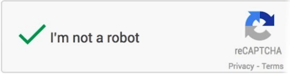
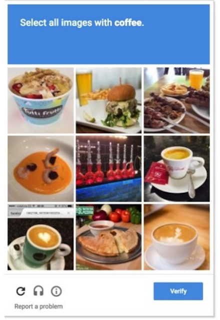
proof of history - social key recovery

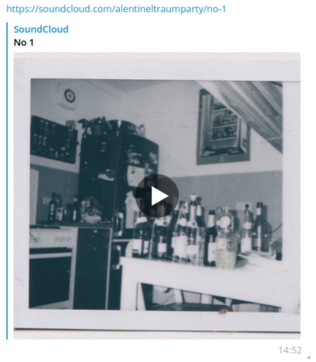




Abstract: Use media content from a chat history as "shared memoy" as a challenge in a challenge-response protocol. Essentially, a user has to prove to several of its peers, that it has knowledge of the content of the (encrypted) conversation and therefore had prior knowledge of the private key. If it success, the user's peers reveal their respective pieces of the key, s.t. the user can recover it.

Note: the media content for the challenges must be filtered to not leak content compromiosing user privacy and must not be guessable by an attacker, e.g. media containing information making the user identiefable should not be used (text and faces must be reomoved, hyperlinks, gifs, videos, music is more suitable). To cope with potential errors, a media set of large enough size has to

Which of the following content is from my private telegram account?

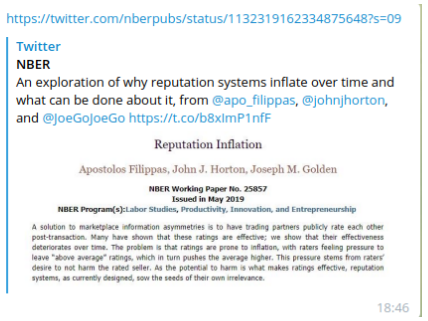


https://soundcloud.com/alentineltraumparty/no-1

SoundCloud

No 1

14:52



https://twitter.com/nberpubs/status/1132319162334875648?s=09

Twitter

NBER

An exploration of why reputation systems inflate over time and what can be done about it, from @apo_filippas, @johnjhorton, and @JoeGoJoeGo https://t.co/b8xImP1nfF

Reputation Inflation

Apostolos Filippas, John J. Horton, Joseph M. Golden

NBER Working Paper No. 25857
Issued in May 2019
NBER Program(s): Labor Studies, Productivity, Innovation, and Entrepreneurship

A solution to marketplace information asymmetries is to have trading partners publicly rate each other post-transaction. Many have shown that these ratings are effective; we show that their effectiveness deteriorates over time. The problem is that ratings are prone to inflation, with raters feeling pressure to leave "above average" ratings, which in turn pushes the average higher. This pressure stems from raters' desire to not harm the rated seller. As the potential to harm is what makes ratings effective, reputation systems, as currently designed, sow the seeds of their own irrelevance.

18:46

We speculate even as we try to minimize uncertainties.
We believe in science fiction, the realism of our time.
The future is neither a nightmare nor a daydream.

We try to come up with stories, answers and possibilities, not with questions, mere observations, data and complaints.

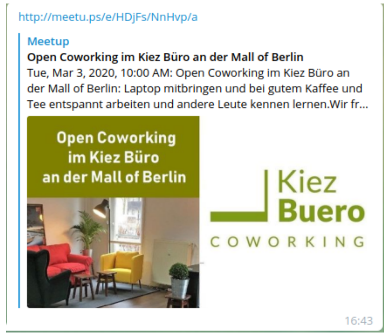
We believe in compression. If arguments don't survive compression, they are bad arguments. So no piece should be longer than five minutes. Or two.

We try to make complex ideas seem simple.
Build arguments, form positions, create a tagline, be populist.

We make programs with recurring episodes, not unique masterpieces.

We try to think politically about the relations between subjects, whether human or nonhuman. Don't count on heroes. The system has to change.
And stop looking at yourself.

We don't believe in the lonely genius. Neither in resistance, withdrawal or anarchy.



