

# CommunityCoin: a crypto currency for community networks

p4u, manos

guifi.net,upc

May 16, 2014



Introduction

BitCoin

BlockChain

CommunityCoin

Motivation

Ideas

Your ideas



# Proof of Work

- Basic concept: each participant must prove his effort
- Originally used for preventing SPAM
- The sender of an e-mail must include a hash with specific requirements
- CPU consumption forces the e-mail sender to spend some time to send the text



# Proof of Work in BitCoin

- BitCoin based on the same concept
- Currency transactions must be validated and included to a shared block chain
- The validation requires some work, so validators (miners) must spend resources
- There is a reward for the validation (this is how currency is generated)



# Bitcoin network

The BitCoin network is a p2p network

Every peer needs to download the whole blockchain

Users use wallets as identifier: a set of asymmetric keys

Users broadcast transactions which are validated by nodes (miners)

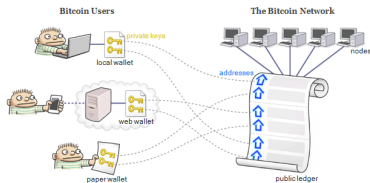


Figure: BitCoin network





# BlockChain

As you can guess, the blockchain can be used for many purposes

- A distributed domain name system (NameCoin)
- A platform to sign legal documents
- A platform to validate that a photo has been taken in a specific time
- A voting system
- etc...

It is just fucking amazing!



Introduction

BitCoin

BlockChain

CommunityCoin

Motivation

Ideas

Your ideas





# Motivation

1. An economic system is needed to organize a community where resources are limited
2. Community is not only about tech stuff, it involves also socio-economic aspects
3. We own our network, why not to own our own economic system?
4. It adds many new ways for funding, thus it makes the community more sustainable
5. It might incentivize community users to work for the community
6. It can be fun :)



# Things to avoid

1. Create just another crypto-scam-coin
2. Make the system very expensive to maintain (PoW)
3. Create a tool to enable speculation
4. Destroy the community volunteer actions



## Things to include

1. Reward based on user contributions to the community
2. Distribute the coins in a fair way
3. Try to restrict its usage only for community related stuff (Proof of Identity)
4. Use some other less-expensive system (PoS?) rather than PoW
5. Create not only a currency but also a platform to organize the community (voting system, dns, etc.)



## Transaction control (PoI)

1. There must be at least 1 SuperNode per Community
2. Community SuperNodes must know which users are valid (active)
3. Each currency transaction must be validated by at least one SN (sender and reciver)
4. SuperNodes are in a trusted ring (a non trusted supernode is not considered a valididator)
5. The acceptance of a new SuperNode must be accepted by at least the 51% of the SuperNodes



# Transaction control (PoI)

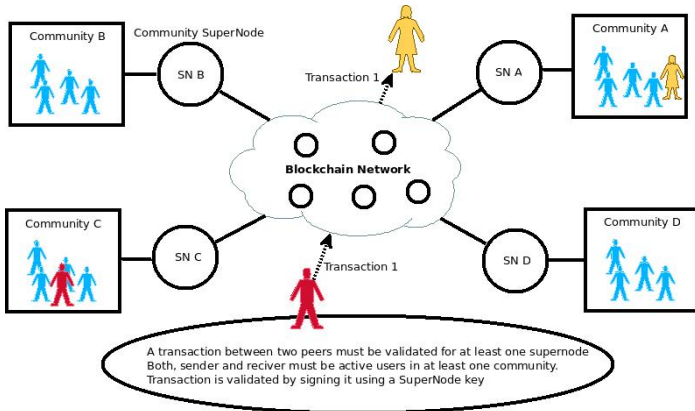


Figure: Transactions



## Reward distribution

1. Proof of stake to keep the blockchain secure (small reward each block)
2. Each N blocks, big reward based on user contribution (C-reward)
  - The C-reward is spread among SuperNodes according to the number of transactions done the last N blocks
  - Communities SN must distribute the coins according its internal metrics
  - These metrics must be based on user contributions but this is up to each community



# Feedback

So, what do you think? <http://piratepad.net/communitycoin>



# Feedback

`http://emmdim.pc.ac.upc.edu:5000/lm/`





# CommunityCoin: a crypto currency for community networks

p4u, manos

guifi.net,upc

May 16, 2014

