Peer-to-Peer Permissionless Consensus via Reputation

Francisco Sant'Anna, Fabio Bosisio, Lucas Pires

github.com/Freechains

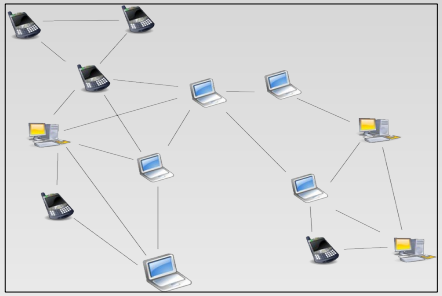
Francisco Sant'Anna

francisco@ime.uerj.br

@_fsantanna

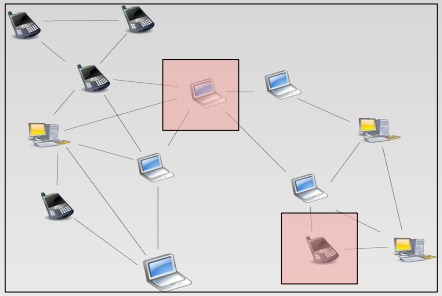
Peer-to-Peer Permissionless Consensus via Reputation

Peer-to-Peer Permissionless Consensus via Reputation



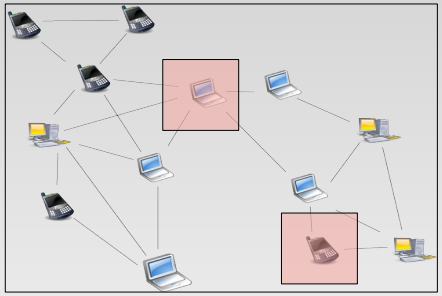
- Peer-to-Peer / **Permissionless**

Peer-to-Peer Permissionless Consensus via Reputation



- Peer-to-Peer / **Permissionless**

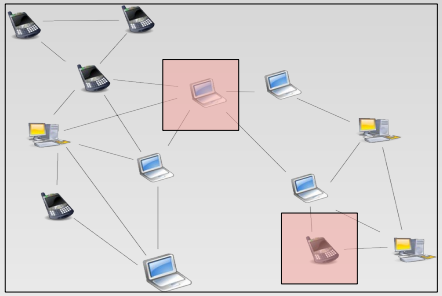
Peer-to-Peer Permissionless Consensus via Reputation

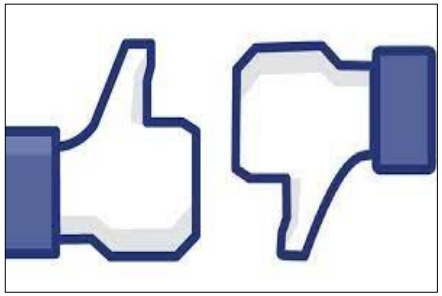


- Peer-to-Peer / **Permissionless**
- Users → Content

Peer-to-Peer Permissionless Consensus via Reputation

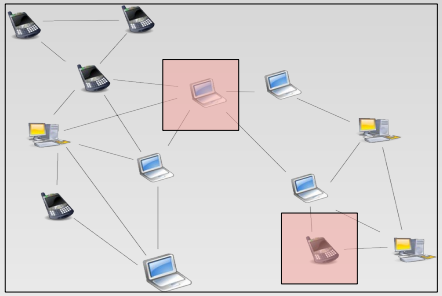
- Peer-to-Peer / **Permissionless**
- Users → Content
- Content → Reputation

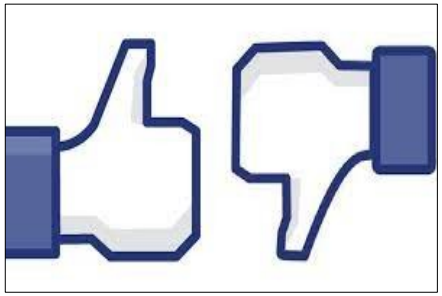




Peer-to-Peer Permissionless Consensus via Reputation

- Peer-to-Peer / **Permissionless**
- Users → Content
- Content → Reputation
- Reputation → Consensus





Public Forums

Public Forums

Public Forums

- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material

Public Forums

- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material
- As a goal, messages must...

Public Forums

- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material
- As a goal, messages must...
  1. reach all users

Public Forums

- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material
- As a goal, messages must...
  1. reach all users
  2. respect a consistent order

Public Forums

- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material
- As a goal, messages must...
  1. reach all users
  2. respect a consistent order
  3. be harmless and on topic (**subjective!**)

Public Forums

- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material
- As a goal, messages must...
  1. reach all users
  2. respect a consistent order
  3. be harmless and on topic (**subjective!**)
- Permissionless systems?

Public Forums

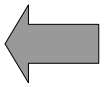
- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material
- As a goal, messages must...
  1. reach all users
  2. respect a consistent order
  3. be harmless and on topic (**subjective!**)
- Permissionless systems?
  - Cryptocurrencies (1,2) ✔

Public Forums

- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material
- As a goal, messages must...
  1. reach all users
  2. respect a consistent order
  3. be harmless and on topic (**subjective!**)
- Permissionless systems?
  - Cryptocurrencies (1,2) ✔

Public Forums

- Possibly malicious communication
  - abuse: excess, SPAM, fake news, illicit material
- As a goal, messages must...
  1. reach all users
  2. respect a consistent order
  3. be harmless and on topic (**subjective!**)



Consensus via Reputation

- Permissionless systems?
  - Cryptocurrencies (1,2) ✔

Parallel with Bitcoin

Parallel with Bitcoin

- Content authoring create reputation
  - (vs proof-of-work)

Parallel with Bitcoin

- Content authoring create reputation
  - (vs proof-of-work)
- Likes and dislikes transfer reputation
  - (vs transactions)

Parallel with Bitcoin

- Content authoring create reputation
  - (vs proof-of-work)
- Likes and dislikes transfer reputation
  - (vs transactions)
- Aggregate reputation determines consensus
  - (vs longest chain)

Parallel with Bitcoin

- Content authoring create reputation
  - (vs proof-of-work)
- Likes and dislikes transfer reputation
  - (vs transactions)
- Aggregate reputation determines consensus
  - (vs longest chain)

How to prevent double spending?

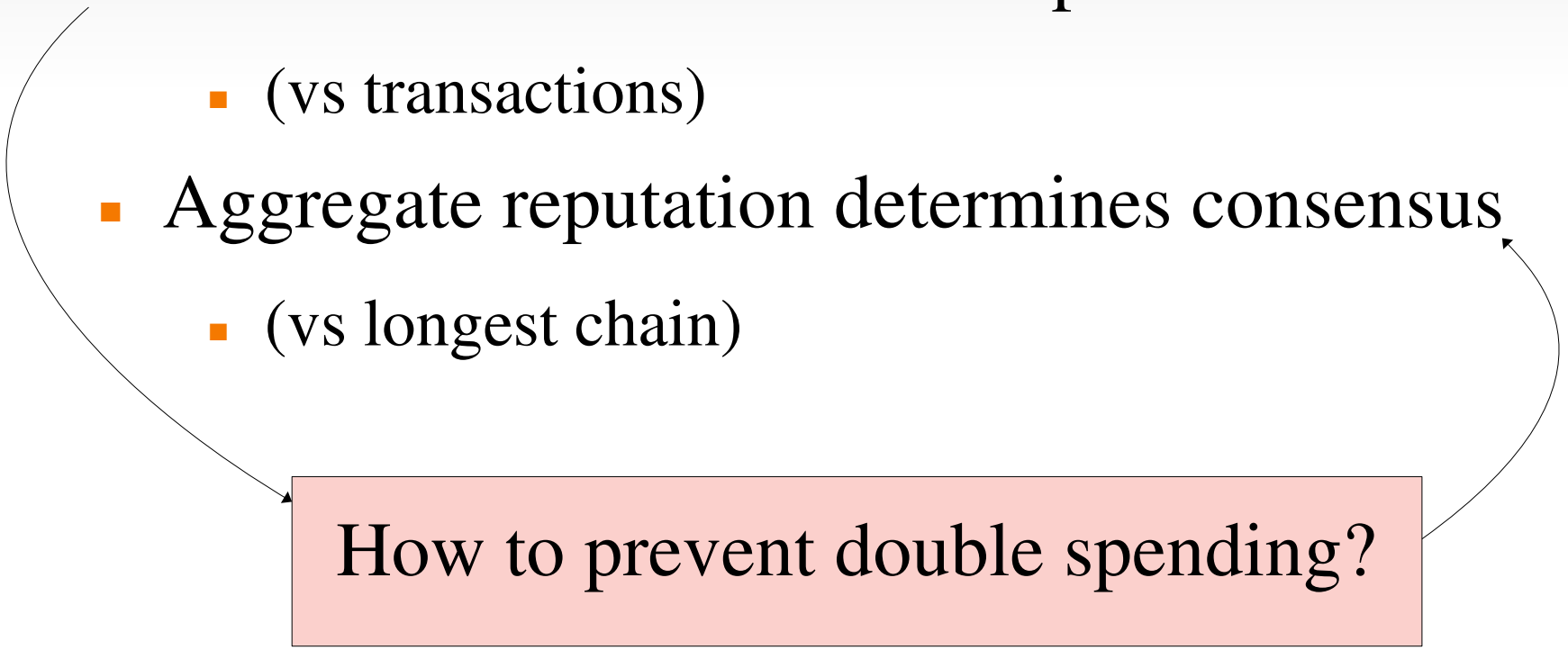
Parallel with Bitcoin

- Content authoring create reputation
  - (vs proof-of-work)
- Likes and dislikes transfer reputation
  - (vs transactions)
- Aggregate reputation determines consensus
  - (vs longest chain)

How to prevent double spending?

Parallel with Bitcoin

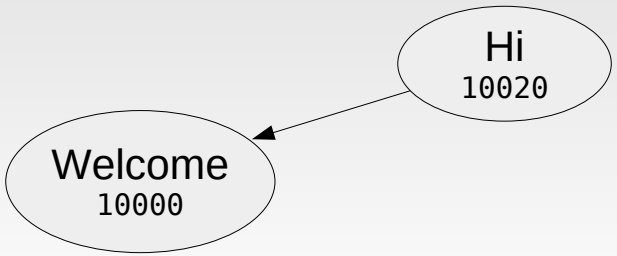
- Content authoring create reputation
  - (vs proof-of-work)
- Likes and dislikes transfer reputation
  - (vs transactions)
- Aggregate reputation determines consensus
  - (vs longest chain)



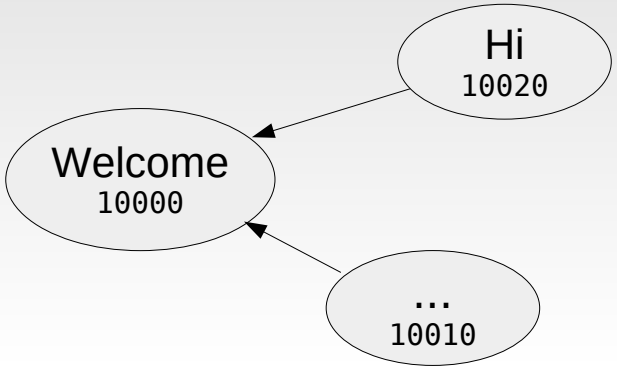
Forums are DAGs

Forums are DAGs

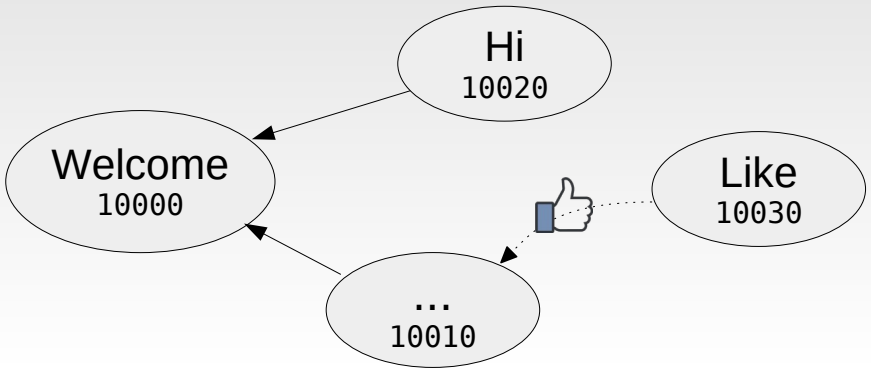
Forums are DAGs



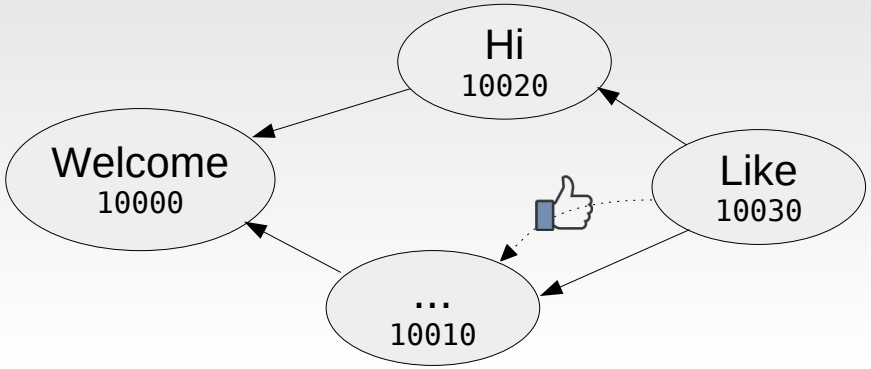
Forums are DAGs



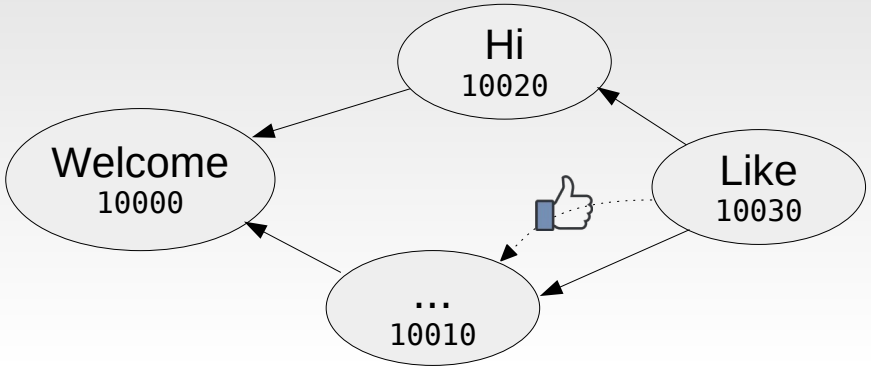
Forums are DAGs



Forums are DAGs

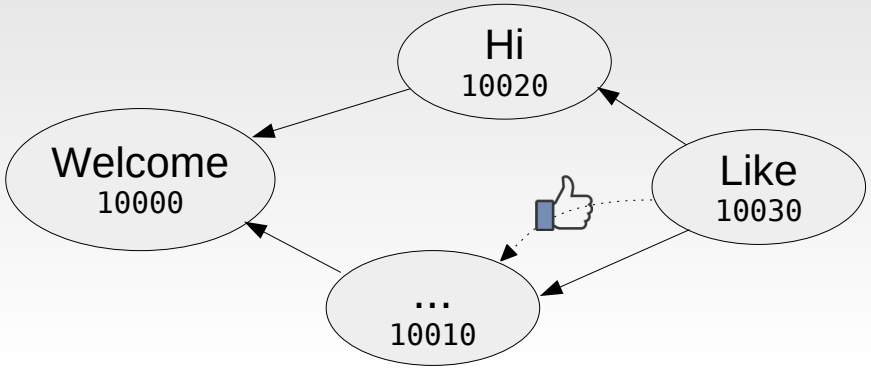


Forums are DAGs



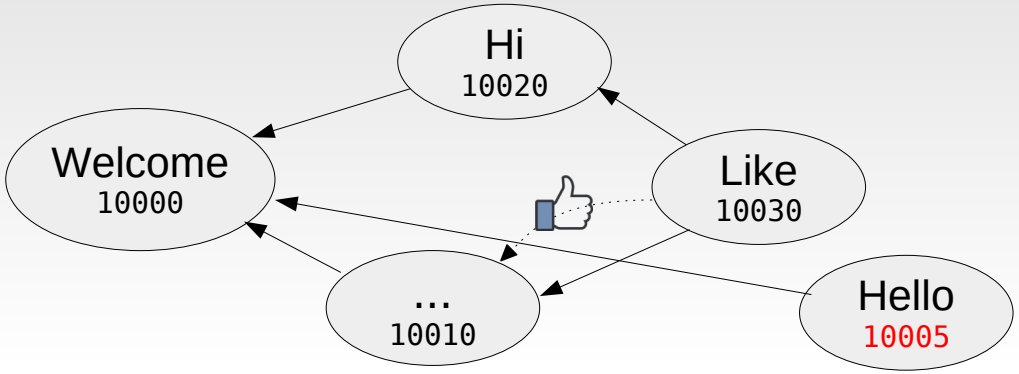
- Permissionless → Untrustworthy

Forums are DAGs



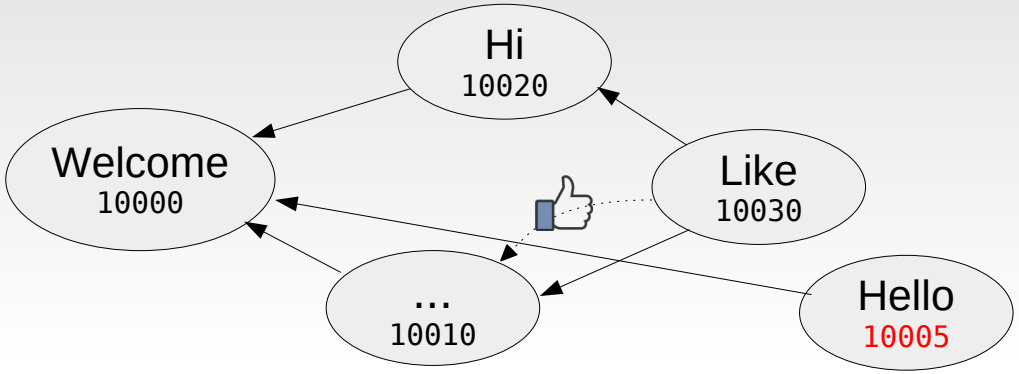
- Permissionless → Untrustworthy
  - Timestamps (order)

