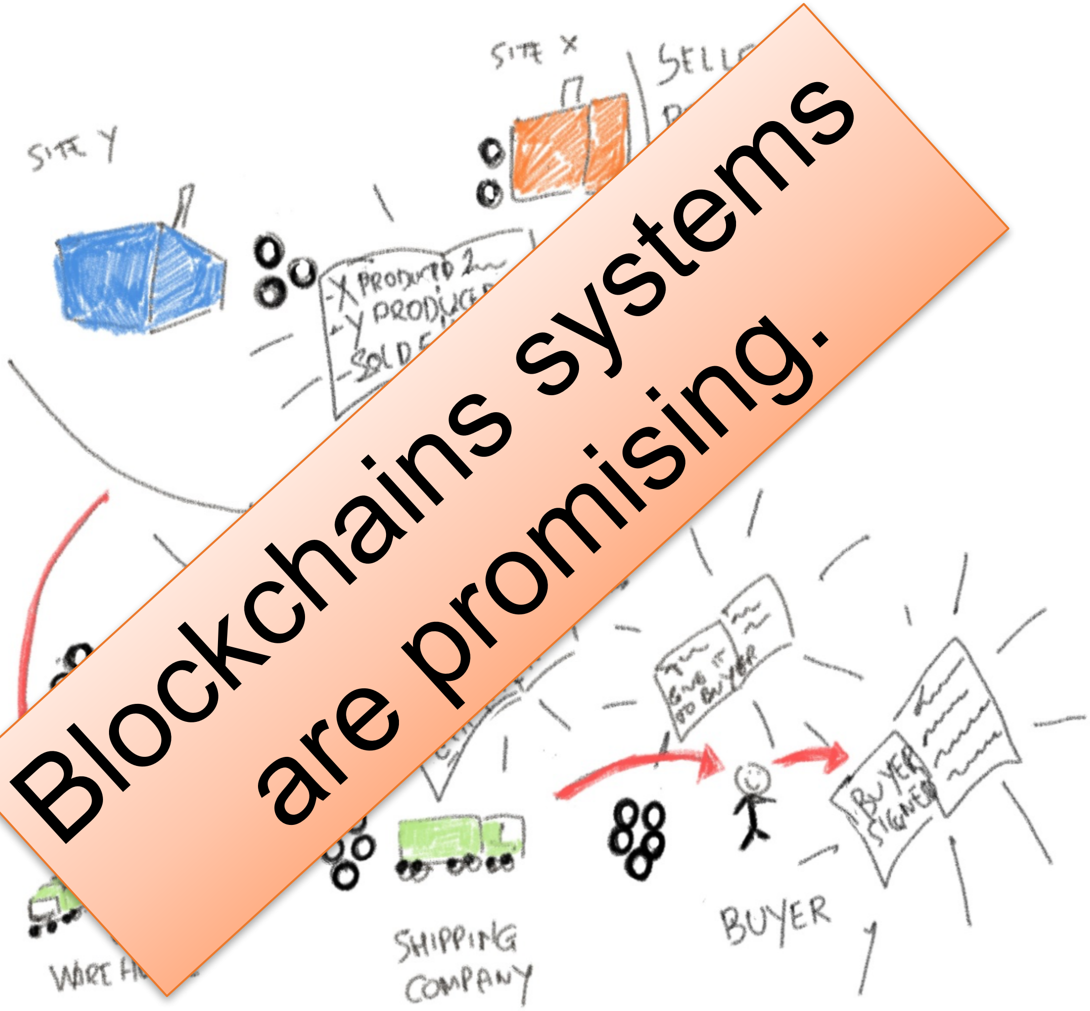
Creating trustworthy supply chains via fairness

Önder Gürcan, Antonella Del Pozzo, Sara Tucci-Piergiovanni
Programme Blockchain @ CEA LIST

