

Software and Cyber
Solutions Symposium 2018

Blockchain

What, How, and Why

Eliezer Kanal

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2018 Carnegie Mellon University. All Rights Reserved.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material is distributed by the Software Engineering Institute (SEI) only to course attendees for their own individual study.

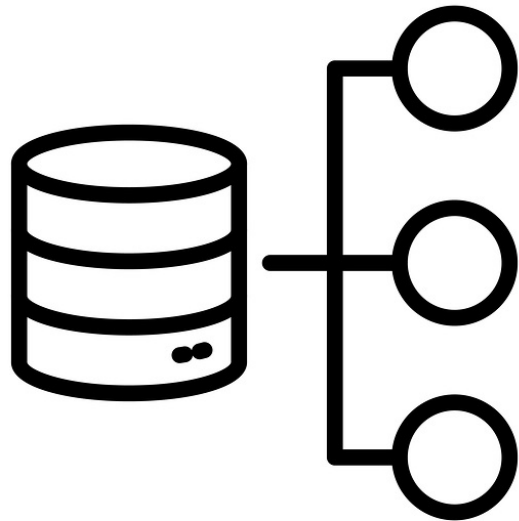
Except for any U.S. government purposes described herein, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.

Although the rights granted by contract do not require course attendance to use this material for U.S. Government purposes, the SEI recommends attendance to ensure proper understanding.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM18-0360

Previous models of computing

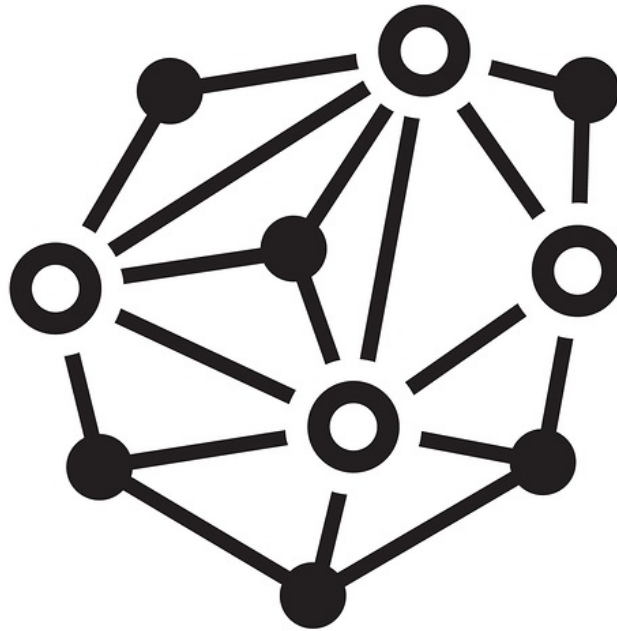


Data Storage:
Database



Program Execution:
Local

Blockchain



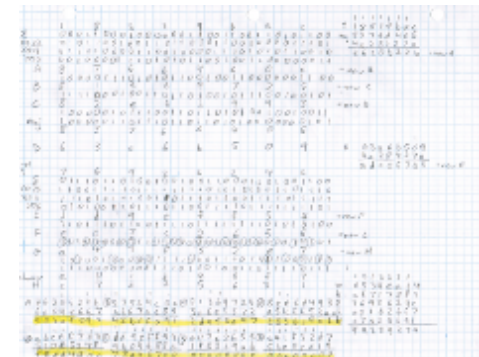
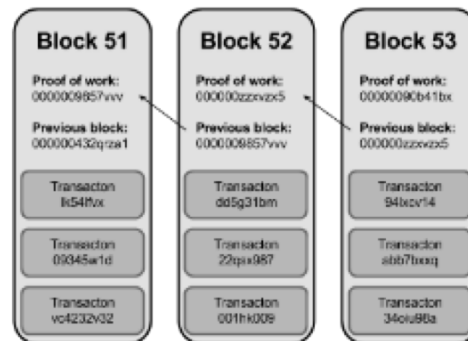
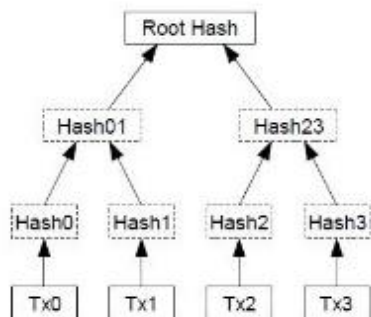
Data Storage:
Blockchain or Network

Program Execution:
Network

Bitcoin: Currency in a Blockchain

Three fundamental elements:

1. Transaction tree (state changes)
2. Blockchain (timeline for 1)
3. “Mining” protocol



<http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html>

Bitcoin: Transactions



Messages

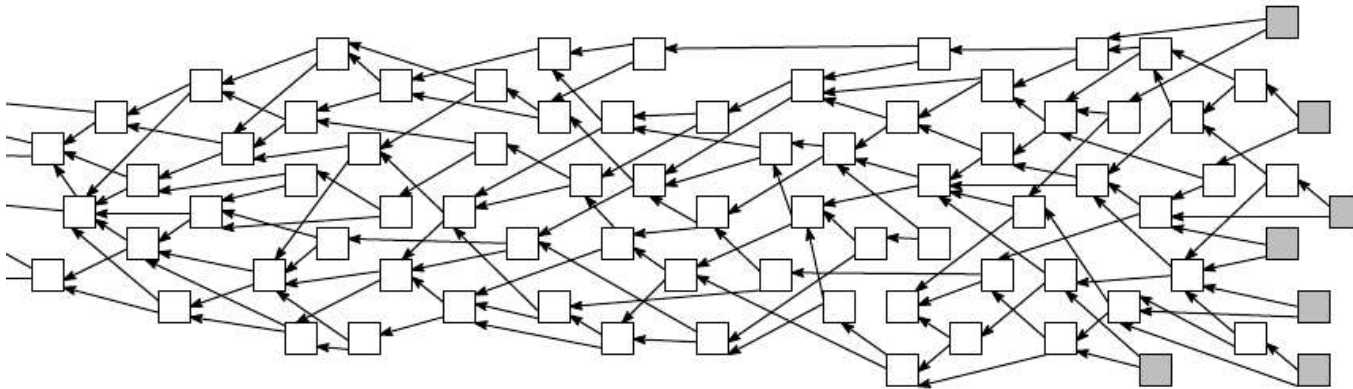
		<u>Signature</u>
Alice → Bob	0.44 BTC	387152...
Alice → Charlie	21.3 BTC	876401...
Alice → Dave	0.06 BTC	746122...
Charlie → Emily	1.80 BTC	076865...
⋮		

