

Peer-to-Peer Consensus via Authoring Reputation



www.freechains.org

Francisco Sant'Anna

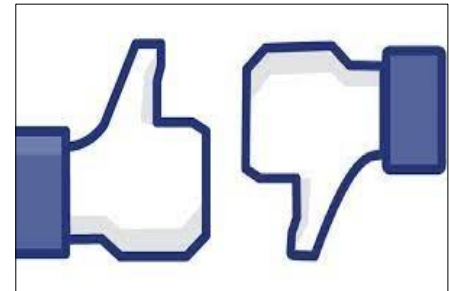
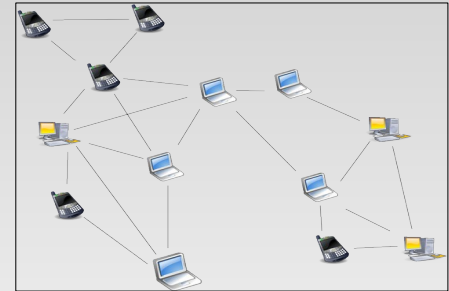
francisco@ime.uerj.br

 [@_fsantanna](https://twitter.com/_fsantanna)



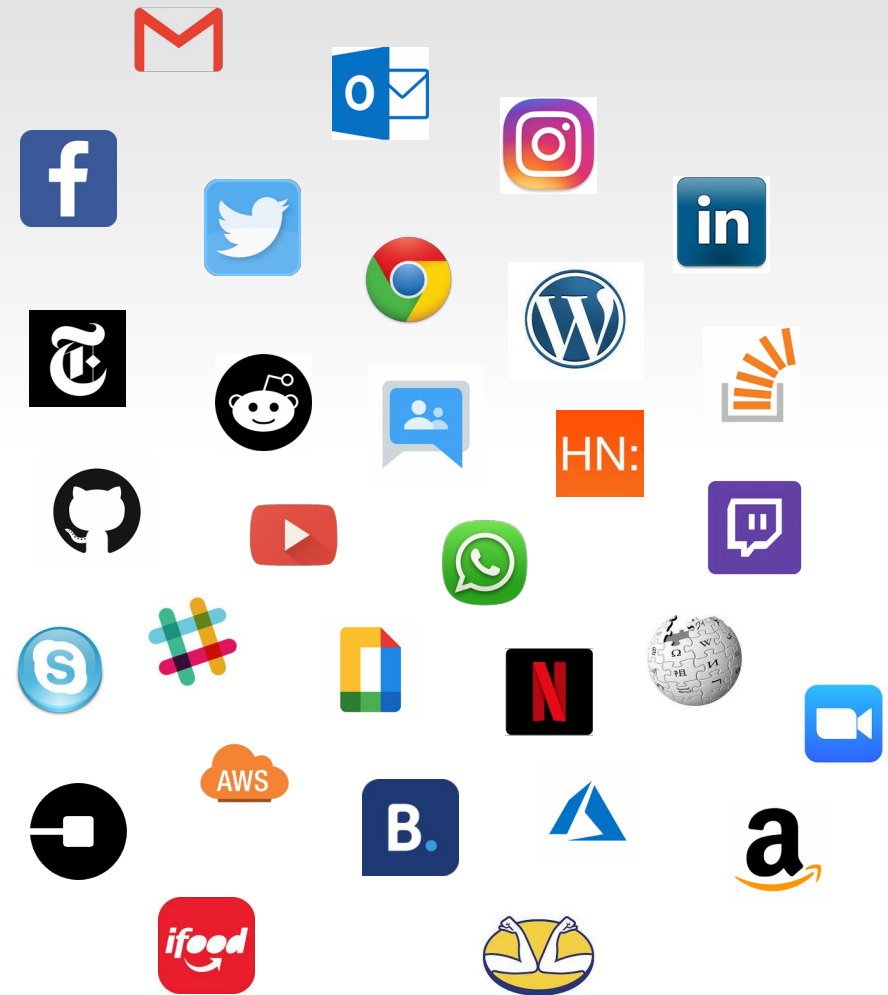
Peer-to-Peer Consensus via Authoring Reputation

- Peer-to-Peer network
- Content created by users
- Authoring reputation
- Consensus based on reputation



Content Publishing

- E-mail
- Social media
- Webpages, News, Blogs
- Forums, Mailing lists
- Collaborative platforms
- Media streaming
- Instant Messages, Chat
- Teleconference
- Cloud Storage
- Services (delivery, auction)



Internet Centralization

- Very few companies...
 - Collect and control our data
 - “Algorithmize” our consumption
 - Obstruct competition



