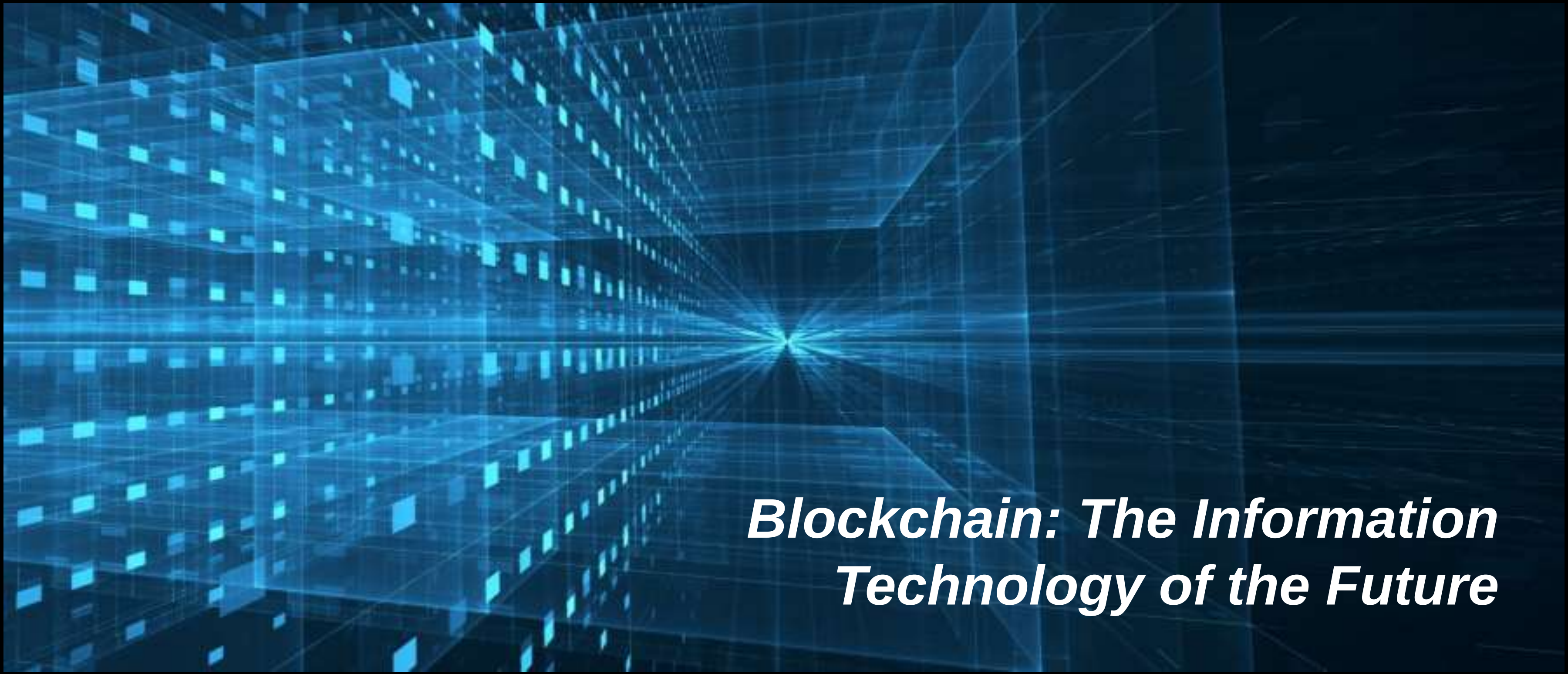


Blockchain: The Information Technology of the Future

October 1, 2014

Bitcoin Meetup

Slides: http://slideshare.net/LaBlogga

Melanie Swan
melanie@BlockchainStudies.org
www.BlockchainStudies.org

Institute for Blockchain Studies

SINGULARITY UNIVERSITY

What is the Blockchain?

We should think about the blockchain as another class of thing like the Internet – a comprehensive information technology with tiered technical levels and multiple classes of applications for any form of asset registry, inventory, and exchange, including every area of finance, economics, and money; hard assets (physical property); and intangible assets (votes, ideas, reputation, intention, health data, information, etc.)

– Melanie Swan, Founder, Institute for Blockchain Studies

New VC investment cycle: Blockchain Tech

“The blockchain is the core innovation,”
Marc Andreessen, CoinSummit (Mar 2014)

“We want a whole sequence of companies: digital title, digital media assets, digital stocks and bonds, digital crowdfunding, digital insurance. If you have online trust like the blockchain provides, you can reinvent field after field after field.”

http://www.bloomberg.com/news/2014-03-28/bitcoin-2-0-shows-technology-evolving-beyond-use-as-money.html

About Melanie Swan

Wharton
UNIVERSITY of PENNSYLVANIA

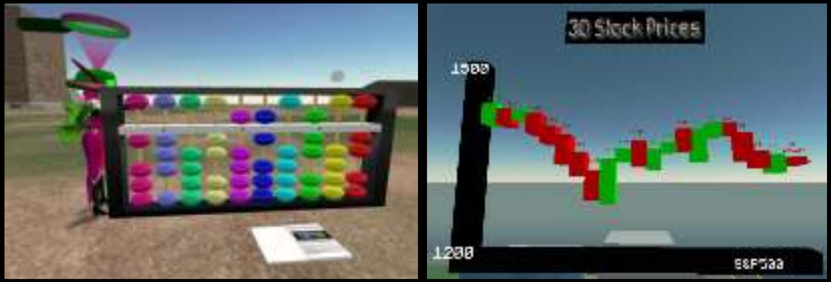
J.P.Morgan

Fidelity
INVESTMENTS

Traditional Background

SINGULARITY
UNIVERSITY

Prediction Markets
Quantitative Methods



New market startups:
Grouppurchase
Virtual World Valuation

Institute for
Blockchain Studies

Blockchain Futures

http://www.slideshare.net/lablogga/singularity-university-live-prediction-markets-simulation-big-data-indicators
http://www.slideshare.net/lablogga/virtual-worlds-economy

Agenda for Blockchain Futures

- Blockchain Industry Status
- Bitcoin Overlay Protocols (Mastercoin, Counterparty)
- Next-gen Bitcoin 2.0 Platform: Ethereum

Based on information synthesized from Internet resources including cryptocurrency expert Andreas M. Antonopoulos and Ethereum project members (Vitalik Buterin, Gavin Wood, Stephan Tual)

Blockchain Industry Status

- Bitcoin
  - Protocol is ossifying (to be stabilized w/in 2 years for 30 years)
  - Harder to make any changes: 5 constituencies for consensus[1]
  - Impossible for any new alt.coins to get network effect traction
  - BIP0032: hierarchical deterministic wallet trees, etc.
- Solution 1:
  - Overlay Protocols (Mastercoin, Counterparty)
  - Innovation moves up-stack: ‘http/smtp to Bitcoin’s TCP/IP’
- Solution 2:
  - New Foundational Protocol (Next-gen Bitcoin 2.0 Platforms): Turing-complete platforms like Ethereum (can run any coin)
  - ‘A new and improved TCP/IP transport protocol’

TREZOR hardware wallet

[1] *Miners (independent & pools), merchant processing gateways, web wallet companies (Blockchain), exchanges (Coinbase, Bitstamp), users, hardware manufacturer s (TREZOR)*