Trustworthy Supply Chains

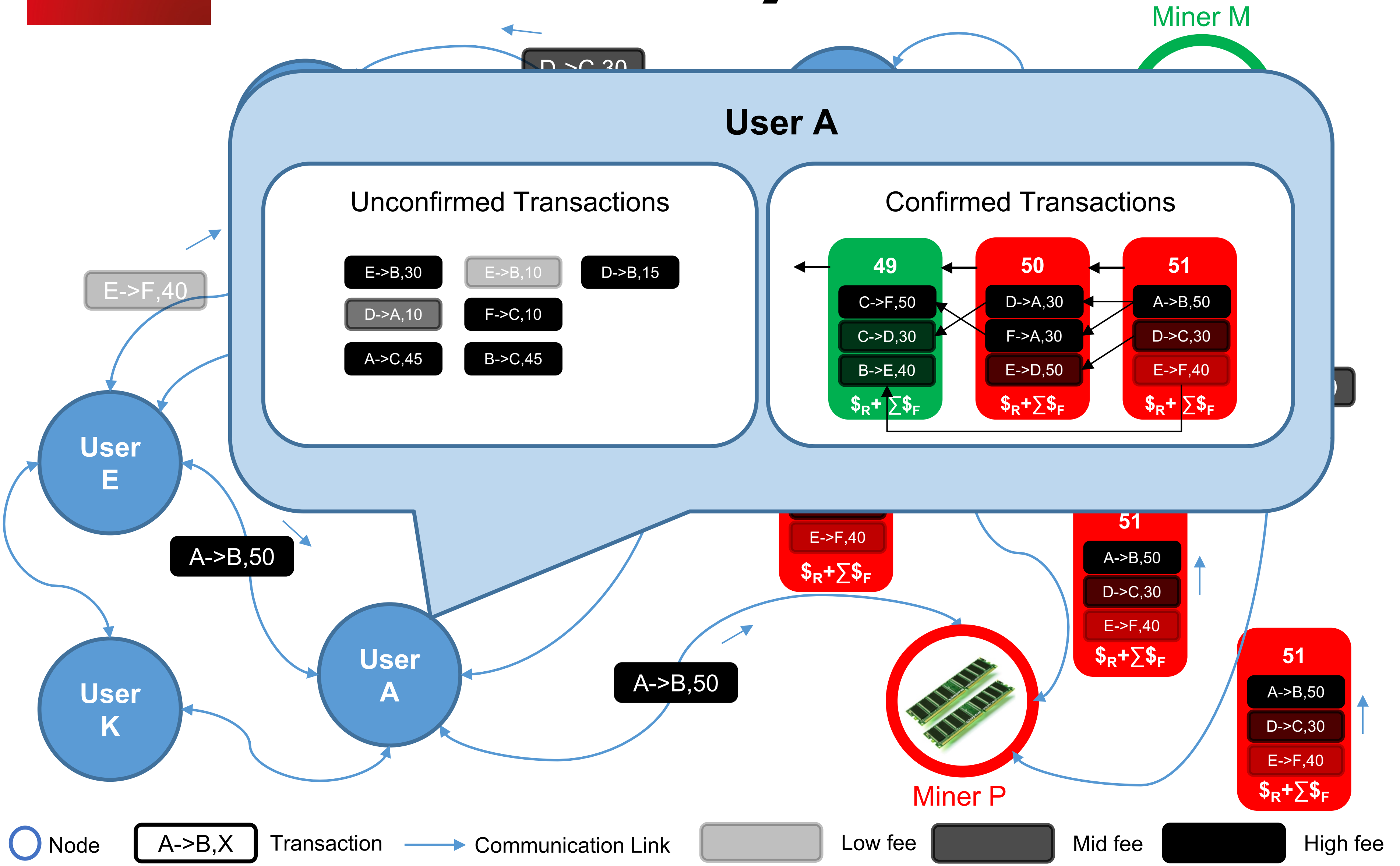
Transfer of ownership (or use) of assets (physical and digital) in a **cooperative** but possibly **competitive** environment.

Need for having an **audit trail**.

