

BLOCKCHAINS 101

Decentralisation for developers

.....
.....
....; fíýz{.²zC,>
gv.a.È.Ã^ŠQ2:Y, a
K.^J) «_Iÿÿ...¬+ |
.....
.....
.....ÿÿÿÿM.ÿÿ..
..EThe Times 03/
Jan/2009 Chancellor on brink of
second bailout f
or banksÿÿÿÿ...ò.
*....CA.gŠý°þUH'
.gñ|q0..\"(à9.|
ybàê.aþ¶Iö¼?Lï8Ä
óU.å.Á.þ\8M÷º..w
ŠLp+kñ._¬....

GENESIS BLOCK

.....

A little backstory...

PRELUDE

- Internet
- Databases
 - SQL
 - NoSQL
 - Big data
- Cryptography
 - Hash trees
 - PGP
- Peer-to-peer networks
 - DHT
 - BitTorrent

“Governments are good at cutting off the heads of a centrally controlled networks like Napster, but pure P2P networks like Gnutella and Tor seem to be holding their own.

-Satoshi Nakamoto

BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM

- “chain of blocks”
 - immutable Merkle data trees
- Censorship-resistant
 - P2P communication
- Coordination
 - Byzantine General
 - Prisoner’s Dilemma
- Protocol governs compliance
 - Incentivised validators
 - Preventing tragedy of the commons

Bitcoin: A Peer-to-Peer Electronic Cash System

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

Abstract. A purely peer-to-peer version of electronic cash system where payments are sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, to ensure messages cannot be forged. The remaining 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 chain of timestamped transactions. The network timestamps transactions by hashing them into a 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 a proof 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 accept the chain, attacks become increasingly difficult, and as long as the network itself requires minimal structure, messages are able to spread through it at the speed of light. Nodes can leave and rejoin the network at will, taking with them their proof-of-work chain as proof of what happened while they were gone.

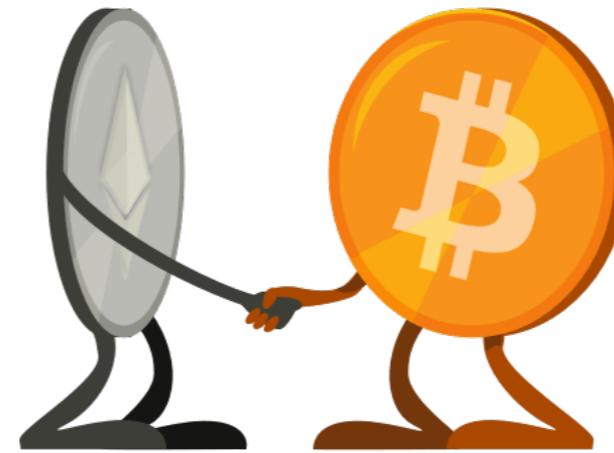
BEYOND BITCOIN

- Proliferation of “alts”
 - Litecoin / 2.5 block time
 - Dogecoin / fun
 - Darkcoin / private
- Not just value transfer
- Innovation in all industries
- Generalised state transition machine as “DApp platform”



BLOCKCHAIN PROJECTS

- Value
 - Bitcoin
 - DASH
- Processing
 - Ethereum
- Storage
 - Namecoin
 - IPFS
 - Maidsafe/Storj
 - BigchainDB
- Messaging
 - BitMessage



BDB

WUT!

Not only for buying drugs?



KEY FEATURES

- Immutable
 - Create Read ~~Update Delete~~
- Non-repudiable
 - Digital signatures
 - Sign & Verify
- Fault-tolerant
 - Censorship resistant
 - Partially-connected mesh resilience