Solution 1: Bitcoin Overlay Protocols

- Mastercoin: financial derivatives
- Colored Coins: issue your own currency on the bitcoin network (by adding metadata to Bitcoin transaction)
- Counterparty: a decentralized exchange between alt.currencies
- Ripple: payment, exchange, and remittance network
  - Direct fund transfers and foreign exchange transactions between institutions; consensus-based ledger
- BitShares: crypto-equity decentralized company stock share exchange
- Namecoin: decentralized domain name registry
- Blockstream: credits (sidechain, treechain,privatechain)

But still, Bitcoin Protocol shortcomings…

- Applications
  - Bitcoin is only for currency
- Functionality and security
  - Anonymity, fungibility, scalability
  - Irreversible transactions, one asset per token, no multisignature
- Complete Step 3 of Satoshi Nakamoto’s original plan
  1. Decentralized database, put assets into a transparent ledger, everyone has a copy
  2. Transaction system to move value between parties without third party interaction
  3. Robust scripting system; instead of just sending currency, send contracts, smart property, anything; requires Turing completeness, solving blockchain bloat

Solution 2: Ethereum

- A decentralized publishing platform featuring stateful user-created digital contracts and a Turing-complete contract programming language
  - Chain implementation & contracts with shared mining
- Ether, the underlying network unit, as payment to execute contracts as a workaround to the Halting Problem
- A network for powering Ethereum-based contracts (not exclusively for transacting monetary value)
  - Open-ended contracts to securely execute services including: voting systems, domain name registries, financial exchanges, crowdfunding platforms, company governance, self-enforcing contracts and agreements, intellectual property, smart property, and distributed autonomous organizations (DAOs)

http://en.wikipedia.org/wiki/Ethereum

What is Ethereum?

- Basic infrastructure, standard, foundation, platform
  - Turing-complete scripting language
  - One-click install dev tools (mining, open transactions, wallet) like iOS and Android apps
- ‘General-purpose’ cryptocurrency network
  - Blockchain + cryptographically-secure transactions platform
  - Create any custom specialized applications on top
- A secure decentralized generalized transaction ledger
- Next-generation cryptocurrency network

Source: Wood, Gavin. Ethereum: A Secure Decentralized Generalized Transaction Ledger: Proof of Concept VI. http://www.gavwood.com/Paper.pdf

$18.4m USD Ethereum Fundraising 7/2014

- Initial Sale
  - (Sliding) 2,000 ether to 1 bitcoin or $620
  - 60m Ether (ETH) sold ($1 USD ~ 3.25 ETH)
- Dev offices in Berlin (expanding to ~20)
- Ongoing Macroeconomic Policy
  - Ether has build-in increase of overall money supply at fixed rate
  - 40% of the amount raised in the fundraiser will be the annual increase in money supply
- Ether subunits
  - Finney (10^{-3}), szabo (10^{-6}), shannon (10^{-9}), babbage (10^{-12})

Vitalik Buterin, Creator

Gavin Wood, Architect

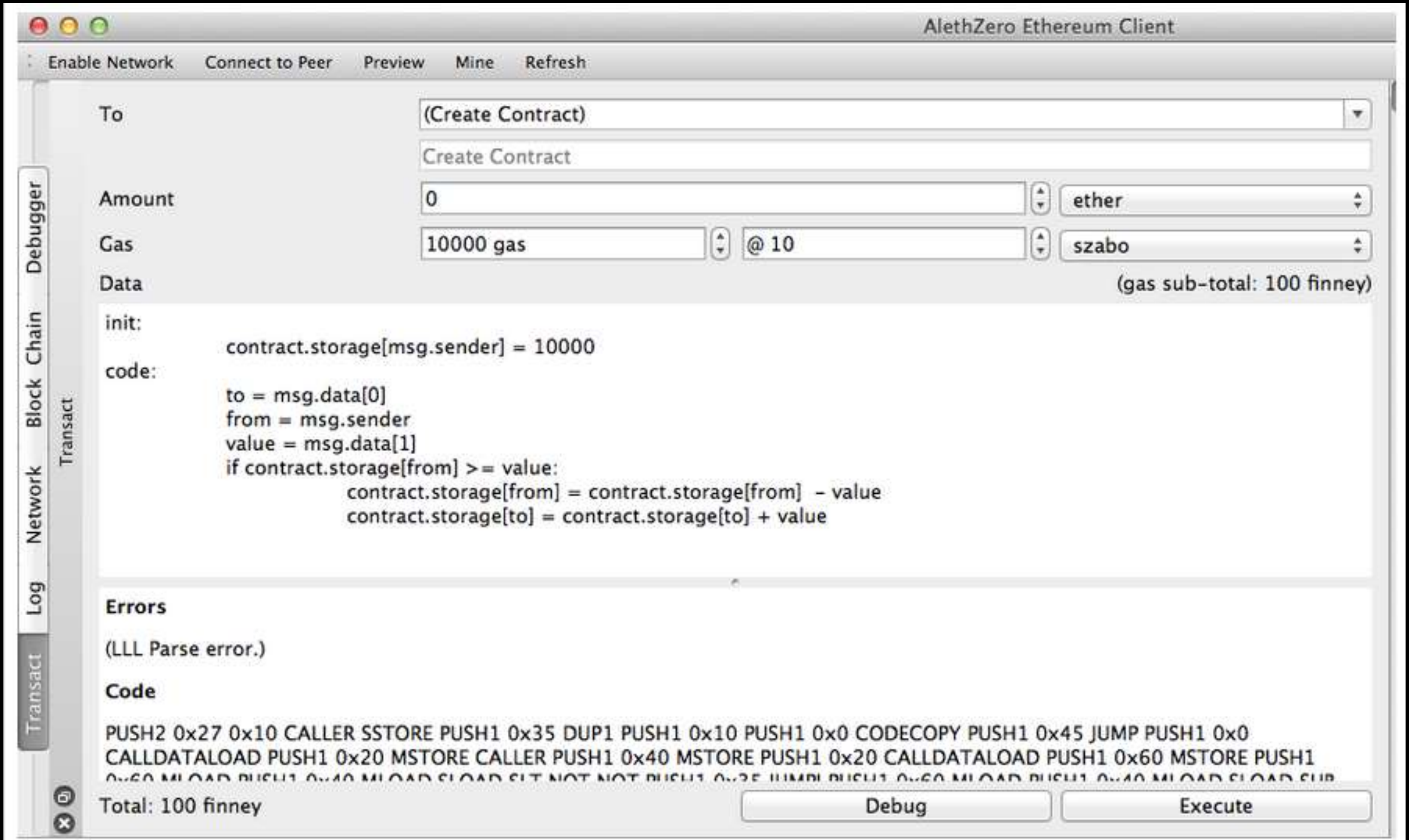
Stephan Tual, CCO

http://www.businessinsider.com/ethereum-launches-ether-2014-7

Smart Contracts: Programmable Money

- Multisignature (multiparty) escrows (~Bitrated 2.0)
- Financial exchanges
- Savings Accounts
- Domain name registries
- Voting systems
- Company governance
- Self-enforcing contracts and agreements
- Crowdfunding platforms, Prediction markets
- Smart property
- Intellectual property
- Nationstate constitution and bill of rights

Easy to Create Ethereum Contracts



To: (Create Contract)

Create Contract

Amount: 0 ether

Gas: 10000 gas @ 10 szabo

Data (gas sub-total: 100 finney)

```
init:
        contract.storage[msg.sender] = 10000
code:
        to = msg.data[0]
        from = msg.sender
        value = msg.data[1]
        if contract.storage[from] >= value:
                contract.storage[from] = contract.storage[from]  - value
                contract.storage[to] = contract.storage[to] + value
```

Errors

(LLL Parse error.)

