



---

# TOP TEN OBSTACLES FOR DISTRIBUTED LEDGERS

SARAH MEIKLEJOHN (UCL)

# TOP TEN OBSTACLES [M18]

---

- 10 Usability
- 9 Governance
- 8 Comparisons
- 7 Key Management
- 6 Agility
- 5 Interoperability
- 4 Scalability
- 3 Cost-Effectiveness
- 2 Privacy
- 1 Scalability

# TOP TEN OBSTACLES

---

## **10 Usability**

9 Governance

8 Comparisons

7 Key Management

6 Agility

5 Interoperability

4 Scalability

3 Cost-Effectiveness

2 Privacy

1 Scalability

1CAbbXyRpdtpA6TKXss2Ydd1gWfPGyCJdK (0.49351286 BTC - Output)  
 17z7pTV1n7gVy6J7Y9uKUqi1VPqyAdwS73 (0.334 BTC - Output)  
 1ArXhpbJcJb7ng2mj6uCW8NR47wDCGu (0.33360272 BTC - Output)  
 1624YkFkRw8yGtg484yznDpifBSAj28qLv (0.329 BTC - Output)  
 1E1Vtqb6jHYfT6JEuKTNF24Z1rAsc34QMw (0.32271551 BTC - Output)  
 17rmhXWZQrwVBG33p11LPBvZiiqRBwYuo5 (0.49214683 BTC - Output)  
 1DcXDP8cTrtW7LNxh7Rr9wpQ1UW6ynKPPq (0.29779446 BTC - Output)  
 1FwZa5NEGPMaUk9dww6HADkGTBMrybFMe9 (0.308 BTC - Output)  
 15a8ciZjezFVBEUgA5JmsbrDuEsAUb2q3q (0.32024259 BTC - Output)  
 1KMwYxPyhrFQfTUnt5sRqajQNSUwCZot3J (0.34964265 BTC - Output)  
 18P4s3AtsSXq5v417ucEaPizACqmnKzP7F (0.29530619 BTC - Output)  
 1NM7nn2E3RDKkn91NSxzF91rhnVbqsotZD (0.5160944 BTC - Output)  
 1FniswCdYUhbUmyp8yLU6yXmbuupiXbrPL (0.3326536 BTC - Output)  
 1Py9pYrZdAGJRpngQvJod7Xp4KXTnxVG24 (0.33238122 BTC - Output)  
 1DeivCdXGjDQa68Ddbd3p4vGbgcQD7a5LA (0.31798686 BTC - Output)  
 1GveNJUw2982pqD7tyNgYGWV53wDaqnmvV (0.31777828 BTC - Output)  
 12yiM7SGE7LT7EqPVZxgMkUN2C2go72SgD (0.32411878 BTC - Output)  
 19MkjA25FyVYMoHjiJdh8xsQ9gXfM5McDc (0.33803037 BTC - Output)  
 1LgcFveG3Aw1tkL25W5EMr2Cw3z5mBeQse (0.318 BTC - Output)  
 13Lxtz8eGATA1jig6hnbGb4N9C8wq54vLq (182.30544491 BTC - Output)  
 1EfCXe188LoQnHfvPQR1xvAwBzKYJ3ziDS (0.336 BTC - Output)  
 144WPEuNgGiEPFBgqgKjvXiNwT3KdR2uBu (0.331 BTC - Output)  
 1LHVP7znzpTv4wzMkWWvkcWMmaPrUcQzuB (0.49217385 BTC - Output)  
 1BYzrWzFSTU47Xdkid87gHpHs7eXbwUZwi (0.52646585 BTC - Output)  
 148LP8cPVBzzXVrVQdLUnswNH4dfPSHo3a (0.31353747 BTC - Output)  
 1L52zb7Yj3m4rYNSszhA4PKMEpi8XqezFz (0.3702 BTC - Output)  
 1FcYMAAtG57ZSvDbTCz7fBDQxA9XfvoXqR9 (0.49522705 BTC - Output)  
 1PN4WV39WshZNNmkkAHaB6b61YkX1qbRDP (0.3471018 BTC - Output)  
 19nDjzrd61B8e7ZoYrnqGiCL9QufooU7xF (0.51101907 BTC - Output)  
 1MSZE1TYTdqhzkoKLWzSSduHtF4omouM21 (0.350404 BTC - Output)  
 14gVdGPDYPzrnrZtQ1Nubu3G9GVoDLd9q (0.34499411 BTC - Output)  
 1BMSVaDpGV7T8TxYo1BkJs33bhkB7rE7x (0.33990561 BTC - Output)  
 1PLmWVRe6TtdvCkwcVyGDRdPm67BiXXGQM (0.32806178 BTC - Output)  
 1EVi1zMtEiFhvuR5TZCuX6NYhh8xMsrNw (0.34360208 BTC - Output)  
 1BdabhFXRbUN2bXH5nNqtnM6A9JRoesn1A (0.349462 BTC - Output)  
 1KGQzrkzPiQ82hV7QKQagGf67emidnptgi (0.49903187 BTC - Output)  
 1Z4NnmAC1Z4E7MnGvrvc22hb8CmZWZVEj (0.32618186 BTC - Output)



