

Society Unchained

by
Christian Lains
Manuel Lains



Presentation at FSCONS 2015
7-8 November, Göteborg, Sweden

Bitcoin and Beyond



The Bitcoin Ecosystem



- Three aspects of Bitcoin
 - as Blockchain
 - as Currency
 - as Ecosystem
- Three aspects of the Ecosystem
 - Bitcoin 1.0 (Currency)
 - Bitcoin 2.0 (Crypto Finance)
 - Bitcoin 3.0 (Beyond Finance)

Bitcoin 1.0



- Cryptocurrencies

- Bitcoin
- Litecoin
- Dogecoin
- Dash
- Primecoin
- Kanyecoin



Bitcoin 2.0



- **Crypto-Finance**
 - Decentralized, cryptographically secure finance
 - Any online transaction of value can now be decentralized in a trustless manner without a controlling authority in the middle
- **Example**
 - BitShares Exchange

BitShares



- Decentralized Exchange
- Trade various financial instruments
 - Cryptocurrencies
 - Smartcoins
 - User-Issued Assets
 - Private / Public equities

Bitcoin 3.0



- Beyond Finance
 - "Bitcoin 3.0 is blockchain applications beyond currency, finance, and markets, particularly in the areas of government, health, science, literacy, culture, and art." - Melanie Swan
- Example
 - Decentralized Voting Application (Follow My Vote)

Follow My Vote



- Problem of E-Voting
 - How to vote remotely, while being able to verify your vote and keeping anonymity?
- Blockchain-based solution
 - Remote voting via internet / Real-time change
 - Get your voting token without revealing identity
 - Vote anonymously
 - Verify that the vote was registered as cast

Decentralized Consensus



Organizational Entities



- Blockchain technology makes a whole new breed of organizational entities possible
 - DAC - (D. Autonomous Company)
 - DAPP - (D. Application)
 - DAP - (D. Autonomous Platform)
 - DAO - (D. Autonomous Organization)
 - DAS - (D. Autonomous Society)

Decentralized Autonomous.. Company



- What is Decentralization?
 - To distribute the powers or functions of (a central authority) over a less concentrated area.
- What is Autonomy?
 - Self-governance: independence; subject to its own laws only.
- What is Company?
 - A number of persons united or incorporated for joint action, especially for business.

Analogy



- Slot Machine
 - Centralized
 - Autonomous
 - Company (Business)
 - Costs
 - Income
 - Profit
- Decentralize it with blockchain technology!



But How?



- Consensus Protocols
 - Proof of Work (PoW)
 - Proof of Stake (PoS)
 - Delegated Proof of Stake (DPoS)

Delegated Proof of Stake



- Decentralization of Power
- Stake Weighted Voting
- Roles
 - Committee
 - Witnesses
 - Workers



Delegated Proof of Stake 2



- Self-Funded Development
- Sources of income
 - Income from transaction fees
 - Income from capital appreciation
 - Share-issuance
- Spending on development
 - Workers
 - Witnesses

Example 1: BitShares Exchange



- Decentralized
 - Nobody is in control of the BitShares Platform
- Autonomous
 - The BitShares platform is Self-Governed
 - Delegated Proof of Stake
- Company
 - Income from fees
 - Costs of Witnessess and Workers

Example 2: PeerTracks



- Decentralized
 - Nobody is in control of the Muse Platform
- Autonomous
 - The MUSE platform is Self-Governed
 - Delegated Proof of Stake
- Company
 - Income from fees
 - Costs of Witnesses and Workers

Society on a blockchain



Image: Scott Rosenberg

Humans - What do we want?



