Blockchain

Eliezer Kanal

2018-03-08

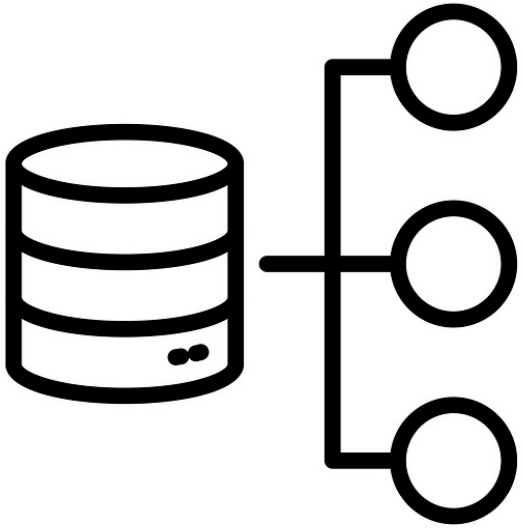
SFST talk

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

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.

DM18-0338

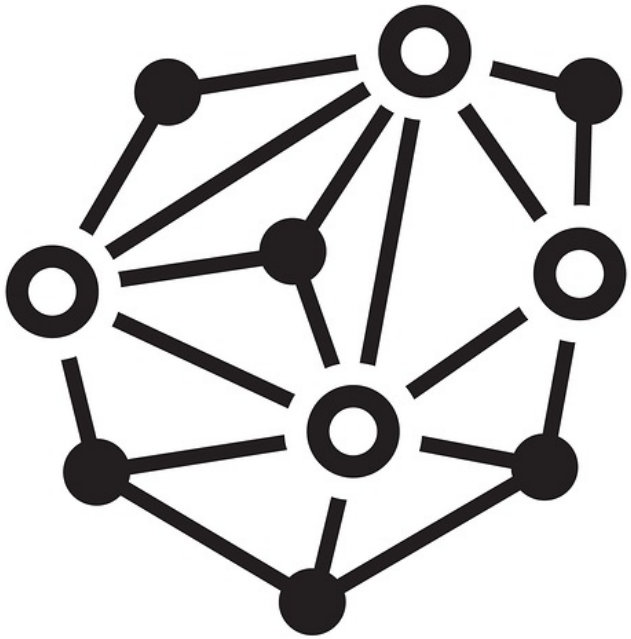
Previous models of computing



Data Storage:
Database

Program Execution:
Local

Blockchain



Data Storage:

Blockchain or Network

Program Execution:

Network

Picture
(optional)

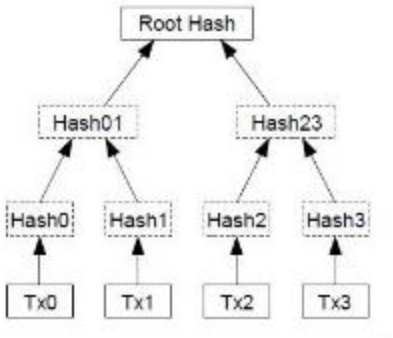
Many of these graphics are lifted directly from Scott Driscoll's excellent set of overviews on Bitcoin. Check him out on Google+.

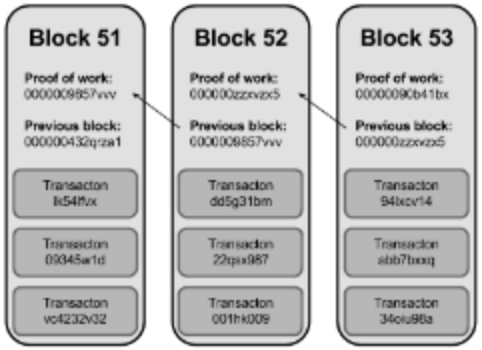
http://www.imponderablethings.com/2013/07/how-bitcoin-works-under-hood.html

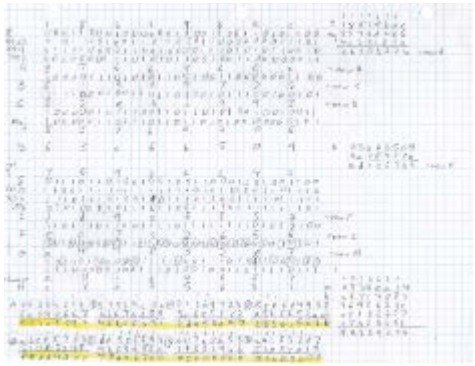
Bitcoin: Currency in a Blockchain

Three fundamental elements:

