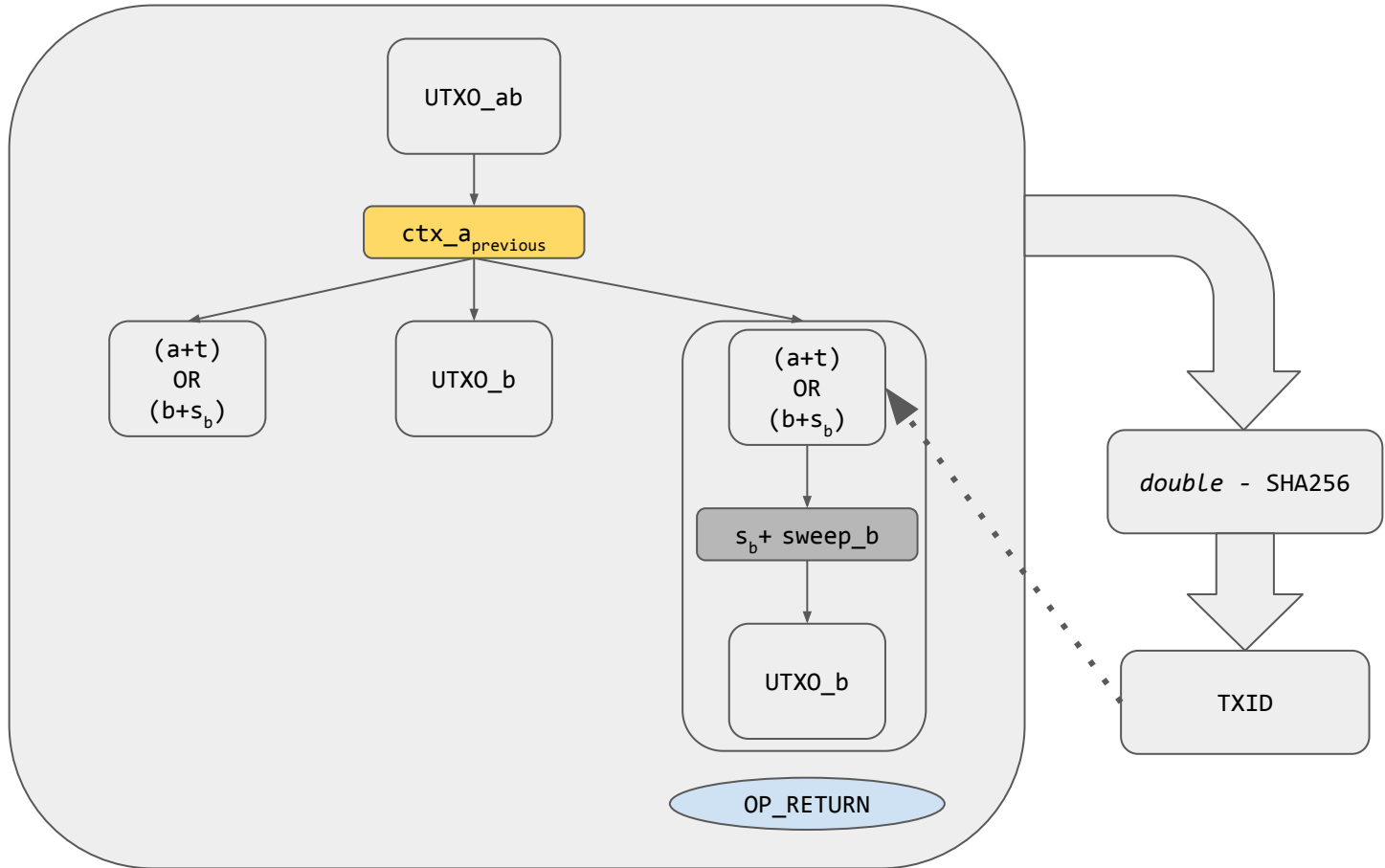
Can we store JTX inside CTX?



