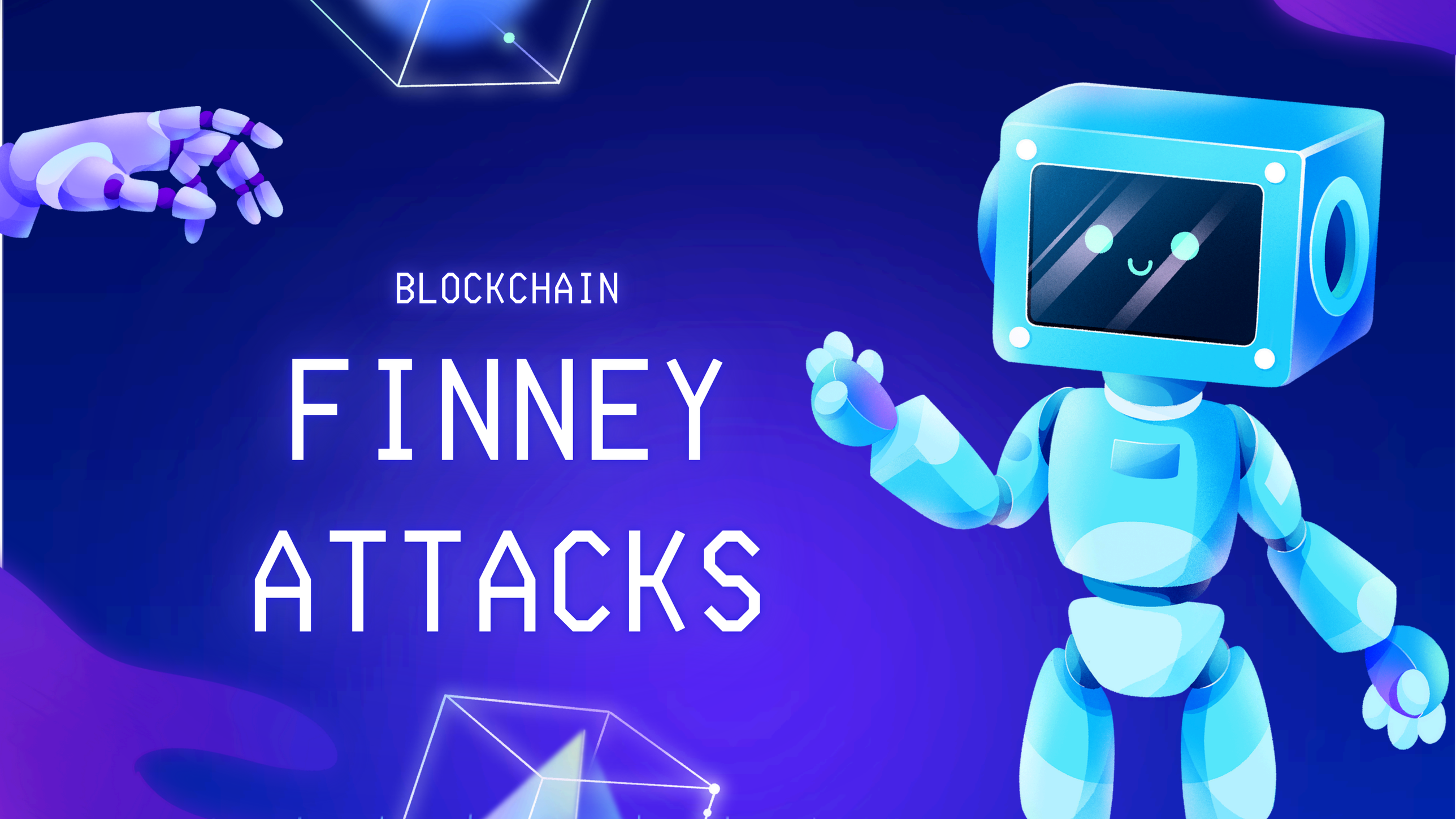
BLOCKCHAIN

FINNEY ATTACKS



INTRODUCTION

A Finney attack is a type of double-spending attack on a blockchain network, first described by Bitcoin pioneer Hal Finney. This attack takes advantage of the fact that unconfirmed transactions (i.e., transactions that have been broadcast but not yet included in a block) can be reversed if a miner, or someone collaborating with a miner, is involved in the attack.

PRECONDITIONS FOR A FINNEY ATTACK

Mining capability

The attacker must control a portion of the mining power of the blockchain. The more mining power they control, the more likely they can successfully mine blocks and carry out the attack.

Merchant accepts unconfirmed transactions

The Finney attack requires that the merchant (the party receiving the payment) accepts unconfirmed transactions. This means that the merchant is willing to provide goods or services before waiting for the transaction to be confirmed in a block.

