

1729

Lecture 12: The Pseudonymous Economy

Separate out your earning name, speaking name, and official name.



6529

@punk6529

...

I still can't believe how right [@balajis](#) was on avatars/pseudo identity.

Jan 2021: Was thinking "ok, sure, [@balajis](#), interesting idea, maybe 10 years from now kids would do it but why would *I* need a pseudo identity?"

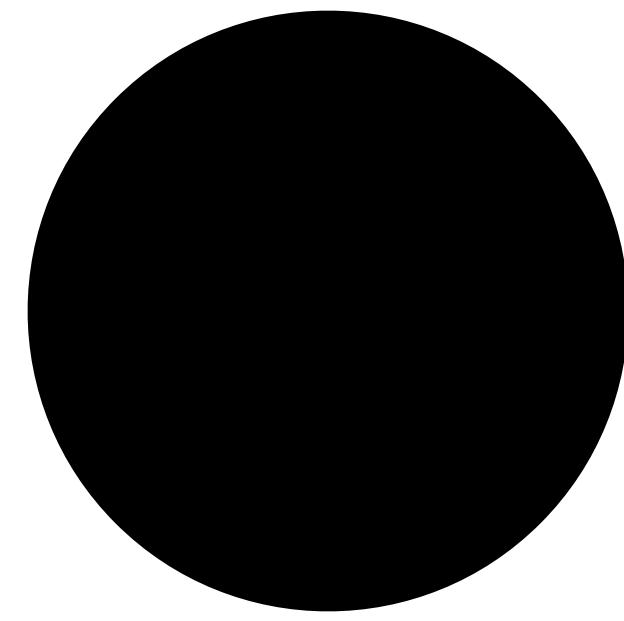
Jan 2022: Well, here we are...

5:46 PM · Jan 16, 2022 · Twitter Web App

103 Retweets

25 Quote Tweets

1,500 Likes



The Pseudonymous Economy

Why should we want it, and how do we build it?

What is pseudonymity?

Why a pseudonymous economy?

How might it work?

How could we build it?

Pseudonymity is not anonymity

Let's distinguish real names, pseudonyms, and
anonyms.

Real names



www.facebook.com/zuck?sk=wall

facebook

Mark Zuckerberg

Works at Facebook Studied Computer Science at Harvard University Lives in Palo Alto, California Knows English, Mandarin Chinese From Dobbs Ferry, New York Born on May 14, 1984

Wall

RECENT ACTIVITY

"I like dangerous thoughts." on Samuel W. Lessin's status.

Mark Zuckerberg

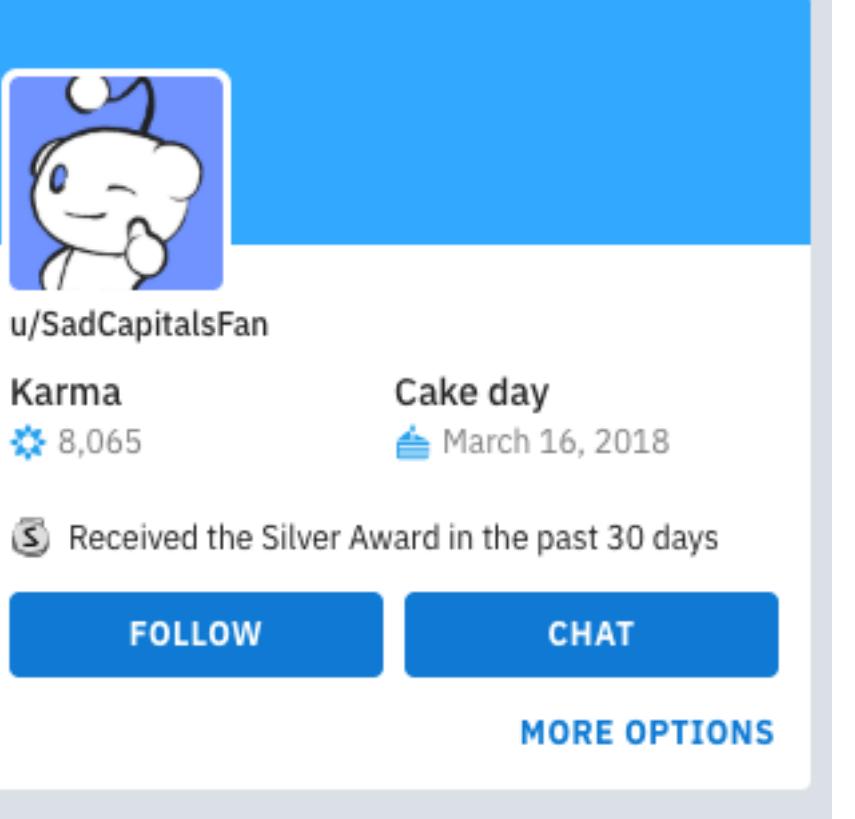
Steve, you've done so much good for the world already. I hope you get better soon.

January 17 at 11:43am via iPhone

150 people like this.

Share Profile Report/Block This Person

Pseudonyms



u/SadCapitalsFan

Karma 8,065

Cake day March 16, 2018

Received the Silver Award in the past 30 days

FOLLOW CHAT MORE OPTIONS



Comfortably Smug

@ComfortablySmug

My Interests: Finance, Whiskey, Politics, Books, Food, Meeting Strangers #altcenter

Anonyms

File: [anon.jpg](#) (62 KB, 1200x797)

Anonymous 12/02/16(Fri)00:14:43 No.713797026 [Reply] ▶
[">>>713803799](#) [">>>713804075](#)

Dear 4chan,

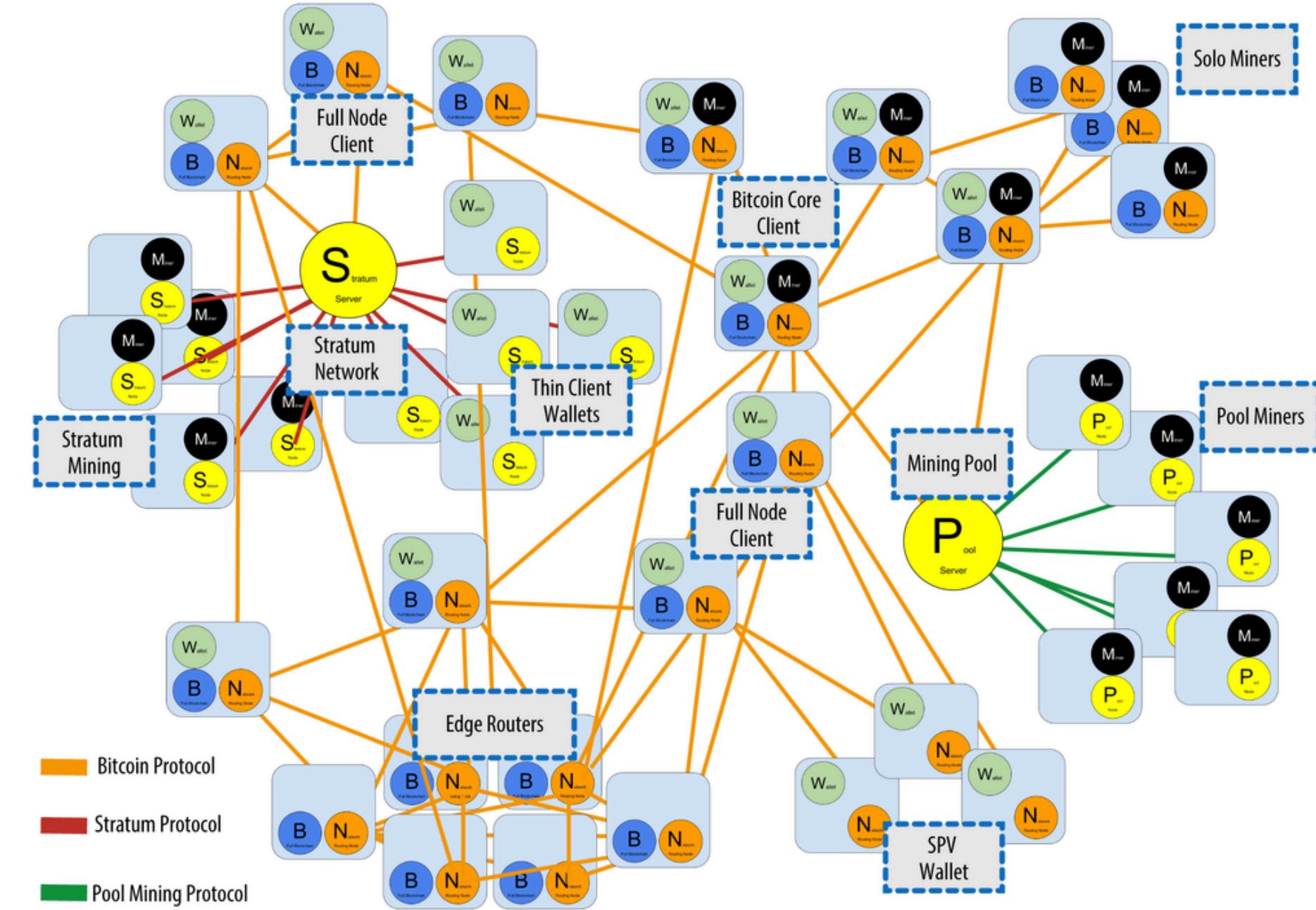
It's us, Anonymous, once again. Except this time it's The Leader speaking.