- Basic Rights
 - Freedom of Speech
 - Freedom of Association
 - Privacy & Protection from malicious actors
- A better tomorrow
 - Same quality of life or better
 - New governance model
 - New business paradigm
- Build something better than what we have

Building The Future



- Internet-based Societies
 - Geographically unbound
 - Freedom of association
- Cryptography and cryptocurrencies
 - Freedom of communication
 - Economic freedom
 - Privacy and Anonymity
- The rest we need to specify and build

Specific Requirements



- Identity
- Life
 - Survival and health
 - Security
- Prosperity
 - Property
 - Economic efficiency
 - Science, technology and education



Identity

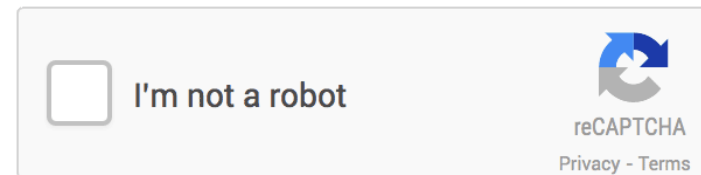


Image: Wikimedia commons

Types of Identity



- Traditional Identity
 - Name
 - Address
 - Citizenship
 - Birth information
 - Parents
 - Biometric Data
- Proof-Of-Human
 - Captcha etc.



Types of Identity 2



- Proof-Of-Individual
 - One sign-up per human
 - Exclusivity (competing associations)
 - Requires Deterministic Proof
- Pseudonym
 - Reputation based
 - Character or Role
- Intelligent Machine?

Components to Identity



- Entity to be identified
 - Human, AI or smart item
- Virtual Presence
 - In-game Character, Pseudonym
 - Legal Person
- Identity Verification
 - Password (weak)
 - Network of Trust (Web-Of-Trust)
 - DNA and one-way cryptography

Associated Properties



- Information
 - Name or nickname
 - Real or virtual address
 - Various other information
- Rights
 - Basic Income
 - Voting Rights
- Property
 - Money
 - Real or Virtual land

Blockchain Identity



- NameID
 - Pseudonym
 - Namecoin + OpenID
- ShoCard
 - Traditional Identity
 - Cryptography-based ID card
 - Secured by Bitcoin

Blockchain Identity 2



- Identabit
 - Financial Blockchain with Identity Component
 - Based on DPOS (BitShares) technology
 - AML/CTF reporting for exchanges
 - Privacy for individual users