STEPS OF THE FINNEY ATTACK

01

Pre mining a block

The attacker starts by mining a block privately, without broadcasting it to the rest of the network. In this block, the attacker includes a transaction sending a certain amount of cryptocurrency from one of their wallets to another wallet they control. This transaction is valid and gets included in the privately mined block, but the block itself is not yet broadcast to the network.

02

Initiating a Purchase

The attacker then initiates a purchase or service request from a merchant using the cryptocurrency they intend to double spend. In this transaction, they send the merchant the exact same amount of cryptocurrency, but this transaction is broadcast to the network (not included in their private block). The merchant receives this unconfirmed transaction and, assuming it's valid, delivers the goods or service

03

Broadcasting the private block

After the goods or service are delivered, the attacker broadcasts the block they mined earlier. This block contains a conflicting transaction—one that sends the cryptocurrency to the attacker's other wallet instead of the merchant.

04

Network Conflict Resolution

When the network receives the privately mined block, it will likely be accepted because the block was mined in a valid way, adhering to the rules of the blockchain protocol. Since blockchain networks typically follow the longest chain rule (accepting the longest valid chain as the true chain), the network discards the unconfirmed transaction that the merchant initially received, as it conflicts with the transaction in the attacker's mined block.

KEY FEATURES

PRE-MINING A BLOCK WITH A CONFLICTING TRANSACTION

The attacker privately mines a block that includes a transaction sending cryptocurrency to themselves. This block is not immediately broadcast to the network, allowing the attacker to create a future conflict.

BROADCASTING AN UNCONFIRMED TRANSACTION TO THE MERCHANT

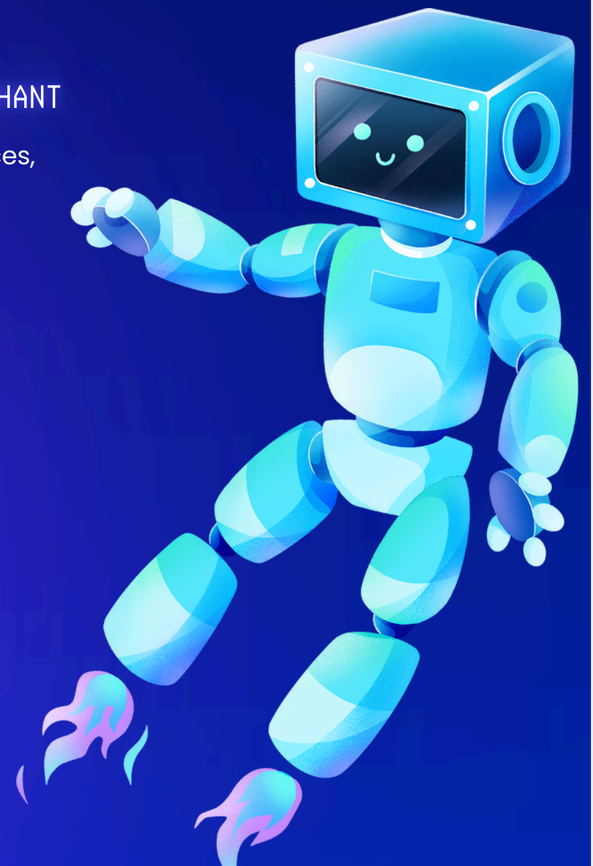
The attacker initiates a transaction to a merchant for goods or services, sending cryptocurrency to the merchant. This transaction is unconfirmed and broadcast to the network.