BENEFITS

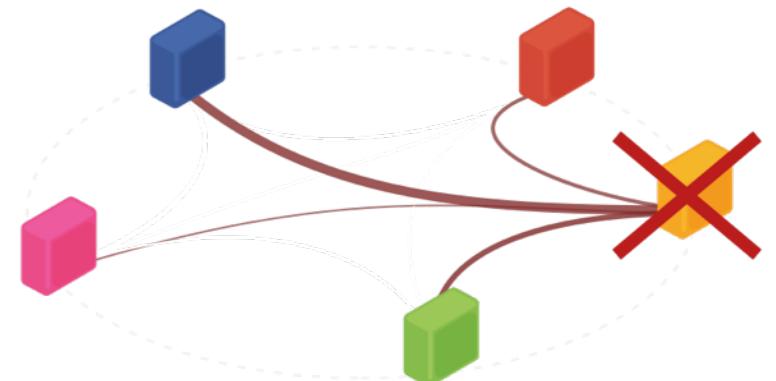
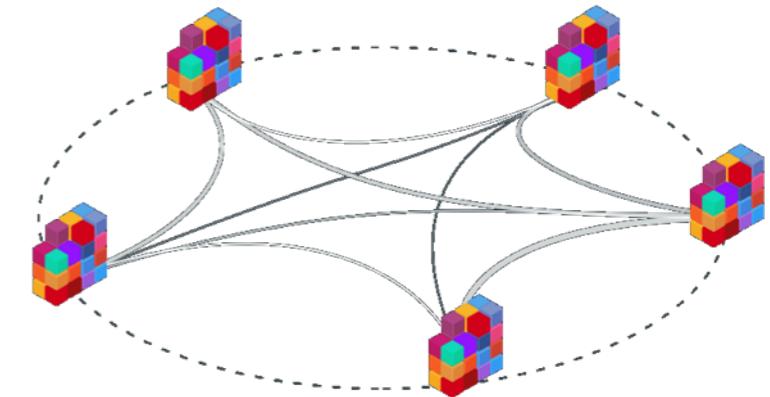
- Zero infrastructure
 - Scaling for free
 - Resilience for free
- Auditable
 - Triple-entry accounting
 - If you want it
- Jurisdiction
 - Estonia e-Residency
 - Everywhere/nowhere
- Censorship-resistant
 - State & corporate actors
 - Controversial ideas
- Identity built-in
 - Sharable reputation
 - No more passwords
- M2M transactions
 - Internet of things (IoT)
 - Microtransactions

CAVEATS

- External data
 - System does not know about outside world
 - Oracles
- Privacy
 - External now
 - Zero Knowledge later?
- Scalability
 - Increase transactions per second
 - Decrease time to finality

PUBLIC, PRIVATE, AND CONSORTIUM CHAINS

- Public chains are secured by pseudonymous validators
 - Proof of Work
 - Proof of Stake
- Consortium chains are secured by known entities
 - Require partial or full approval
 - May disregard unknown entities
- Private chains are... a fuzzy idea?
 - Privacy & fungibility with public chains unknown
 - Not clear if ledger is private or participants are exclusive





UGG WANT MORE

ETHEREUM ECOSYSTEM

- Ethereum Virtual Machine implemented in 7 languages!
 - Python, Java, C++, Haskell, Go, JavaScript, Rust
 - Partial support: .NET, Ruby
- JSON-RPC
 - Transport agnostic (HTTP, IPC, ...)
 - Suited for automated processes
- web3.js JavaScript library
 - Use JavaScript to interact with the blockchain DApp
 - No complicated crypto maths!

Console: Geth

```
> listProposal(42)
Proposal #42 Send 100 ether to "Bob" for "Website Design". 4 votes
for, 2 against, 6 hours remaining.
> MyVote = Against
> MyOwnDemocracy.vote.sendTransaction(42, MyVote, {from: me}) |
```

Ethereum Wallet

Wallet Overview

CONTRACT BASED WALLETS

Wallets are contracts that hold and secure ether. They can have multiple accounts as owners and keep a full log.

SAFE WALLET 5,051.96 usd 0x15c81792377438436...	MIST WALLET 3.60 usd 0x97e58c7d37cbalale...
--	--

+ ADD WALLET

ACCOUNTS

Accounts are password protected keys that control contracts.