Life

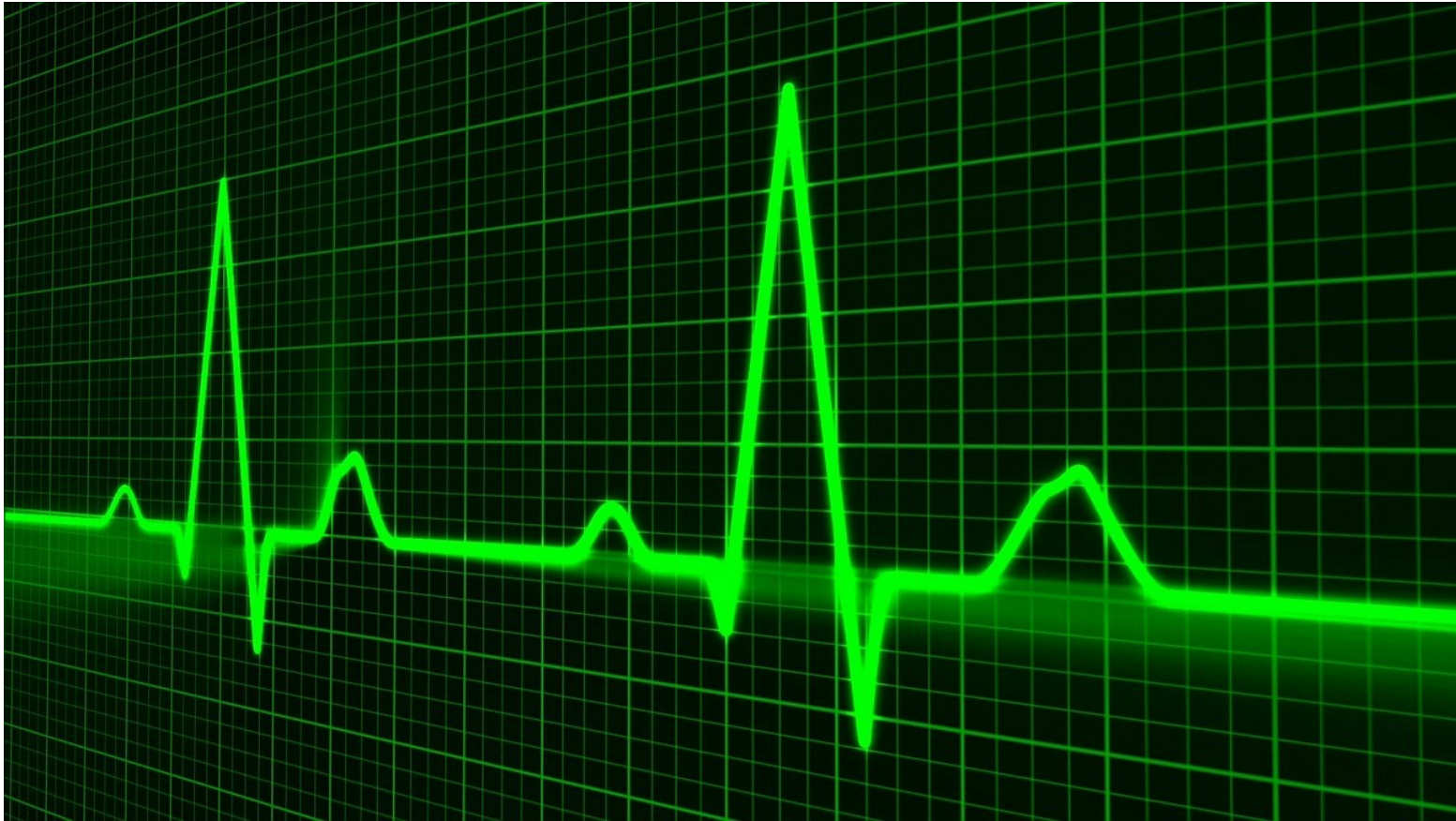


Image: Pixabay

Surviving the night



- Food
 - Food production and distribution
 - Value transfer between producer and customer
 - openfoodnetwork.org
- Shelter
 - Land
 - Property
- No money – charity?



Basic Income



- Will it appear first on a blockchain?
- Identity combined with cryptocurrency
 - E.g. DPOS gives users control of inflation
 - Genuine users bring value to an ecosystem
 - Now we can give value back to the user
 - Requires Proof-Of-Individual, Proof-Of-Effort, Proof-Of-Attention or similar to avoid exploitation
 - Voluntary socialism constructed in an anarcho-capitalist ecosystem

Basic Income Projects



- Frontier concept
 - No live projects yet
 - Negative associations to socialism and coercion
- basicincome.co
 - DApp – Decentralized Application
 - Based on BitNation

Healthcare



- Blockchain health society funding
 - Direct Funding
 - Community Health Insurance
- DIY healthcare
 - Wikipedia for Healthcare?
- Strongly connected to Science
 - Automation, reduce need for doctors
 - Crowdfunding Research on blockchain
 - Blockchain incentives for medicinal research



Security



- Crowdfunded "neighborhood watch"
- Armies of vigilantes (BitNation)
- Sensitive topic, governments' turf



Image: Internet Defense League

Prosperity



Image: Pixabay

Property and Money



- Cryptocurrencies
- Financial Instruments
- Smart Contracts
- Land registration and deeds
- Proof-of-ownership
- Proof-of-existence

Science, Technology and Education



- Research is generally funded by the public
 - Forced taxes
 - Politically controlled research?
- Crowdfunding research is a good idea!
 - The will of the people perfectly represented
 - Communities or companies can fund the research they want, instead of lobbying politicians
 - Renewal of Academia

Governance



- Traditional Representative Democracy
- New Democratic Tools
 - FollowMyVote
 - Stake-weighted voting (BitShares)
- Holacracy
 - Distributed Governance
 - Self-organizing teams
 - Bottom-up instead of top-down
 - BitNation

Funding Human Achievements



- How will we explore our solar system?
- How will we build new worlds?
- How will we explore the frontiers of science?
- How will we discover the mysteries of our past?
- If our efforts are restrained by power-hungry politicians and war-mongering armies...
- Soon we can, with the Internet of Money

IF SKY IS
THE
LIMIT,
THEN GO
THERE.



BitSpace



- BitSpace.no
 - Group Focused on Cryptocurrency Applications
 - Building the Future with Blockchain technology
 - Follow My Vote
- BitGate
 - Gateway to the BitShares Exchange
 - Trade Cryptocurrencies, Equities, IOUs, Assets, Tokens, and SmartCoins