POST-PURCHASE BROADCAST OF THE PRIVATE BLOCK

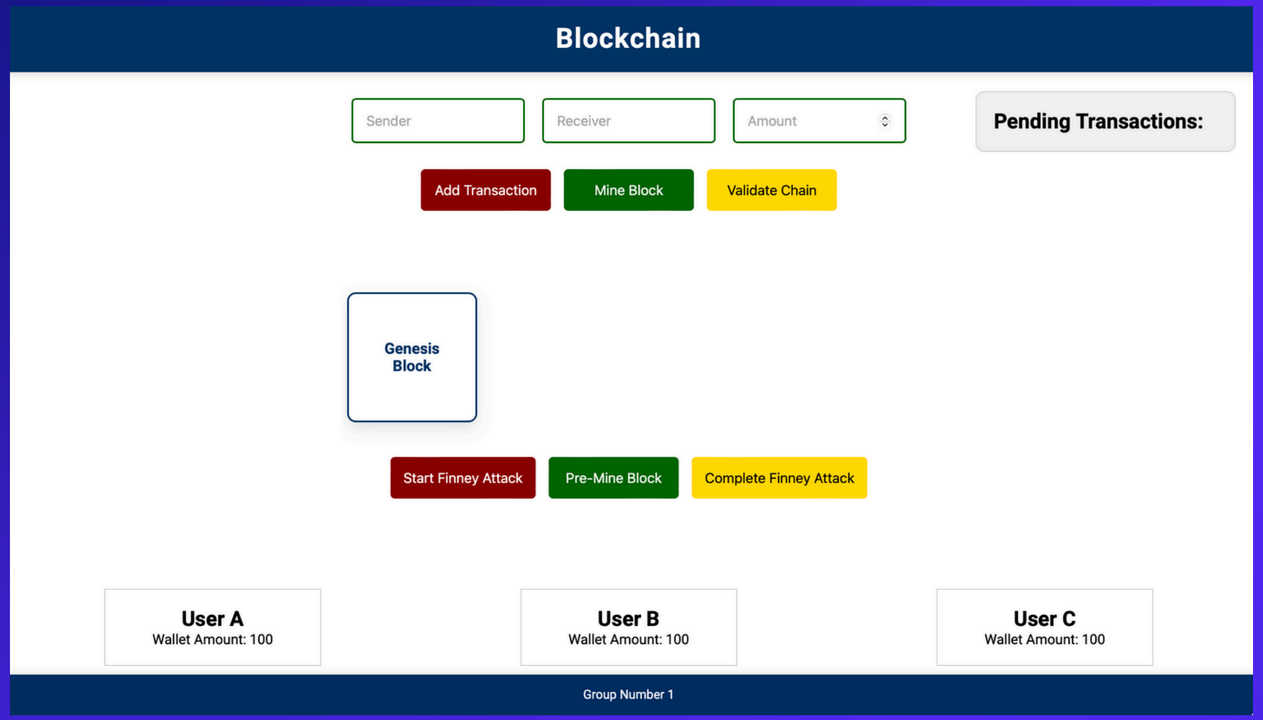
Once the attacker receives the goods or services, they broadcast the privately mined block, which includes a conflicting transaction. The blockchain will recognize this new block and discard the earlier unconfirmed transaction.

EXPLOITING THE LONGEST CHAIN RULE

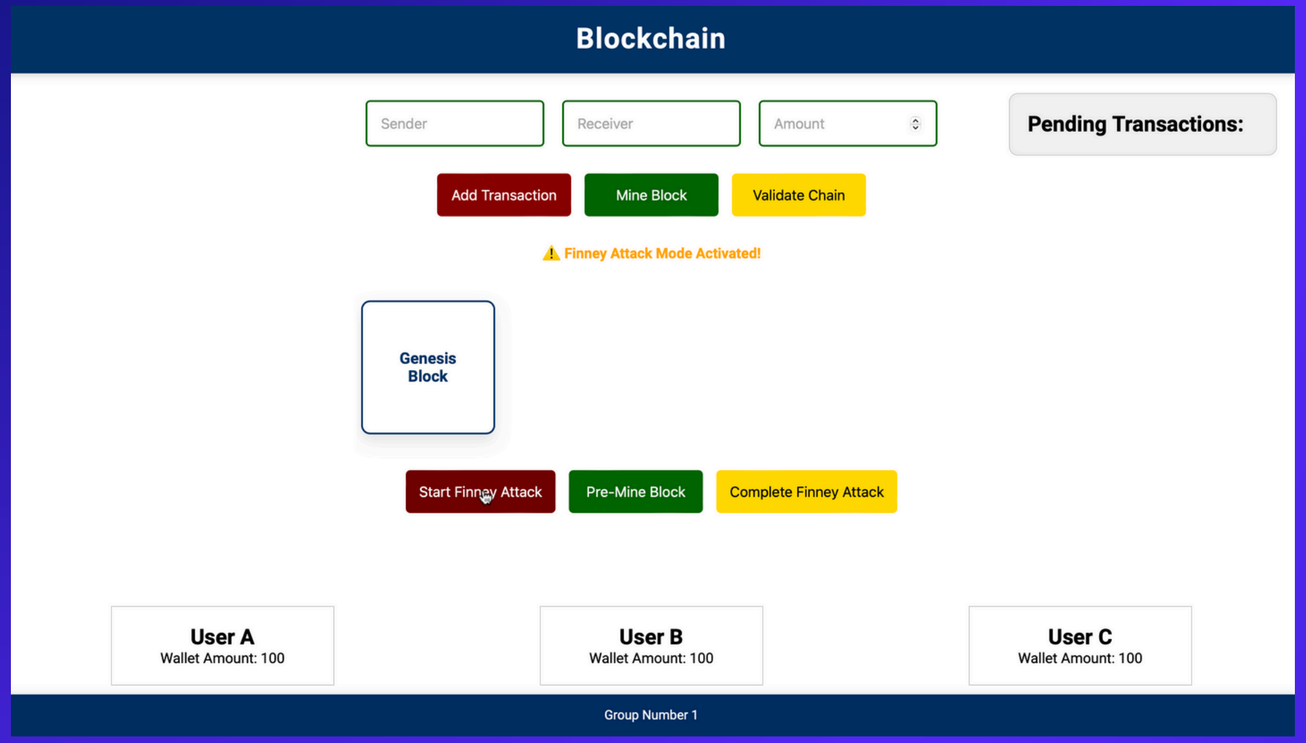
Since the blockchain follows the longest chain rule, the network accepts the attacker's private block, invalidating the unconfirmed transaction to the merchant. The attacker keeps both the cryptocurrency and the goods or services.



