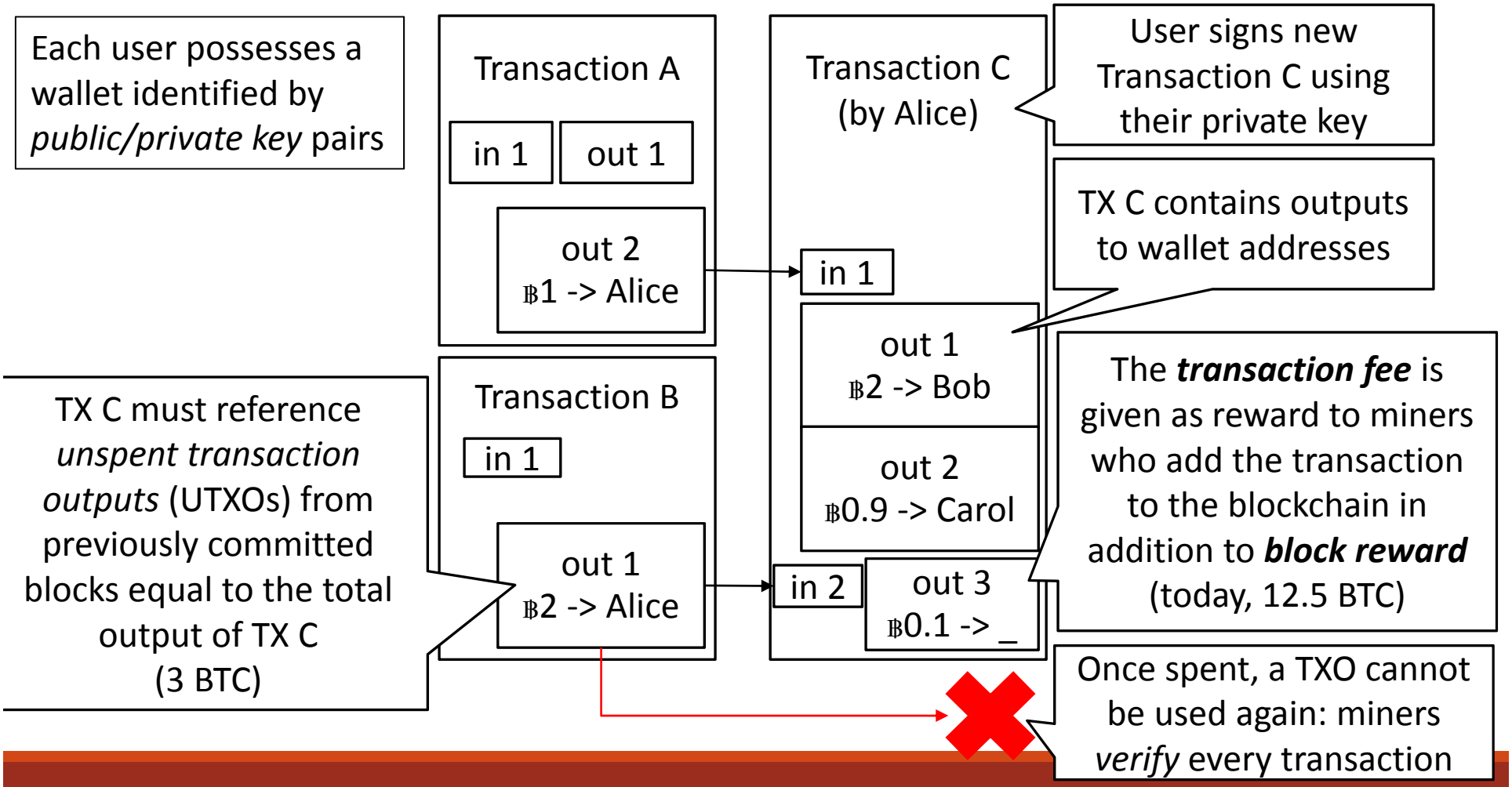
MIDDLEWARE SYSTEMS
RESEARCH GROUP
MSRG.ORG

Deconstructing Blockchains: Concepts, Systems and Applications

TRANSACTIONS AND TRANSACTION FLOW

Bitcoin Transactions



Wallets and Addresses

Users require a **wallet** to store money

- Includes any user, including but not limited to miners

Wallet is authenticated and identified by a **public/private key pair**

- Generated using ECDSA (Elliptic curve cryptography)