Pseudonymity is as important as decentralization

Satoshi's pseudonymity was as important as Bitcoin's decentralization.

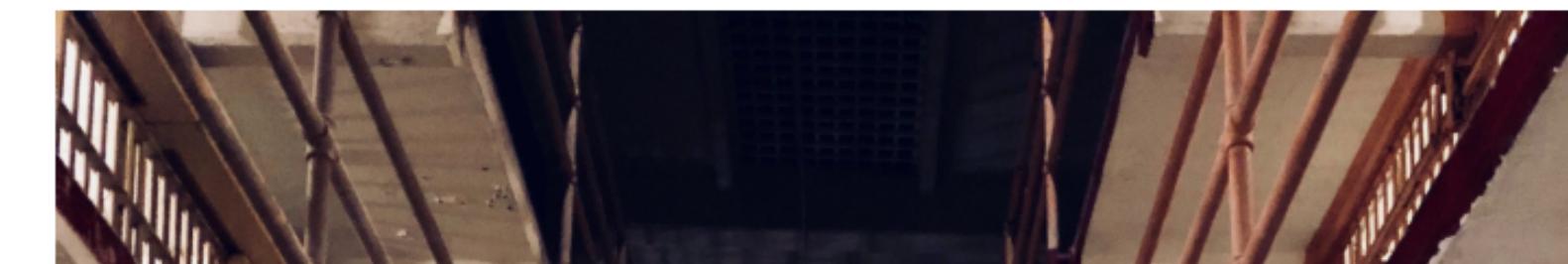
They couldn't play either the man or the ball.



Should Satoshi Nakamoto Go to Jail?

October 14th 2019

[TWEET THIS](#)



The Information That Is Needed to Identify You: 33 Bits

Pseudonymity is a continuum

The concept of 33 bits allows us to quantify the degree of privacy for a given pseudonym.

By WSJ Staff

Aug 4, 2010 12:20 am ET

2^{33}	8.6B	33 bits
World population	7.5B	32.8 bits
Twitter MAUs	330M	28.3 bits
Twitter verified	330K	18.3 bits

Pseudonymity is already mainstream

From Comey and Romney to Finstas/Rinstas and hundreds of millions on Reddit.

NICKNAMES | OCT. 21, 2019

Mitt Romney Is Pierre Delecto: A Brief Guide to Political Pseudonyms

By Adam K. Raymond



Acts of Faith

Why did James Comey name his secret Twitter account 'Reinhold Niebuhr'? Here's what we know.

Comey's secret Twitter, according to the internet



Technology & Science · Analysis

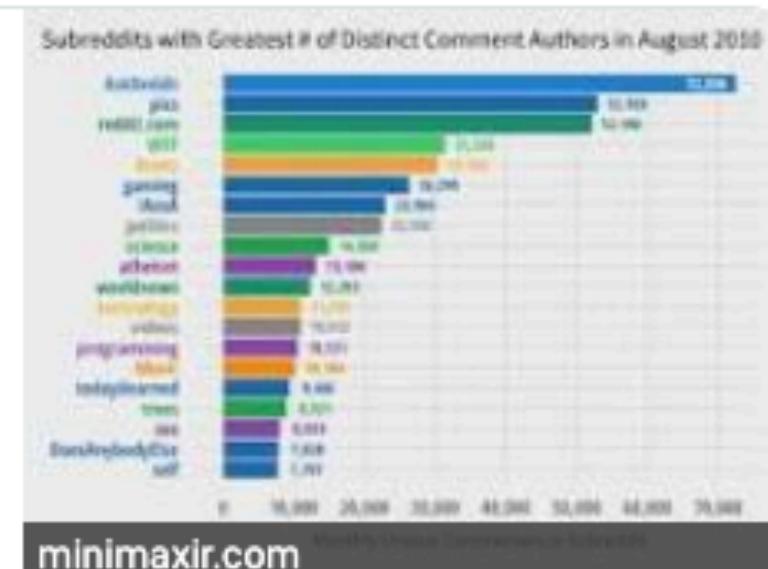
Finstas: Using 'fake' social media accounts to reveal your authentic self

330 million Reddit users

" As of 2018, there are approximately 330 million **Reddit users**, called "redditors". The site's content is divided into categories or communities known on-site as "subreddits", of which there are more than 138,000 active communities.

[Reddit - Wikipedia](#)

<https://en.wikipedia.org/wiki/Reddit>



Pseudonymity is where society is going

Multiple accounts, hiring practices, social mob attacks, remote, crypto, and encryption