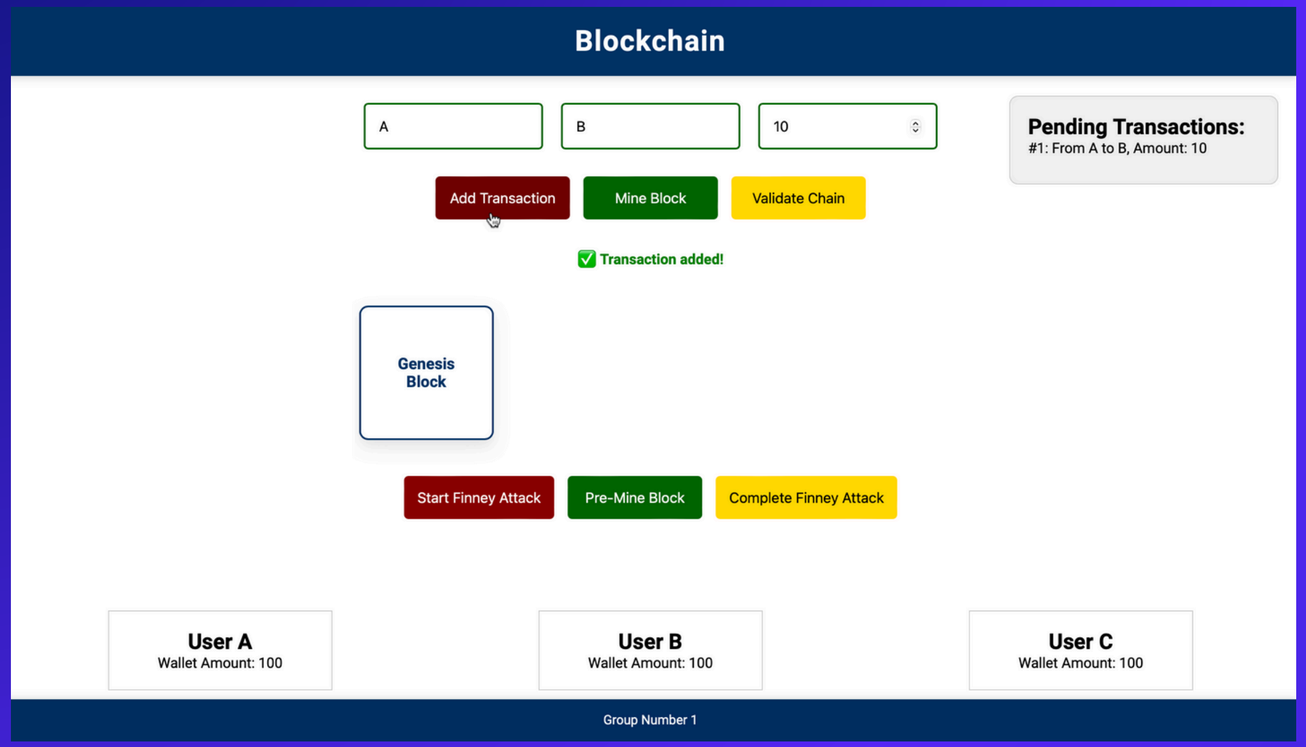
WORKING



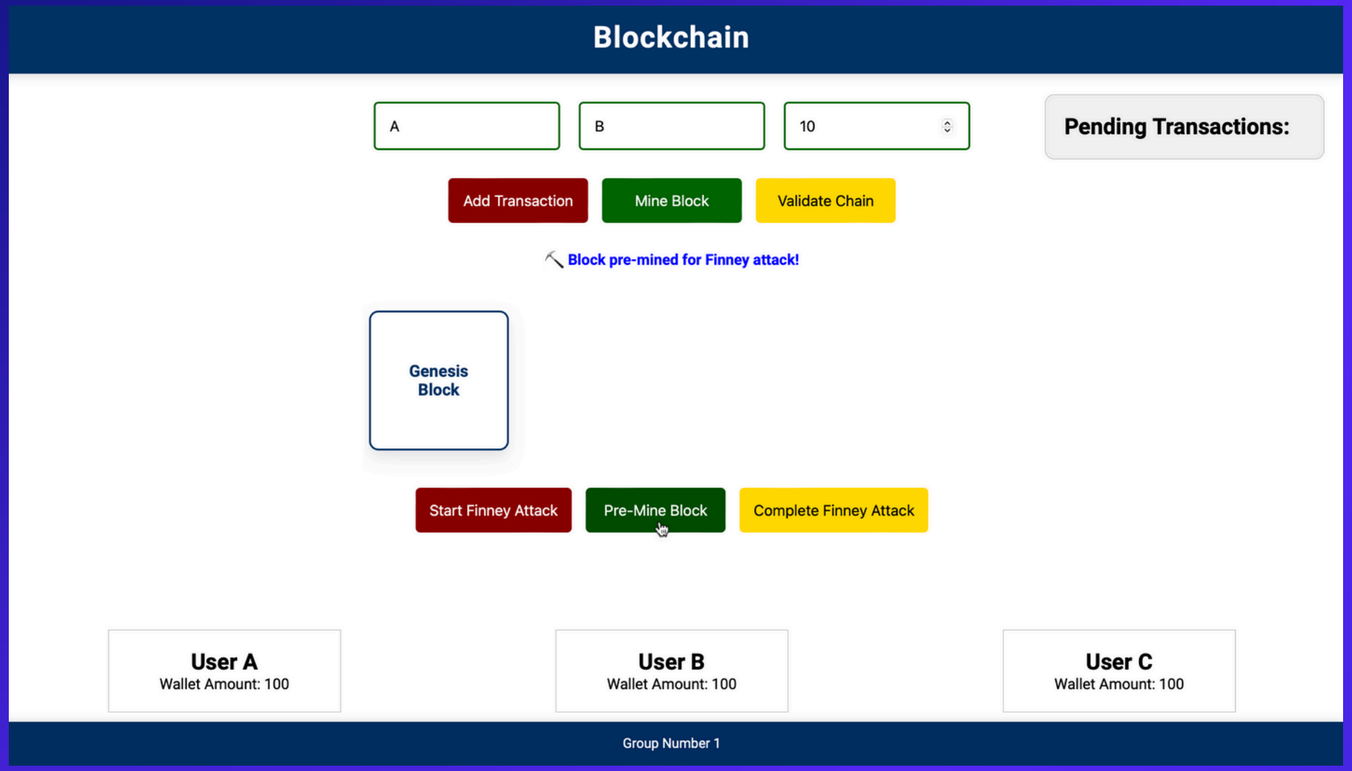
This is the general UI. User A and User B are the members initiating the attack. User C is the vendor.



