The Private Web

Kevin O'Dwyer
Co-founder
R&D Engineer
Our vision:

To build a private web where end users are in control of their data
Self-certifying web protocol

Peergos client

Content addressed storage
- hash => data

Mutable pointers
- public key => hash

Public key infrastructure
- username => (identity public key, storage public key)
https://github.com/peergos/ipfs-nucleus

- p2p http proxy
- id
- block.get + Block Level Access Control (BATs)
- block.put
- block.stat
- refs
- block.rm & refs.local (only needed by GC)
Architecture

IPFS

Peergos server

TLS 1.3 encryption

Alice's storage server

PKI server

Bob's storage server

Web browser

IPFS

Peergos server

localhost

TLS 1.3 encryption

https encryption
Trust boundaries

- Blockstore
- IPFS
- Peergos server
- Peergos client
- Apps
- Apps
Access control

directory

base key

parent key

ianopolous

sub directory

base key

parent key

work

file

base key

thesis.txt modified:
2009-07-25 2:31
text/plain

data key

file contents
Metadata protection

- File – size, name, path, mime type, modified date etc
- Folder – topology
- File/Folder – look the same to the network
- # of Files/Folders
- Sharing – who has access, # have access
public class MessageEnvelope implements Codable {

    public final Id author;
    public final TreeClock timestamp;
    public final LocalDateTime creationTime; // Stored as

    @JsMethod
    public CompletableFuture<Optional<String>> sendInitialFollowRequests(String[] targetUsernames) {
        Set<String> usernames = new HashSet<>(Arrays.asList(targetUsernames));
        return Futures.reduceAll(usernames,
                (a, b) -> sendFollowRequest(targetUsername, SymmetricKey.random()),
                a, b -> a);
    }

    that.context.sendInitialFollowRequests(this.targetUsernames).thenApply(function(success) {
        ... });
    }

    ... optionally(function(throwable) {
        ... });
Static hosting
# Calendar

### September 2021

<table>
<thead>
<tr>
<th>Sun</th>
<th>Mon</th>
<th>Tue</th>
<th>Wed</th>
<th>Thu</th>
<th>Fri</th>
<th>Sat</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>29</td>
<td>30</td>
<td>31</td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>12:00 Philosophy...</td>
<td></td>
<td>18:30 Dance ses...</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td>10:00 Weekly c...</td>
<td>FOSDEM Conference...</td>
<td>12:00 Philosophy...</td>
<td>18:30 Dance ses...</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>12</td>
<td>13</td>
<td>14</td>
<td>15</td>
<td>16</td>
<td>17</td>
</tr>
<tr>
<td></td>
<td>10:00 Weekly c...</td>
<td>21:30 Presentation...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>19</td>
<td>20</td>
<td>21</td>
<td>22</td>
<td>23</td>
<td>24</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10:00 Weekly c...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Presentation**

- **Date:** 2021-09-14 09:30 pm - 10:30 pm
- **Location:** https://example-videoconferencing.com

- **Abstract:**
  - The stunning properties we have
  - How it works under the hood
  - Security analysis

**Actions:**
- Edit
- Delete
To-do lists

Project Board

:: Back log
:: 1. faster ×
:: 2. better ×
:: 3. cheaper ×

add new item

:: In Development
:: 1. make shiny ×
:: 2. add bells ×
:: 3. add whistles ×

add new item

:: In Test
:: 1. functional bits ×
:: 2. non-functional bits ×

:: Done
:: 1. MVP ×

add new item
Email bridge

Inbox

- test@peergos.com
  - Event: status meeting - Tue Aug 17 2021 12:00:00 GMT+0100
  - status meeting

- test@peergos.com
  - how about lunch?
  - What to grab a bite to eat at 1:00pm?

- test@peergos.com
  - test email
  - Hi Alice,
  - Just testing out the new email clien...

Search...
Group chat

Holiday Plans - you,bob,charlie

Charlie
2021-12-28 21:11:46
Document attached

Holiday Plans
2021-12-28 21:10:53
alice invited charlie

Gulf
2021-12-28 21:05:46
where's the bar? 😊

Lunch
2021-12-28 21:03:57
be there in 5 mins...

Decided to stay another week
Original message: bob | 2021-12-28 20:55:02

Gail:

Alice:

It's raining in London 😥

Alice:

Bob

Now where is my passport?

Bob

And my wallet?

2021-12-28 21:08:52 - alice invited charlie

Type a message
Future developments
IQ Test

Your email address: test@example.com
What is the answer?
A) 1 B) 42 C) Off-by-One

Submit!

req.open(“POST”, “form/survey.txt”, true);

{"emailAddress":"test@example.com","answer":"42"}

Type something

fetch(‘data/list.dat’, { method: ‘GET’ });

let body = encoder.encode(JSON.stringify(items));
fetch(‘data/list.dat’, { method: ‘PUT’, headers: headers, body: body });

1. Milk ×
2. Bread ×
3. Chocolate ×
Sign up for an account on beta.peergos.net

50 GiB for £5 per month

Usernames taken on a first come first served basis
Questions?

Kevin O’Dwyer
kevin@peergos.org
beta.peergos.net
book.peergos.org

@peergos

Control your data.
Control your destiny.