

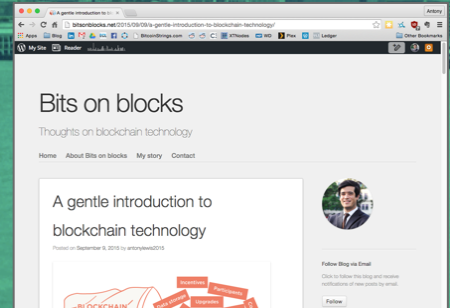


# FF16

## SIDELINE SUMMIT #1 Blockchain & Crypto: The brilliant basics and beyond 26 Jan 2016

**Antony Lewis**  
*Blockchain consultant  
Mentor, Startup Bootcamp FinTech SG*

@antony\_btc  
antony@bitsonblocks.net  
www.bitsonblocks.net



2013 / 14

- **Bitcoins**
- Bitcoin for everyone!
- Currency of the internet!
- Mass global adoption!
- Price, mining
- Virtual currencies
- Regulation of value transfer
- Scams, bankruptcies, Silk Road

2015

- **Blockchains**
- Blockchains for everything!
- Distributed ledgers
- Back office efficiencies
- Bitcoin for cross-border payments
- Bitcoin licences in US
- Bitcoin scalability

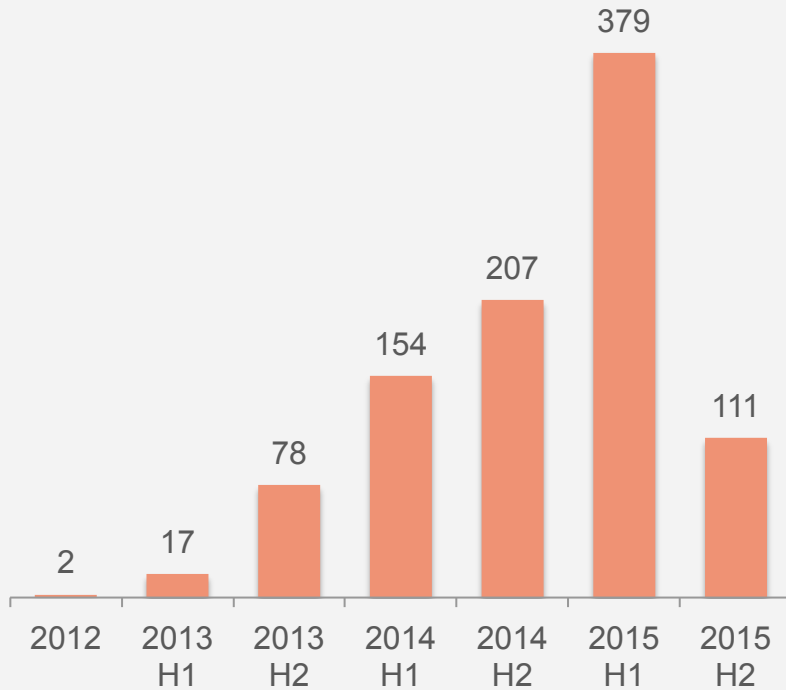
2016

- **Smart contracts**
- Shared ledgers for industries / governments
- Privacy vs transparency
- Scalability

