# OpenBazaar and Namecoin Integration

Kostis Lolos
Chara Podimata

National Technical University of Athens

*lolos.kostis@gmail.com*
*charapod@gmail.com*

April 3, 2015

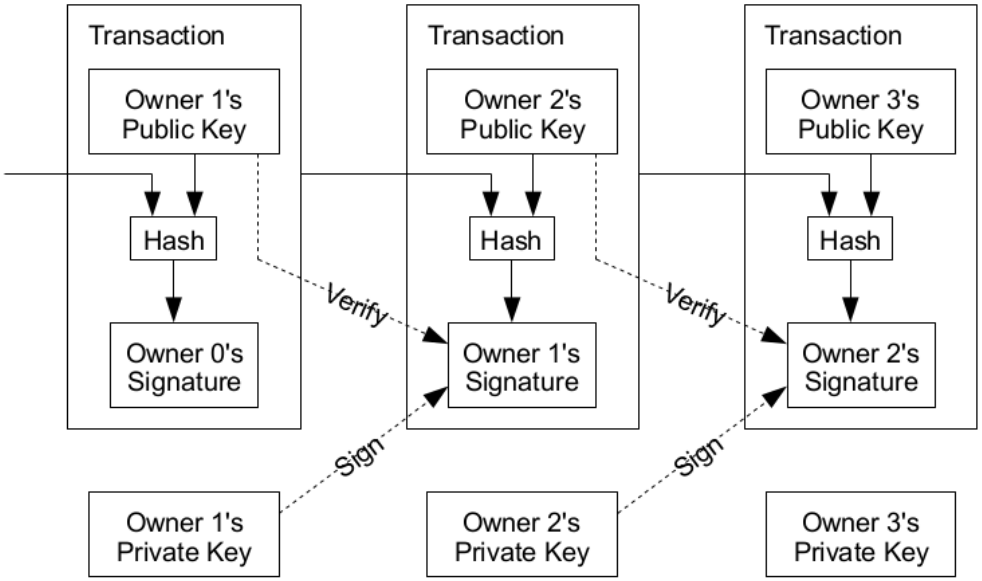
# Overview

- Bitcoin
  - What is it
  - How it works
- Namecoin
  - Differences from Bitcoin
- OpenBazaar
  - What is OpenBazaar?
  - How does OB work
  - Proof-of-burn and Reputation Pledges
- OB and Namecoin
  - Why OB and Namecoin

# Bitcoin: A new kind of currency

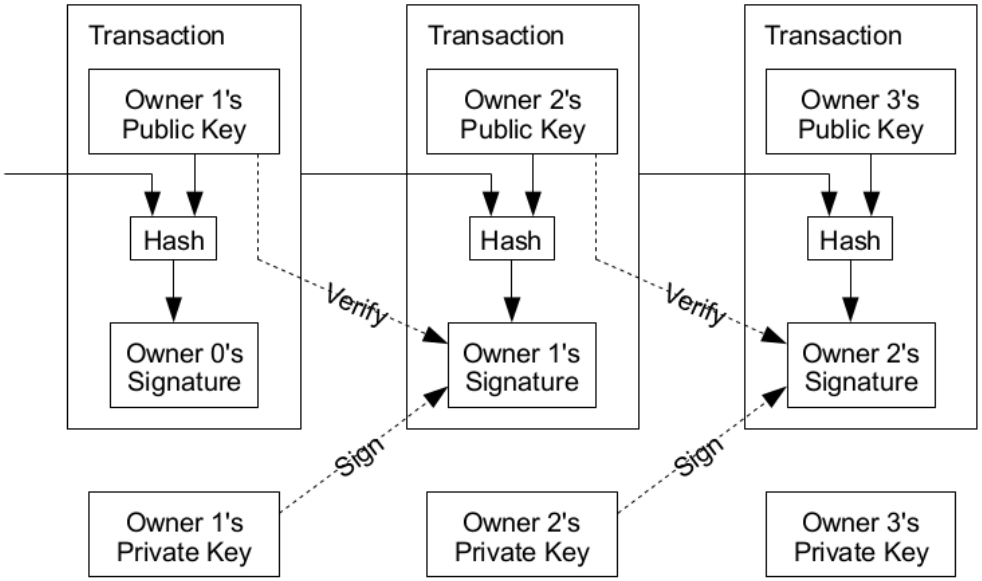
- Proposed by Satoshi Nakamoto in 2008
- Open Source implementation in 2009
- $10 Billion total value of coins in 2014
- Decentralized
- No central authority or control
- Potentially Anonymous
- Extremely low transaction fees

# Bitcoin: A new kind of currency




- Series of signatures

# Bitcoin: A new kind of currency




- Series of signatures
- Transactions stored in a block chain
- Proof-of-work to prevent changes

# Namecoin: A child of Bitcoin

- The first fork of Bitcoin

# Namecoin: A child of Bitcoin

- The first fork of Bitcoin
- Names represented as special coins
- Data associated with them

