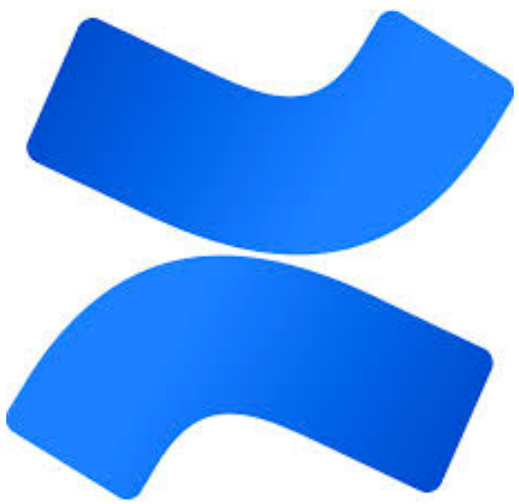
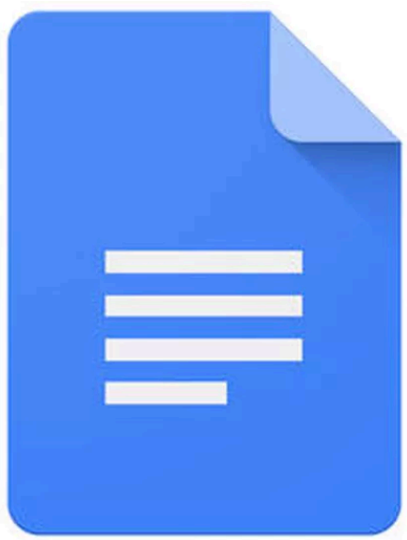
Managing Teams and Keys with Keybase

Max Krohn (https://keybase.io/max)





etc.

qmail

cvs

moinmoin
wiki

ircd

“just scp it
from my
machine”

18.26.4.239

- Federated management was better than what we have today but was never good enough.

- Managed apps in the cloud: maybe that ship has sailed

- **But at the very least, can we decentralize trust and key management?**

Basic Requirements

- Multi-device support
    - Get new phone for Christmas, enter username and password, and get instant access to all history
- Namable teams with mutable membership
- Authenticated invitation of new members

Threat Model

- Bad guys own any server infrastructure

Matthew Green
@matthew_d_green

Following

GCHQ has proposal to surveill encrypted messaging and phone calls. The idea is to use weaknesses in the “identity system” to create a surveillance backdoor. This is a bad idea for so many reasons. Thread. 1/

Principles for a More Informed Exceptional Access...
GCHQ officials outline how to enable the majority of the necessary lawful access without undermining the values we all hold dear.
lawfareblog.com

11:16 AM - 10 Dec 2018

808 Retweets **939** Likes

29 808 939

Security Goals

- PCS by default (this talk)
- Forward-secrecy is opt-in per-message and can be layered on top (outside scope)

Insufficient Solutions


micro
4 GB
cruzer


Search


9:41
Tuesday, September 12


MacBook Air

Keybase's Approach

- Users think about "devices" not "keys"
- Each device in a user's cloud is equally powerful. Why?
  - We've all lost phones, laptops, slips of paper
    - The more devices, the less likely you are to lose your data
    - And you're most likely to discard your **oldest** device
- Reuse this abstraction for teams:
  - Devices are to Users as Users are to Teams

T-Mobile 11:04 PM 66%

Devices

+ Add new...

iphone 8
Current device

cry glass

home mac mini - meuse

MacBook - seine

rhine 2018-08

volga

work - piave-ubuntu

Work iMac 5k 2015-11

Revoked devices

T-Mobile 11:07 PM 65%

keybase
TEAM
24 members • Owner
Write a brief description

Chat | Add people...

MEMBERS (24) | INVITES (0) | SUBTEAMS (28)

chris
Chris Coyne • Owner

max
You • Owner

adamjspooner
Adam Spooner • Writer

aimeedavid
Aimee David • Writer

akalin

How Apps Work

- Every team has a random shared symmetric key that rotates when:
  - Users are removed from the team
  - Or any team member revokes a device
- All updates to the chat channel (or git repo or file system) are:
  - Encrypted for current shared team symmetric key
  - Signed by the user that made the update
    - To prevent Alice from putting words into Bob’s mouth

Keybase

Chat

Jump to chat

#github
#kbfs
#log-enthusiasts
#lunch
#monorepo
#nyc
#otr
#product-ideas
#random
#releases
#saltpack
#security
#spread-the-word
#stellar
#windows

keybase.bots
#alerts
#general
#github

keybasefriends
#general

keybasefriends.stellar_test...
#general

sdfkb.dev
#general

stellar.public
#general

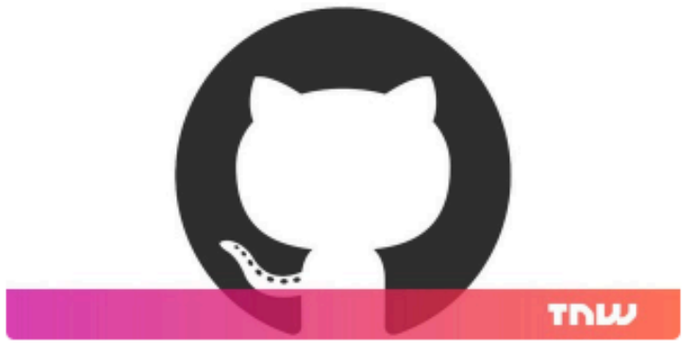
stronghold.public
#general

max

keybase **#random**

akalin 1:31 PM
https://thenextweb.com/dd/2019/01/05/github-now-gives-free-users-unlimited-private-repositories/

The Next Web
GitHub now gives free users unlimited private repositories
Finally!



zanderz 1:41 PM
@mlsteele @chrisnojima @max The WWI/War of the Worlds mashup I mentioned: https://vimeo.com/107454954

Vimeo
Great martian war
Archive recreation taken from The Great Martian War documentary by impossible factual for History Canada. Directed by Mike Slee VFX/Animation Director : Christian...