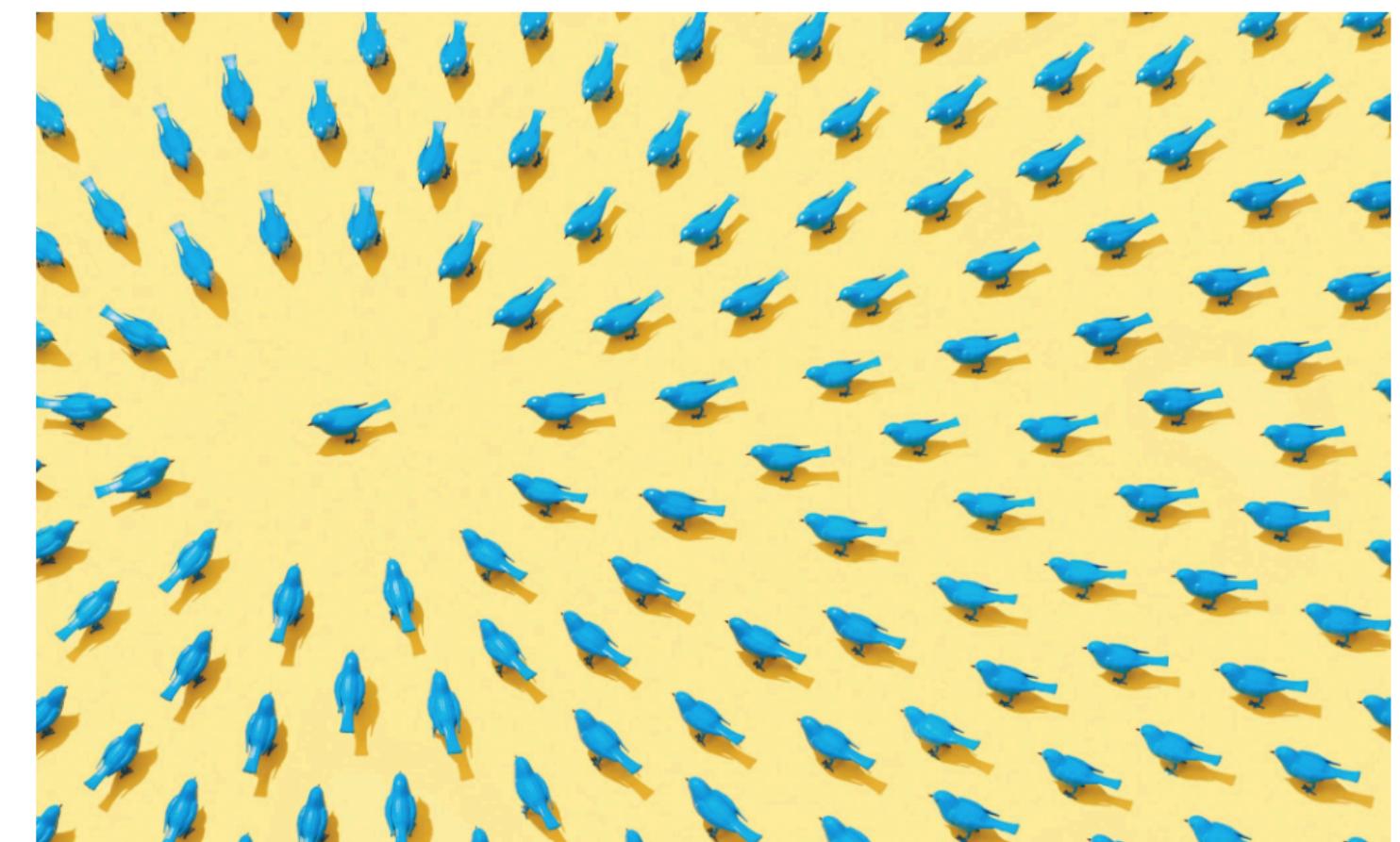
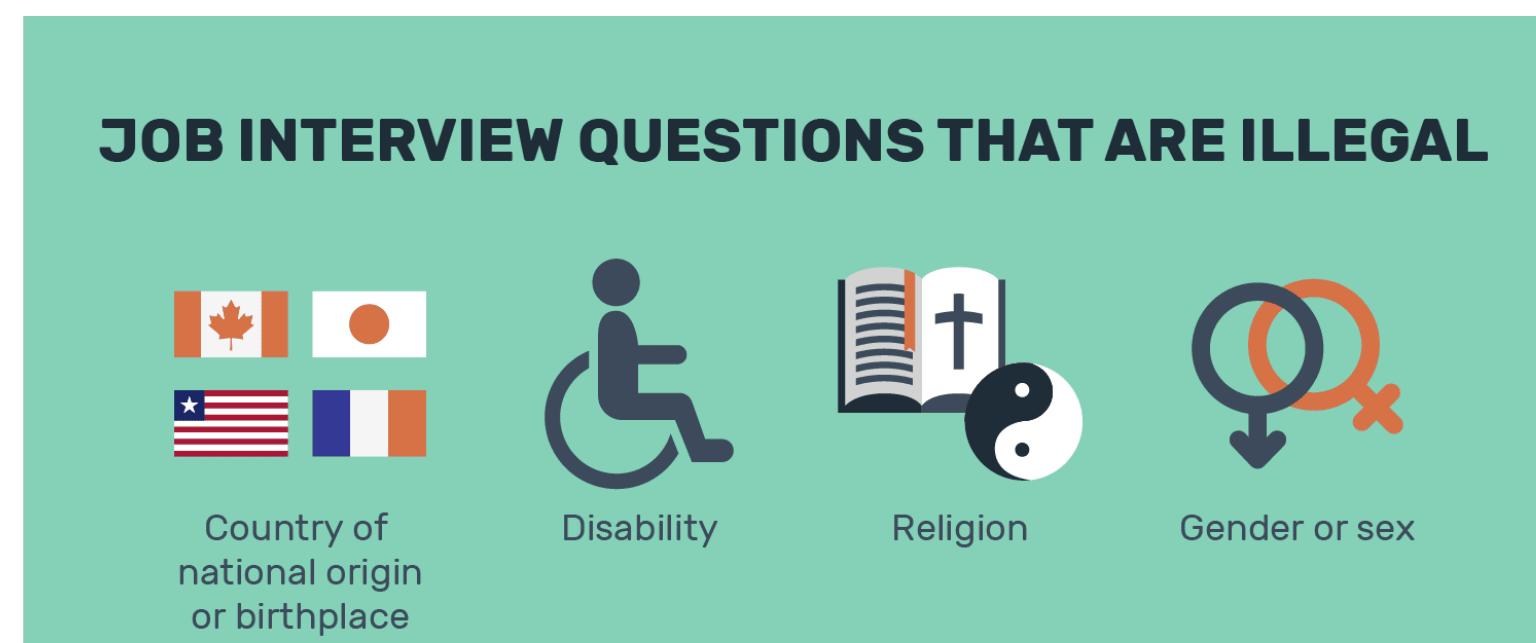
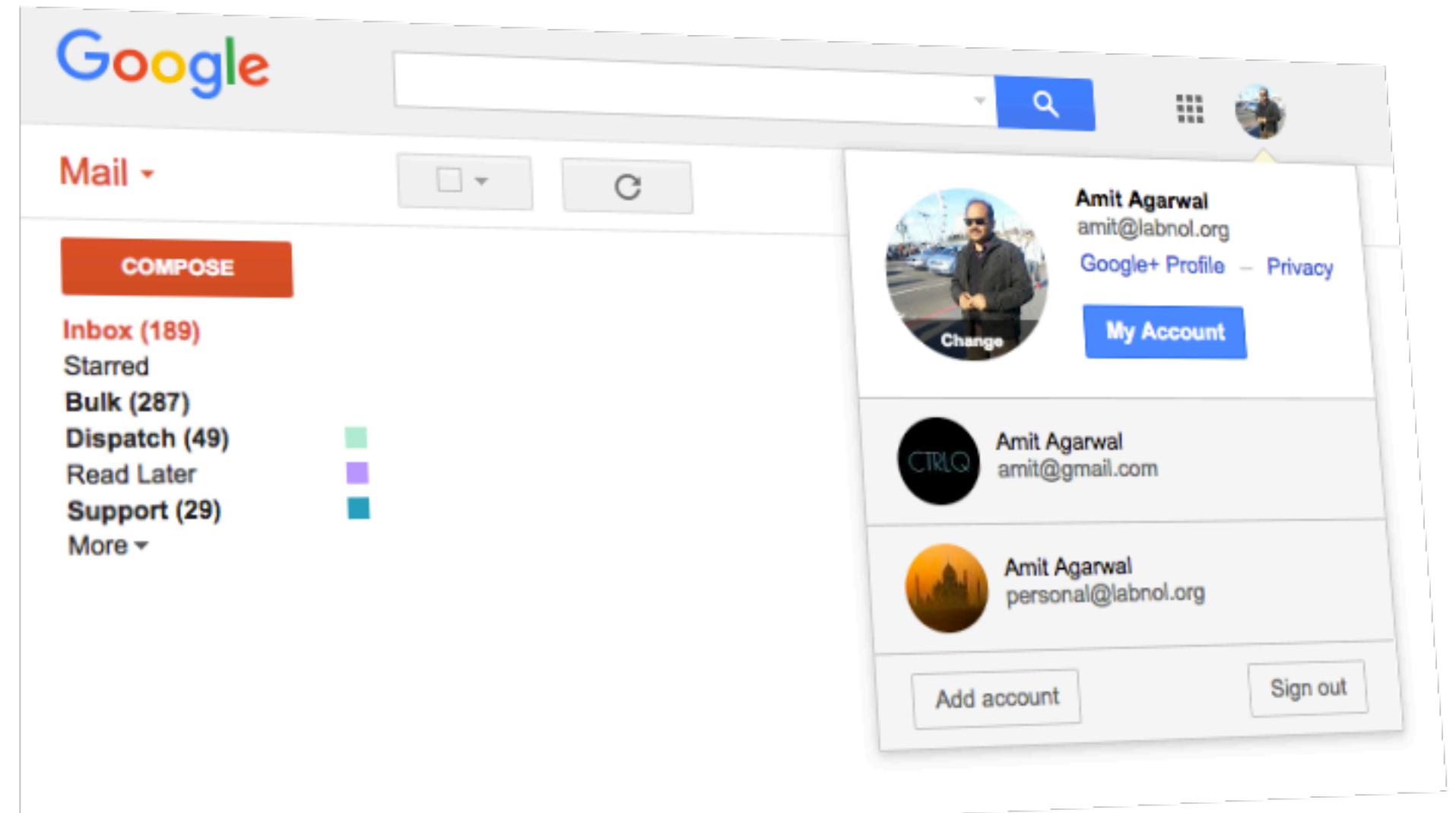