# Namecoin: A child of Bitcoin

- The first fork of Bitcoin
- Names represented as special coins
- Data associated with them
- Distributed DNS (.bit)

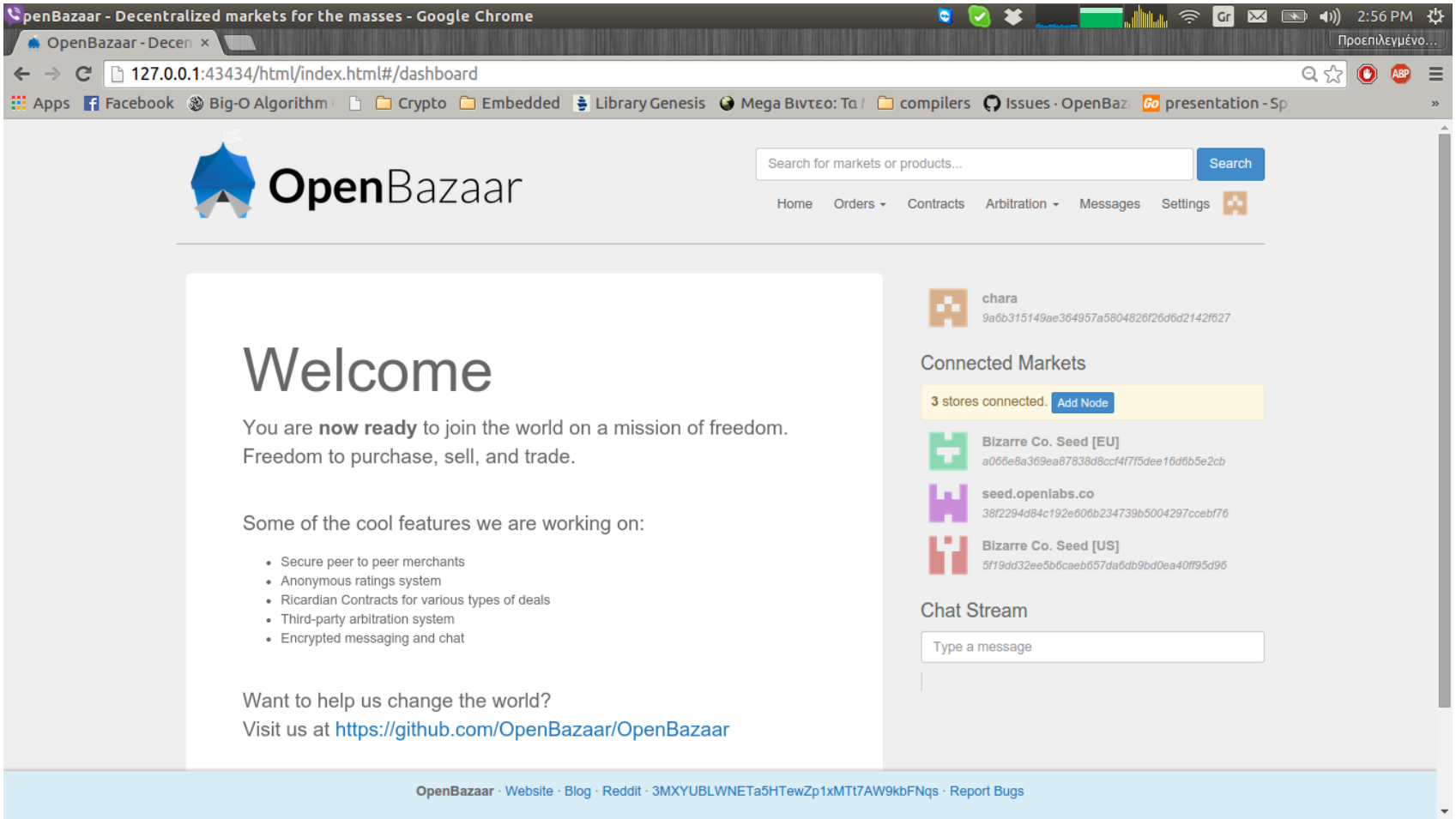



Figure : Homepage

# General Info

# General Info


- open-source project for a decentralized marketplace using BTC
- **no fees, no censorship**
- p2p
- OB = eBay + BitTorrent

# Up to now online commerce means

- centralized services

# Up to now online commerce means

- centralized services
- restrictive policies

# Up to now online commerce means

- centralized services
- restrictive policies
- fees for listing/selling goods

# Up to now online commerce means

- centralized services
- restrictive policies
- fees for listing/selling goods
- only forms of payment accepted: credit cards, PayPal

# Up to now online commerce means

- centralized services
- restrictive policies
- fees for listing/selling goods
- only forms of payment accepted: credit cards, PayPal
- personal info required $\Rightarrow$ this info can be stolen or sold

# Up to now online commerce means

- centralized services
- restrictive policies
- fees for listing/selling goods
- only forms of payment accepted: credit cards, PayPal
- personal info required $\Rightarrow$ this info can be stolen or sold
- $\exists$ censorship

# Up to now online commerce means

- centralized services
- restrictive policies
- fees for listing/selling goods
- only forms of payment accepted: credit cards, PayPal
- personal info required $\Rightarrow$ this info can be stolen or sold
- $\exists$ censorship

OB puts back the power to users! No more users through a centralized service! We are directly connected, not censored, not charged!