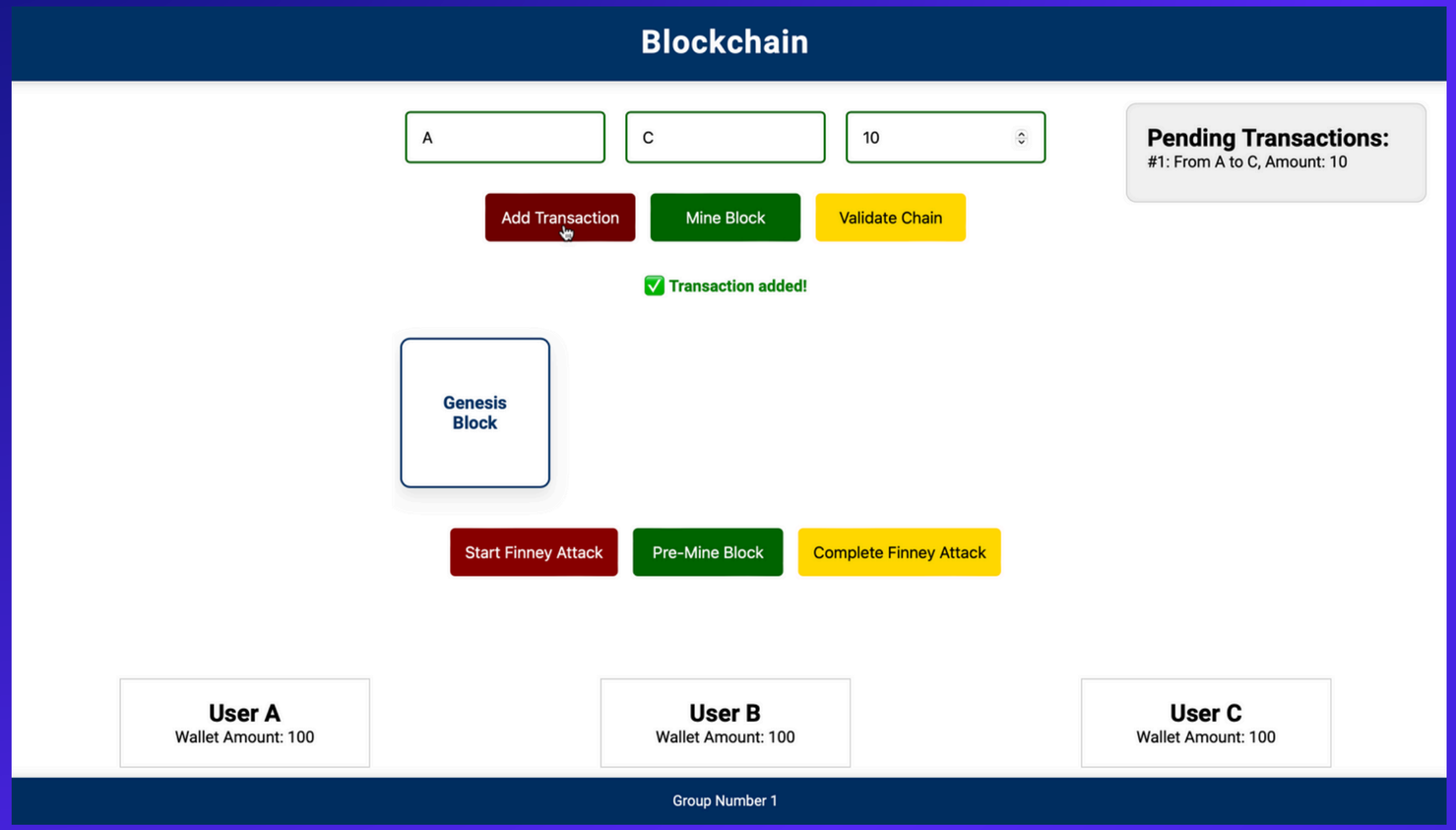
We activate the Finney mode to initiate the Finney attack.