2 1

7d Write an exploding message boom!

bold, _italics_, `code`, >quote

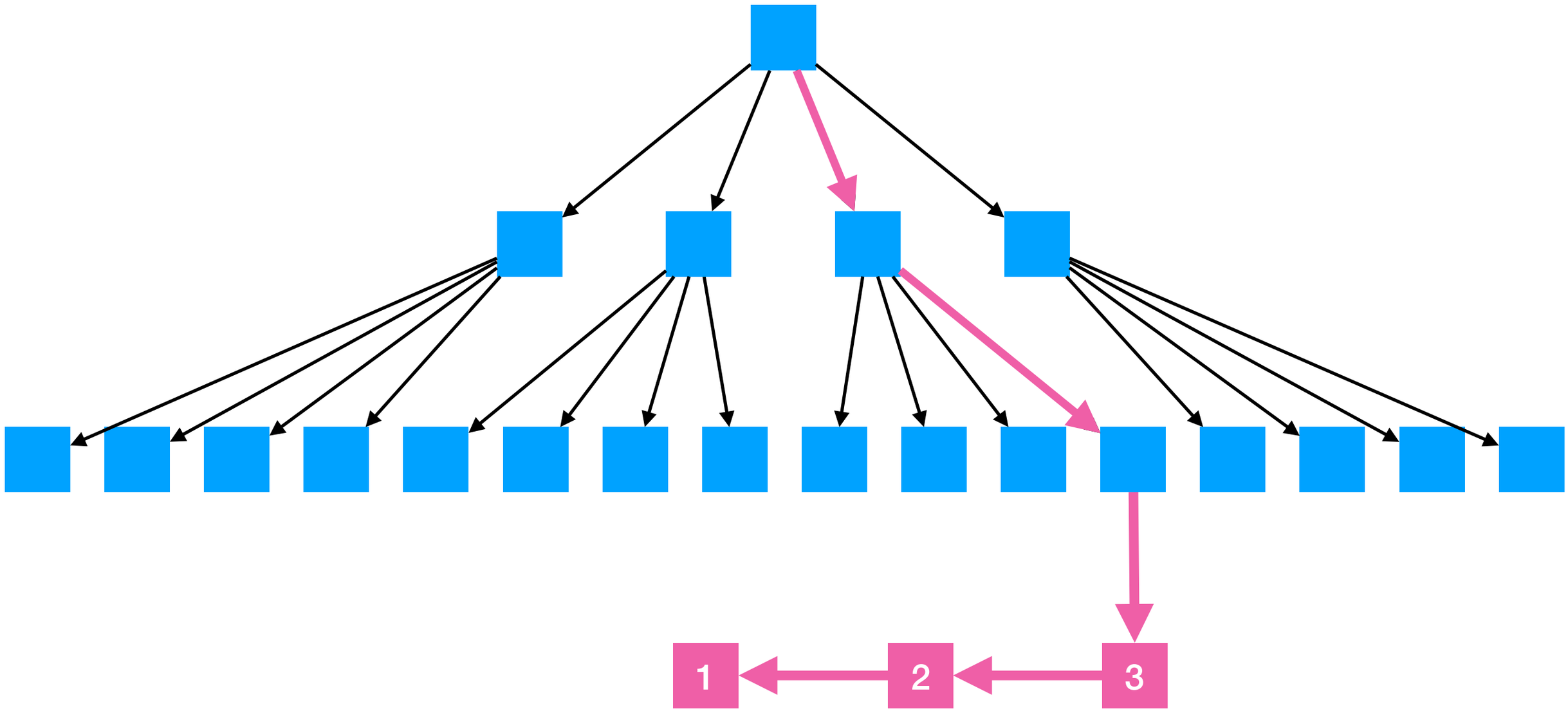
Talk Outline

- How devices sign statements to constitute a user
- How users sign statements to constitute a team

How to Define a User

Account Creation

- Picks a new username *n*
- Rolls a new Ed25519 Signing Key Pair (*s*,*S*)
- Rolls a new Curve25519 DH Key Pair (*d*,*D*)
- Rolls a new “per-user-key” Curve25519 DH Key Pair (*u*,*U*)
- Signs *D* with *s*
- Encrypts *u* for *D*
- Crucially, *s* and *d* never leave the device; encryption of *u* does
- Posts 3 sigchain links to the Keybase Merkle Tree under *n*



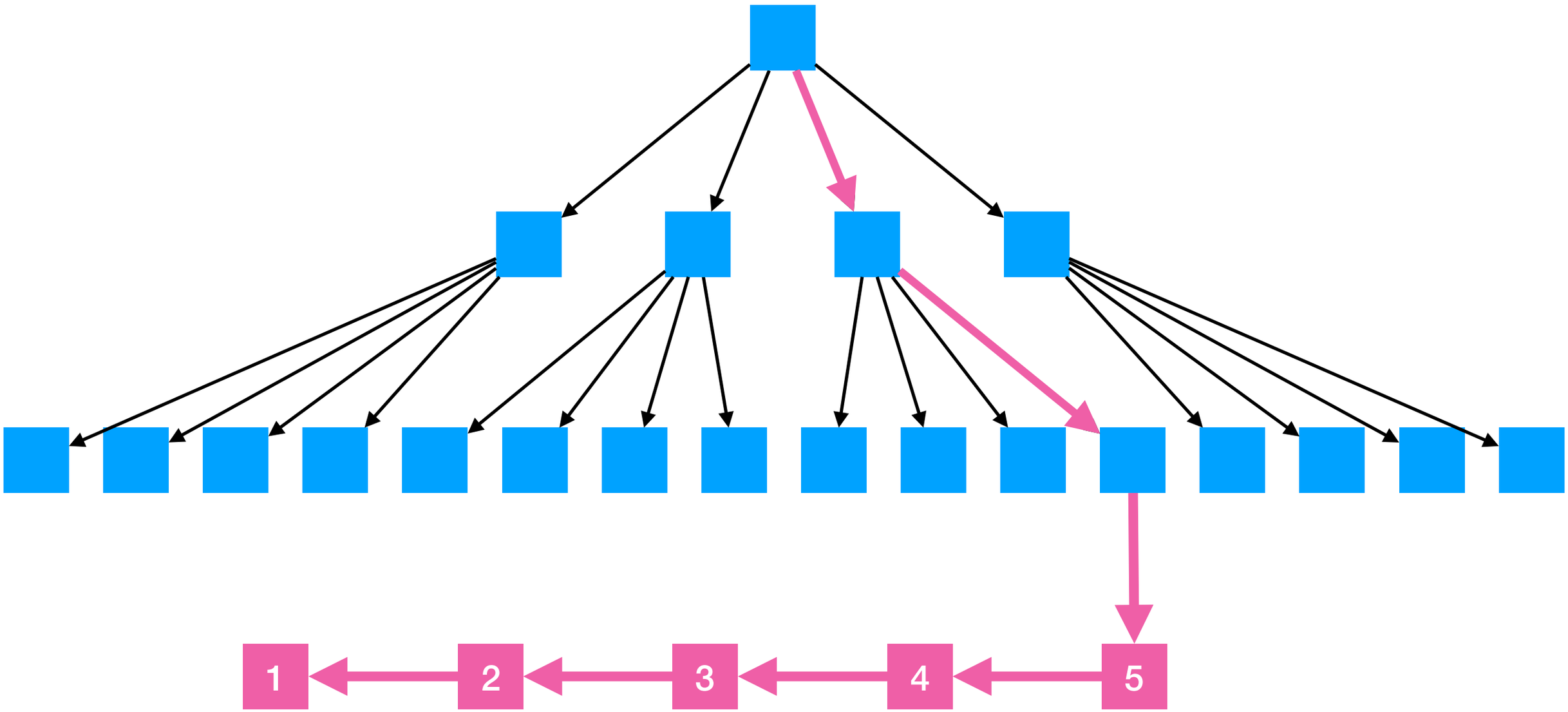
Link 1:
Alice=*S*,
σ_s(Alice=*S*)