Forums are DAGs



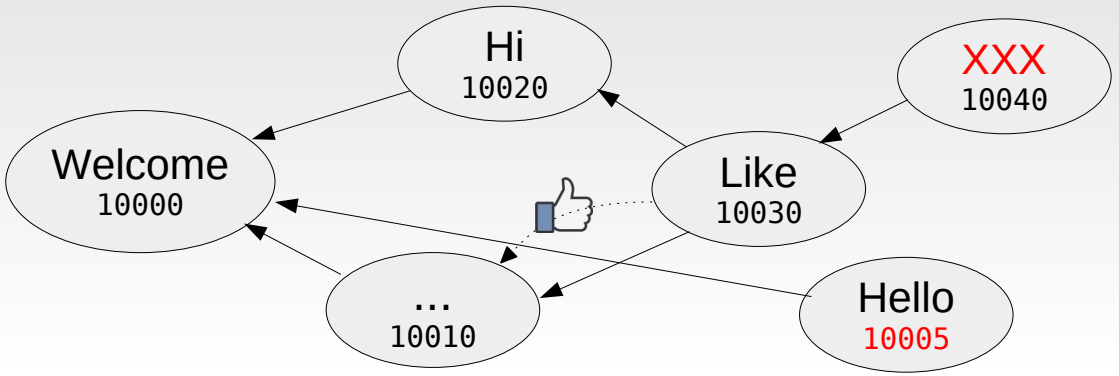
- Permissionless → Untrustworthy
  - Timestamps (order)

Forums are DAGs



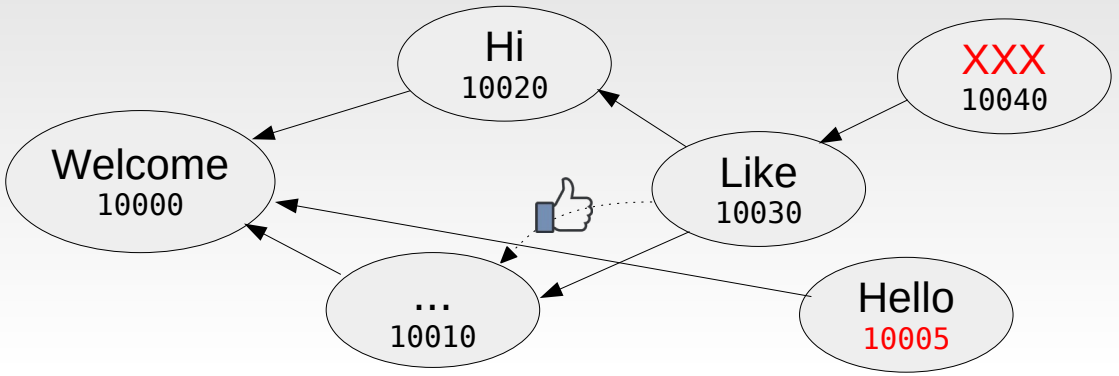
- Permissionless → Untrustworthy
  - Timestamps (order)
  - Content (quality)

Forums are DAGs



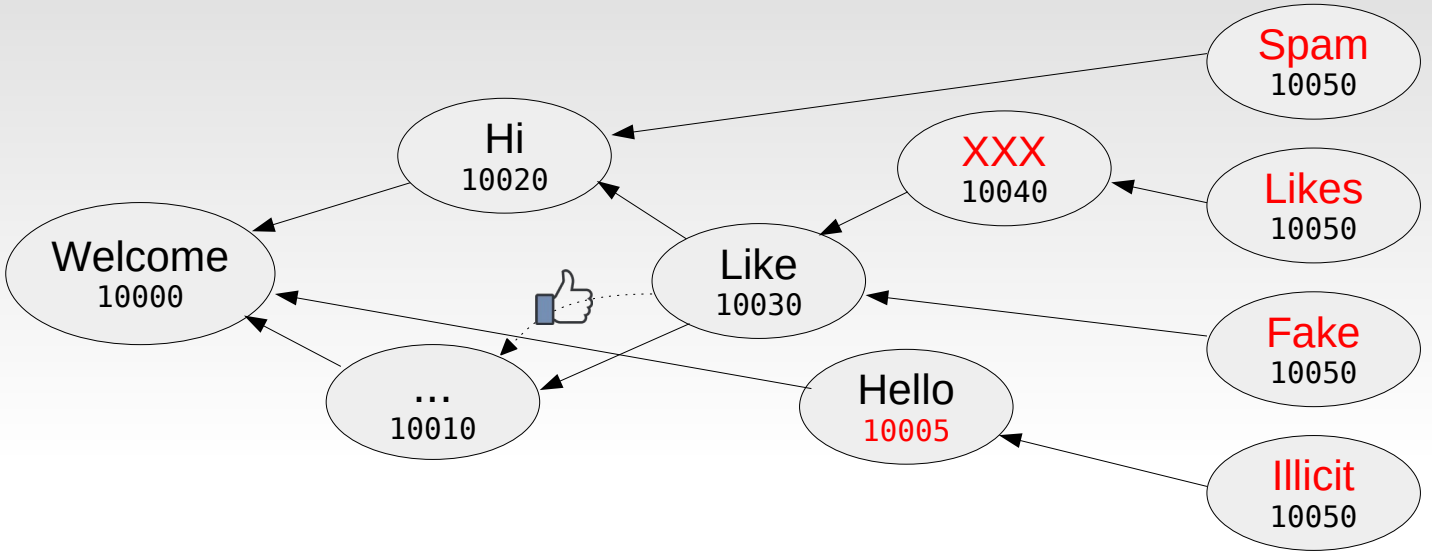
- Permissionless → Untrustworthy
  - Timestamps (order)
  - Content (quality)

Forums are DAGs



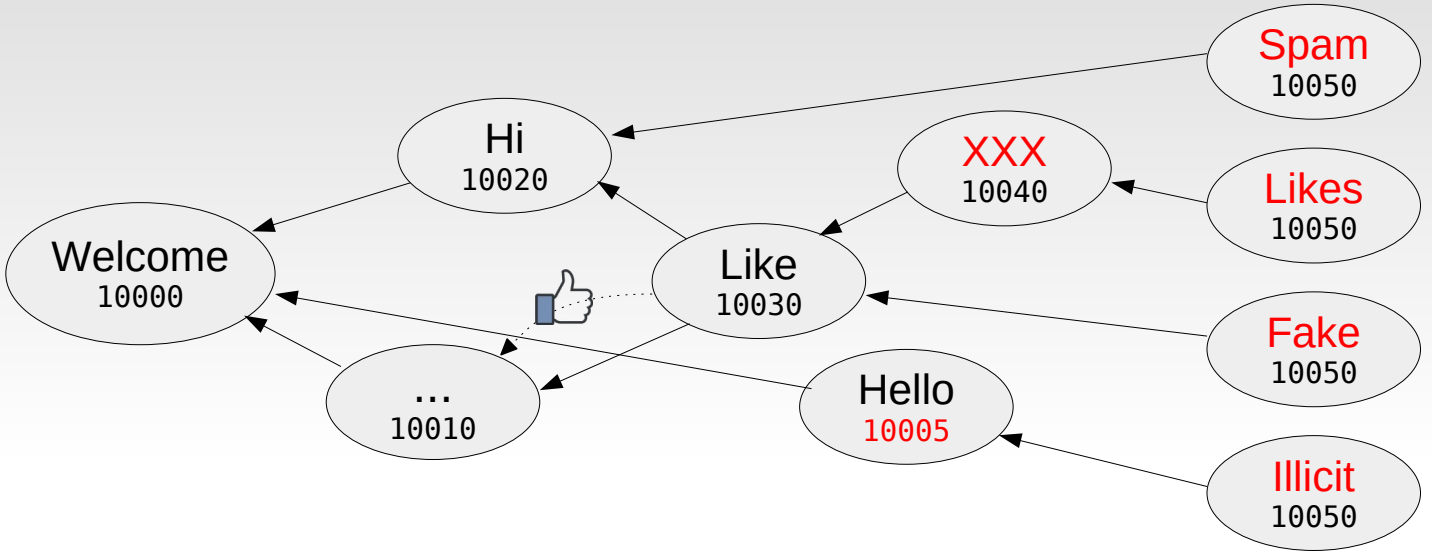
- Permissionless → Untrustworthy
  - Timestamps (order)
  - Content (quality)
  - Sybils (quantity)

Forums are DAGs

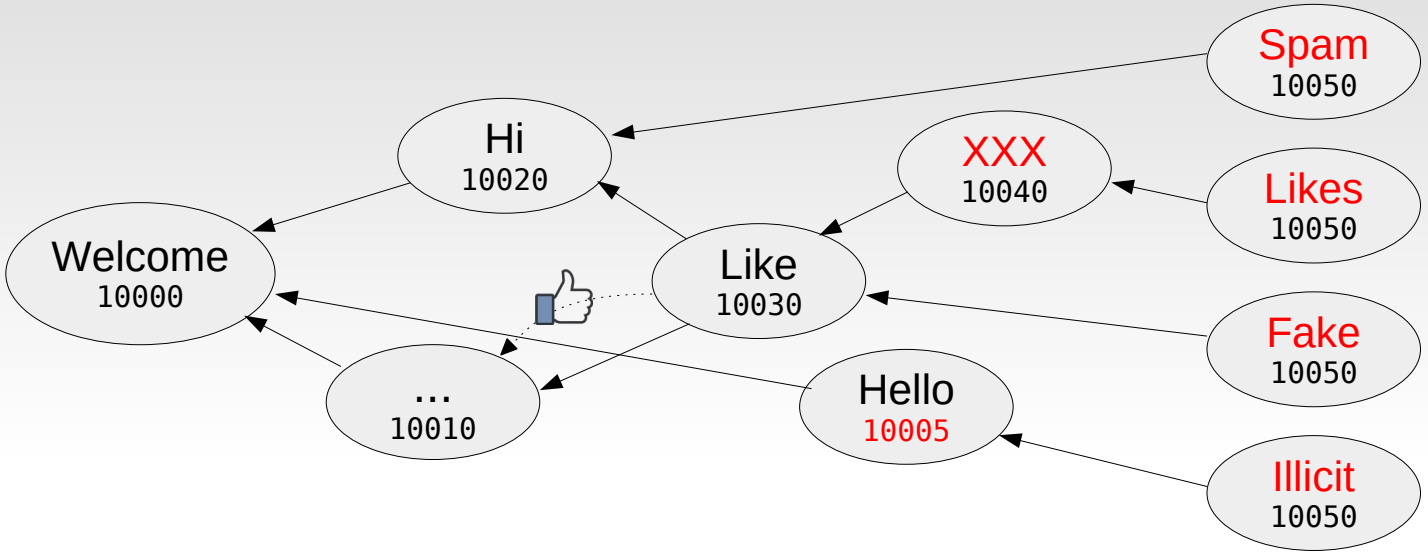


- Permissionless → Untrustworthy
  - Timestamps (order)
  - Content (quality)
  - Sybils (quantity)

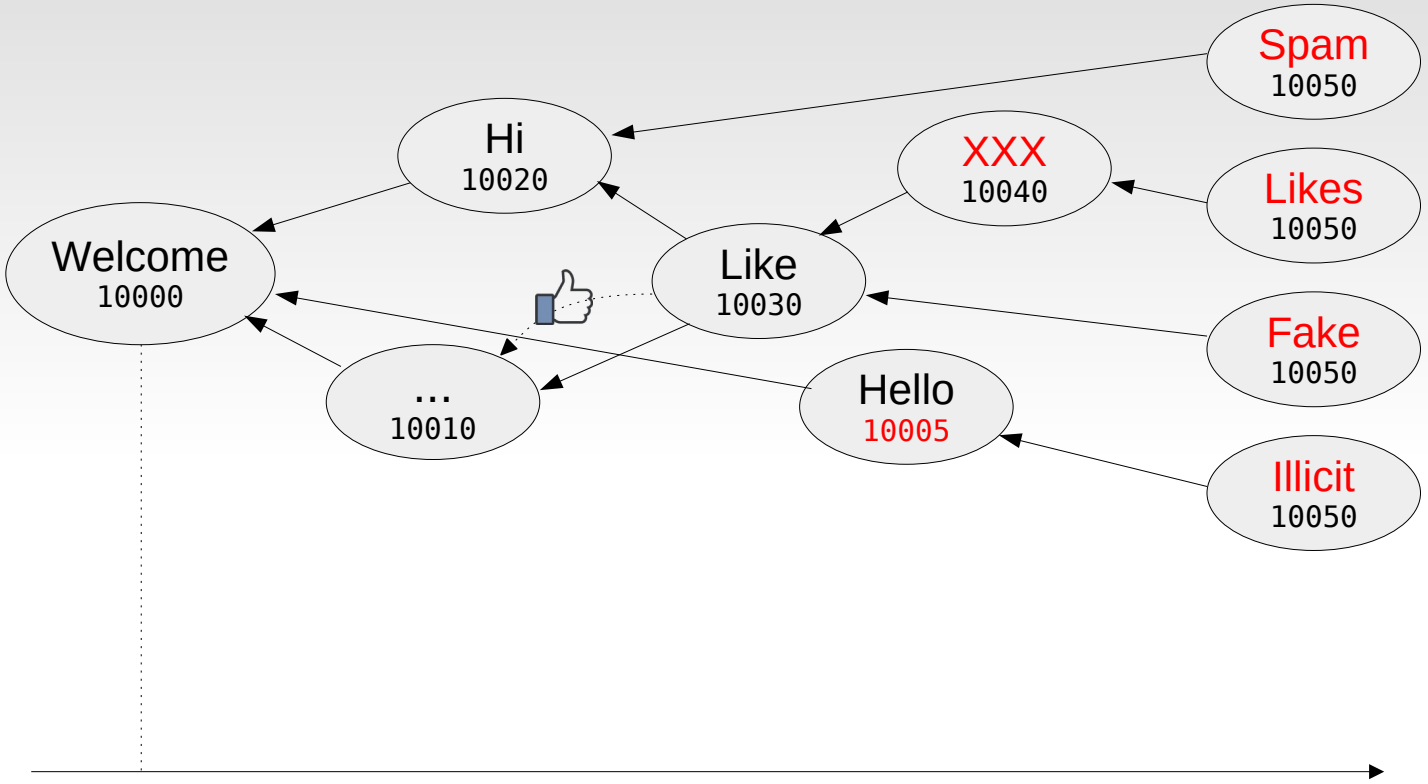
(?) DAGs → Consensus (?)



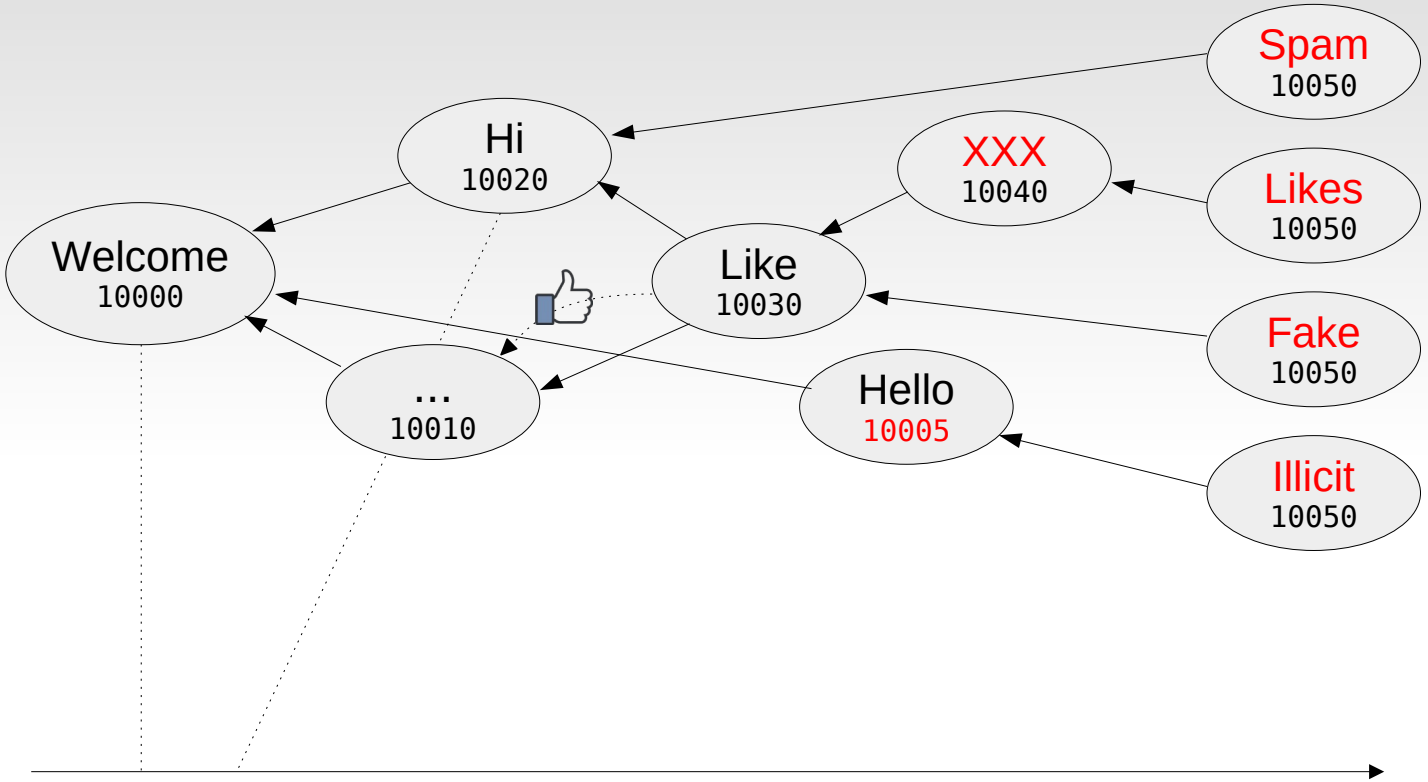
(?) DAGs → Consensus (?)