Code

```
PUSH2 0x27 0x10 CALLER SSTORE PUSH1 0x35 DUP1 PUSH1 0x10 PUSH1 0x0 CODECOPY PUSH1 0x45 JUMP PUSH1 0x0
CALLDATALOAD PUSH1 0x20 MSTORE CALLER PUSH1 0x40 MSTORE PUSH1 0x20 CALLDATALOAD PUSH1 0x60 MSTORE PUSH1
0x60 MLOAD PUSH1 0x40 MLOAD SLOAD SLT NOT NOT PUSH1 0x35 JUMPI PUSH1 0x60 MLOAD PUSH1 0x40 MLOAD SLOAD SUB
```

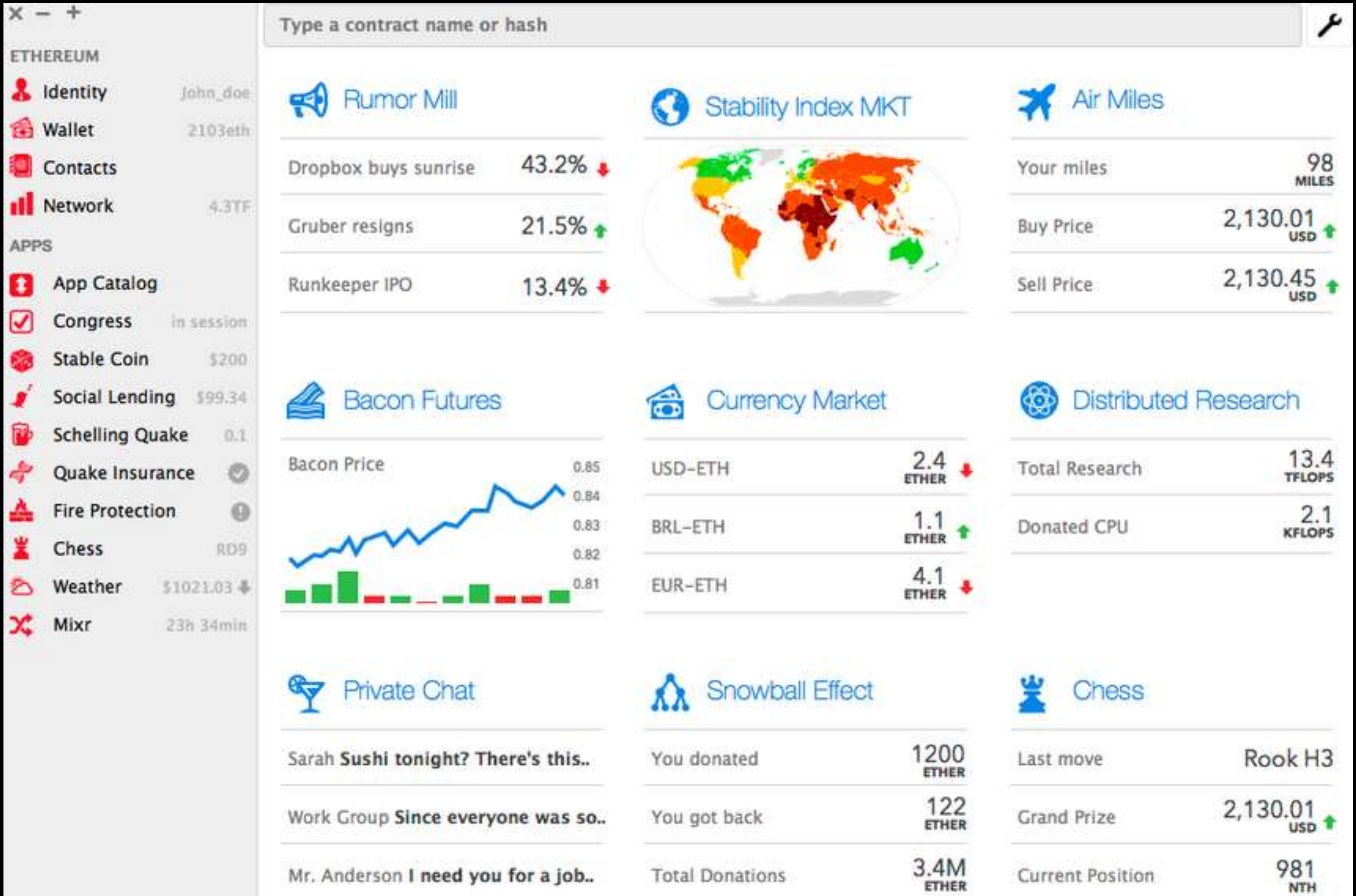
Total: 100 finney

http://forum.ethereum.org/discussion/1402/how-to-get-started-your-first-dapp-under-one-hour

Example: Smart Property

- Instead of trading coin, shares, trade/buy-sell assets
- Encode asset to the blockchain via unique key
- Trade cars on the blockchain through a decentralized exchange
- Entire used auto market trades via blockchain
- Blockchain becomes an inventory, tracking, and exchange mechanism for all hard assets

Ethererum Browser ‘Mist’ Mock-up



Type a contract name or hash

ETHEREUM

Identity	John_doe
Wallet	2103eth
Contacts	
Network	4.3TF

APPS

App Catalog	
Congress	in session
Stable Coin	$200
Social Lending	$99.34
Schelling Quake	0.1
Quake Insurance	✓
Fire Protection	!
Chess	RD9
Weather	$1021.03 ↓
Mixr	23h 34min

Rumor Mill

Dropbox buys sunrise	43.2% ↓
Gruber resigns	21.5% ↑
Runkeeper IPO	13.4% ↓

Stability Index MKT

Air Miles

Your miles	98 MILES
Buy Price	2,130.01 USD ↑
Sell Price	2,130.45 USD ↑

Bacon Futures

Bacon Price

Currency Market

USD–ETH	2.4 ETHER ↓
BRL–ETH	1.1 ETHER ↑
EUR–ETH	4.1 ETHER ↓

Distributed Research

Total Research	13.4 TFLOPS
Donated CPU	2.1 KFLOPS

Private Chat

Sarah **Sushi tonight? There's this..**

Work Group **Since everyone was so..**

Mr. Anderson **I need you for a job..**

Snowball Effect

You donated	1200 ETHER
You got back	122 ETHER
Total Donations	3.4M ETHER

Chess

Last move	Rook H3
Grand Prize	2,130.01 USD ↑
Current Position	981 NTH

http://forum.ethereum.org/discussion/1402/how-to-get-started-your-first-dapp-under-one-hour

The key benefit of Ethereum for the automated-economy is that it is a Turing-complete VM