TXID



TXID makes it self-referential



OP_RETURN alternatives

P2SH Data Drop

- vulnerable to scriptSig malleability

P2SH Data Hash

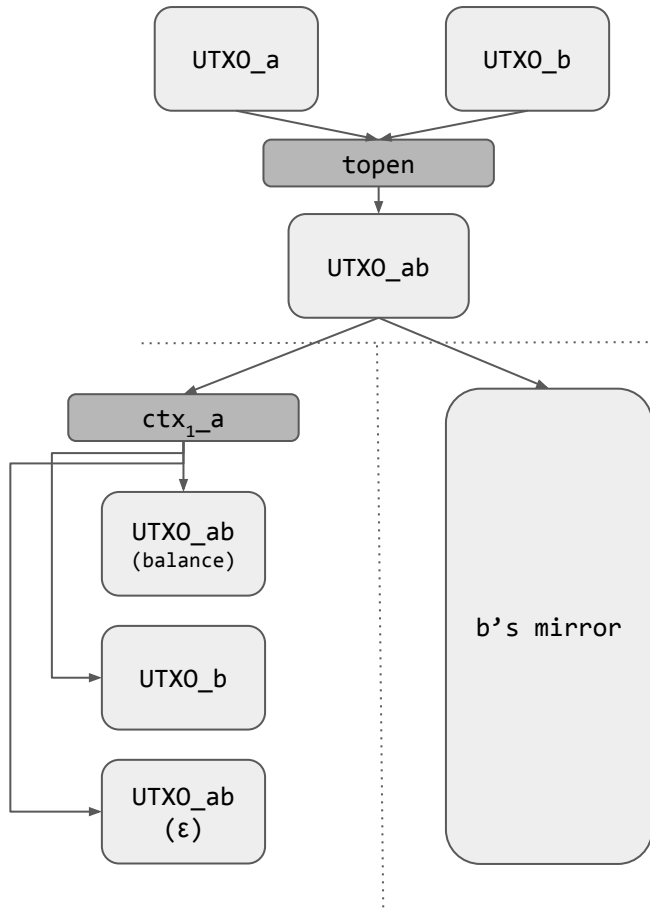
- vulnerable to self-loop in the redeem_script hash

SIGHASH_NOINPUT

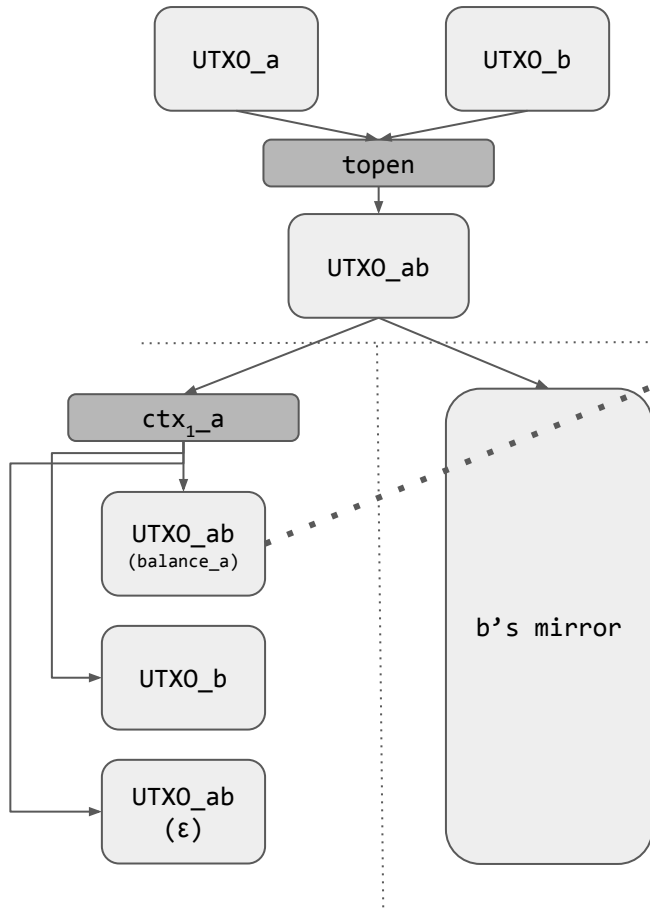
- If Eltoo, why Lightning?