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

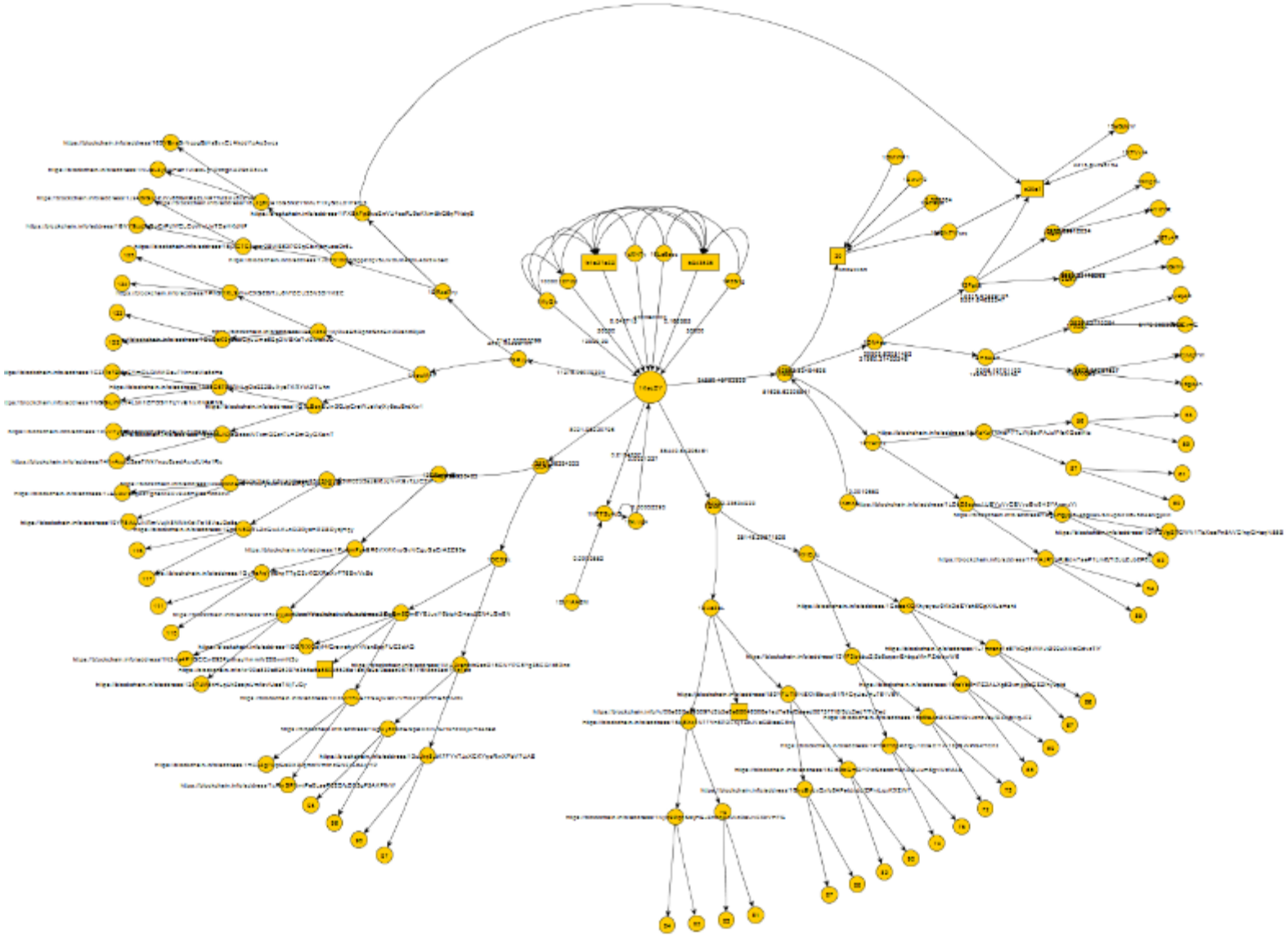




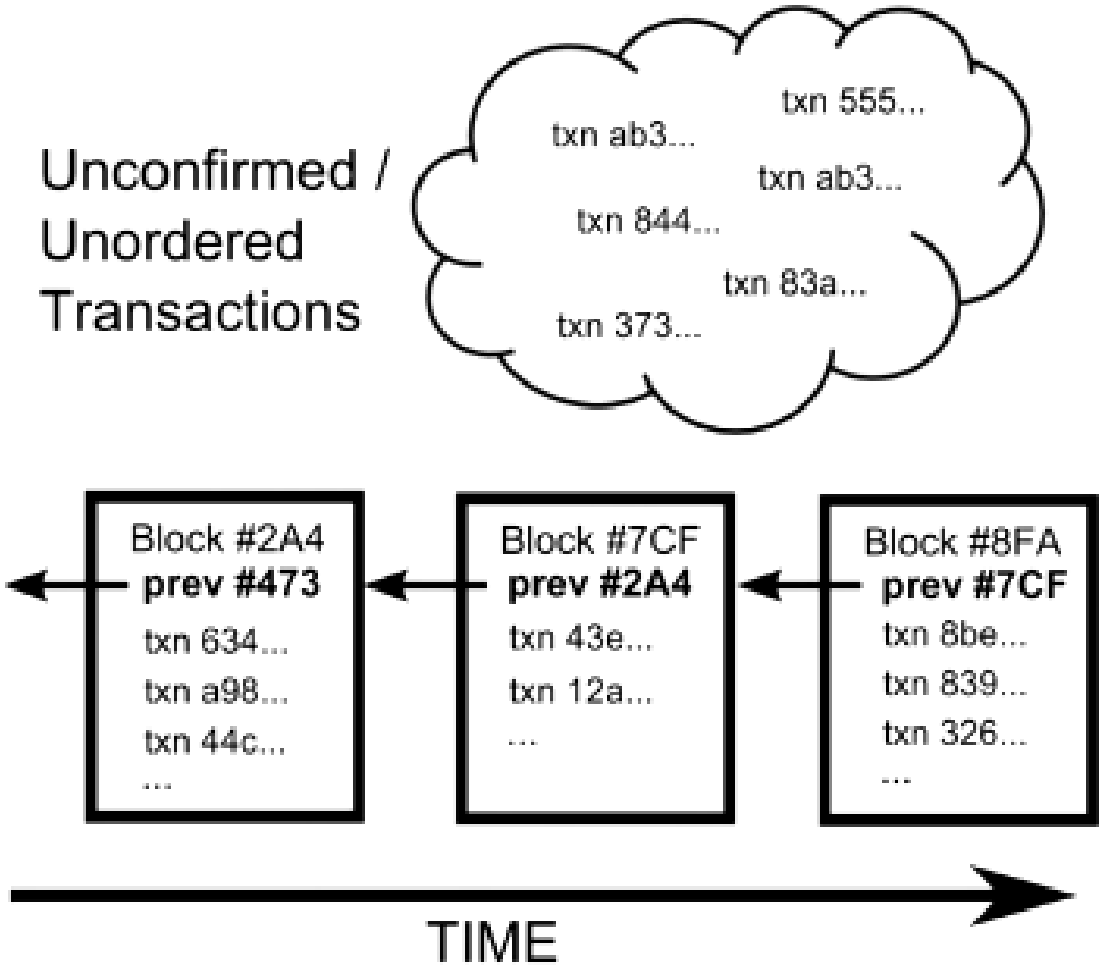


Bitcoin: Transactions

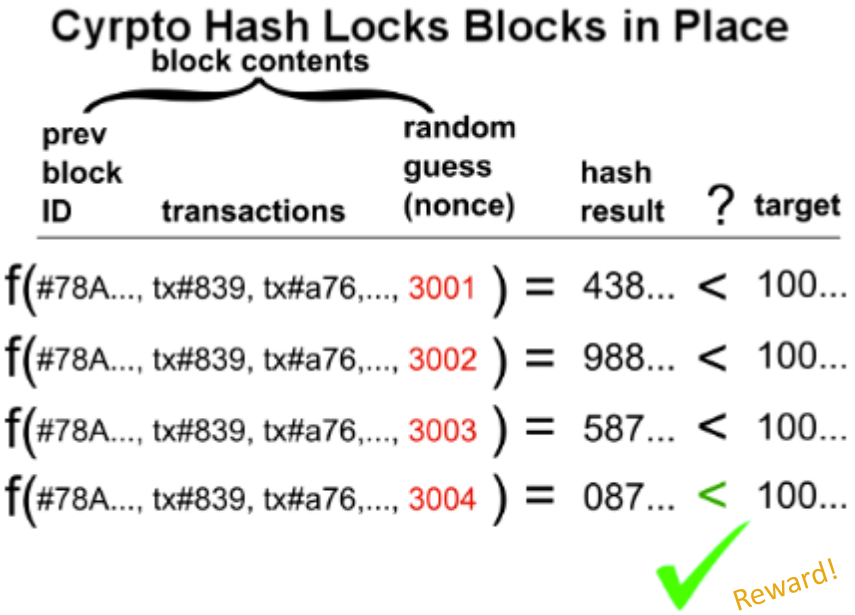
Bitcoin: Transaction Tree

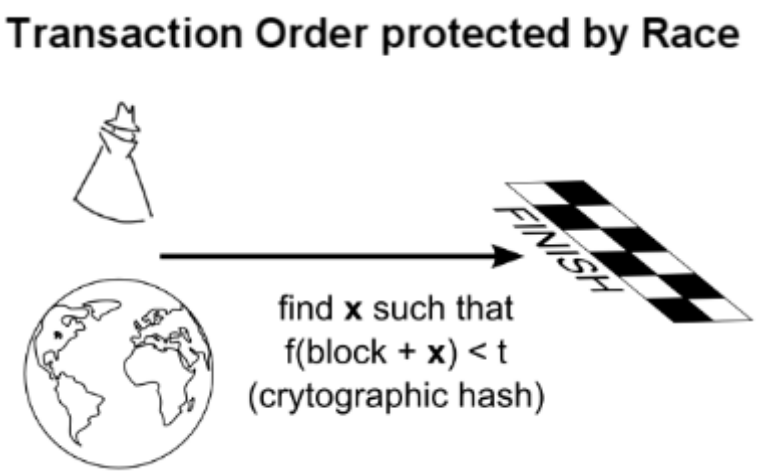


Bitcoin: Blockchain



Bitcoin: Mining





https://www.youtube.com/watch?v=l9jOJk30eQs&t=121

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	
Number Of Transactions	1915
Output Total	10,289.28130284 BTC
Estimated Transaction Volume	1,818.68925455 BTC
Transaction Fees	0.4893378 BTC
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

Hashes	
Hash	00000000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Previous Block	00000000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471
Next Block(s)	
Merkle Root	3ad680735c45cc62b1ea6b7efeb34f82a2660c5e8280354c45f7ffa03c9137e2

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 1GpqR4vsdvEfgtNyiUrDrfDLTBJvnsentX 1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	0.4983 BTC 0.1495 BTC 5.01651602 BTC

5.66431602 BTC

Block #509169

1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	→	12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131	0.4983 BTC
		1GpqR4vsdvEfgtNyiUrDrfDLTBJvnsentX	0.1495 BTC
		1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	5.01651602 BTC
			5.66431602 BTC

Estimated Transaction Volume	1,818.68925455 BTC
Transaction Fees	
Height	
Timestamp	2018-02-14 15:16:59
Received Time	
