



BLOCKCHAIN

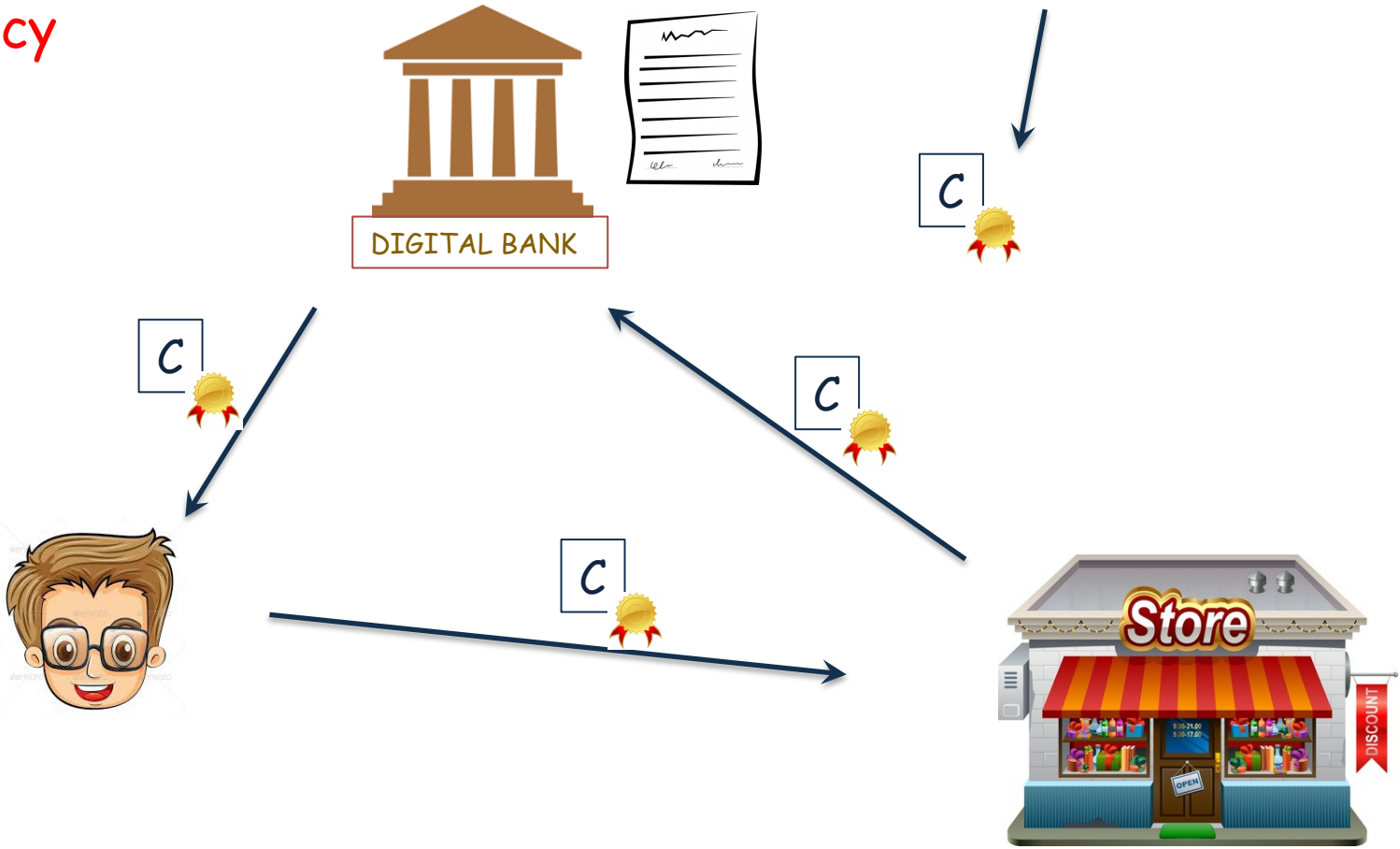
Murat Osmanoglu

E-Cash

- ✓ Double-spending
- ? Privacy

- check the list

1 C = 0101000...11100011



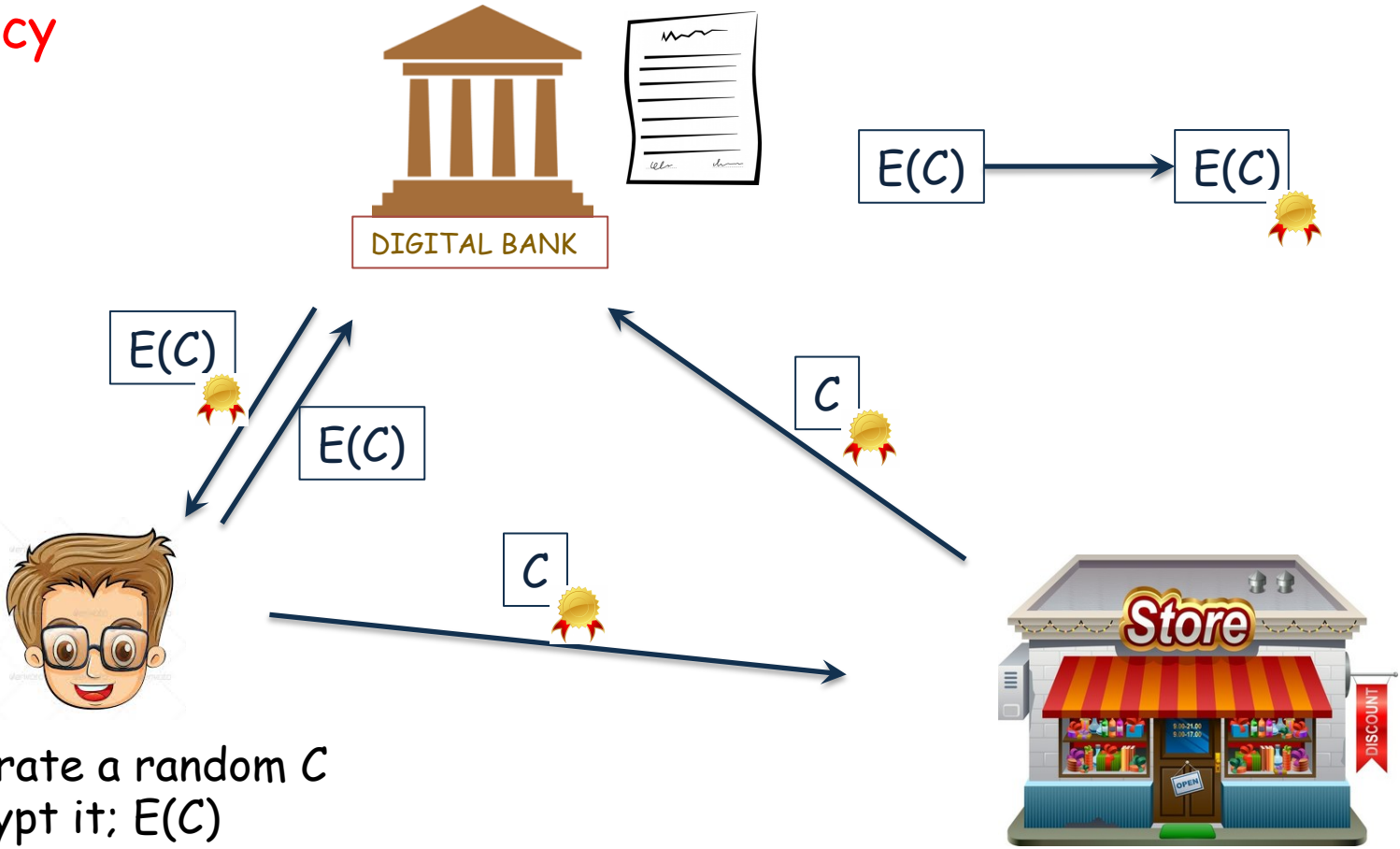
- check the signature
- send it to the bank for double-spending

E-Cash

- ✓ Double-spending
- ✓ Privacy

David Chaum, *Blind Signatures for Untraceable Payments*, 1982

- check the list



- generate a random C
- encrypt it; $E(C)$
- decrypt $S(E(C))$ as $S(C)$

- check the signature
- send it to the bank for double-spending



BITCOIN

BITCOIN

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model.

BITCOIN



Ali sends 3 bitcoins to Bulent

Bulent sends 2 bitcoins to Necla

Ali sends 5 bitcoins to Necla

·
·
·



Necla	20.2
Ali	15.2
Bulent	13
·	·
·	·
·	·

BITCOIN



Ali sends 3 bitcoins to Bulent

Ali sends 2 bitcoins to Bulent

Ali sends 4 bitcoins to Necla



DIGITAL BANK

Necla	17.2
Ali	14.2
Bulent	20
.	.
.	.
.	.

BITCOIN



Ali sends 3 bitcoins to Bulent

Bulent sends 2 bitcoins to Necla

digital signature



DIGITAL BANK

Necla	13.2
Ali	23.2
Bulent	15
.	.
.	.
.	.