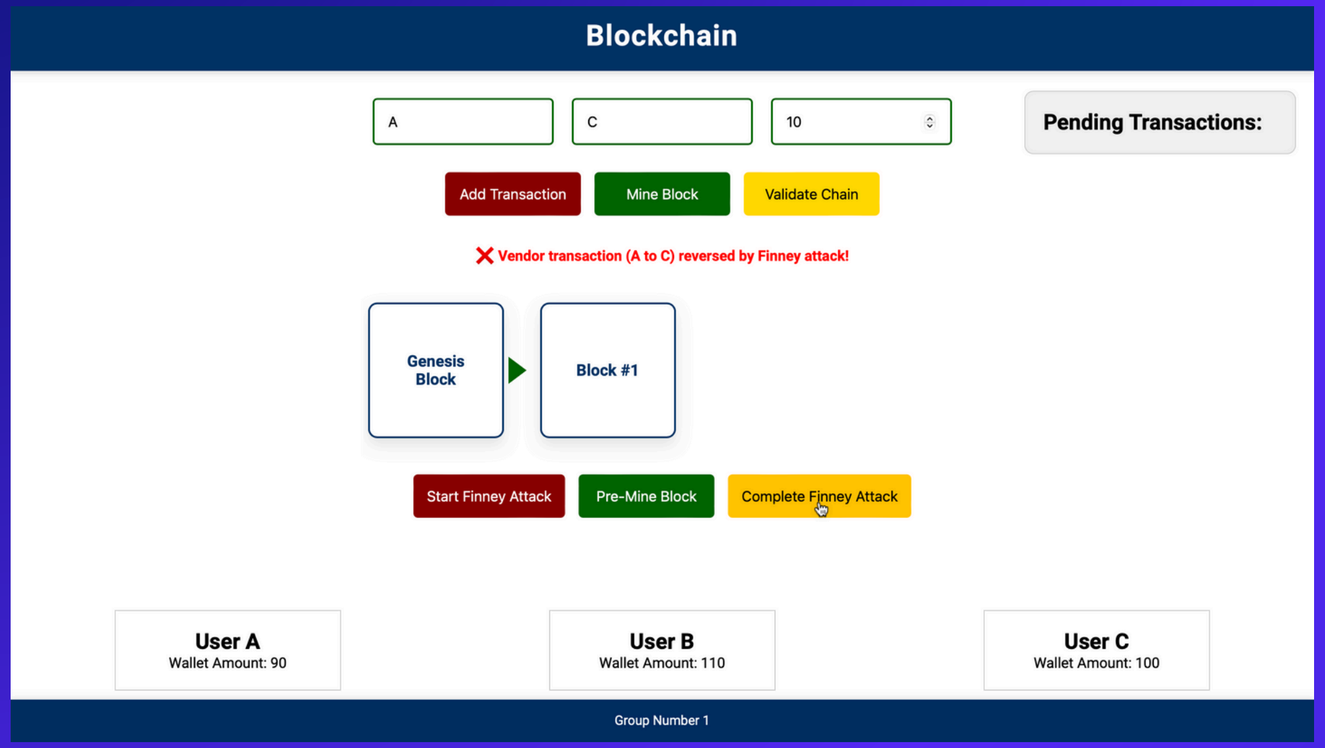
Transaction from user A to user B takes place and is added to the mempool.