Loosing Your Private Key

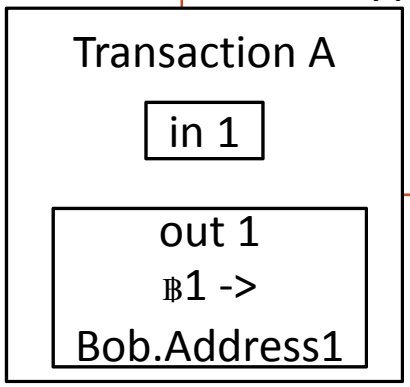
- Loss of private key means the wallet and its **funds are permanently locked**, as it is no longer possible to sign proofs redeeming existing UTXOs.
- This **money is** essentially **lost**, thereby reducing the total amount of currency in Bitcoin
- Trusting an online service to store key is also risky, since there is no way to prove that you are the rightful owner if the key is stolen or misused
- **The most reliable solution is to store your private keys on tamper-proof hardware wallets**

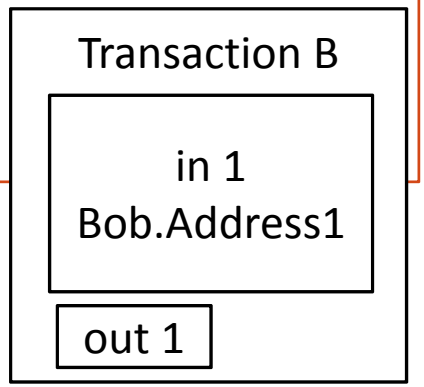
Transaction Flow

Alice
(Sender)

Bob
(Receiver)

1. Bob generates and sends a public key address.
2. Alice creates a transaction using this address.
3. Alice sends the new transaction to the network.
4. Transaction is broadcasted using gossiping.
5. Transaction is included in a mined block.
6. Bob can verify the transaction is in the blockchain.
7. Bob can now sign new transactions which redeems this address.





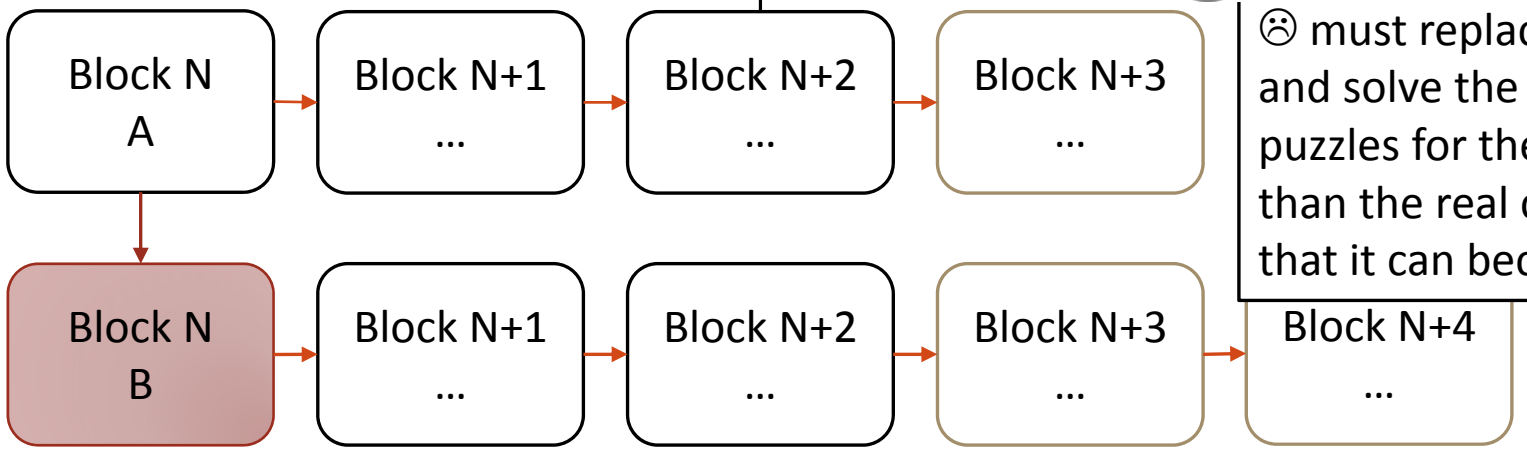
Preventing Double Spending: 51% Attack

- The "Magic Watch" is the ***continuous generation*** of blocks in the main chain which *limits the amount of time* an attacker has to create its own chain.
- If the attacker owns *>51% of the power* in the network, the "Magic Watch" gives *enough time* to the attacker to *tamper with the data (i.e., re-write history)*!