BIG BOY 170.44 usd 0x70e3e34c0100b1e05...	POCKET MONEY 33.45 USD 0xd1220a0cf47c7b9be...	ACCOUNT 4 6.00 usd 0x6f773928e8c137426...
--	--	--

ACCOUNT 1 **ACCOUNT 2** **ACCOUNT 5**

```

contract token {
    mapping (address => uint) public coinBalanceOf;
    event CoinTransfer(address sender, address receiver, uint amount);

    /* Initializes contract with initial supply tokens to the user */
    function token(uint supply) {
        if (supply == 0) supply = 10000;
        coinBalanceOf[msg.sender] = supply;
    }

    /* Very simple trade function */
    function sendCoin(address receiver, uint amount) returns (bool success) {
        if (coinBalanceOf[msg.sender] < amount) return false;
        coinBalanceOf[msg.sender] -= amount;
        coinBalanceOf[receiver] += amount;
        CoinTransfer(msg.sender, receiver, amount);
        return true;
    }
}
```

New block created

Manage Scenario

Add Transaction... Add Block

GENESIS BLOCK Edit Starting Parameters

BLOCK 1

0x38f388fadf4a6a3... → 0x609a31a6... (Bob)

BLOCK 2

0x609a31a6... (Bob) → 0x38f388fadf4a6a3...

BLOCK 3

0x38f388fadf4a6a3... → token.token()

0x38f388fadf4a6a3... → token.sendCoin()