Relayed By	
Difficulty	
Bits	392292856
Size	
Weight	
Version	
Nonce	1858980081

Next Block(s)

280354c45f7ffa03c9137e2

Number Of Transactions	1915
Nonce	1,858,980,081
Difficulty	2,874,674,234,415.94
Hash	00000000000000002c4b94355945eea353bc720c58a73c2b8593f489550cb3
Previous Block	00000000000000001d620a2e3ad126ec5038bf42343c419eb6fcdf7240a471

ab0da64ea834fd2acb81eb081d8103c9e31fd14a7d055f2ce2718c59dd4fa5df — 2018-02-14 15:16:59

No Inputs (Newly G	Block Reward	12.5 BTC

12.9893378 BTC
0 BTC
12.9893378 BTC

4feb8981da942b10a2a384003fba1c1d78c8f192cd2747e43ae552ed237f267d — 2018-02-14 15:16:59

1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	→	12PaHiRJBmvJYmTpZ32Pswf8eYbKcAE131	0.4983 BTC
		1GpqR4vsdvEfgtNyiUrDrfDLTBJvnsentX	0.1495 BTC
		1H6ZZpRmMnrw8ytepV3BYwMjYYnEkWDqVP	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

Ethereum – Account properties

	EOA	Contract account
Nonce	Count of transactions sent	Count of new contracts created
Balance	Wei (= $1x10^{18}$ Ether) owned	
Storage	Hash of account storage contents	
Code	Hash of blank string	Hash of account code

Ethereum – Messages

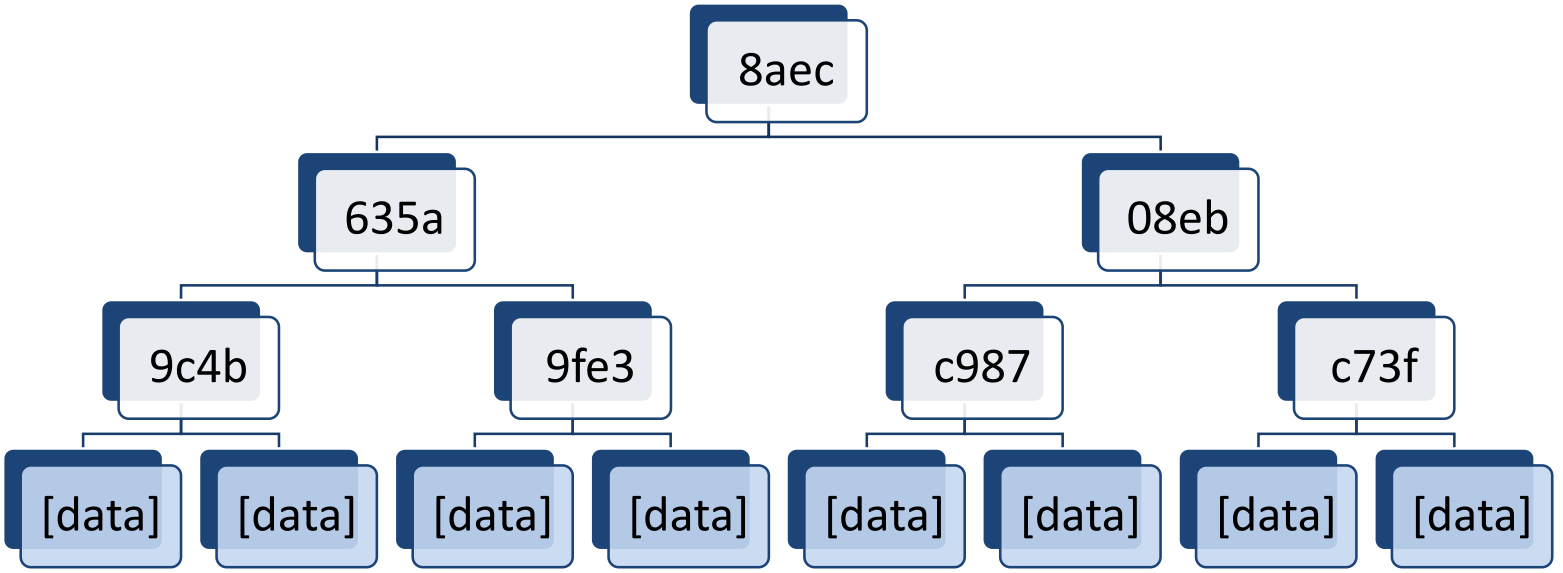
	Message	Contract creations
Gas price	Ether to be paid for unit of gas	
Gas limit	Max gas allowed	
To address	Recipient address	Empty string
Value	Ether being sent	Starting balance of new contract
Sig stuff	Stuff to validate sender of transaction	
Init code	N/A	New contract code
data	Function parameters	N/A