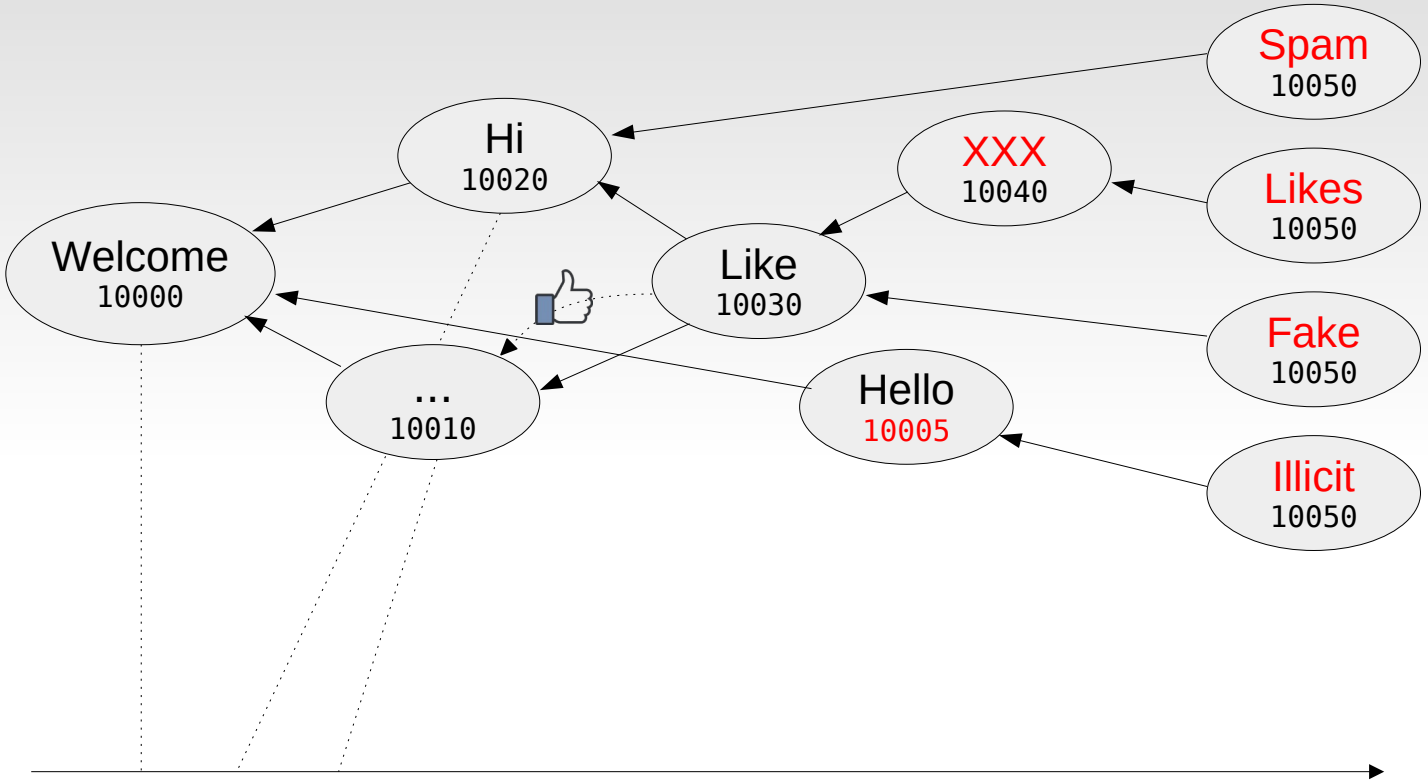
(?) DAGs → Consensus (?)



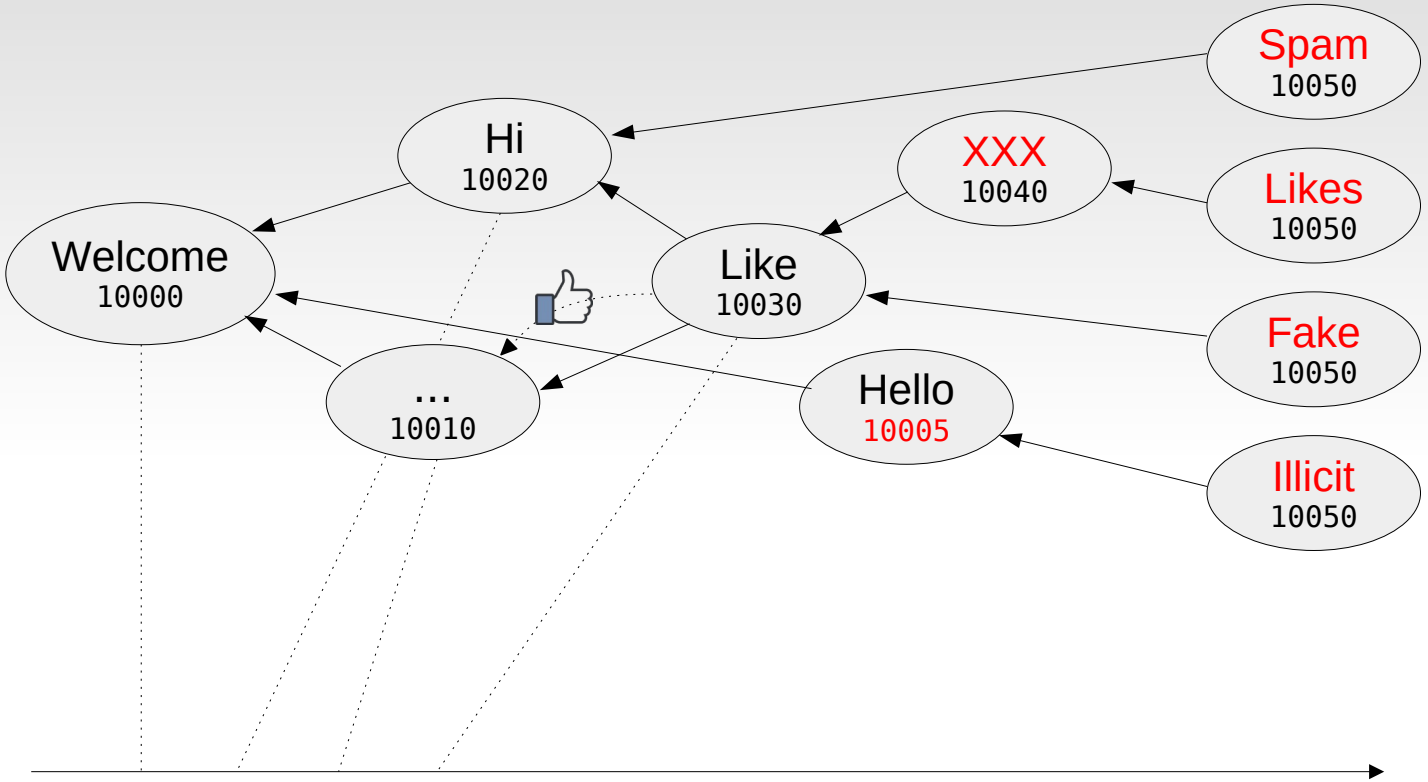
(?) DAGs → Consensus (?)



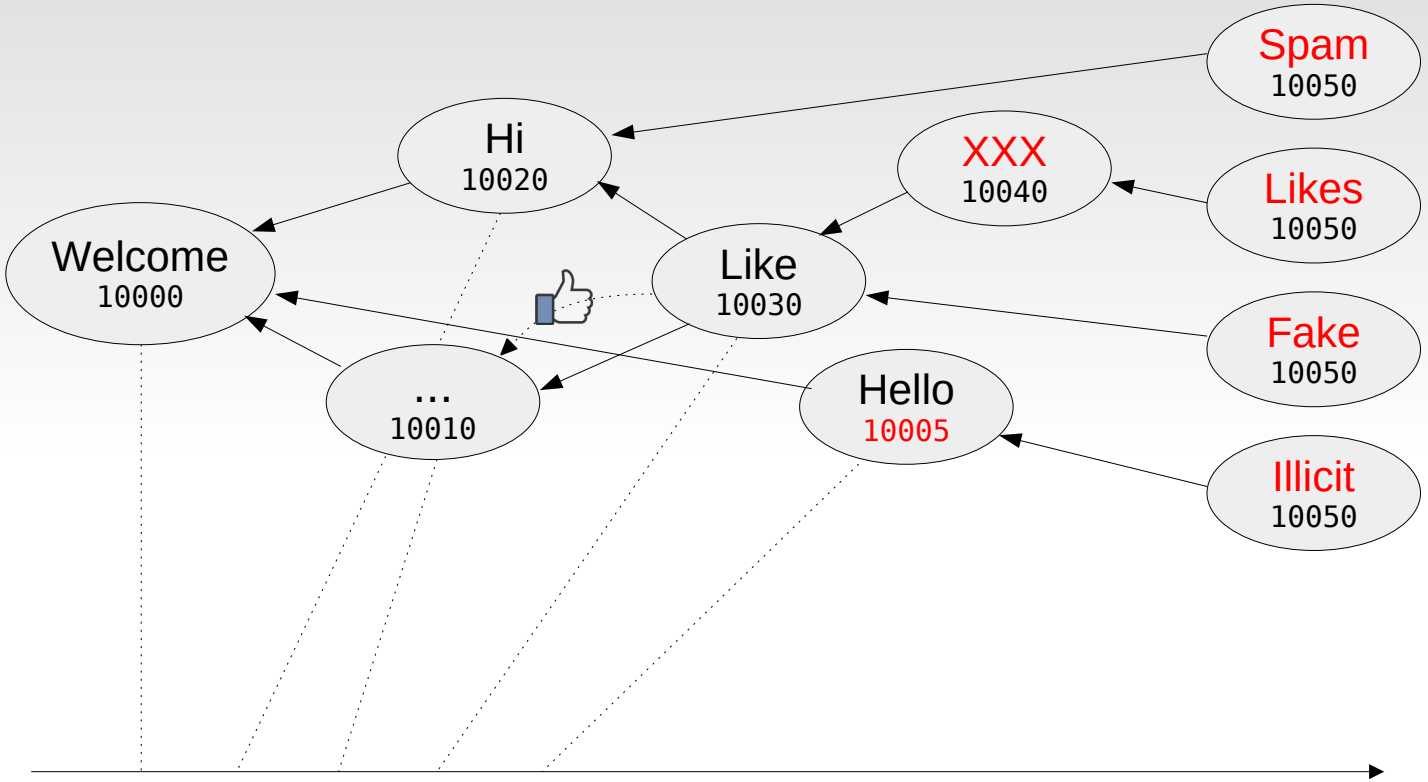
(?) DAGs → Consensus (?)



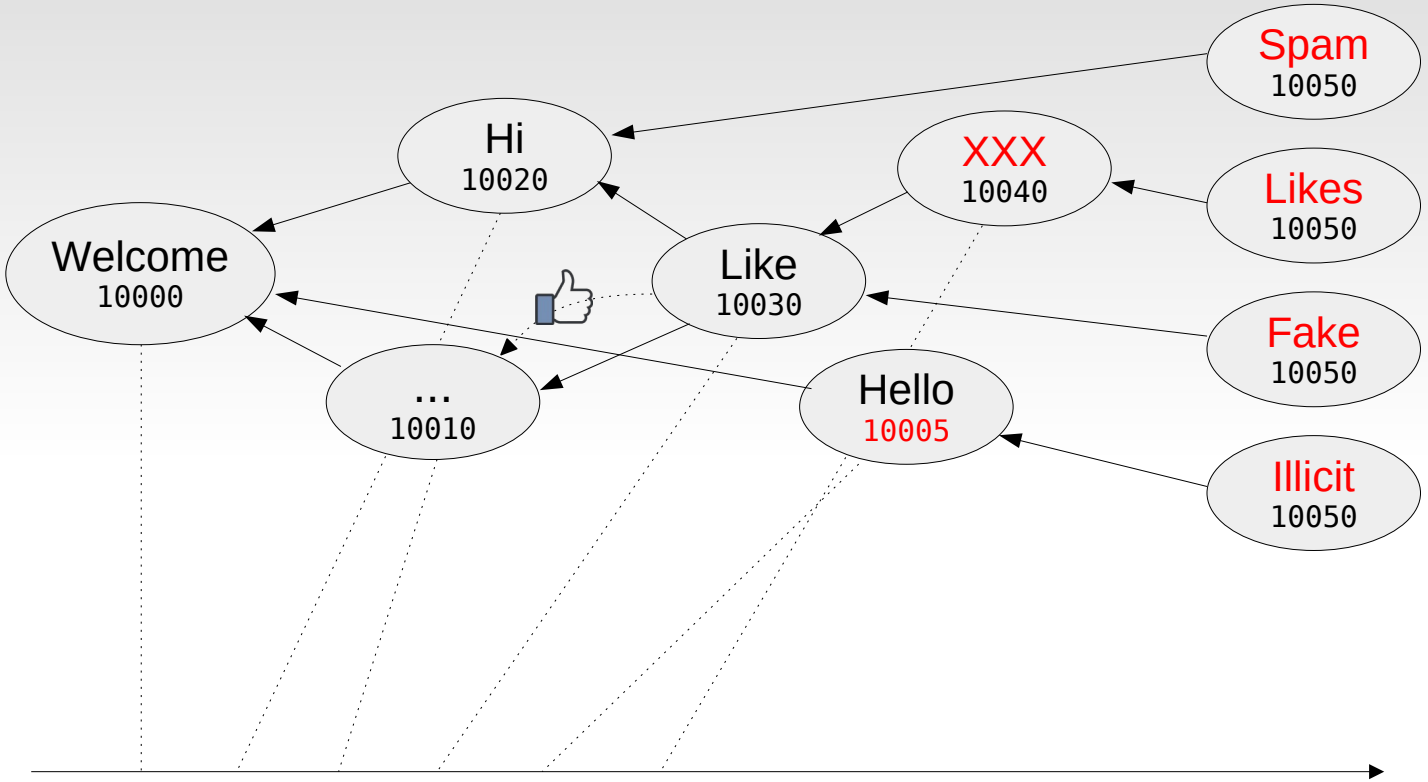
(?) DAGs → Consensus (?)



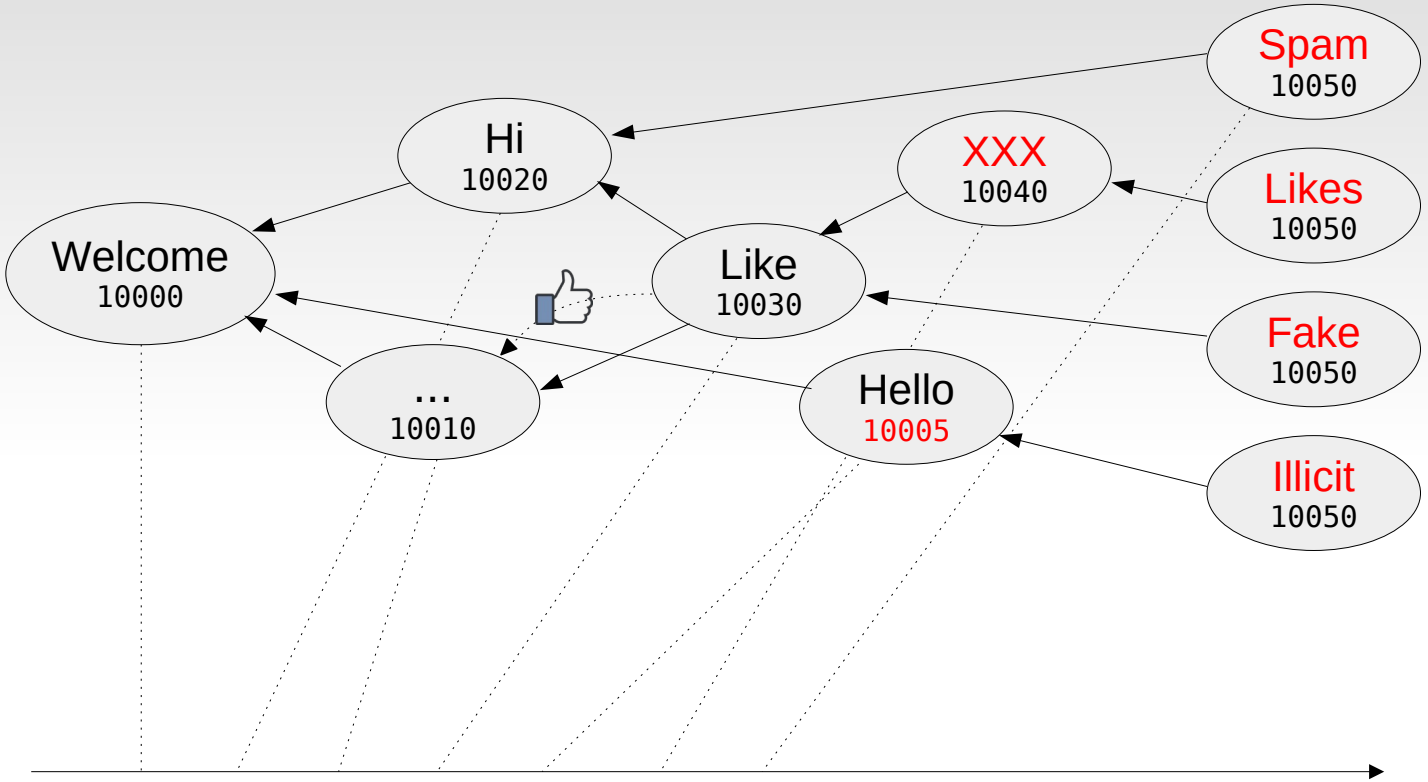
(?) DAGs → Consensus (?)



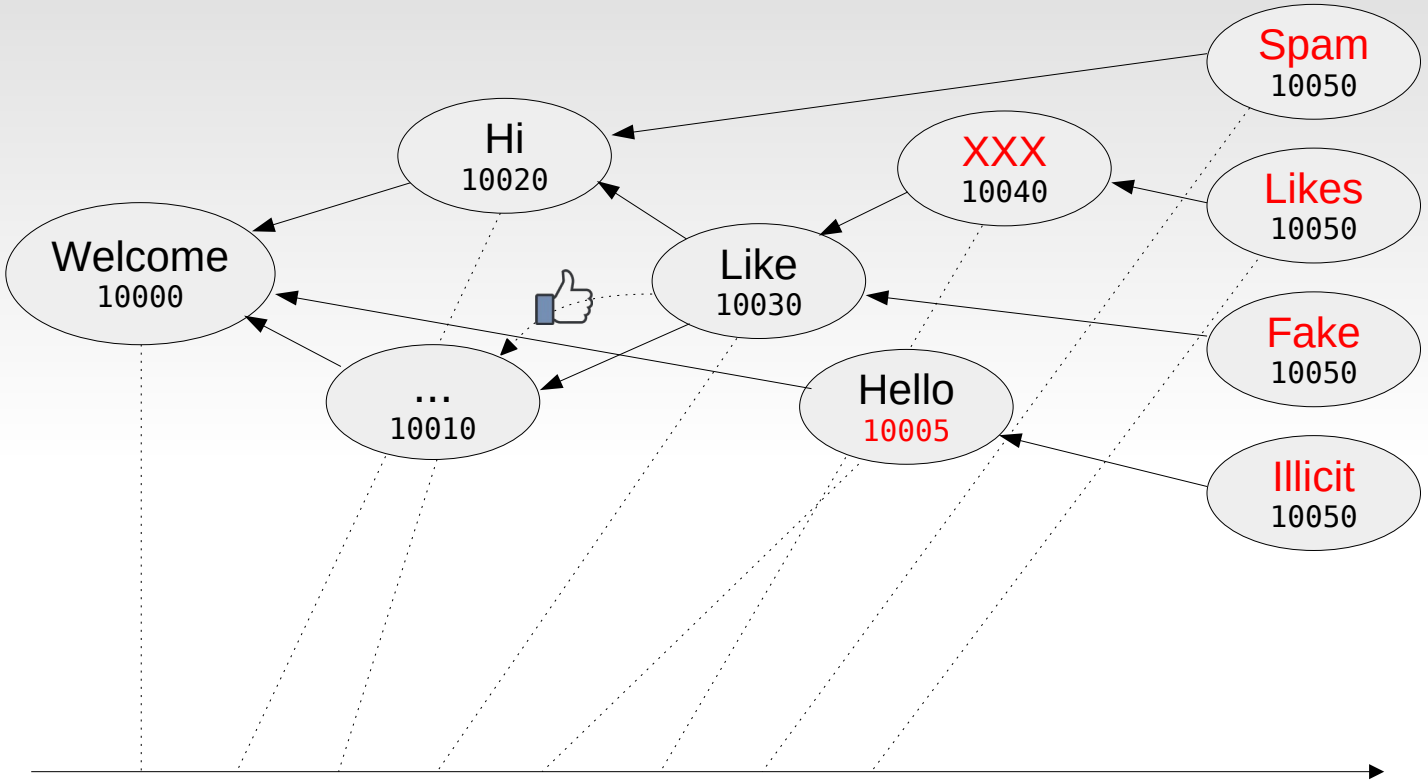
(?) DAGs → Consensus (?)



