



Cross-Chain Commerce
Trustless Trading of Tokens

including:

- EVM ERC-20 (**DeFi**)
- EVM ERC-721 (**NFT**)
- Stacks Clarity (**CityCoins**)
- Bitcoin (**Bitcoin**)

Step 1: parties agree on the trade



Discover other parties to transact with



Connect over common interests and terms



Agree on the parameters of the trade



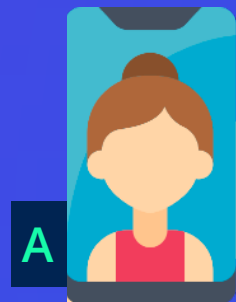
Sign the hash of the payload with trade info:

Blockchain 1: A sends to B amount X1 of token Y1

Blockchain 2: B sends to A amount X2 of token Y2

Blockchain 3: B sends to C amount X3 of token Y3

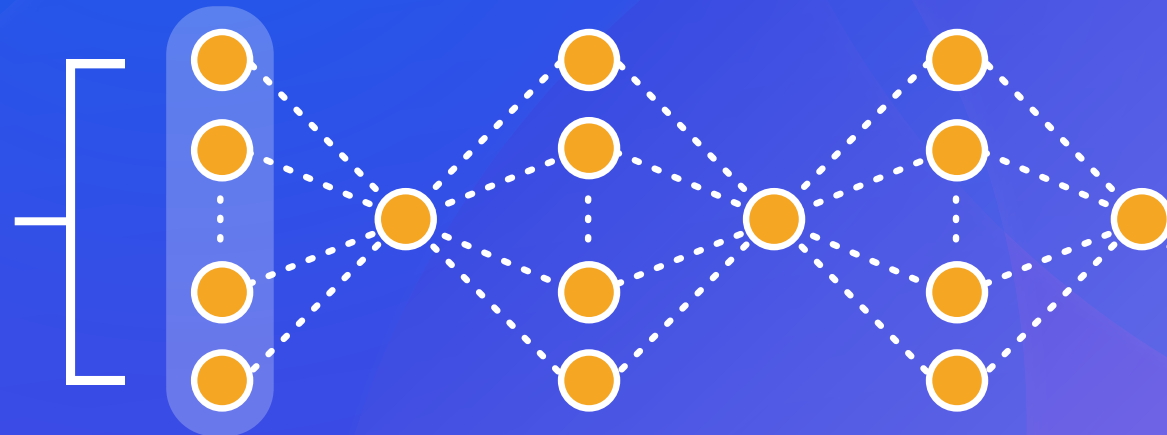
Step 2: parties lock money in escrow on their respective **blockchains**