(Aside) Merkle Trie

Picture (optional)

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

- Full node stores all data
- Light node just stores root hash



Ethereum – Ether & Gas

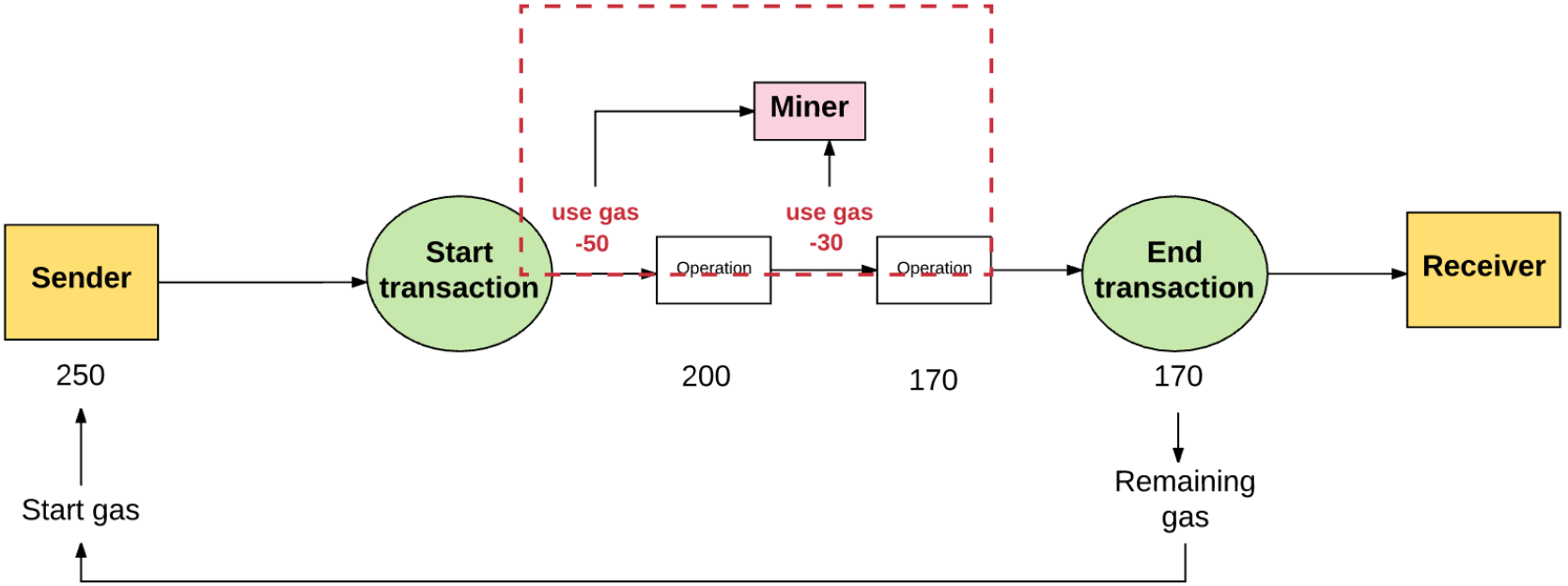
Design philosophy: *"There's no free lunch"*

Allowing arbitrary programs requires careful incentive structure

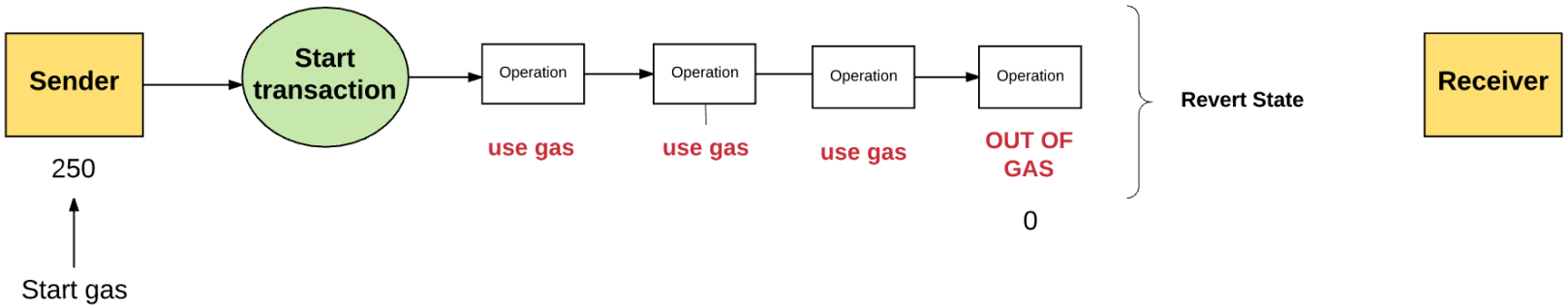
- **Ether** is currency (1 Eth ~ $850 today)
- **Gas** is fuel for **computations** and **storage**; "usage tax"
- Gas converts directly to Ether

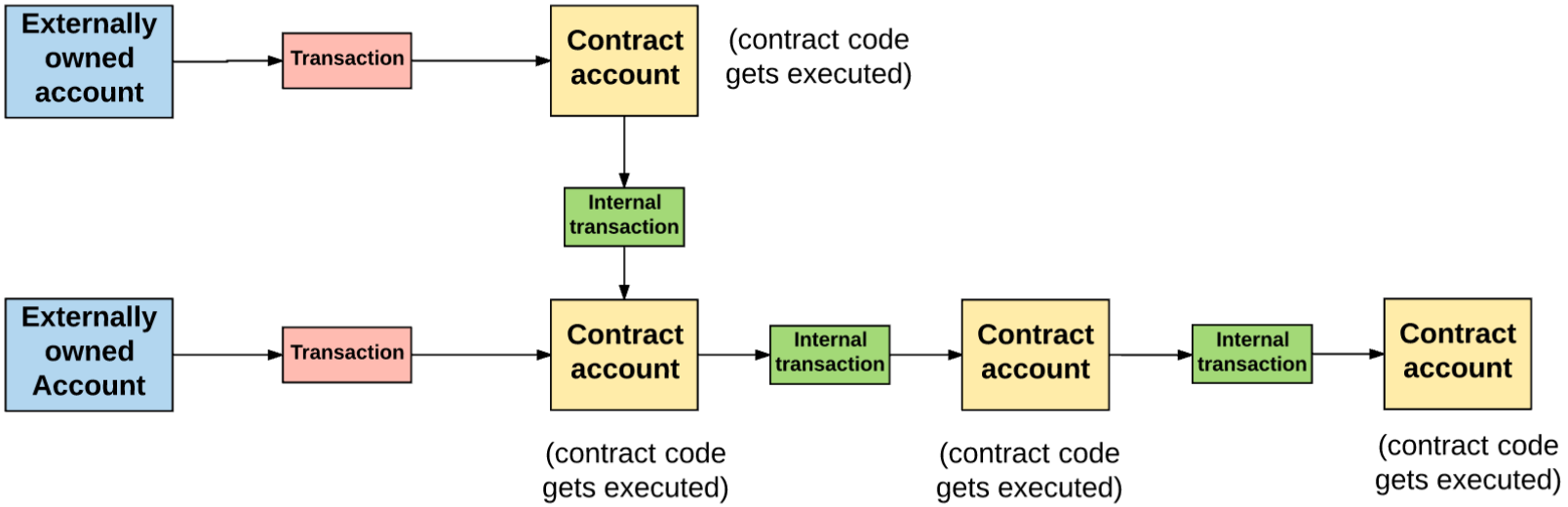
Ethereum most useful for low-complexity programs!