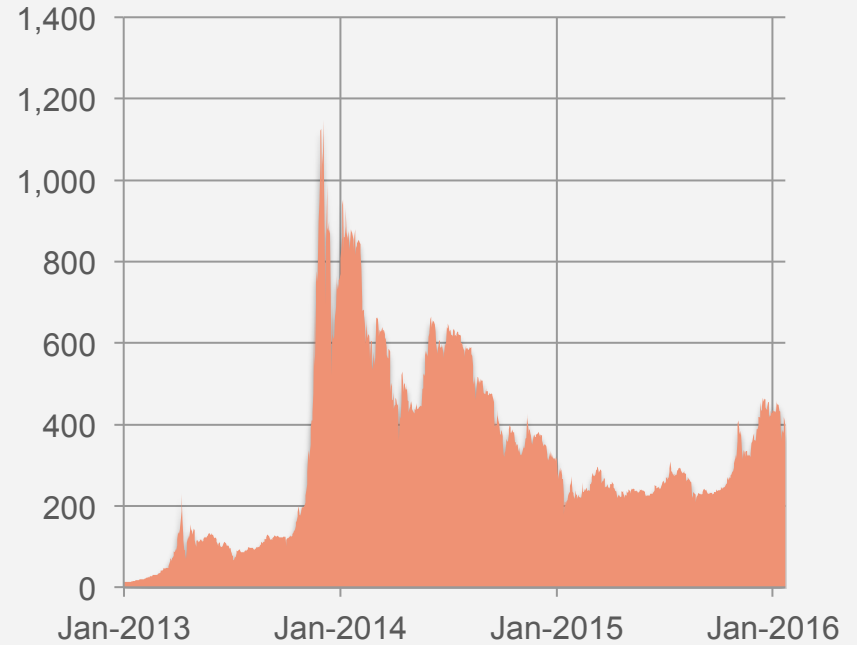


# THE FUNDING STORY - BITCOINS

## Publicly disclosed funding US\$m



## Bitcoin price US\$ per BTC



Source: <http://www.coindesk.com/bitcoin-venture-capital/>





Mike Hearn

Jan 15 · 18 min read

## The resolution of the Bitcoin experiment

Search Bitcoin blockchain...

Recent Blocks Chart Table

Height	Time	Miner	# tx	Block Value	Total Fees	Size
391,749	8m ago - 04-Jan 20:16	KNCminer	828	7,435.29309157	0.15469282	919,660 B
391,748	11m ago - 04-Jan 20:13	GHash.IO	1926	8,155.24409918	0.44422321	749,068 B
391,747	28m ago - 04-Jan 19:55	Slush	1149	6,162.02364364	0.21166204	749,235 B
391,746	35m ago - 04-Jan 19:48	F2Pool	2661	15,690.32350929	0.45387087	999,979 B
391,745	59m ago - 04-Jan 19:25	BitClub Network	1260	8,464.59176673	0.25470972	998,179 B
391,744	1h 08m ago - 04-Jan 19:15	AntPool	1696	11,637.16319187	0.30519275	920,064 B
391,743	1h 22m ago - 04-Jan 19:01	AntPool	1415	7,758.25586043	0.28373387	926,872 B
391,742	1h 33m ago - 04-Jan 18:50	AntPool	1058	8,140.55398159	0.22354992	919,489 B
391,741	1h 36m ago - 04-Jan 18:47	F2Pool	1287	7,526.75309818	0.20394481	999,766 B
391,740	1h 39m ago - 04-Jan 18:45	BitFury	2461	22,312.37360131	0.47520445	996,159 B
391,739	2h 03m ago - 04-Jan 18:20	AntPool	1736	9,002.44393527	0.25546217	933,796 B
391,738	2h 10m ago - 04-Jan 18:13	Slush	2212	20,340.40376476	0.45504844	749,138 B
391,737	2h 35m ago - 04-Jan 17:48	AntPool	1949	10,974.21178140	0.26763504	933,982 B
391,736	2h 43m ago - 04-Jan 17:41	BTCChina	1996	11,147.33313806	0.37077070	949,089 B
391,735	2h 54m ago - 04-Jan 17:30	F2Pool	1918	13,514.08757737	0.30345411	999,942 B
391,734	3h 03m ago - 04-Jan 17:20	BitFury	2681	19,943.18324530	0.47434414	996,148 B
391,733	3h 25m ago - 04-Jan 16:58	F2Pool	2210	10,445.16301857	0.32329187	999,965 B
391,732	3h 32m ago - 04-Jan 16:52	AntPool	3075	26,574.71165375	0.59391099	932,720 B

### Bitcoin Core

- Count data differently

### Bitcoin XT

- 8MB, doubling every 2 years

### Bitcoin Classic

- 2MB

### Bitcoin Unlimited

- User configured

Consensus is hard!  
Collaboration is hard!





