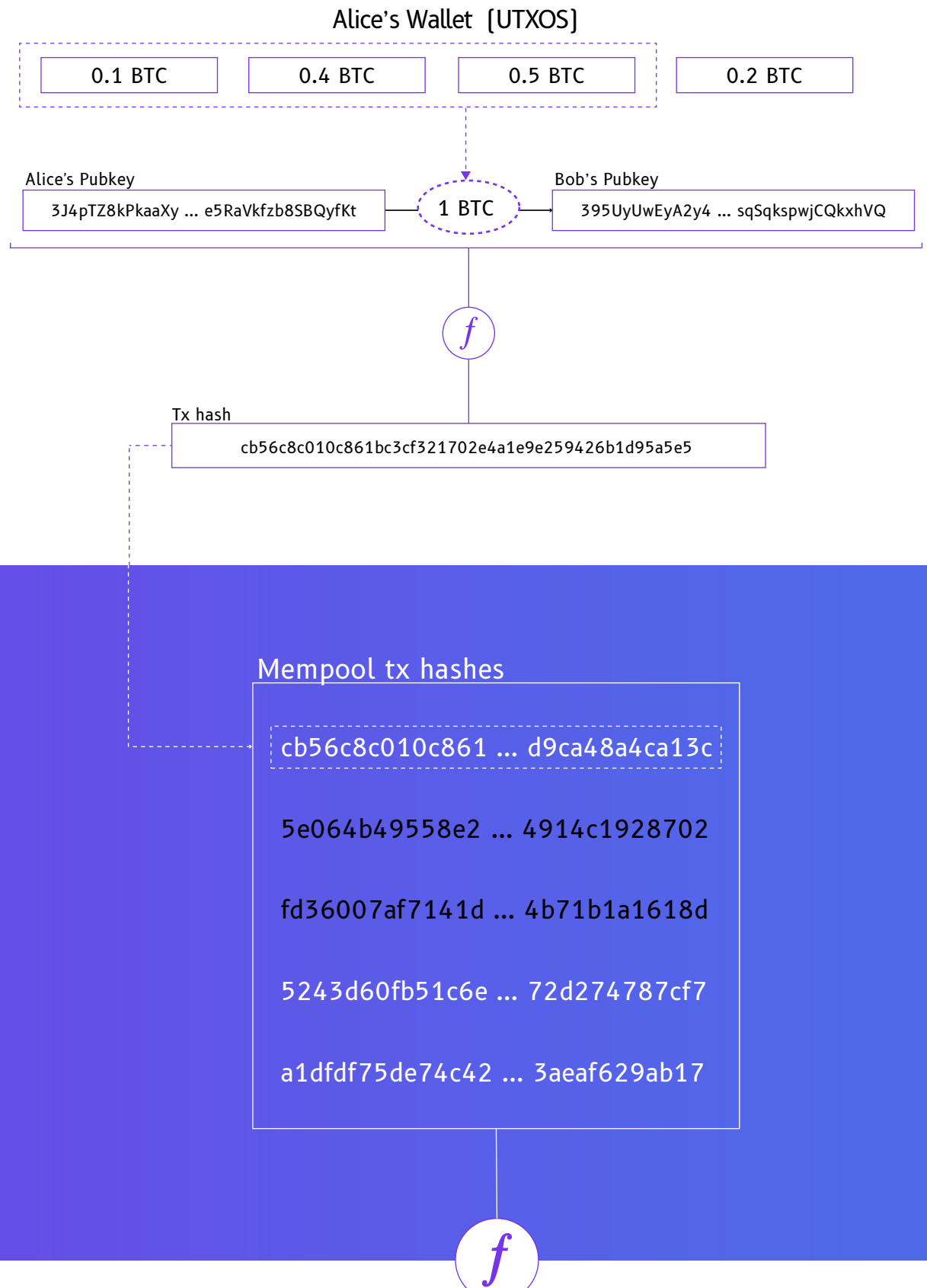
crypto testers

The Journey Of A Bitcoin Transaction

1 Transaction creation and broadcasting

Alice enters Bob's public key on her wallet and enters the amount to send: 1 BTC. Her wallet assembles a UTXO set from her available UTXOs, creates the transaction and broadcasts it to the network.