1MQ9wTnSMABoPLo6uze7rkW969GAuifvKM - (Spent) 1.11009124 BTC  
 1JMx2YQq8hDT68KwdpcotADE5qanRJHhag - (Spent) 1.03263711 BTC  
 1JTr8iWdjwTKnsaHC6yMPAxbSePDLpqzeW - (Spent) 0.96532807 BTC  
 1EP3sDKzeNHmPFsE7nXyeEpSoSbyVuva4R - (Spent) 0.99034642 BTC  
 1NdLcTXm1KossL3m3bg3n3izQt3wjezXmQ - (Spent) 0.95985165 BTC  
 157DkvZ5fdoyui9SBnbnmSs9nRz31e2mh56 - (Spent) 1.0460556 BTC  
 13Cst9ErTxDfYNe39BuZA2Pqiyf3FLzUT - (Spent) 1.04012544 BTC  
 15TyYkyZWk8Xm7jaSE5ug5a9fBMNqxMUTV - (Spent) 1.09853614 BTC  
 1LbmSrETzEfWPZJojsA2Vq7NmMZ8AnNHPBH - (Spent) 0.99762768 BTC  
 1APaJRKUtBSJHNSqqcBHmuCeRp4KNU6zBz - (Spent)  
 1PtLzhHkCywHf8St3TNb8xudiSDdVU6XTw - (Spent) 1.04519906 BTC  
 13EfNEbVpmGpc8aCzKYuymysHrHodTEiP5 - (Spent) 1.03320177 BTC  
 1hBgKb7YGSSGb64d67svTvifiFCZdSFdm - (Spent) 0.99505215 BTC  
 1P2dJRewoeEsKdCXVvSVZwN29EgTxpyqYn - (Spent) 1.10898935 BTC  
 1KUfW1bHptXRj5N6PzWBCxLr8Xp5mquoDz - (Spent) 1.03873536 BTC  
 1CjHhyKESaXdyoCdG3q2QSS2P2TcUFd43V - (Spent) 1.07513614 BTC  
 13ef6gEBpRBnSZnbu6efY4iY35bRnWhEsW - (Spent) 0.9360219 BTC  
 1AxRUvU9LCqtszERgmqb5KU5bT5peTxAuU - (Spent) 0.94561868 BTC  
 1bfwZ9KaB4miraL1QTitPB7Ke2VjN8bra - (Spent) 1.06755426 BTC  
 13ykZwWajKpH2r6qr5XqXCJmQ8CqPPxCMV - (Spent) 1.12150712 BTC  
 194G5fwgUApHCGFKM1vJPuBotVgWXMtW71 - (Spent) 0.98511548 BTC  
 1N9mFfPwUpoEUGurnQngCPp5opg4hD8aua - (Spent) 1.02630932 BTC  
 1Jc3HLyKqXbEhM6D73WjGBDuvfYjVjTqP - (Spent) 0.9491876 BTC  
 1363BvZVEx6dn2DwciuKnRktEWFJDNdTbv - (Spent) 0.94748384 BTC  
 1KYjfqkyx1gADXK3dfz3hKgaMW6sf6nuZd - (Spent) 0.96147492 BTC  
 1QDpuuktmMDo9EQMzD4GgJeNSKNAch23AN - (Spent) 0.90706647 BTC  
 1.04059457 BTC  
 14qWyTg79UYBvLF9D1hoayr3g1QU8AApC6 - (Spent) 1.12381189 BTC  
 1GLUmZSS7sWs2gQKLKbFBQ1HyH5v8BG8Qy - (Spent)  
 12dPDGaUtsvxEeovKZkrhupmyevkySKmzN - (Spent) 0.94860091 BTC  
 1GXPeZVb2YV5YdnpatVG1mZuJLU6wv7sXt - (Spent) 1.07438381 BTC  
 1795pWUsNYE6DL3qcAJDDjFyPTNk33eHxf - (Spent) 0.94347978 BTC  
 16TaRnwEXKJpvSe3UpEpJgZ8cthkY9bDL - (Spent) 1.12598 BTC  
 1W1KZVo4LmfhtD83avCB4v2SvKZxXSejU - (Spent) 153.48631148 BTC  
 1DxVSWmuCcVHND2AYkFLhoonwaN9CZ6bRW - (Spent) 1.10072263 BTC  
 1.00659829 BTC  
 1L5d7WsjU7hkG3D5nTnncNMx1VSJ6LRM9U - (Spent) 0.9948825 BTC  
 1ADCq8gmV1mjMFujAvNEWuz1fvRuAZJVzG - (Spent) 1.05596004 BTC  
 1vDC2eMKwC2YMGqA57L6qWki7HphQd12Q - (Spent) 1.12557235 BTC  
 1jhqJLhcnmC9bX9Db6VqV3EH9DbxeYq4v - (Spent) 1.04838227 BTC  
 1QFLhpRtCxYWhu1XbZHZ9tAhHepnYLZZww - (Spent) 0.95676223 BTC  
 1FrrK3tbNcABVpjbir1KyyTrPvgPzhAUob - (Spent) 1.0807014 BTC


TxHash: 0x6636118adf44427c0f14ea23c16019e25fc119b7b494467956360618385bf2b3

TxReceipt Status: **Success**

Block Height: **5821793** (80 block confirmations)

TimeStamp: 21 mins ago (Jun-20-2018 09:29:35 AM +UTC)

From: **0x35632b6976b5b6ec3f8d700fabb7e1e0499c1bfa**

To: Contract **0x06012c8cf97bead5deae237070f9587f8e7a266d** (CryptoKittiesCore) 

Value: 0.008 Ether (\$4.22)

Gas Limit: 119977

Gas Used By Txn: 79985

Gas Price: 0.000000003 Ether (3 Gwei)

Actual Tx Cost/Fee: 0.000239955 Ether (\$0.13)

Nonce & {Position}: 433 | {94}



Input Data:

```
Function: breedWithAuto(uint256 _matronId, uint256 _sireId)
```

```
MethodID: 0xf7d8c883
```

```
[0]: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000c5858
```

```
[1]: 000000000000000000000000000000000000000000000000000000000000000000000000000000000000000ad3e7
```

[Convert To UTF8](#)