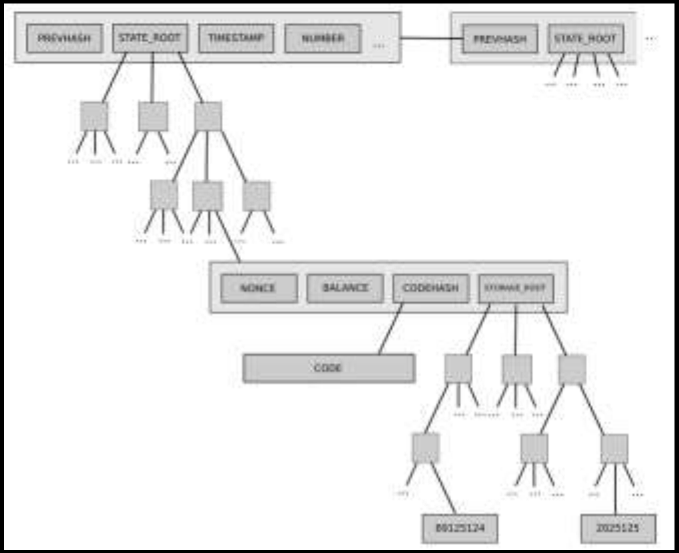
Ethereum Virtual Machine (EVM)

- The Ethereum blockchain is…
  - A blockchain with a built-in programming language
  - The decentralized, massively replicated database in which the current state of all accounts is stored
  - A consensus-based globally executed virtual machine
- The Ethereum Virtual Machine (EVM) handles internal state and computation
  - Large decentralized computer with millions of account objects
- Each account object
  - Has its own internal code
  - Contains a 32-byte key/value database called storage
  - Can call or send messages to other objects

https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial

Tech Specs
Accounts stored in a Patricia tree (like a Merkle tree)

- A root hash refers to the entire tree; tree contents cannot be modified without changing the root hash
- A miner produces a new block each minute with the latest transactions and the root hash of the Patricia tree representing the new state



- 4-tuple stored per account
  - [account_nonce, ether_balance, code_hash, storage_root]
    - account_nonce: the number of transactions sent from the account (kept to prevent replay attacks)
    - ether_balance: the balance of the account
    - code_hash: the hash of the code if the account is a contract
    - storage_root: the root of another Patricia tree with the storage data

https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial

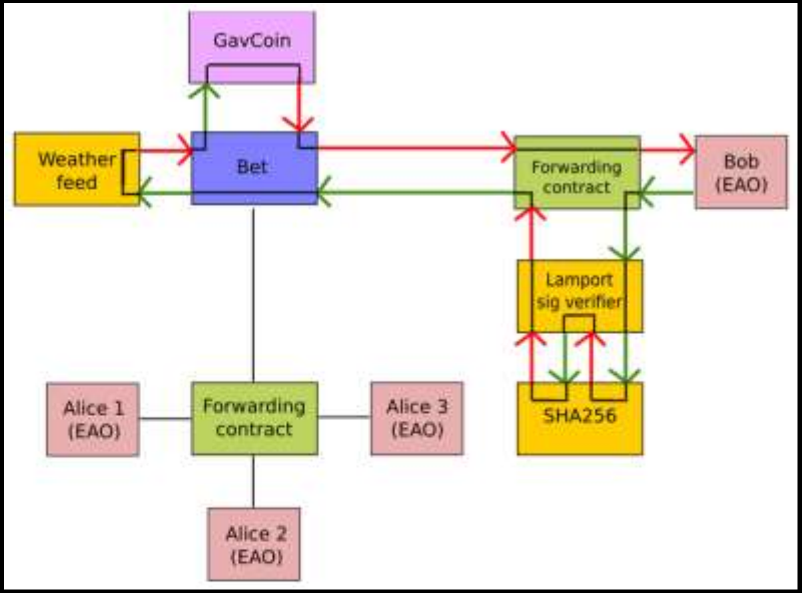
Ethereum Contract Processing

- Two account object types
  - Contract
  - EOA (externally owned account)
- Contract receives a message and runs the code
  - Ability to read/write to its own internal storage
  - Read the storage of the received message
  - Send messages to other contracts, and to itself
  - The contract is the code that executes the contract
- Contract can interact with the world outside the EVM
  - EOA (externally owned account) messages the contract
  - Transaction is sent signed by the EOA’s private key
  - Advanced: SchellingCoin Universal Data Feed for derivatives (minimal trust, two-step commitment protocol per round)

https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial
https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/

Ethereum Contract Example

- GavCoin weather bet between Bob and Alice
  - Automated EVM communications
  - Heterogeneous user security preferences
- A transaction is sent, triggering forwarding contract and EAO messaging
- GavCoin is stored as entries in the GavCoin contract's database
- The bet contract sees the temperature and messages the GavCoin contract to payout (object autonomy)



EAO (externally owned account)

https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial

EVM Operation / “Gas” Fees

- Ethereum consensus model
  - Each operation executed in the EVM is simultaneously executed by every full node
  - Benefit: any contract on the EVM can call any other contract at almost zero cost
  - Cost: computational steps on the EVM are very expensive
- Transaction fee and block operation limit
  - The Ethereum protocol charges a market-based fee in ether per computational step (prevent deliberate attacks and abuse)
  - Floating limit on the number of operations contained in a block
  - Even miners who can afford to include transactions at close to no cost are forced to charge a fee commensurate with the cost of the transaction to the entire network

https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial

Smart Contract-DOA/DAC Progression

- Smart Contract
  - Transaction protocol that executes the terms of a contract
  - Smart property: property whose ownership is controlled via the blockchain using contracts (examples: cars, phones, houses)
- Ðapp (Decentralized Application)
  - Contract plus graphical interface for contract execution
    - JavaScript API ‘eth object’ interacts with Ethereum blockchain
- DAO (Decentralized Autonomous Organization)
  - Self-enforcing smart contract (group of contracts) on a cryptographic blockchain, multiparty complexity
  - (Like remittances) avoid local business jurisdictional costs
  - Own Ethereum address (key) and balance, send and receive transactions, EtherScript scripts can modify their own code

http://www.slideshare.net/mids106/ethereum-decentralized-autonomous-organizations
Egalitarian DAO contract explained: https://www.youtube.com/watch?v=Q_gxDytSvuY

Decentralized Autonomous Corporations

- DACs, automated markets, and tradenets
  - Fully-autonomous business entity
  - Autonomous property, example: self-owned, self-driving car

Vehicles use the tradenet to find customers and bid for road space

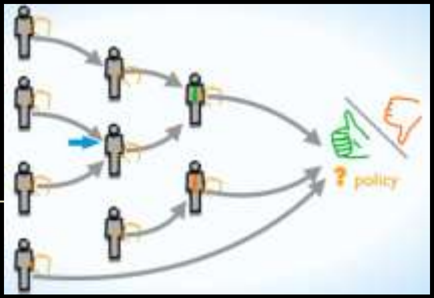
- Example:
- Storj.io (decentralized cloud storage) - Gregory Maxwell
  - MetaDisk: upload your data to the Storj network
  - DriveShare: earn money by being a part of the Storj network
  - Doesn’t work on bitcoin due to scripting language limitations

http://www.slideshare.net/mikehearn/future-of-money-26663148, http://storj.io/
http://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/

Tech Specs
State Machine, Languages, and Code

- Current Release
  - Proof of concept build - PoC5, GitHub release on July 22, 2014 with the launch of the Ether pre-sale
- EVM computation via a stack-based bytecode language
  - Bitcoin Script, traditional assembly and Lisp
  - A program in EVM is a sequence of opcodes
- Contract programming with high-level languages
  - LLL, serpent, Mutan compiles into EVM
  - Create contracts by sending the transaction containing the EVM bytecode
- One-click installation for everything (like mobile apps)
  - Wallet, Open Transactions, Ripple