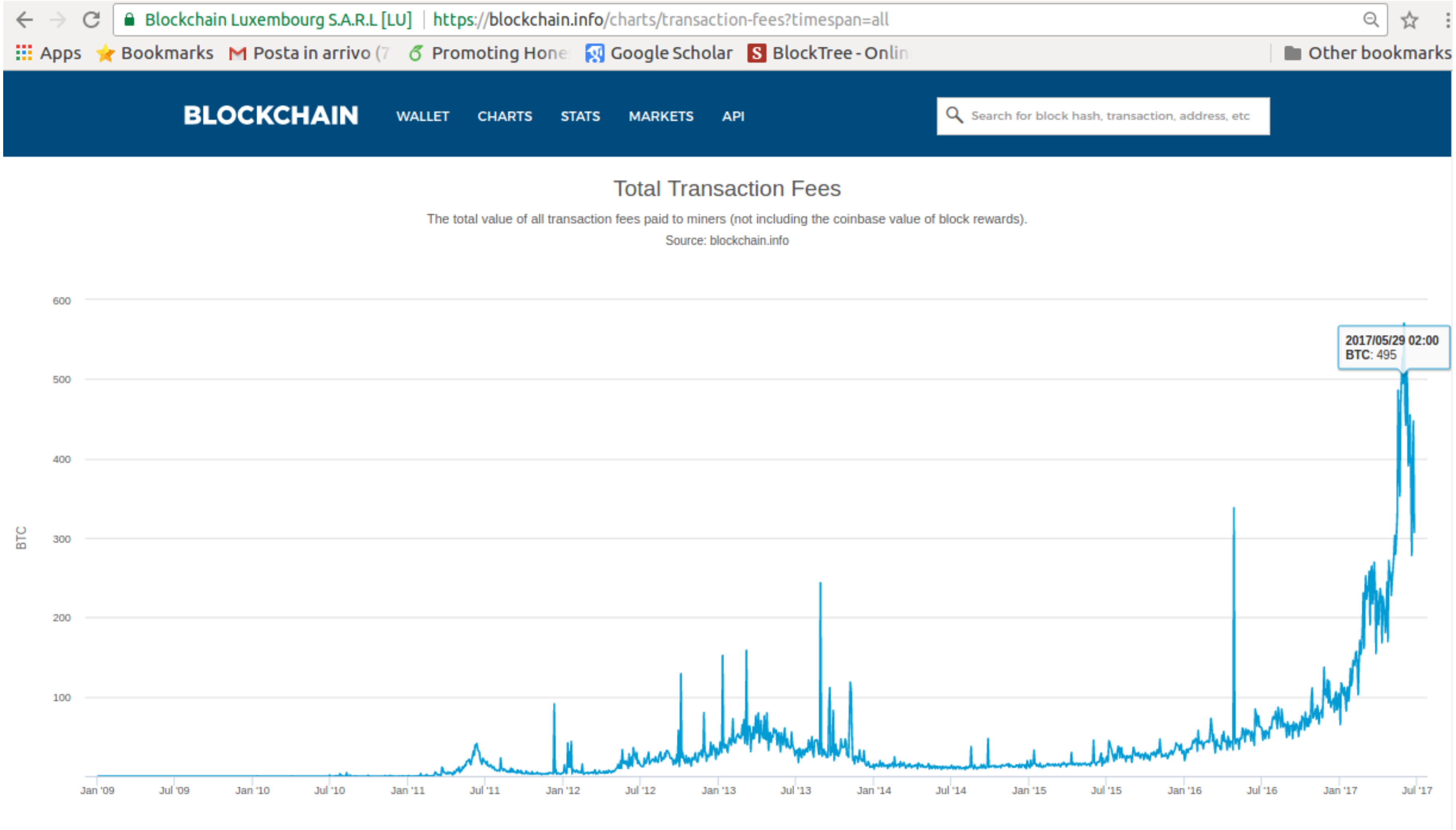


Blockchains systems are promising.

Blockchain Systems



Transaction fees over time

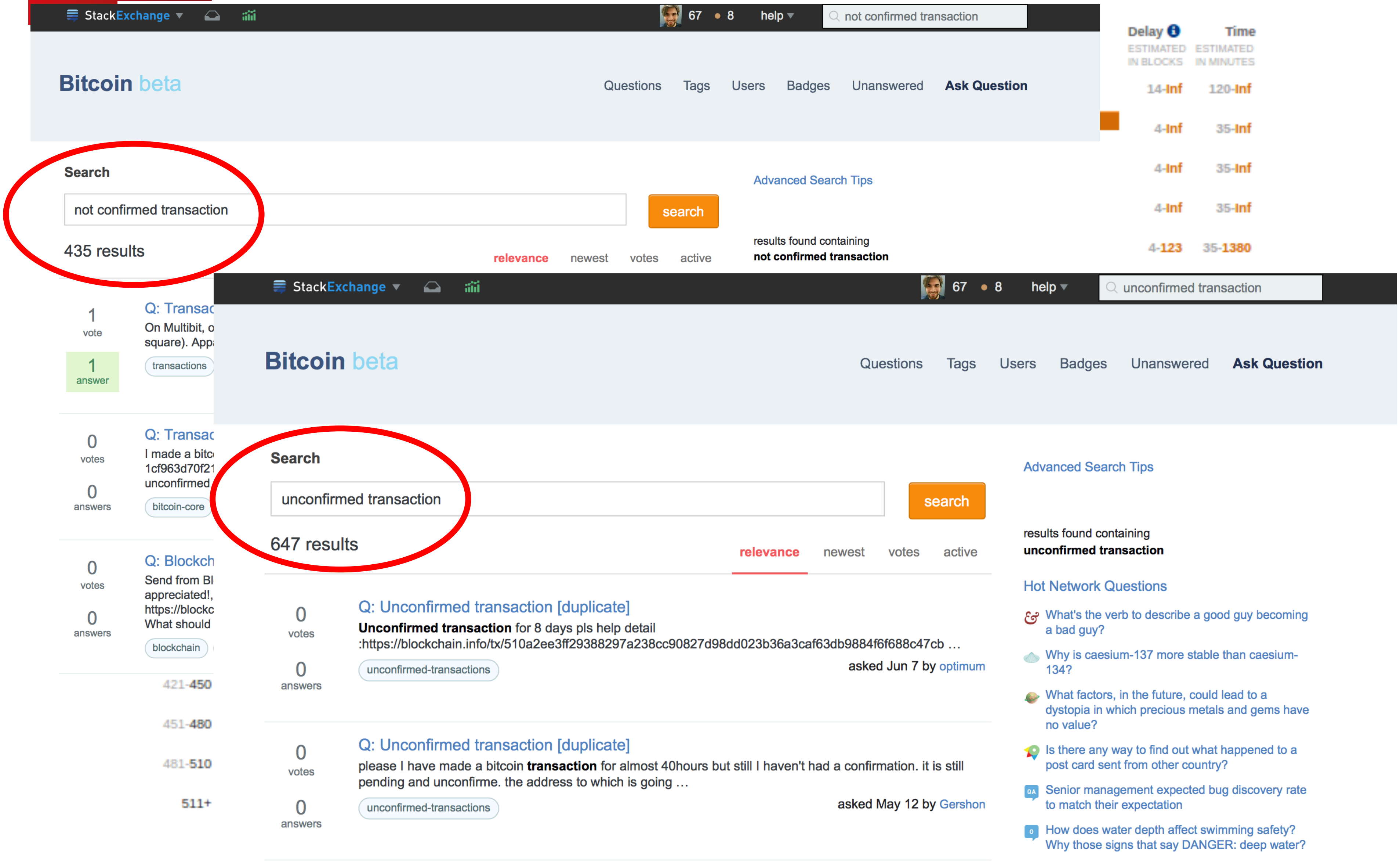

Blockchain Luxembourg S.A.R.L [LU]
https://blockchain.info/charts/transaction-fees?timespan=all
Apps
Bookmarks
Posta in arrivo (7
Promoting Hone
Google Scholar
BlockTree - Onlin
Other bookmarks
BLOCKCHAIN
WALLET
CHARTS
STATS
MARKETS
API
Search for block hash, transaction, address, etc

Total Transaction Fees

The total value of all transaction fees paid to miners (not including the coinbase value of block rewards).