- Raised \$52m
- ASX project
- JP Morgan (lead), Citi, PNC
- BNP Paribus, ABN Amro, Santander
- ASX, CME, Deutsche Boerse (Clearstream), DTCC, Accenture, Broadridge, ICAP



Consortium approach, subscription fees

- **Barclays**
- **BBVA**
- **CBA**
- **Credit Suisse**
- **Goldman Sachs**
- **J.P. Morgan**
- **RBS**
- **State Street**
- **UBS**
- Bank of America
- BNY Mellon
- Citi
- Commerzbank
- Deutsche Bank
- HSBC
- Mitsubishi UFJ Financial Group
- Morgan Stanley
- National Australia Bank
- Royal Bank of Canada
- Skandinaviska Enskilda Banken
- Société Générale
- Toronto-Dominion Bank

*Mizuho Bank, UniCredit, Nordea, BNP Paribus, Canadian Imperial Bank of Commerce, ING, Macquarie, Wells Fargo & Co  
BMO Financial Group, Danske Bank, Intesa Sanpaolo, Natixis, Nomura, Northern Trust, OP Financial Group, Banco Santander, Scotiabank, Sumitomo Mitsui Banking Corporation, U.S. Bancorp and Westpac Banking Corporation*



# A REAL-LIFE BLOCKCHAIN

Name	^	Date Modified	Size	Kind
▼ Bitcoin		Today 9:33 pm	--	Folder
bitcoind.pid		13 Aug 2015 10:15 pm	4 bytes	Document
▼ blocks		Today 8:15 am	--	Folder
blk00000.dat		16 Dec 2014 12:23 pm	134.2 MB	Document
blk00001.dat		16 Dec 2014 12:27 pm	134.2 MB	Document
blk00002.dat		16 Dec 2014 12:32 pm	134.2 MB	Document
blk00003.dat		16 Dec 2014 12:36 pm	134.2 MB	Document
blk00004.dat		16 Dec 2014 12:40 pm	134.2 MB	Document
blk00005.dat		16 Dec 2014 12:52 pm	134.2 MB	Document
blk00006.dat		16 Dec 2014 12:56 pm	134.2 MB	Document
blk00007.dat		16 Dec 2014 1:01 pm	134.2 MB	Document
blk00008.dat		16 Dec 2014 1:05 pm	134.2 MB	Document
blk00009.dat		16 Dec 2014 2:48 pm	134.2 MB	Document
blk00010.dat		16 Dec 2014 2:51 pm	134 MB	Document
blk00011.dat		16 Dec 2014 2:56 pm	134 MB	Document




# DIVE INTO A BLOCK

```
{
  "status": "success",
  "data": {
    "hash": "000000000002917ed80650c6174aac8dfc46f5fe36480aaef682ff6cd83c3ca",
    "confirmations": 269574,
    "size": 4179,
    "height": 123456,
    "version": 1,
    "merkleroot": "0e60651a9934e8f0dec1c5fde39309e48fca0c1c84a21ddfd95033762d86c",
    "tx": [
      "5b75086dafecde555fc8f9a810d8b10df57c46f9f176ccc3dd8d2fa20edd685b",
      "e3d0425ab346dd5b76f44c222a4bb5d16640a4247050ef82462ab17e229c83b4",
      "137d247eca8b99dee58e1e9232014183a5c5a9e338001a0109df32794cdcc92e",
      "5fd167f7b8c417e59106ef5acfe181b09d71b8353a61a55a2f01aa266af5412d",
      "60925f1948b71f429d514ead7ae7391e0edf965bf5a60331398dae24c6964774",
      "d4d5fc1529487527e9873256934dfb1e4cdbc39f4c0509577ca19bfad6c5d28f",
      "7b29d65e5018c56a33652085dbb13f2df39a1a9942bfe1f7e78e97919a6bdea2",
      "0b89e120efd0a4674c127a76ff5f7590ca304e6a064fbc51adffbd70e3a3deef",
      "603f2044da9656084174cfb5812feaf510f862d3addef70cacce3dc55dab446e",
      "9a4ed892b43a4df916a7a1213b78e83cd83f5695f635d535c94b2b65ffb144d3",
      "dda726e3dad9504dce5098dfab5064ecd4a7650bfe854bb2606da3152b60e427",
      "e46ea8b4d68719b65ead930f07f1f3804cb3701014f8e6d76c4dbdc390893b94",
      "864a102aedf53dd9b2baab4eeb898c5083fde6141113e060cb664c41fe15e1f"
    ],
    "time": 1305200806,
    "nonce": 2436437219,
    "bits": "1a6a93b3",
    "difficulty": 157416.40184365,
    "chainwork": "000000000000000000000000000000000000000000000000000000000000000541788211ac227bc",
    "previousblockhash": "0000000000000b60bc96a44724fd72daf9b92cf8ad00510b5224c6253ac40095",
    "nextblockhash": "00000000000129f5f02be247070bf7334d3753e4ddee502780c2acaec6d66"
  },
  "code": 200,
  "message": ""
}
```

```
"vins": [
  {
    "address": "184CQ7agrApMYpnKTzWnsMjV9Wx3raRw7S",
    "is_nonstandard": false,
    "amount": "-50.00000000",
    "n": 1,
    "type": 0,
    "vout_tx": "4600bf5f3d49660a546c1b9acd3e6b85479ab227115f741cf12e50506ab24b54"
  },
  {
    "address": "1Atyy5h4SSdqWRuS8pzxgTb4bMe7ZpdunP",
    "is_nonstandard": false,
    "amount": "43.61000000",
    "n": 0,
    "type": 1,
    "is_spent": 1
  },
  {
    "address": "18CisDmjM1MmM1MjtqUHPgmoLhZcSJJTKD",
    "is_nonstandard": false,
    "amount": "6.39000000",
    "n": 1,
    "type": 1,
    "is_spent": 1
  }
],
"fee": "0.00000000",
"days_destroyed": "995.83",
"is_unconfirmed": false,
"extras": null
},
"code": 200,
"message": ""
}
```