# TOP TEN OBSTACLES

---

10 Usability

**9 Governance**

8 Comparisons

7 Key Management

6 Agility

5 Interoperability

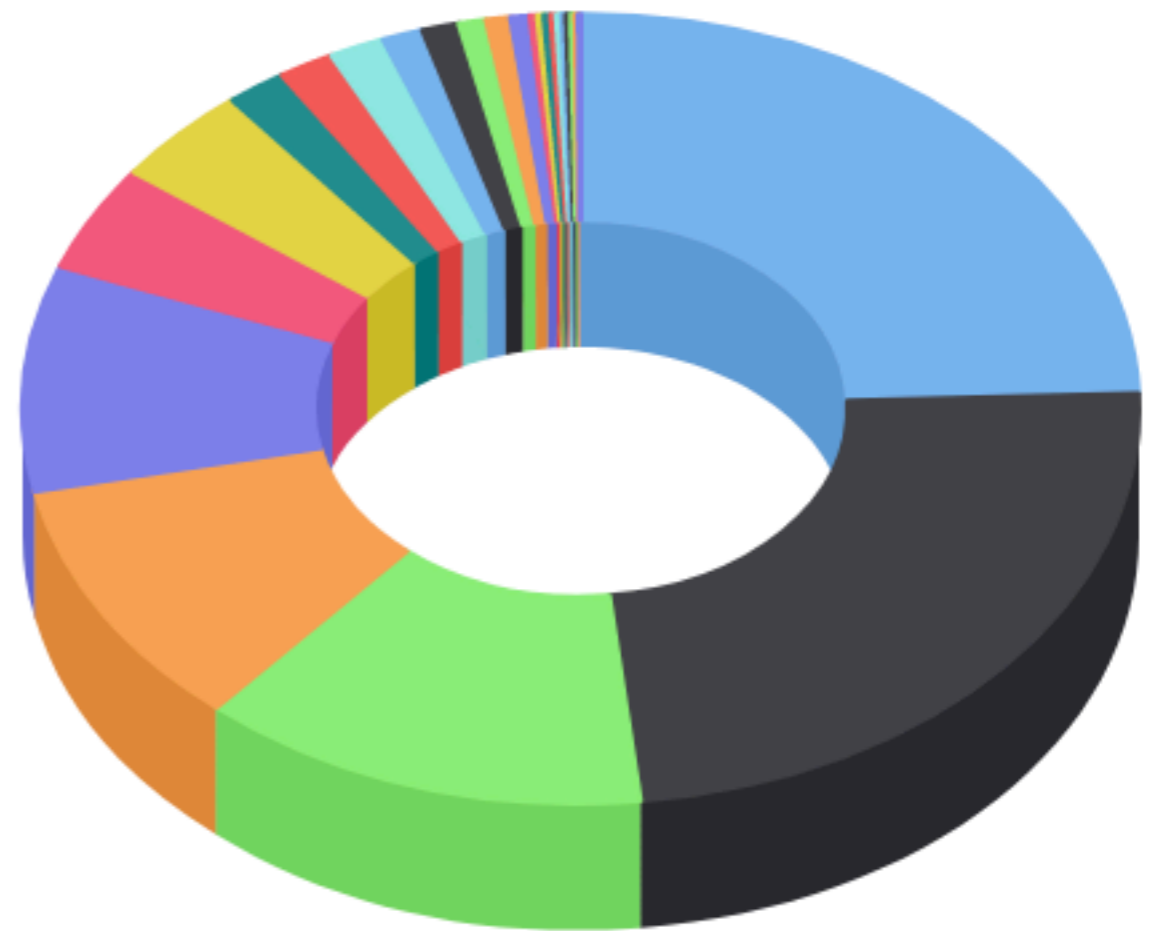
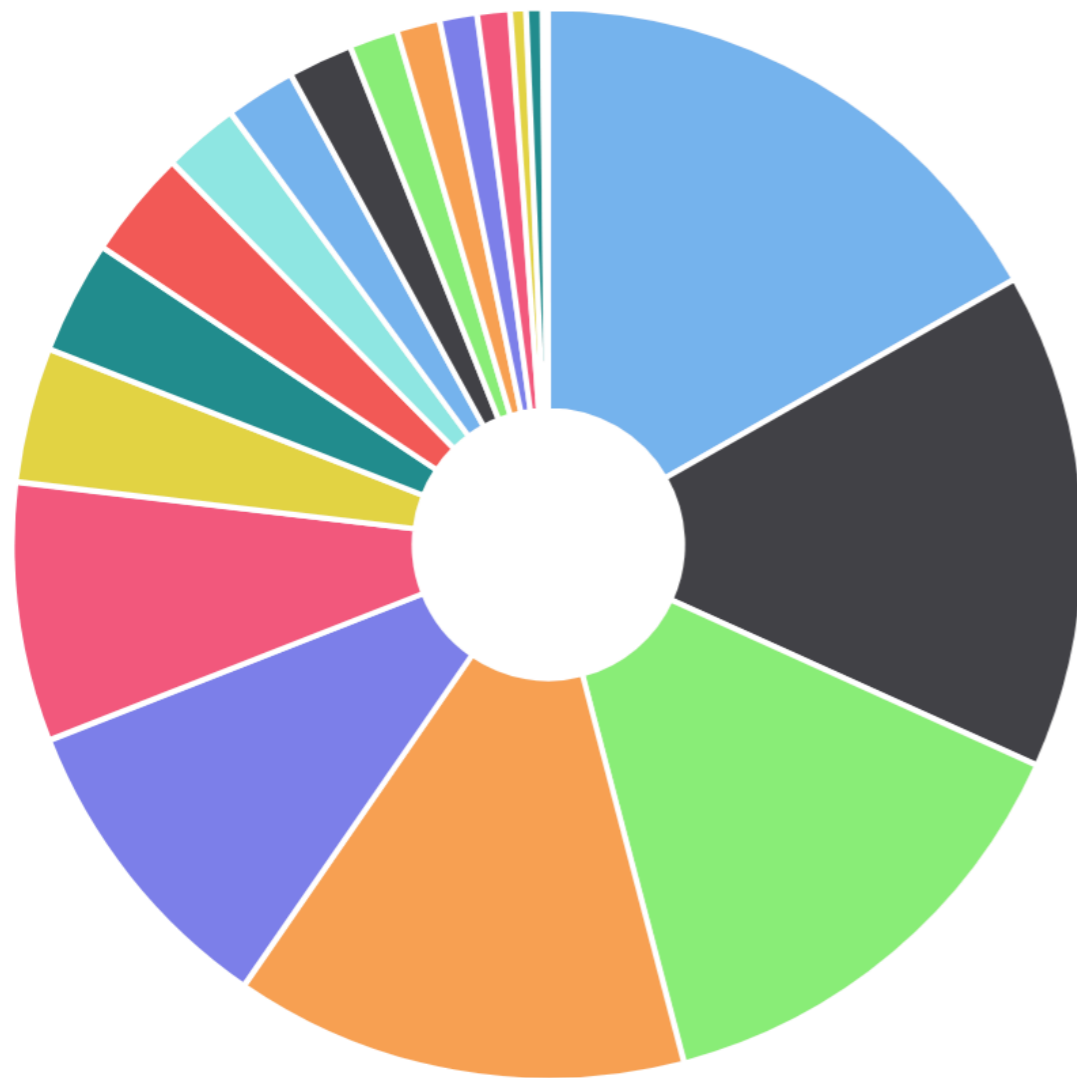
4 Scalability