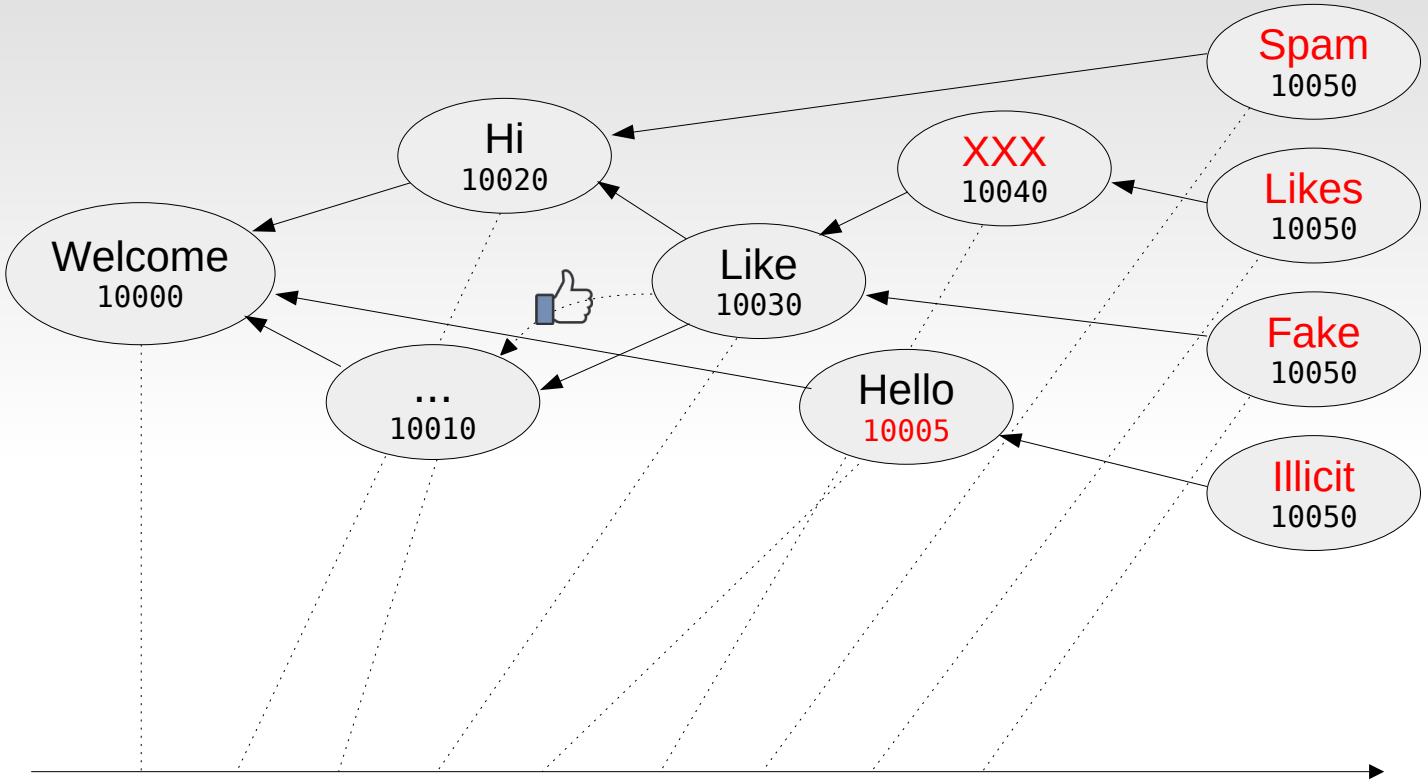
(?) DAGs → Consensus (?)



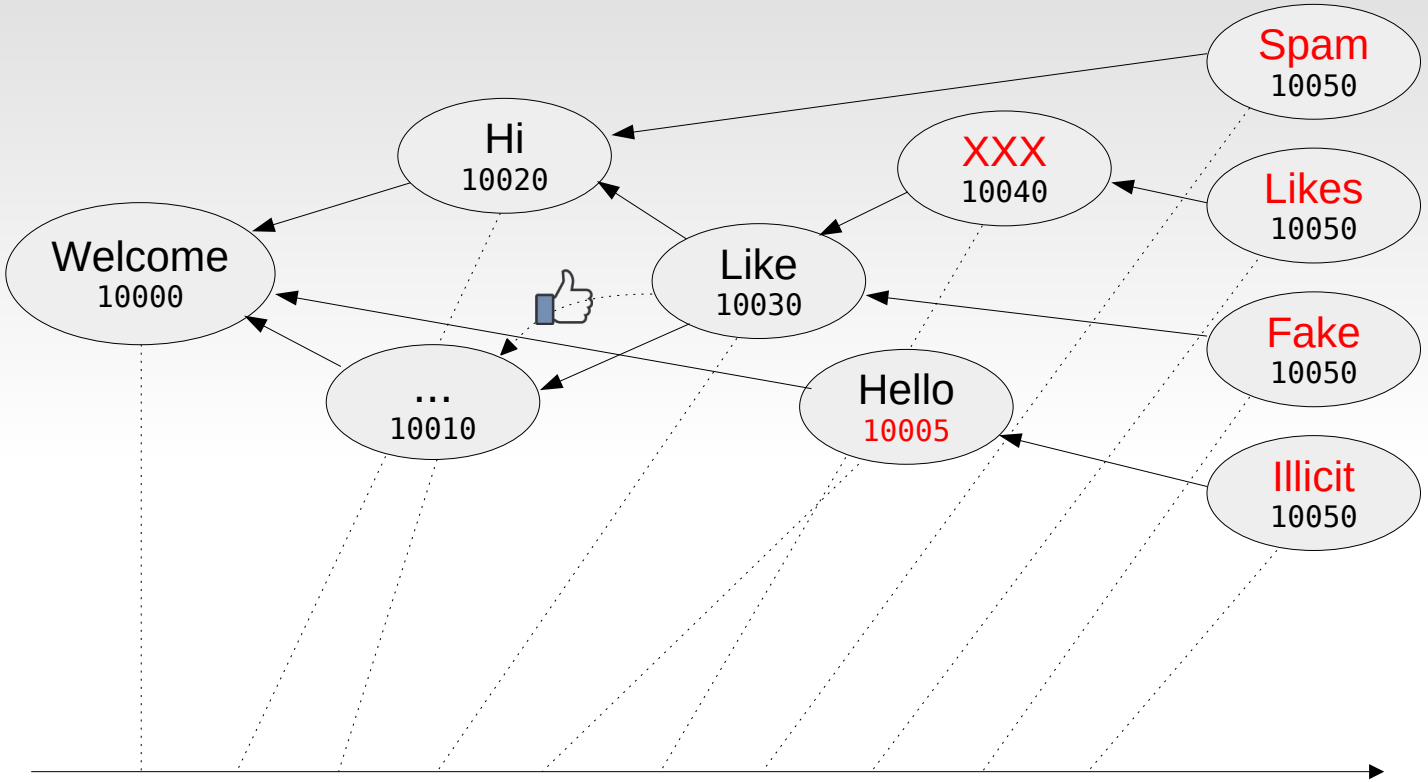
(?) DAGs → Consensus (?)



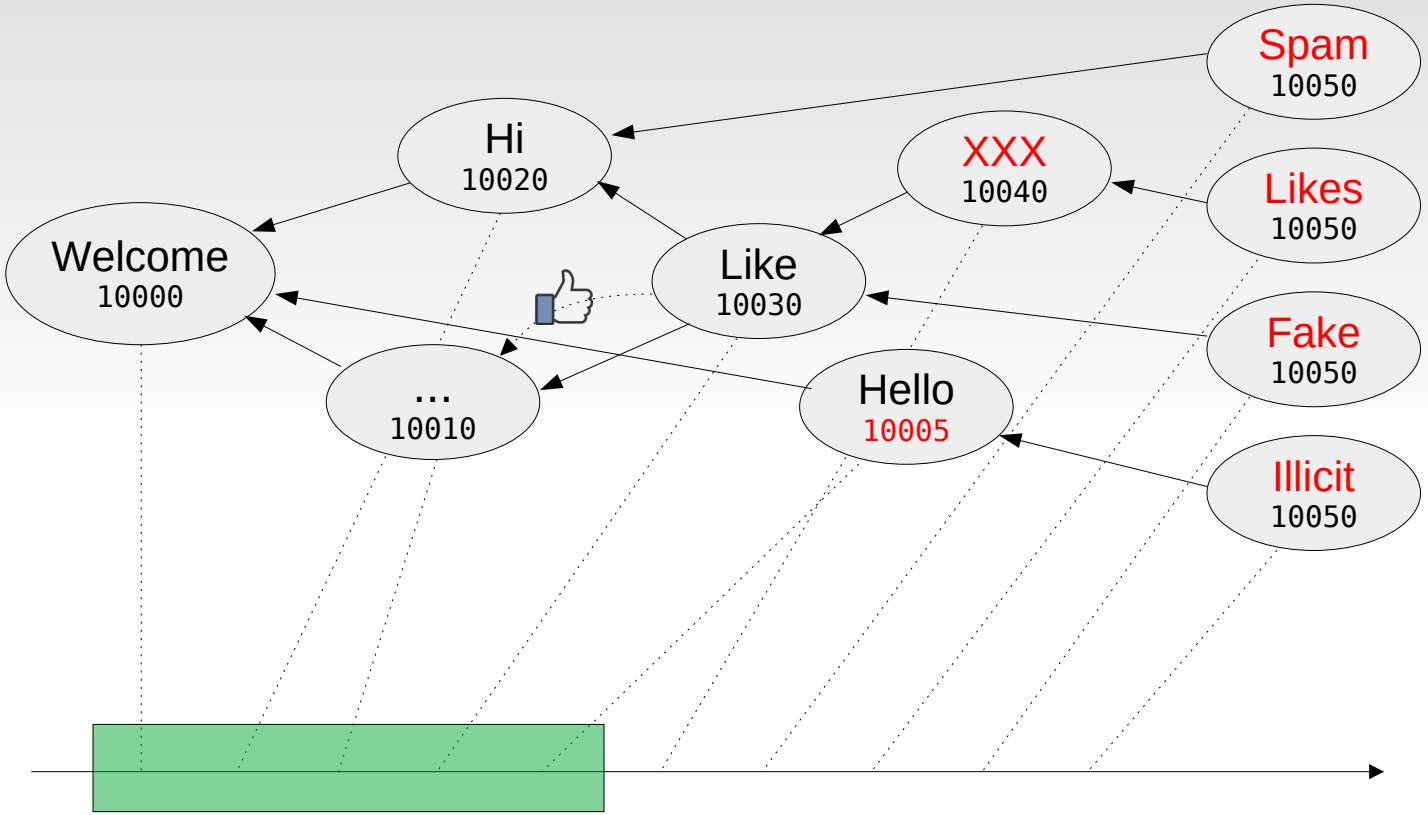
(?) DAGs → Consensus (?)



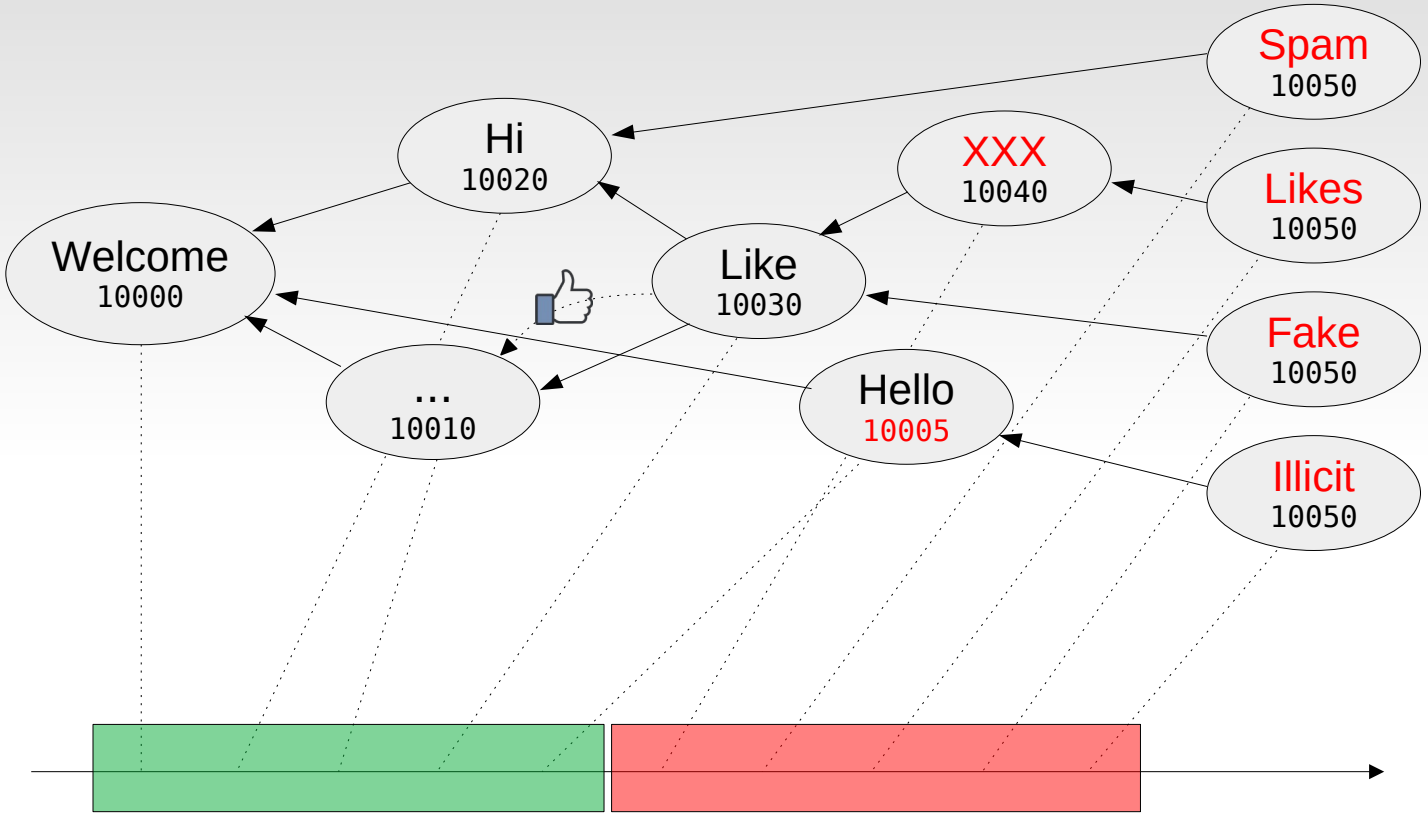
(?) DAGs → Consensus (?)



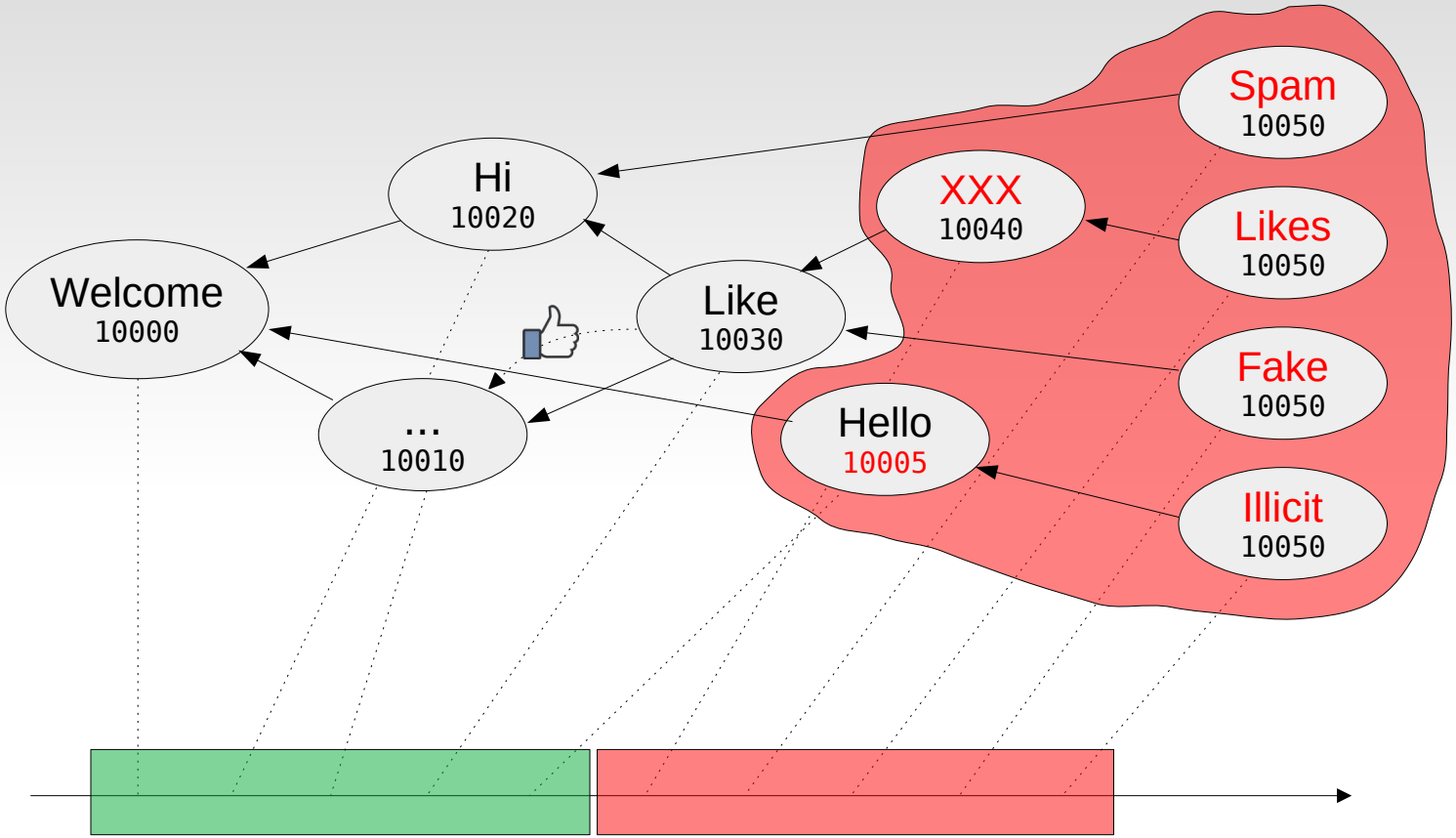
(?) DAGs → Consensus (?)