Link 2:
σ_s(*D*, Hash(*link1*))

Link 3:
σ_s(*U*, Hash(*link2*))

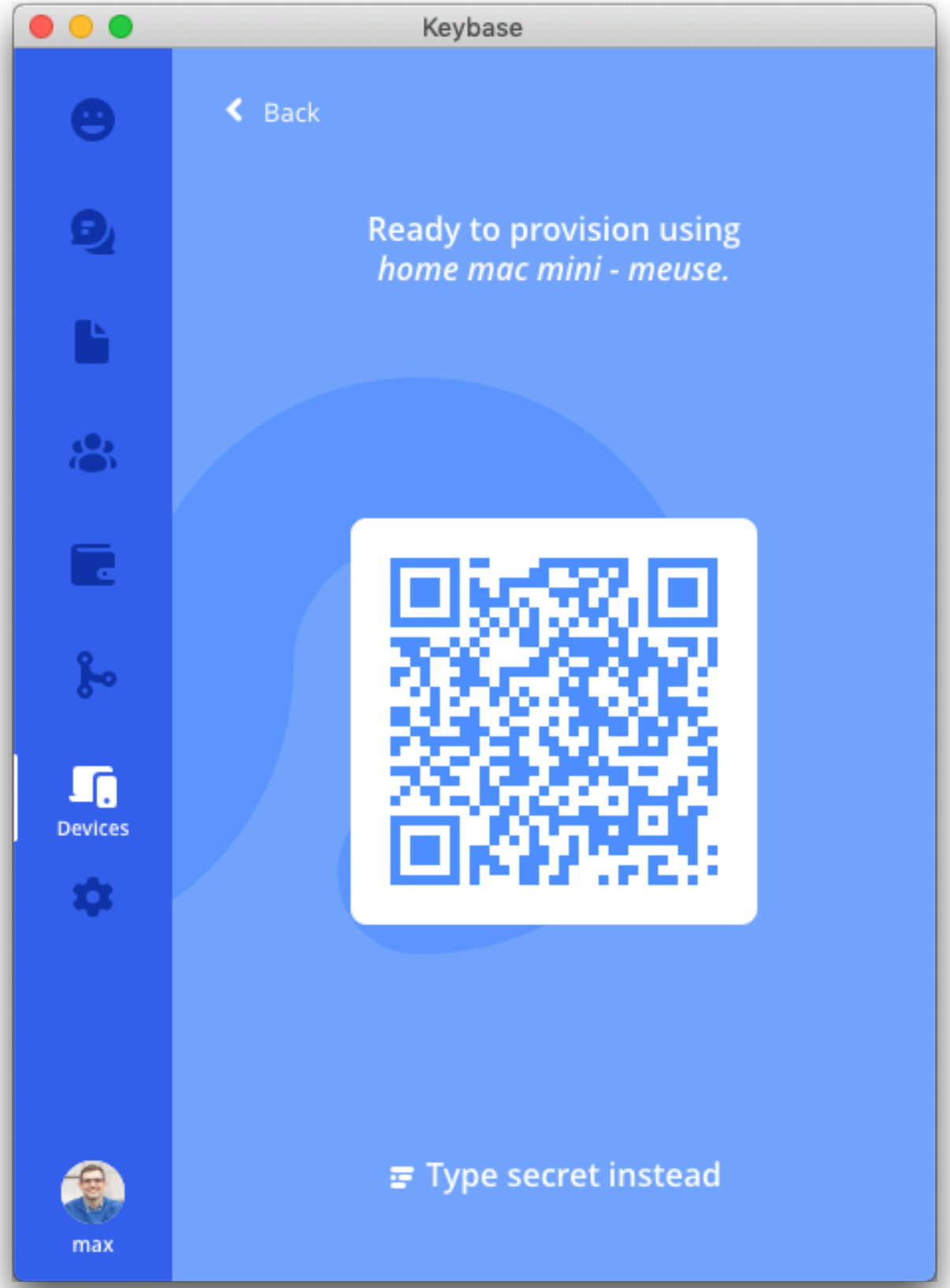
New Device Addition

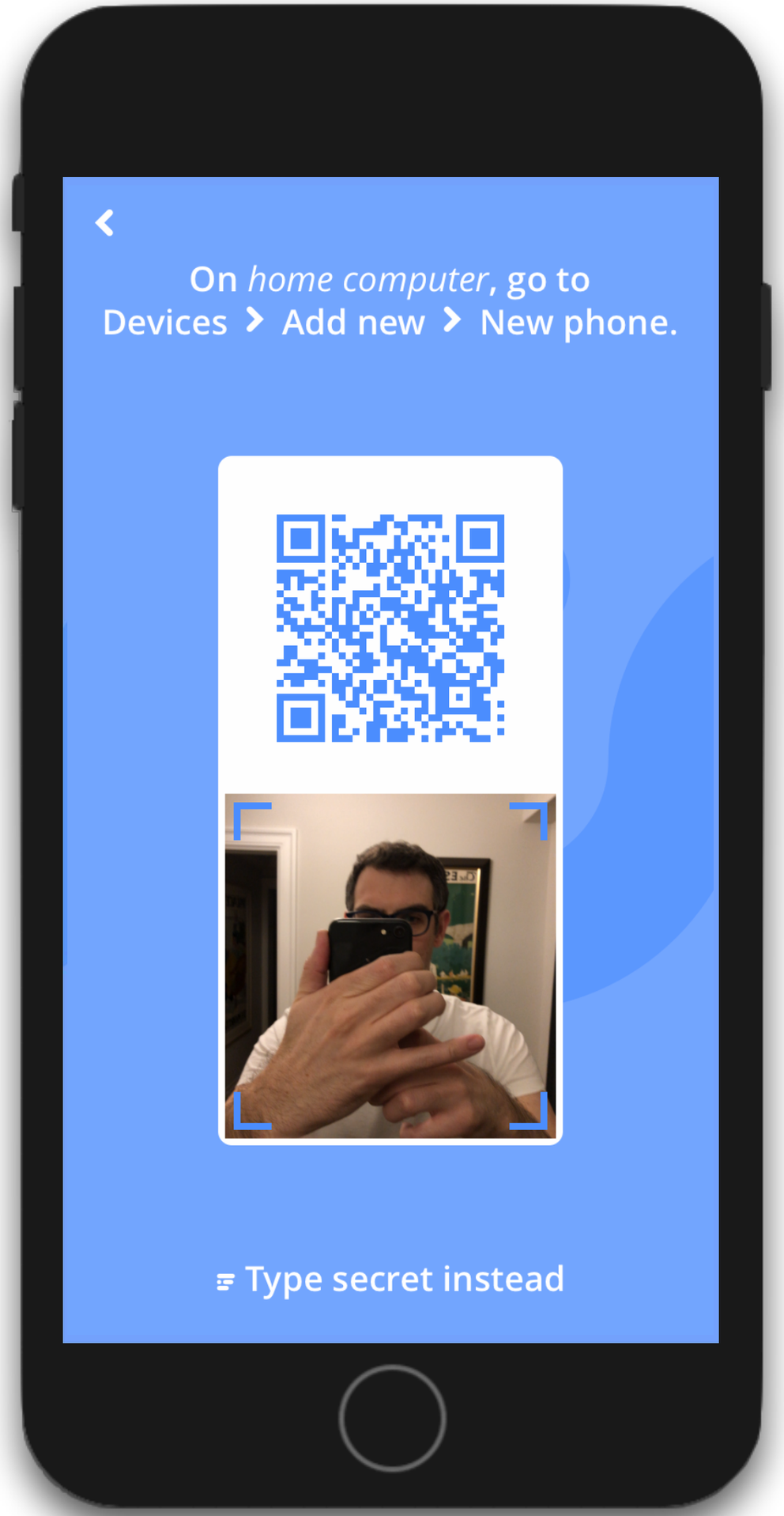
- New Ed25519 Key: (*s*',*S*')
- New Curve25519 Key: (*d*', *D*')
- Signs *S* with *s*' and *S*' with *s*
- Signs *D*' with *s*' as before
- Encrypts *u* for *D*'
- Posts 2 new sigchain links