BITCOIN

attack the network, they must generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

BITCOIN



Ali sends 3 bitcoins to Bulent

Bulent sends 2 bitcoins to Necla

digital signature



Necla	13.2
Ali	23.2
Bulent	15
.	.
.	.
.	.

BITCOIN



Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.



Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.

Ali sends 3 bitcoins to Bulent

Necla sends 4 bitcoins to Bülent

Bülent sends 2 bitcoin to Necla



Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.

BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

Ali sends 3 bitcoins to Bulent

Necla sends 4 bitcoins to Bülent

Bülent sends 2 bitcoin to Necla



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

BITCOIN




Ali	20.2
Bülent	15
Necla	1.12
.	.
.	.
.	.

Ali sends 3 bitcoins to Bulent

Necla sends 4 bitcoins to Bülent

Bülent sends 2 bitcoin to Necla



Ali	23.2
Bülent	10
Necla	3.12
.	.
.	.
.	.



Ali	23.2
Bülent	6
Necla	7.12
.	.
.	.
.	.

BITCOIN



Ali	20.2
Bülent	15
Necla	1.12
.	.
.	.
.	.

Ali sends 3 bitcoins to Bülent

Necla sends 4 bitcoins to Bülent

Bülent sends 2 bitcoin to Necla

Ali	23.2
Bülent	10
Necla	3.12
.	.
.	.
.	.

Ali	23.2
Bülent	6
Necla	7.12
.	.
.	.
.	.

- How to avoid 'forking' ?



BITCOIN



Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.

Ali sends 3 bitcoins to Bülent

Necla sends 4 bitcoins to Bülent

Bülent sends 2 bitcoin to Necla



Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.



Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.

BITCOIN



Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.

Ali sends 3 bitcoins to Bulent

Necla sends 4 bitcoins to Bülent

Bülent sends 2 bitcoin to Necla

Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

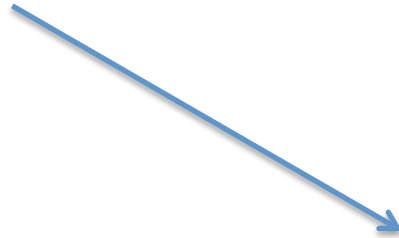
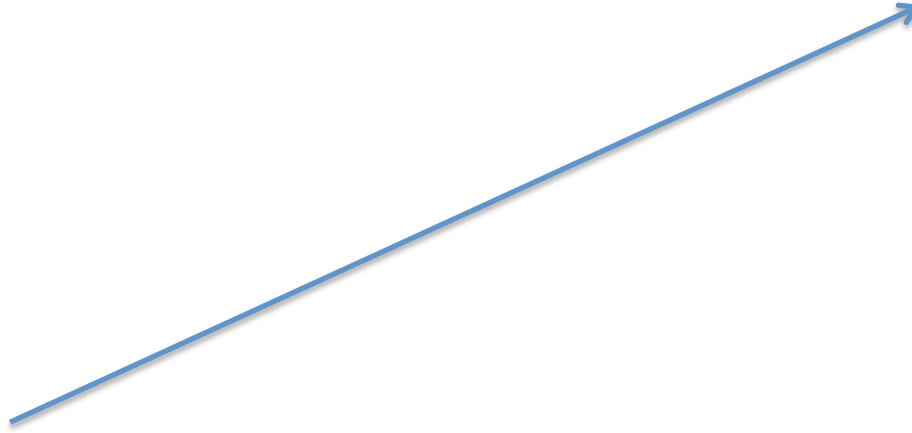


Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.

BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.