Photo illustration by Andrew B. Myers. Prop stylist: Sonja Rentsch.

What is pseudonymity?

Why a pseudonymous economy?

How might it work?

How could we build it?

Pseudonymity allows freedom after speech

Prevents retaliation against the person for expressing an idea, often by a social media mob



In Soviet Russia, we too have freedom of speech. But in America, you have freedom after speech!

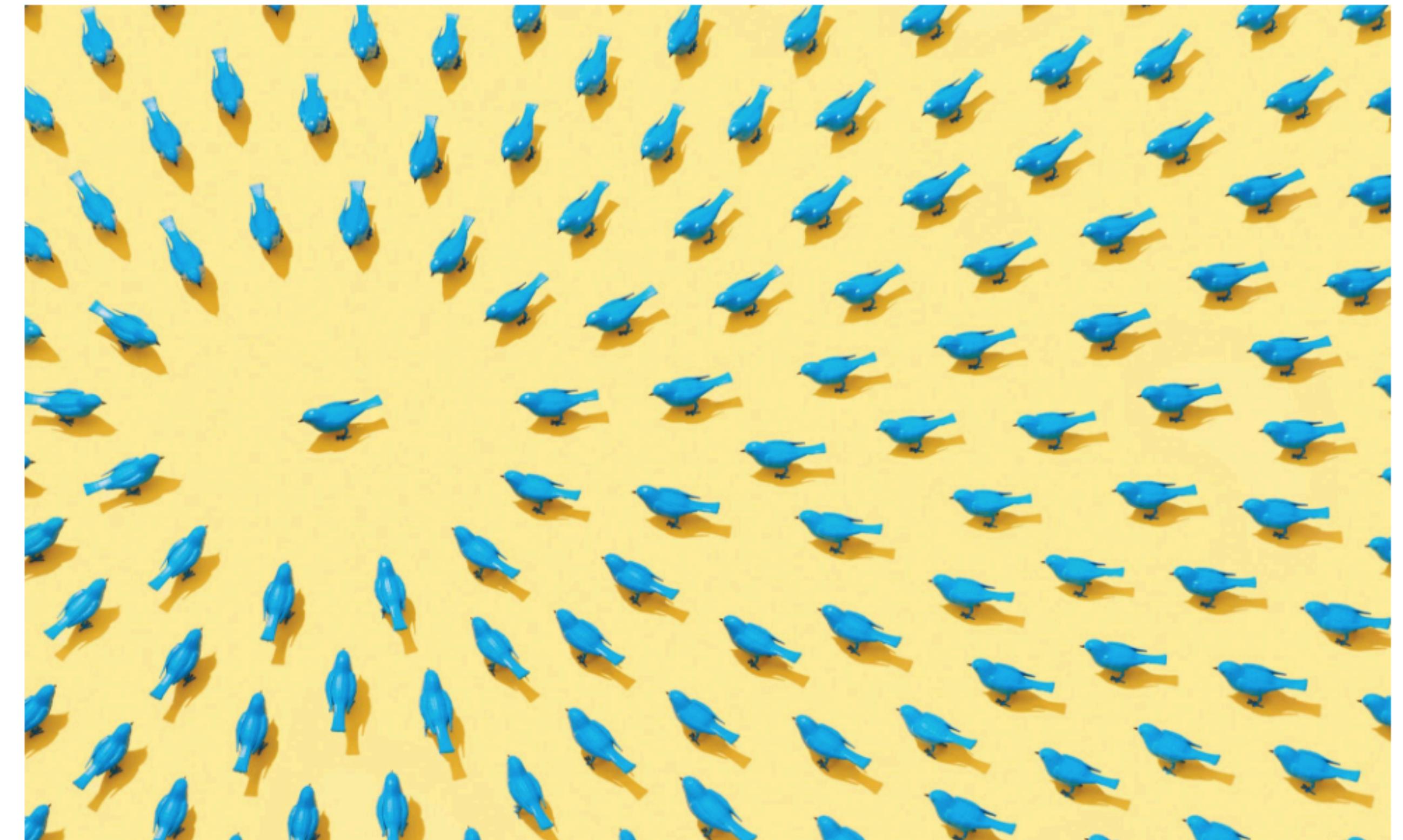
Yakov Smirnoff

Why? Because social media mobs are now routine

Everyone is a journalist, and everyone is a public figure.