Outpost

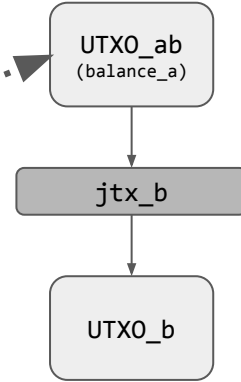
Outpost



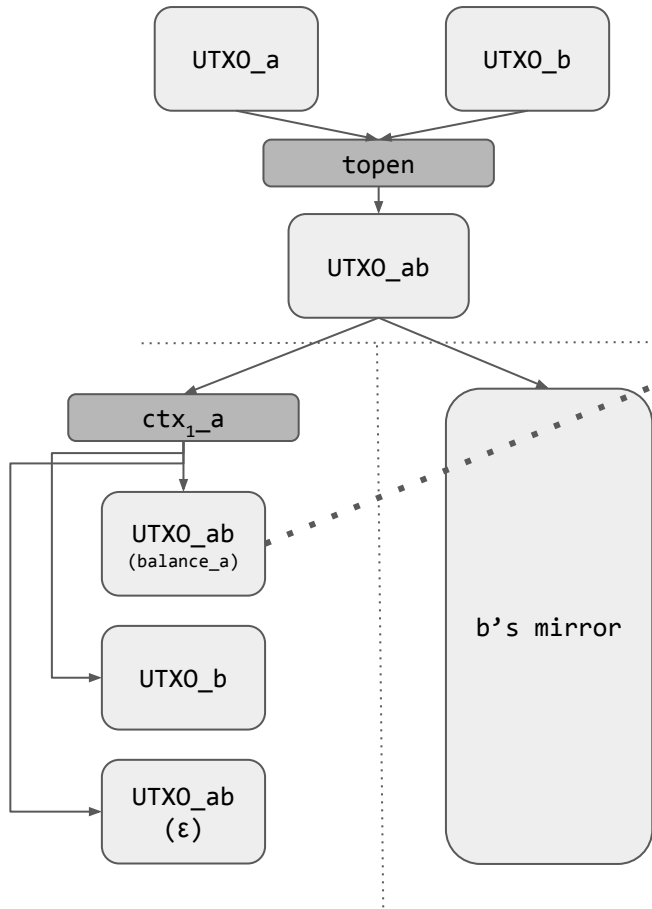
Outpost



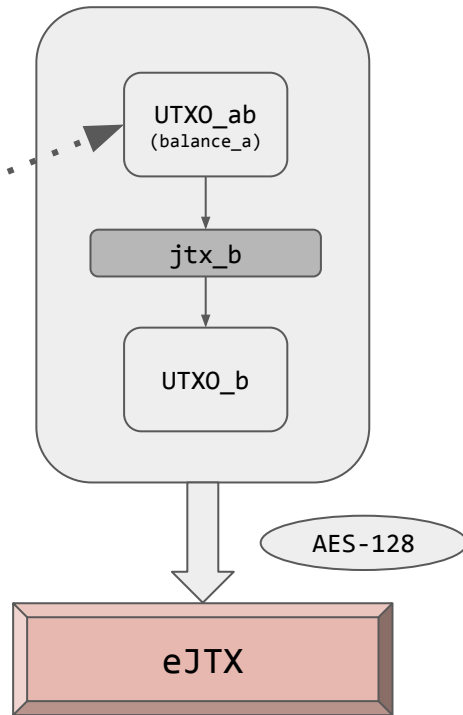
Justice Transaction



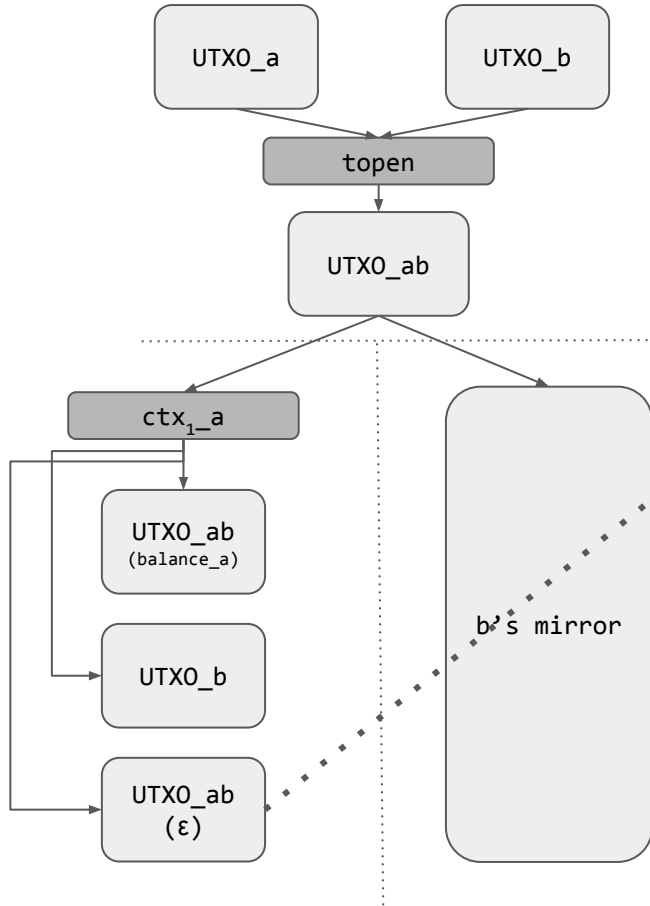
Outpost