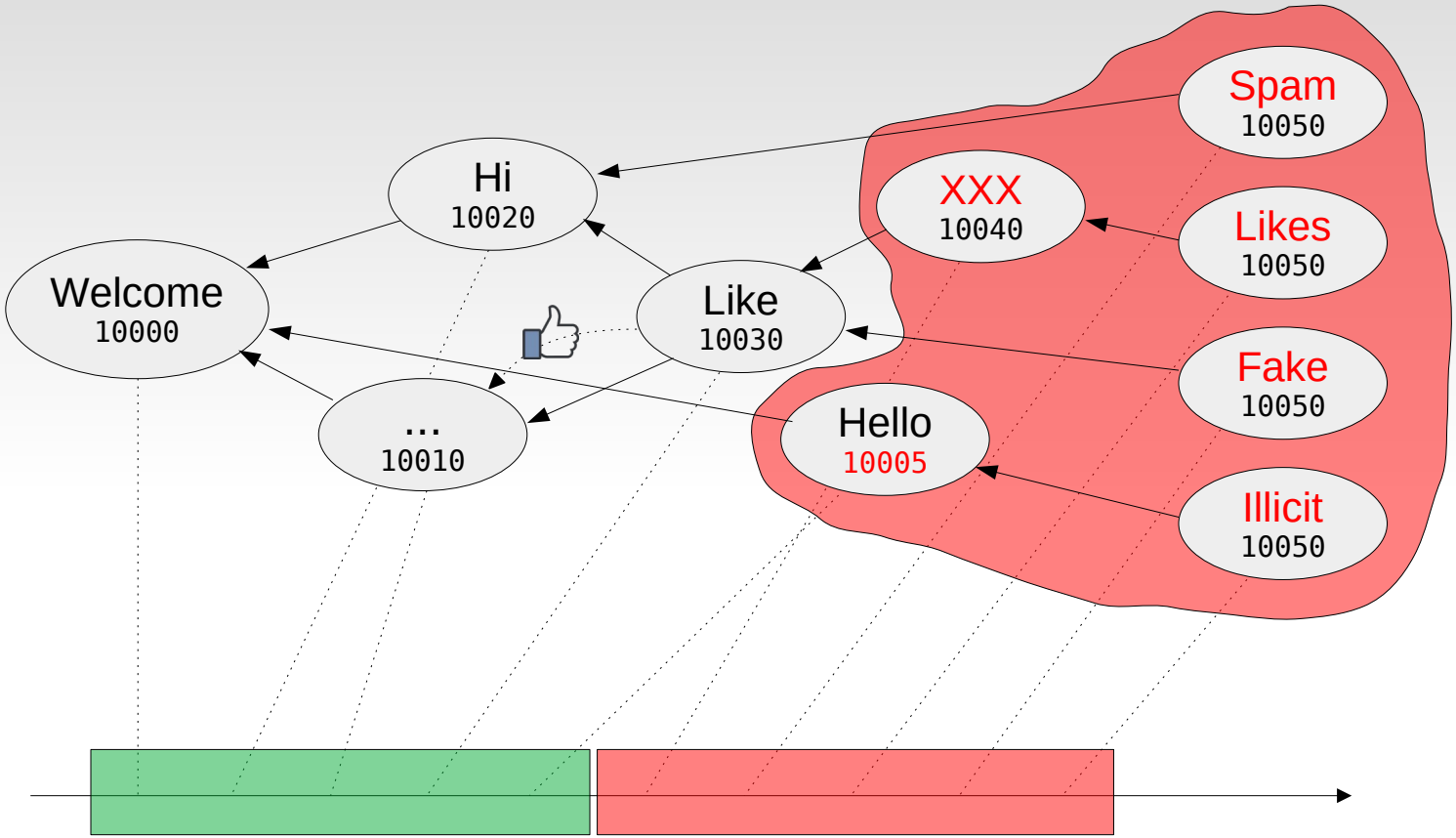
(?) DAGs → Consensus (?)



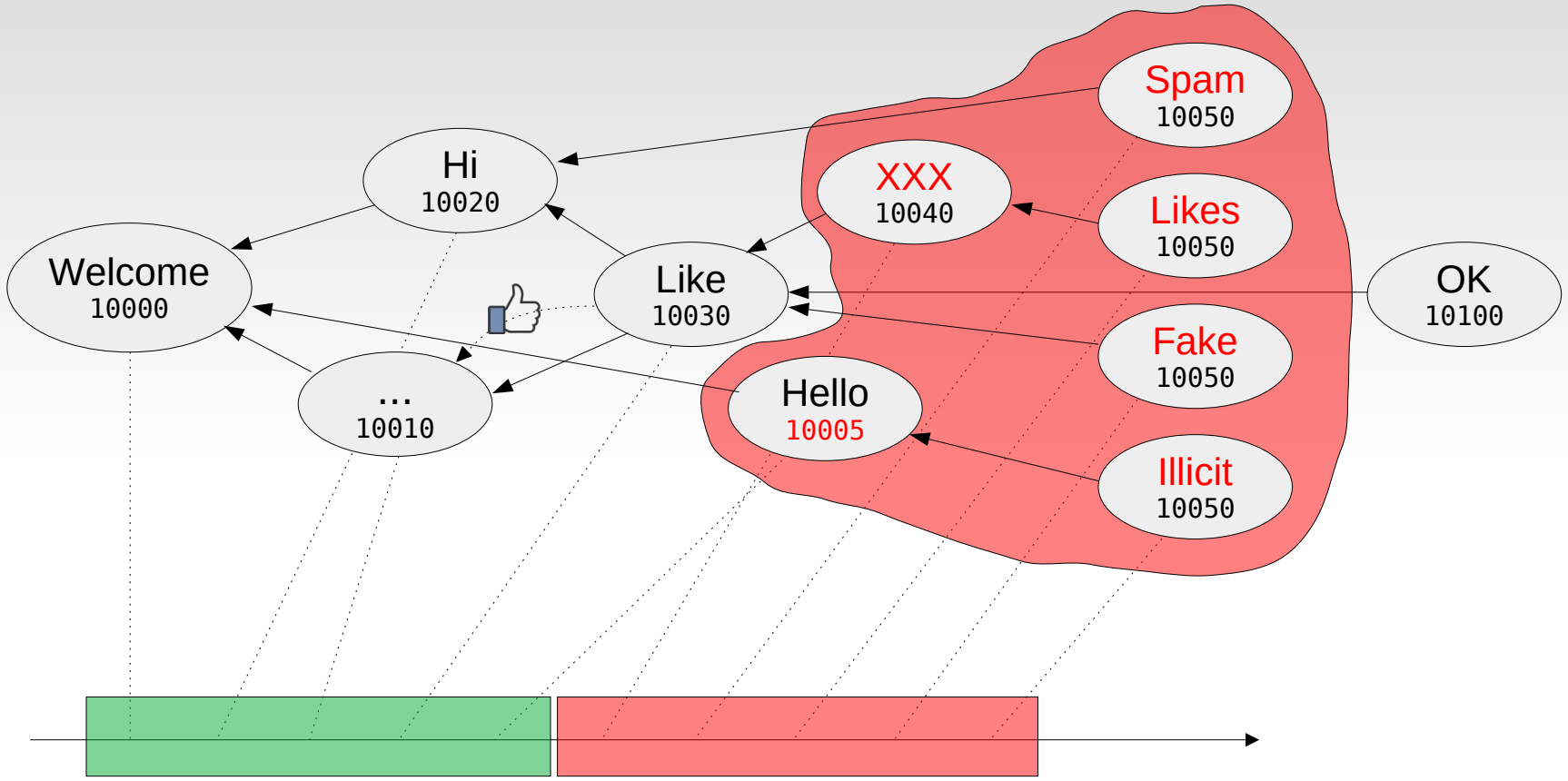
(?) DAGs → Consensus (?)



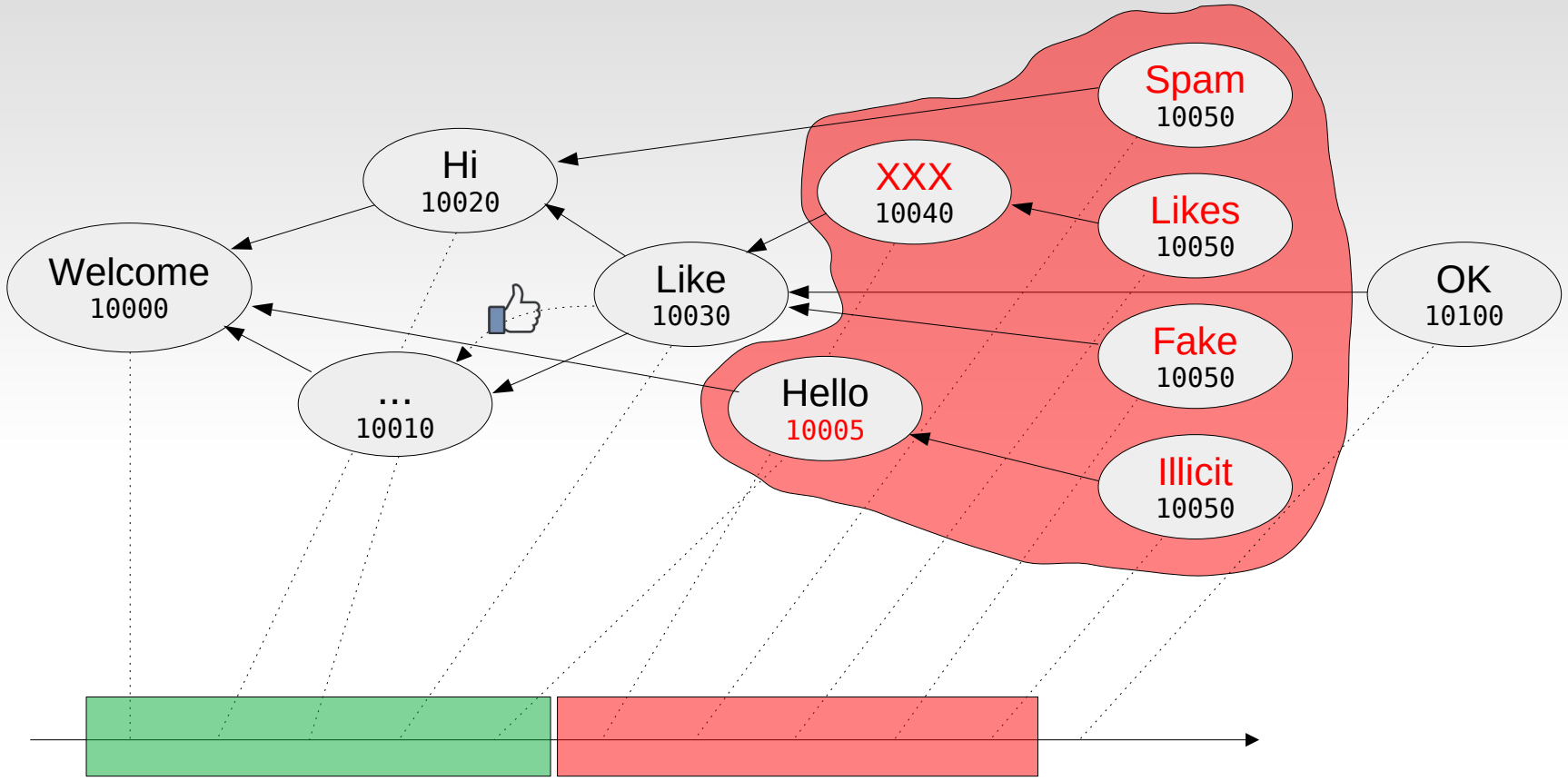
(?) DAGs → Consensus (?)



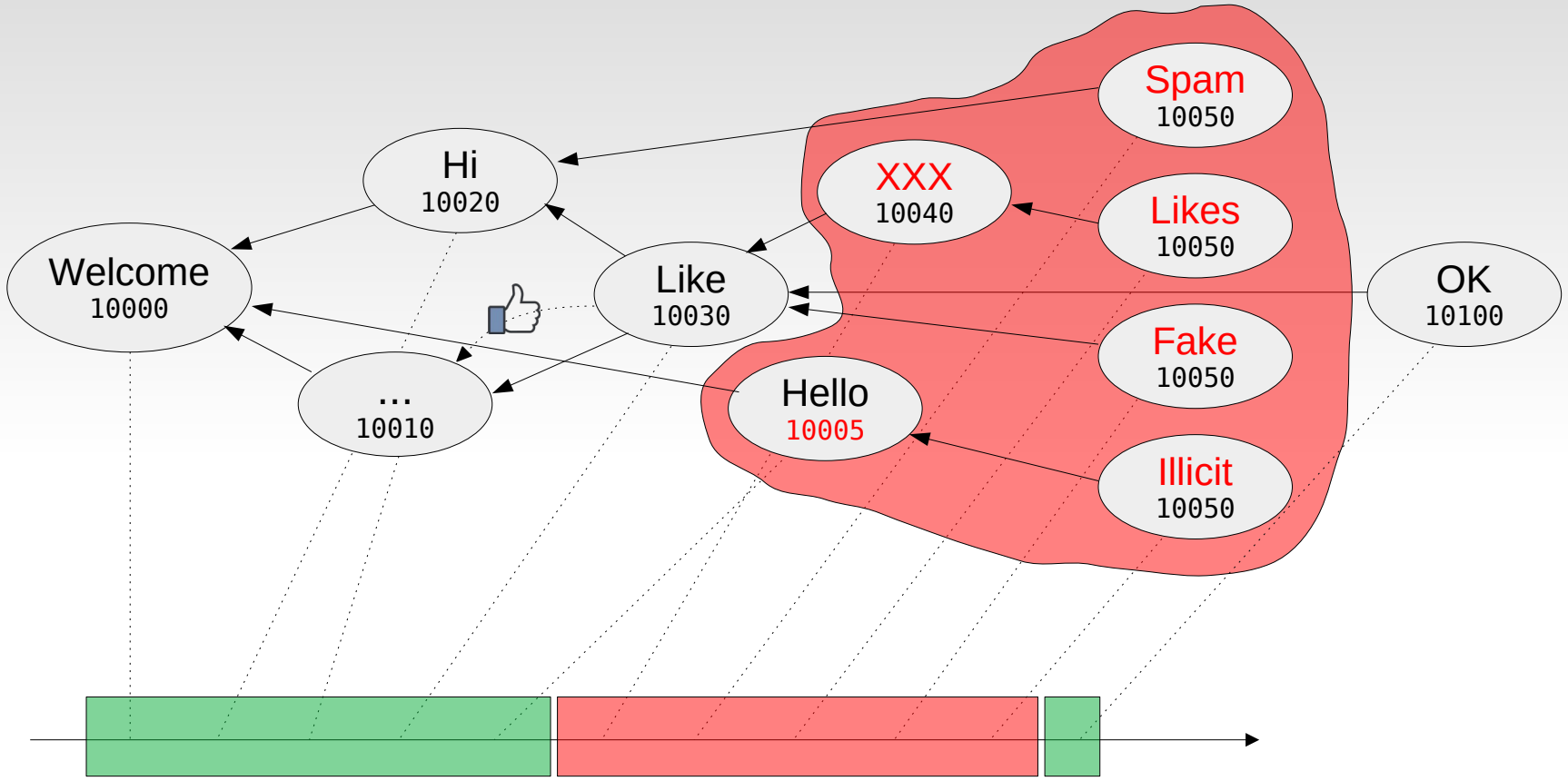
(?) DAGs → Consensus (?)



(?) DAGs → Consensus (?)



(?) DAGs → Consensus (?)



