



O'Reilly 2015

Ethereum

Introduction: Blockchain

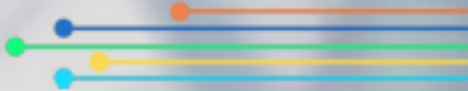


- Distributed consensus
- Bitcoin, Namecoin, Colored coins



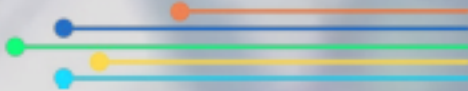
Ethereum

- Idea: blockchain + programming language
- Before: special-purpose blockchains
 - eg. calculator
- Now: general purpose blockchain
 - eg. Android - calculator is an app



Contracts

- Scripts that run in the cloud
- Contracts can:
 - Send money
 - Read/write to an internal database
 - Talk to other contracts



Contracts

- Contracts are:
 - Fully transparent/auditable
 - Guaranteed to execute
 - 10000x slower
- Excellent for business logic, not for heavy computing

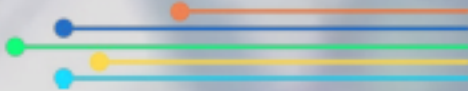
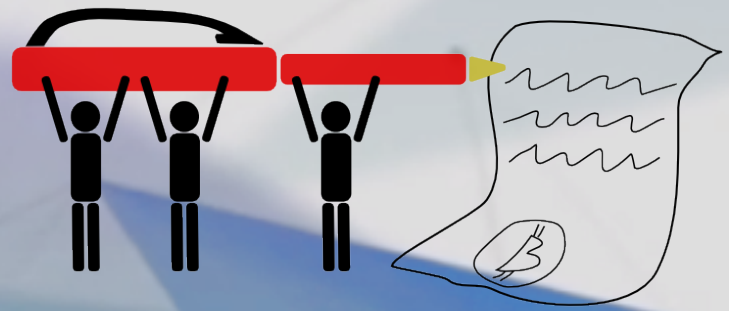


The Lego of Crypto-Finance

```
if contract caller = 0xf9f8456c7a03bb7556fa0476d8751589a7746357
then
  when 1st input = 0
  then
    in save slot 2nd input
    put 3rd input
  when 1st input = 1
  then spend 3rd input to 2nd input
else
  when 1st input = 2
  then
    when 3rd input ≤ data at save slot contract caller
    then spend 3rd input to 2nd input
```

Use cases

- Organizational
 - Contracts (B2B)
 - Asset permissions
 - Blockchain-based governance
 - Shareholder agreements
 - Prediction markets



Use cases

- Peer-to-peer Finance
 - Crowdfunding
 - Derivatives, hedging
 - Insurance
 - Mutual aid style: <http://bit.ly/econeng>



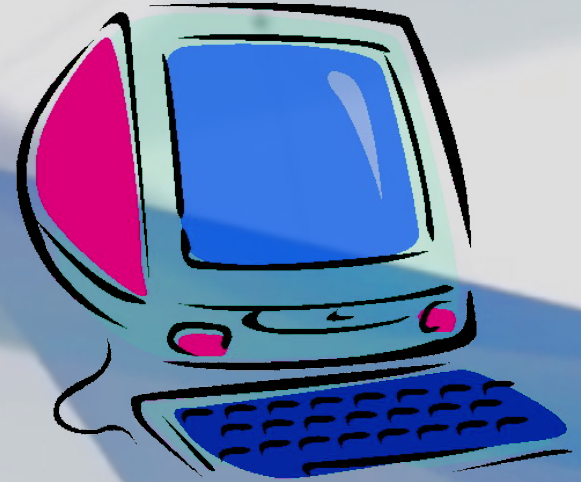
Use cases

- Consumer
 - Escrow
 - Personal asset storage
 - Smart property



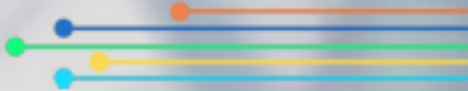
Use cases

- Computational resources
 - Cloud storage
 - “Permanent Web”
 - Cloud computing
 - Mesh networking
 - Solution to net neutrality?