# BITCOIN'S BLOCKCHAIN IS TRANSPARENT!

Transaction `5d246d10bc07ae5e8c27b06a1c480ad76376cdf4235dc3d5b978e4976c863e21` 

Details		Volumes	
Block	<b>Unconfirmed</b>	Total Inputs	0.24940000
Time Received	25 Jan 2016 01:02:31 (a few seconds ago)	Total Outputs	0.24920000
Size	294 B	Miner Fee	0.00020000
Fee/size	68.02721088 sat/B		

Inputs (1)	Outputs (4)
<code>&lt; 12utH6R9Vb86x1DXbJdMSq5GyAuxQCsc1w</code>	<code>*AkrMVAsVeoYYv5F8jY1NBSX1fa7RBSie1</code>
<code>-0.24940000</code>	<code>1J7Sn4qjdR4q6GNCTszZDZgRRWBv277fMd</code>
	<code>1C69u1vCRzXeD6gca1kG3SWBBY3YDDz5kC</code>
	<code>13riwEZUEYfuxPMwilMpipZcBQLBTZ6ELXC</code>

Source: [www.tradeblock.com](http://www.tradeblock.com)



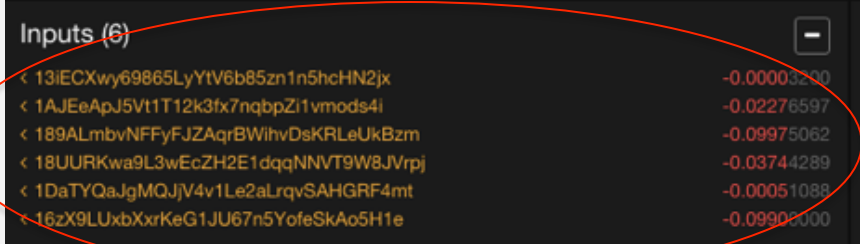

# BITCOIN'S BLOCKCHAIN IS REALLY TRANSPARENT!

Transaction 00965d2eea9e302bc8836e5d8e909ddd4908efabbc5e4aefdbe9f6d64d212835 ₿

Details		Volumes	
Block	394,817 (6 confs)	Total Inputs	0.25950236
Time Received	25 Jan 2016 00:15:02 (an hour ago)	Total Outputs	0.25940236
Size	963 B	Miner Fee	0.00010000
Fee/size	10.38421599 sat/B		

Inputs (6)	Outputs (2)
< 13IECXwy69865LyYtV6b85zn1n5hcHN2jx	> 12utH6R9Vb86x1DXbJdMSq5GyAuxQCsc1w
< 1AJEeApJ5Vt1T12k3fx7nqbpZi1vmods4i	> 18xDgr6R9SL5dDNgY MaoXpFn6KCJc6qPtg
< 189ALmbvNFFyFJZAqrBWihvDsKRLeUkBzm	
< 18UURKwa9L3wEcZH2E1dqQNNVT9W8JVrpj	
< 1DaTYQa.JgMQJjV4v1Le2aLrqvSAHGRF4mt	
< 16zX9LUXbXxrKeG1JU67n5YofeSkAo5H1e	



Source: [www.tradeblock.com](http://www.tradeblock.com)



**Public blockchains** attempt to solve for agreement about **valid transactions** across a **censorship-resistant network** where some small portion of the **participants may behave dishonestly** and there is **no legal recourse**.