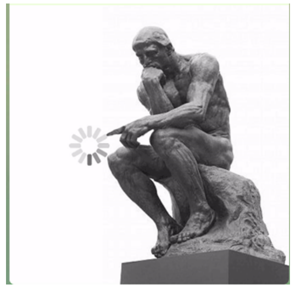
http://meetu.ps/e/HDjFs/NnHvp/a

Meetup

Open Coworking im Kiez Büro an der Mall of Berlin

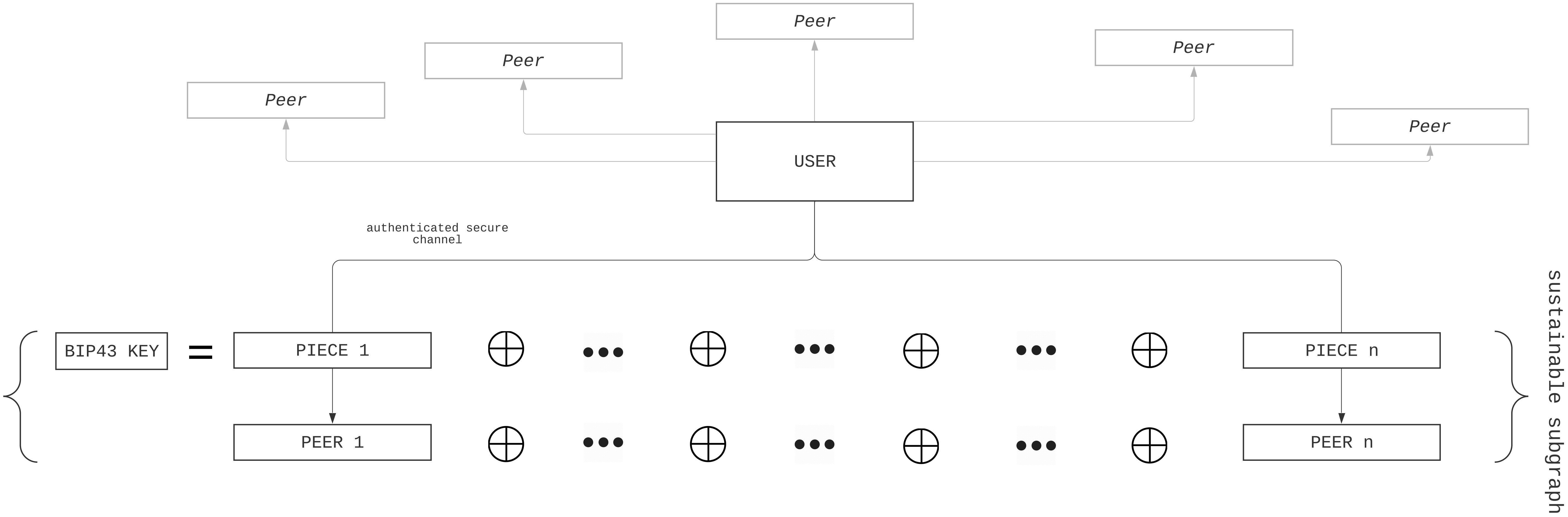
Tue, Mar 3, 2020, 10:00 AM: Open Coworking im Kiez Büro an der Mall of Berlin: Laptop mitbringen und bei gutem Kaffee und Tee entspannt arbeiten und andere Leute kennen lernen.Wir fr...

16:43



proof of history - social key recovery: setup

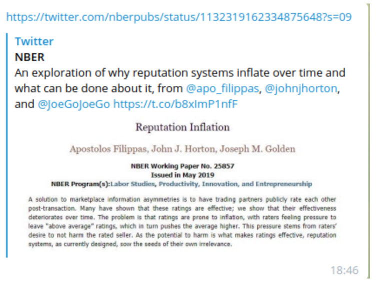
v0, n=k, manual peer selection



02-25-2020

Alice want's to recover.
She calls Bob and
Charlie.

