How to build a private social network

Definition of Privacy

- Privacy is the ability of an individual or group to seclude themselves or information about themselves, and thereby express themselves selectively.
- DOS attack
- Relative privacy

Compare private / transparent

- Anonymous message boards:
  - Is this because of privacy ?
  - Or sock puppet : Proof of individuality
  - Or lack of reputation: Reputation system
- facebook, tiktok
  - Prevent sock puppets
  - Have transparent reputation system

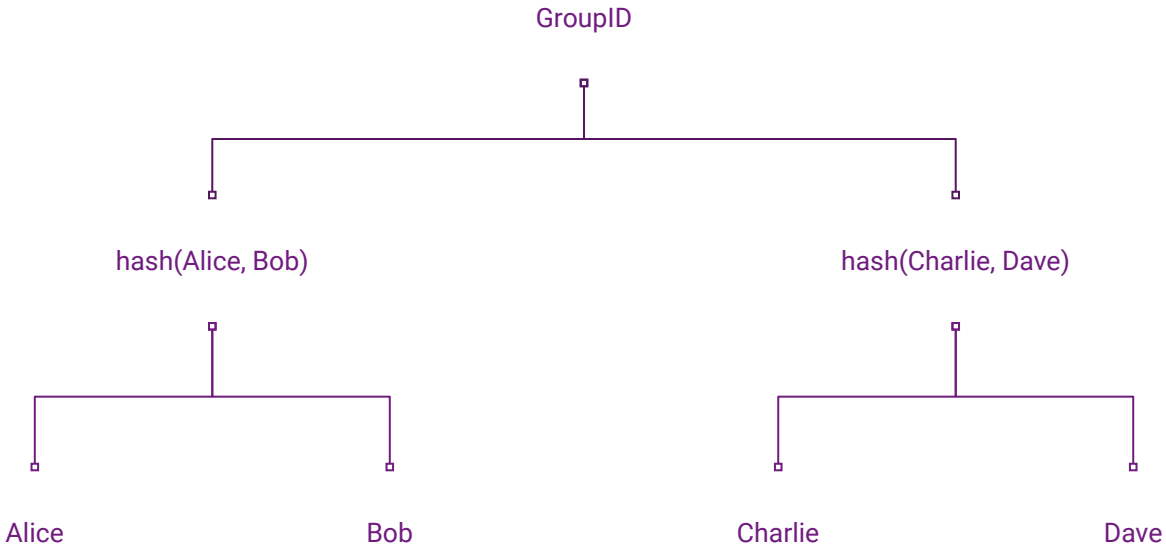
Neutral social media

- Why don’t we have social media that is neutral?
- Like use my facebook reputation on airbnb.
- Because it's transparent it can’t be publicly verifiable
- So privacy is important to make neutral social media
    - Because we want to make things that can be verified publicly
    - But we dont’ want to publish every thing everyone says to someone on chain.

Decentralized social media

- Posts / Upvote / Downvotes
- Reputation system
  - Social Graph
  - Based upon influence
- Direct messages
- Anti collusion infrastructure
- Moderation
- Content suggestion
- Easy to recover if you forget your private key

