Secure Incentivization for Decentralized Content Delivery

Prateesh Goyal\textsuperscript{1}, Ravi Netravali\textsuperscript{2}, Mohammad Alizadeh\textsuperscript{1}, Hari Balakrishnan\textsuperscript{1}

MIT CSAIL\textsuperscript{1}, UCLA\textsuperscript{2}
Reducing price for content delivery

- CDN - Good QoS but expensive for content providers
Reducing price for content delivery

- P2P content delivery (e.g., Akamai Netsession, Peer5)
  - Use unused bandwidth and storage resource at peers
  - Cheaper but insufficient participation by peers [1]

Increasing adoption by peers

Tit-for-tat incentivization (e.g., bit torrent, dandelion)

- To consume content, clients must serve content (act as peers)
- Doesn’t work for content delivery
Increasing adoption by peers

Tit-for-tat incentivization (e.g., bit torrent, dandelion)

- To consume content, clients must serve content (act as peers)
- Doesn’t work for content delivery
  - Restricts clients who do not wish to contribute resources
Increasing adoption by peers

Tit-for-tat incentivization (e.g., bit torrent, dandelion)

- To consume content, clients must serve content (act as peers)
- Doesn’t work for content delivery
  - Restricts clients who do not wish to contribute resources
  - Fails to provide incentives to peers who do not wish to consume the content
Gringotts: Monetary incentivization for peers

Content providers

Peers

Clients
Contributions

● Proof of Delivery (PoD)
  ○ Peers get paid by content providers for delivering content
  ○ Secure against financially motivated attacks. E.g., Peer gets paid without delivering content

● Decentralized P2P content delivery
  ○ No centralized authority (trustless)
  ○ Peers ensured payment by broadcasting PoD on blockchain

● Consumer Survey
  ○ Sample size: 876-person
  ○ 51% respondents would participate
Contributions

● **Proof of Delivery (PoD)**
  ○ Peers get paid by content providers for delivering content
  ○ Secure against financially motivated attacks. E.g., Content provider refuses to pay peer

● **Decentralized P2P content delivery**
  ○ No centralized authority (trustless)
  ○ Peers ensured payment by broadcasting PoD on blockchain

● **Consumer Survey**
  ○ Sample size: 876-person
  ○ 51% respondents would participate
Contributions

● Proof of Delivery (PoD)
  ○ Peers get paid by content providers for delivering content
  ○ Secure against financially motivated attacks. E.g., Content provider refuses to pay peer

● Decentralized P2P content delivery
  ○ No centralized authority (trustless)
  ○ Peers ensured payment by broadcasting PoD on blockchain

● Consumer Survey
  ○ Sample size: 876-person
  ○ 51% respondents would participate
Design

Smart contract
1. Payment source
2. Defines PoD

Blockchain

Content file

Chunk 1

Chunk 2

Chunk N

Peers
Downloading a file with Gringotts

1. List of peers
2. Signature

Initial Certificate

Peer 1
Peer i
Peer N
Downloading a file with Gringotts

Proof of Delivery
PoD(i)
1. Hash(PoD(i-1))
2. Peer’s signature

Initial Certificate (IC)
1. List of peers
2. Signature
Proof of Delivery Chain (PoDC)

Proof of Delivery
PoD(i)
1. Hash(PoD(i-1))
2. Peer’s signature

Clients should download chunks sequentially
Detecting and thwarting attacks

● Content provider refuses to pay peer
● Peer earns money without delivering content
Collusion between clients and peers (Sybil)

- Attack: Clients and peers collude to generate PoD without serving any content

- Solution:
  - Random assignment of peers
  - PoDC ensures that client does not only contact colluding peer
Collusion between clients and peers (Sybil)

- Attack: Clients and peers collude to generate PoD without serving any content

Solution:
- Make attacks financially infeasible
  - Random assignment of peers
  - PoDC ensures that client does not only contact colluding peers

List of peers in IC

<table>
<thead>
<tr>
<th>Chunk #</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>
Collusion between clients and peers (Sybil)