Bob's
challenge



https://twitter.com/nberpubs/status/1132319162334875648?s=09

Twitter

NBER

An exploration of why reputation systems inflate over time and what can be done about it, from @apo_filippas, @johnjhorton, and @JoeGoJoeGo https://t.co/b8xImP1nfF

Reputation Inflation

Apostolos Filippas, John J. Horton, Joseph M. Golden

NBER Working Paper No. 25857
Issued in May 2019
NBER Program(s): Labor Studies, Productivity, Innovation, and Entrepreneurship

A solution to marketplace information asymmetries is to have trading partners publicly rate each other post-transaction. Many have shown that these ratings are effective; we show that their effectiveness deteriorates over time. The problem is that ratings are prone to inflation, with raters feeling pressure to leave "above average" ratings, which in turn pushes the average higher. This pressure stems from raters' desire to not harm the rated seller. As the potential to harm is what makes ratings effective, reputation systems, as currently designed, sow the seeds of their own irrelevance.

18:46

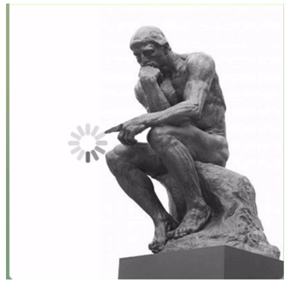
#ATraditionOfTrust

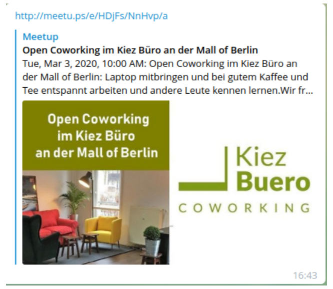
WE ARE HIRING

Sales Executives

Submit your application to
recruitment@username.co.ke
on or before 8th March 2019

Visit **https://usernameproperties.com/careers**





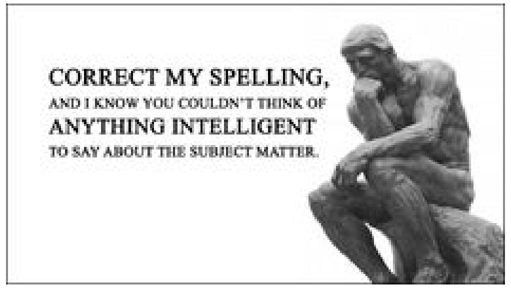
http://meetu.ps/e/HDjFs/NnHvp/a

Meetup

Open Coworking im Kiez Büro an der Mall of Berlin

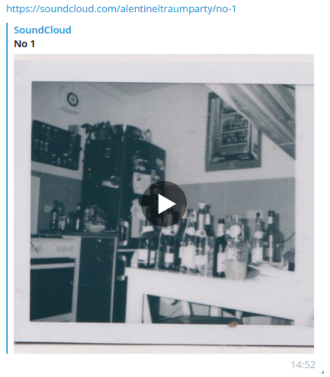
Tue, Mar 3, 2020, 10:00 AM: Open Coworking im Kiez Büro an der Mall of Berlin: Laptop mitbringen und bei gutem Kaffee und Tee entspannt arbeiten und andere Leute kennen lernen.Wir fr...

16:43



CORRECT MY SPELLING,
AND I KNOW YOU COULDN'T THINK OF
ANYTHING INTELLIGENT
TO SAY ABOUT THE SUBJECT MATTER.

Charlie's
challenge

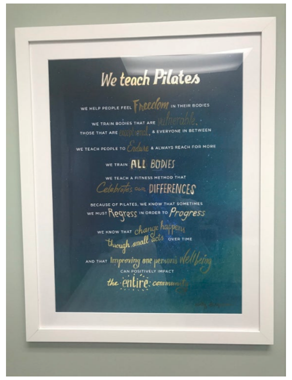


https://soundcloud.com/alentineltraumparty/no-1

SoundCloud

No 1

14:52



We teach Pilates

WE HELP PEOPLE FEEL Freedom IN THEIR BODIES

WE TRAIN BODIES THAT ARE vulnerable,
THOSE THAT ARE exceptional, & EVERYONE IN BETWEEN

WE TEACH PEOPLE TO Endure & ALWAYS REACH FOR MORE

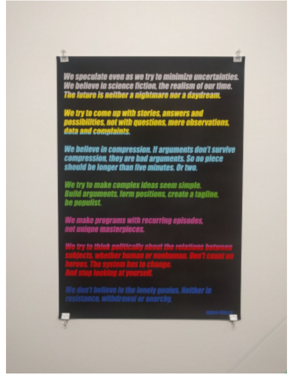
WE TRAIN ALL BODIES

WE TEACH A FITNESS METHOD THAT
Celebrates our DIFFERENCES

BECAUSE OF PILATES, WE KNOW THAT SOMETIMES
WE MUST Regress IN ORDER TO Progress

WE KNOW THAT change happens
through small acts OVER TIME

AND THAT Improving one person's Wellbeing
CAN POSITIVELY IMPACT
the entire community



We speculate even as we try to minimize uncertainties.
We believe in science fiction, the realism of our time.
The future is neither a nightmare nor a daydream.