Bitcoin: Transaction Tree

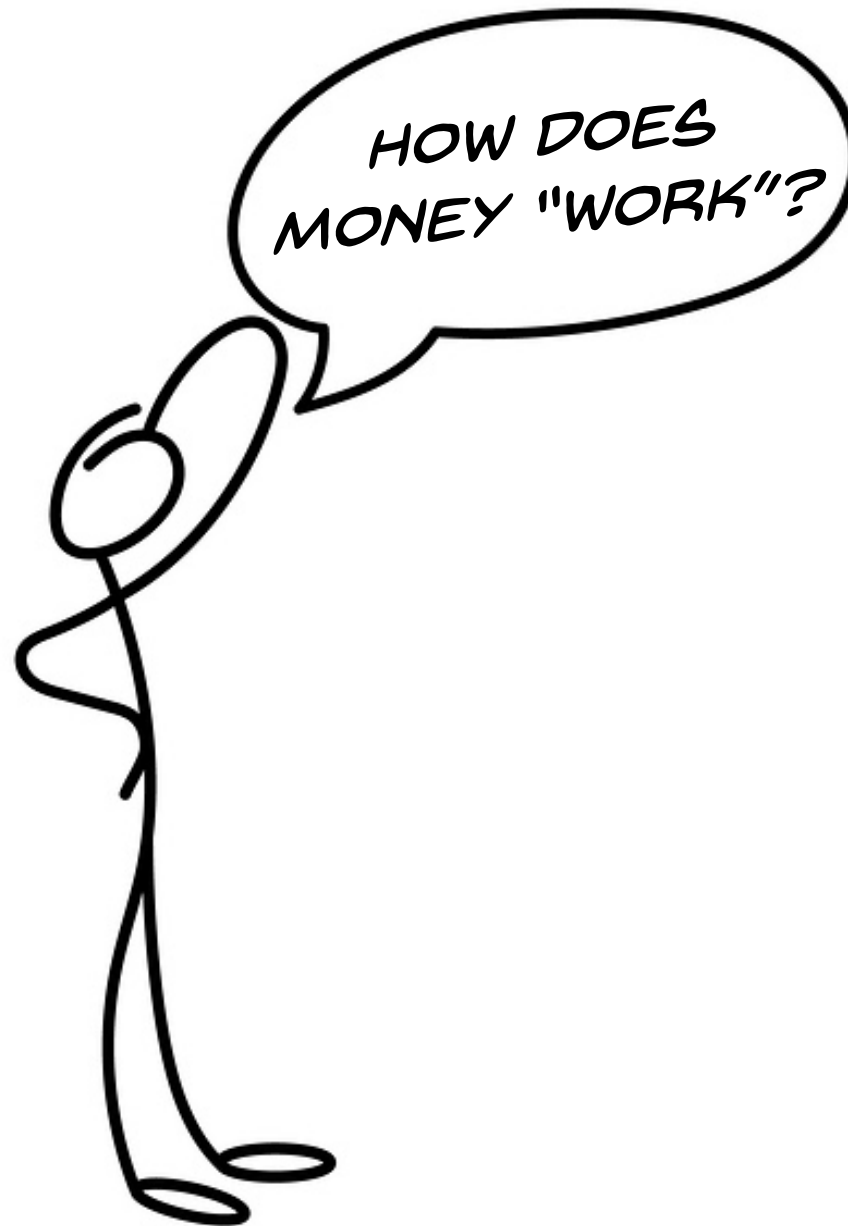
New transactions come from old ones

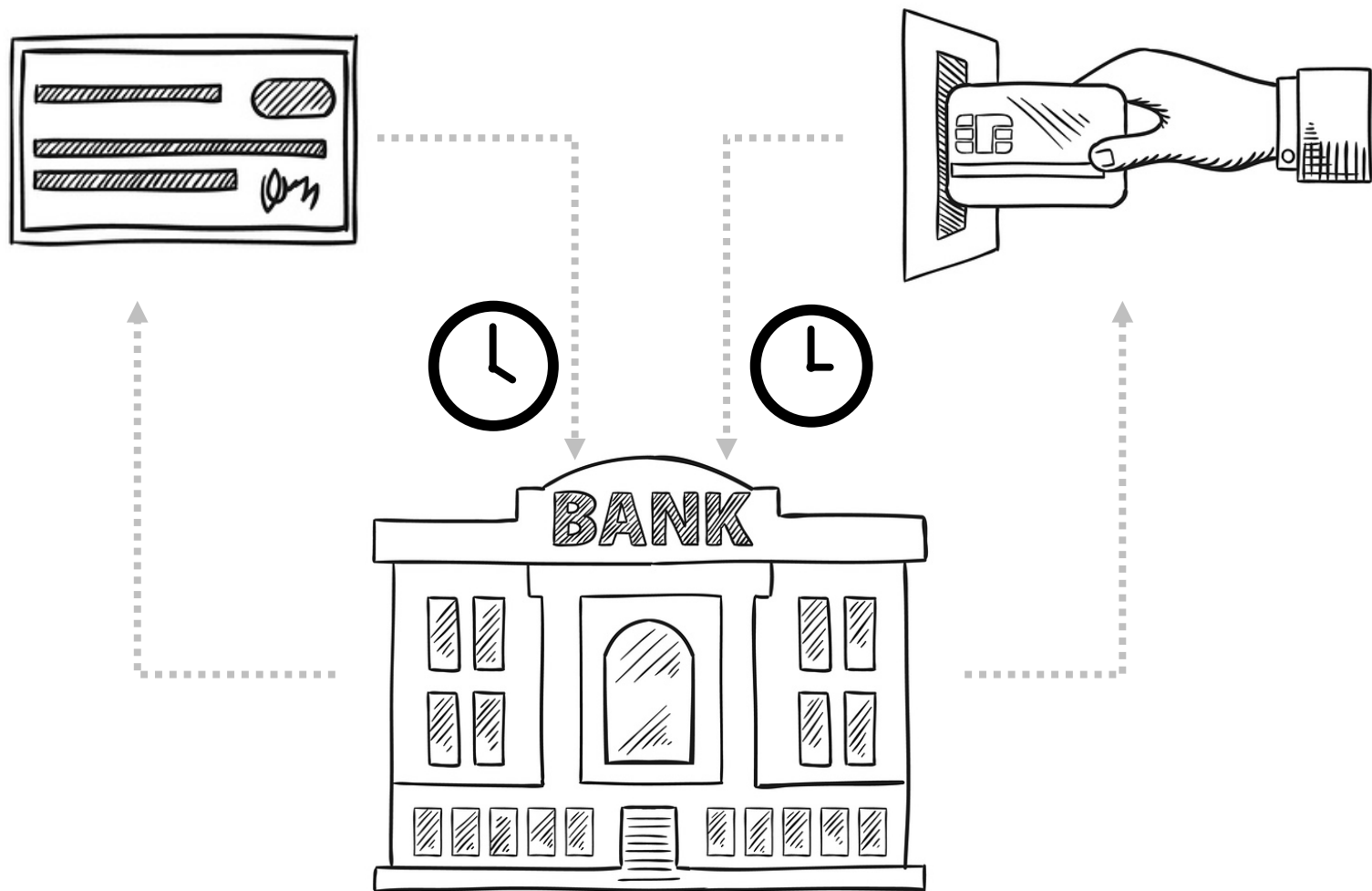
Balance = sum up incoming transactions

Auditable!