3 Cost-Effectiveness

2 Privacy

1 Scalability

# MINING CENTRALIZATION

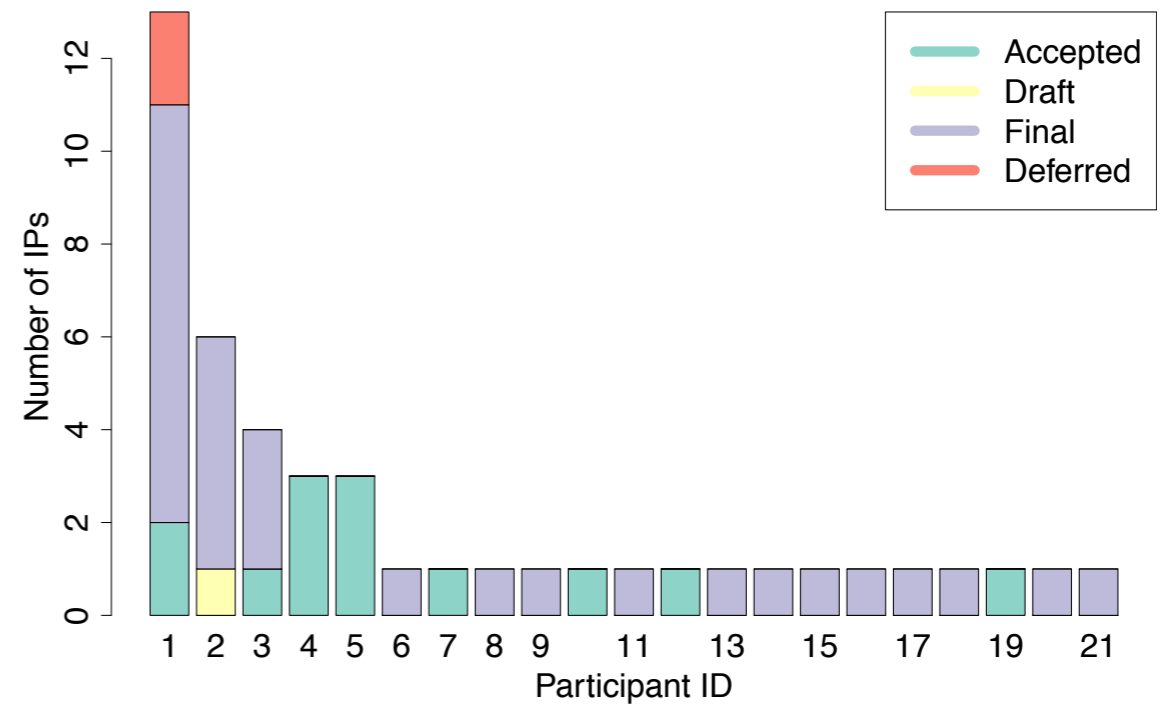
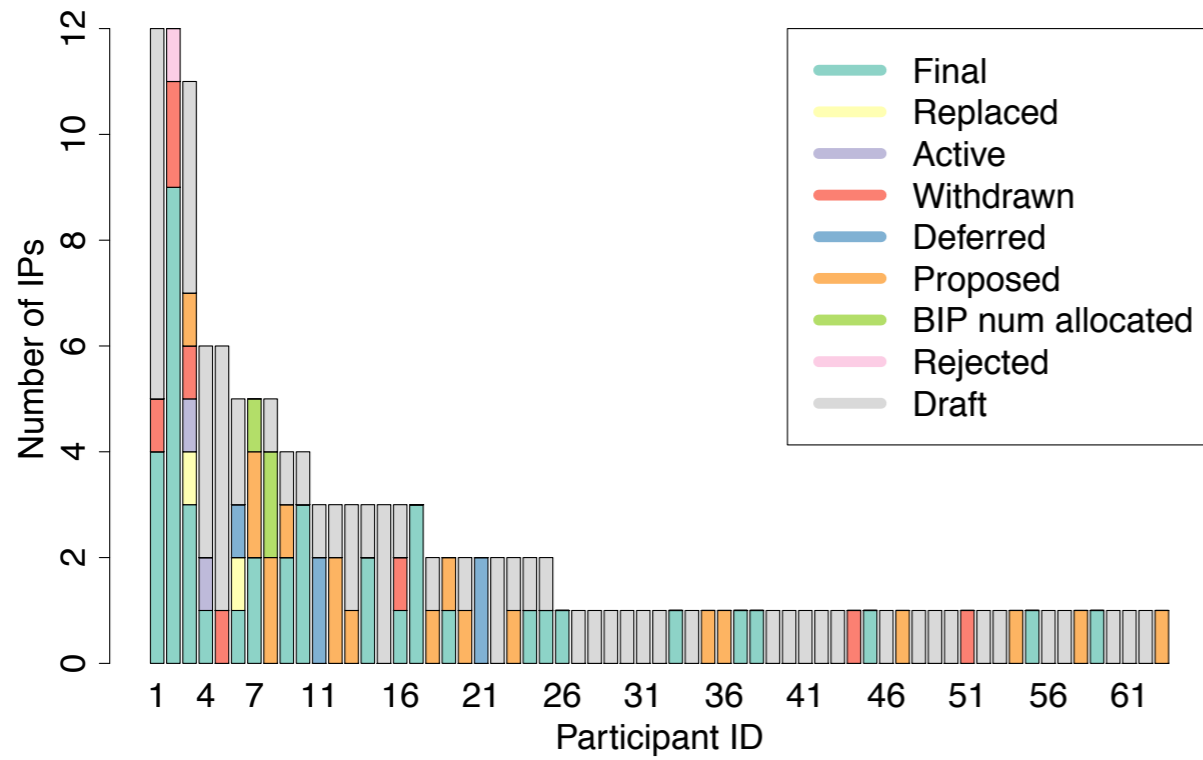


“Who makes the rules (i.e.,  
governance) is at least as important  
as how the rules are enforced”

