MINIATURE WORLD: MEASURING AND REPLICATING REAL-WORLD BLOCKCHAIN DEPLOYMENTS

Adem Efe Gencer

with Ittay Eyal, Emin Gün Sirer, and Robbert van Renesse

Jan 26th, 2016

Initiative for CryptoCurrencies and Contracts (IC3)
Computer Science Department, Cornell University
Blockchain Technology

- Promise to revolutionize Fintech
- Trustless auditability
- Innovative use-cases
- Scalability and performance barriers
Evaluating Blockchain Protocols

What is the state-of-the-art for evaluating blockchain proposals?
Evaluating Blockchain Protocols

1. Technical Tradeoffs
Evaluating Blockchain Protocols

1. Technical Tradeoffs
2. Identify Metrics
Evaluating Blockchain Protocols

1. Technical Tradeoffs
2. Identify Metrics
3. End-to-end Evaluation
Some proposals are strictly better than others and can be proven to be so:

- Better signatures
- More efficient use of blocks
- Sharding schemes
EVALUATION BY DISCUSSION
Evaluation by Discussion

2009

1MB

\[ t \]
Evaluation by Discussion

2009

Reparameterization Debate*

@bitcoin-dev:
1000 discussions
77 threads

* BIPs 100, 101, 102, 103, 105, 106, 107, …
Evaluation by Discussion

<table>
<thead>
<tr>
<th>2009</th>
<th>Reparameterization Debate*</th>
</tr>
</thead>
<tbody>
<tr>
<td>1MB</td>
<td>@bitcoin-dev:</td>
</tr>
<tr>
<td></td>
<td>1000 discussions</td>
</tr>
<tr>
<td></td>
<td>77 threads</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Today</th>
</tr>
</thead>
<tbody>
<tr>
<td>1MB</td>
</tr>
</tbody>
</table>

* BIPs 100, 101, 102, 103, 105, 106, 107, …
Evaluation in the Wild

Release the protocol and observe it in the wild

: Altcoins
Goals

- Build a representative environment that enables protocols to be evaluated
- Identify good metrics for blockchain protocols
- Perform repeatable evaluations under different scenarios and constraints
MINIATURE WORLD
Miniature World

Actual Code

010110
110011
101000
0001
Miniature World

Efficient  Accurate  Repeatable

Actual Code  Large-scale Emulation  Data

MINIATURE WORLD
Miniature World

Efficient

Accurate

Repeatable

Actual Code

Large-scale Emulation

Data
Miniature World

- Efficient
- Accurate
- Repeatable

Actual Code → MINIATURE WORLD

Large-scale Emulation

Data
Miniature World Vision

6K × 📀: One-to-one replica of Bitcoin system

🚨⏰🌍: Calibration based on measurements

☑️: Detailed real world scenarios
Measurement and Characterization of Bitcoin Network

- P2P Latency
- Provisioned Bandwidth
- Protocol-level traffic
- Temporal and event-driven variations
P2P Latency
P2P Latency

\[ t_2 = ? \]
P2P Latency

\[ |t_1 - t_2| \leq \mathcal{O} \leq (t_1 + t_2) - \]
P2P Latency

\[ |t_1 - t_2| \leq \text{Clock} \leq (t_1 + t_2) - t_3 - t_4 \]
P2P Latency

\[ |t_1 - t_2| \leq \leq (t_1 + t_2) \]

\[ |t_3 - t_4| \leq \leq (t_3 + t_4) \]
P2P Latency

\[ |t_1 - t_2| \leq \leq (t_1 + t_2) - \]

\[ |t_3 - t_4| \leq \leq (t_3 + t_4) \]

\[ \ldots \]

\[ |t_{2n-1} - t_{2n}| \leq \leq (t_{2n-1} + t_{2n}) \]
P2P Latency

Latency range estimation per virtual link

\[
\begin{align*}
\text{MAX} \{ & \mid t_1 - t_2 \mid, \mid t_3 - t_4 \mid, \ldots, \\
& \mid t_{2n-1} - t_{2n} \mid \} \leq \underbrace{\cdots}_{\text{MIN}} \leq \text{MIN} \{ & (t_1 + t_2), \\
& (t_3 + t_4), \ldots, \\
& (t_{2n-1} + t_{2n}) \} \n\end{align*}
\]
Provisioned Bandwidth
Provisioned Bandwidth

\[ bw_1 \]
Provisioned Bandwidth

\[ bw_1 \parallel bw_2 \]
Provisioned Bandwidth

\[ \text{bw}_1 \parallel \text{bw}_2 \parallel \text{bw}_3 \parallel \ldots \]
Provisioned Bandwidth

Lower bound on per-node provisioned bandwidth

$$\max(\ldots)$$

$$(bw_1, bw_2, bw_3)$$
Protocol-level Traffic

1. TCP Connection Time
2. Bitcoin Protocol Handshake Time
3. Bitcoin Pong Time
Miniature World

Efficient

Accurate

Repeatable

Actual Code

Large-scale Emulation

Data
Metrics for Blockchain Protocols

- Mining Power
- Utilization
- Fairness
- Consensus Delay
- Time to Win &
- Time to Prune