By Tiagodimas2 (Own work) [CC BY-SA 4.0 (<https://creativecommons.org/licenses/by-sa/4.0/>)], via Wikimedia Commons







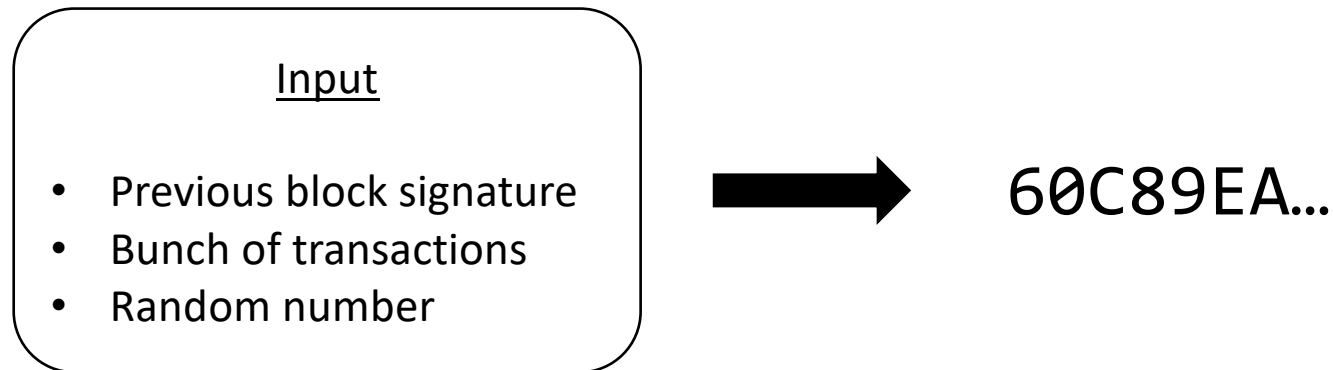
Bitcoin's challenge:

Timing

Bitcoin's solution:

Mining

Bitcoin: Mining



Signature	Transactions	Random #	Output
482AA...	txn 1, 17, 88, 452	1	854A3...
482AA...	txn 1, 17, 88, 452	2	B4221...
482AA...	txn 1, 17, 88, 452	3	0249F...
⋮			

Demo

Access demo online at <https://anders.com/blockchain/hash.html>

Play with the **Hash**, **Block**, and **Blockchain** sections (links in top-right of page)

Block #509169

Summary		Hashes	
Number Of Transactions	1915	Hash	000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Output Total	10,289.28130284 BTC	Previous Block	000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcd7240a471
Estimated Transaction Volume	1,818.68925455 BTC	Next Block(s)	
Transaction Fees	0.4893378 BTC	Merkle Root	3ad680735c45cc62b1ea6b7efeb34f82a2660c5e8280354c45f7ffa03c9137e2
Height	509169 (Main Chain)		
Timestamp	2018-02-14 15:16:59		
Received Time	2018-02-14 15:16:59		
Relayed By	58COIN		
Difficulty	2,874,674,234,415.94		
Bits	392292856		
Size	1132.416 kB		
Weight	3992.574 kWU		
Version	0x20000000		
Nonce	1858980081		
Block Reward	12.5 BTC		

Transactions

ab0da64ea834fd2acb81eb081d8103c9e31fd14a7d055f2ce2718c59dd4fa5df		2018-02-14 15:16:59
No Inputs (Newly Generated Coins)	➡ 14DjTuAUh87cwRsbU1z6W8hZY6FnEkpflS Unable to decode output address	12.9893378 BTC 0 BTC 12.9893378 BTC
4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552ed237f267d		2018-02-14 15:16:59
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	➡ 12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131 1GpqR4vsdvEfgtNyiUrDrfDLTBjvnstX 1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	0.4983 BTC 0.1495 BTC 5.01651602 BTC 5.66431602 BTC

Block #509169

1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP



12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131
1GpqR4vsdvEfgtNyiUrDrfDLTBjvnsentX
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP

0.4983 BTC
0.1495 BTC
5.01651602 BTC

5.66431602 BTC

Estimated Transaction Volume

1.818.68925455 BTC

Next Block(s)

Transaction Fees

Height

Timestamp

2018-02-14 15:16:59

Received Time

Relayed By

Difficulty

Bits

392292856

Size

Weight

Version

Nonce

1858980081

Number Of Transactions

1915

Nonce

1858980081

Difficulty

2,874,674,234,415.94

Hash

000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3

Previous Block

000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471

ab0da64ea834fd2acb81eb081d8103c9e31fd14a7d055f2ce2718c59dd4fa5df

2018-02-14 15:16:59

No Inputs (Newly Generated)

Block Reward

12.5 BTC

12.9893378 BTC
0 BTC

12.9893378 BTC

4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552ed237f267d

2018-02-14 15:16:59

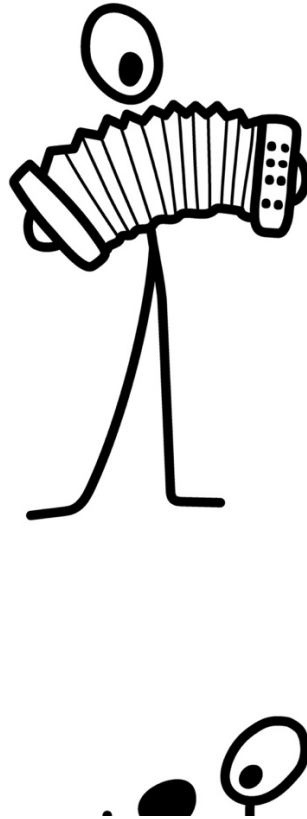
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP



12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131
1GpqR4vsdvEfgtNyiUrDrfDLTBjvnsentX
1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP

0.4983 BTC
0.1495 BTC
5.01651602 BTC

5.66431602 BTC



Blockchains – General Purpose

More than just a currency:

1. Transfer more than just cash
2. General purpose programming



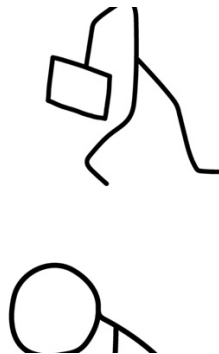
Ethereum

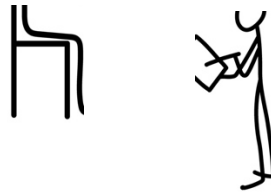
*Ethereum is a **transaction-based state machine***

Similar to Bitcoin, miners mine for “Ether”

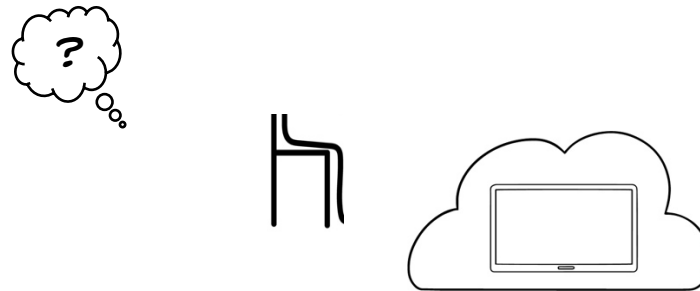
Two types of users:

1. Externally Owned Accounts (EOA) – “real people”
2. Contract Accounts – code

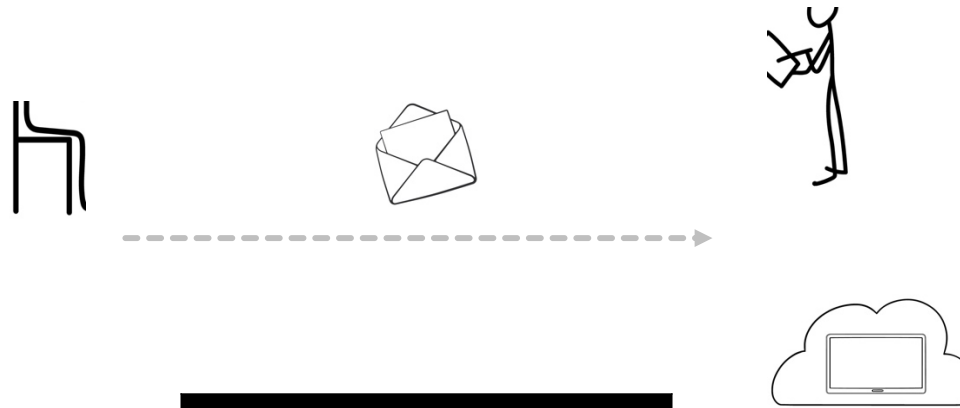




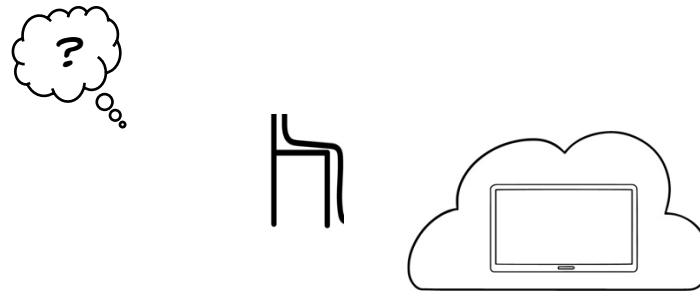
EOA properties
Ether balance
“Storage” contents



Contract properties
Ether balance
“Storage” contents
Code!