- **Attack**: Clients and peers collude to generate PoD without serving any content
- **Solution**: Make attacks financially infeasible
  - PoD ensures that client downloads chunk sequentially
  - Random assignment of peers

<table>
<thead>
<tr>
<th>Chunk #</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>
Collusion between clients and peers (Sybil)

- Attack: Clients and peers collude to generate PoD without serving any content
- Solution: Make attacks financially infeasible
  - PoD ensures that client downloads chunk sequentially
  - Random assignment of peers
- Model: Cost of creating client is 0 (Insufficient: Client can terminate connection)

List of peers in IC

<table>
<thead>
<tr>
<th>Chunk #</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>
Collusion between clients and peers (Sybil)

- Attack: Clients and peers collude to generate PoD without serving any content
- Solution: Make attacks financially infeasible
  - PoD ensures that client downloads chunk sequentially
  - Random assignment of peers
- Model: Cost of creating client is 0 (*Insufficient: Client can terminate connection*)

List of peers in IC

<table>
<thead>
<tr>
<th>Chunk #</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>H</td>
<td>M</td>
<td>H</td>
<td>H</td>
</tr>
</tbody>
</table>
Collusion between clients and peers (Sybil)

- **Attack**: Clients and peers collude to generate PoD without serving any content
- **Solution**: Make attacks financially infeasible
  - PoD ensures that client downloads chunk sequentially
  - Random assignment of peers
- **Model**: Cost of creating client is 0 *(Insufficient: Client can terminate connection)*

<table>
<thead>
<tr>
<th>List of peers in IC</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chunk #</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
</table>
Collusion between clients and peers (Sybil)

Gringotts: Collusion is financially infeasible

- Clients download first chunk from a secure node
- Overhead to client generation
  - Client must expend bandwidth resources before colluding with a peer
Consumer survey

- Understand expectations and requirements for peers
- 876 responders across USA
- Questions on
  - Payments
  - Resource availability
  - Participation concerns
Findings: Payments

- **Will you participate in the service?**
  - Yes: 60%
  - No: 40%

- **Will you accept cryptocurrency as your payment?**
  - Yes: 20%
  - Maybe: 40%
  - No: 40%
Findings: Concerns

<table>
<thead>
<tr>
<th>Concern</th>
<th>Fraction concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security and Privacy</td>
<td>82.8%</td>
</tr>
<tr>
<td>Liability for Illegal Content</td>
<td>50.5%</td>
</tr>
<tr>
<td>Performance Impact on Device</td>
<td>47.1%</td>
</tr>
<tr>
<td>Payment Concerns</td>
<td>42.1%</td>
</tr>
<tr>
<td>Personal Ethics</td>
<td>29.4%</td>
</tr>
</tbody>
</table>
Conclusion and discussion

Gringotts: Secure monetary incentivization for decentralized content delivery
Conclusion and discussion

Gringotts: Secure monetary incentivization for decentralized content delivery

- Feedback
  - Additional challenges in P2P content delivery
Conclusion and discussion

Gringotts: Secure monetary incentivization for decentralized content delivery

● Feedback
  ○ Additional challenges in P2P content delivery

● Controversial aspects
  ○ Gringotts increases upstream traffic and cost for ISPs
  ○ Use of cryptocurrency for payments
Conclusion and discussion

Gringotts: Secure monetary incentivization for decentralized content delivery

● Feedback
  ○ Additional challenges in P2P content delivery

● Controversial aspects
  ○ Gringotts increases upstream traffic and cost for ISPs
  ○ Use of cryptocurrency for payments

● Open issues
  ○ Consumer study (security and liability)
  ○ Ensuring QoS (file placement)
Conclusion and discussion

Gringotts: Secure monetary incentivization for decentralized content delivery

● Feedback
  ○ Additional challenges in P2P content delivery

● Controversial aspects
  ○ Gringotts increases upstream traffic and cost for ISPs
  ○ Use of cryptocurrency for payments