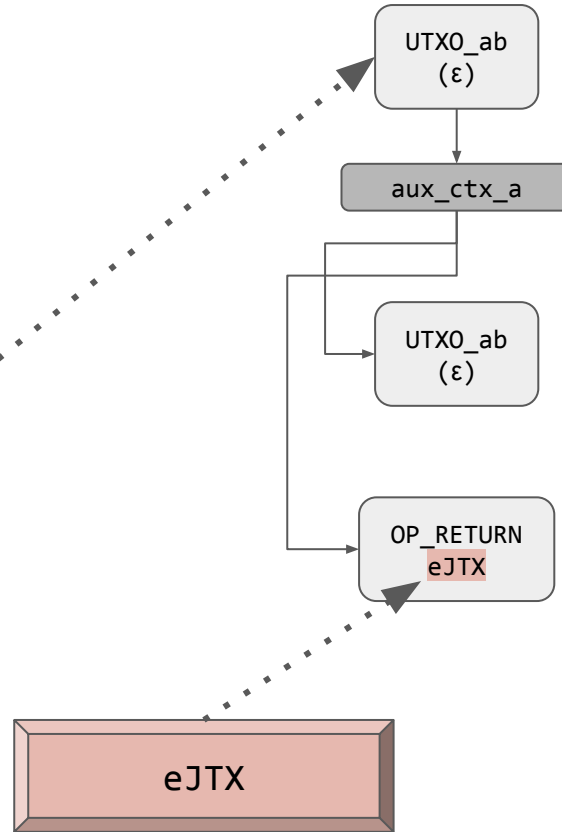
Encrypted Justice Transaction



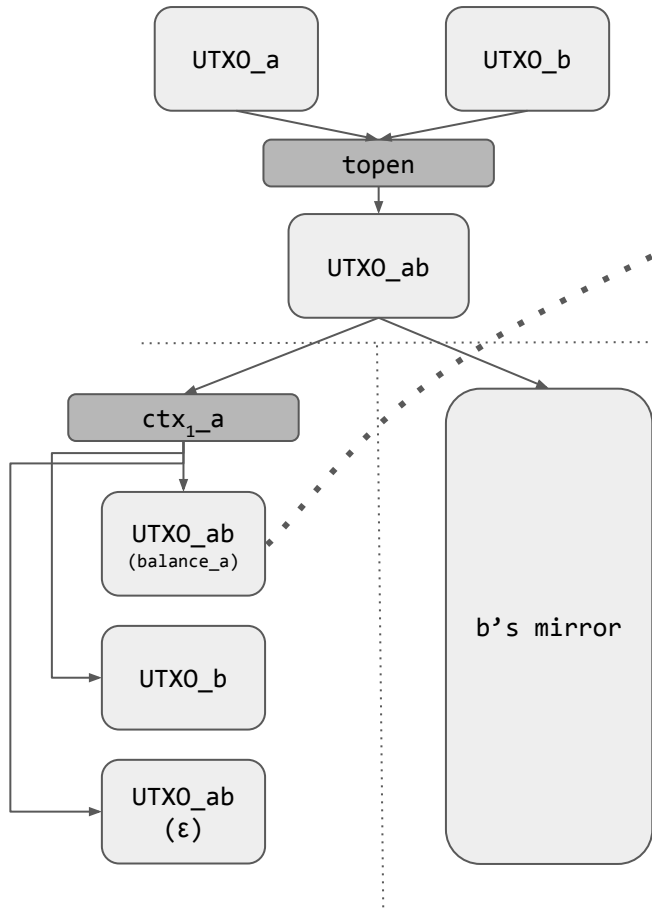
Outpost



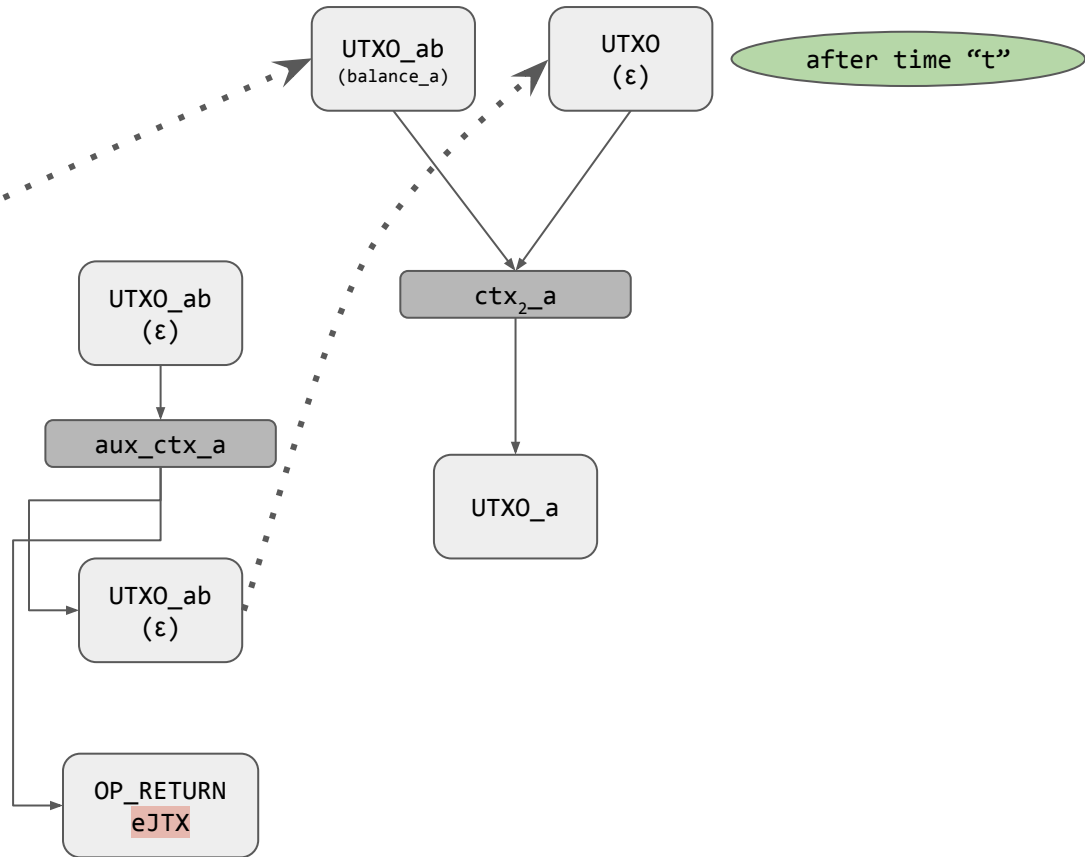
Auxiliary Transaction



Outpost



Commitment Transaction-2



The money slide

Classic Lightning

	Per channel, with N updates	20k channels, 1M updates
Known Channel	$N \cdot \text{size}(\text{ejtx}) + 1 \cdot \text{size}(\text{txid})$	7.00 TB
Unknown Channel	$N \cdot \text{size}(\text{ejtx}) + N \cdot \text{size}(\text{txid})$	7.65 TB