PENDING TRANSACTIONS

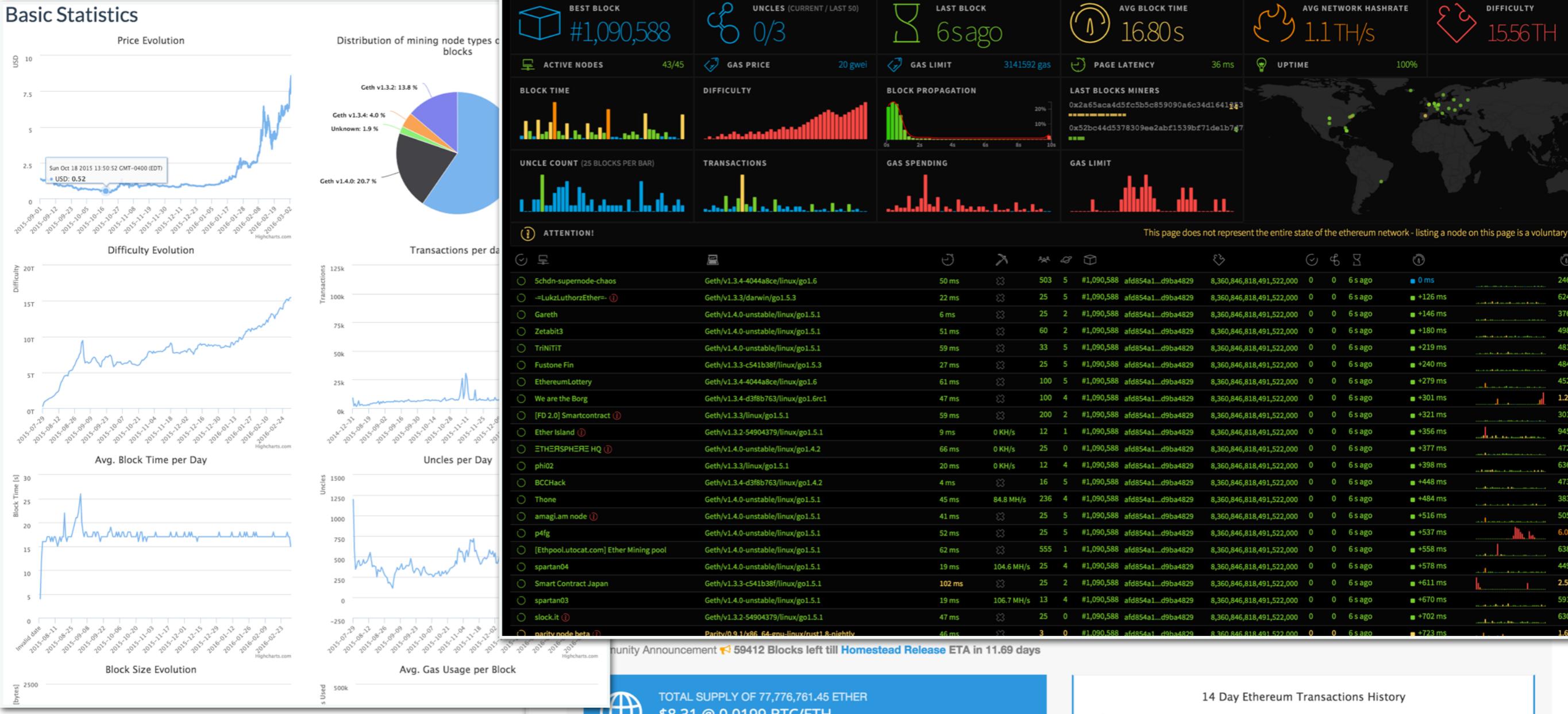
User Account

0x38f388fadf4a6a35c61c3f88194ec5ae162c8944 = 1 Met

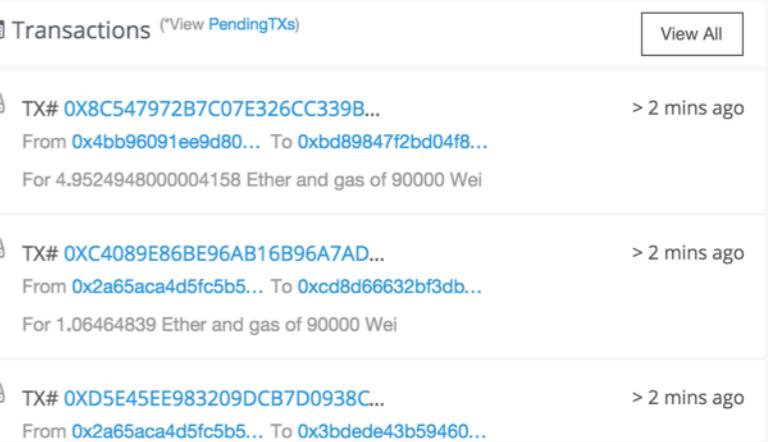
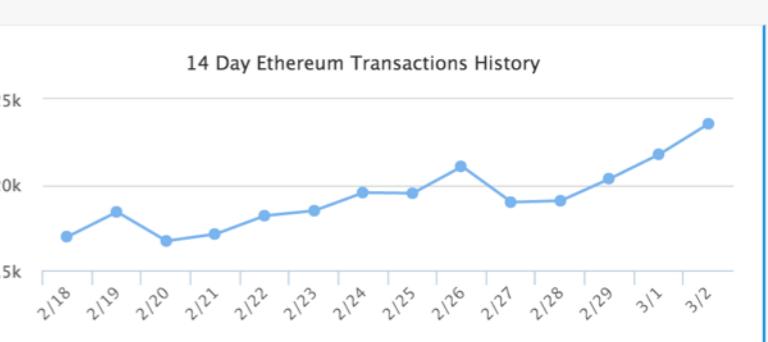
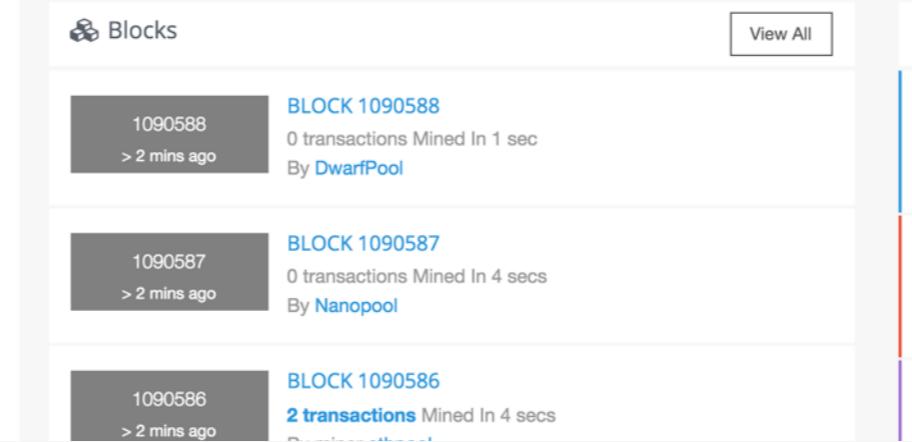
Contract Account