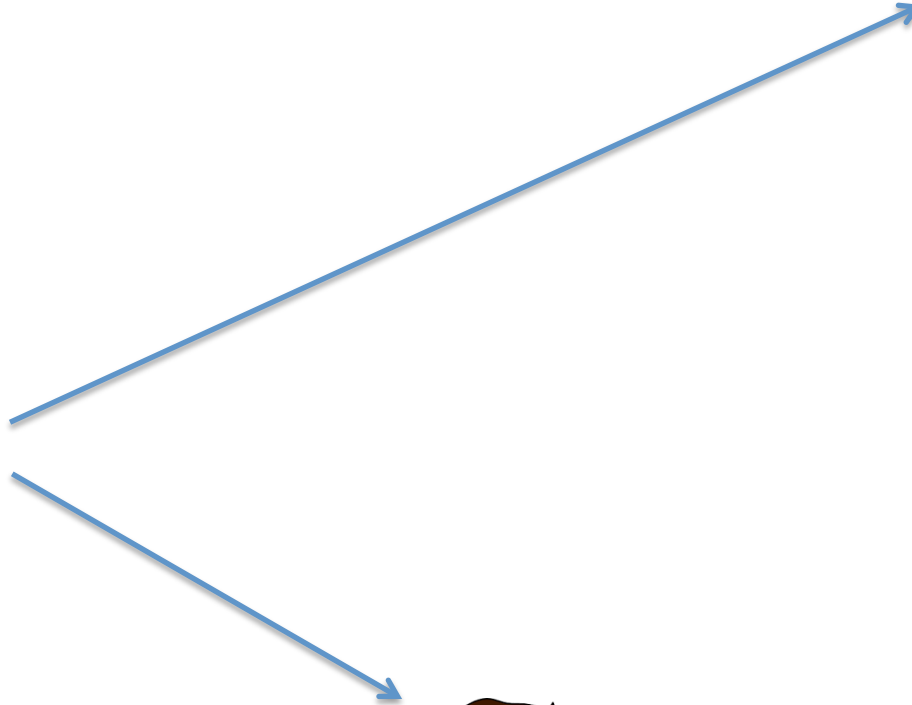


Ali	23.2
Bülent	8
Necla	5.12
.	.
.	.
.	.

BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



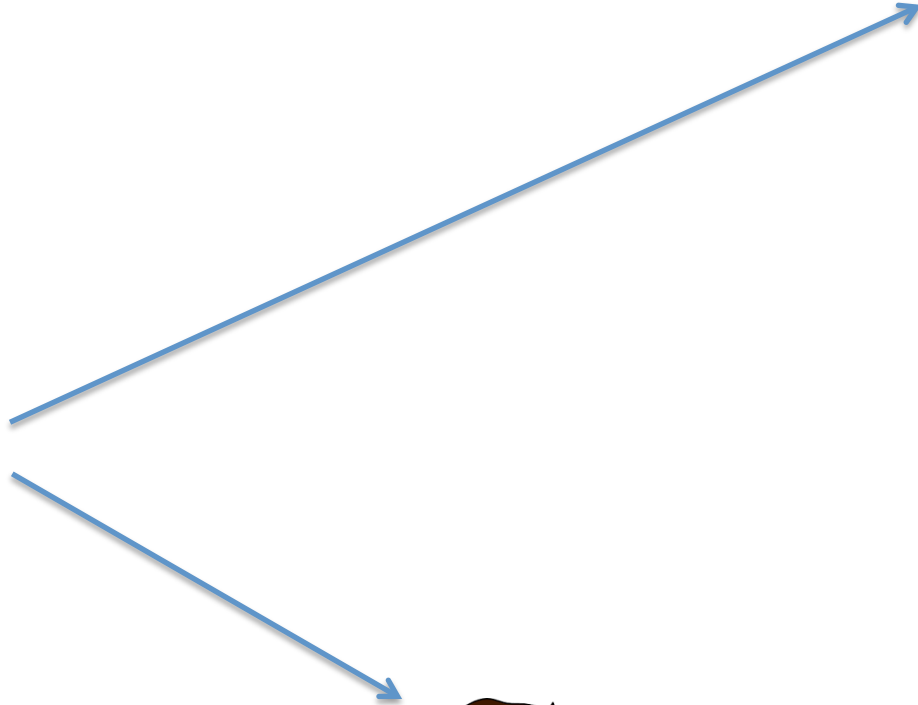
Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



