# mas.s62
# lecture 11
## fees

2018-03-14

Tadge Dryja

# today

pset3 description

fees

CPFP / RBF

long term incentives

# pset03

grab utxos

install bitcoind, sync to testnet3

build transactions in code, submit to network

Block explorers aren't cheating. But they're also not as fun.

# pset03

try to get familiar with bitcoin-cli

use any scripting you like (bash, python, go, node -- or anything that can talk to bitcoind's rpc)

I will add more utxos to grab in the next few days

# transaction fees

difference between sum of input amounts and sum of output amounts

implicit; not encoded in the transaction

paid to whoever mines the block containing that tx

# transaction fees

fee rate expressed in "satoshis per byte", one satoshi being 0.00000001

prioritize based on tx size as space is limited

unrelated to amount transferred; fee is "flat"

# fee market

fee rate set by transaction signer

txs chosen by miners

auction process

bid for space in future blocks

# miner side

sort mempool txs by fee rate

choose the top ~1MB

compute merkle root, mine

but not that simple... why?

# miner side - CPFP

tx dependencies make this into a much harder optimization problem

txs can depend on others

a "cheap" tx which allows a "expensive" tx to also be confirmed is called "child pays for parent"

# transactor side

want to minimize fees

set to 1 sat / byte, sign and send

... easy right?

# transactor side

want to minimize fees

set to 1 sat / byte, sign and send

... easy right?

it doesn't confirm!

# transactor side

poor user experience

wallets with fixed fee per tx

fixed fee rates

user chooses fee rates (I dunno!)

low fee, outbid by other users

# transactor side

many wallets are "stuck" once tx is sent, can't increase fee

child pays for parent - send a tx to yourself with high fee

# CPFP downsides

inefficient - extra tx

exacerbates problem it's trying to solve! wastes space dealing with lack of space

dependency graphs are complex

# replace by fee

double spend the tx with higher fee (lower change output)

simple, right?

# replace by fee

double spend the tx with higher fee (lower change output)

simple, right?

default relay behavior is ignore double spends

(defined as any conflicting tx)

# replace by fee

relay conflicting txs

require increase in fee; do not relay txs with same or lower fee

(why?)

# replace by fee

relay conflicting txs

require increase in fee; do not relay txs with same or lower fee

DoS attack: make lots of conflicting txs with same fee, flood network

# RBF controversy

hurts security of unconfirmed txs

could contact miners directly, but some effort to double spend if all nodes go with first-seen tx

RBF make double spends much easier (that's the point)

# RBF controversy

0-conf txs have no security anyway; that's the point of the blockchain

UI issue: show unconfirmed tx?

show unconfirmed tx in SPV?

connect to multiple nodes?

# RBF compromise

"opt in" RBF.  Flag in the tx (input sequence number) to indicate RBF

IMHO: ugly code.  Can't even tell what RBF policy nodes have

# RBF compromise

"opt in" RBF.  Flag in the tx (input sequence number) to indicate RBF

IMHO: ugly code.  Can't even tell what RBF policy nodes have

# inter mission

0x7f sec

# fees in practice

highly variable!

very hard to predict!

further research needed

my favorite: locktime & RBF ramp

# fees in practice

exchanges overpay

bitcoind wallet overpays

nobody cared for 7 years

gas price goes up, hummer -> prius

# long term incentive

mining reward drops in half every 210000 blocks

eventually all coins mined (100 y)

rewards become negligible sooner than you might think!

# long term incentive

no new coins to mine...

why mine?

tx fees

# long term incentive

problem with tx fee only incentive:

tx fees are variable

without a backlog, fees are near 0

0 fees = no incentive to mine

miners stop

# miner "attacks"

you're a miner

no fees in mempool, no reward

turn off your chips, turn back on once the mempool fills up

# miner "attacks"

you're a miner

no fees in mempool, no reward

turn off your chips, turn back on once the mempool fills up

or...?

# miner "attacks"

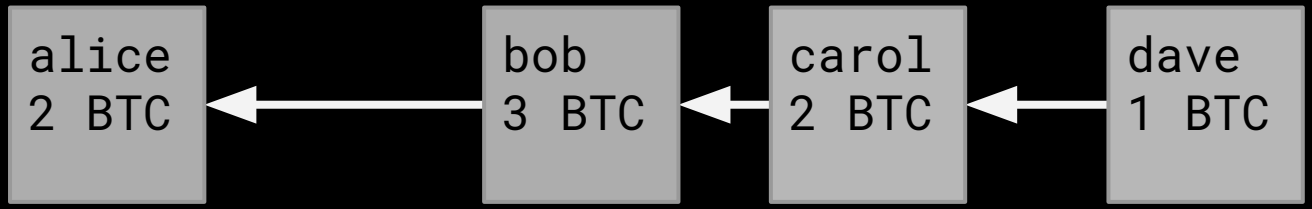
that last block had a couple coins in fees

re-mine it yourself!

if you find another (maybe empty) block on top, you take the fees!