● Open issues
  ○ Consumer study (security and liability)
  ○ Ensuring QoS (file placement)

● Circumstance for failure
  ○ Failure to attract enough peers
Thank You
Detecting and thwarting attacks

- **Single entity attacks**
  - Malicious peer
  - Malicious content provider

- **Collusion attacks**
  - Collusion between clients and peers (Sybil attack)
Single entity attacks

- Malicious peer
  - Attack: Generate PoD without serving content
  - Peer requires PoDC, client can refuse PoDC if peer doesn’t serve content
Single entity attacks

- Malicious peer
  - Attack: Generate PoD without serving content
  - Peer requires PoDC, client can refuse PoDC if peer doesn’t serve content

- Malicious content provider
  - Attack: Generate IC so that peers produce PoD not eligible for payments
  - Content provider can’t predict hash of PoD
Blockchain overheads

- Existing blockchains can only support 25 tx/sec
- Probabilistic payments to reduce overhead
  - Peers submit PoD to the blockchain, if Hash(PoD) % N = 0
Single entity attacks

- Malicious peer
  - Attack: Generate PoD without serving content
  - Peer requires PoDC, client can refuse PoDC if peer doesn’t serve content

- Malicious content provider
  - Attack: Generate IC so that peers produce PoD not eligible for payments
  - Content provider can’t predict hash of PoD
  - Corner case: Content provider reusing IC
  - Include nonce in IC to avoid regenerating the IC
Collusion between clients and peers (Sybil)

- $x$: Client’s download cost per chunk
- $y$: Price paid by content provider per chunk
- $z$: Peer’s upload cost per chunk
- $M$: Fraction of malicious peers
Sybil attack: example

- $x$: Client’s download cost, $y$: Price paid by content provider, $z$: Peer’s upload cost, $m$: fraction of malicious peers
- Expected cost of download upto chunk $i$

\[
\text{Cost}[i] = 1 \cdot x + (i-1) \cdot (m \cdot 0 + (1-m) \cdot x)
\]
Sybil attack: example

- $x$: Client’s download cost, $y$: Price paid by content provider, $z$: Peer’s upload cost, $m$: fraction of malicious peers
- Expected cost of download upto chunk $i$

$$\text{Cost}[i] = 1 \cdot x + (i-1) \cdot (m \cdot 0 + (1-m) \cdot x)$$

- Expected payment to malicious peers

$$\text{Payment}[i] = (i-1) \cdot m \cdot y$$
Sybil attack: example

- $x$: Client’s download cost, $y$: Price paid by content provider, $z$: Peer’s upload cost, $m$: fraction of malicious peers
- An attack is economically unfeasible if
  \[ \text{Payment}[i] < \text{Cost}[i], \quad \forall i \in \mathbb{N} \]
  \[ \implies y \leq x \left( \frac{1}{m} - 1 \right) \]

- E.g., If $m=33\%$, then attack is economically infeasible if
  - $y \leq 2 \cdot x$ (or payment $\leq 2 \cdot$ Clients download cost)
Findings: Feasibility

● 82% users have more than 20GB free disk space
  ○ Store 100 videos

● Average uplink bandwidth: 22 Mbit/s
  ○ Stream 4 HD video streams simultaneously
Findings: Payment Concerns

<table>
<thead>
<tr>
<th>Concern</th>
<th>Fraction concerned</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t Know How to Use/Sell</td>
<td>59.7%</td>
</tr>
<tr>
<td>Not Setup to Receive</td>
<td>54.7%</td>
</tr>
<tr>
<td>Volatility and Risk</td>
<td>49.1%</td>
</tr>
<tr>
<td>Don’t Know What it is</td>
<td>21.9%</td>
</tr>
<tr>
<td>Other</td>
<td>6.9%</td>
</tr>
</tbody>
</table>

Table 2: Concerns for users who specified that they would not be willing to accept payment in cryptocurrency.
Downloading a file with Gringotts