Messages
"To" address
Ether balance
Data
Gas price
Gas limit

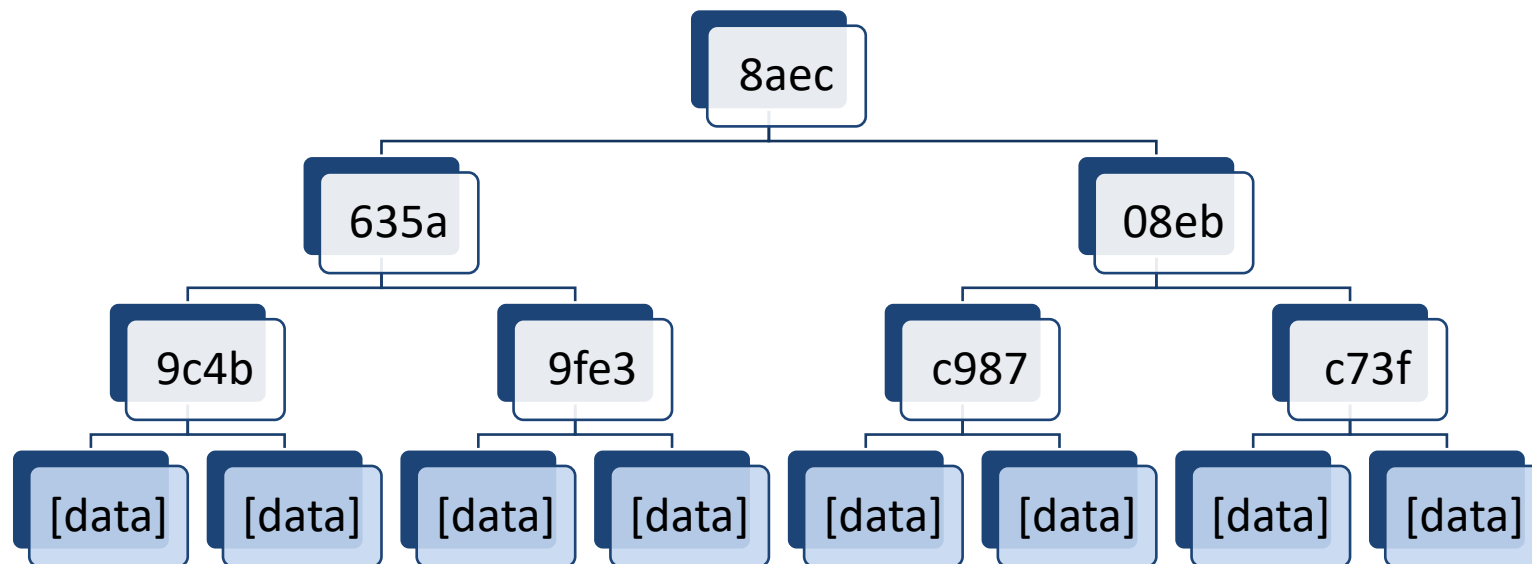


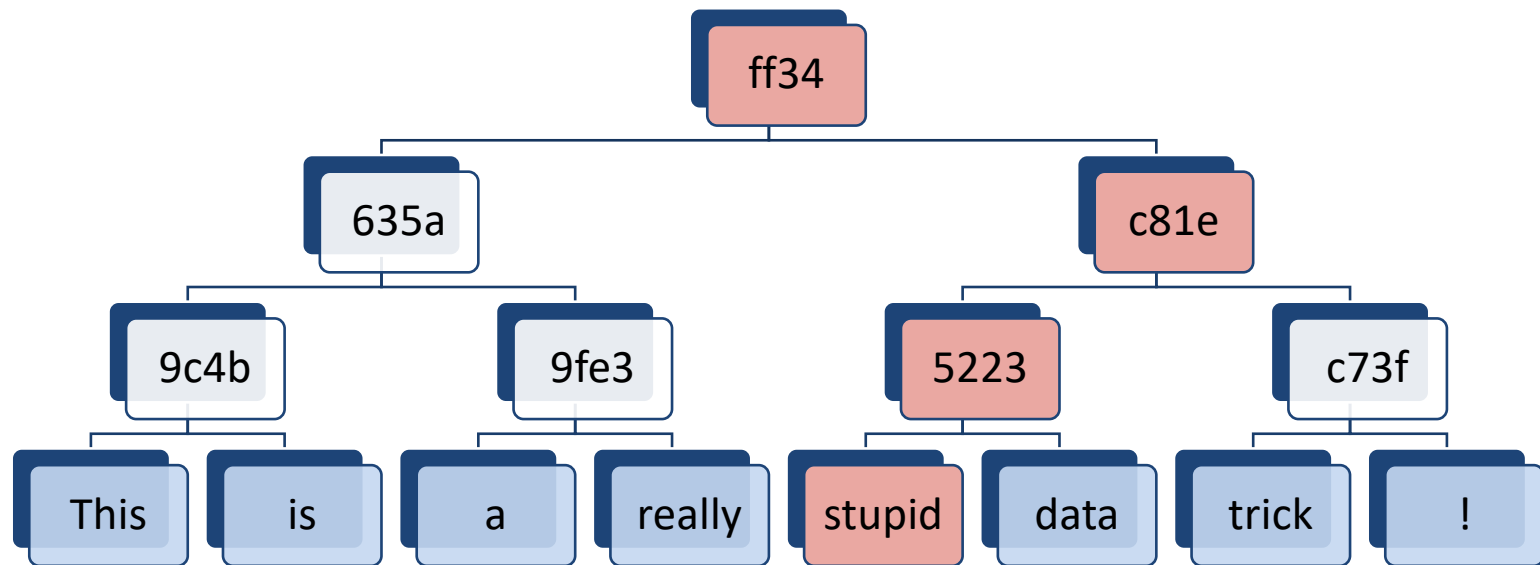
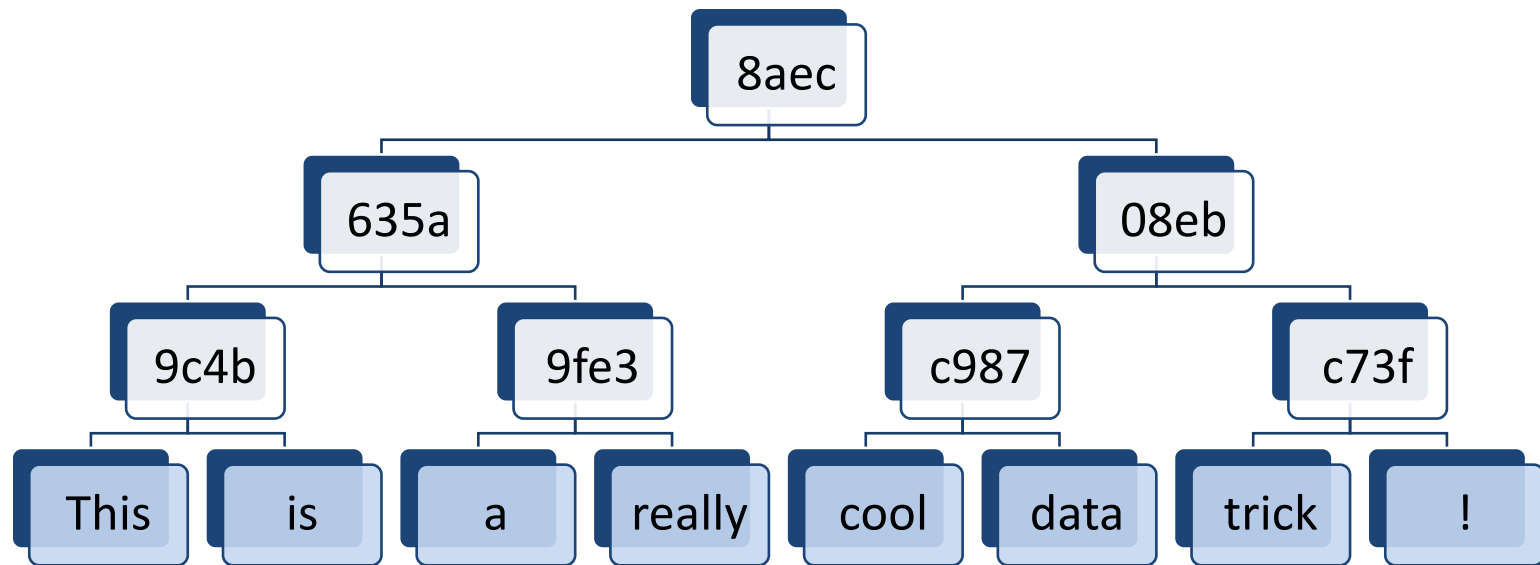
Contract properties
Ether balance
“Storage” contents
Code!