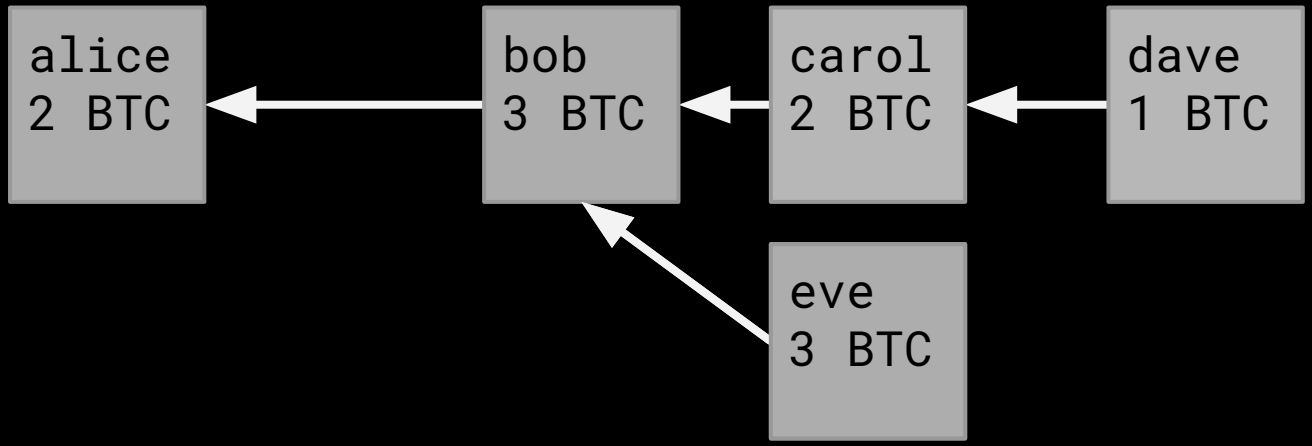
# miner "attacks"

instead of sequentially building the chain, miners keep fighting over the same block height



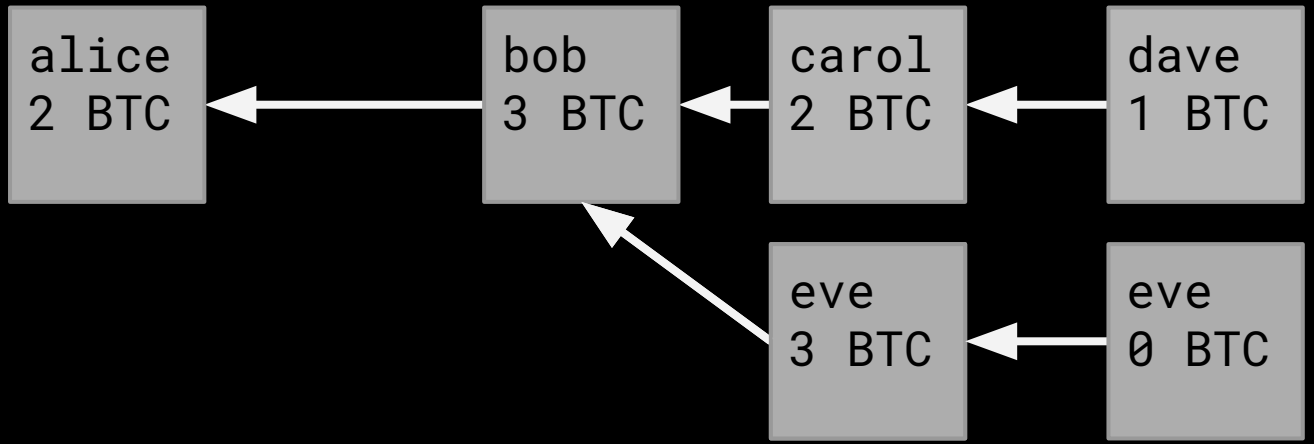
# miner "attacks"

instead of sequentially building the chain, miners keep fighting over the same block height