Classes of Ethereum Applications

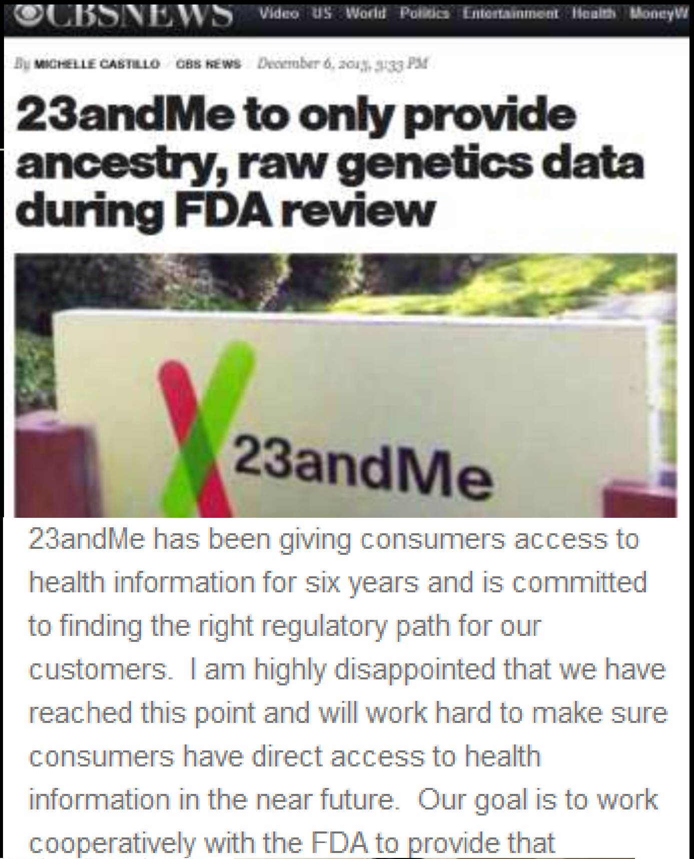


- Finance and Economics
  - BitCloud (decentralized escrow), OpenLibernet (open comms)
  - Debt market, futures (derivatives), savings
- Voting (futarchy, Liquid Democracy)
- Resource exchange: eBay, Amazon, Uber, AirBnB
  - Functions: authentication, validation, escrow, delivery
  - P2P Package Courier Service (notified as you leave location)
- Real-time cost-based data center storage swapping
- Loyalty, everyone’s own currency: JefCoin

- Automated markets, tradenets
  - Economics: transactions/contracts pay-on-board network Ether
- GBI (Guaranteed Basic Income) – Switzerland freicoin

One use for Ethereum
Blockchain Genomics

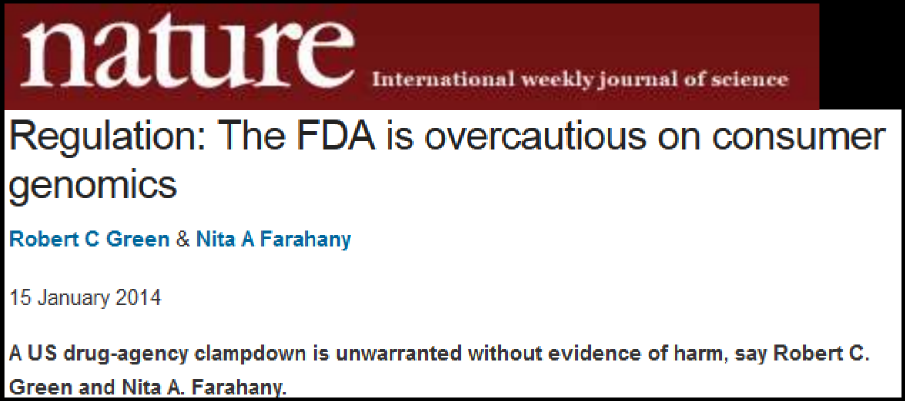
- Jurisdictional regulation prevents individuals from having access to their own genetic data



By MICHELLE CASTILLO / CBS NEWS / December 6, 2013, 3:33 PM

23andMe to only provide ancestry, raw genetics data during FDA review

23andMe has been giving consumers access to health information for six years and is committed to finding the right regulatory path for our customers. I am highly disappointed that we have reached this point and will work hard to make sure consumers have direct access to health information in the near future. Our goal is to work cooperatively with the FDA to provide that



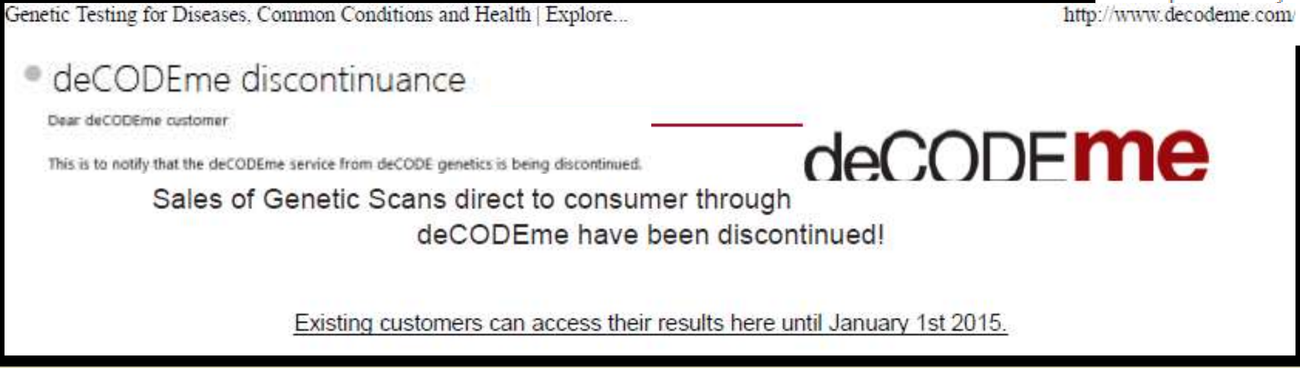
nature International weekly journal of science

Regulation: The FDA is overcautious on consumer genomics

Robert C Green & Nita A Farahany

15 January 2014

A US drug-agency clampdown is unwarranted without evidence of harm, say Robert C. Green and Nita A. Farahany.



Genetic Testing for Diseases, Common Conditions and Health | Explore... http://www.decodeme.com/

- deCODEme discontinuance

Dear deCODEme customer

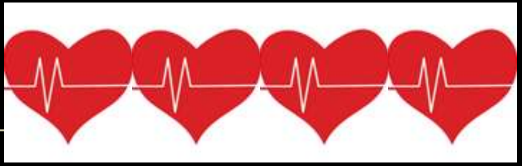
This is to notify that the deCODEme service from deCODE genetics is being discontinued.

Sales of Genetic Scans direct to consumer through deCODEme have been discontinued!