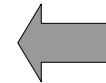
Peer-to-Peer Alternatives

- Eliminate intermediaries
- Push responsibilities to users
(data & connectivity)
- New challenges!
 - no authority
 - no infrastructure



Public Forums

- Untrusted (possibly malicious) communication
 - abuse: excess, SPAM, fake news, illegal content
- Messages should...
 1. reach all users (even those temporarily disconnected)
 2. arrive in a consistent order
 3. be respectful and on topic
- Peer-to-Peer systems?
 - Bitcoin (1,2) ✓

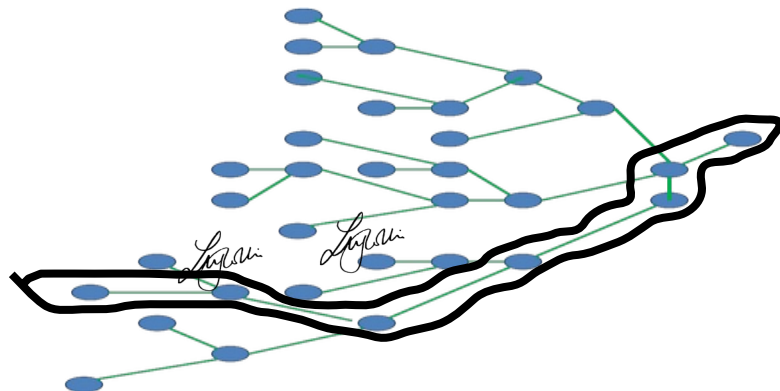


**Consensus via
Authoring Reputation**



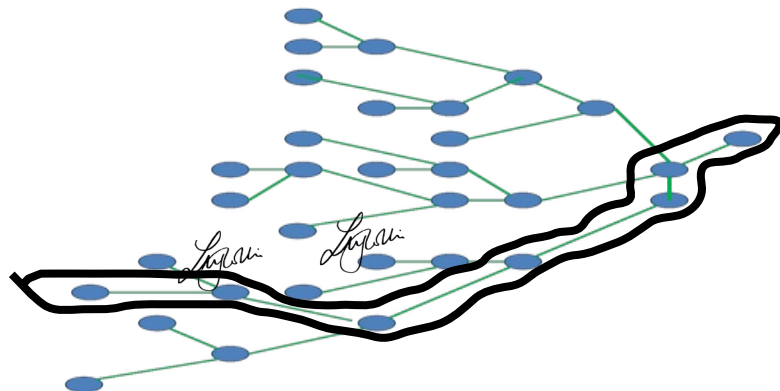
Bitcoin

- Permissionless consensus protocol
- Scarce virtual assets (*bitcoin tokens*)
- **Proof-of-work** to reach consensus and earn *bitcoins*
- Solves the *double-spending* problem
- **No subjective** judgment about transactions



Our Proposal

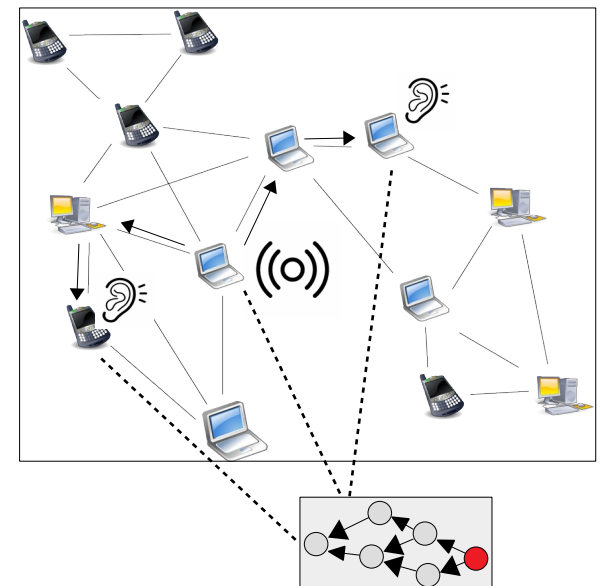
- Permissionless consensus protocol
- Scarce virtual assets (*reps* tokens)
- *Authoring reputation* to reach consensus and earn *reps*
- Solves the *double-spending* problem
- *Subjective* judgment about posts (*likes & dislikes*)