Time-Locked
3000 USDT in
escrow contract
0xA.... for 1 hour



Time-Locked
2 NFT tokens in
escrow contract
0xB.... for 1 hour



Step 3: parties verify each other's lockups

they only proceed to the next steps if **satisfied**



Time-Locked
3000 USDT in
escrow contract
0xA.... for 1 hour



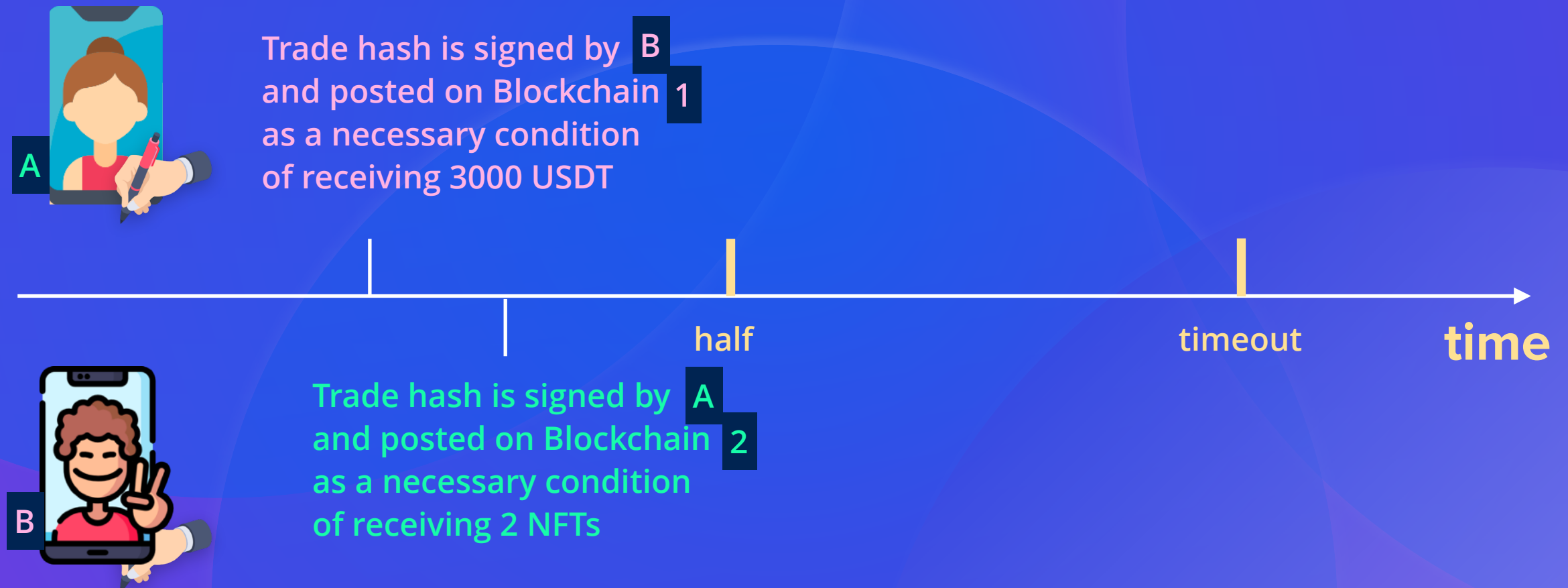
Time-Locked
2 NFT tokens in
escrow contract
0xB.... for 1 hour



in the worst case, one party locked tokens for an hour

Step 4: parties post on each other's chains

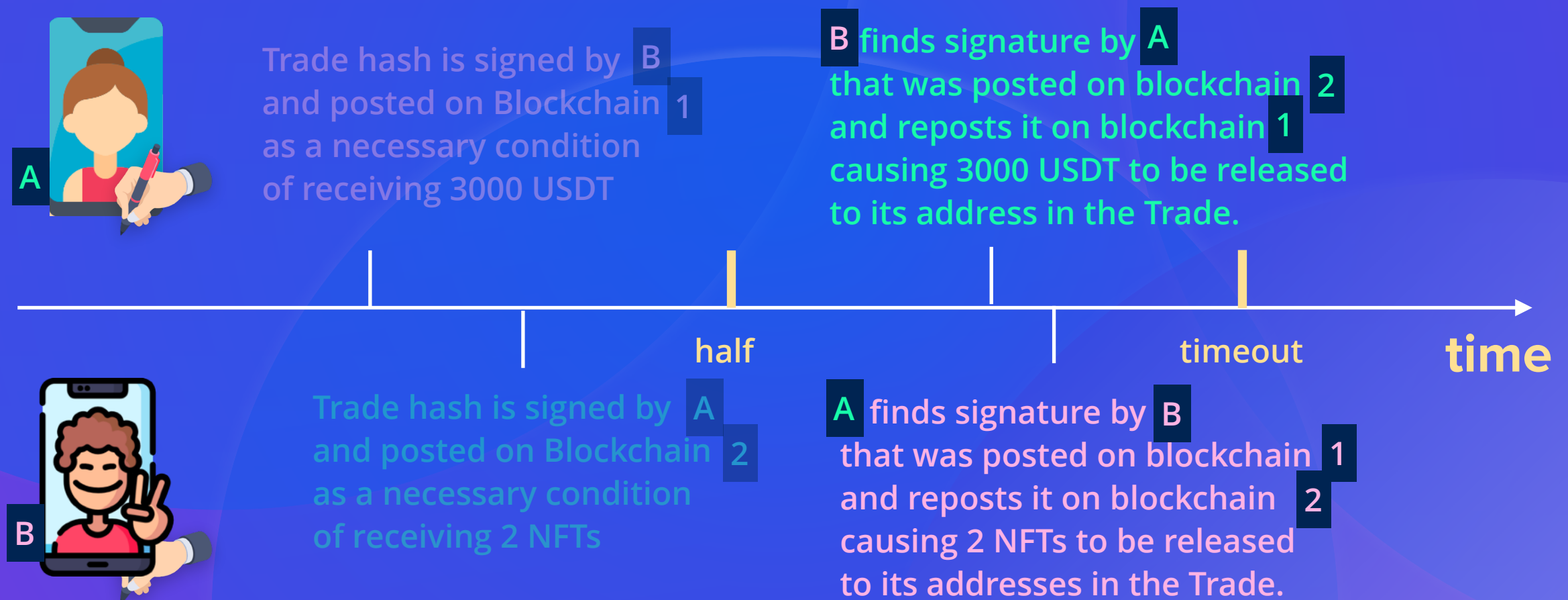
they must do it in the **first half** of the timeout period