Existing customers can access their results here until January 1st 2015.

http://genomesunzipped.org/2011/03/people-have-a-right-to-access-their-own-genetic-information.php

Alt.apps: Blockchain Health



- Using blockchain tech for health-related applications

1. Personal Health Record Storage
   - Personal health records stored and administered via blockchain
   - Users key-permission doctors and other parties into records
2. Health Research Commons
   - Aggregated personal medical records, quantified self data commons (DNA.bits)
3. Health Document Notary Services
   - Proof-of-insurance, test results, prescriptions, status, condition, treatment, physician referrals
4. Doctor Vendor RFP Services
   - (Like Uber drivers) doctors and health practices bid to supply medical services; automated bidding via tradenets

http://futurememes.blogspot.fr/2014/09/blockchain-health-remunerative-health.html

Fitbit is a demurrage (action-inciting) health currency

Demurrage Blockchain Health

- Demurrage currency: built-in mechanism for spend/action-taking
  - Freicoin: Switzerland GBI (Guaranteed Basic Income)
  - GBHA (Guaranteed Basic Health Initiative): paid out and payable in HealthCoin; HSA (Health Savings Account) 2.0
  - Fitbit and smartwatch are demurrage health currencies
- Health itself as a demurrage currency, a continually auto-redistributing commodity among synapses, cells, humans; body and brain as a DAO/DAC AI
- Concept: demurrage resource-allocation + Đapp
  - Automatic redistribution of any commodity within a system (brain or mindfile (potentiation, optogenetic stimulation)), body (‘health’ (oxygen, waste removal nanobots, circulating lab-on-chips)), work team (ideas), society (liberty)

Alt.apps: Blockchain Futures

- Any venue for decentralized contracts (Đapp)
- ‘Bitcoin MOOCs’ (‘Kickstarter for literacy’)
  - Like remittances, blockchain-improved aid, microcredit, development economics 2.0
  - Write Ethereum Literacy Contracts to emerging market peers
    - Reading, Technical, Agricultural, Vocational Literacy
  - New implementation of education in the blockchain

- Blockchains as a public good
  - Wikileaks, ICANN, Wikipedia, Genomics
  - Uplifted to cloud from jurisdiction

Alt.apps: Blockchain Futures

- Community supercomputing time
  - Blockchain tech as resource allocation for science efforts
  - Funding markets like crypto-equity and crowdfunding for ***any*** resource
- Reputation systems (OpenBazaar), insurance (SchellingQuake), Key recovery (wallet key protection)
- Blockchain GAAP: valuation, amortization, retirement
- Intangible asset encoding, tracking, and trade
  - Attention, intention, reputation, health, ideas
- Cryptoledger, financial cryptography, consensus-based ledger: revolutionizing concept for traditional institutions and startups in finance and beyond

Ethereum: Vitalik 9/14 Silicon Valley update

- Key progress: proof of stake
  - Custody mining, hybrid proof-of-stake proof-of-work, Slasher, TenderMint, dbus
- Decentralized application architecture
  - Ethereum: account registry
  - Whisper: generalized P2P messaging (decentralized Twitter)
  - Swarm: off-chain P2P data storage (images)
- Dev priorities: fully decentralized Internet Ðapps
  - Proof of Concept 6 (?) – consensus algorithm
  - Ethereum 1.0 core, optimization, security, virtual machine
  - UI, mobile client, DevTools, SchellingCoin (decentralized oracle)

Tech Specs
Ethereum JavaScript API: eth object

- Ethereum contract execution interface is implemented as an HTML/CSS/JS webpage
- JavaScript API, eth object interacts with the Ethereum blockchain, JavaScript API components:
  - eth.transact(from, ethervalue, to, data, gaslimit, gasprice) - sends a transaction to the desired address from the desired address (note: from must be a private key and to must be an address in hex form) with the desired parameters
  - (string).pad(n) - converts a number, encoded as a string, to binary form n bytes long
  - eth.gasPrice - returns the current gas price
  - eth.secretToAddress(key) - converts a private key into an address
  - eth.storageAt(acct, index) - returns the desired account's storage entry at the desired index
  - eth.key - the user's private key
  - eth.watch(acct, index, f) - calls f when the given storage entry of the given account changes
- Required: Ethereum client (not regular web browser)
- JavaScript API example: see source of link below

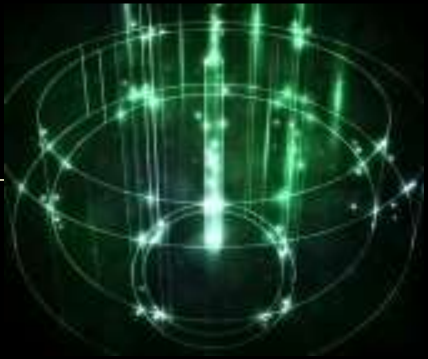
https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial

Tech Specs
Ethereum Code

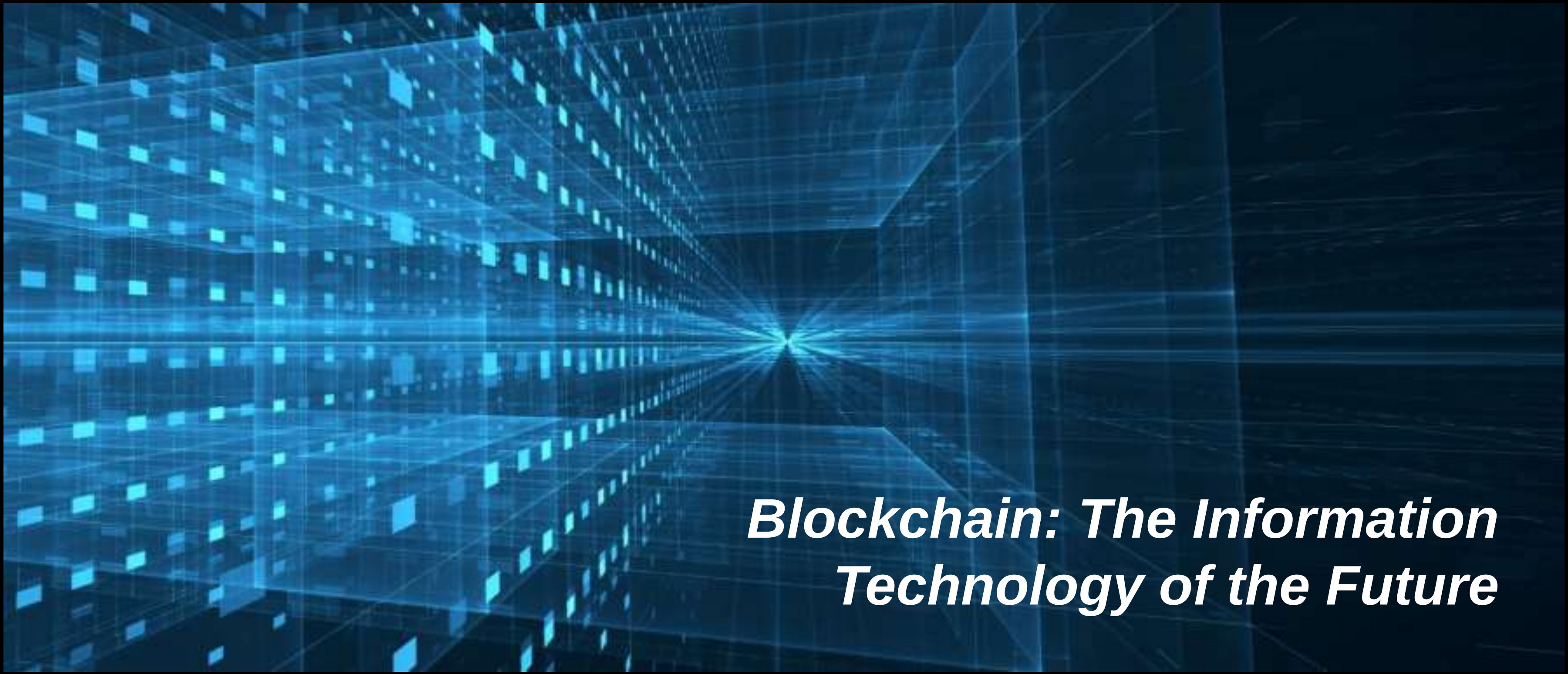
- Currently stable clients are available for PoC5 (Proof of Concept #5):
  - AlethZero (C++)
  - Ethereal (Go)
  - pyeth (Python)
- Bleeding edge PoC6 code can be cloned from their git repositories:
  - https://github.com/ethereum/cpp-ethereum/
  - https://github.com/ethereum/go-ethereum
  - https://github.com/ethereum/pyethereum