Link 4:
$\sigma_{s}(S', \sigma_{s'}(S), \text{Hash}(\textit{link3}))$

Link 5:
$\sigma_{s'}(D', \text{Hash}(\textit{link4}))$

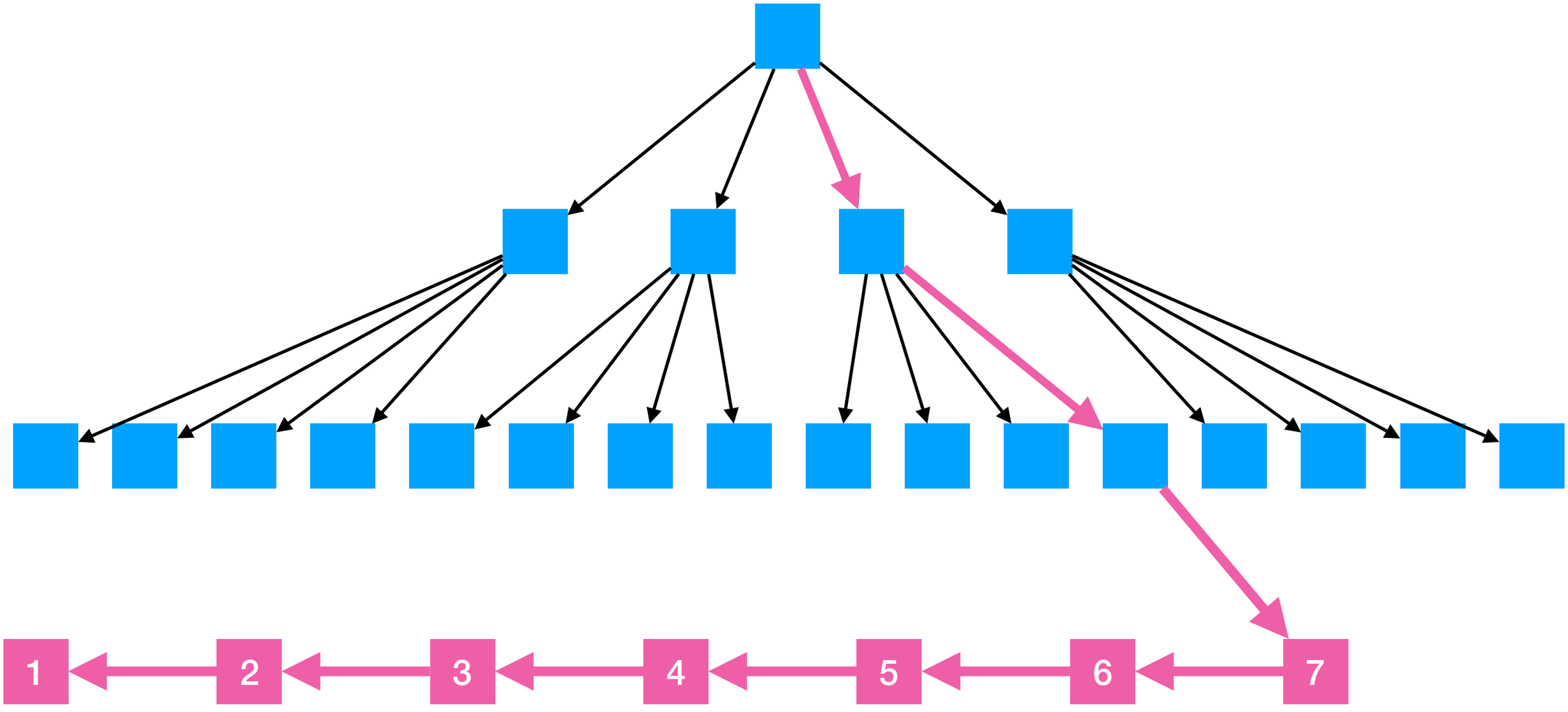

Keybase
Back
Ready to provision using
home mac mini - meuse.
Devices
max
Type secret instead


On home computer, go to
Devices › Add new › New phone.