Source: blockchain.info

Unconfirmed Transactions



StackExchange 67 ● 8 help not confirmed transaction

Bitcoin beta

Questions Tags Users Badges Unanswered **Ask Question**

Search

not confirmed transaction

search

Advanced Search Tips

435 results

relevance newest votes active

results found containing
not confirmed transaction

1 vote | 1 answer — Q: Transac
On Multibit, o
square). App
transactions

0 votes | 0 answers — Q: Transac
I made a bitc
1cf963d70f21
unconfirmed
bitcoin-core

0 votes | 0 answers — Q: Blockch
Send from Bl
appreciated!,
https://blockc
What should
blockchain

Delay ESTIMATED IN BLOCKS	Time ESTIMATED IN MINUTES
14-Inf	120-Inf
4-Inf	35-Inf
4-Inf	35-Inf
4-Inf	35-Inf
4-123	35-1380

421-450
451-480
481-510
511+

StackExchange 67 ● 8 help unconfirmed transaction

Bitcoin beta

Questions Tags Users Badges Unanswered **Ask Question**

Search

unconfirmed transaction

search

Advanced Search Tips

647 results

relevance newest votes active

results found containing
unconfirmed transaction

0 votes | 0 answers

Q: Unconfirmed transaction [duplicate]

Unconfirmed transaction for 8 days pls help detail :https://blockchain.info/tx/510a2ee3ff29388297a238cc90827d98dd023b36a3caf63db9884f6f688c47cb …

unconfirmed-transactions

asked Jun 7 by optimum

0 votes | 0 answers

Q: Unconfirmed transaction [duplicate]

please I have made a bitcoin **transaction** for almost 40hours but still I haven't had a confirmation. it is still pending and unconfirme. the address to which is going …

unconfirmed-transactions

asked May 12 by Gershon

Hot Network Questions

- What's the verb to describe a good guy becoming a bad guy?
- Why is caesium-137 more stable than caesium-134?
- What factors, in the future, could lead to a dystopia in which precious metals and gems have no value?
- Is there any way to find out what happened to a post card sent from other country?
- Senior management expected bug discovery rate to match their expectation
- How does water depth affect swimming safety? Why those signs that say DANGER: deep water?

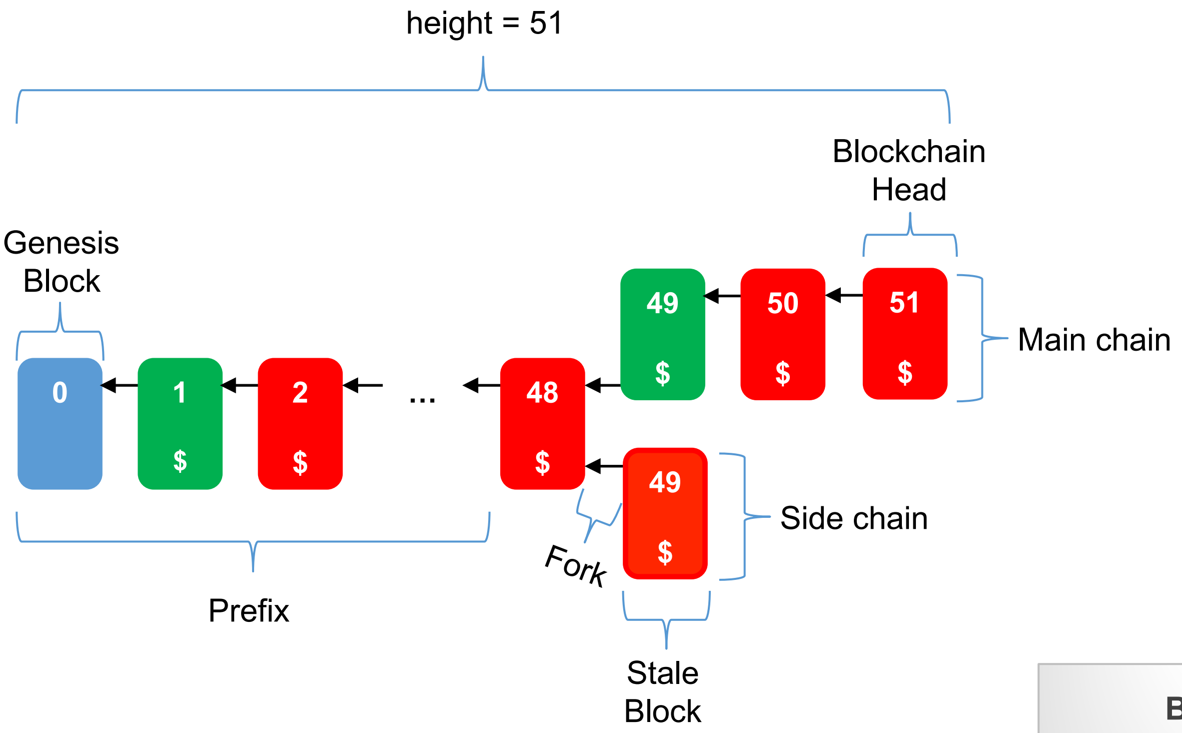
Fairness

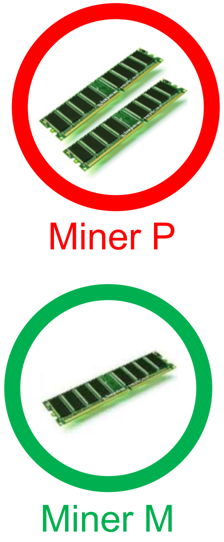
- A node *finds* a blockchain system ***fair***, if its overall *expectations* are *satisfied* to a certain degree.
  - Utility as a sum of expectation satisfaction