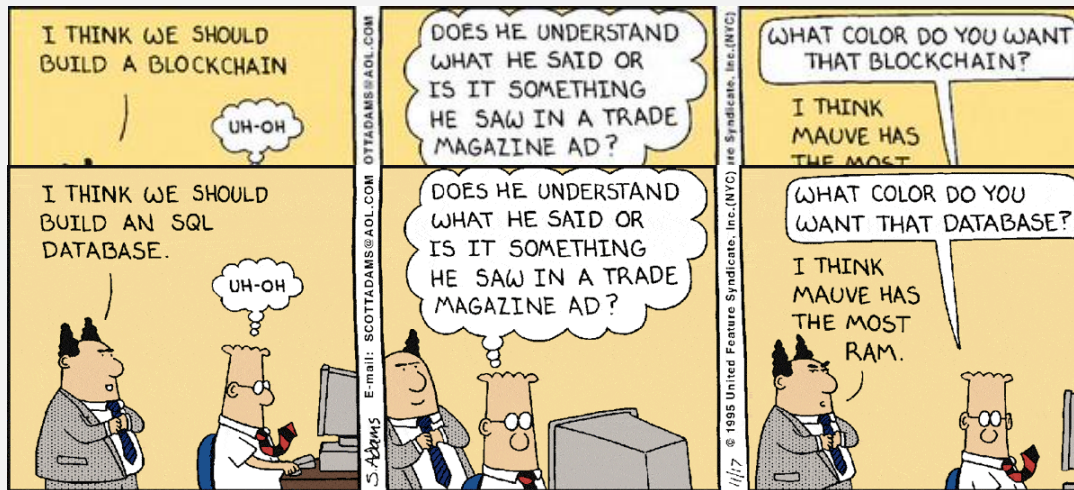
Bitcoin's blockchain is a bunch of data about transactions stored in blocks that refer to each other in a linear chain.



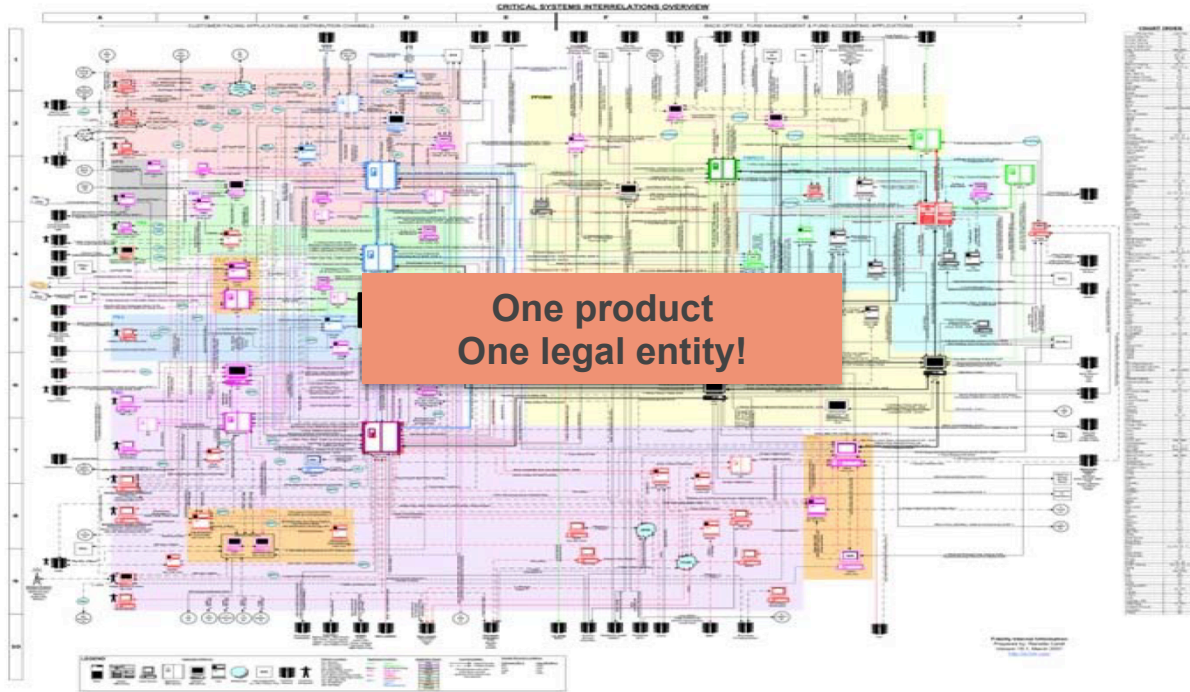
Ethereum's blockchain is a bunch of data about transactions **and imbedded instructions that are automatically executed by computers**, stored in blocks that refer to each other in a linear chain.