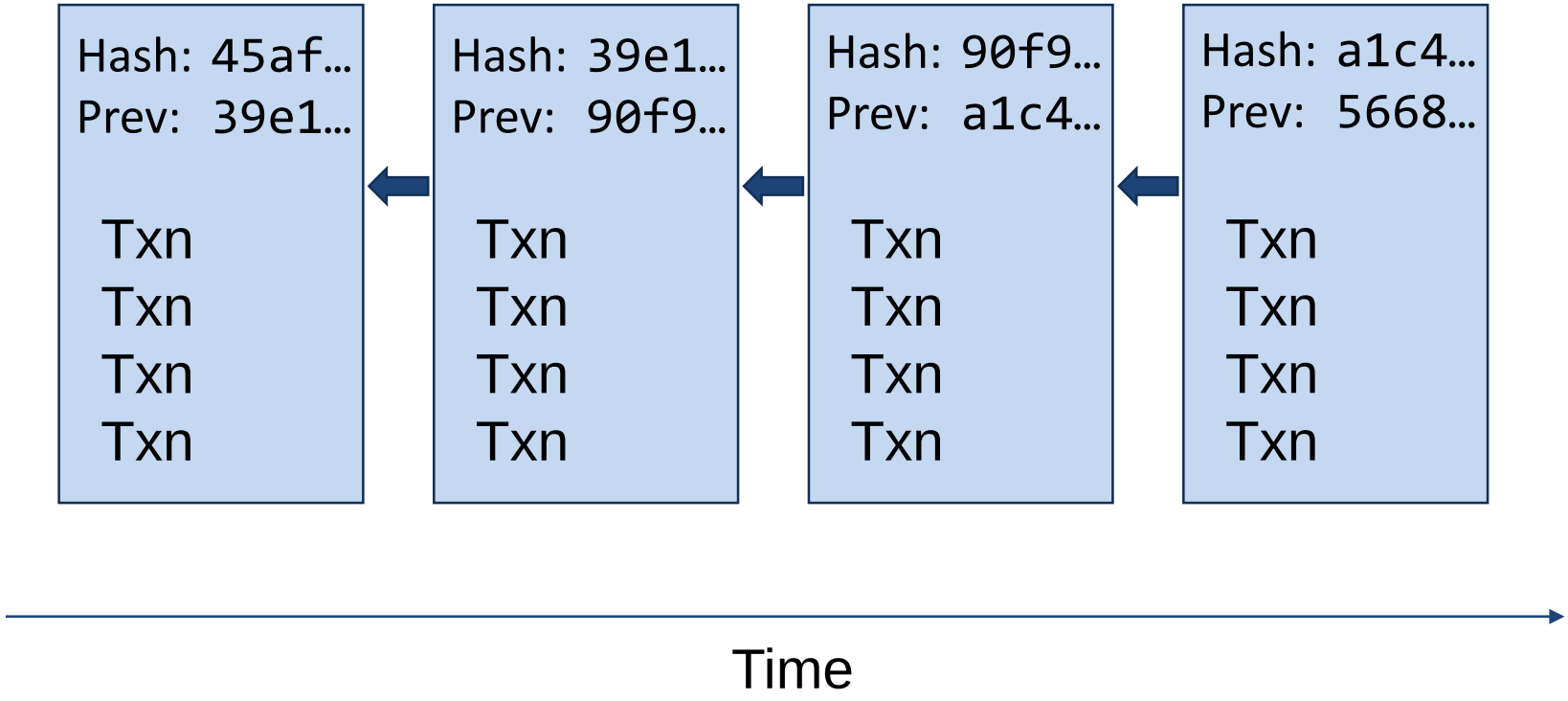
Ethereum – Gas

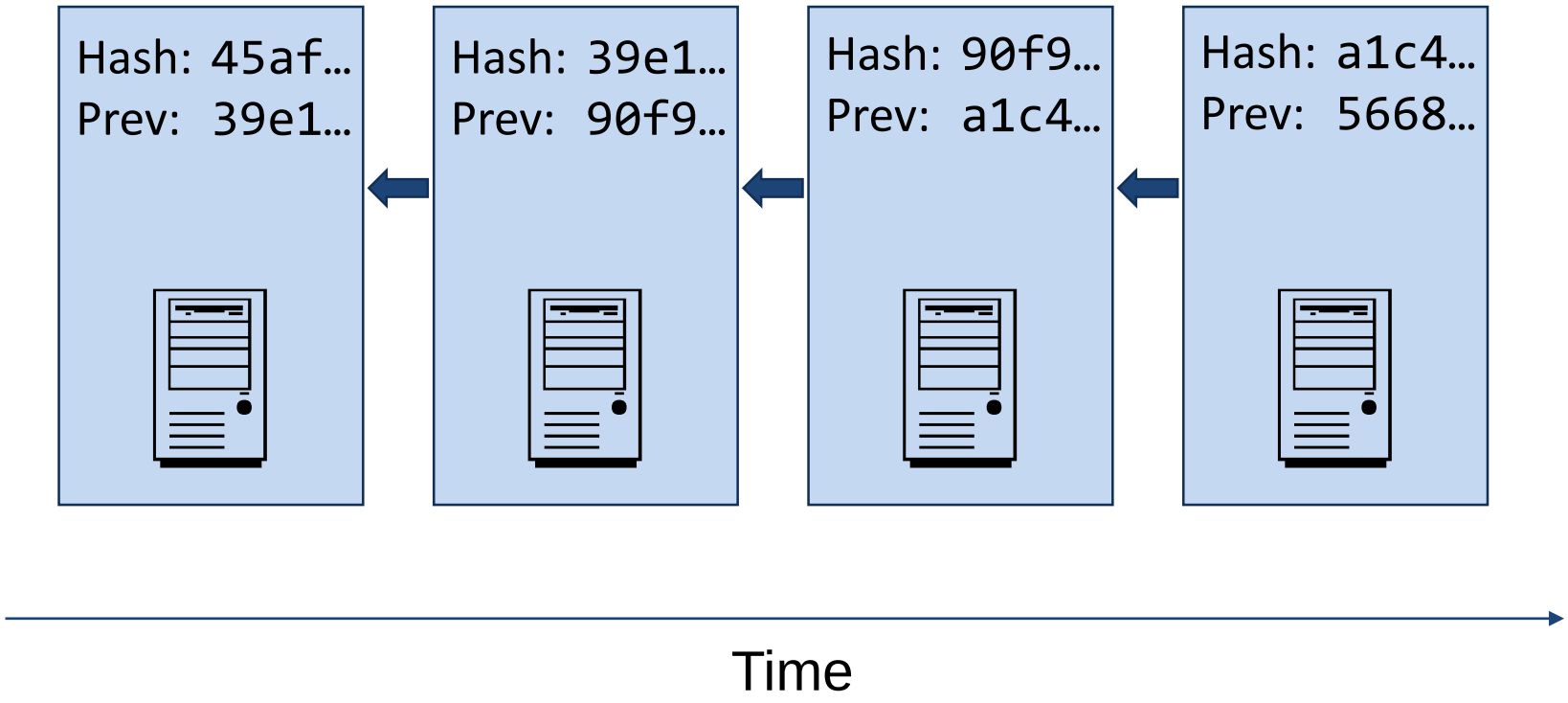


Ethereum – Gas

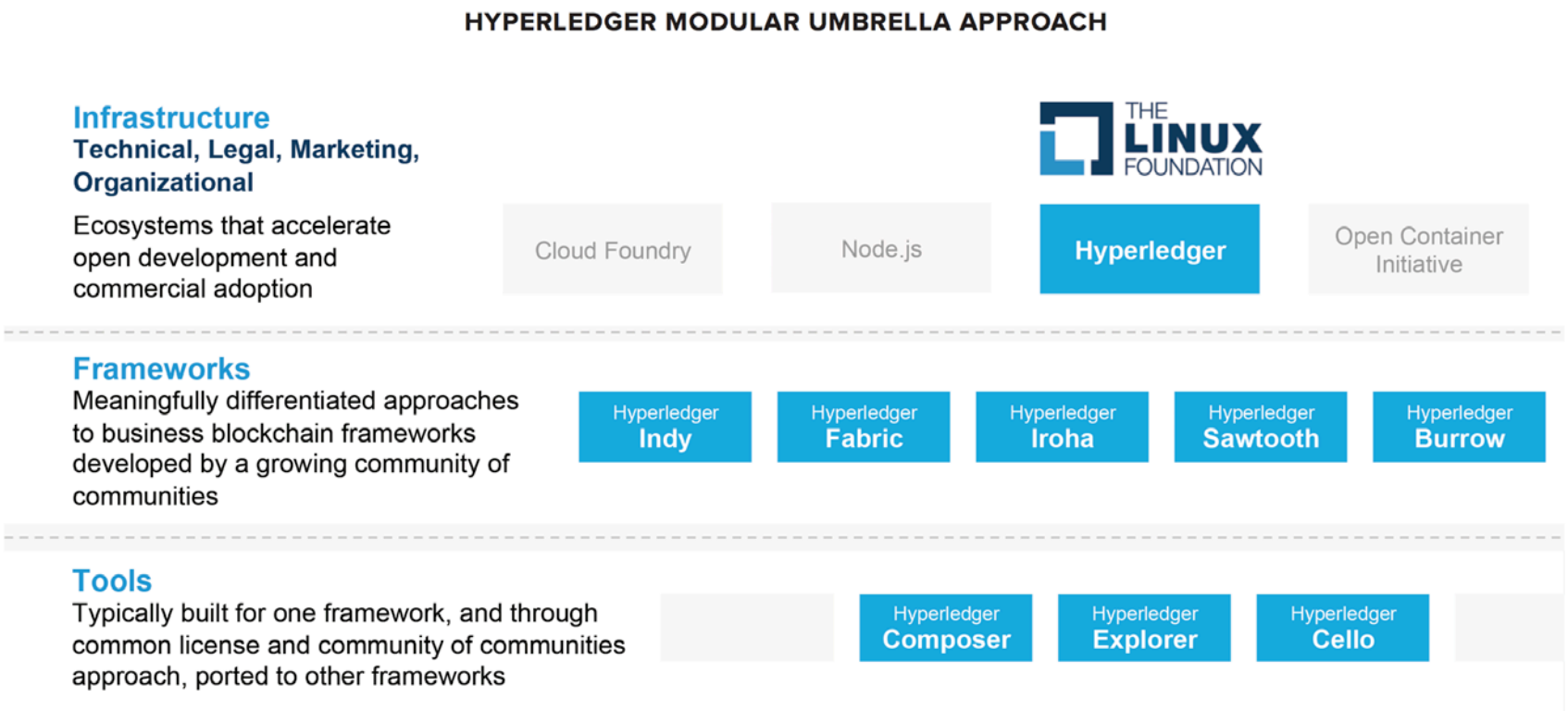




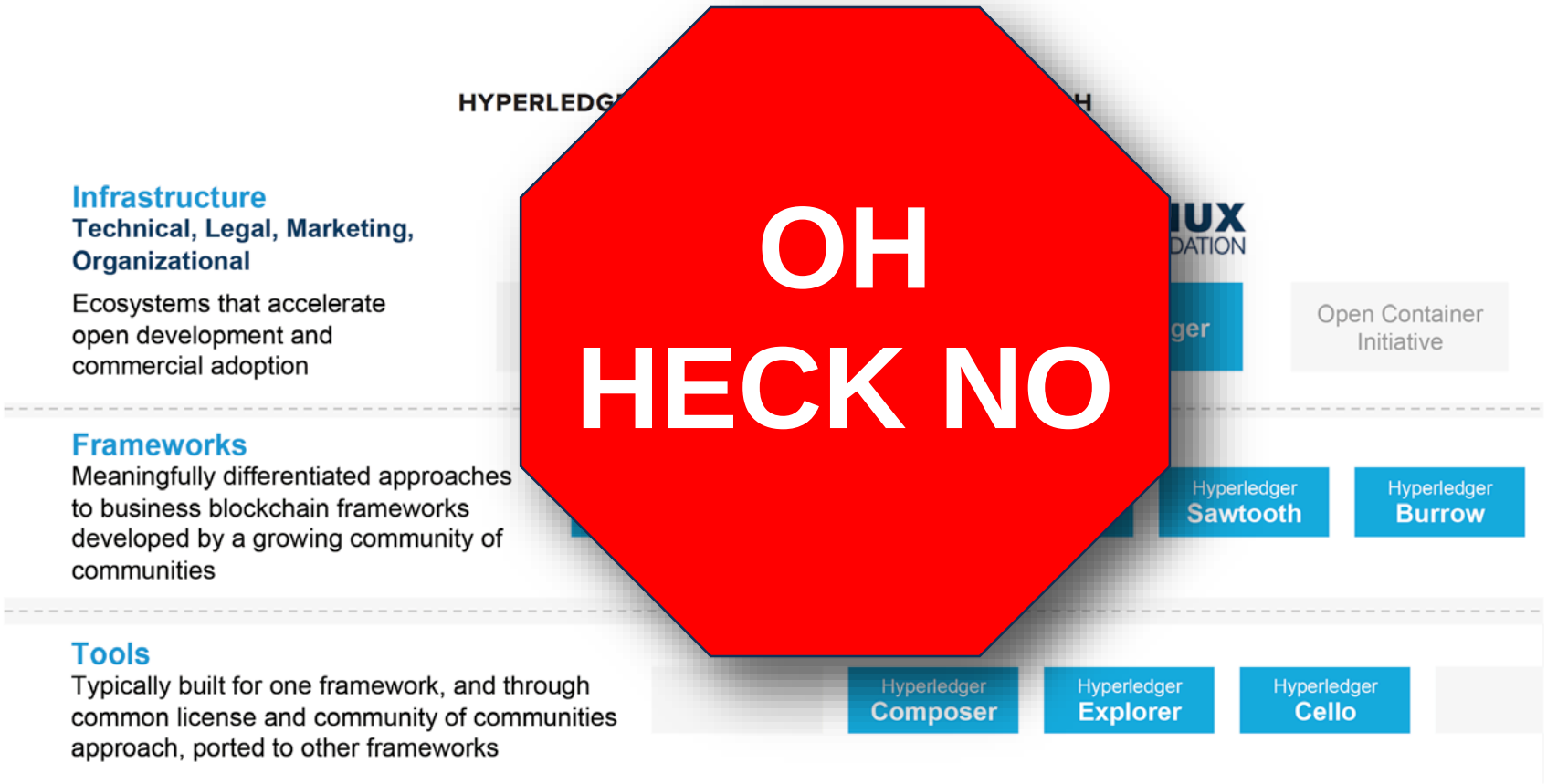




Hyperledger



Hyperledger



Hyperledger Fabric

High level – similar to Ethereum

Adds features to enable **permissioning** and **privacy**

Three types of accounts (called “nodes”):

1. Client — Initiates transactions
2. Peer — Maintains ledger state, commits transactions
3. Orderer — Communication service via *channels*

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)

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

Consensus alternatives

Algorithm	Properties
Proof of Work	• Probabilistic solution • Random winner, weighted by computational power