Reputation (reps)

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

Reputation (reps)

- Forum pioneer → + reps

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

Reputation (reps)

- Forum pioneer → + reps
- New content → - reps

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

Reputation (reps)

- Forum pioneer → + reps
- New content → - reps
- Consolidated content → + reps

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

Reputation (reps)

- Forum pioneer → + reps
- New content → - reps
- Consolidated content → + reps
- Likes & Dislikes → +/- reps

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

Reputation (reps)

- Forum pioneer → + reps
- New content → - reps
- Consolidated content → + reps
- Likes & Dislikes → +/- reps

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

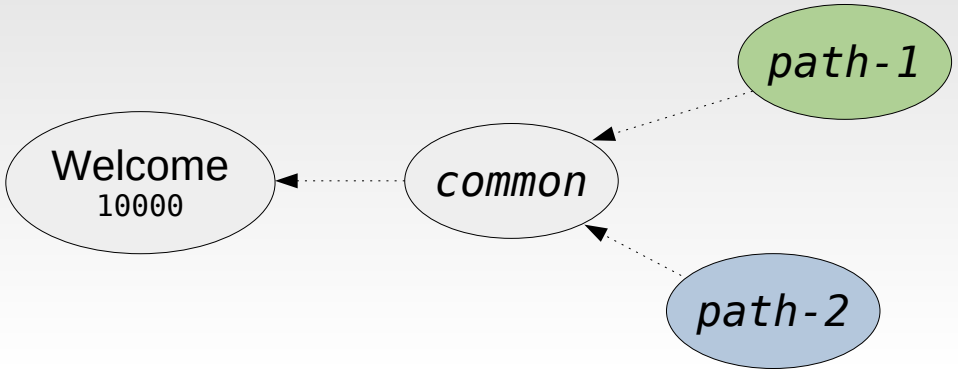
Reputation (reps)

- Forum pioneer → + reps
- New content → - reps
- Consolidated content → + reps
- Likes & Dislikes → +/- reps