Type secret instead

Revoking a Device

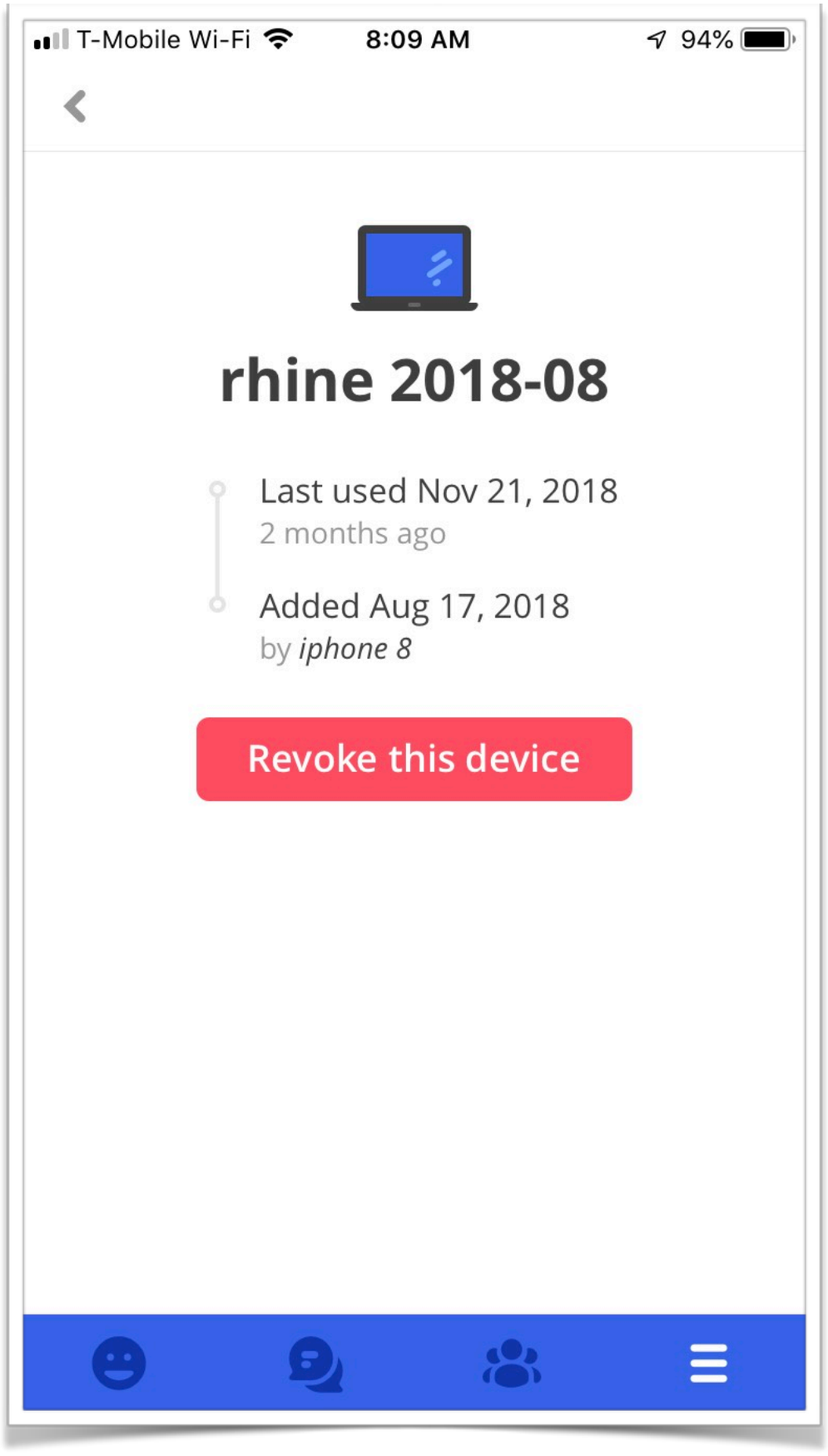
- Sign a statement to revoke *S* and *D* from lost/stolen/ retired device

- Rotate per-user-key to (*u*', *U*'), and re-encrypts *u*' for all non-revoked devices



Link 6:
$\sigma_{s'}$(revoke(*S*,*D*), Hash(*link5*))