Freechains

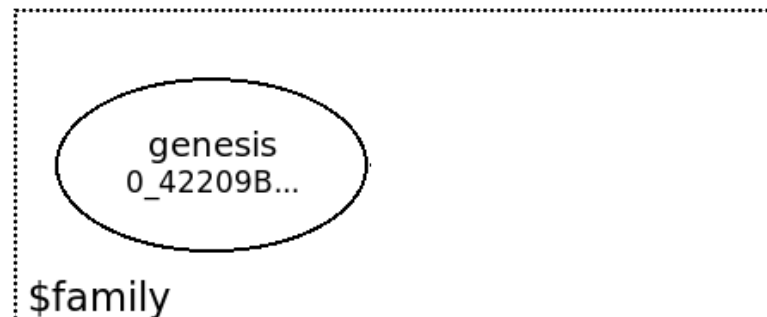
- Topic-based *pubsub*, Unstructured P2P
- Topic (*chain*) is a replicated Merkle DAG

| Type | Prefix | Examples |
|-----------------|--------|---|
| Private Group | \$ | - E-mails - WhatsApp groups - Backup of documents. |
| Public Identity | @ | - News sites - Streaming services - Public profiles in social media |
| Public Forum | # | - Q&A forums - Chats - Consumer-to-consumer sales |



Demo - Private Group

```
> freechains-host start /tmp/freechains/  
Freechains v0.8.4  
Waiting for connections on Host(..., port=8330)...  
  
> freechains crypto shared 'senha-muito-forte'  
FD6C47C27F5CF6839EDE047CE7EE4285E633E26CBA929913  
  
> freechains chains join '$family' FD6C47...  
42209BBF280D4444E39ECEA199C23037058D4F66629D90D7BF1B8C9088B8D0ED  
  
> freechains chain '$family' post inline 'Good morning!'  
1_EF5DE364B7F9C0D40550E01FB9AB510F4AFFBBD79DF54302B68B7DB2ECD3F550
```



Demo - Private Group (Peer 2)

```
> freechains-host --port=8331 start '/tmp/8331/'
Freechains v0.8.4
Waiting for connections on Host(..., port=8331)...

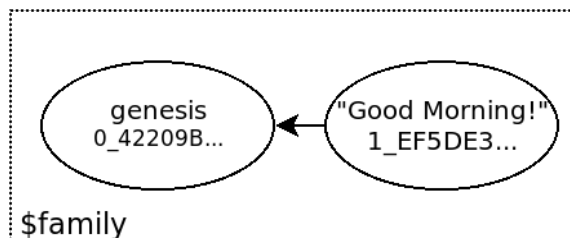
> freechains --port=8331 crypto shared 'strong-password'
FD6C47C27F5CF6839EDE047CE7EE4285E633E26CBA929913

> freechains --port=8331 chains join '$family' FD6C47...
42209BBF280D4444E39ECEA199C23037058D4F66629D90D7BF1B8C9088B8D0ED

> freechains --port=8331 peer localhost:8330 recv '$family'
1/1

> freechains --port=8331 chain '$family' heads
1_EF5DE364B7F9C0D40550E01FB9AB510F4AFFBBD79DF54302B68B7DB2ECD3F550

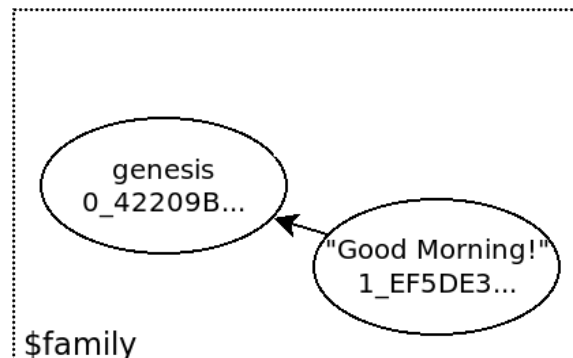
> freechains --port=8331 chain '$family' get payload 1_EF5DE3...
Good Morning!
```



Forks

- Typical DAGs are not lists (local-first *dApps*)
 - Fundamental obstacle for consensus

```
> freechains --port=8331 chains join '$family' FD6C47...  
42209BBF280D4444E39ECEA199C23037058D4F66629D90D7BF1B8C9088B8D0ED  
  
> freechains --port=8331 chain '$family' post inline "I'm also here!"  
1_A224FCA3F66E1A1CD68812AA51DCAF6699DA1ABC44561D37AB1EE1001AB429A  
  
> freechains --port=8331 peer localhost:8330 recv '$family'  
1/1
```