[Diagram showing Security and Performance]
Mining Power Utilization

Measure of robustness against rollback

\[ \frac{\sum \text{green}}{\sum (\text{green} + \text{red})} \]
## Fairness

### Measure of robustness against centralization

<table>
<thead>
<tr>
<th>mined blocks*</th>
<th>in main chain</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Diagram" /></td>
<td><img src="image" alt="Diagram" /></td>
</tr>
</tbody>
</table>

*Sorted*
### Fairness

**Measure of robustness against centralization**

<table>
<thead>
<tr>
<th>mined blocks*</th>
<th>in main chain</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Mining Blocks" /></td>
<td><img src="image2" alt="Blocks in Chain" /></td>
</tr>
</tbody>
</table>

*Sorted

- Actual presence
- Fair presence

*Sorted
Fairness

Measure of robustness against centralization

\[
\text{Actual presence} \quad \underline{\text{Fair presence}}
\]
Consensus Delay

Measure of time it takes for system to reach agreement

- Percent of the time that the nodes agree
- Percent of the nodes that agree
Miniature World

Actual Code → Large-scale Emulation → Data
MEASUREMENTS
Measurement Infrastructure

Cornell & PlanetLab
Measurement Infrastructure

17 nodes
5 continents

Cornell & PlanetLab
Distribution of Bitcoin Nodes

*Distribution of 5743 full nodes obtained from https://bitnodes.21.co/ (Jan 9th, 2017)
Distribution of Mining Power

*Based on blocks generated in 2016*
Distribution of Mining Power

*Based on blocks generated in 2016*
Distribution of Stale Peers

*Height is more than 1% behind the best blockchain.*
LATENCY
IPv4 Latency from Single Beacon

Minimum Network Ping Times
(μ: 0.10, 10th: 0.03, 50th: 0.09, 90th: 0.20)

Minimum Network Ping Times (CDF)
(μ: 0.10, 10th: 0.03, 50th: 0.09, 90th: 0.20)
IPv4 Latency from Single Beacon

Minimum Network Ping Times
(\(\mu: 0.10\), 10\(^{th}\): 0.03, 50\(^{th}\): 0.09, 90\(^{th}\): 0.20)

Minimum Network Ping Times (CDF)
(\(\mu: 0.10\), 10\(^{th}\): 0.03, 50\(^{th}\): 0.09, 90\(^{th}\): 0.20)
IPv4 Latency from Single Beacon

Distance vs Minimum Ping Time

Ping Time (s) vs Distance (km)
IPv4 Latency from Single Beacon

Distance vs Minimum Ping Time

Ping Time (s)

Distance (km)
IPv4 Latency from Single Beacon

Distance vs Minimum Ping Time

Ping Time (s) vs Distance (km)
IPv4 Latency Across All Beacons

Pairwise Minimum Network Ping Times
($\mu: 0.14$, $10^{th}: 0.05$, $50^{th}: 0.11$, $90^{th}: 0.30$)

Pairwise Minimum Network Ping Times (CDF)
($\mu: 0.14$, $10^{th}: 0.05$, $50^{th}: 0.11$, $90^{th}: 0.30$)
IPv4 Latency Across All Beacons

\( \sim 5.2 \text{ million links} \)
IPv6 Latency from Single Beacon

Minimum Network Ping Times
(μ:0.11, 10th:0.04, 50th:0.10, 90th:0.16)

Minimum Network Ping Times (CDF)
(μ:0.11, 10th:0.04, 50th:0.10, 90th:0.16)
IPv6 Latency from Single Beacon

Distance vs Minimum Ping Time

Ping Time (s)

Distance (km)

0  2K  4K  6K  8K  10K  12K  14K

0  0.05  0.1  0.15  0.2  0.25  0.3  0.35  0.4  0.45
IPv6 Latency from Single Beacon
IPv4 Bandwidth

Bandwidth [~800KB blocks]
($\mu$: 67.74, 10$^{th}$: 4.99, 50$^{th}$: 49.55, 90$^{th}$: 159.24)

Bandwidth (CDF) [~800KB blocks]
($\mu$: 67.74, 10$^{th}$: 4.99, 50$^{th}$: 49.55, 90$^{th}$: 159.24)
IPv4 Bandwidth

Bandwidth [~800KB blocks]
(μ: 67.74, 10th: 4.99, 50th: 49.55, 90th: 159.24)

Bandwidth (CDF) [~800KB blocks]
(μ: 67.74, 10th: 4.99, 50th: 49.55, 90th: 159.24)
IPv4 Maximum Epoch Bandwidth

Maximum Epoch Bandwidth
[\sim 800\text{KB blocks}]

\[
(\mu: 76.74, 10^{\text{th}}: 3.95, 50^{\text{th}}: 56.19, 90^{\text{th}}: 182.38)
\]
IPv4 Maximum Epoch Bandwidth

Distance vs Maximum Epoch Bandwidth
[~800KB blocks]
Evolution of Provisioned Bandwidth (IPv4 Nodes)

Provisioned Bandwidth Per Node (Median)