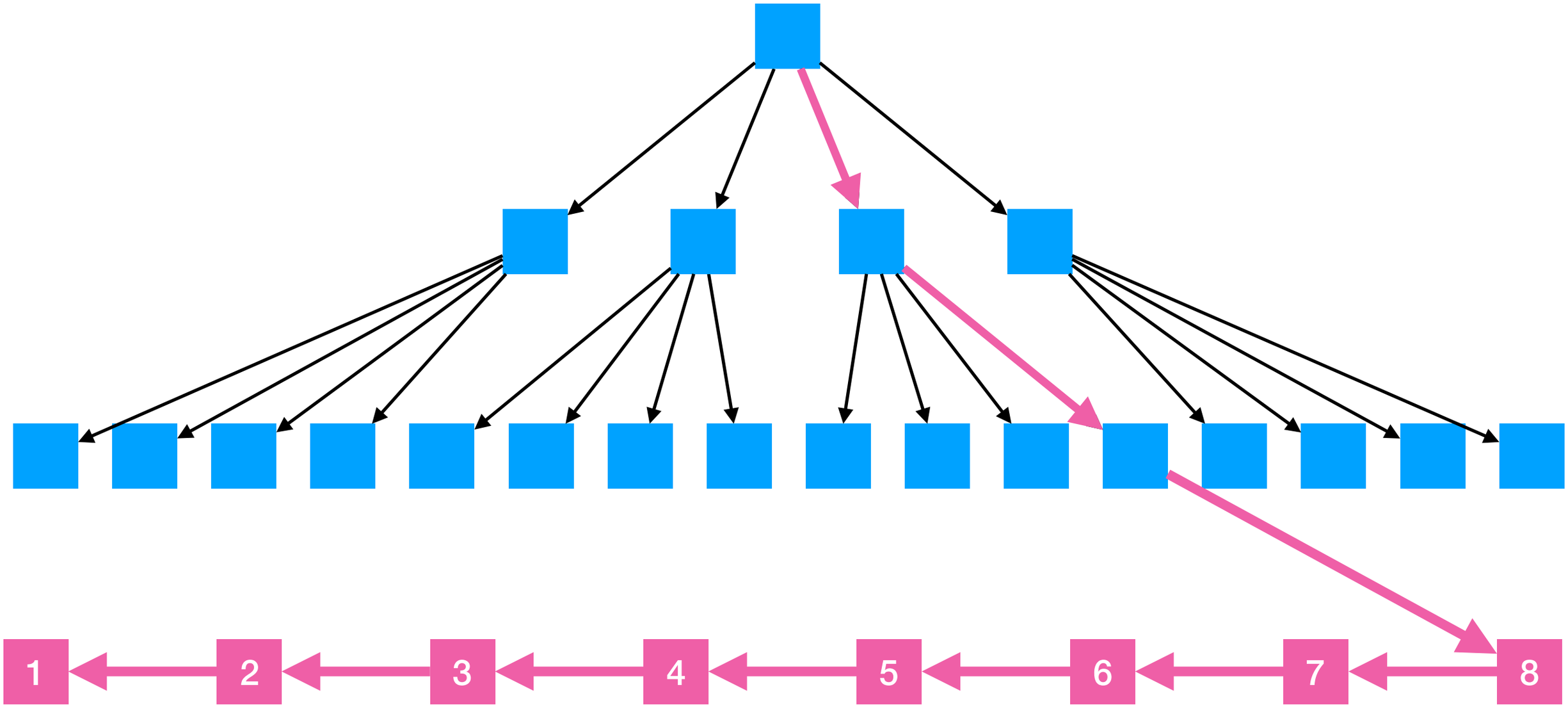
Link 7:
$\sigma_{s'}$(*U'*, Hash(*link6*))


T-Mobile Wi-Fi
8:09 AM
94%
rhine 2018-08
Last used Nov 21, 2018
2 months ago
Added Aug 17, 2018
by iphone 8
Revoke this device

Proving External Corroboration

- Alice posts a signature saying she is `@theRealAlice` on Twitter

- Then posts a hash of that signature to twitter



Link 8:
$\sigma_{s'}$(twitter: `@theRealAlice`**, Hash(*link7*))**

Review: Looking up Alice

- Descend the Merkle tree to Alice's leaf
- Fetch tail of her "sigchain"
- Playback chain from beginning to compute:
  - Signing Keys: {*S*'}
  - DH Keys: {*D*'}
  - Per-User-Key: *U*'
  - Claimed external identities: { twitter: `@theRealAlice` }

Keybase

People

4

Back

Search people

tammy

Tammy Camp

51 Followers · Following **13**

Founder and CEO of Stronghold

San Francisco, CA

Following | Chat | ...

Teams

stronghold.public OPEN

womenwhocrypto

16J4vfpoZ5sKGA7BQr5ZirMqd5mT1KeYf3@btc

tammycamp@twitter

tammyfcamp@facebook

tammycamp@github

hodl_strong@reddit

tammycamp@hackernews

E357 0FB4 2537 6D03@pgp

tammy*keybase.io NEW

public/tammy

FOLLOWERS (52) FOLLOWING (13)