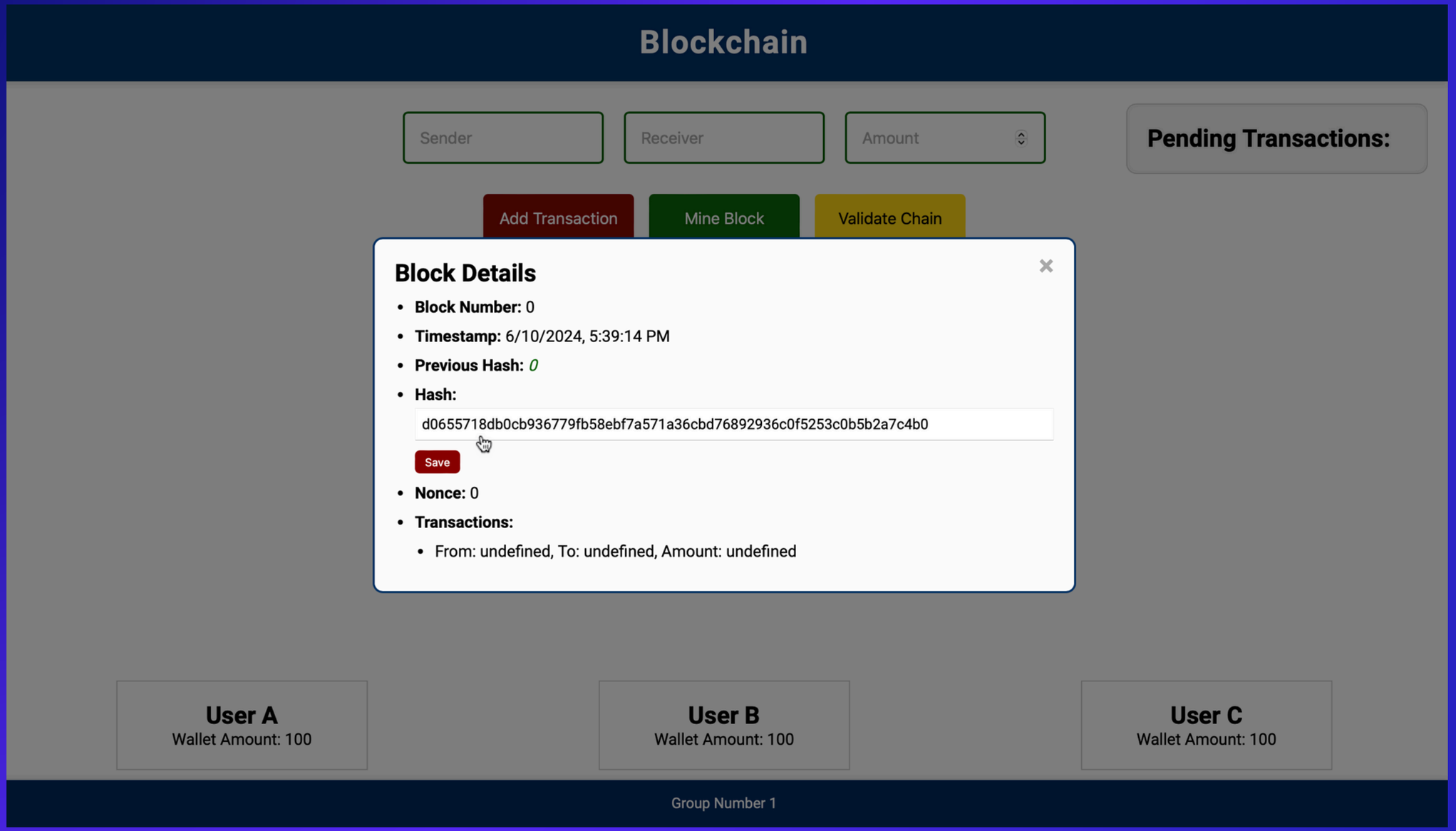
A block containing the transaction of A to B is pre-mined for the Finney attack, but it isn't broadcasted to the blockchain.