Proof of Stake	• Probabilistic solution • Random winner, weighted by stake in the overall system • "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

BLOCKCHAIN, bitpay, coins.ph, case, uphold, NETKI, coinplug, wyre, SNAPCARD, Streami, xapo, ripio, CIRCLE, ABRA, COINJAR, Ledger

EXCHANGES & CRYPTOCURRENCY TRADING

coinbase, Tech bureau Corp. - the Crypto-Fintech Laboratory -, BTCChina, KORBIT, BITKAN, Polychain Capital, QUOINE, kraken, BITSTAMP, bitt, PAYMIUM, BITSO, bitaccess, coinsecure, cryptofacilities, LUNO, bitFlyer, SHAPE SHIFT, BKCoin, Unocoin

P2P MARKETPLACES & P2P LENDING

Atlas, OpenBazaar, BTCjam

MERCHANT SERVICES

POSaBIT, Coinify, Purse, BitPesa, bitWAGE, loyyal, simplex, billon, BitGo, Align Commerce

ENTERPRISE SERVICES & CURRENCIES

Gem, 区块链数字资产平台, 小蚁 AntShares, blocko, FACTOM, orb, BIGCHAINDB, HASHED HEALTH, BLOCKCYPHER, colu.

SOCIAL & BROWSERS

brave, Reveal, blockstack

CRYPTOCURRENCY MINING

HASHRABBIT, BitFury

IoT, IDENTITY & CONTENT MANAGEMENT

BITMARK, mediachain, SatoshiPay, FILAMENT, ShoCard, evernym, Cambridge Blockchain, CHRONICLED, ascribe®

STORAGE, SECURITY & REGULATORY

Skry, CHAINALYSIS, ELLIPTIC, STORJ

CAPITAL MARKETS & FINANCIAL SERVICES

ripple, symbiont, PEERNOVA, LedgerX, Chain, Hijro, Blockstream, AXONI, Digital Asset Holdings, JU 矩阵金融 JUZHEN.IO, SOLIDX, PAXOS, DIGITAL CURRENCY GROUP, SETL, funderbeam, NEUFUND, CRYEX

CBINSIGHTS

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 0xa188e5a3da203f8ebc72ec7578532926dc1d3bec 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 Farkas