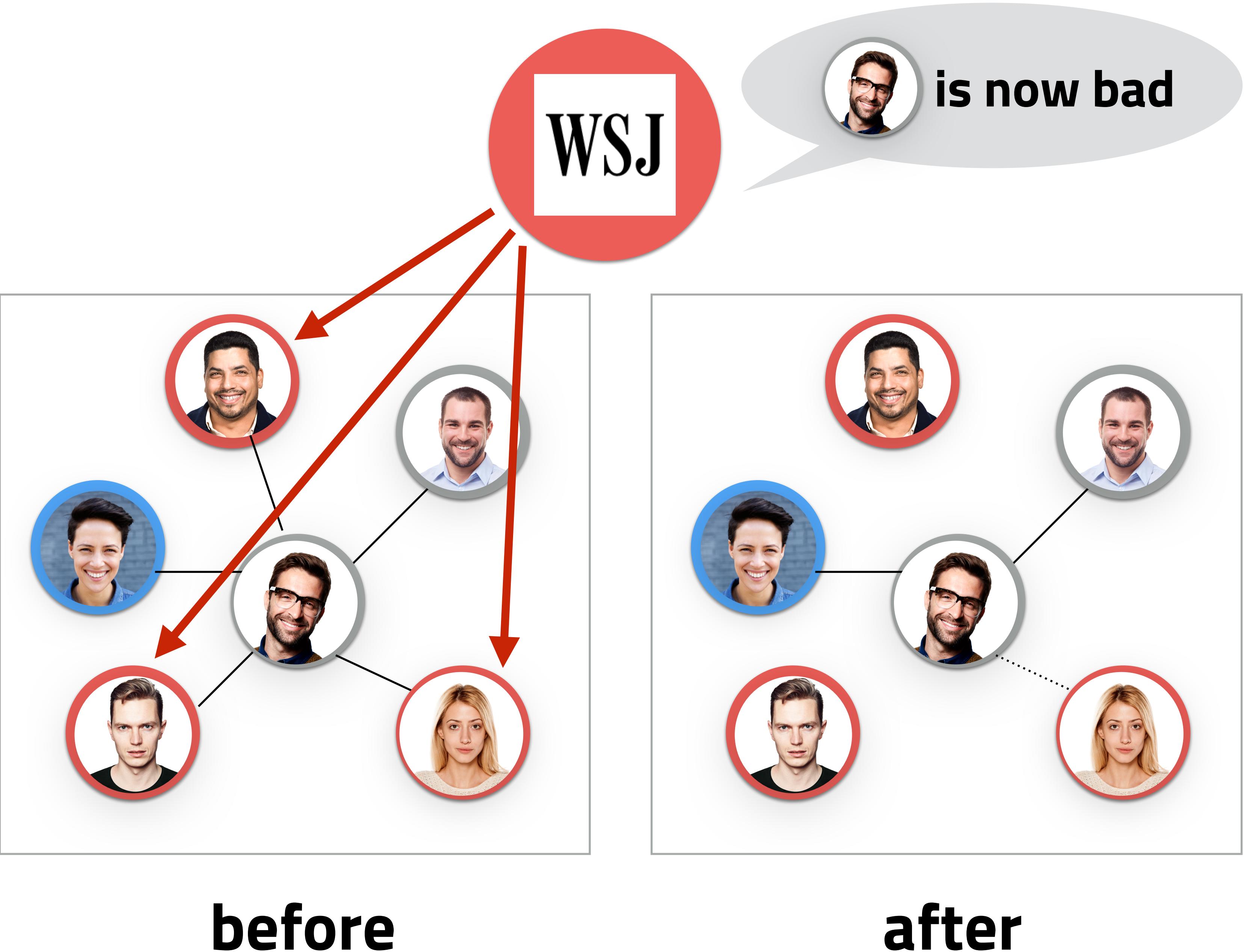
How One Stupid Tweet Blew Up Justine Sacco's Life

By JON RONSON FEB. 12, 2015



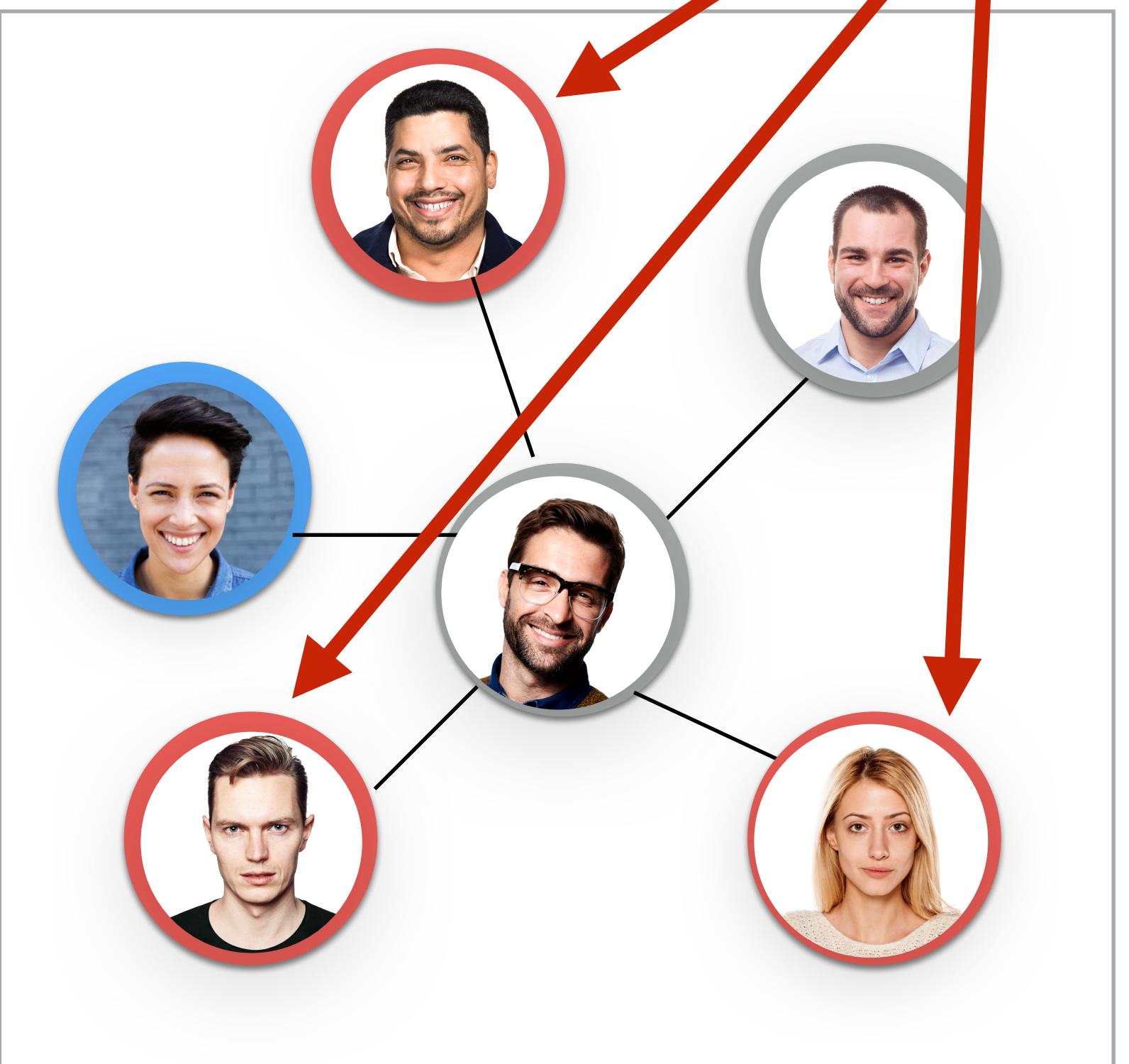
**And negative press is
an attack on your
social network**

Call this a social network supply chain
disruption.



Pseudonymity defends against social supply chain disruptions

There are others, like maximizing personal runway / financial independence, or maintaining multiple options for each supply chain node.



before



after



is now bad

What is pseudonymity?