# PRIVATE BLOCKCHAINS

- **Private blockchains** can be “bitcoin-flavoured”, “Ethereum-flavoured” or build your own, with your own spec, for a known set of participants.
- **Shared ledgers** don’t even need data to be in blocks (hence, shared ledgers), or even distributed.
- Don’t get confused between:
  - Blockchains
  - Shared ledgers
  - Distributed data
  - Digital identities
  - Payments
  - Encrypted stuff
- Think hard about privacy vs transparency!



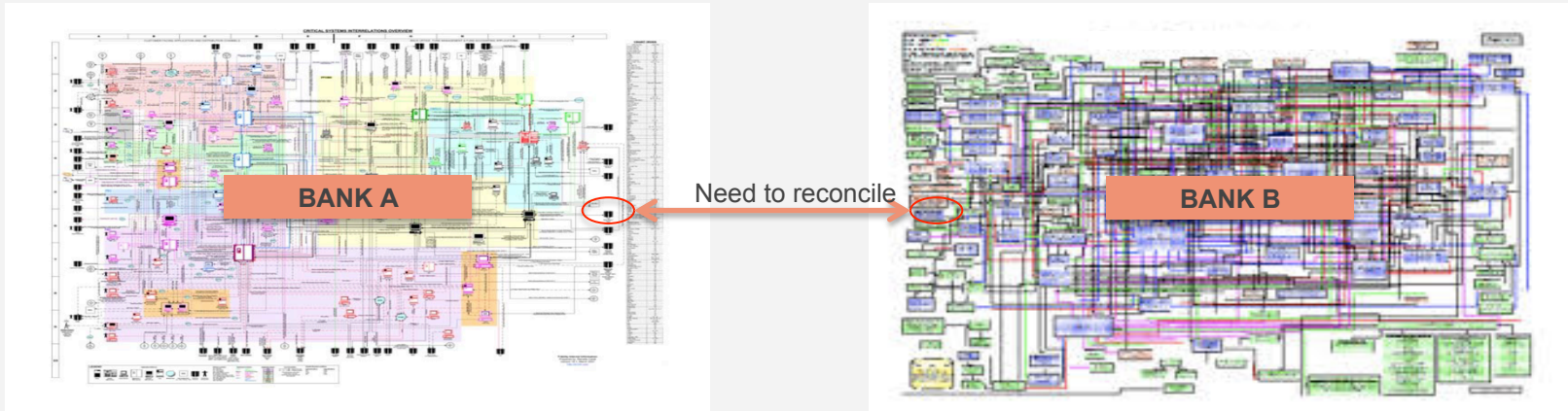
# BLOCKCHAINS FIXING ENTERPRISE ISSUES



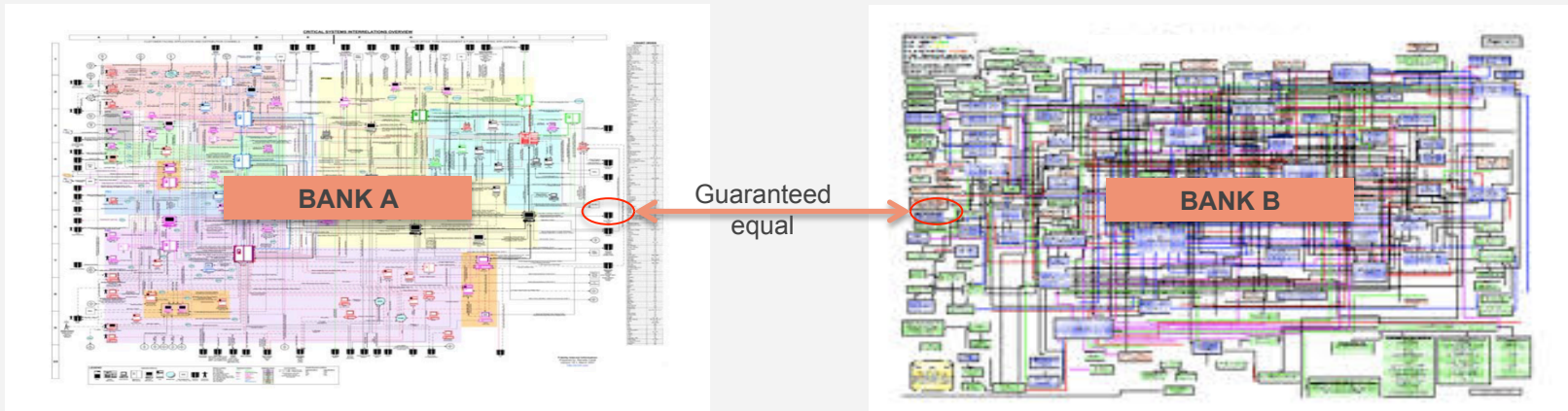
Source: [https://insights.sei.cmu.edu/assets/content/carriere-panel-saturn2012\\_Page\\_6.png](https://insights.sei.cmu.edu/assets/content/carriere-panel-saturn2012_Page_6.png)

# THE REAL PROBLEM WITH BANKING TECHNOLOGY

Before



After



Source: <http://www.nqlogic.com/2009/07/cit-definition.html>





## Introducing: Ethereum Blockchain as a Service (EthBaaS)

incubating disruption

Marley Gray – Director Technology Strategy US FS @ Microsoft



Source: [https://devcon.ethereum.org/slides/ethBaas\\_gray.pdf](https://devcon.ethereum.org/slides/ethBaas_gray.pdf)