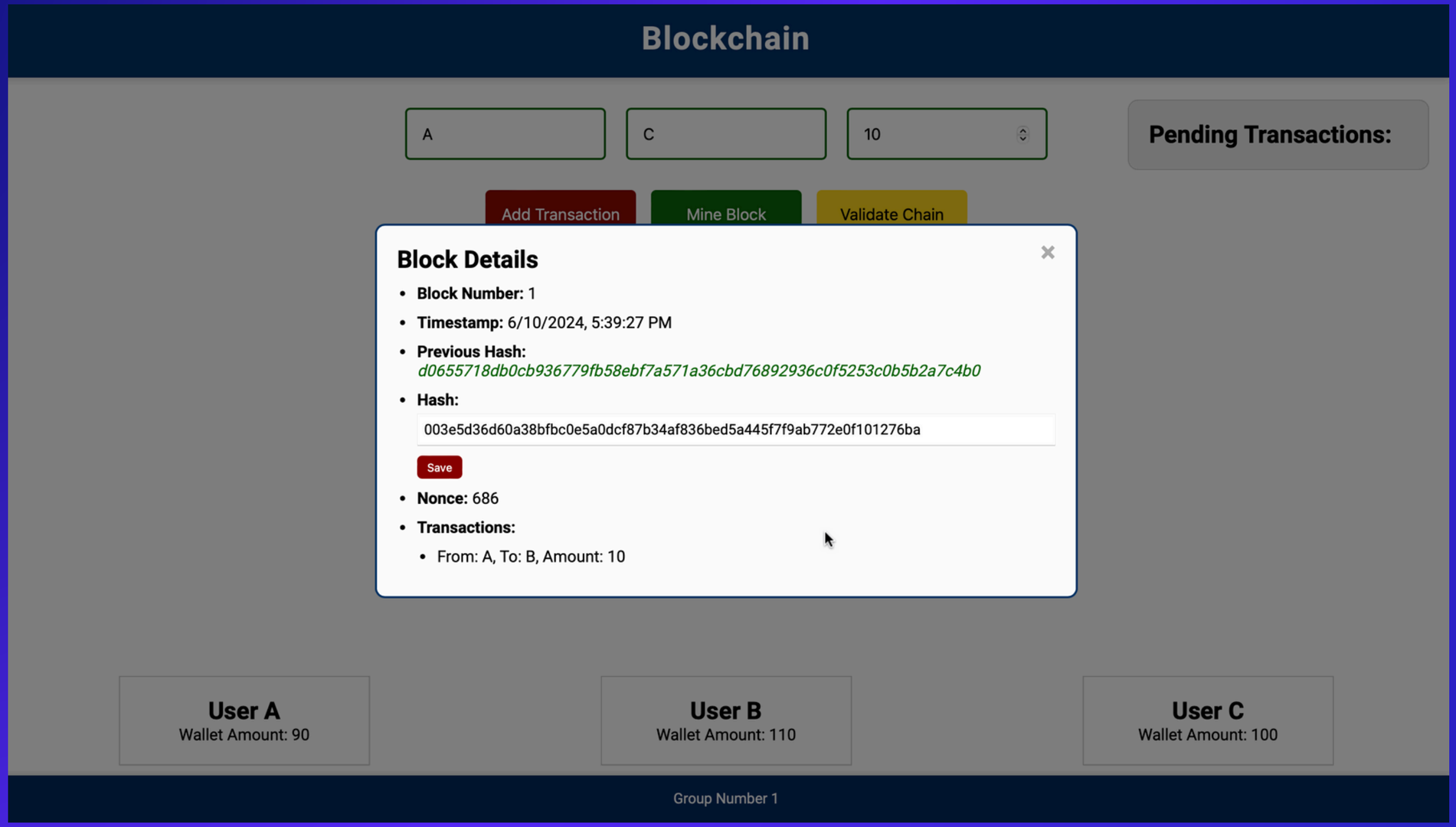
Transaction from user A, the initiator of attack and user C, the vendor, takes place and is added to the mempool



We complete the Finney attack by broadcasting the pre-mined block which contains the transaction of A to B. The pre-mined block gets added to the chain finalizing the transaction of A to B. And since the pre-mined block spends A's balance in transaction to B, the A to C transaction in the mempool becomes invalid.



These are the hash details of the genesis block. Since it's the first block, the previous hash is 0.



These are the hash details of the block containing the transaction from A to B.