Outpost

Known Channel	$\text{size}(\text{key}) + \text{size}(\text{txid})$	0.96 MB (WTF)
Unknown Channel	$N \cdot \text{size}(\text{key}) + N \cdot \text{size}(\text{txid})$	0.96 TB

Note: $\text{size}(\text{key}) \ll \text{size}(\text{ejtx})$ i.e. 16 \ll 350

Outpost keeps Lightning's key features

- Unilateral closure: broadcaster has to wait
 - Not cheating
 - Cheating

- Exchange revocation keys vs. AES-128 decryption keys

Cheating (Alice wants to profit)

Time ↓	Alice broadcasts older ctx_{1_a} , aux_ctx_a	Bob is watching the blockchain
	Wait	Bob sees aux_ctx_a
	Wait	Bob has key to decrypt eJTX & get JTX_b
	Wait	Bob broadcasts JTX_b
	Wait	JTX_b is confirmed on the blockchain 😎
	Wait	ctx_{2_a} is now invalid
	Alice can broadcast ctx_{2_a} - but...	

Unilateral Closure(Bob has disappeared)

Time ↓	Alice broadcasts latest ctx_{1_a} , aux_ctx_a	Bob is secretly watching the blockchain
	Wait	Bob sees aux_ctx_a
	Wait	Bob cannot decrypt eJTX
	Wait	ctx_{2_a} is still valid
	Alice can broadcast ctx_{2_a} - 😎	

Griefing `^-_(\ツ)_/^-`

Time ↓

Alice broadcasts <code>ctx_{1-a}</code>	Bob is watching the blockchain
Wait	Bob sees <code>ctx_{1-a}</code> confirmed
Wait	Bob's own <code>ctx_{1-b}</code> is now invalid 😡
Wait	Bob's <code>JTX_b</code> is valid, if he has it
Gone...	

Can we have `ctx1-a` send all its balance to Bob? Much later.

Profit

Outpost

- CTX and eJTX on the blockchain
- eJTX's key in the node (16 bytes)

Classic Lightning

- CTX on the blockchain
- JTX in the node (~350 bytes)

Cost

Outpost

- 3 txns
- ϵ

Classic Lightning

- 1 txn
- No ϵ

Limitations

- OP_RETURN limited to 80 bytes.
 - IsStandard \emptyset
 - Split aux_ctx into 2; P2SH Data-hash across them

- Bloat
 - Not on the blockchain (happy case)
 - On the blockchain, 3 txns vs 1 txn

Optimize!!

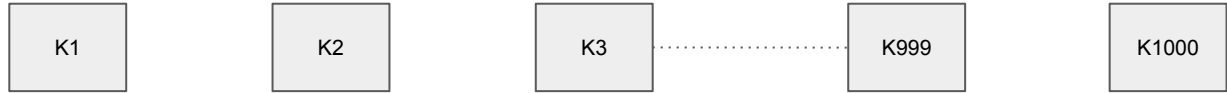
SHACHAIN

(Fast)

Pre-compute



Use*



RSA-CHAIN

(Slow)

Pre-compute

No



Use*

*Key derivation function

Size estimates

Classic Lightning

	Per channel, with N updates	20k channels, 1M updates
Known Channel	$N \cdot \text{size}(\text{ejtx}) + 1 \cdot \text{size}(\text{txid})$	7.00 TB
Unknown Channel	$N \cdot \text{size}(\text{ejtx}) + N \cdot \text{size}(\text{txid})$	7.65 TB

Outpost

Known Channel	$\text{size}(\text{key}) + \text{size}(\text{txid})$	0.96 MB (WTF)
Unknown Channel	$N \cdot \text{size}(\text{key}) + N \cdot \text{size}(\text{txid})$	0.96 TB

Note: $\text{size}(\text{key}) \ll \text{size}(\text{ejtx})$ i.e. 16 \ll 350

What's next?

- HTLC
- Implementation

Thanks

- Store justice transactions inside commitment transactions
- tejaswin@ethz.ch
- mkhabbazian@ualberta.ca
- wattenhofer@ethz.ch