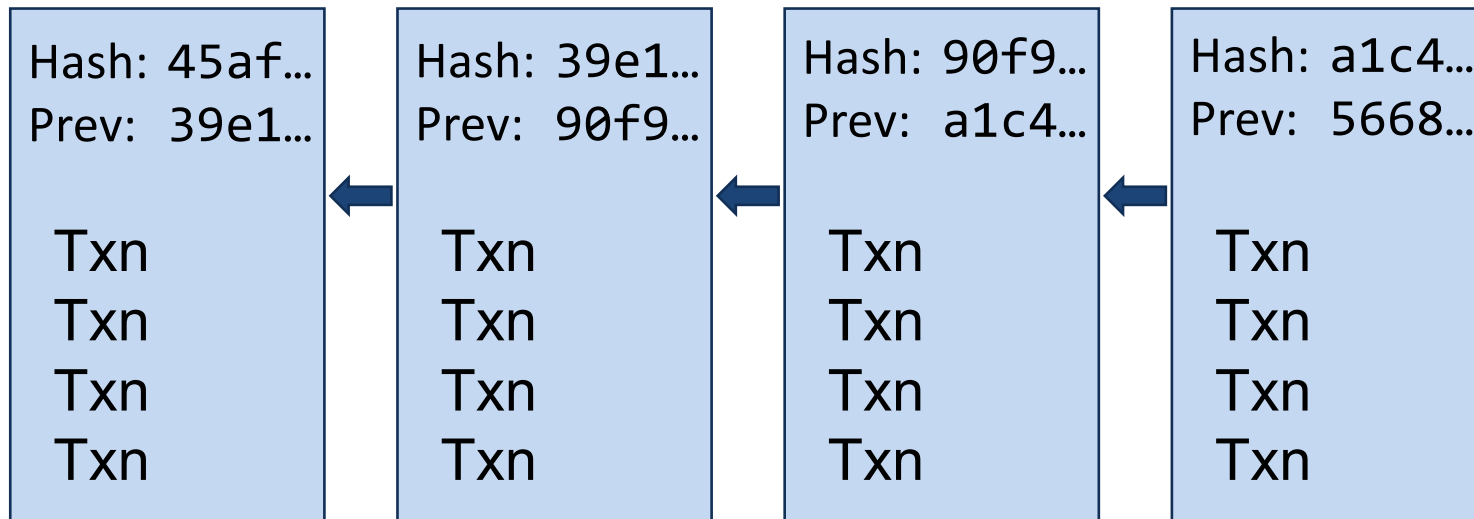
(Aside) Merkle Trie

Useful way to enable **data verification** without the requiring data

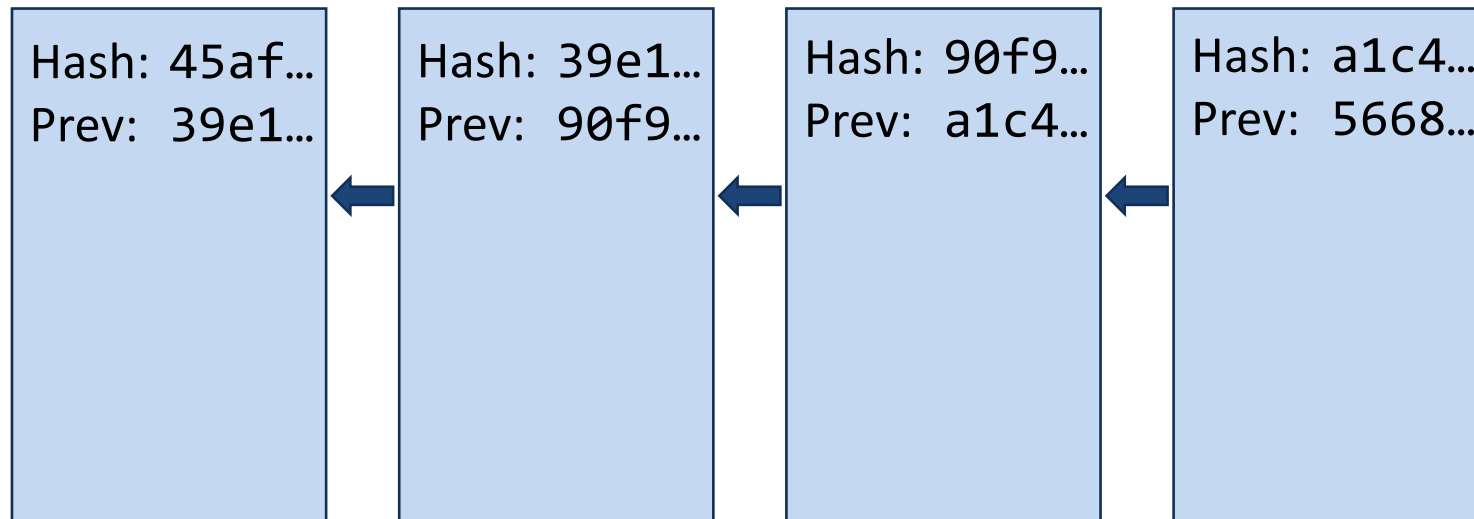
- Full node stores all data
- Light node just stores root hash
- Easy to find exactly which element of data changed!







Time →



Time

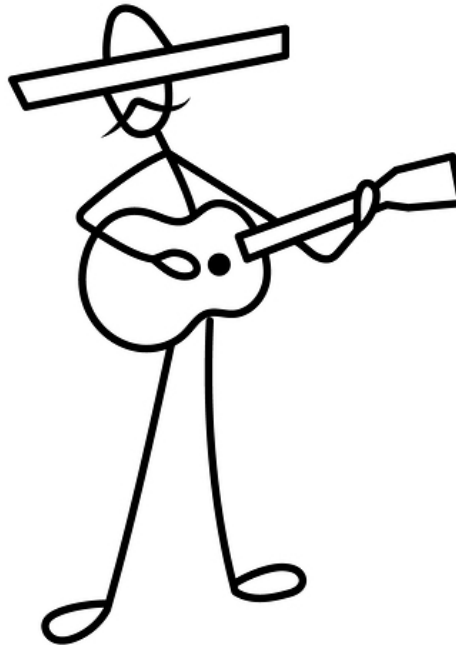
Ethereum – Ether & Gas

Design philosophy: *“There’s no free lunch”*

Allowing arbitrary programs requires careful incentive structure

- **Ether** is currency (1 Eth ~ \$850 today)
- **Gas** is fuel for **computations** and **storage**; “usage tax”
- Gas converts directly to Ether

Ethereum most useful for low-complexity programs!



Three problems:

1. Difficult to set up
2. Difficult to use
3. No privacy!



Hyperledger

HYPERLEDGER MODULAR UMBRELLA APPROACH

Infrastructure

Technical, Legal, Marketing, Organizational

Ecosystems that accelerate open development and commercial adoption



Cloud Foundry

Node.js

Hyperledger

Open Container Initiative

Frameworks

Meaningfully differentiated approaches to business blockchain frameworks developed by a growing community of communities

Hyperledger
Indy

Hyperledger
Fabric

Hyperledger
Iroha

Hyperledger
Sawtooth

Hyperledger
Burrow

Tools

Typically built for one framework, and through common license and community of communities approach, ported to other frameworks

Hyperledger
Composer

Hyperledger
Explorer

Hyperledger
Cello

Hyperledger Fabric

Three types of accounts (called “nodes”):

- | | |
|------------|--|
| 1. Client | Initiates transactions |
| 2. Peer | Maintains ledger state, commits transactions |
| 3. Orderer | Communication service via <i>channels</i> |

Purpose:

- Separate the multiple role of Miners into distinct entities
- Enable private communication between nodes

Blockchain – Step back



Pros:

- Transaction-based state machine
- Easy for anyone to audit history (examine chain)
- Easy to detect & stop data manipulation (Merkle Trees)
- Very difficult to disrupt (simultaneous distributed execution)

Blockchain – Step back



Cons:

- Proof-of-work is very inefficient
- State updates are slow (~1 hr Bitcoin, ~1 min Ethereum)
- Only simple computations

Blockchain – Step back

Cons-that-aren't-really-cons:

Con	-that-isn't-really-a-con
Can't store all data on-chain, too big	Store data off-chain, use Merkle Trees to verify (git)
Quantum computers will break PKA omg haxxorzzz!1!!	If PKA breaks, blockchain security is the least of our problems
Illegal “stuff” can't be removed from chain if ever added (link)	Policy can help prevent
No good way to link users to real identities	• Not just blockchain problem • “Chip”-ed ID cards, key fobs, etc

Blockchain – Step back

Pros:

- Transaction-based state machine
- Easy for anyone to audit history (examine chain)
- Easy to detect & stop data manipulation (Merkle Trees)
- Very difficult to disrupt (simultaneous distributed execution)

Cons:

- **Proof-of-work is very inefficient**
- State updates are slow (~1 hr Bitcoin, ~1 min Ethereum)
- Only simple computations

Bitcoin.com **Wallet** BTC/USD \$9139 ▼ BCH/USD \$1050 ▲ menu

NEWS

MINING



1 day ago | Jamie Redman | 6639

'Cryptomatoes' Using Excess Mining Heat to Grow Produce

- The original blockchain runs on an algorithm that could eat up more energy than Argentina this year, Morgan Stanley estimates.

[Helen Zhao](#) | @ZhaoMeow

Published 4:44 PM ET Fri, 23 Feb 2018 | Updated 2:23 PM ET Tue, 27 Feb 2018

VICE

video

MAKE IT VIDEO SHOWS MORE

on
t amount
neers are

ell University and tech
en blockchain

logy behind bitcoin -
efficiency is key, developers

Consensus alternatives

Algorithm	Properties
Proof of Work	• Probabilistic solution • Lottery by computational power
Proof of Stake	• Probabilistic solution • Lottery by total number of shares • “Nothing at stake”
BFT-based POS (“ Tendermint ”)	• Multi-round voting process, removes possibility of forking • May stall out if 1/3 voters offline • Favors Consistency
Proof-by-bet POS (“ Casper ”)	• Validators must place deposits on their “preferred” fork • Favors Availability

Blockchain – Step back

Pros:

- Transaction-based state machine
- Easy for anyone to audit history (examine chain)
- Easy to detect & stop data manipulation (Merkle Trees)
- Very difficult to disrupt (simultaneous distributed execution)
- Identity tied to transactions (PKA)

Cons:

- ~~Proof-of-work is very inefficient~~ (under research)
- State updates are slow (~1 hr Bitcoin, ~1 min Ethereum)
- Only simple computations

Uses, Uses, Wherefore Art Thou Uses?

Auditable, tamper-proof, robust, identifiable, slow, simple...?

- Finance
- Health care
- Voting
- Supply chain management
- Basically any records management system

BITCOIN & BLOCKCHAIN STARTUPS MARKET MAP

WALLETS & MONEY SERVICES



EXCHANGES & CRYPTOCURRENCY TRADING



P2P MARKETPLACES & P2P LENDING



MERCHANT SERVICES



ENTERPRISE SERVICES & CURRENCIES



SOCIAL & BROWSERS



CRYPTOCURRENCY MINING



IoT, IDENTITY & CONTENT MANAGEMENT



STORAGE, SECURITY & REGULATORY



CAPITAL MARKETS & FINANCIAL SERVICES



Blockchain in Government

DoD	Secure data files for Additive Manufacturing (3D printing) of parts
CDC	Attributable, distributed information dissemination
FDA	EMR replacement
GSA	"...automate the FASt Lane process for IT Schedule 70 contracts."
DHS	Exploratory (air travel, international trade, anti-money laundering)
Treasury	Asset management
Illinois Blockchain Initiative	"Give me some of that blockchain goodness"

[Unofficial and definitely incomplete list](#)

This conveyance has been recorded in smart contract 0xa188e5a3da203f8ebc72ec7578532926dcd3bec of the public Ethereum blockchain.

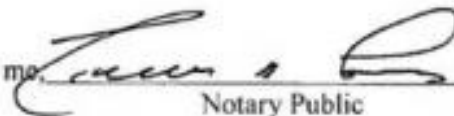


IN WITNESS WHEREOF, the parties do hereby execute this Warranty Deed this 20th day of February, 2018.

Katherine M. Purcell

STATE OF VERMONT
COUNTY OF CHITTENDEN, SS.

On this 20th day of February, 2018, personally **KATHERINE M. PURCELL**, to me known to be the person who executed the foregoing instrument, and she acknowledged this instrument, by her signed, to be her free act and deed.

Before me, 
Notary Public

Printed Name: Michelle N Farbas

Notary commission issued in Chittenden County
My commission expires: 2/10/19

Tools & Utilities ▾

TxReceipt Status: Success

TimeStamp: 20 days 3 hrs ago (Feb-16-2018 01:15:24 PM +UTC)

To: [Contract 0xa188e5a3da203f8ebc72ec7578532926dc1d3bec Created] 

Value: 0 Ether (\$0.00)

Gas Limit: 2284690

Gas Used By Txn: 472258

Gas Price: 0.000000001 Ether (1 Gwei)

Actual Tx Cost/Fee: 0.000472258 Ether (\$0.35)