Vili Lehdonvirta



# GOVERNANCE CENTRALIZATION



# TOP TEN OBSTACLES

---

10 Usability

9 Governance

**8 Comparisons**

7 Key Management

6 Agility











5 Interoperability

4 Scalability

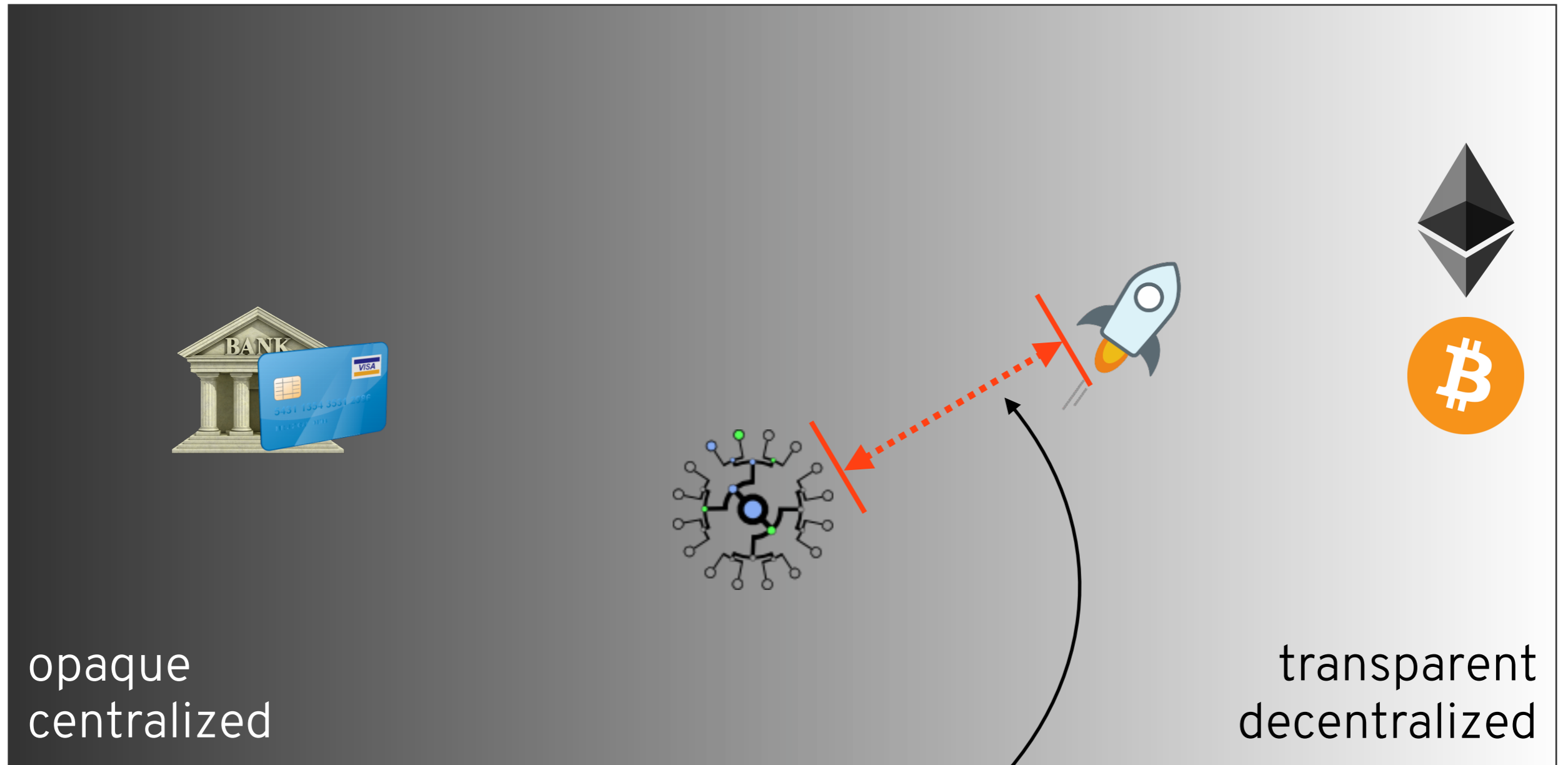
3 Cost-Effectiveness

2 Privacy

1 Scalability

1	 <b>Bitcoin</b>	\$114,305,992,325	\$6,682.90	\$4,139,650,000	17,104,250 BTC
2	 <b>Ethereum</b>	\$53,038,082,853	\$529.38	\$1,831,740,000	100,189,435 ETH
3	 <b>Ripple</b>	\$20,874,145,859	\$0.531889	\$291,709,000	39,245,304,677 XRP *
4	 <b>Bitcoin Cash</b>	\$15,074,416,610	\$876.76	\$445,785,000	17,193,400 BCH
5	 <b>EOS</b>	\$9,294,145,613	\$10.37	\$939,063,000	896,149,492 EOS *
6	 <b>Litecoin</b>	\$5,495,862,937	\$96.32	\$294,544,000	57,058,378 LTC
7	 <b>Stellar</b>	\$4,272,598,744	\$0.229599	\$40,253,900	18,608,960,596 XLM *
8	 <b>Cardano</b>	\$4,136,871,521	\$0.159558	\$89,486,900	25,927,070,538 ADA *
9	 <b>IOTA</b>	\$3,160,242,546	\$1.14	\$75,727,900	2,779,530,283 MIOTA *
10	 <b>TRON</b>	\$3,125,915,070	\$0.047544	\$463,402,000	65,748,111,645 TRX *

# HOW TO COMPARE SOLUTIONS?



what is this distance? can we quantify it?