max
Max Krohn

aalpanigrahi
Aashish Loknath Panigrahi

haenry

coreyballou
Corey Ballou

andreaborio
Andrea Borio

kungfooio
Matthew Clarke

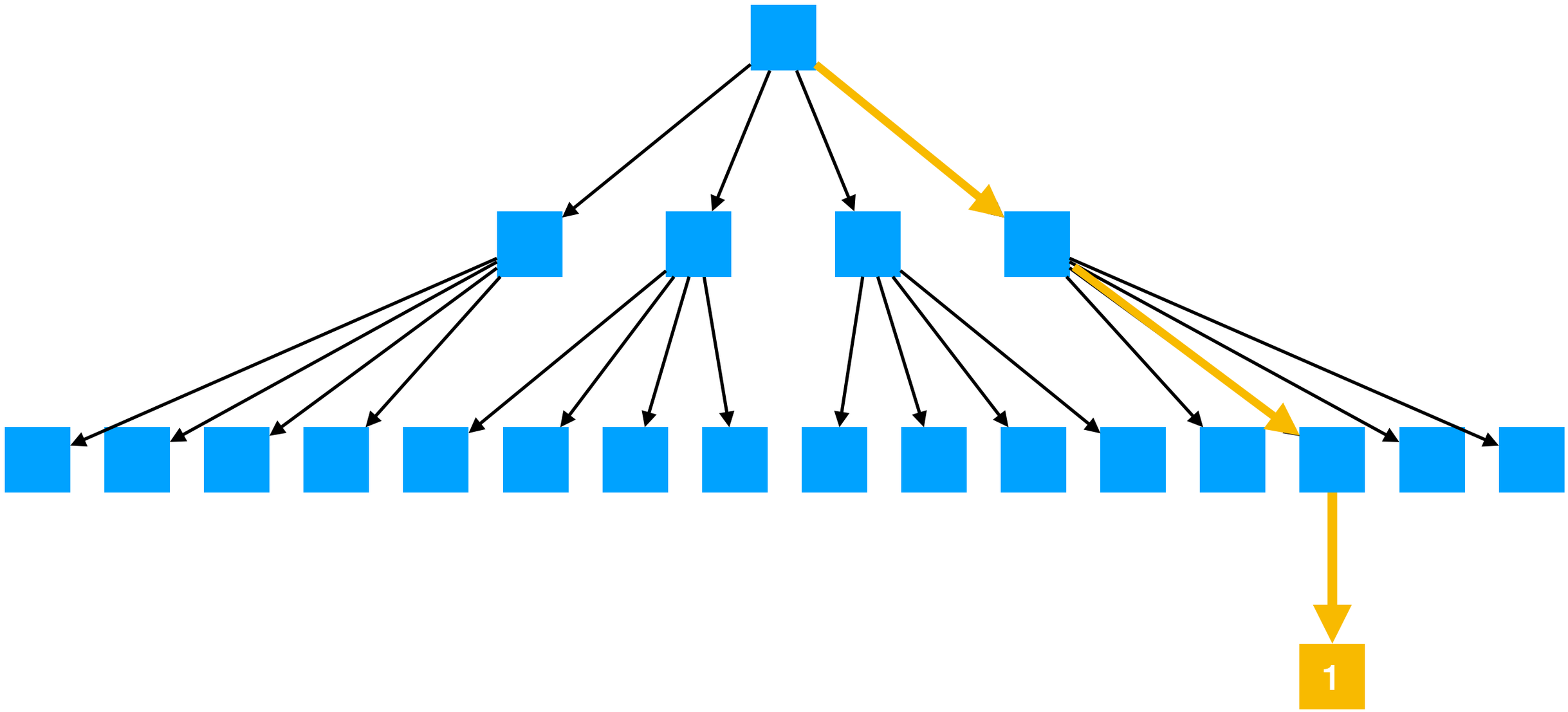
sgehrman
Steve Gehrman

max

How to Define a Team

Creating a Team

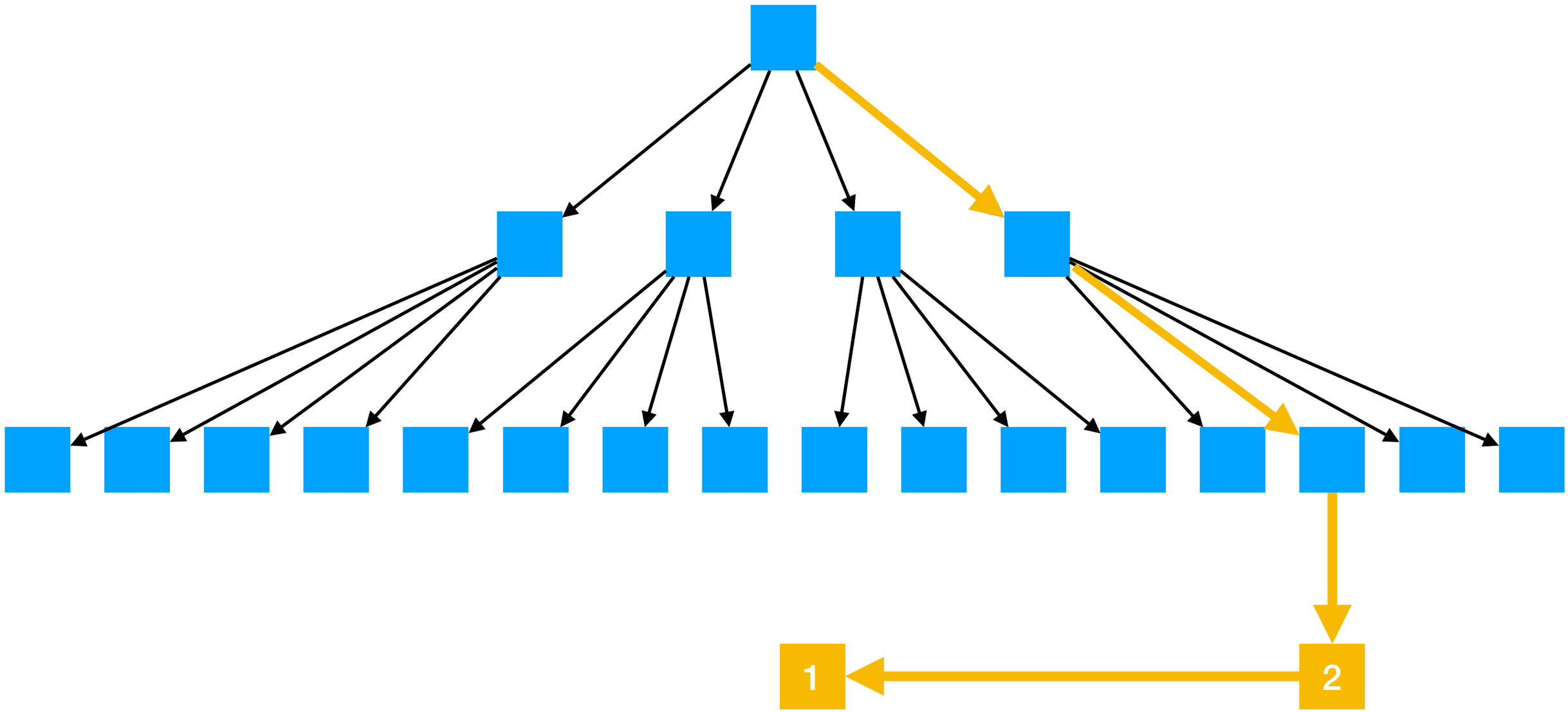
- Alice creates the team "coinco" with two admins, her and Bob.
- Rolls a new team secret: *t*
  - From *t*, generates team public keys:
    - (s_t, S_t) for signing
    - (d_t, D_t) for Diffie-Hellman
    - And a symmetric key for encrypted shared team data
- Encrypts *t* for U_A and U_B