Nonce: 65

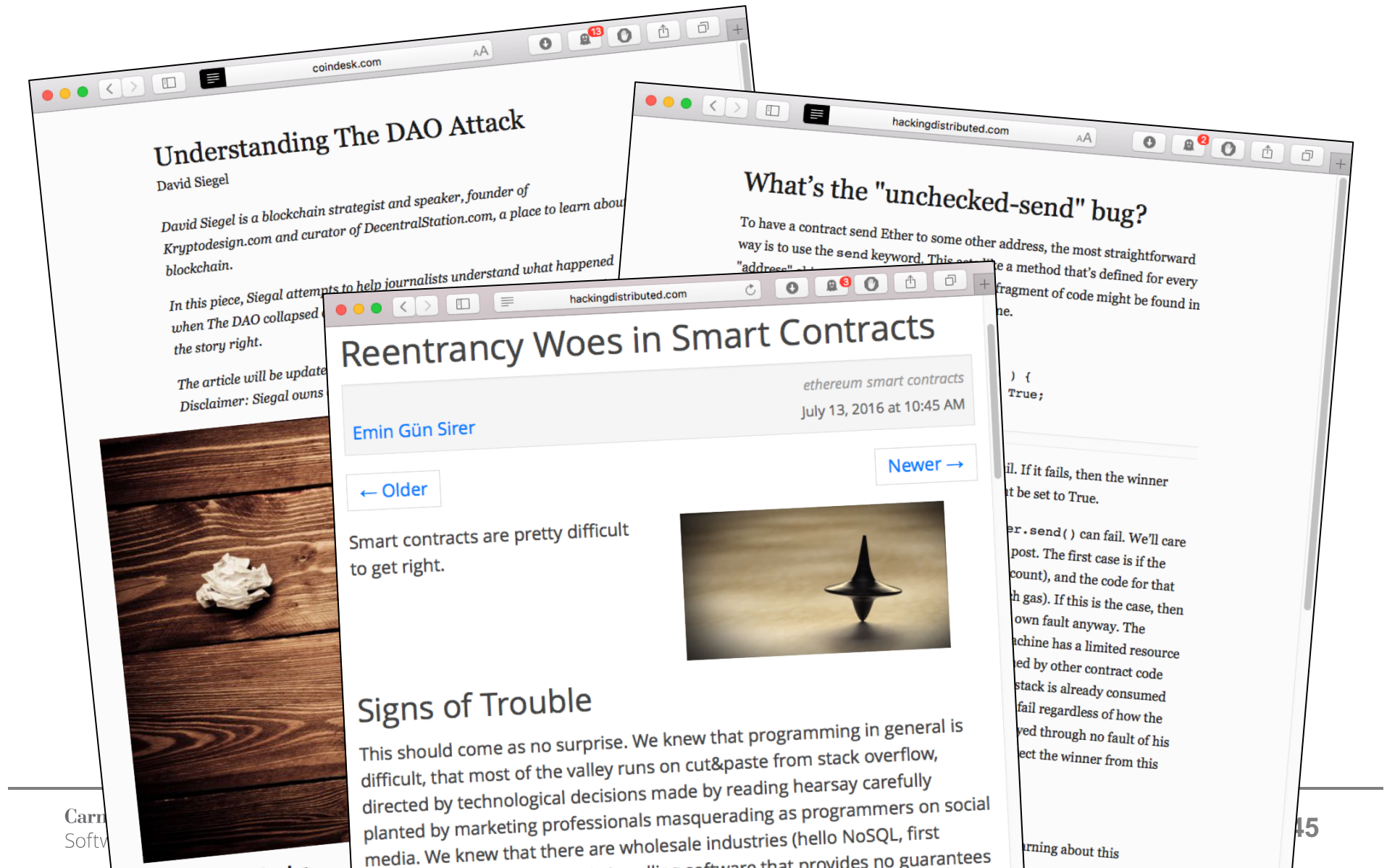
Input Data:

[illegible][Convert To Ascii](#)

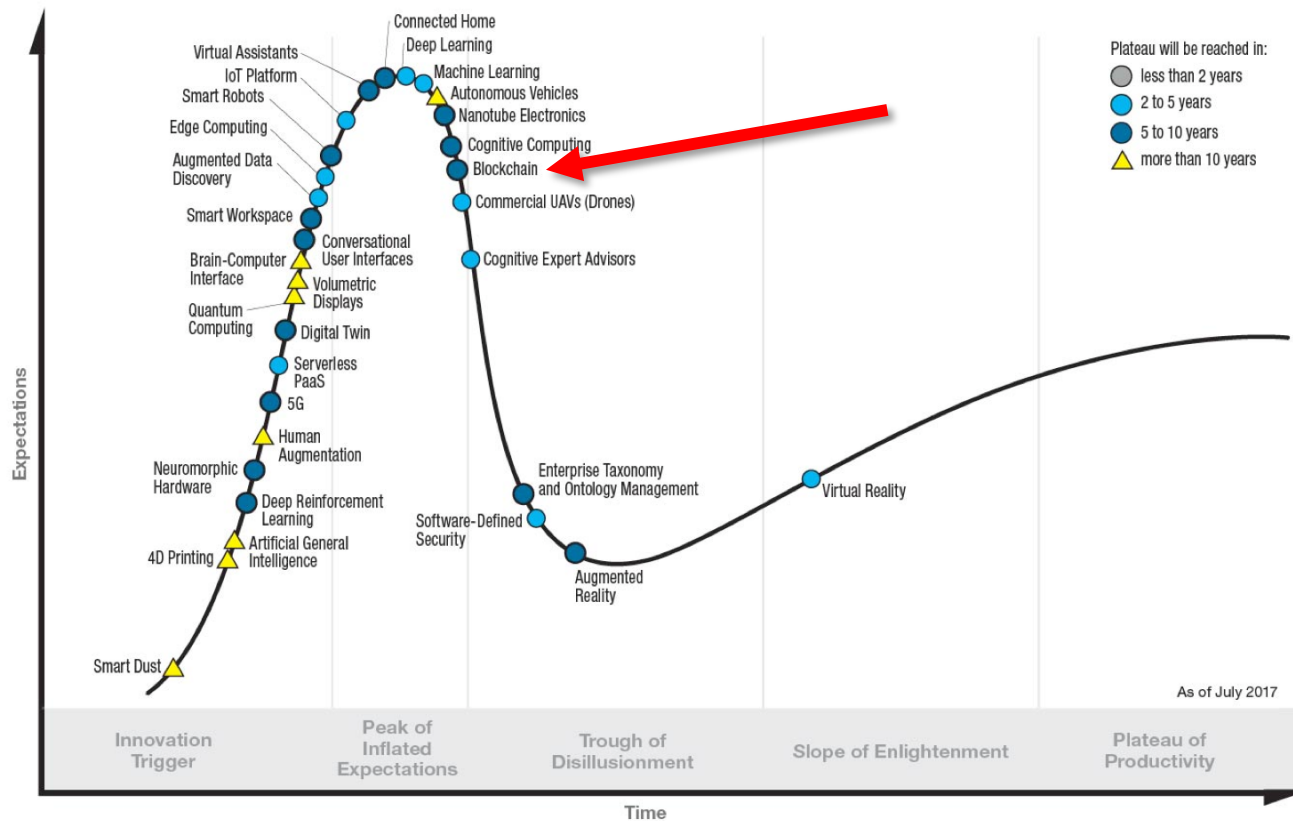
Private Note:

<To access the private Note feature, you must be [logged in](#)>

Still in infancy!



Gartner Hype Cycle for Emerging Technologies, 2017



gartner.com/SmarterWithGartner

Source: Gartner (July 2017)
© 2017 Gartner, Inc. and/or its affiliates. All rights reserved.

Gartner

Thanks!