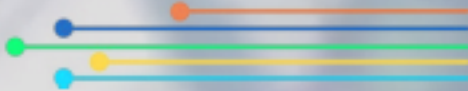
Beyond finance

- Name registries
- Non-currency tokens
- Whisper (messaging)
- Decentralized applications (DApps)



Decentralized Applications

- A DApp is:
 - Decentralized
 - Provides value to people
- “Server-side”: blockchain
 - Ethereum = “decentralized operating system”
- Client-side: Web



Building a DApp

1. Write contract code
 - Languages exist similar to Python, Go, JS, Lisp
 - EtherScripter (graphical environment)
2. Write in-browser code
 - HTML / CSS / JS, just like the “old web”
3. Release

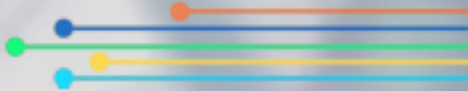


Example DApp

The screenshot shows the Mist wallet interface. On the left is a sidebar menu with the following items: **ETHEREUM** (Wallet: 0 Wei, Browser), **APPS** (JeffCoin: 0 JEF), and **DEBUG** (New transaction, Network, Information, Pending Transactions, JavaScript). At the bottom of the sidebar is a 'Start Mining' button (0 Wei). The main area is titled 'DApp URL' and contains a text input field with the value 'file:///home/vub/0.html'. Below this are three input fields: 'Account:' (empty), 'Limit:' (3000), and 'Value:' (empty). There are 'Set' and 'Withdraw' buttons. The bottom status bar shows '#12458 7/10'.

Benefits

1. Easy to write
2. Trustworthy
 - No need to trust you, can inspect the code
3. Transparent
4. No maintenance required
 - Even if you disappear, app lives on as long as it has users



Crowdfund

The screenshot shows the Mist Ethereum wallet interface. On the left is a sidebar menu with sections: ETHEREUM (Wallet: 0 Wei, Browser), APPS (JeffCoin: 0 JEF), and DEBUG (New transaction, Network, Information, Pending Transactions, JavaScript). The main area is titled 'Crowdfund' and contains the following fields and controls:

- DApp URL:
- Address:
- Username or address:
- Goal:
- Time limit (days):
- Info:

The purpose of this crowdfunding project is to collect funds to pay for the development of a blockchain-aware lock that could be put onto cars, bicycles, etc to allow the ability to use the property to transfer automatically with ownership. For more details see <http://smartcontractlocks.eth>
- Image: No file selected
-

At the bottom of the interface, there is a 'Start Mining' button (0 Wei) and a progress indicator showing 7/10.

Messaging

The screenshot shows the Mist Ethereum client interface. On the left is a sidebar menu with the following items: **ETHEREUM** (Wallet: 0 Wei, Browser), **APPS** (JeffCoin: 0 JEF), **DEBUG** (New transaction, Network, Information, Pending Transactions, JavaScript). At the bottom of the sidebar is a **Start Mining** button (0 Wei) and a slider set to 8/10.

The main window is titled "Mist" and contains a messaging interface. At the top, there is a "DApp URL" input field containing "file:///home/vub/2.html". Below this is a chat area with the following messages:

- caed7d78b8a:** be careful there, Facebook is data-mining all our conversations; don't want them to accidentally start showing you ads for baby products when your mom is looking over your shoulder.
- salazar:** well, luckily we're using a decentralized messenger over an encrypted channel, so it's not really data-minable at all :)
- caed7d78b8a:** wait, really?
- caed7d78b8a:** but who's encrypting and storing the data? don't they have access to it like Google?

A text input box contains the message: "data's encrypted client side, and it's stored only for a few minutes in completely encrypted form so only the recipient can decipher it. No backdoors here :)", with a **Send** button below it.

At the bottom of the chat area, there is a registration section:

- Current ID:** be35508fc4c
- Desired name:** josephine
- Register** button

Conclusion

- Build: <http://bit.ly/ethdapp>
- Learn: <http://ethereum.org>
- Contact: v@buterin.com

What will you do on Ethereum?