https://github.com/ethereum/wiki/wiki

Resources



- Ethereum
  - http://www.reddit.com/r/ethereum/
  - https://www.youtube.com/user/EtherCasts
  - https://github.com/ethereum/wiki/wiki
  - https://github.com/ethereum/wiki/wiki/Ethereum-Development-Tutorial
  - https://github.com/ethereum/wiki/wiki/White-Paper
  - http://gavwood.com/Paper.pdf (Yellow Paper)
- Bitcoin
  - Satoshi Nakamoto’s design for the blockchain (2008) https://bitcoin.org/bitcoin.pdf
- News
  - SATOSHI'S REVOLUTION: How The Creator Of Bitcoin May Have Stumbled Onto Something Much, Much Bigger http://www.businessinsider.com/the-future-of-the-blockchain-2014-4
  - The Future of Bitcoin and Math-Based Digital Currencies http://www.youtube.com/watch?v=Yg1JnbIS60g



Blockchain: The Information Technology of the Future

Thank You! Questions?

October 1, 2014

Bitcoin Meetup

Slides: http://slideshare.net/LaBlogga

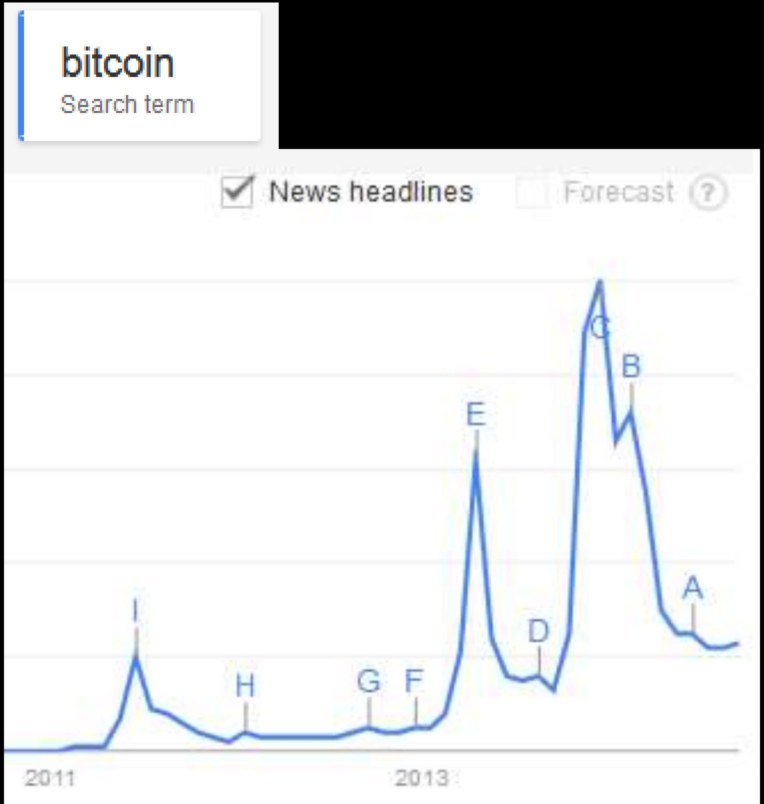
Melanie Swan
melanie@BlockchainStudies.org
www.BlockchainStudies.org