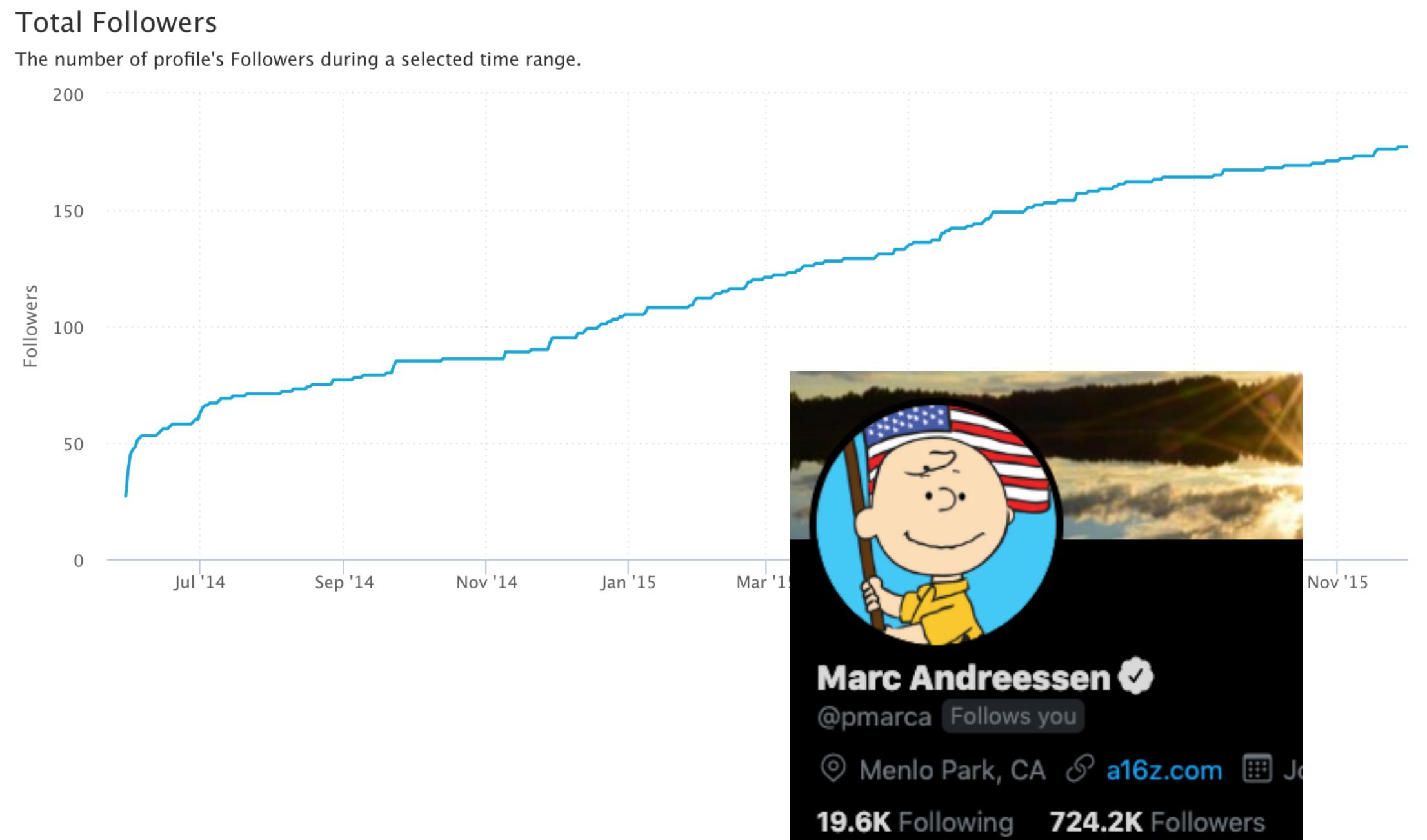
Why a pseudonymous economy?

How might it work?

How could we build it?