# TOP TEN OBSTACLES

---

10 Usability

9 Governance

8 Comparisons

**7 Key Management**

6 Agility

5 Interoperability

4 Scalability

3 Cost-Effectiveness

2 Privacy

1 Scalability

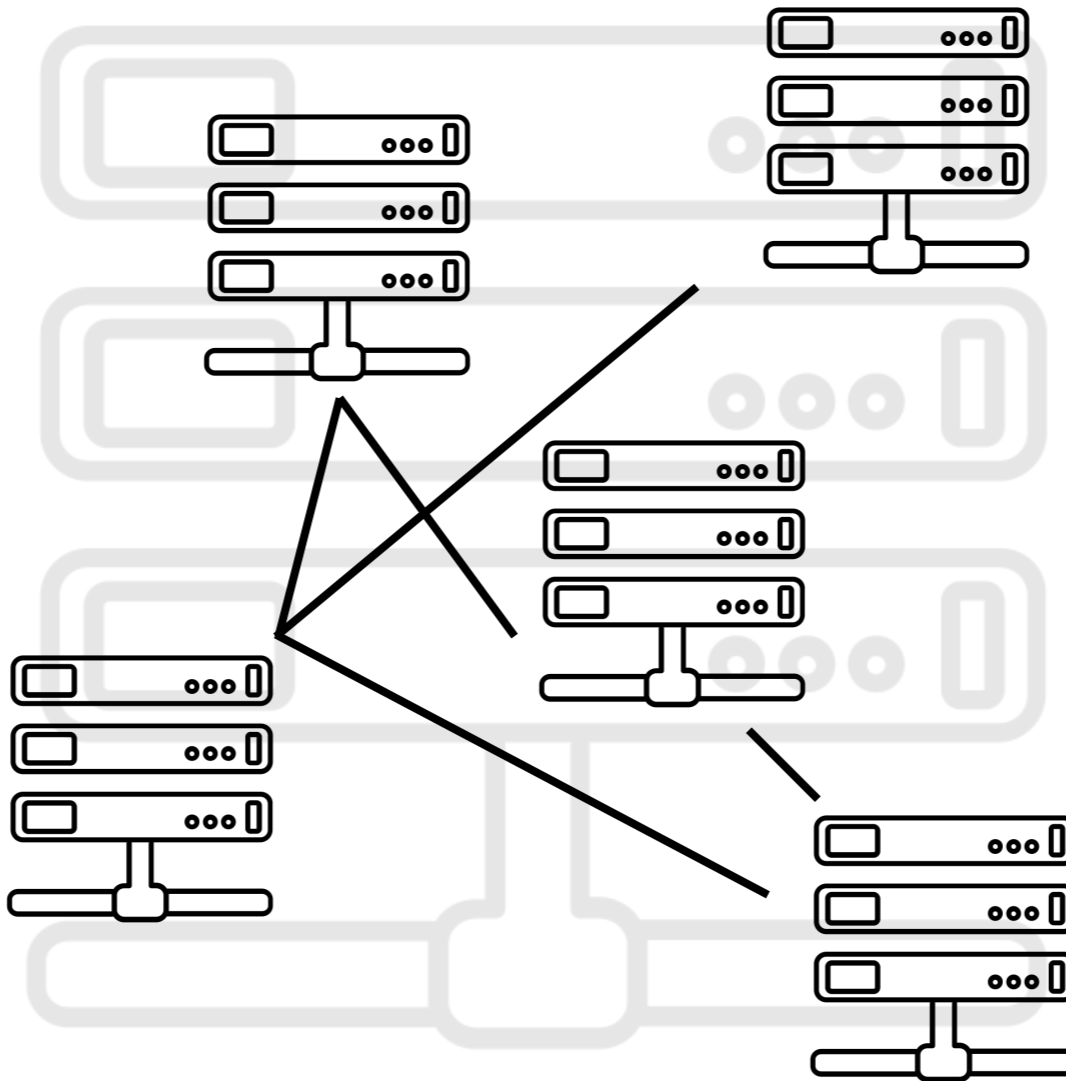
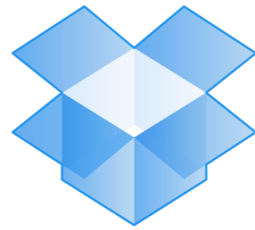


(image from Provenance report: <https://www.provenance.org/tracking-tuna-on-the-blockchain>)

# TOP TEN OBSTACLES

---

- 10 Usability
- 9 Governance
- 8 Comparisons
- 7 Key Management
- 6 Agility
- 5 Interoperability**
- 4 Scalability
- 3 Cost-Effectiveness
- 2 Privacy
- 1 Scalability



DATA  
CONSUMERS

DATA  
PRODUCERS



(icons by parkjisun from noun project)



# TOP TEN OBSTACLES

---

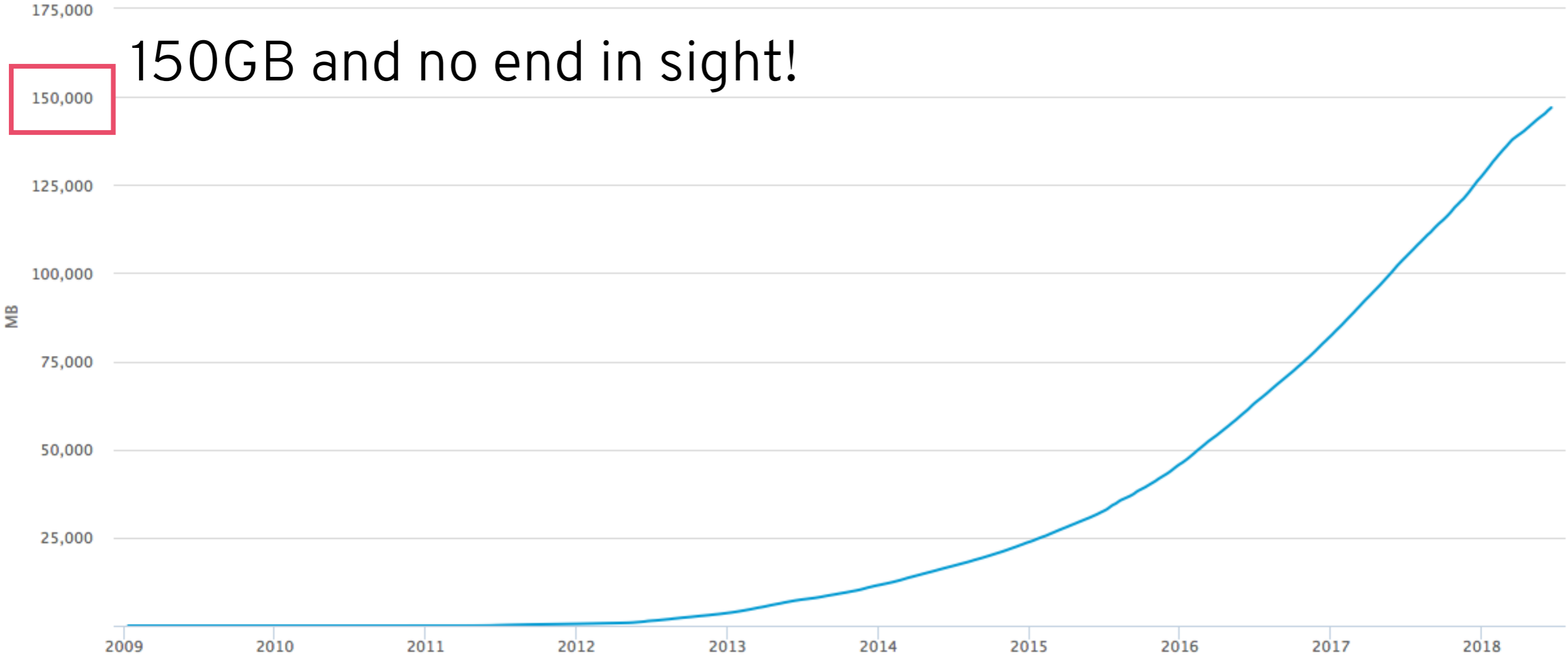
- 10 Usability
- 9 Governance
- 8 Comparisons
- 7 Key Management
- 6 Agility
- 5 Interoperability
- 4 Scalability**
- 3 Cost-Effectiveness
- 2 Privacy
- 1 Scalability

# SCALABILITY

## Blockchain Size

source: blockchain.info

150GB and no end in sight!