token - c069cb45291acafdd701e9341e7bf730255abbe1 - 0

- Geth Console
- Mix IDE
- Mist GUI



Community charts, graphs, and chain explorers



STATE OF THE DAPPS

 Search



Category	Name	Creator	Description	License	Status	Last Update	Notes
Game	Etheroll	James Britt	Ether dice game casino / gamble ether	proprietary  	Live	2016-03-02	A smart contract game
Game	Syng	Jarrad Hope	open source mobile ethereum client	GPL  	Working Prototype	2016-02-26	A decentralized mobile client
Game	EthereumWall	LPMitchell	Decentralized unmoderated public message board		Live	2016-02-25	A decentralized message board
Game	LETH	Inzhoop	LETH is the first hybrid mobile app to manage an Ethereum wallet	GPL 	Working Prototype	2016-02-25	A smart contract wallet
Protocol	EtherDoubler	Satoshi :)	The first doubler with verified contract	Unlicense  	Live	2016-02-17	Verifiable oracle
Protocol	Solether	Francesco 'makevoid' + KristinaB	Autonomous Electrical Energy Entities - Prototype +EntityConcept	Unlicense  	Working Prototype	2016-02-17	Ethereum energy market
Protocol	EtherAPIs	Péter Szilágyi & Jeffrey Wilcke	Micropayment platform for generic API calls	GPL  	Working Prototype	2016-02-16	A bridge between the Bitcoin blockchain & Ethereum smart contracts
Protocol	btcrelay	Joseph Chow	A bridge between the Bitcoin blockchain & Ethereum smart contracts	MIT 	Working Prototype	2016-02-15	Working Prototype
Storage	Icebox	Christian Lundkvist	A cold storage solution for Ether	MIT  	Live	2016-02-11	Venture capital
Storage	KingOfTheEtherThrone	Kieran Elby	Will make you a King or Queen, might grant you riches, and will immortalize your name.	proprietary  	Working Prototype	2016-02-06	Decentralized storage
Finance	Dactuary	Vignesh Sundaresan	Decentralized actuary built on Ethereum		Concept	2016-02-04	insurETH
Finance	insurETH	Thomas Bertani, Kristina Butkute, Francesco Canessa	P2P flight insurance	Apache 	Work in Progress	2016-01-21	Decentralized insurance
Contracts	dappsys	Nexus Dev	Solidity Contract System Framework	MIT 	Working Prototype	2016-01-02	Decentralized contracts
Contracts	Dapple	Nexus Dev	smart contract package manager and build tool	MIT 	Live	2016-01-02	Decentralized contracts
Cryptocurrency	Maker / Dai	Maker	Stable Cryptocurrency	MIT 	Work In Progress	2016-01-02	KYC-chain
Cryptocurrency	KYC-chain	Edmund John	Proof of KYC Requirements		Concept	2015-12-27	Decentralized currency
Decentralization	Decentralized Twitter						4G Capital Smart Contracts
Decentralization	etherforum						Decentralized forums
Decentralization	ethID						Decentralized identity
Decentralization	4G Capital Smart Contracts						Decentralized contracts

I CAN HAZ?

- ethereum.org
- ethereum.stackexchange.com
- reddit.com/r/ethereum
- ethstats.net
- etherchain.org
- etherscan.io



ETHEREUM



TAYLOR GERRING

DIRECTOR OF TECHNOLOGY
ETHEREUM FOUNDATION

@TaylorGerring
github.com/tgerring
blockchainconsulting.expert