- Satisfied node -> Stays in the system
  - Increased # of participants
  - Increased security and stability

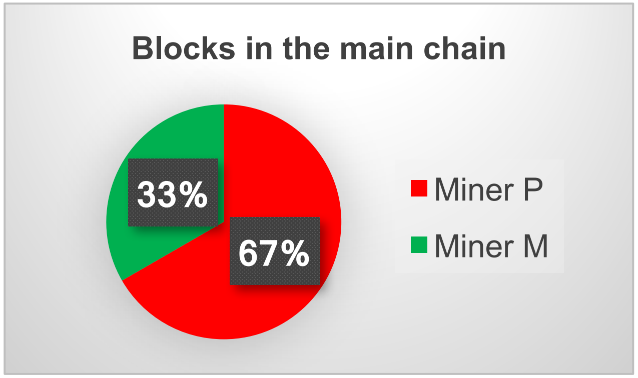
- Unsatisfied node -> Leaves the system
  - Decreased # of participants
  - Decreased security and stability
  - If everyone leaves -> no system at all

Anatomy of Blockchains





Quality of the chain



Garay et al. Study

Properties

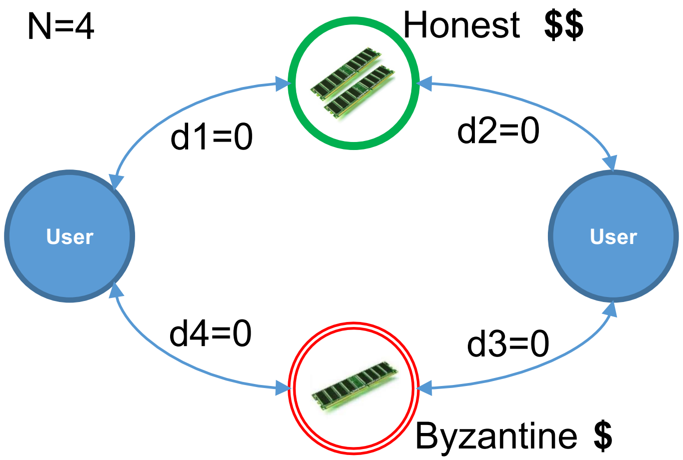
- Common prefix
  - Same blocks except for the recent ones.
- Chain quality
  - The number of blocks created by byzantines is limited.

Assumptions

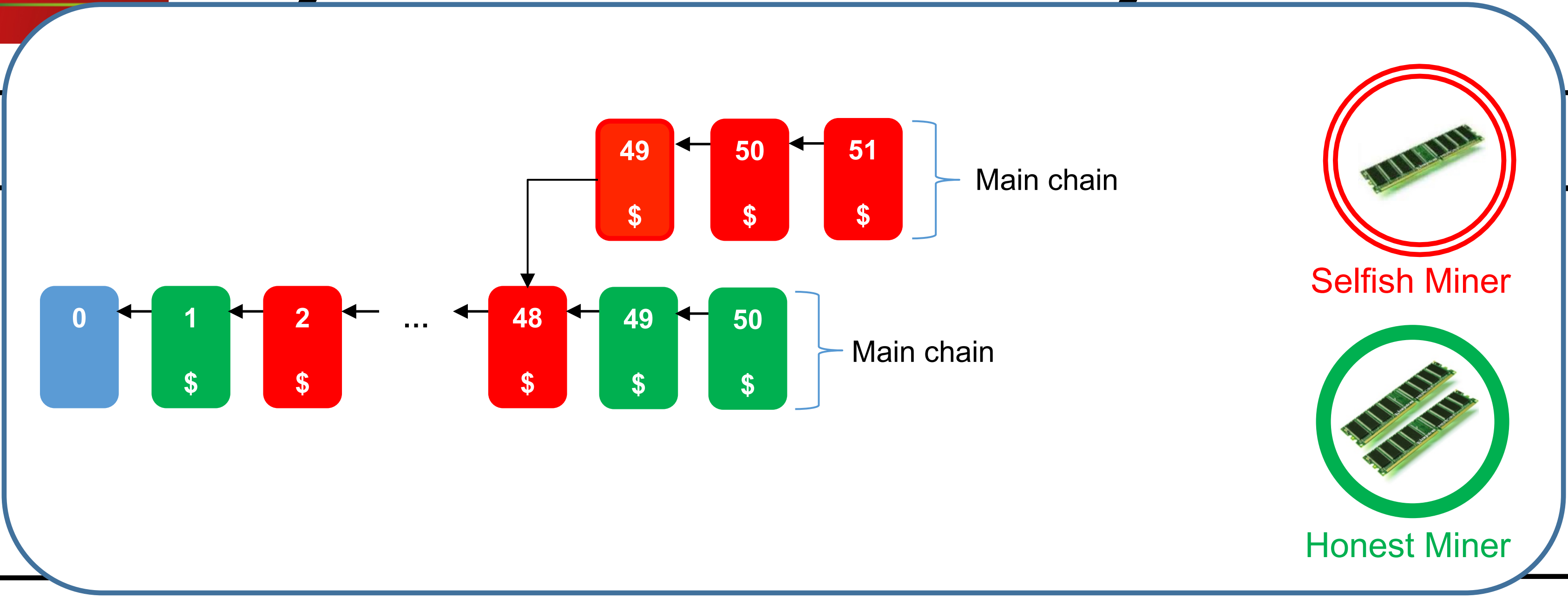
- Fix # of participants
- Honest and Byzantine miners
- Equal computational power q
- q-bounded synchronous setting
- No message delays (d=0)