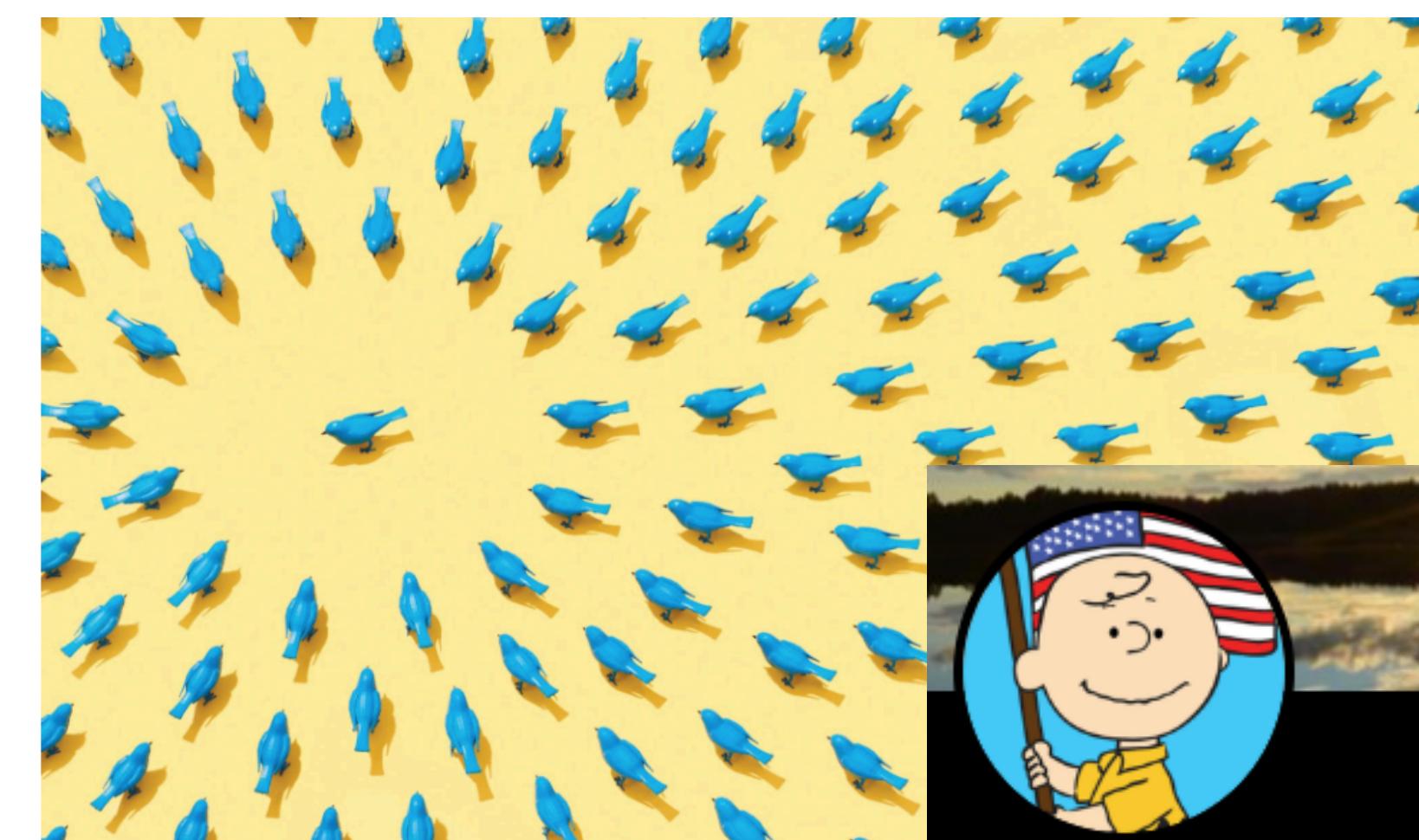
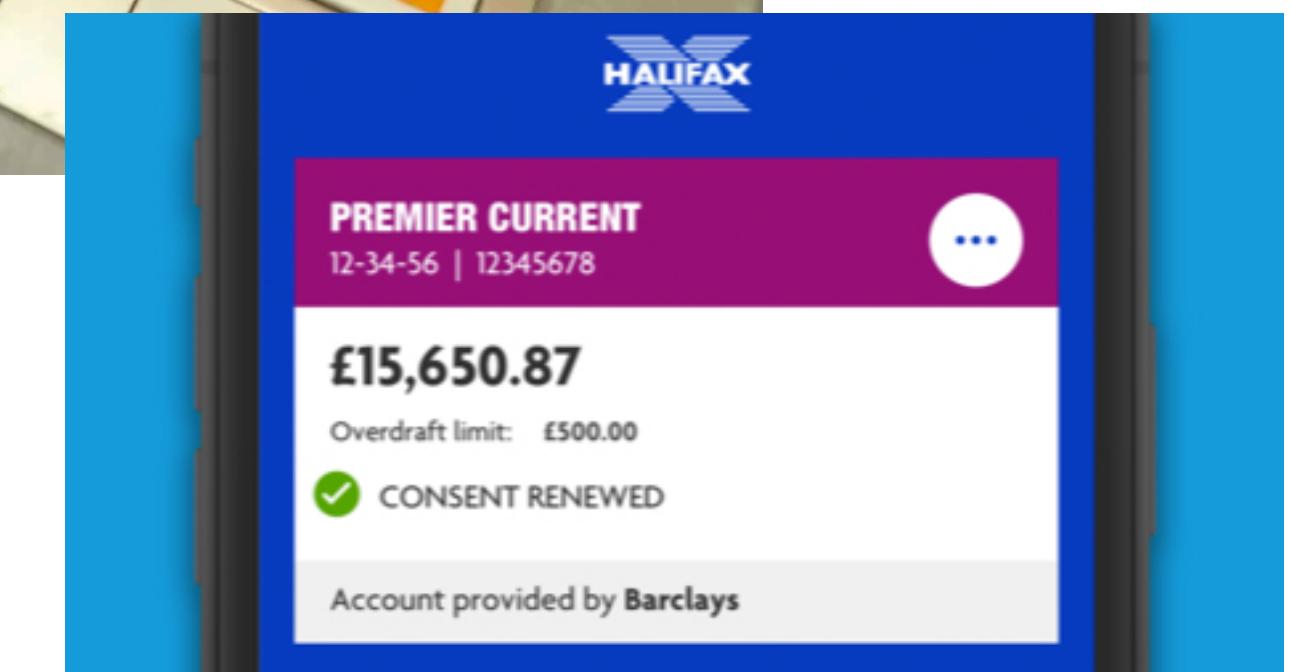
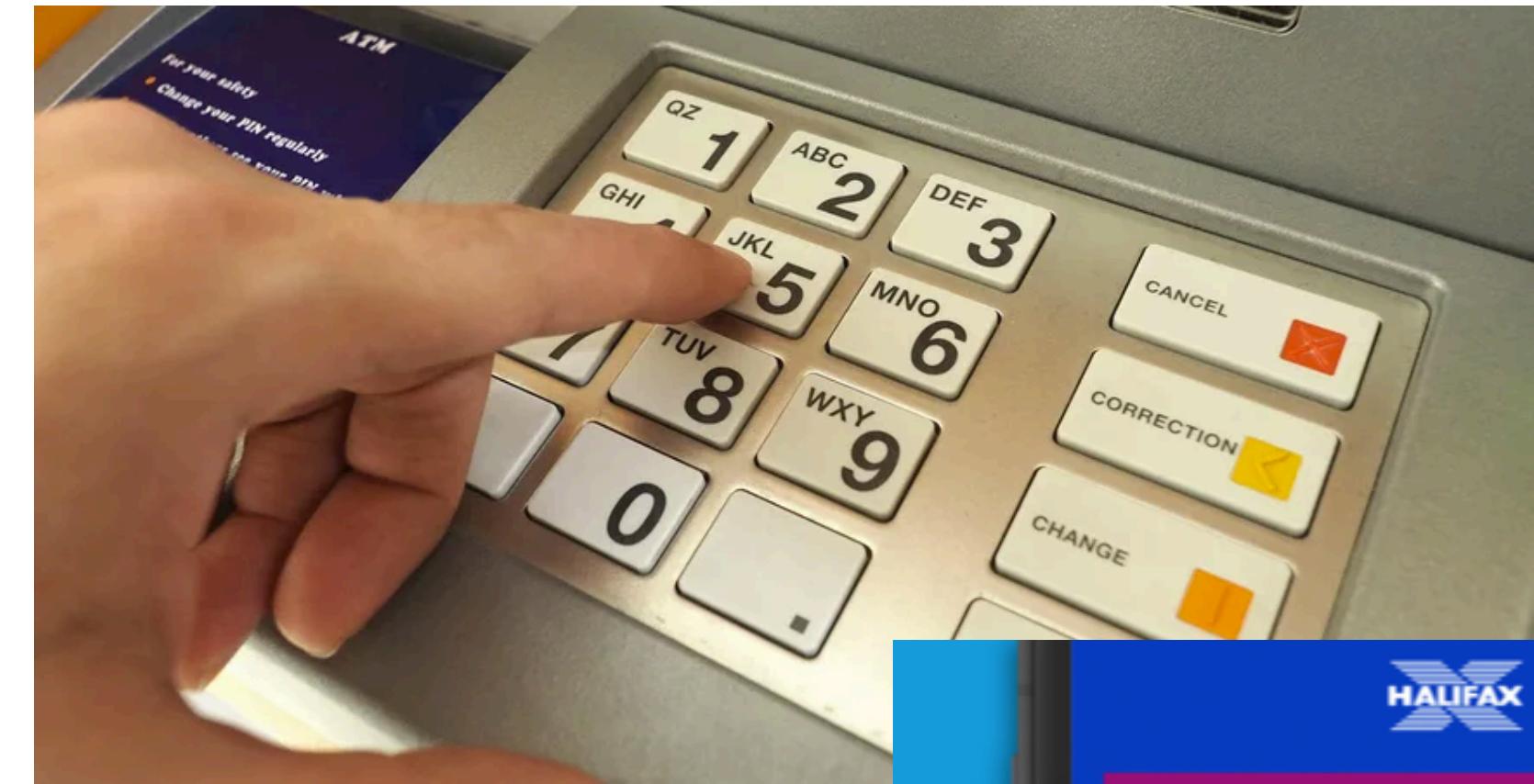
Your bank account is stored wealth. Your real name is stored reputation.

Just like you increase your bank balance over time, you increase reputation over time. One quantifiable dimension of this is social media.



Only you can debit your bank account. Anyone can debit your reputation.

You need an authorization to send money, but a social mob can debit reputation without recourse.



Separate your earning, speaking, and real names

Every problem in computer science can be solved with another level of indirection. Like AWS bastions or HD wallets.