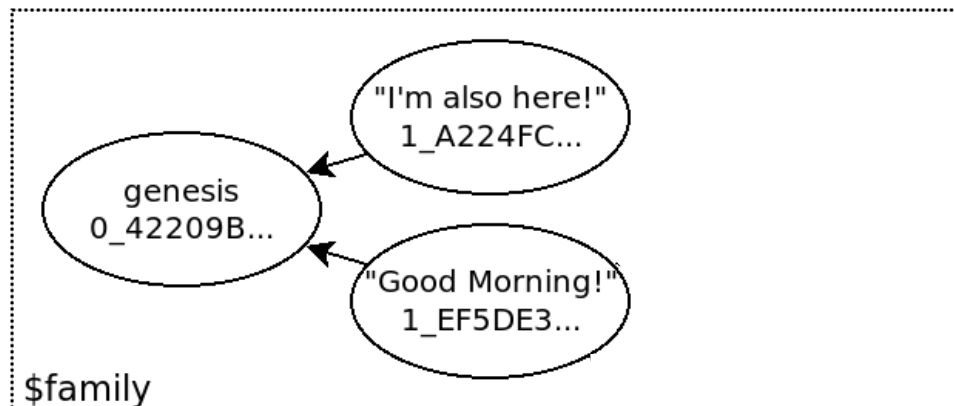
Likes and Dislikes

...

```
> freechains crypto pubpvt 'my-password'  
328B7D... 35CA69...
```

```
> freechains chain '$family' like 1_EF5DE36... --sign=35CA69...  
2_DDA222EDFD4BE333CF2017D54E91900806DF5006CAC35DFB3E97CD0690EDB22E
```

```
> freechains chain '$family' reps 1_EF5DE36...  
1
```



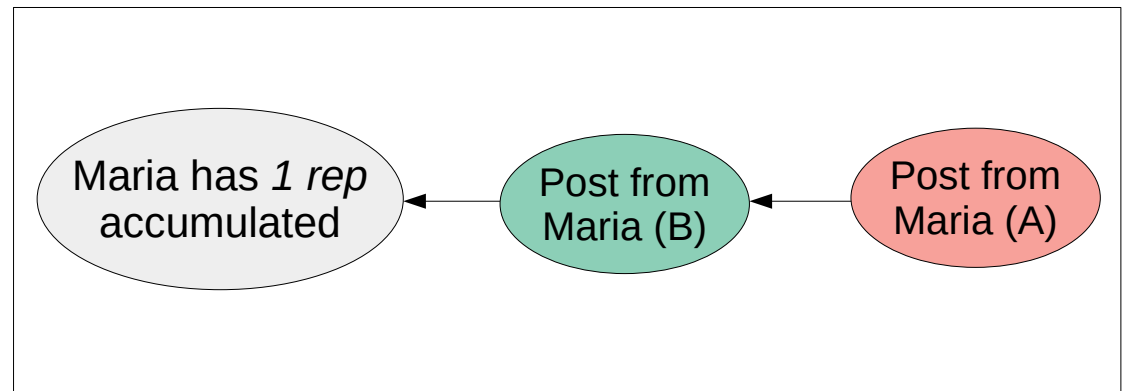
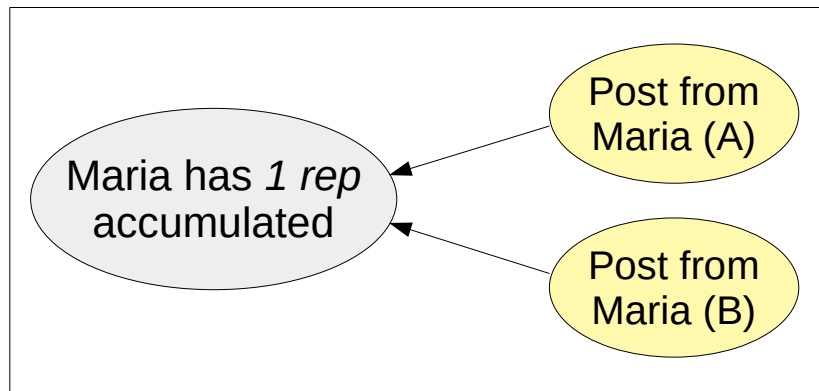
Public Forums

- **Permissionless** public forums
- Sybil attacks
 - generate fake IDs and disseminate SPAM
- Token *reps* to post and rate content
 - New posts expend *reps*
 - Old posts award *reps*
 - human work immune to *automation*
 - Likes & Dislikes transfer *reps*

| Operation | Effect | Goal |
|-----------|--|--|
| Emission | Old posts award <i>reps</i> to author. | Encourage content authoring. |
| Expense | New posts deduct <i>reps</i> from author temporarily. | Discourage excess of content. |
| Transfer | Likes & dislikes transfer <i>reps</i> between authors. | Highlight content of quality. Combat abusive content. |