Rewards are proportional to a fraction of computational power $\phi = q/\sum q_i$

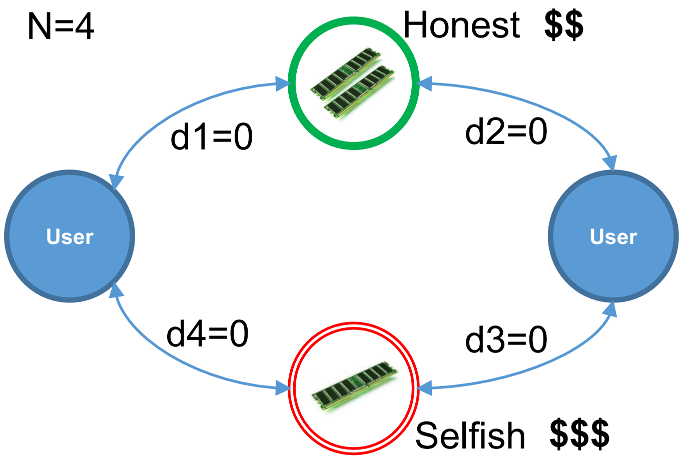
if $\phi_H > 50\%$.



Eyal et Sirer Study



- Even if most of the miners are honest (ϕ_H>50%), a byzantine
  - having enough resource + good connectivity
  - can **selfishly** increase rewards by *selectively withholding blocks*
- Blockchain is not « incentive compatible ».



Sapirshtein et al. Study

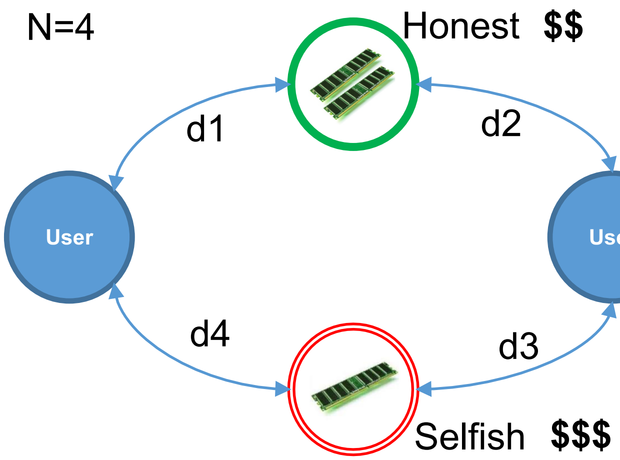
Properties

- Profit threshold
  - Minimum resources required for a profitable attack

Assumptions

- Fix # of participants
- Honest and Selfish miners
- Absence and presence of message delays

- Absence of delays
  - $\phi_H < 50\%$ is enough for a profitable attack.
- Presence of delays
  - The profit threshold vanishes
  - Any size of attacker can attack



d*=0 => pt < 50%

d*>0 => pt = 0%

Summary of Mining Studies

	No Delay / Delay is too small*	Delay is considerable
Honest mining	rewards are proportional to ϕ_H *(Garay et al., Pass and Shi)*	*(no published results yet)*
Selfish Mining + Honest Mining	ϕ_S > 50% and good connectivity => selfishly increase rewards *(Eyal and Sirer)* ϕ_S < 50% => selfishly increase rewards *(Sapisthein et al.)*	any ϕ_S => selfishly increase rewards *(Sapisthein et al.)*

These models focus on only miners and do not capture the necessary *properties* and *behaviors* for a fair blockchain system from **users** point of view.

* with respect to the time to block creation interval.

ϕ_S : fraction of selfish miners' computational power.
ϕ_H : fraction of honest miners' computational power.

So... for the users

- Unconfirmed Transactions
  - Workarounds:
    - 1: Resend it again as it is.
    - 2: Resend it with higher fees.
    - 3: Resend it directly to an **altruistic miner** (accept lower fees)
  - Free market => Increased fees.

- Transaction Cancellation
  - Workarounds:
    - 1: Try to double spend the same output (send to yourself).
    - 2: Wait several days for it to be forgotten.
  - No guarantee for cancellation.
  - In general they do not work.