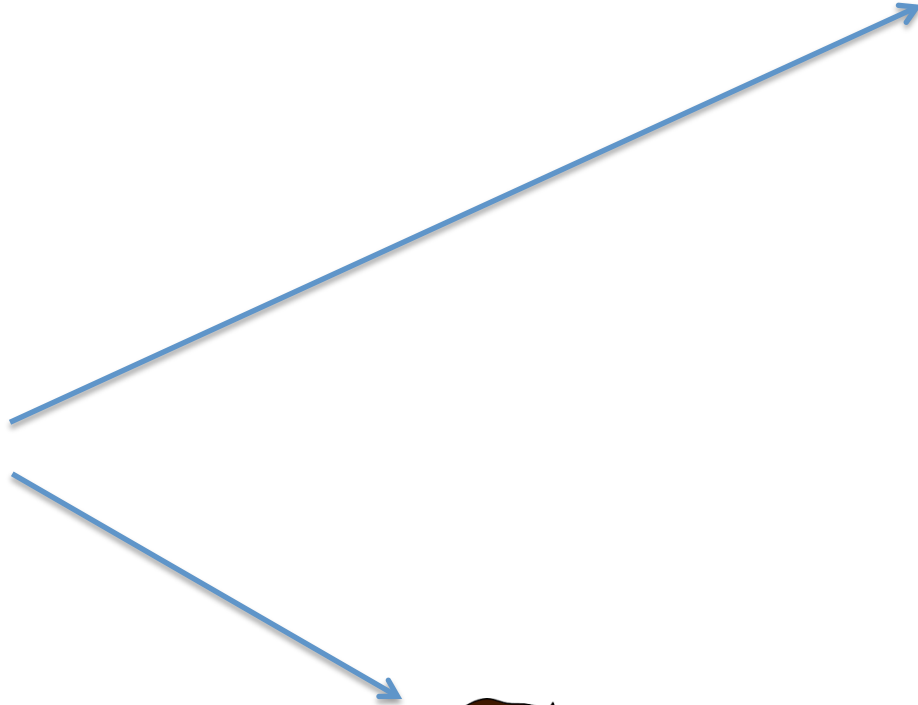
- How to avoid 'forking' ?

BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



- How to avoid 'forking' ?
- Incentive ?

BITCOIN

messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

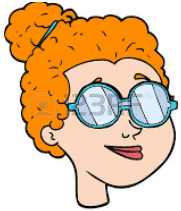
6. Incentive

By convention, the first transaction in a block is a special transaction that starts a new coin owned by the creator of the block. This adds an incentive for nodes to support the network, and provides a way to initially distribute coins into circulation, since there is no central authority to issue them. The steady addition of a constant amount of new coins is analogous to gold miners expending resources to add gold to circulation. In our case, it is CPU time and electricity that is expended.

The incentive can also be funded with transaction fees. If the output value of a transaction is less than its input value, the difference is a transaction fee that is added to the incentive value of the block containing the transaction. Once a predetermined number of coins have entered circulation, the incentive can transition entirely to transaction fees and be completely inflation free.

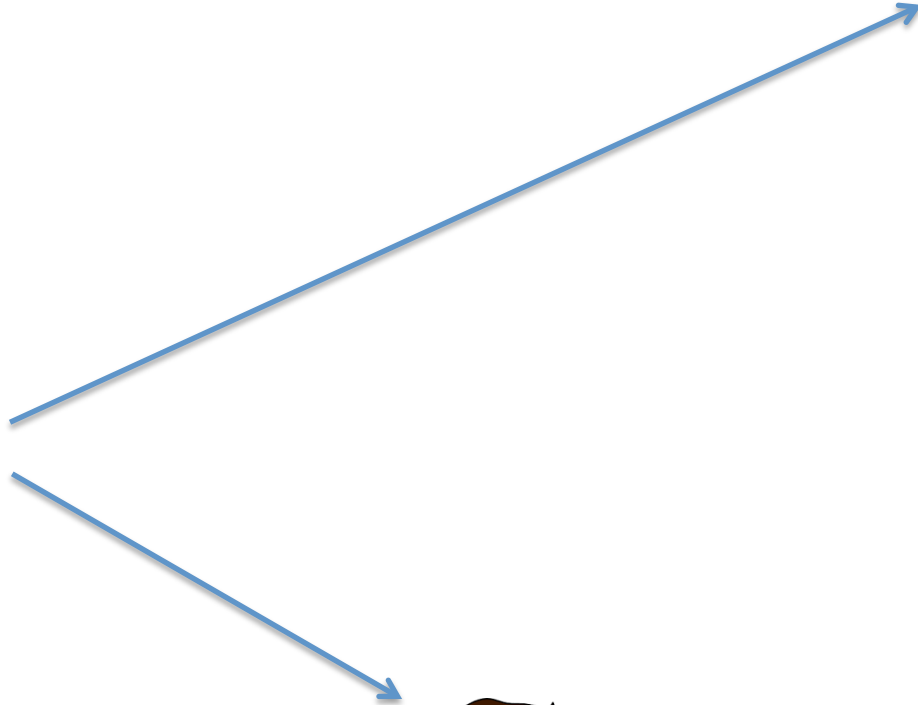
The incentive may help encourage nodes to stay honest. If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.

BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

- ✓ • How to avoid 'forking' ?
- ✓ • Incentive ?

BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

- ✓ • How to avoid 'forking' ?
- ✓ • Incentive ?

BITCOIN



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.

Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.



Ali	20.2
Bülent	13
Necla	3.12
.	.
.	.
.	.