# TOP TEN OBSTACLES

---

10 Usability

9 Governance

8 Comparisons

7 Key Management

6 Agility

5 Interoperability

4 Scalability

3 Cost-Effectiveness

**2 Privacy**

1 Scalability

# RISKS OF ANONYMOUS PAYMENTS



## ONLINE DRUG SALES

Shop by C

**LAB TESTED USA DOMESTIC FENTANYL HCL 98% pure**  
**-1400mg - Thanks Giving Special 1400mg per order til holiday/ 2500mg per order only on black friday(normally the 1000mg listing)**

From now until ThanksGiving, I am running a special on all my Fentanyl listings and discounting them drastically. The 1000mg listing will now get you 1400mg until the holiday passes. On black friday and only black friday, this amount will be 2500mg. There is no limit to the amount you can order so get your bitcoins ready This is HCL Fentanyl, the strongest you can get. this is as pure FENTANYL ...

Sold by [redacted] - 41 sold since Mar 4, 2016  
**Vendor Level 7** **Trust Level 5**

## “CYCLE THEFT”



## THEFTS



## EXTORTION

Cryptolocker 2.0

**Payment will be raised on**  
5/16/2017 00:47:55

**Time Left**  
02:23:57:37

Your files w  
without pay

**EXTORTION**

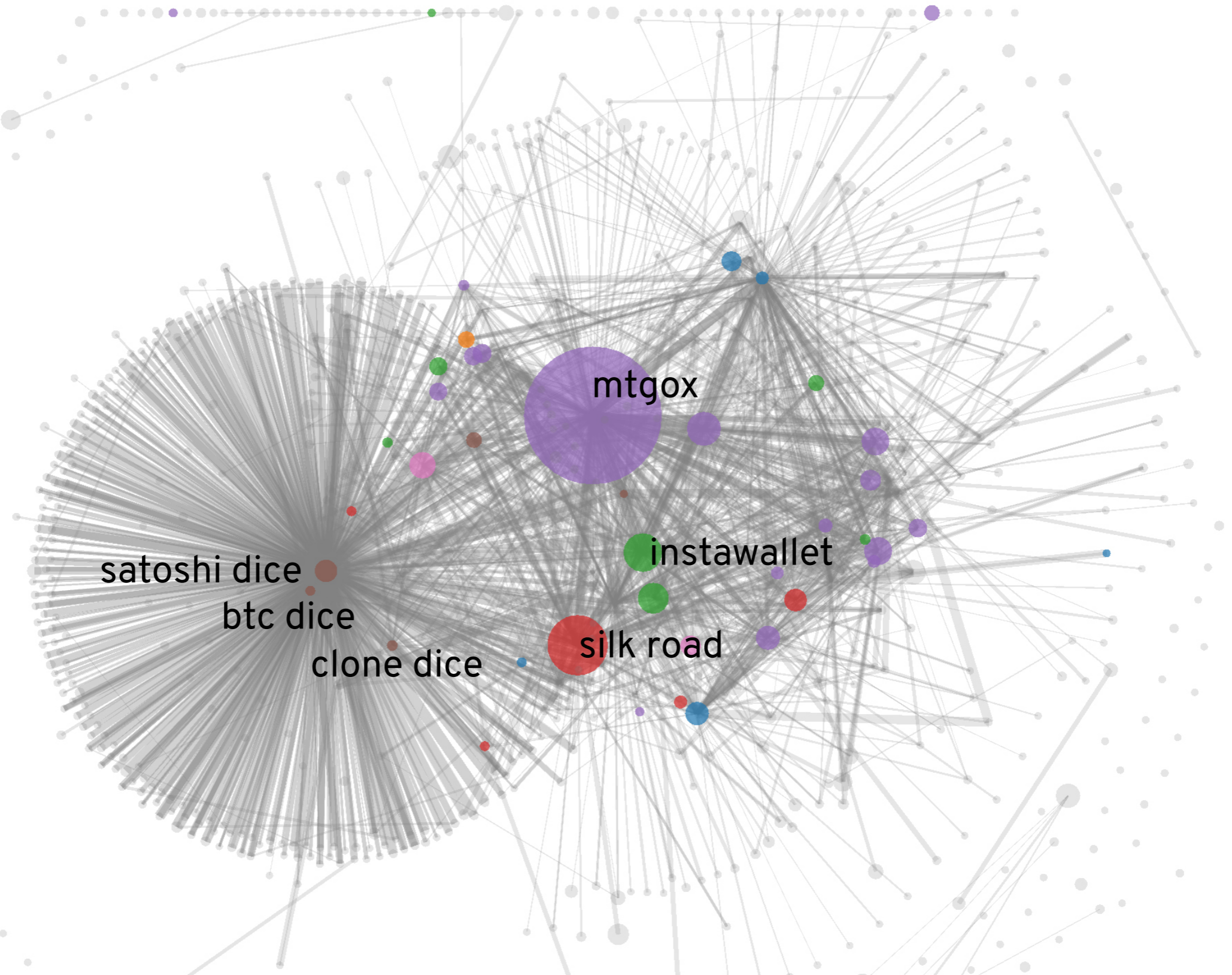
Pizzeria, has been targeted for extortion. The triggered by any event under your control.

etary tribute, by the deadline provided below, arably damaged. The following methods are pliance:

**Anonymous Reports of:**

- Health Code Violations
- OSHA Violations
- Criminal Tax Evasion
- Money Laundering
- Illegal Drug Sales
- Marijuana Grow Operations
- Methamphetamine Production
- Terrorist Training Activity

# FISTFUL OF BITCOINS [MPJLMVS'13]



# REAL-WORLD BITCOIN TRACKING

---

**Prosecutors Trace \$13.4M in Bitcoins From the Silk Road to Ulbricht's Laptop**

**The Imperfect Crime: How the WannaCry Hackers Could Get Nabbed**



Quanta**Bytes**



ELLIPTIC



**CHAINALYSIS**

# IMPROVING ANONYMITY

Approach 1: Design a **standalone** privacy-enhanced currency

**Zerocash: Decentralized Anonymous Payments from Bitcoin**

Eli Ben-Sasson\*, Alessandro Chiesa†, Christina Garman‡, Matthew Green‡, Ian Miers‡, Eran Tromer§, Madars Virza†