it is in their own self-interest to post, or they won't receive tokens and after the timeout expires, the other party can take them back.

Step 5: parties complete the transaction

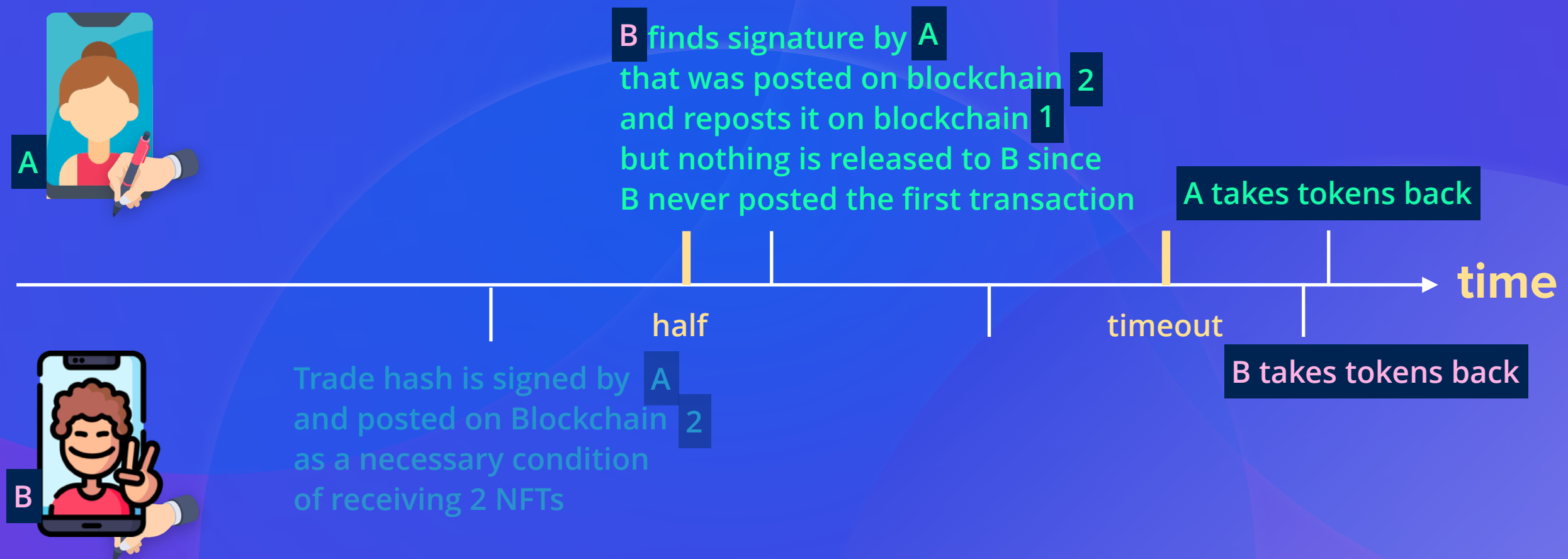
on each blockchain, tokens are released to the other party only if they had posted a signed transaction in the first half



and having done that, the other parties have an entire half of the timeout period to repost it on their own blockchains

Canceling: what if one party doesn't post?