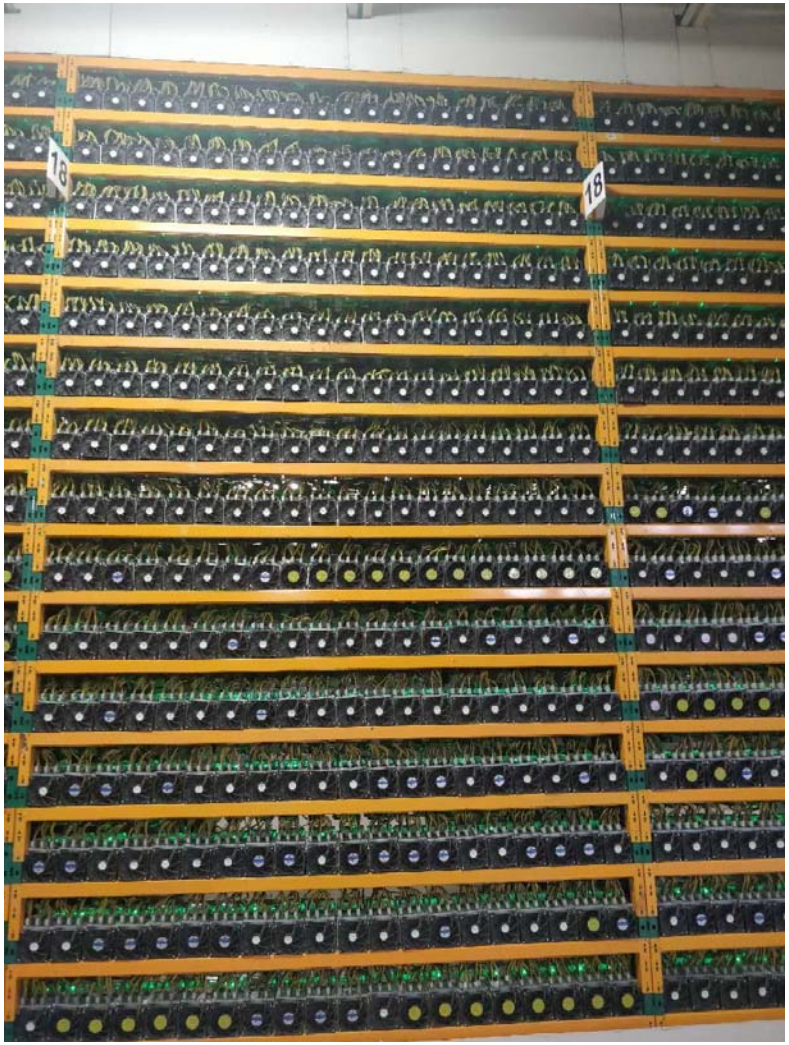
creates two transactions
double-spending)

ded to Block N, and
irms the transaction
few blocks

☹ must replace A with B in N, and solve the modified puzzles for the blocks faster than the real chain grows so that it can become longer



Attacker chain



Mining ASICs,
200 PETA Hashes
per second

Limitations of Bitcoin

Limited expressiveness

- Cryptocurrency only
- Each app requires new platform (e.g. NameCoin, PrimeCoin, CureCoin)

Slow block time (10 mins)

- Also slow confirmation time (1+ hour for 6 confirmations)

Hard/Soft forks

- Updates to the code cause forks
- Hard forks are not compatible
- Duplicated money
- 5 Bitcoin forks (e.g., Bitcoin Classic)

Slow transaction rate

- 7 transactions/second
- VISA Network: 2000 tps (average)
- Limited block size (1MB -> 2MB)

Environmental impact of PoW

- ~1000x more energy than credit card
- Ahead of 159 countries for energy consumption (e.g. Ireland)

Long bootstrap time for a miner

- Full ledger: 270 GB (2020/04)
- CPU/I/O cost to verify each transaction/block
- Takes hours/days