Starting simple: Semaphore



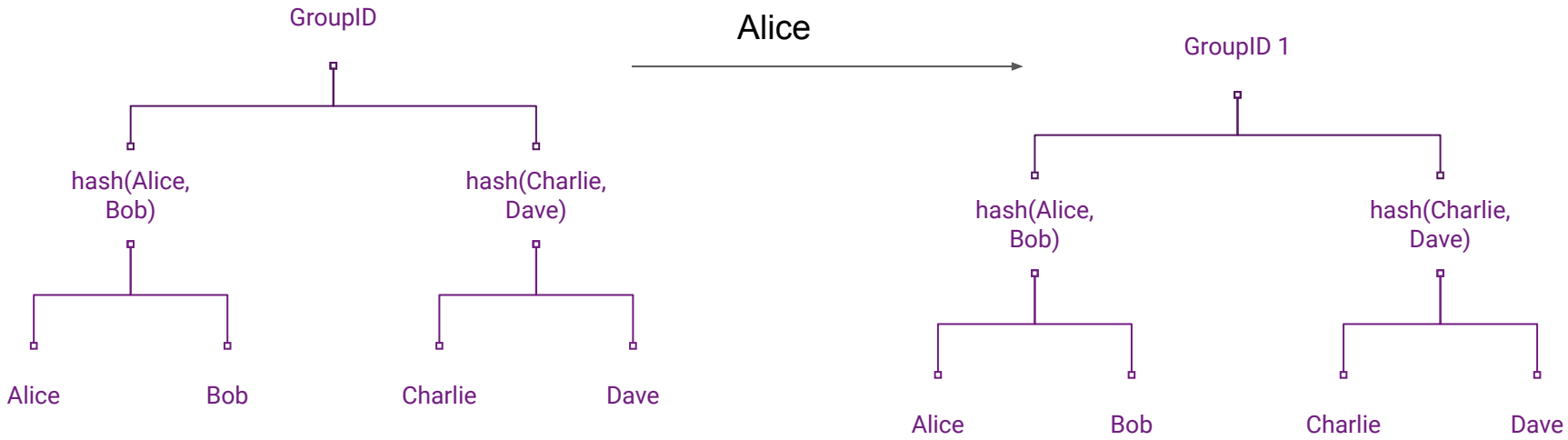
Properties of semaphore

- Its a nice way to prove you are in a group.
- But no persistence you can signal but not gain / loss reputation
- https://github.com/appliedzkp/semaphore

Unirep

- Allows you to gain and lose reputation
- Have a temporal address that reputation can be sent to
- Have many different reputations that different smrat contracts / people can write to.
- https://github.com/NIC619/UniRep

Unirep


GroupID
hash(Alice, Bob)
hash(Charlie, Dave)
Alice
Bob
Charlie
Dave
Alice
GroupID 1
hash(Alice, Bob)
hash(Charlie, Dave)
Alice
Bob
Charlie
Dave

Unirep

- Smart contracts to define when to transition
- Build social network similar to upvote / downvote forum with this.
- We can add usernames to connect users posts but this is not the default.

Unirep Wishlist

- Reputation system for getting free devcon tickets
  - Attendees / winners at hackathons get rep tokens from hackathon
  - Bug bounty winners get reputation tokens
  - People who help with translations get rep tokens
  - To get a free ticket for devcon you have to prove you have above x reputation
- Find some interesting ways to use unirep reputation
  - Get testnet eth with some tokens

Direct messages

- So we have upvote / downvotes
- How can we send DM
- Easy right with encryption …
- How to hide who is messaging who ?
- But what about spam ?

RLN

- Prove membership
- Shamir secret share of private key
- If I reveal two secrets i reveal the private key
- If I reveal just one secret i reveal nothing
- Have smart contract that allows slashing if you know private key
- https://github.com/kilic/rln

RLN wishlist

- Simple group chat app for anyone who has NFT from events.
- Use this in eth2 for p2p network,
  - make a wrapper for libp2p that uses rln to limit messages
  - Think there is some nice proof of stake things we can prove if we limit the total number of messages.

Blind find

- List of people who commit to their friends list
- Use MPC to search for a target peer
- If you can’t find that ask your friends
- Exponential growth of querys.
    - So only works well for small networks
    - With recursion we can improve

Blind Find wishlist

- Experiment with UI for small groups
  - Maybe ethereum meetup group membership proof
- Explore recursion to reduce the amount of searching you need to do.

Moderation

- Moderation multisig
- Prediction market for if some post will be marked as invalid
  - So we can automatically hide posts that prediction markets think will be marked as against the policy
  - Idea is that multisig will have to do very little work other than resolving issues where its unclear.
- Can have multiple competing moderation multisig
- TODO: Build this for some sample forum. We have some code but looking for someone to take the next steps with it.

Anti collusion infrastructure

- Maci
- Make it impossible to prove how i voted
- Like zk rollup with no data availability
- All actions are encrypted
- ZKP used to enforce all votes are processed
- Because every action is encrypted you can’t see if a previous action invalidated the one someone is trying to get bribed with

Maci todo

- Quadratic.page merges million dollar home page with quadratic voting. Need someone to more forward with that project.
- clr.fund improvements
  - Trying to run several local rounds of quadratic funding
  - Need to improve UI / UX
  - https://vitalik.ca/general/2019/10/01/story.html would be have
- Add maci to popular voting sites products
- Maci depends upon proof of individuality
  - In Japan MyNumber give ntc signatures to verify owner of the card has japanese government credentials
  - Apply this to maci using ZKP to verify
  - Similar to ID system in India

Content suggestion

- User state channels
- Deposit system
- Suggester (Deposit) User (Deposit)
- Suggester suggests a link
  - If users likes it gives a reward
  - If user does not like it can destory suggesters deposit as long as they destroy their own.
- TODO: Finish build this and do some experiments

Conclusion

- A lot of things to apply zkps to
- Excited to work with more people to build them

Bonus: ZKEVM

- Proof of validity for evm
- Plonk + Plookup
- Plookup: Prove membership of a set
- Key value mappings