Proposed User Strategy

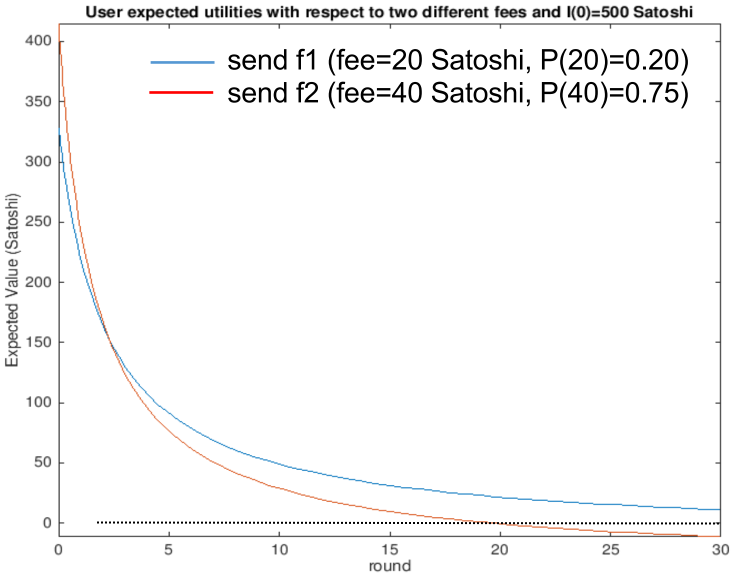
actions	tx confirmed during round r		tx unconfirmed during round r	Expected Value (EV)
send(tx, $f_{k(r-1)}$)	$(I(r) – f_{k(r-1)}) * P(f_{k(r-1)})$	+	$(I(r) – C_{k(r-1)}) * (1 – P(f_{k(r-1)}))$	$= EV(send(tx, f_{k(r-1)}))$
send(tx, $f_{k(r)}$)	$(I(r) – f_{k(r)}) * P(f_{k(r)})$	+	$(I(i) – C_{k(r)}) * (1 – P(f_{k(r)}))$	$= EV(send(tx, f_{k(r)}))$

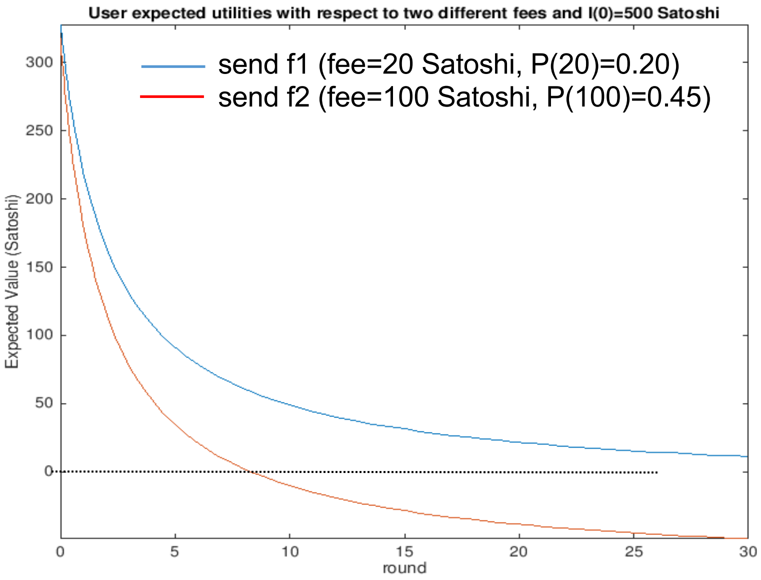
$f_{k(r-1)} < f_{k(r)}$, $0 \leq P(f_{k(r-1)}) \leq P(f_{k(r)}) \leq 1$, $I(r-1) < I(r)$, $C_{k(r-1)} < C_{k(r)}$

I(r): interest in tx at round r, C: cost of waiting for confirmation

A transaction re-sent with a higher fee overwrites the previous one, not true for a transaction re-sent with a lower fee.

The more the user has to wait for confirmation, the more it loses.





Proposed Definition of Fairness

Fairness for users means that:

$$\exists\ i > 0\ \wedge\ S = \{tx_1, tx_2, \ldots, tx_i\}$$

such that

$$\sum_i(\mathit{max}\mathrm{EV}(tx_j)) > 0$$

Conclusions

- Strong focus on miners, but *not on users*.
  - But every node is important.
- *Sustainability*, *security* and *stability* of blockchain systems depends on their **fairness**.
  - Since it promotes participation.
- We proposed initial user *strategies* for a fair blockchain system.
  - Initial simulation results.
- Bitcoin does not provide any proactive mechanisms to improve the situation of the users.
  - The proposed strategies are the best a user can do.

Prospects

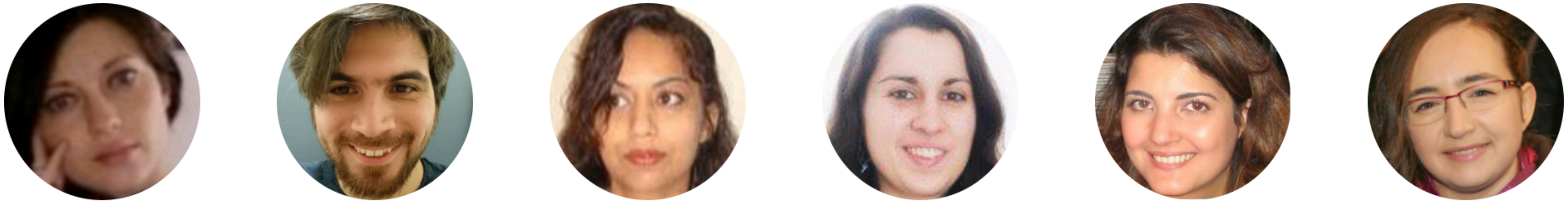
- Improving the strategies for users.
- Defining the fairness and the strategies for miners.
    - A preliminary work for selecting transactions confirming the fact that
        - if the proportion of the fixed reward is low, the miners tend to be more *picky*.
- Teratec as an ”altruistic miner” (accepting low fees)
    - Rebalancing the network (e.g., to decrease the average expected fees)
    - Increased user satisfaction, security and stability.