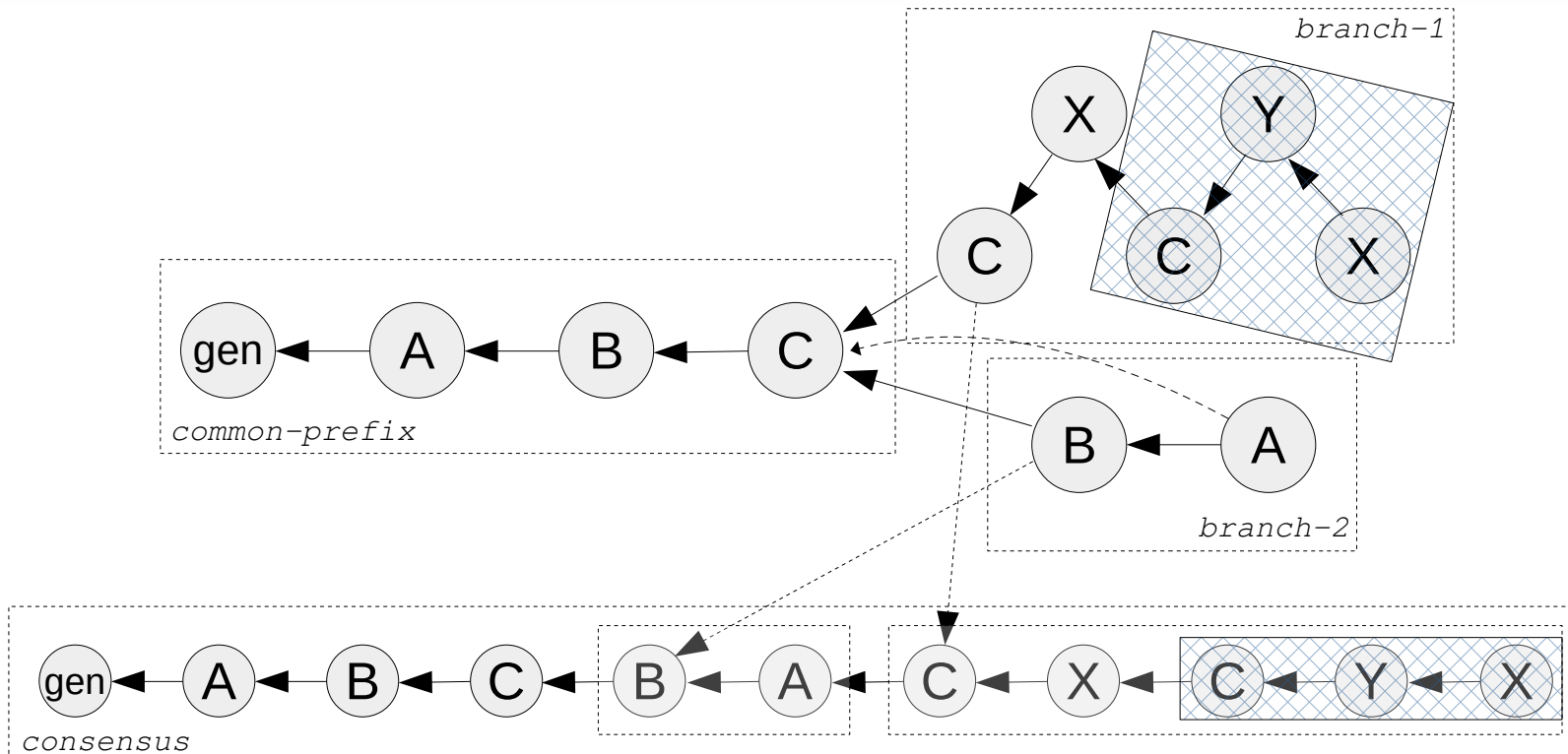
Reputation & Consensus

- Scarce operations are not yet sufficient
 - ✓ ■ Sybils
 - ✗ ■ Conflicting operations (double spend)
- Need for consensus
 - But how to determine a total order among messages?