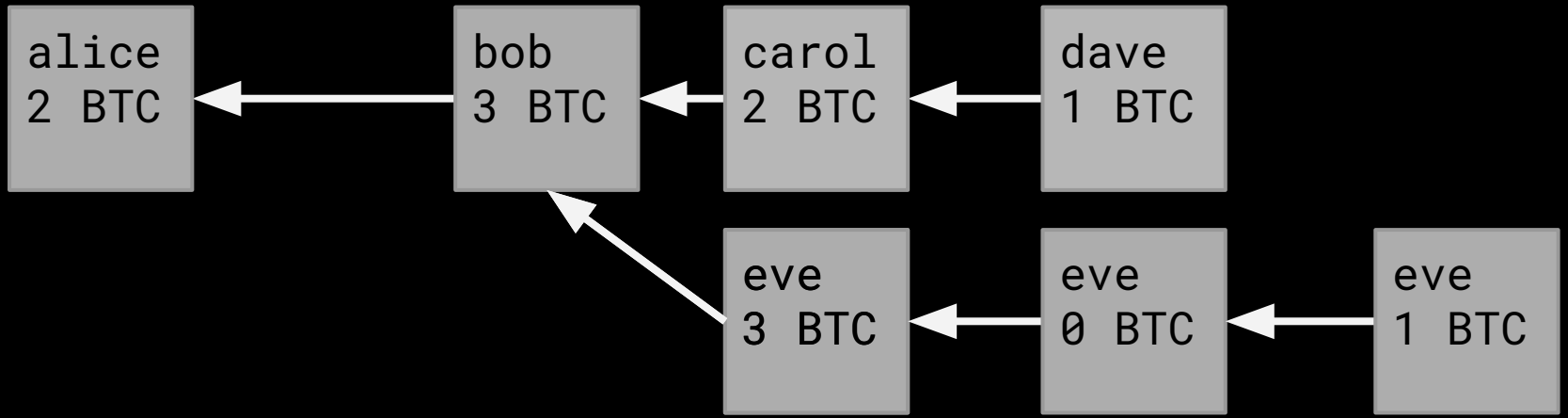
# miner "attacks"

instead of sequentially building the chain, miners keep fighting over the same block height



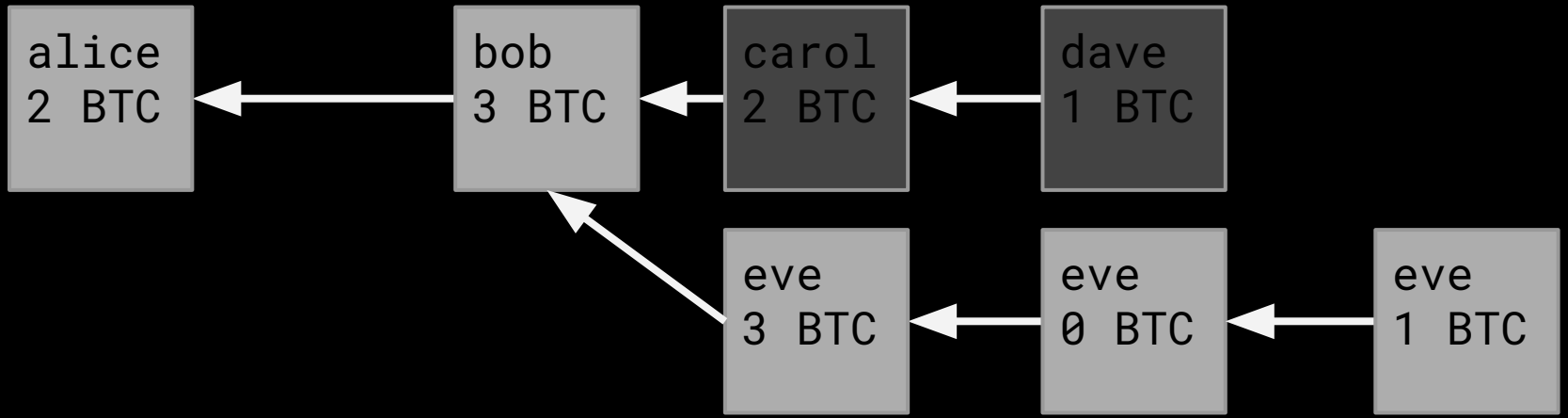
# miner "attacks"

instead of sequentially building the chain, miners keep fighting over the same block height



# miner "attacks"

instead of sequentially building the chain, miners keep fighting over the same block height



# miner "attacks"

is this even an attack?

they're just trying to get paid

not a problem if low reward variance

which means... backlog

# scalability balance

tx rate in Bitcoin, other systems

tradeoff:

too small -> few can have utxos, own their private keys

too large -> few can validate utxo set, verify rules

# scalability balance

fee sniping / reorg is not harware related. Happens with arbitrarily powerful computers / networks

too large -> constant reorg races

largest miner wins (no longer memoryless)

# dawn of the fee

we're just starting to understand fee markets

seems highly inelastic

people wasting millions of dollars

fun research area!

hope this works!

MIT OpenCourseWare
https://ocw.mit.edu/

# MAS.S62 Cryptocurrency Engineering and Design

Spring 2018

For information about citing these materials or our Terms of Use, visit: https://ocw.mit.edu/terms.