# BLOCKCHAINS IN THE MEDIA

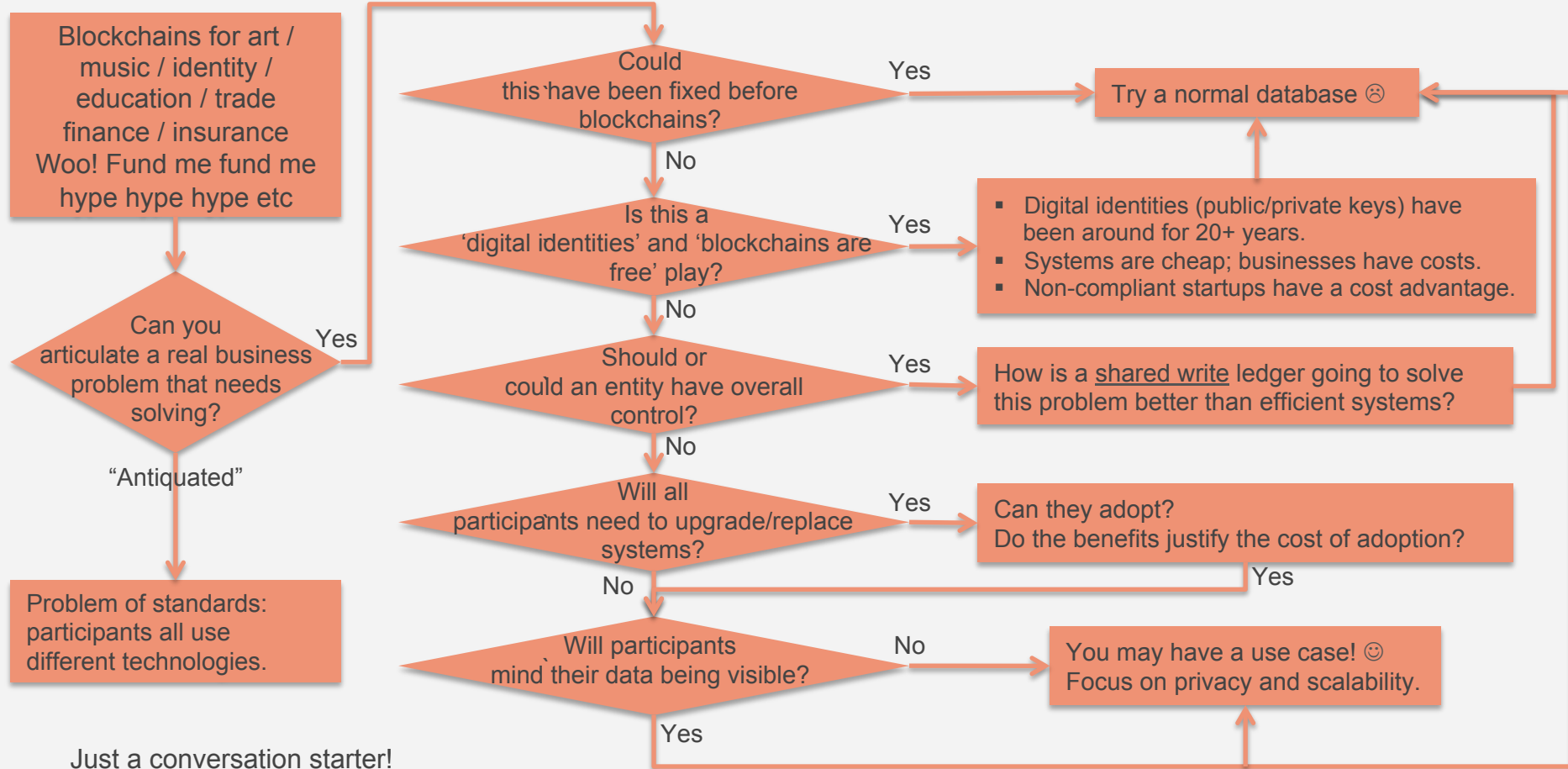
The screenshot shows the 'Blockchains' section of the Ethereum Marketplace. On the left is a navigation sidebar with categories like 'Everything', 'Compute', 'Web + Mobile', 'Data + Storage', 'Data Analytics', 'Internet of Things', 'Networking', 'Media + CDN', 'Hybrid Integration', 'Security + Identity', 'Blockchains' (highlighted), 'Management', and 'Container Apps'. The main content area is titled 'Blockchains' and features a search bar. Below the search bar, there are two rows of product cards. The first row is labeled 'Recommended' and contains five cards, all for 'ETH Baas - Ethereum Blockchain as a Service' by ConsenSys. The second row contains five cards for 'Ethereum BlockApps' by ConsenSys, with the first card also listing 'Microsoft' as a provider. The cards describe various services such as 'Ethereum Node Windows Server Consensys Tools', 'Ethereum Private Blockchain Network', 'Ethereum Blockapps Strato Windows', and 'Ethereum Blockapps Strato Ubuntu'.