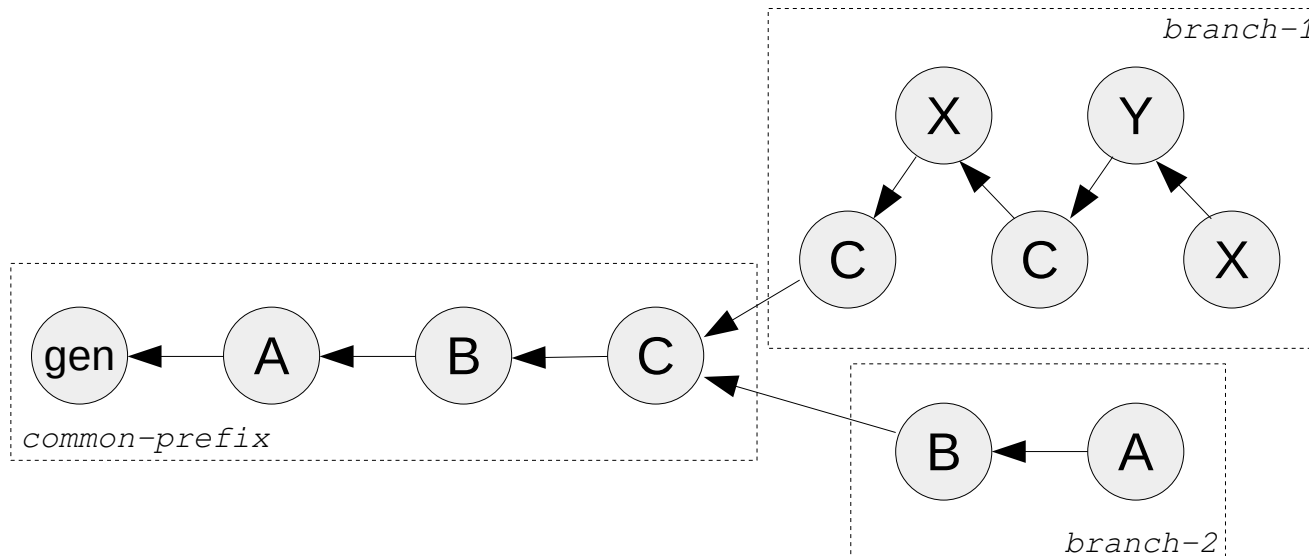
Consensus Criteria

- Favor branches with more reputation
 - **c-prefix:** $\text{reps}(A) + \text{reps}(B) > \text{reps}(C)$
 - **branch-1:** C high activity
 - **branch-2:** A/B low activity



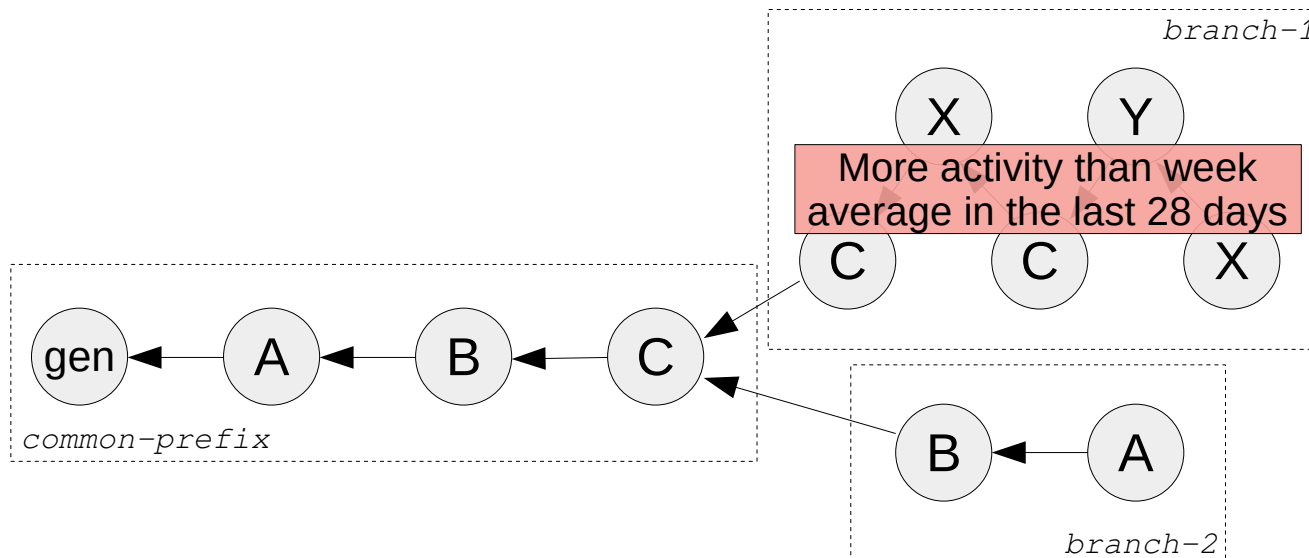
Consensus Criteria

- Favor branches with more reputation
- Blocks after a failure “never existed”
- Peers may need to reorder blocks
- What if *branch-1* is legit?