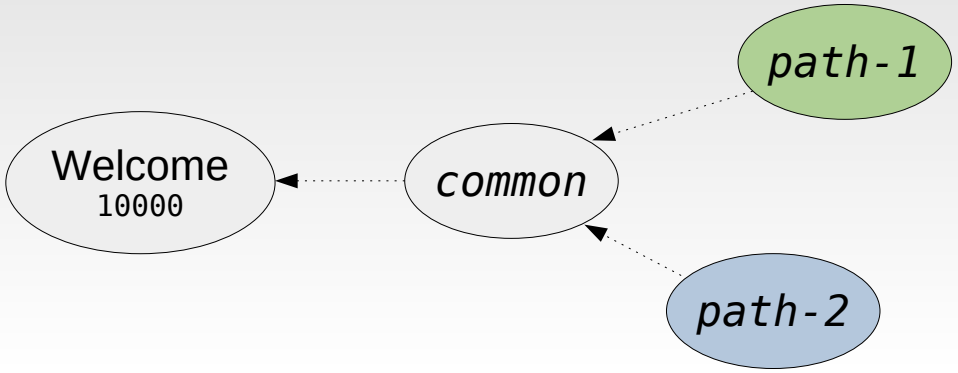
Sybil Resistance

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

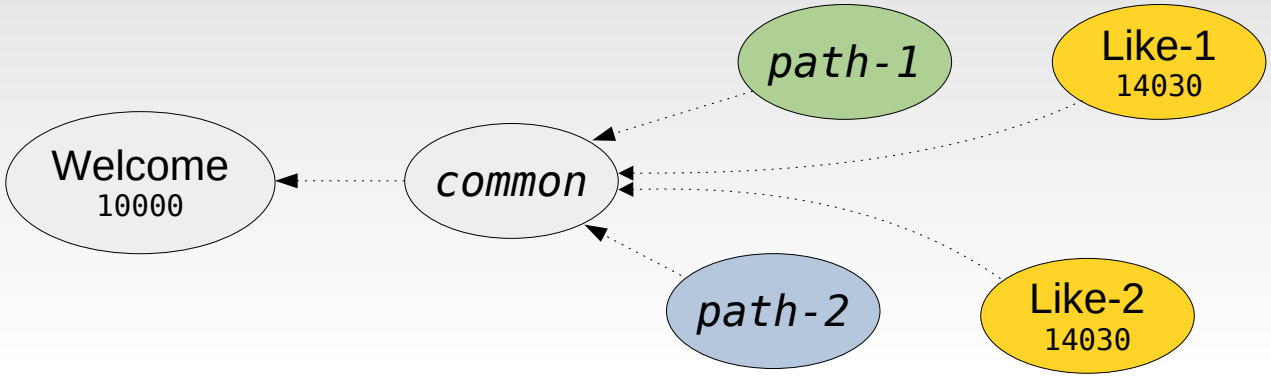
Reputation → Consensus



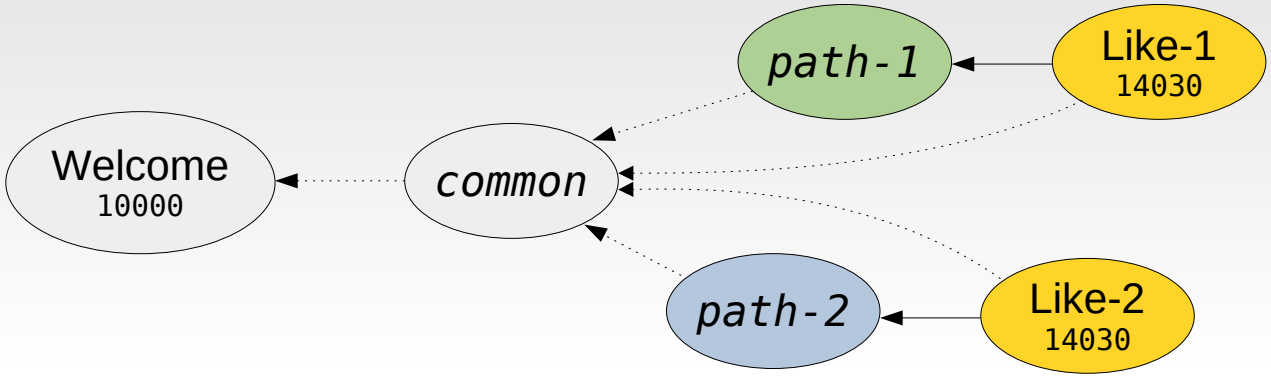
Reputation → Consensus



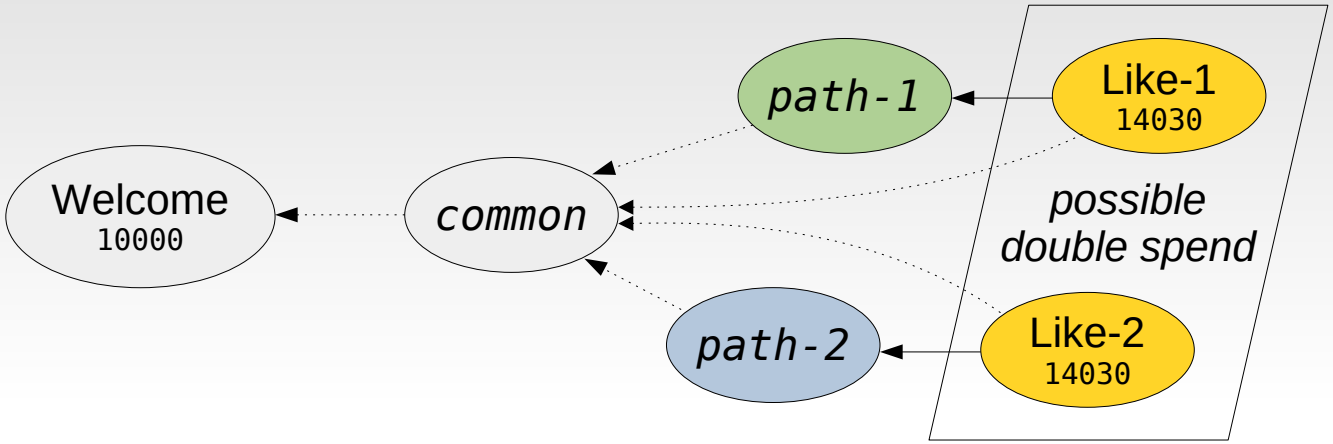
Reputation → Consensus



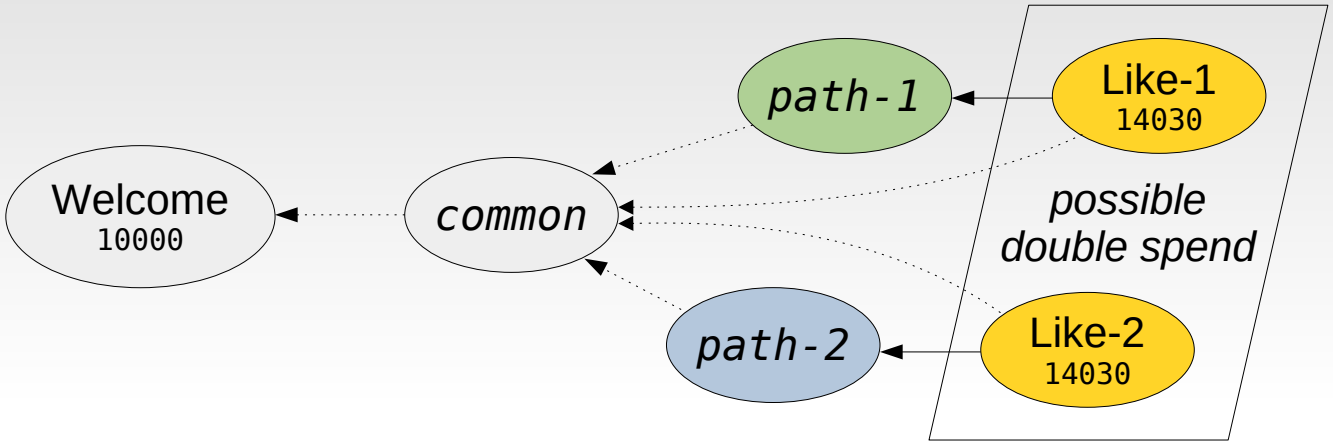
Reputation → Consensus



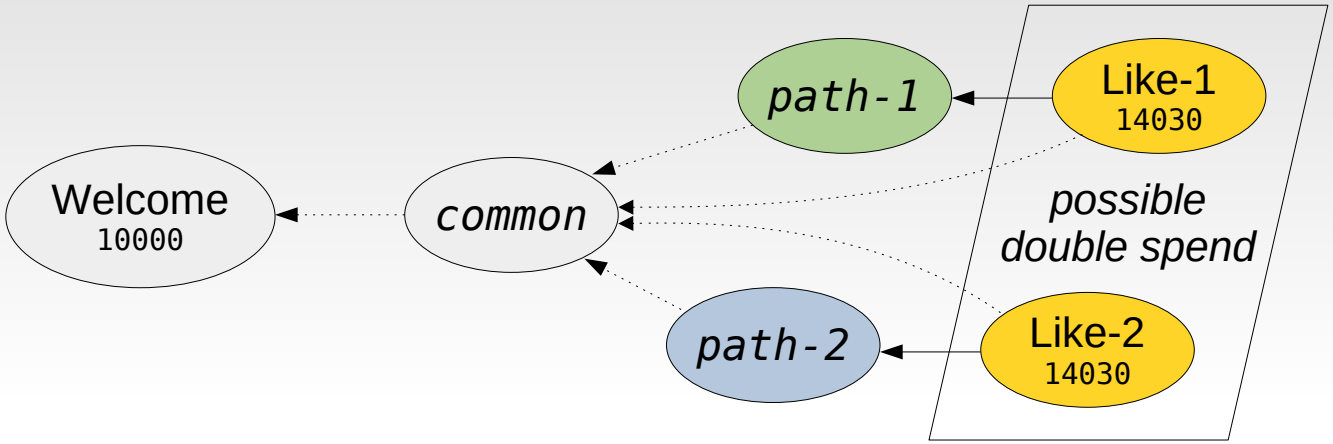
Reputation → Consensus



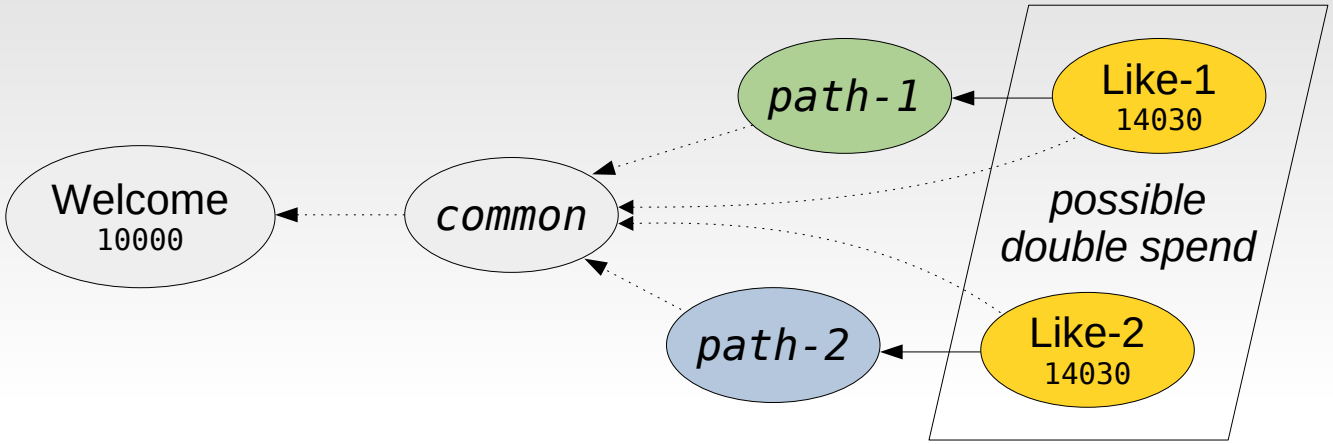
Reputation → Consensus

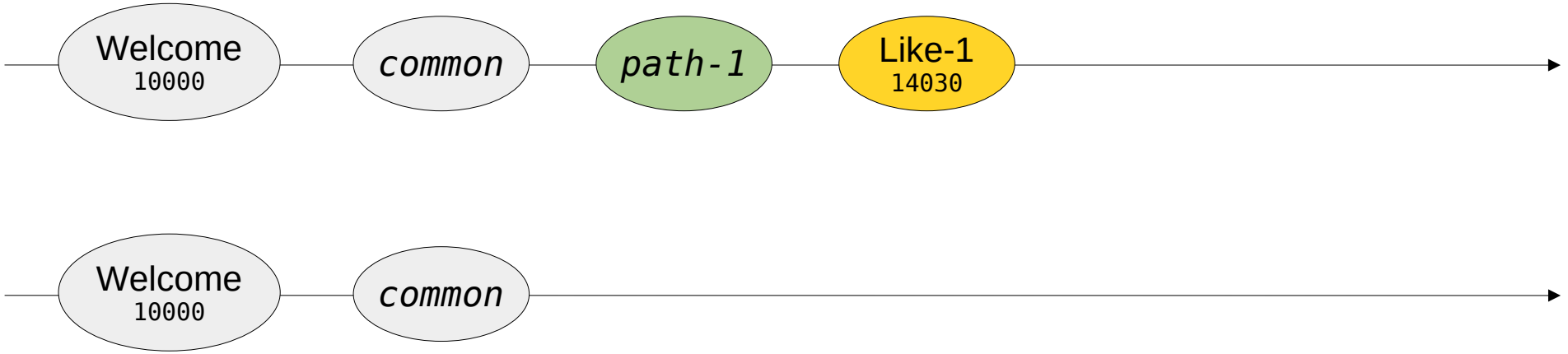


Reputation → Consensus

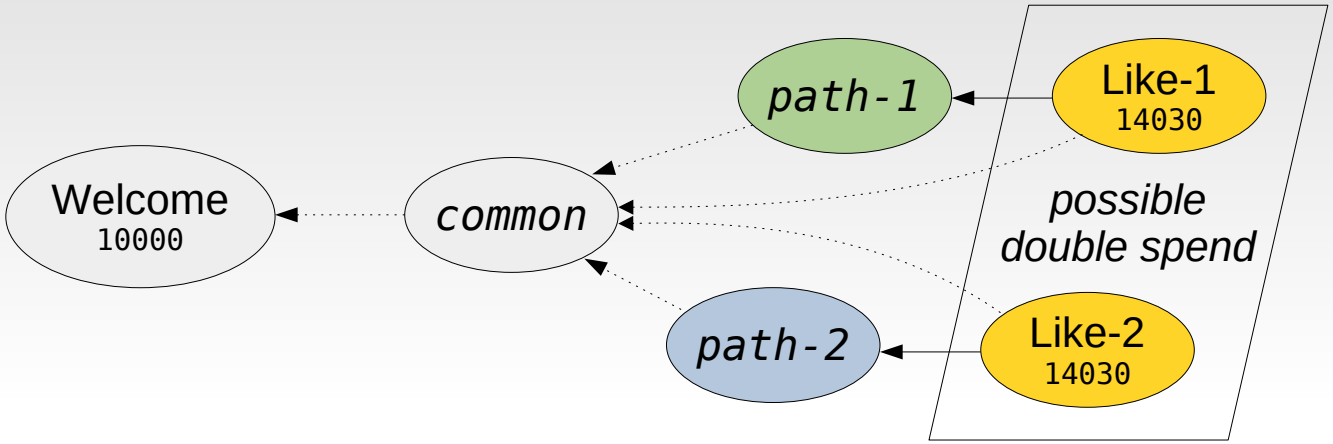


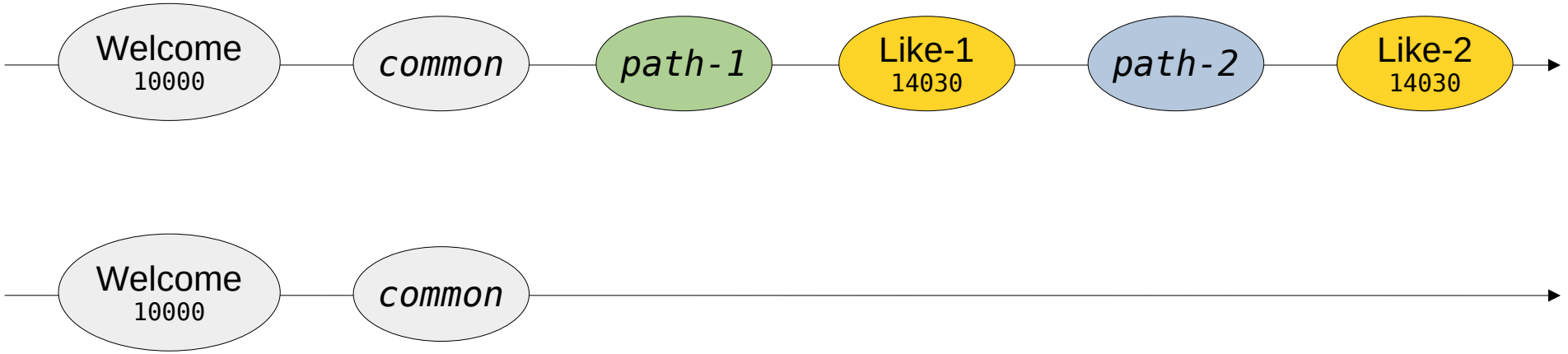
Reputation → Consensus



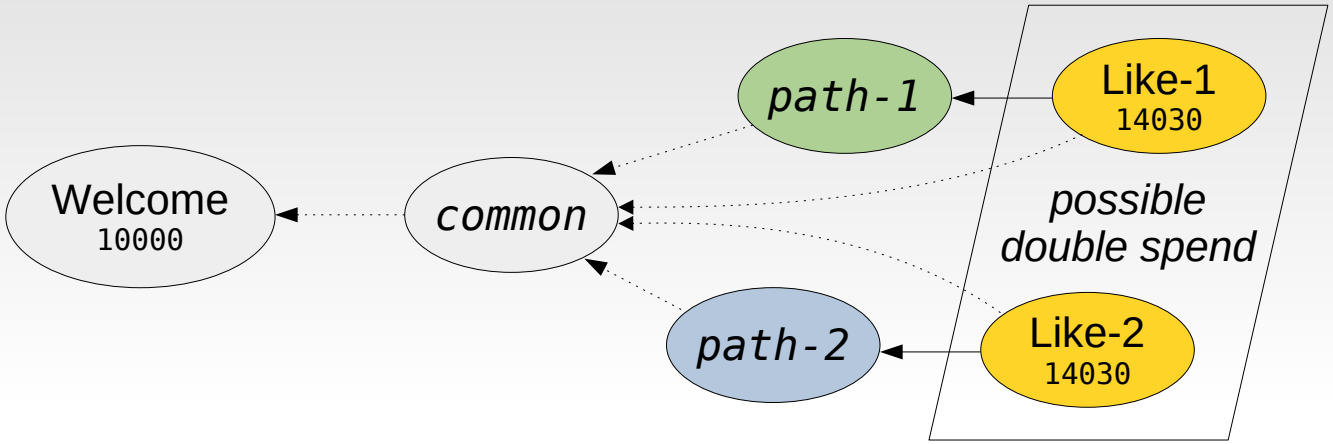


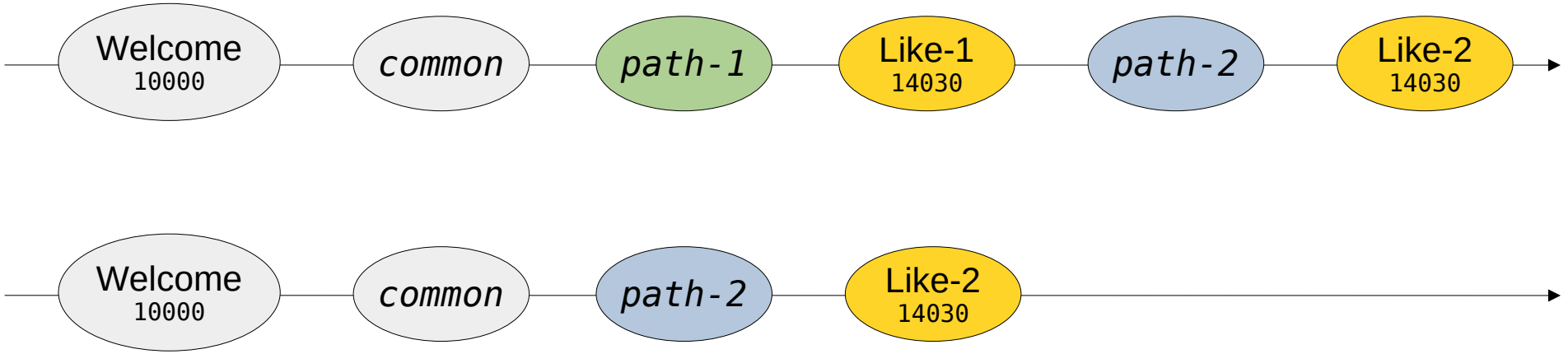
Reputation → Consensus



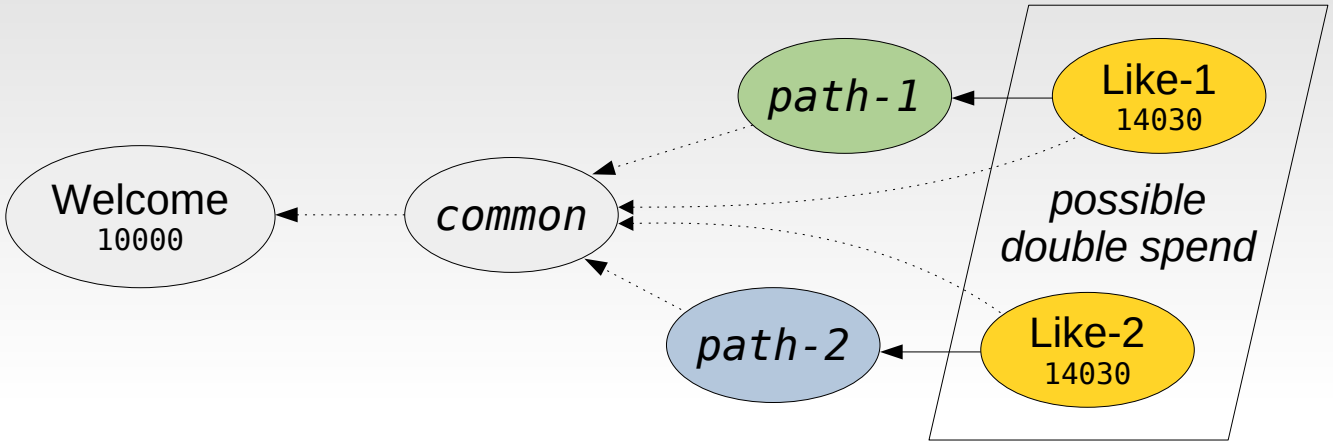


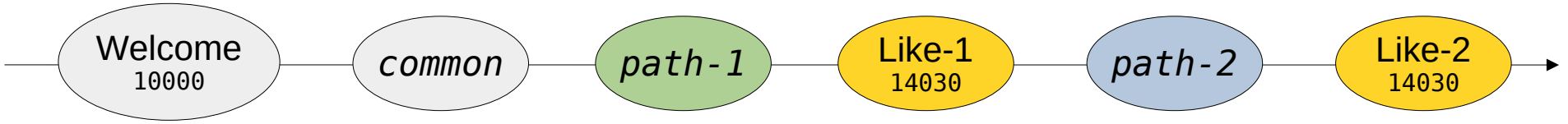
Reputation → Consensus

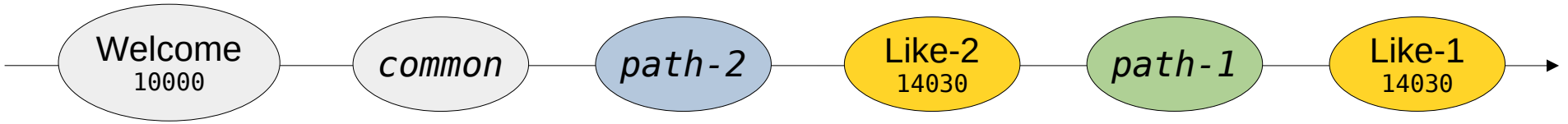




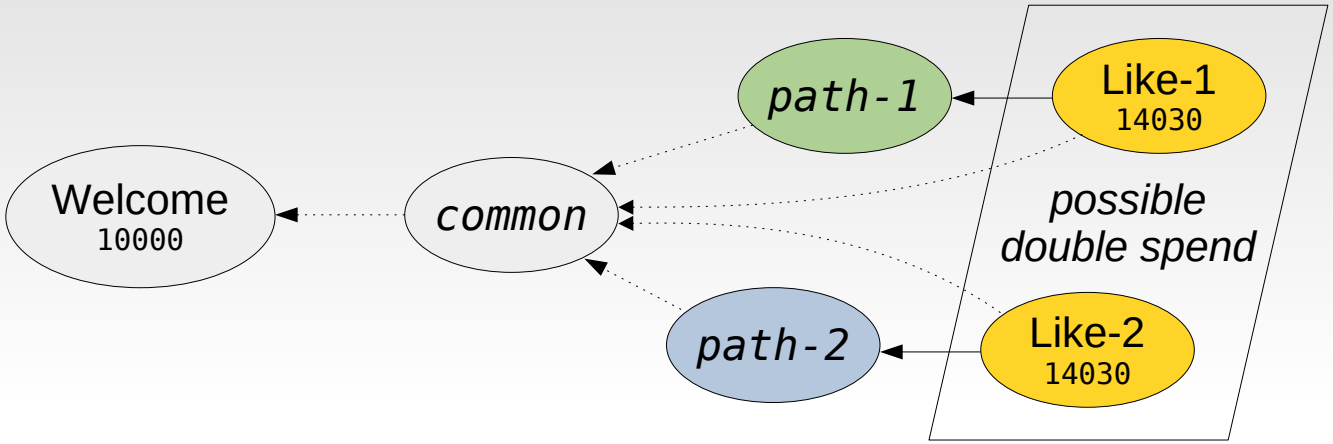
Reputation → Consensus

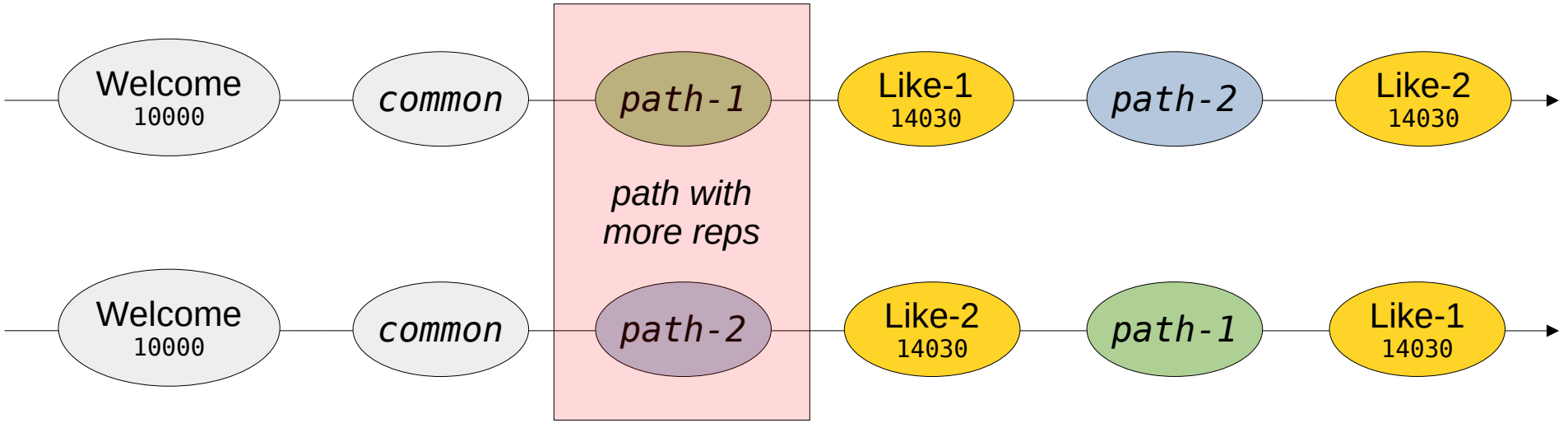




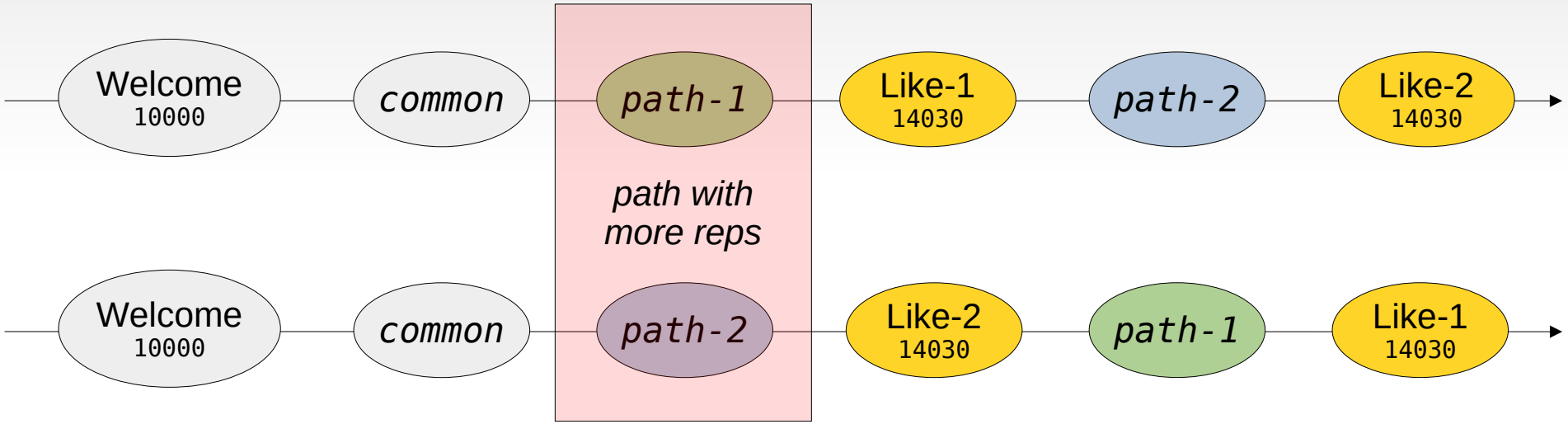


Reputation → Consensus

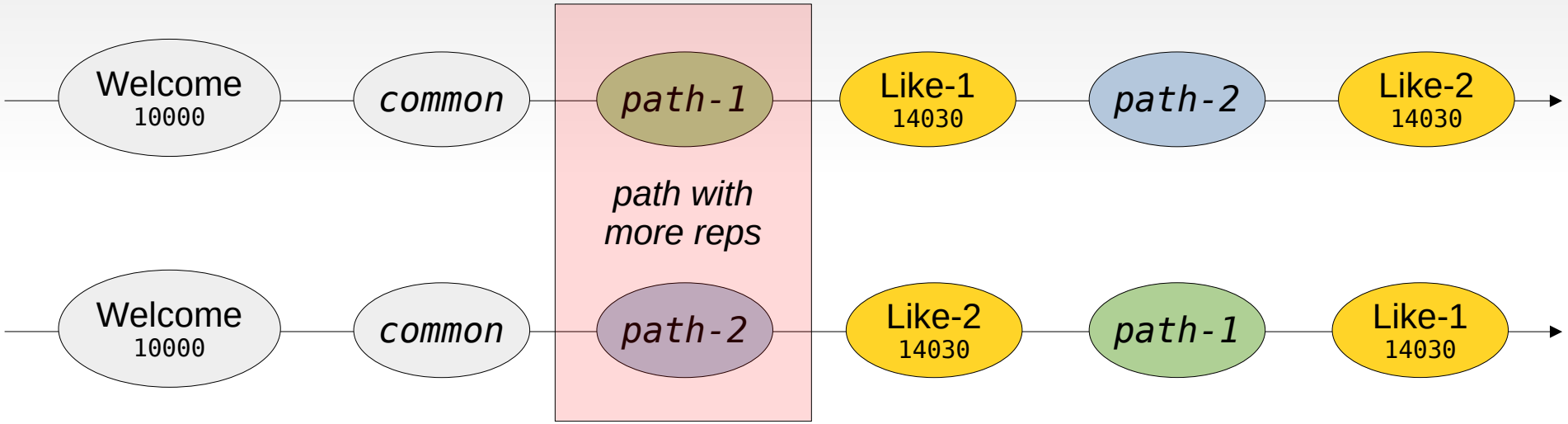




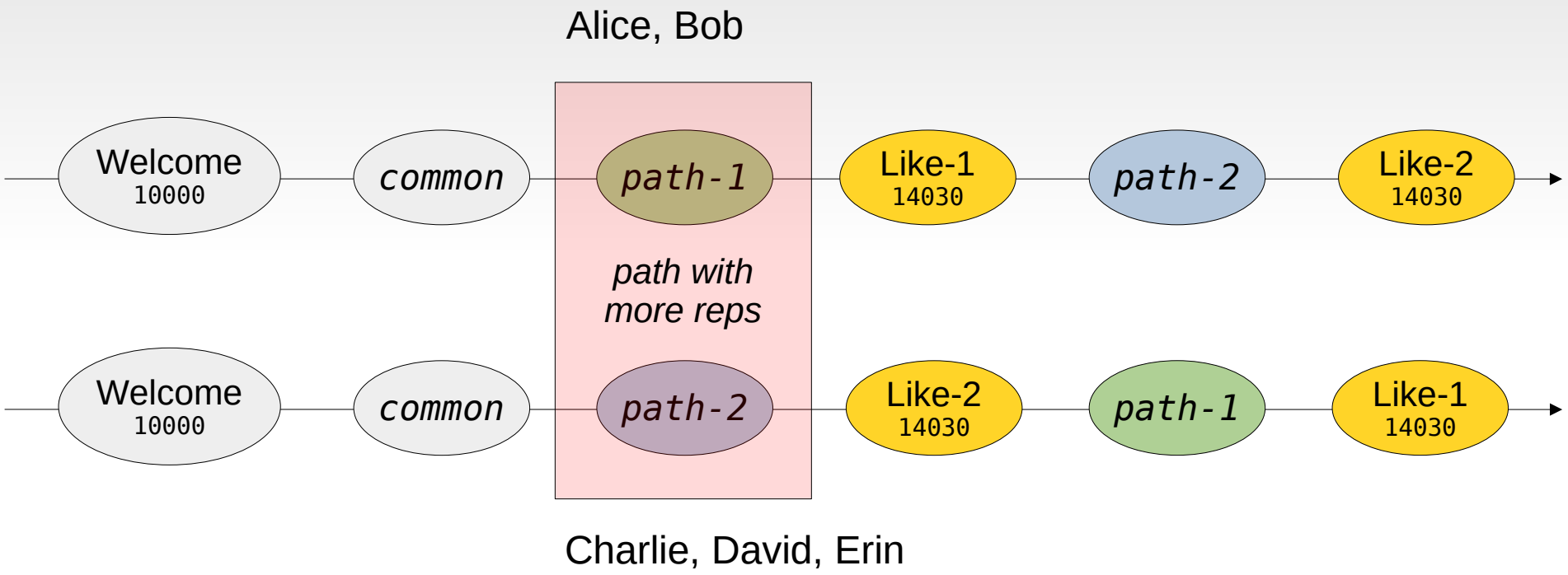
Reputation → Consensus



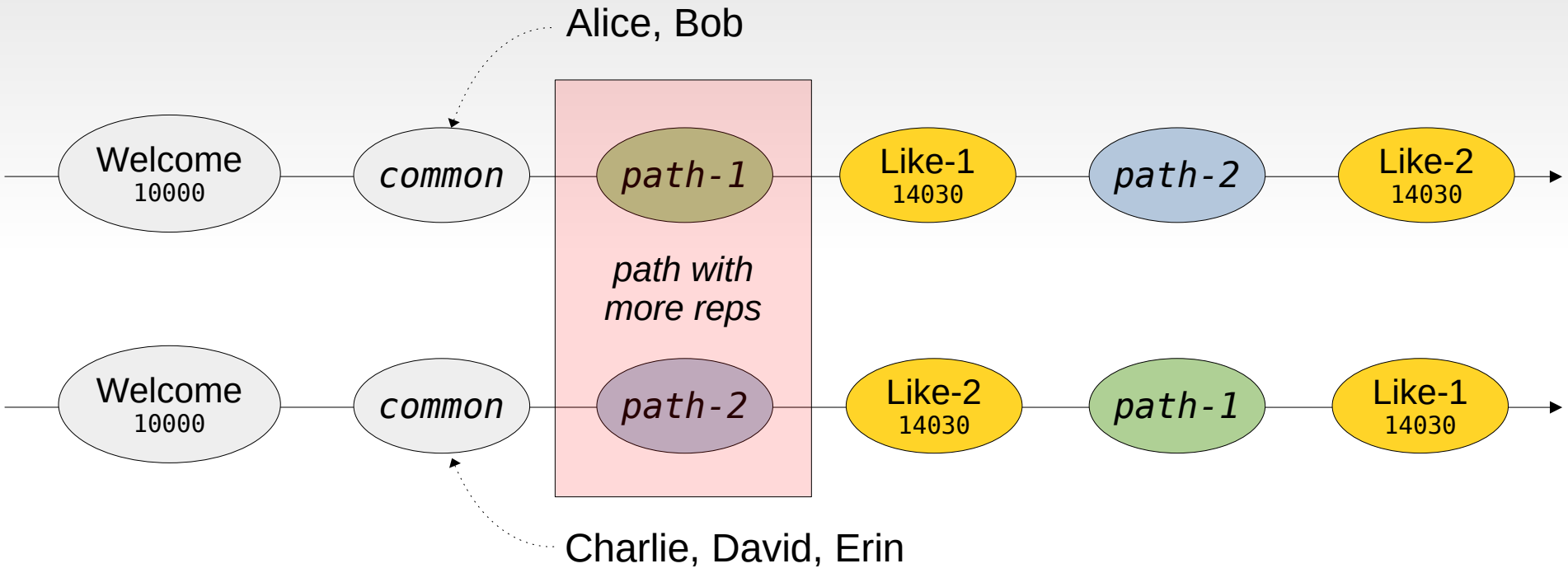
Reputation → Consensus



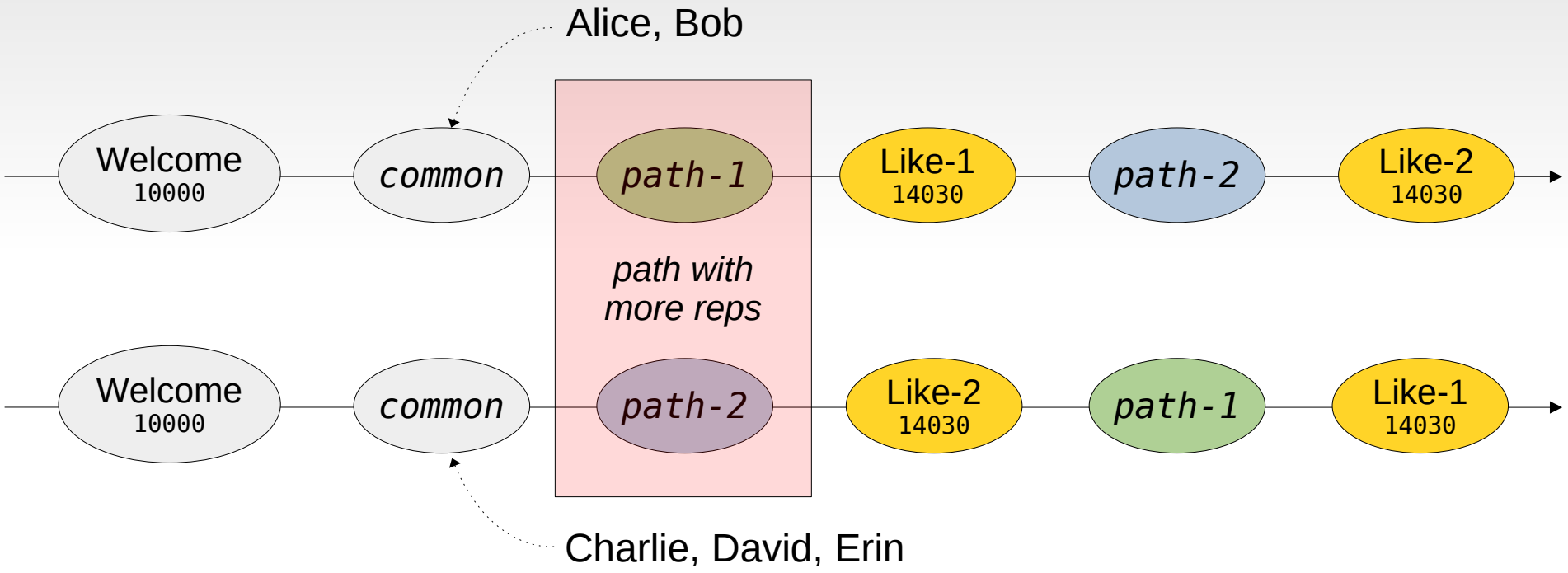
Reputation → Consensus



Reputation → Consensus

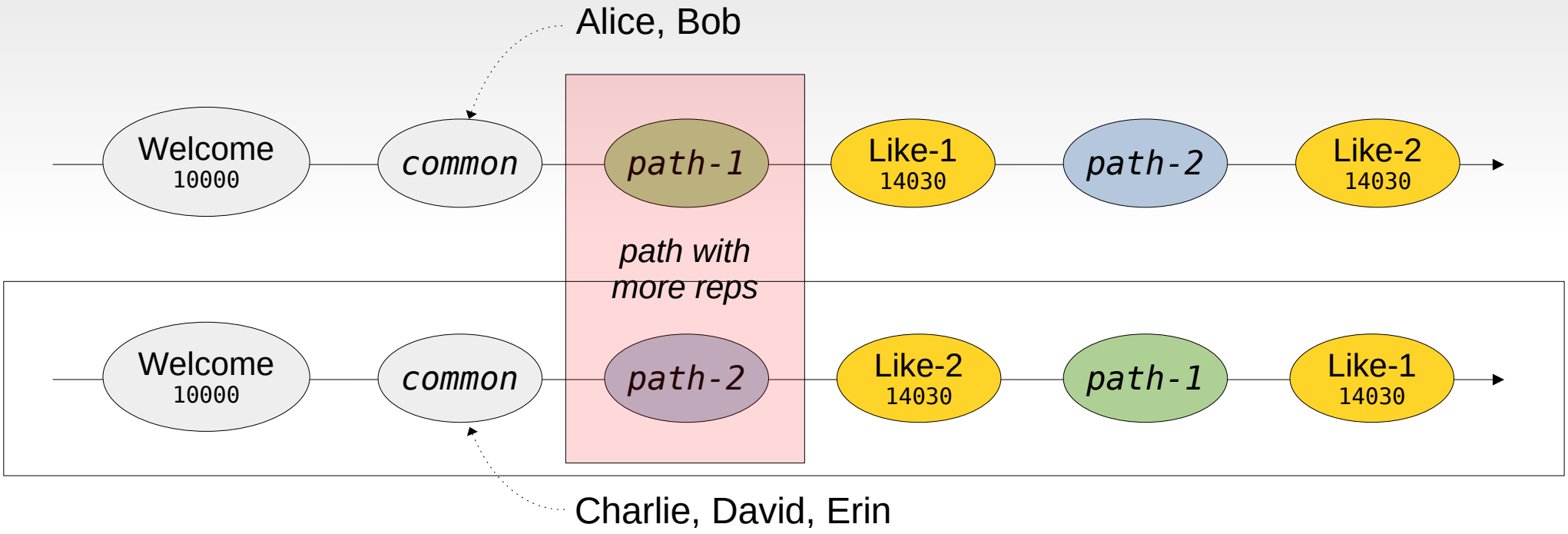


Reputation → Consensus



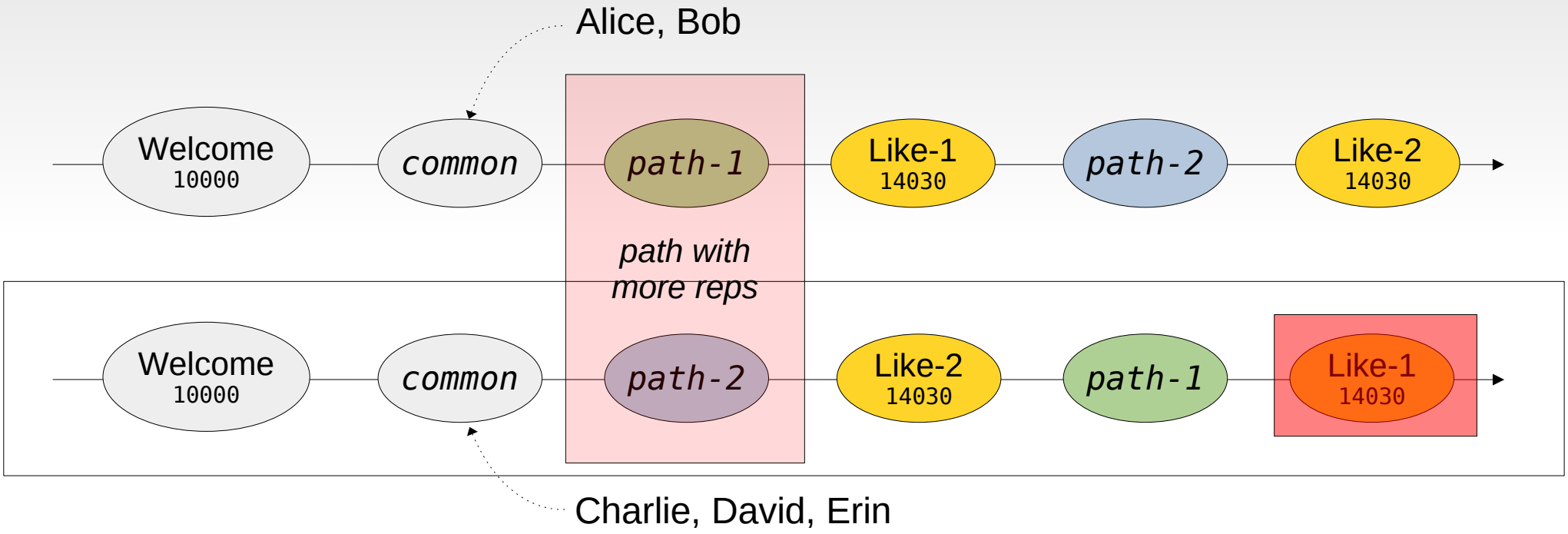
$$R(A)+R(B) < R(C)+R(D)+R(E)$$

Reputation → Consensus



$$R(A)+R(B) < R(C)+R(D)+R(E)$$

Reputation → Consensus



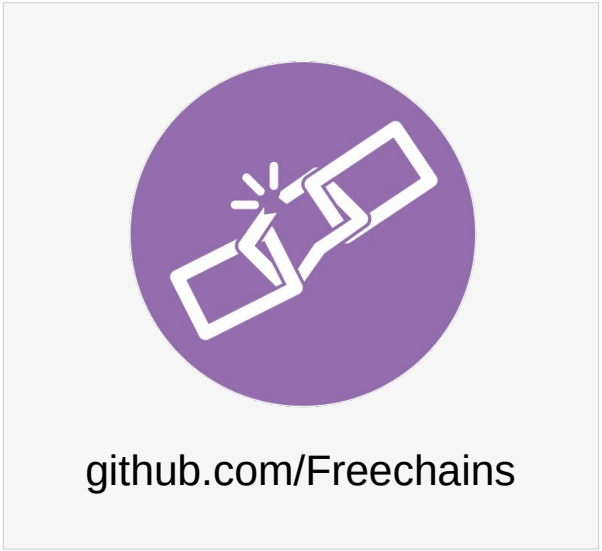
$$R(A)+R(B) < R(C)+R(D)+R(E)$$

Freechains

github.com/Freechains

Freechains

- Permissionless consensus protocol



Freechains

- Permissionless consensus protocol
- Consensus via reputation (*proof-of-authoring*)

github.com/Freechains

Freechains

- Permissionless consensus protocol
- Consensus via reputation (*proof-of-authoring*)
- Subjective judgment (likes & dislikes)

github.com/Freechains

Freechains

- Permissionless consensus protocol
- Consensus via reputation (*proof-of-authoring*)
- Subjective judgment (likes & dislikes)
- Solves the *double-spending* problem

github.com/Freechains

Main Contributions

Main Contributions

- Recognizing published contents as scarce resources

Main Contributions

- Recognizing published contents as scarce resources
- Using the reputation system to determine consensus

Main Contributions

- Recognizing published contents as scarce resources
- Using the reputation system to determine consensus
- Allowing users to create diversified forums of interest

Main Contributions

- Recognizing published contents as scarce resources
- Using the reputation system to determine consensus