Link 1:
σ_A(name=coinco,
admins={Alice,Bob}, keys={S_t,D_t})

Adding a User to a Team

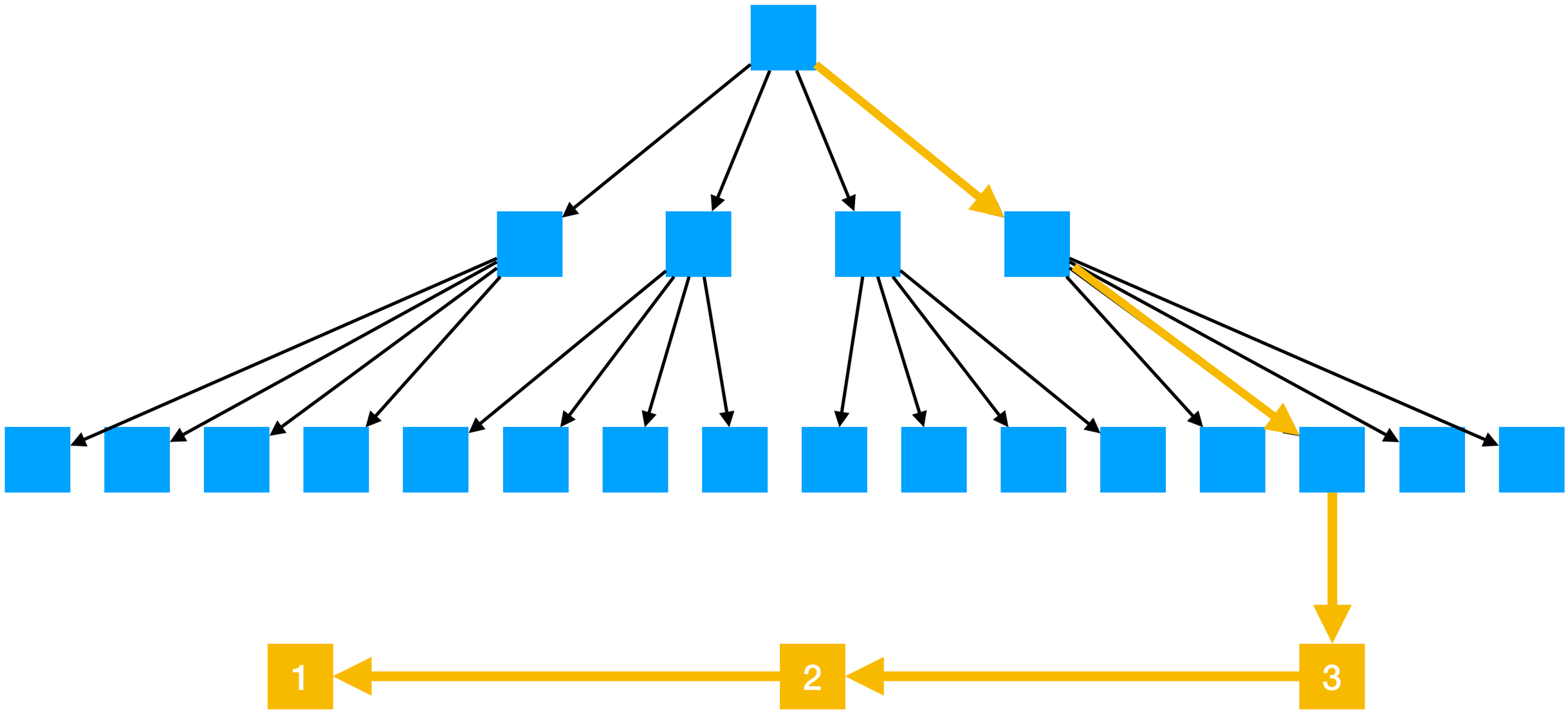
- Alice or Bob can now add Chuck to the team:
  - Admins can make membership changes
  - Non-admins just get to see team secrets
- Adds a sigchain link
- Encrypts *t* for U_C



Link 2:
σ_B(admins={Chuck}, Hash(*link1*))

Removing a User

- Admins can remove users, but must re-roll the team keys



Link 3:
σ_C(remove(Alice), keys={S'_t,D'_t}, Hash(*link2*))

Revoking a Device, Revisited

- Whenever team members revoke devices, their per-user-keys re-roll

- Therefore all teams they are in must re-roll their keys

- This can be done **lazily**, just before the next time someone chats, or writes a file for the team

Key Learning: PUKs

- v1.0 was built without
- Alice's mobile provisions a new laptop:
  - for all teams Alice is in:
    - Reencrypt team secret for laptop
- Rekey races Alice backgrounding the app
- Can resulting viral data loss across devices!

Details Elided / Other Lessons Learned

- Root of Merkle Tree gets posted to Bitcoin blockchain periodically to prevent “forking attacks”

- Ephemeral Messaging easily Scaling up to a 2k user team

- Users **still** need “education” on key management

In Sum…

- Key problem: multi-device with instant access on new device
    - Solution: Per-user-keys
- Users are chains of device additions/removals
    - All devices are equally powerful
- Teams are chains of user additions/removals
    - All admins are equally powerful
- From there, build a shared secret key for teams that rotates on revocation or member removal.

Keybase

Jump to chat

Chat

max 2:46 PM
Np!

tammy 1:56 PM
exciting times.

nextinpact 1:53 PM
jxerome: Bonne année ...

chris 1:44 PM
team page would be go...

keybase.design 1:33 PM
chris: cool, the website ...

+196 more

keybase

#bestcoast
#design
#frontend
#general
#kbfs
#music
#otr
#random
#releases

cecileb

keybase #general

FYI - we changed the default KBFS plan to 250GB instead of the 1TB. Very few people are hitting the limit so it's less wo
upgrading right now.

oconnor663
@chris Sweet!

cecileb
Team announcement GIFFF

jinyang
Cute!!!

chris
Ship it!

Write a message
songgao is typing

quote

5:07 PM
keybase
#general
@chris Sweet!
Fri 4:55 PM
cecileb
Team announcement GIFFF

jinyang
Cute!!!
chris
Ship it!
Write a message
NEW