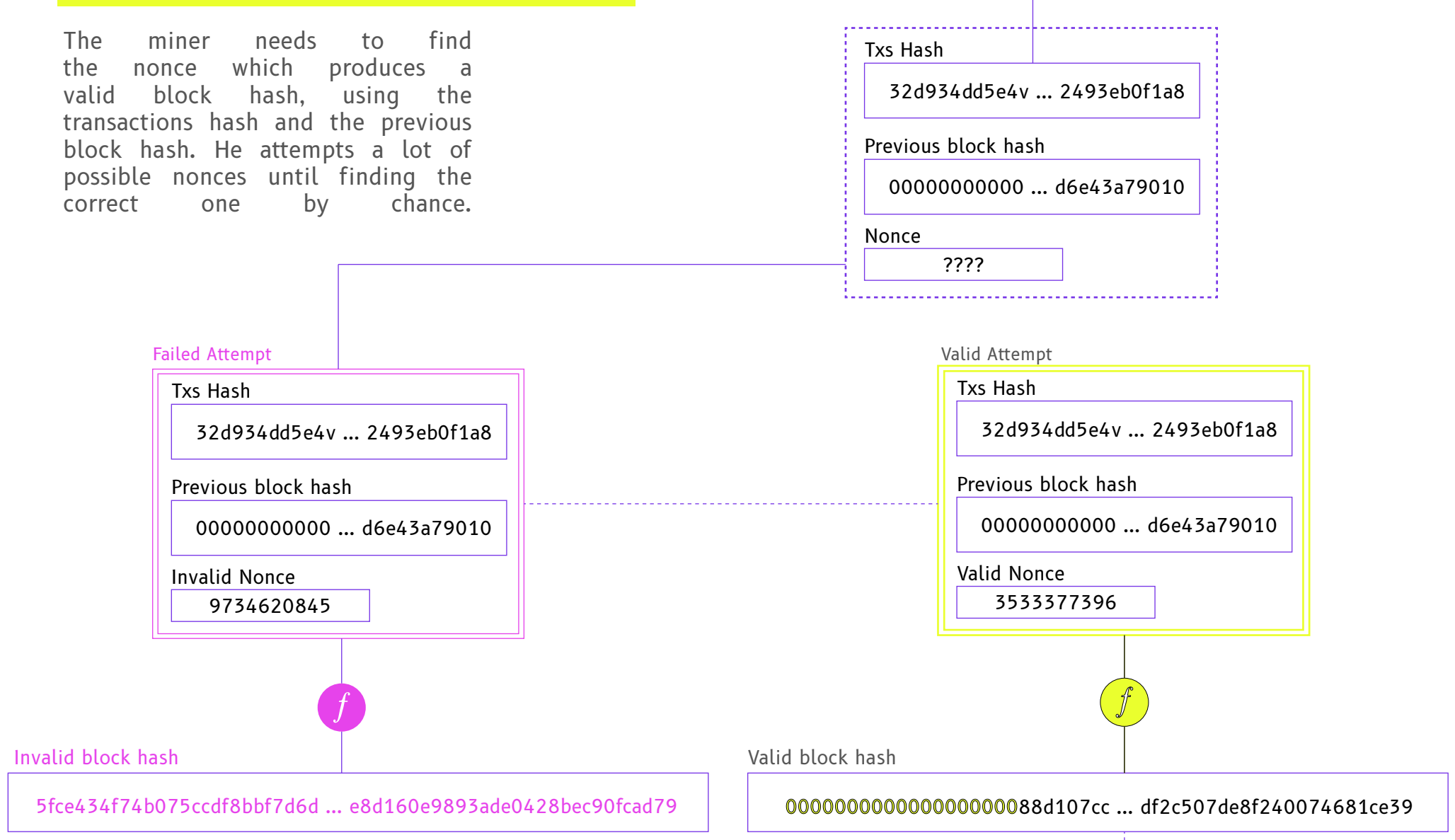
f : hash function

2 Transaction in mempool

Some miner on the network receives the transaction in his memory pool (or mempool). He picks a set of transactions from the mempool which he wants to validate, including

3 Solving the cryptographic puzzle

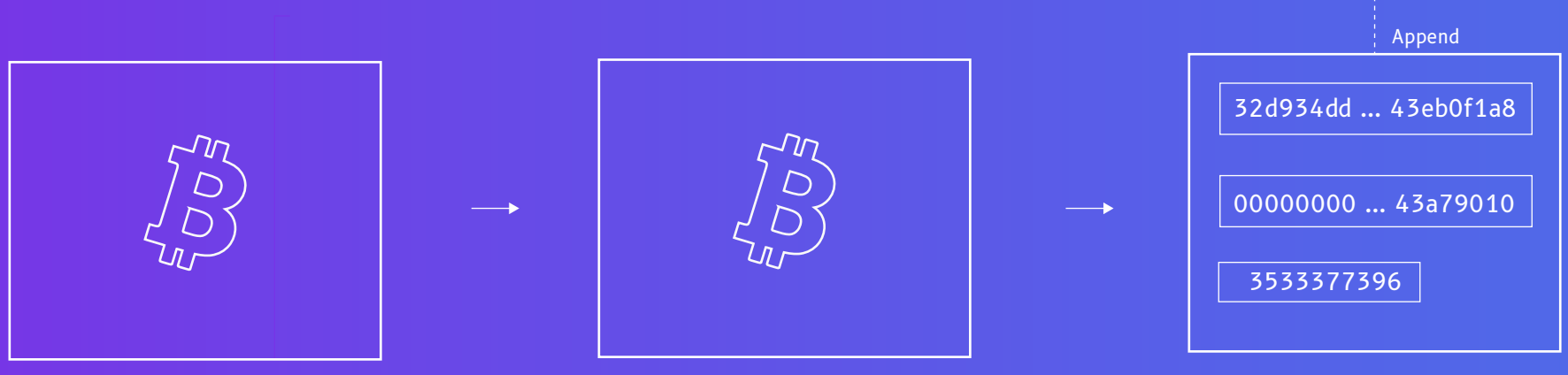
The miner needs to find the nonce which produces a valid block hash, using the transactions hash and the previous block hash. He attempts a lot of possible nonces until finding the correct one by chance.



* there are actually more elements taken into account for the Bitcoin SHA256 mining algorithm

4 Add valid transaction set to the blockchain

When the correct nonce is found, a valid block is created by the miner and broadcasted to the network. The network can verify the block is valid by replicating the solution. Once verified, the block is appended to each bitcoin node's version of the blockchain. Alice's transaction is



DISCLAIMER all hashes and public addresses are fictional and don't show a true valid block hash

https://cryptotesters.com @cryptotesters designed by @Stelios_Rms