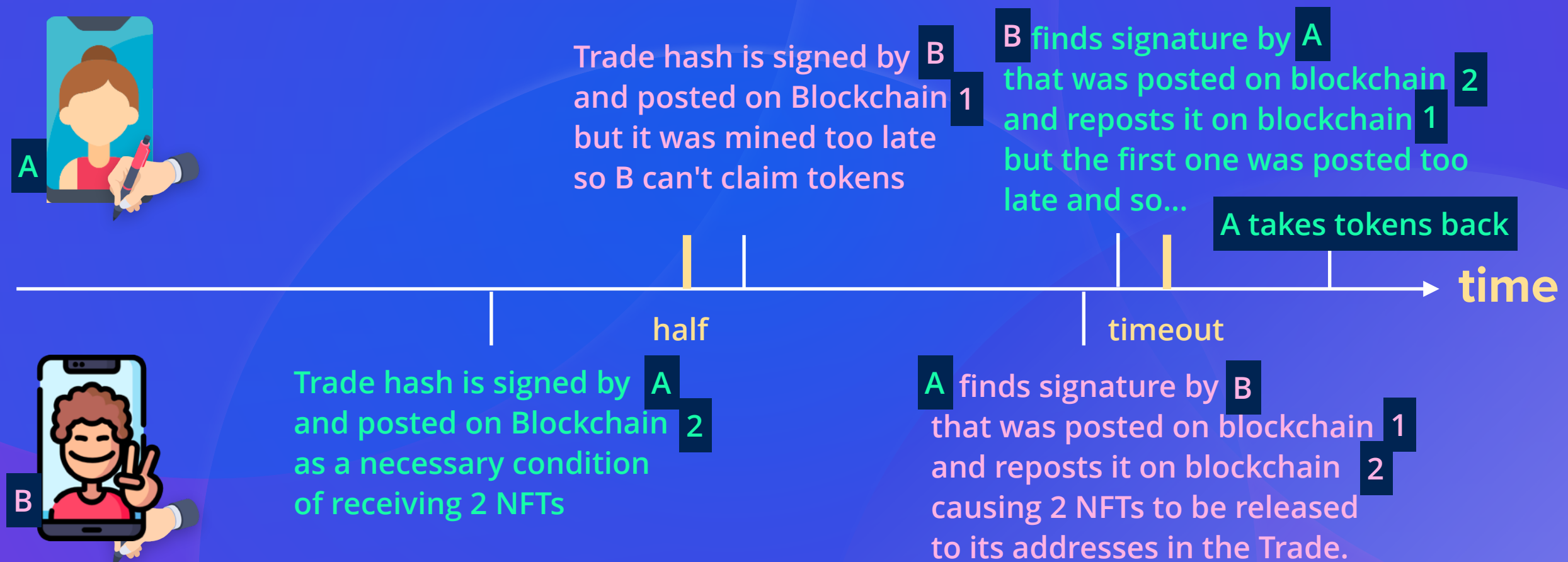
suppose that B's transaction was never mined
in the first half of the timeout period



then the trade would be canceled on both blockchains,
as neither A nor B could complete it before the timeout.

Failure Mode: transactions being mined late

if B's first transaction was delayed and mined after the halfway point then A could repost it on Blockchain 2 (e.g. from mempool) and receive B's tokens, even though B won't get A's tokens.



Same applies to transactions in the second half of the timeout.

Therefore, it's vital that the timeout period is long enough and enough gas is spent by all parties to get transactions mined.

Team



Greg Magarshak
Founder, Architect



Norman Qian
Team Manager



Marsilda Bialczak
Media Director



Stacey Brown
Community Director



Artem Subbotin
Smart Contract Developer



Chris Kim
DApp Developer



Igor Martsekha
Native App Developer



Ivan Alekseev
Visual Designer

Advisors



Elena Rivers
Acumen Capital Partners



Sara Hanks
CEO, CrowdCheck



Dallas Johnston
CEO of Credify



Petar Maymounkov
Inventor of Kademlia



Schedule a call with our team
calendly.com/intercoin/15min