Thank you!

Block∞chain Program

CEA LIST

Sara Tucci-Piergiovanni	*Permanent, Team Leader*
Önder Gürcan	*Permanent*
Lea Zaynah Dargaye	*Permanent*
Antonella Del Pozzo	*Post-Doc*
Selma Azaiez	*Permanent*
Mathilde Arnaud	*Permanent*



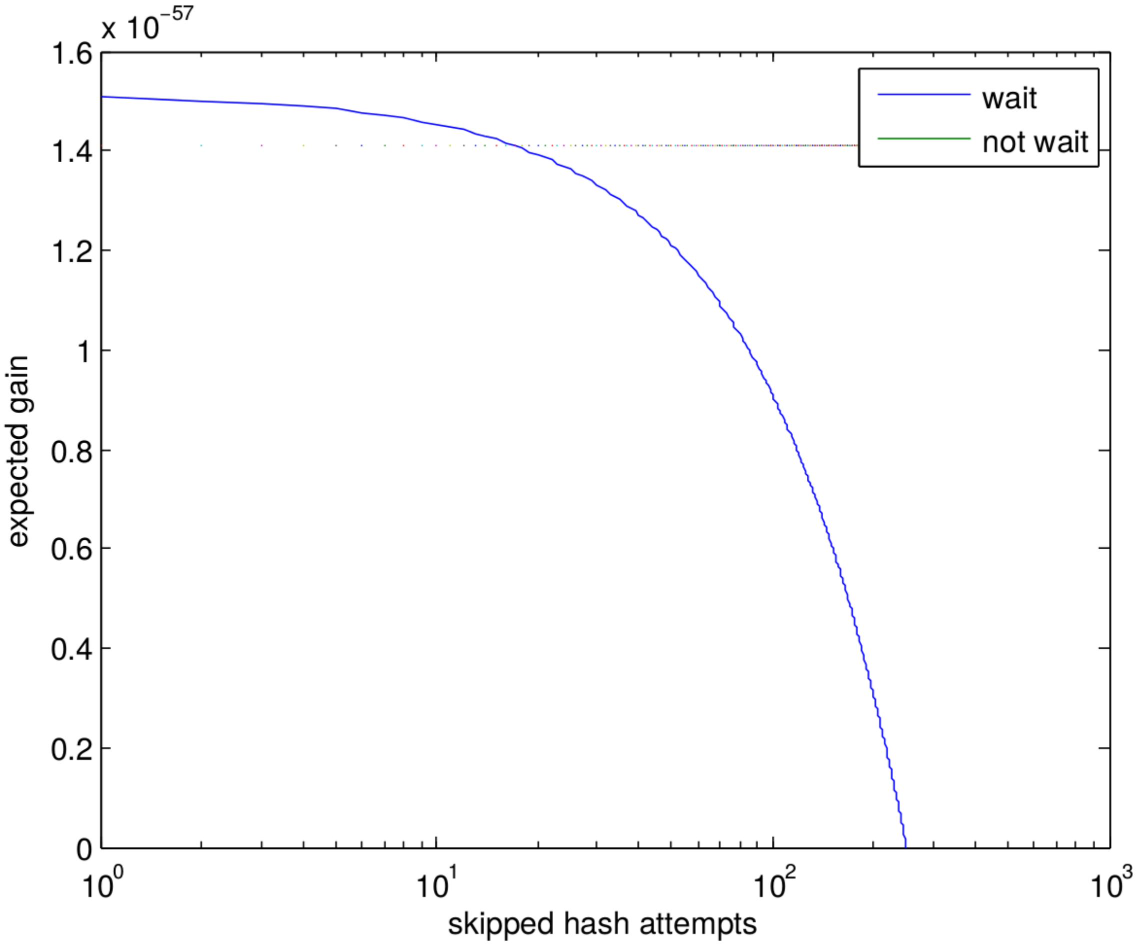
Commissariat à l'énergie atomique et aux énergies alternatives
91191 Gif-sur-Yvette Cedex
www-list.cea.fr

Établissement public à caractère industriel et commercial | RCS Paris B 775 685 019

Miner Strategy

When a new block is mined, the miner should start to mine given the transaction in its memory pool.
We consider the miner selects the transactions with the highest fees associated to be in the next block.
What if there are not enough “interesting” transaction in the memory pool?
P(q-q’): the probability to solve the POW from the moment q’ in a round of q attempts..

actions	“interesting”	no “interesting” tx arrives
wait	(12,5BTC+tx1+tx2)*P(q-q’)	(12,5BTC+tx1)*P(q-q’)
start mining	(12,5BTC+tx1)*P(q)	(12,5BTC+tx1)*P(q)


x 10^-57
1.6
1.4
1.2
1
0.8
0.6
0.4
0.2
0
expected gain
10^0
10^1
10^2
10^3
skipped hash attempts
wait
not wait