Category	Product Name	Provider
Recommended	ETH Baas - Ethereum Blockchain as a Service	ConsenSys
	ETH Baas - Ethereum Blockchain as a Service	ConsenSys
	ETH Baas - Ethereum Blockchain as a Service	ConsenSys
	ETH Baas - Ethereum Blockchain as a Service	ConsenSys
	ETH Baas - Ethereum Blockchain as a Service	ConsenSys
Ethereum BlockApps	Ethereum BlockApps Strato Windows	ConsenSys
	Ethereum Blockapps Strato Windows Sandbox	ConsenSys
	Ethereum Blockapps Strato Ubuntu	ConsenSys
	Ethereum BlockApps Strato Windows	ConsenSys
	Ethereum BlockApps Strato Ubuntu	ConsenSys

Source: [https://devcon.ethereum.org/slides/ethBaas\\_gray.pdf](https://devcon.ethereum.org/slides/ethBaas_gray.pdf)



# BLOCKCHAIN CHEAT SHEET v0.1



Just a conversation starter!







# FF16

## SIDELINE SUMMIT #1 Blockchain & Crypto: The brilliant basics and beyond 26 Jan 2016

**Antony Lewis**  
*Blockchain consultant  
Mentor, Startup Bootcamp FinTech SG*

@antony\_btc  
antony@bitsonblocks.net  
www.bitsonblocks.net