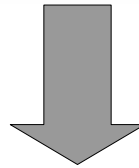
Consensus Criteria

- a) Branch with more reputation is ordered first
- b) Hard fork if other branch has 7+ days of posts



Freechains - Public Forums

| Operation | Effect | Goal |
|-----------|--|--|
| Emission | Old posts award <i>reps</i> to author. | Encourage content authoring. |
| Expense | New posts deduct <i>reps</i> from author temporarily. | Discourage excess of content. |
| Tranfer | Likes & dislikes transfer <i>reps</i> between authors. | Highlight content of quality. Combat abusive content. |



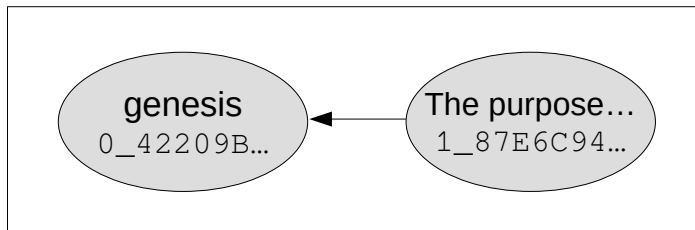
| | | | |
|-------------|-----|----------|---------------------------------|
| Emission | 1.a | pioneers | +30 <i>reps</i> to pioneers |
| | 1.b | old post | +1 <i>rep</i> to author (>24h) |
| Expense | 2 | new post | -1 <i>rep</i> to author (0-12h) |
| Tranfer | 3.a | like | -1 <i>rep</i> -> +1 <i>rep</i> |
| | 3.b | dislike | -1 <i>rep</i> -> -1 <i>rep</i> |
| Constraints | 4.a | min | +1 <i>rep</i> to post |
| | 4.b | max | +30 <i>reps</i> max |
| | 4.c | size | 128Kb max |

Demo - Public Forum

```
> freechains crypto pubpvt 'pioneer-password'
ADB56B... CBBA77...

> freechains chains join '#forum' ADB56B...
42209BBF280D4444E39ECEA199C23037058D4F66629D90D7BF1B8C9088B8D0ED

> freechains chain '#forum' post --sign=CBBA77... \
    inline 'The purpose of this chain is...'
1_87E6C94F232F7182B6E1DF3ACE48DAC08BA999A7CEA3A4FF08DED9AA18C78FE2
```



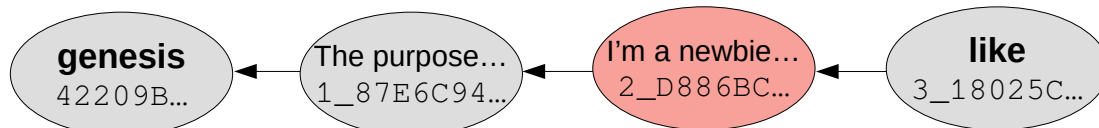
```
Pioneer: 30 reps (1.a)
          29 reps (2)
          30 reps (2)
```

| | | | |
|-------------|-----|----------|--------------------------|
| Emission | 1.a | pioneers | +30 reps to pioneers |
| | 1.b | old post | +1 rep to author (>24h) |
| Expense | 2 | new post | -1 rep to author (0-12h) |
| Tranfer | 3.a | like | -1 rep -> +1 rep |
| | 3.b | dislike | -1 rep -> -1 rep |
| Constraints | 4.a | min | +1 rep to post |
| | 4.b | max | +30 reps max |
| | 4.c | size | 128Kb max |


```
> freechains crypto pubpvt 'new-author-password'
5DCF47... EFA735...

> freechains chain '#forum' post --sign=EFA735... \
  inline "I'm a newbie..."
2_D886BC6DDD6343BB7A01B33270158BE45DE47358B48CF7C2F46D5EAE8D52806

> freechains chain '#forum' like 2_D886BC... --sign=CBBA77...
3_18025C6A9FDC322762EF9BA8A3B1D24973D2271077F9777D4645D5B6F435BBA8
```



```
Pioneer: 30 reps
          29 reps (3.a)

Newbie:   0 reps
          0 reps (2)
          1 rep (3.a)
          1 reps (2)
          2 reps (1.b)
```

| | | | |
|-------------|-----|----------|---------------------------------|
| Emission | 1.a | pioneers | +30 <i>reps</i> to pioneers |
| | 1.b | old post | +1 <i>rep</i> to author (>24h) |
| Expense | 2 | new post | -1 <i>rep</i> to author (0-12h) |
| Transfer | 3.a | like | -1 <i>rep</i> -> +1 <i>rep</i> |
| | 3.b | dislike | -1 <i>rep</i> -> -1 <i>rep</i> |
| Constraints | 4.a | min | +1 <i>rep</i> to post |
| | 4.b | max | +30 <i>reps</i> max |
| | 4.c | size | 128Kb max |