<table>
<thead>
<tr>
<th>Year</th>
<th>Bandwidth (Mbit/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016</td>
<td>30</td>
</tr>
<tr>
<td>2017</td>
<td>50</td>
</tr>
</tbody>
</table>
IPv4 Bandwidth

- Common bandwidth caps around 10 Mbit/s and 100 Mbit/s
- Only 10% with bandwidth under 5 Mbit/s
- Median bandwidth around 50 Mbit/s
- Long-tailed distribution
- Increase in median bandwidth since 2016
IPv6 Bandwidth

Bandwidth [~800KB blocks]
\( \mu: 84.97, 10^{th}: 7.19, 50^{th}: 73.55, 90^{th}: 205.72 \)

Bandwidth (CDF) [~800KB blocks]
\( \mu: 84.97, 10^{th}: 7.19, 50^{th}: 73.55, 90^{th}: 205.72 \)
IPv6 Bandwidth

Bandwidth [~800KB blocks]
\(\mu: 84.97, 10^{th}: 7.19, 50^{th}: 73.55, 90^{th}: 205.72\)

Bandwidth (CDF) [~800KB blocks]
\(\mu: 84.97, 10^{th}: 7.19, 50^{th}: 73.55, 90^{th}: 205.72\)
IPv6 Maximum Epoch Bandwidth

Maximum Epoch Bandwidth
[\sim 800\text{KB blocks}]

\((\mu: 105.32, 10^{th}: 14.43, 50^{th}: 92.58, 90^{th}: 236.39)\)
IPv6 Bandwidth

- Relatively higher bandwidth caps compared to IPv4 nodes
- Only 10% with bandwidth under 15 Mbit/s
- Median provisioned bandwidth close to 100 Mbit/s
Tor Bandwidth

Bandwidth [≈800KB blocks]
(μ: 3.91, 10th: 2.77, 50th: 3.62, 90th: 5.76)

Bandwidth (CDF) [≈800KB blocks]
(μ: 3.91, 10th: 2.77, 50th: 3.62, 90th: 5.76)
Tor Maximum Epoch Bandwidth

Max Loan Epoch Bandwidth
[~800KB blocks]
($\mu: 5.90$, $10^{th}: 2.33$, $50^{th}: 5.60$, $90^{th}: 9.21$)

Max Loan Epoch Bandwidth (CDF)
[~800KB blocks]
($\mu: 5.90$, $10^{th}: 2.33$, $50^{th}: 5.60$, $90^{th}: 9.21$)
Tor Bandwidth

- An order of magnitude lower bandwidth compared to IPv4 and IPv6
- Not incredibly slow – 90% of nodes are faster than 2 Mbit/s
- Median provisioned bandwidth around 6 Mbit/s
TCP Connection Time

Connection Times
$(\mu: 0.13, 10^{th}: 0.03, 50^{th}: 0.09, 90^{th}: 0.23)$

Connection Times (CDF)
$(\mu: 0.13, 10^{th}: 0.03, 50^{th}: 0.09, 90^{th}: 0.23)$
Version – Verack Time

Verack Times
(\(\mu: 0.21, \ 10^{th}: 0.04, \ 50^{th}: 0.10, \ 90^{th}: 0.27\))

Verack Times (CDF)
(\(\mu: 0.21, \ 10^{th}: 0.04, \ 50^{th}: 0.10, \ 90^{th}: 0.27\))
Bitcoin Pong Time

Minimum Bitcoin Pong Times
($\mu: 0.11, 10^{th}: 0.03, 50^{th}: 0.09, 90^{th}: 0.22$)

Minimum Bitcoin Pong Times (CDF)
($\mu: 0.11, 10^{th}: 0.03, 50^{th}: 0.09, 90^{th}: 0.22$)
Protocol-level Traffic

- Similar network level latencies and protocol level measurements for IPv4 and IPv6 nodes.
- Useful for modelling P2P latencies for Tor nodes in Miniature World.
Miniature World Architecture

MINIATURE WORLD

Controller
- Bootstrapper
- Event-driven Emulator

In Situ Controller
- Logger
- Blockchain Client

User
Miniature World Architecture

- Initiate topology and emulate wide area network
- Control latency and bandwidth through kernel rate limiting and virtual network interfaces
- Start clients and bootstrap the blockchain

Bootstrapper
Miniature World Architecture

- Trigger block and transaction generation events
- Coordinate In Situ Controllers
- Keep track of cluster health

Event-driven Emulator
Miniature World Architecture

- Record experiment progress and events
- Upload local measurements to controller
- Audit clock drift
Conclusion

A principled way of evaluating protocols

- Full control over: latency, bandwidth, traffic
- Large-scale setup based on measurement and characterization of existing network
- Custom metrics for blockchain protocols
IC3 Open House: Feb 23 in SF!

What & Where? A Technical Forum at Chain in SF

- Session 1: Blockchain Scaling and Consensus
- Session 2: Smart Contracts and Confidentiality

Who Can Apply to Attend?

- Employees of Prospective IC3 Members
- Outstanding Students with an Interest to Pursue Graduate Studies with IC3

More info and Registration?

- [http://www.initc3.org/events](http://www.initc3.org/events)