We try to come up with stories, answers and
possibilities, not with questions, mere observations,
data and complaints.

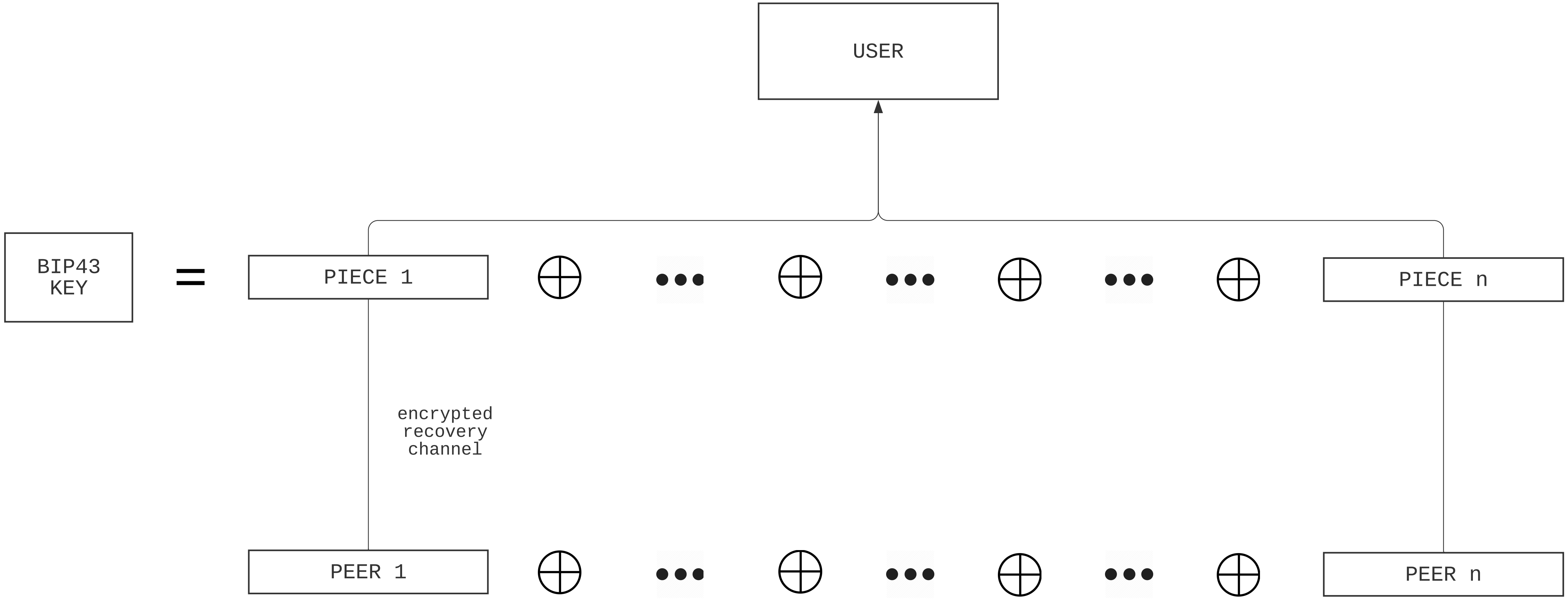
We believe in compression. If arguments don't survive
compression, they are bad arguments. So no piece
should be longer than five minutes. Or two.

We try to make complex ideas seem simple.
Build arguments, form positions, create a tagline,
be populist.

We make programs with recurring episodes,
not unique masterpieces.

We try to think politically about the relations between
subjects, whether human or nonhuman. Don't count on
heroes. The system has to change.
And stop looking at yourself.

We don't believe in the lonely genius. Neither in
resistance, withdrawal or anarchy.


USER
BIP43
KEY
=
PIECE 1
PIECE n
encrypted
recovery
channel
PEER 1
PEER n