Let's say you 've decided to sell your old laptop

- create a listing with product details + price and publish it on the network $\Rightarrow$ it now appears when keywords are searched
- Prominent buyer can either accept your price or offer a new one
- Once you have agreed on the price $\Rightarrow$ sign a contract with **digital signatures**
- contract sent to a third party (notaries, arbiters) $\Rightarrow$ she witnesses contract so as to release BTC

# What if something goes wrong?

People are no angels. Sellers may ship products in poorer condition or not ship products at all.

# What if something goes wrong?

People are no angels. Sellers may ship products in poorer condition or not ship products at all.
**What can we do about that?**

# What if something goes wrong?

People are no angels. Sellers may ship products in poorer condition or not ship products at all.
**What can we do about that?** Third party!
**Remember!** BTC is released after 2 of 3 parties agree
**Ok, but how can I trust the third party?**

# What if something goes wrong?

People are no angels. Sellers may ship products in poorer condition or not ship products at all.
**What can we do about that?** Third party!
**Remember!** BTC is released after 2 of 3 parties agree
**Ok, but how can I trust the third party?** OB: **reputation + rating system!**
$\Rightarrow$ users are allowed to rate (give feedback) about other users
$\Rightarrow$ scam a user $\rightarrow$ your reputation will suffer
$\Rightarrow$ when you are about to select a third party, pick one that the network trusts

# Proof-of-burn

## Proof-of-burn

Term used to describe the intentional and provable destruction of BTC for a particular purpose. Funds are intentionally sent to an address that is unspendable, meaning **those coins are gone forever**.

# Proof-of-burn

## Proof-of-burn

Term used to describe the intentional and provable destruction of BTC for a particular purpose. Funds are intentionally sent to an address that is unspendable, meaning **those coins are gone forever**.

**Ok, but why would anyone destroy BTC on purpose?**

# Proof-of-burn

## Proof-of-burn

Term used to describe the intentional and provable destruction of BTC for a particular purpose. Funds are intentionally sent to an address that is unspendable, meaning **those coins are gone forever**.

**Ok, but why would anyone destroy BTC on purpose?**

1. Past: to bootstrap one cryptocurrency from another (people burning coins in exchange for the new currency)
2. ... proof-of-burn as reputation pledges (OB)

# Reputation Pledges

- users in OB are anonymous

# Reputation Pledges

- users in OB are anonymous ⇒ sometimes difficult to determine whether they are trustworthy or not
- **Reputation System**:

# Reputation Pledges

- users in OB are anonymous ⇒ sometimes difficult to determine whether they are trustworthy or not
- **Reputation System**: helps you know which users have acted honestly in the past, and which haven't
- For example, let's think of travelling salesmen ...
- Similarly in OB: You 've invested resources that create an incentive to keep a good reputation and impose significant cost for abandoning that reputation.

# Why OB and Namecoin

- Human-readable address names

# Why OB and Namecoin

- Human-readable address names
  - Users declare their Namecoin from the UI
  - Claimed Namecoin is relayed to other users
  - Namecoin is displayed as the unique Store URL

# Why OB and Namecoin

- Human-readable address names
  - Users declare their Namecoin from the UI
  - Claimed Namecoin is relayed to other users
  - Namecoin is displayed as the unique Store URL
- Security

# Why OB and Namecoin

- Human-readable address names
  - Users declare their Namecoin from the UI
  - Claimed Namecoin is relayed to other users
  - Namecoin is displayed as the unique Store URL
- Security
  - Each user: EC key $\Rightarrow$ GUID
  - GUIDs stored in the blockchain
  - Namecoin owner's GUID is matched with sender's GUID

# Why OB and Namecoin

- Human-readable address names
  - Users declare their Namecoin from the UI
  - Claimed Namecoin is relayed to other users
  - Namecoin is displayed as the unique Store URL
- Security
  - Each user: EC key $\Rightarrow$ GUID
  - GUIDs stored in the blockchain
  - Namecoin owner's GUID is matched with sender's GUID
  - $\Rightarrow$ remote node is verified to be the Namecoin owner

# Why OB and Namecoin

- Human-readable address names
  - Users declare their Namecoin from the UI
  - Claimed Namecoin is relayed to other users
  - Namecoin is displayed as the unique Store URL
- Security
  - Each user: EC key $\Rightarrow$ GUID
  - GUIDs stored in the blockchain
  - Namecoin owner's GUID is matched with sender's GUID
  - $\Rightarrow$ remote node is verified to be the Namecoin owner
  - $\Rightarrow$ messages verified to be composed and encrypted by the same person

# Thank you ☺