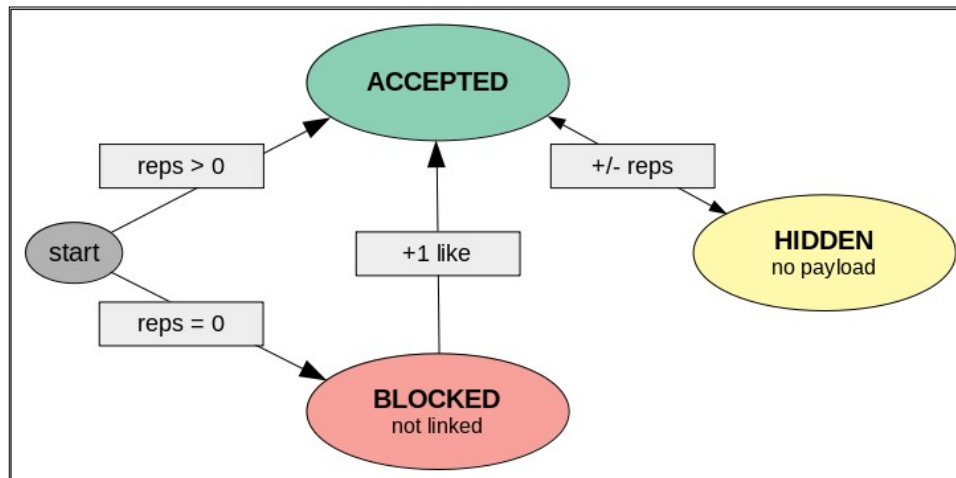
Reputation System

- Rule **pioneers** (1.a) bootstraps chains
- Rule *old post* (1.b) stimulates authoring
- Rule *new post* (2) prevents SPAM with dynamic cost
- Rule *like* (3.a) welcomes new users at a cost
- Rule *dislike* (3.b) censors abusive content
- Rule *min* (4.a) blocks Sybils
- Rule *max* (4.b) stimulates rating and decentralization
- Rule *size* (4.c) prevents DDoS

| | | | |
|-------------|-----|----------|--------------------------|
| Emission | 1.a | pioneers | +30 reps to pioneers |
| | 1.b | old post | +1 rep to author (>24h) |
| Expense | 2 | new post | -1 rep to author (0-12h) |
| Transfer | 3.a | like | -1 rep -> +1 rep |
| | 3.b | dislike | -1 rep -> -1 rep |
| Constraints | 4.a | min | +1 rep to post |
| | 4.b | max | +30 reps max |
| | 4.c | size | 128Kb max |

Likes & Dislikes

1. Welcoming new users
 2. Measuring quality of posts
 3. Censoring abuse (SPAM, fake news, etc)
- Post is hidden with at least 3 dislikes and less likes



| | | | |
|-------------|-----|----------|---------------------------------|
| Emission | 1.a | pioneers | +30 <i>reps</i> to pioneers |
| | 1.b | old post | +1 <i>rep</i> to author (>24h) |
| Expense | 2 | new post | -1 <i>rep</i> to author (0-12h) |
| Transfer | 3.a | like | -1 <i>rep</i> -> +1 <i>rep</i> |
| | 3.b | dislike | -1 <i>rep</i> -> -1 <i>rep</i> |
| Constraints | 4.a | min | +1 <i>rep</i> to post |
| | 4.b | max | +30 <i>reps</i> max |
| | 4.c | size | 128Kb max |

Reputation & Consensus

- P2P permissionless consensus based on reputation
- Reputation:
 - Generation is expensive
 - Verification is cheap (and distributed)
- Consensus:
 - Human authoring ability as a scarce resource
 - vs extrinsic resources (dispendious, opaque, oddly distributed)

Contributions

- Make decentralized public forums viable
 - Reputation & Consensus mechanism
 - Depends exclusively on human work
 - Any system that structure messages as DAGs
 - Supports local-first software
 - *Freechains* peer-to-peer system
- Support CRDTs in collaborative platforms
 - Causal order (DAGs) + Total order (consensus)

Peer-to-Peer Consensus via Authoring Reputation



www.freechains.org

Francisco Sant'Anna

francisco@ime.uerj.br

 @_fsantanna