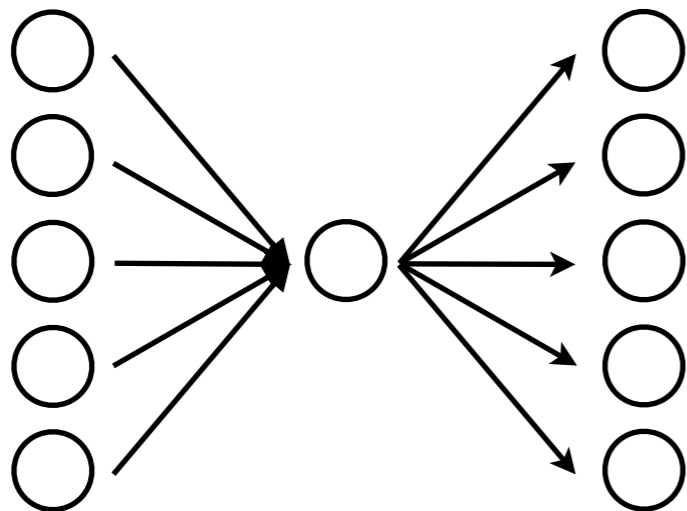


**RING CONFIDENTIAL TRANSACTIONS**

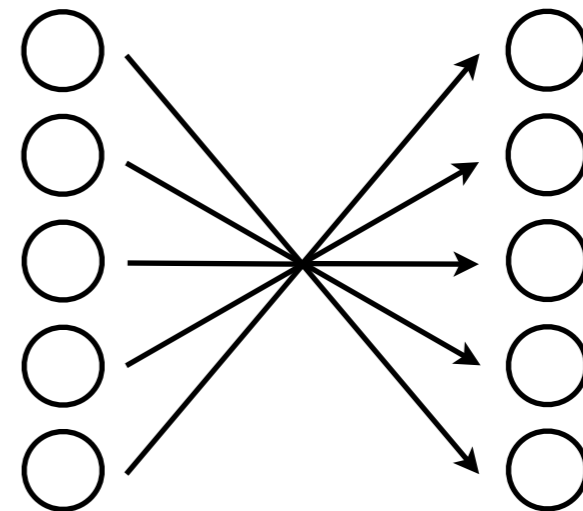
SHEN NOETHER- MONERO RESEARCH LABS

Approach 2: Design a **privacy overlay** for an existing currency

**centralized**



**decentralized**



# TOP TEN OBSTACLES

---

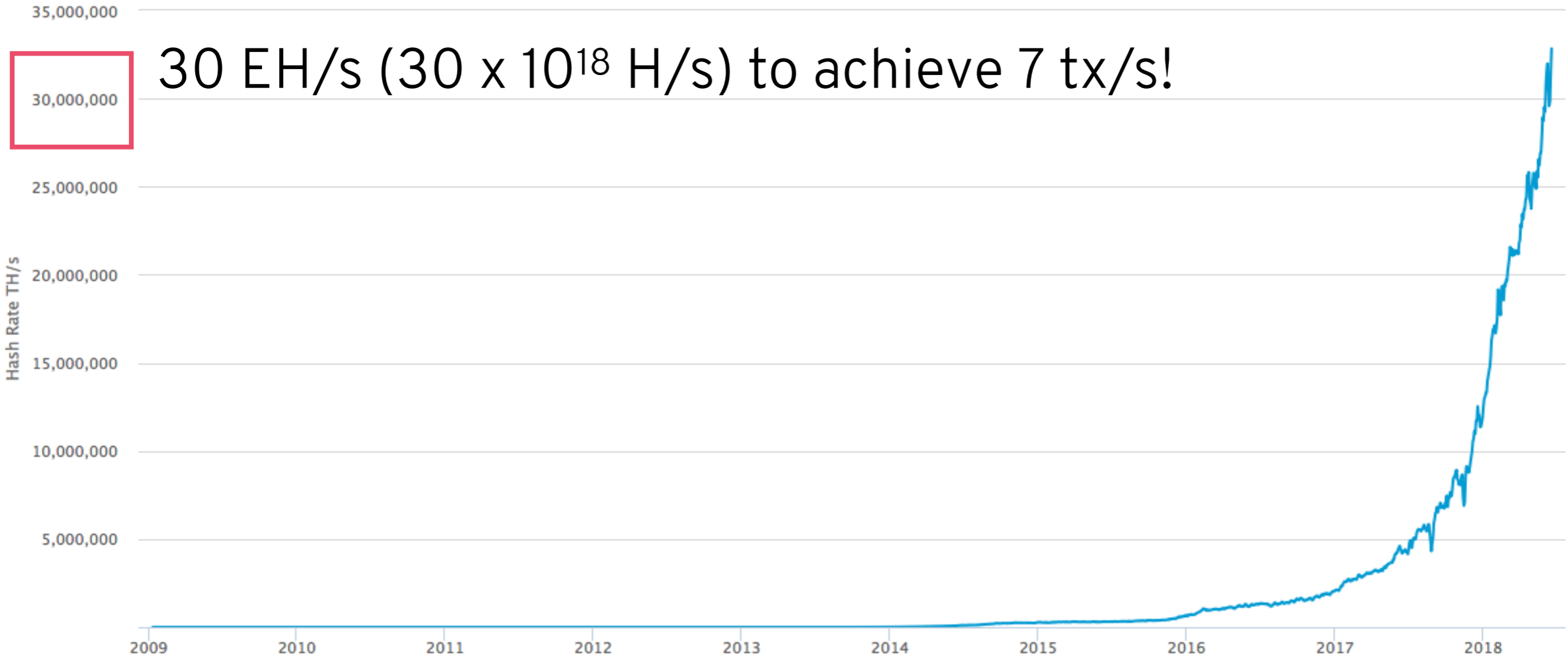
- 10 Usability
- 9 Governance
- 8 Comparisons
- 7 Key Management
- 6 Agility
- 5 Interoperability
- 4 Scalability
- 3 Cost-Effectiveness
- 2 Privacy
- 1 Scalability**



# SCALABILITY

## Hash Rate

source: blockchain.info



# SCALABILITY

## Hash Rate

source: blockchain.info

35,000,000

30,000,000

25,000,000

30 EH/s ( $30 \times 10^{18}$  H/s) to achieve 7 tx/s!

↑ COMPUTATIONAL POWER ⇒ ↓ THROUGHPUT

10,000,000

5,000,000

2009

2010

2011

2012

2013

2014

2015

2016

2017

2018

# TOP TEN OBSTACLES

---

- 10 Usability
- 9 Governance
- 8 Comparisons
- 7 Key Management
- 6 Agility
- 5 Interoperability
- 4 Scalability
- 3 Cost-Effectiveness
- 2 Privacy
- 1 Scalability



---

THANKS!  
ANY QUESTIONS?