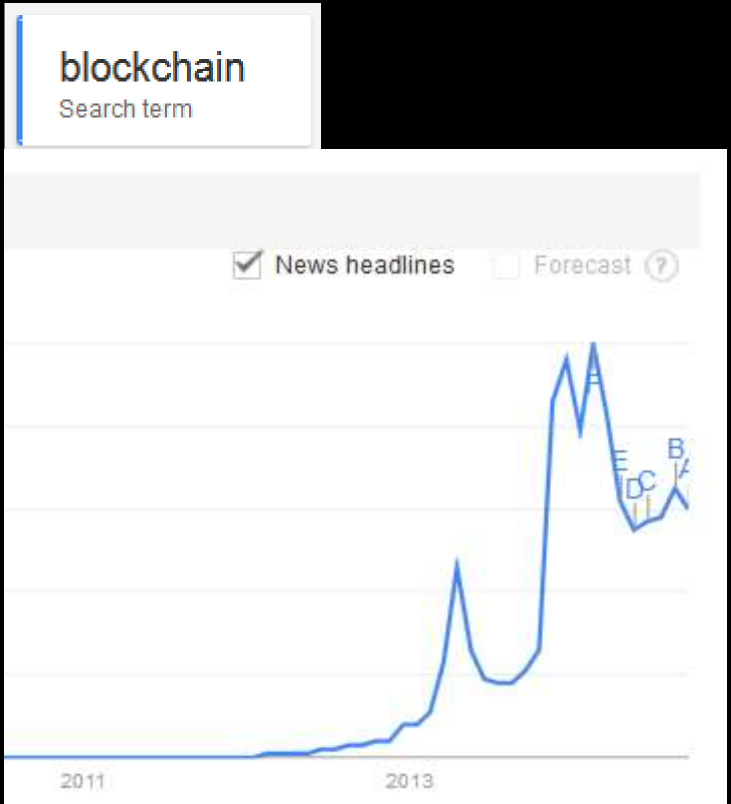
SINGULARITY UNIVERSITY

Institute for Blockchain Studies

Appendix: Bitcoin/Blockchain Background

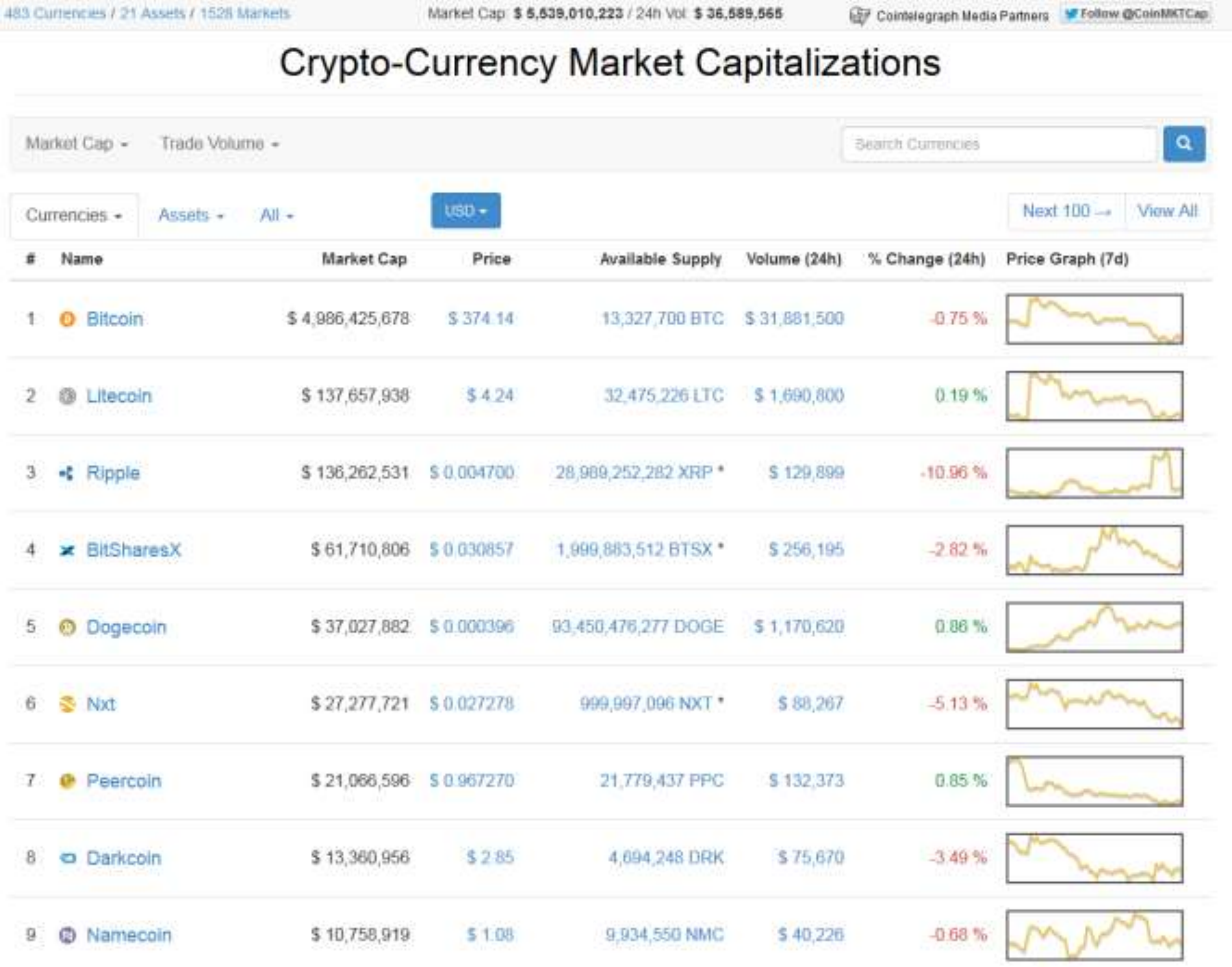
- *The New Economy…*





http://www.google.com/trends/explore#q=bitcoin

Cryptocurrency Market Cap Tracking



483 Currencies / 21 Assets / 1528 Markets   Market Cap: **$ 5,539,010,223** / 24h Vol: **$ 36,589,565**   Cointelegraph Media Partners   Follow @CoinMKTCap

Crypto-Currency Market Capitalizations

#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$ 4,986,425,678	$ 374.14	13,327,700 BTC	$ 31,881,500	-0.75 %	
2	Litecoin	$ 137,657,938	$ 4.24	32,475,226 LTC	$ 1,690,800	0.19 %	
3	Ripple	$ 136,262,531	$ 0.004700	28,989,252,282 XRP *	$ 129,899	-10.96 %	
4	BitSharesX	$ 61,710,806	$ 0.030857	1,999,883,512 BTSX *	$ 256,195	-2.82 %	
5	Dogecoin	$ 37,027,882	$ 0.000396	93,450,476,277 DOGE	$ 1,170,620	0.86 %	
6	Nxt	$ 27,277,721	$ 0.027278	999,997,096 NXT *	$ 88,267	-5.13 %	
7	Peercoin	$ 21,066,596	$ 0.967270	21,779,437 PPC	$ 132,373	0.85 %	
8	Darkcoin	$ 13,360,956	$ 2.85	4,694,248 DRK	$ 75,670	-3.49 %	
9	Namecoin	$ 10,758,919	$ 1.08	9,934,550 NMC	$ 40,226	-0.68 %	

https://coinmarketcap.com/

What is Bitcoin?

- Digital currency, payments system, decentralized ledger
- History: by combining BitTorrent technology (peer-to-peer file sharing) and public key cryptography a new form of currency was made possible
- Arose as a solution to the double-spend problem
  - Prior to bitcoin and the blockchain concept, a centralized third party had to issue and reconcile digital cash transactions to prevent the digital cash from being spent multiple times (digital cash, like an image attached to an email, can be copied infinite times like any digital cash)
- Implication: any transaction on the Web can be decentralized and stripped of a controlling authority

http://codinginmysleep.com/bitcoin-mining-in-plain-english/, https://github.com/ethereum/wiki/wiki/White-Paper
http://offtheblockchain.com/2014/02/22/read-the-original-satoshi-nakamoto-bitcoin-white-paper/

What is the blockchain?

- A ledger of all transactions owned and monitored by everyone and controlled by none
  - Like a giant interactive spreadsheet everyone has access to and updates to confirm that each digital credit is unique
- Literally blocks (of transactions) in a chain, a sequential ledger of bitcoin transactions
- What is a Digital Wallet? (it is not a wallet) Stores keys
- Bitcoin's public ledger (the blockchain) was started on January 3rd, 2009 at 18:15 UTC by Satoshi Nakamoto
  - First block is known as the genesis block
  - First transaction recorded in the first block was a single transaction paying the reward of 50 new bitcoins to its creator

Source: Wood, Gavin. Ethereum: A Secure Decentralized Generalized Transaction Ledger: Proof of Concept VI. http://www.gavwood.com/Paper.pdf

What is the blockchain?

- A concept
- A transaction database
- A decentralized public ledger
- A technology layer protocol like TCP/IP
- An information technology
- An asset administration tool
- Application areas
  - Finance and economics: payments, asset exchange
  - Exchange of all assets (physical and intangible)
- A registry, inventory, listing of all the world’s stuff

Economic Arguments for Bitcoin

- Banking services market: 5 billion individuals worldwide without access to banking, financial, credit services
- Remittances market: $4T global market 5-30% transaction fee, immediate funds transfer
- Payments market: 1-3% merchant transaction fee
- Successful examples indicate demand for digital payments: Starbucks mobile payment app

What is Bitcoin Mining?

- The process of adding transaction records to Bitcoin’s public ledger of past transactions (the blockchain)
- Confirms to the rest of the network that unique transactions have taken place
- Bitcoin nodes use the block chain to distinguish legitimate Bitcoin transactions from attempts to re-spend coins that have already been spent elsewhere
- Intentionally designed to be resource-intensive so that the number of blocks found each day by miners remains steady
- Individual blocks must contain a proof of work to be considered valid. This proof of work is verified by other Bitcoin nodes each time they receive a block. Bitcoin uses the hashcash proof-of-work function

http://codinginmysleep.com/bitcoin-mining-in-plain-english/