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

Overview | Comments

Transaction Information

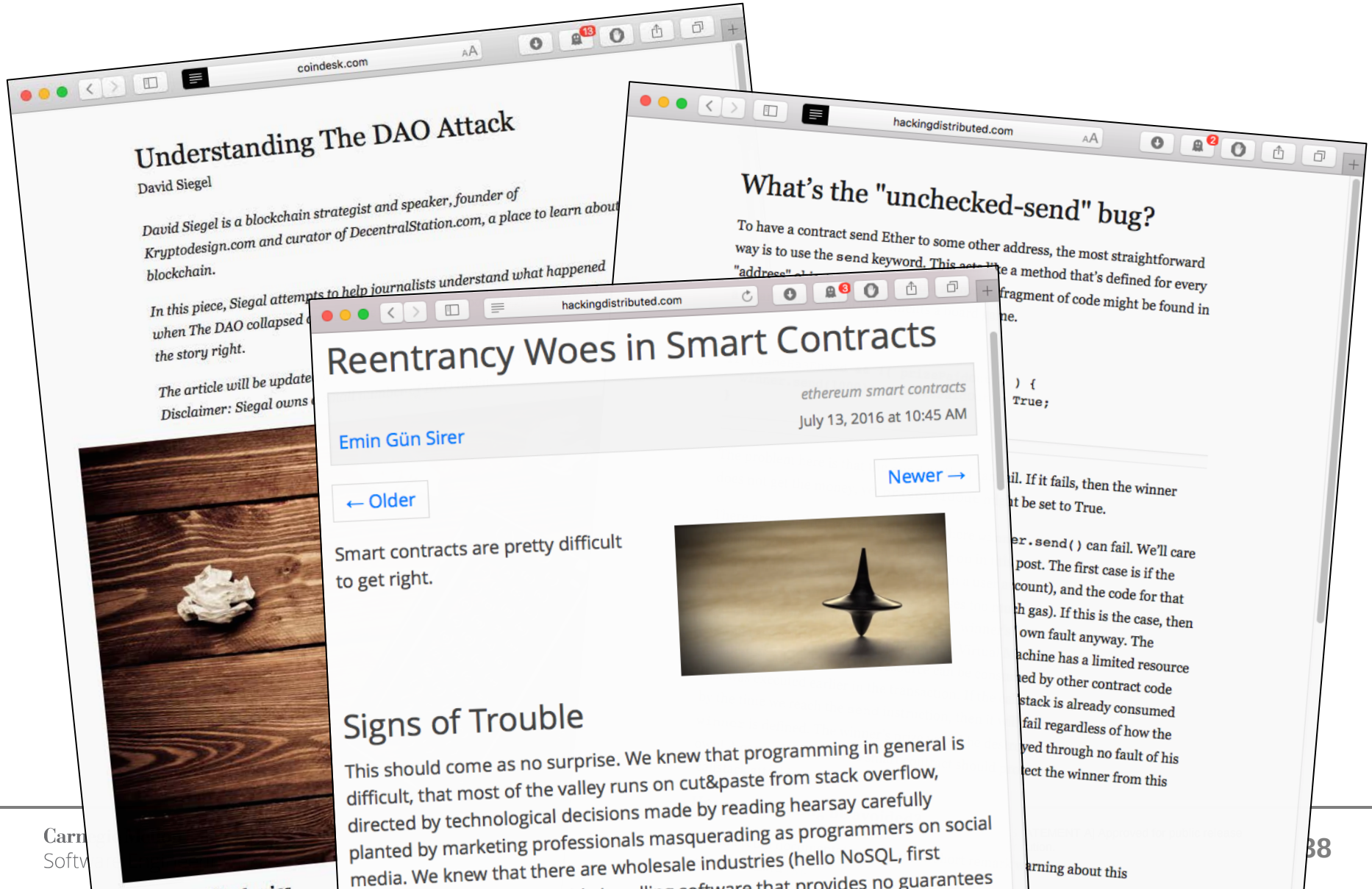
Tools & Utilities

TxHash:	0xa42a4535548a55390519ba936a5f12781d61fdafdf1c02657b12ca19895ecc18
TxReceipt Status:	Success
Block Height:	5100827 (118721 block confirmations)
TimeStamp:	20 days 3 hrs ago (Feb-16-2018 01:15:24 PM +UTC)
From:	0x9d207257f410303a779837fa0b55e7cafb15fec6
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:	0x60606040523415610000f57600080fd5b6040516060806105b8339810160405280805191906020018051919060200180516000805 4600160a060020a03338116600160a060020a0319928316178355600280549882169883169890981790975560048054968816968216 9690961790955560058054929096169190941617909355506104c991508190610092903960000f300606060405260043610610da576 3fffffff7c0100000000000000000000000000000000000000000000000000000000600035041663085 1a5381146100df57806317

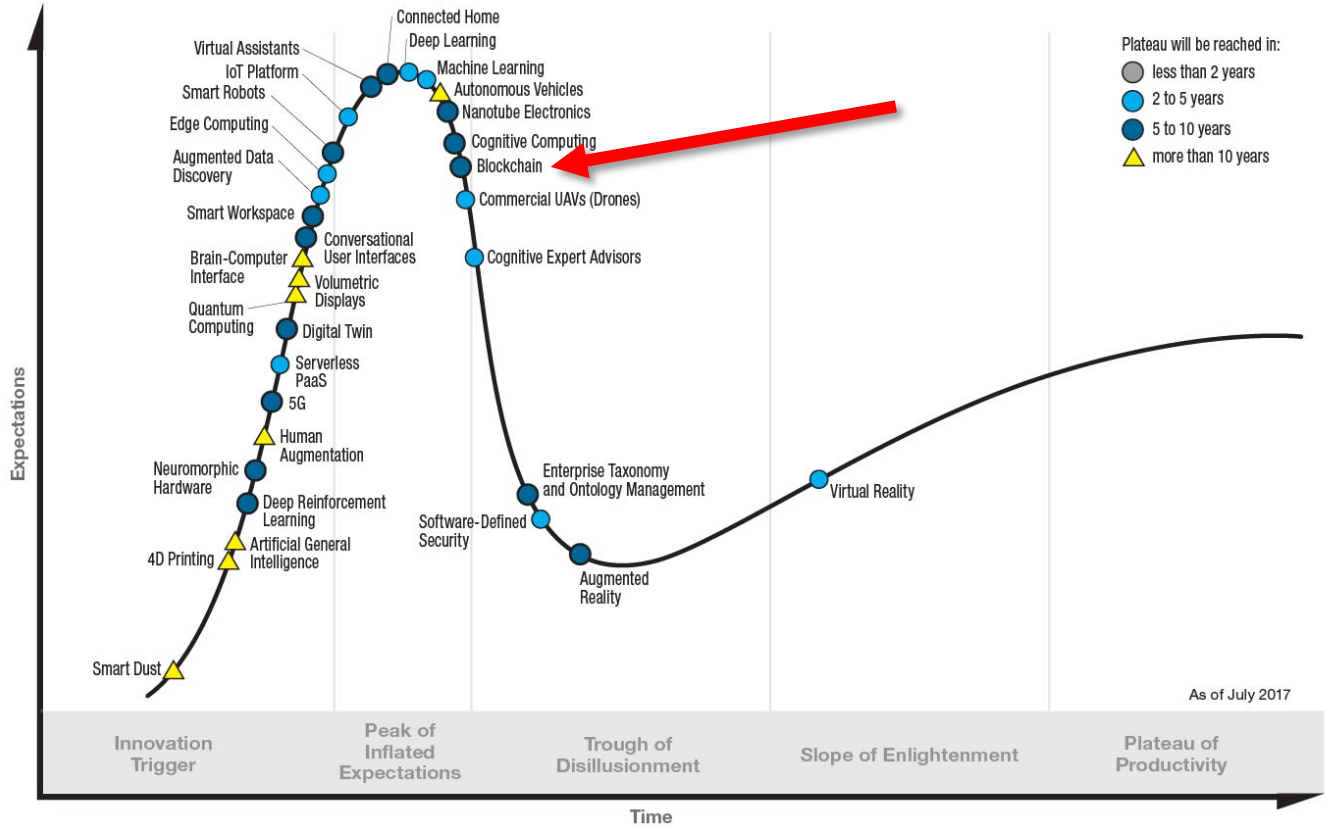
Convert To Ascii

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)

Gartner

Thanks!