- Allowing users to create diversified forums of interest
- Allowing users to work offline

Main Contributions

- Recognizing published contents as scarce resources
- Using the reputation system to determine consensus
- Allowing users to create diversified forums of interest
- Allowing users to work offline
- Supporting content removal without compromising the integrity of the blockchain

Peer-to-Peer Permissionless Consensus via Reputation

Francisco Sant'Anna, Fabio Bosisio, Lucas Pires

github.com/Freechains

Francisco Sant'Anna
francisco@ime.uerj.br
@_fsantanna

Extra Slides

Problems with Crypto

- They enforce a unique timeline to preserve value and immunity to attacks
- They lean towards concentration of power due to scaling effects
- They impose an external economic cost to use the protocol
- They rely exclusively on objective rules to reach consensus
- They require peers to be permanently online.

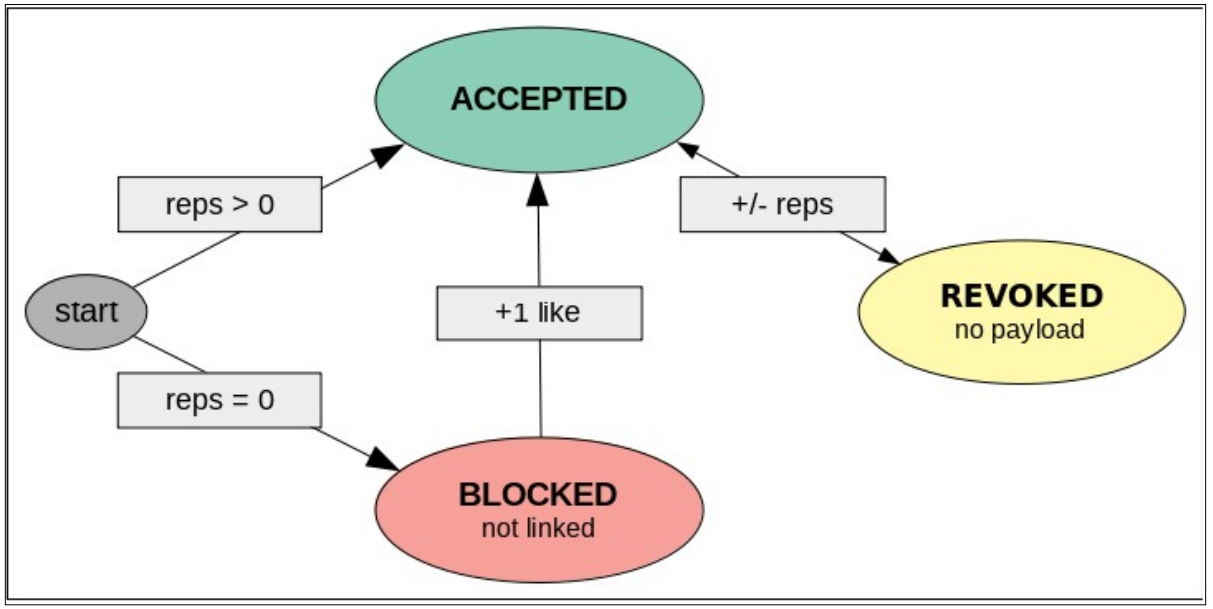
Local-First Software (*)

- Users can work offline
- Forks are not only permitted but encouraged
- Blocks are individual posts
  - (intrinsic vs extrinsic value)
- Primary blockchain is a DAG not a list
- But...
  - the longer disconnected, the more conflicts
  - posts reordering when rejoining

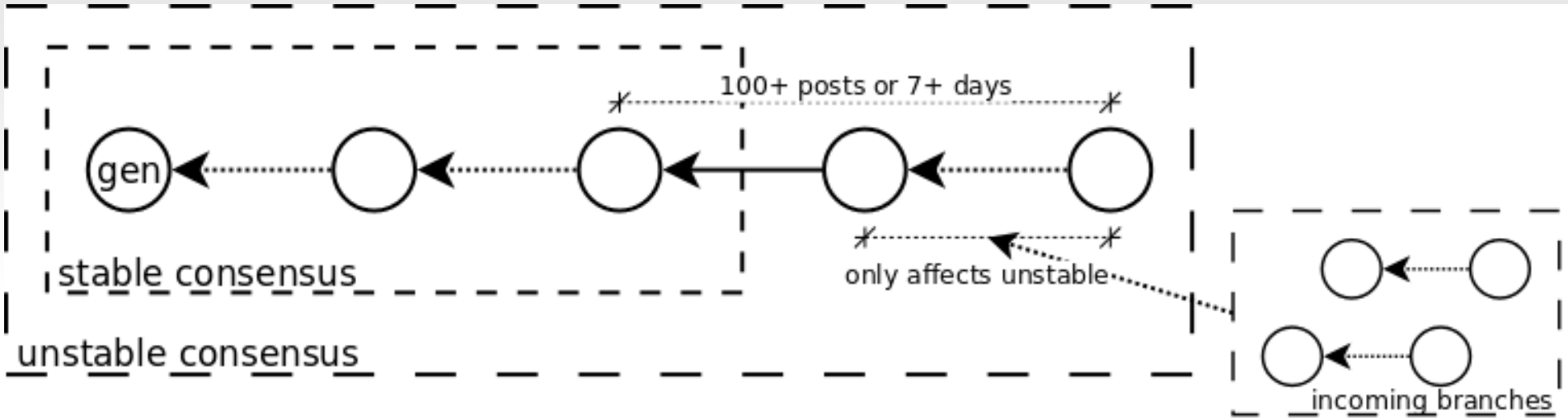
(*) M. Kleppmann et al. Local-first software: you own your data, in spite of the cloud. In Onward'19, pages 154–178, 2019.

Content Removal

- Users can revoke posts with dislikes.
- Peers are forced to remove payloads, only forwarding associated blockchain metadata.
- Does not compromise the integrity of the blockchain.



Stable Consensus



- Freezes the order of posts once they cross the threshold
- Prevents long-lasting local branches to merge
- Creates a hard fork
- Reconciling branches is no longer possible

Evaluation

- Internet Archives
  - 10k messages
  - chat channel, 3 months, *Wikimedia Foundation*
  - newsgroup forum, 9 years, *comp.compilers*
- Evaluate
  - metadata overhead
  - consensus runtime
  - graph forks (asynchronicity)
  - blocked messages (bookkeeping)

Evaluation

- Metadata overhead
  - Chat: 10x
  - Newsgroup: 50%
- Consensus runtime
  - Chat: 125s and **50ms**
  - Newsgroup: 100s and **70ms**
- Graph forks (asynchronicity)
  - Chat: 18%
  - Newsgroup: 14%
- Blocked messages (bookkeeping)
  - Chat: 3.7%
  - Newsgroup: 3.5%

Conclusion

Finally, we do not claim that the proposed reputation system enforces "good" human behavior in any way. Instead, it provides a transparent and quantitative mechanism to help users understand the evolution of forums and act accordingly. Human creativity contrasts with plain economic resources (e.g., proof-of-work), which do not appraise social interactions and also tend to concentrate power over the time.