Earning



Tristan Su
foobar

📍 China
✉️ Sign in to view email
🔗 http://foobar.github.io



Zcash

Speaking



Comfortably Smug

@ComfortablySmug

My Interests: Finance, Whiskey, Politics, Books, Food, Meeting Strangers
#altcenter

"Real" name

Customs Declaration

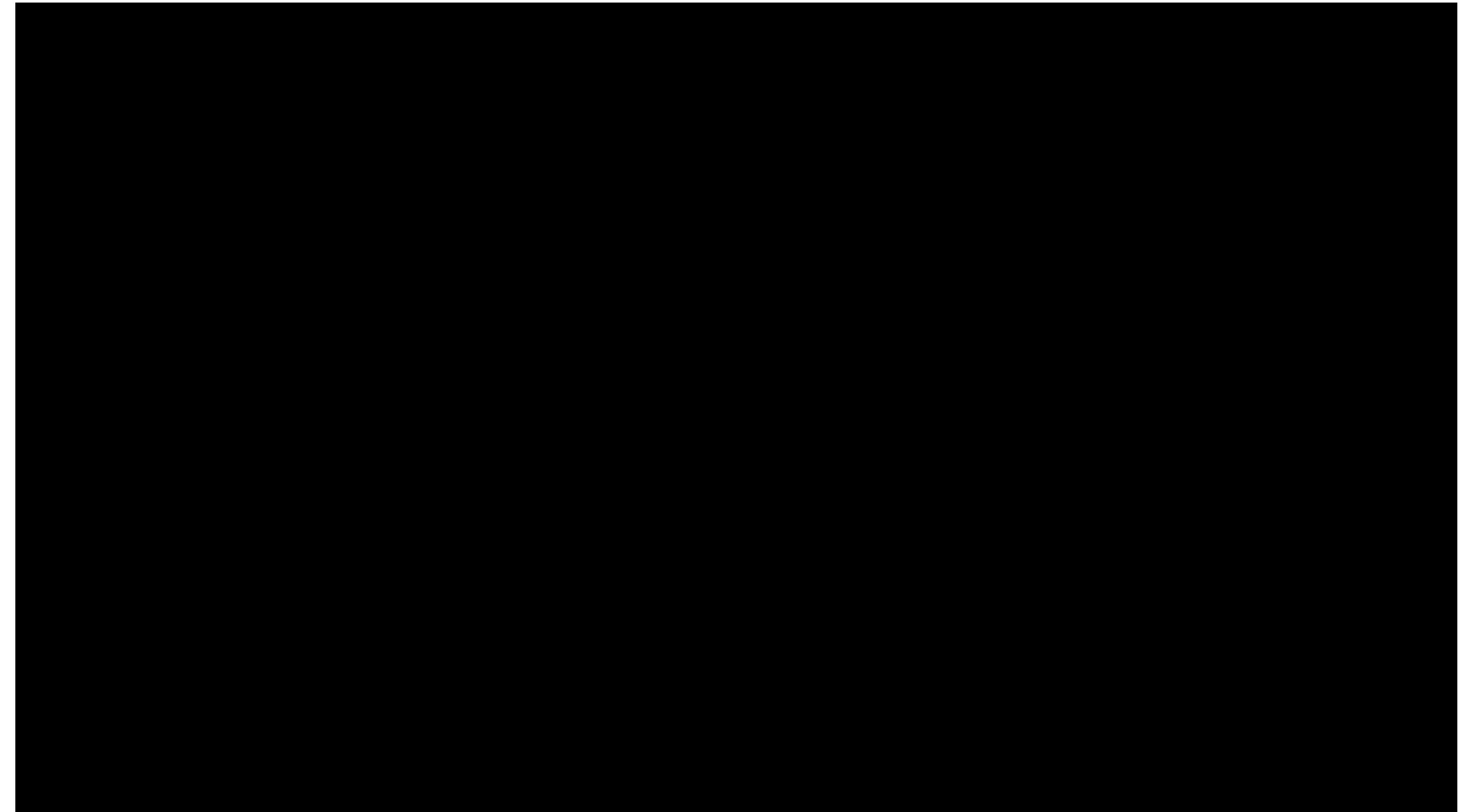
FORM APPROVED
19 CFR 122.27, 148.12, 148.13, 148.150, 148.111, 1488.21 CFR 83.16
OMB NO. HHS-0099

Each arriving traveler or responsible family member must provide the following information (only ONE written declaration per family is required). The term "Family" is defined as "members of a family residing in the same household who are related by blood, marriage, domestic relationship, or adoption."

1 Family Name
First (Given) Middle

Use VR & AI Avatars for all remote interactions

Zoom is today. But by 2030, you may not use your real face, voice, language, or accent online.



#GameTrailers #Gaming #MetaHuman

Epic Games' MetaHuman Creator Character Demo

11,248 views • Feb 10, 2021

1362

22



SHARE



SAVE

...

Crypto domain names > real names

Start using yourname.eth and then asdf93.eth in all contexts where you'd normally use a legal/fiat/official/state name.

balajis.com ✅ @balajis · Dec 15, 2020
Real names weren't built for the internet.

balajis.com ✅ @balajis · Dec 15, 2020
Real names give both too much information & too little. They allow people to index and stalk you in countless bizarre ways.

But they also aren't built for attaching metadata, like DNS is. You can't pay someone's name directly, for example.

All that changes with tools like ENS.

Replying to [@balajis](#)

See this thread for details. In short, crypto domains like ENS and HNS collapse concepts from usernames, domain names, real names, payment handles, login mechanisms, and more into one thing.

balajis.com ✅ @balajis · Aug 4, 2020
Suppose we combine the following:

- pseudonym
- domain name
- decentralized DNS (ENS, HNS, etc)
- HD wallet

So your karma & balance are at yourpseudonym.eth. In the event a particular pseudonym is deprecated, you can move it privately to another in the HD wallet tree. [twitter.com/balajis/status...](#)

[Show this thread](#)

3:12 AM · Dec 15, 2020 · Twitter for iPhone

8 Retweets 3 Quote Tweets 103 Likes

But there's one problem.

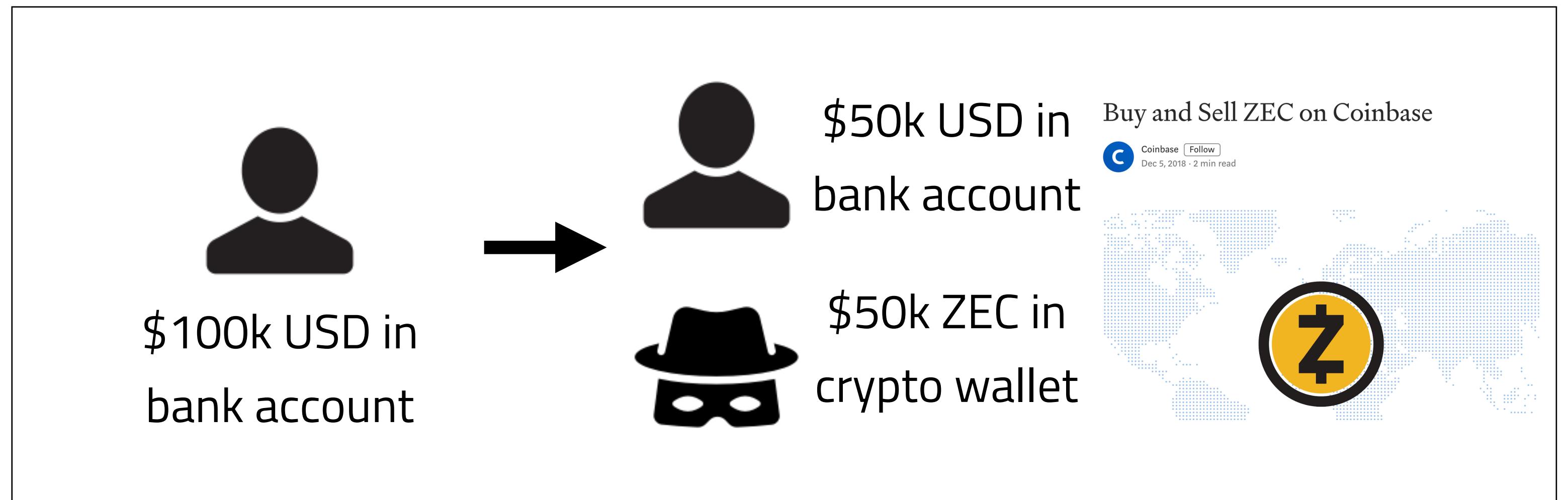
How do you boot up a new pseudonym efficiently?

What is pseudonymity?

Why a pseudonymous economy?

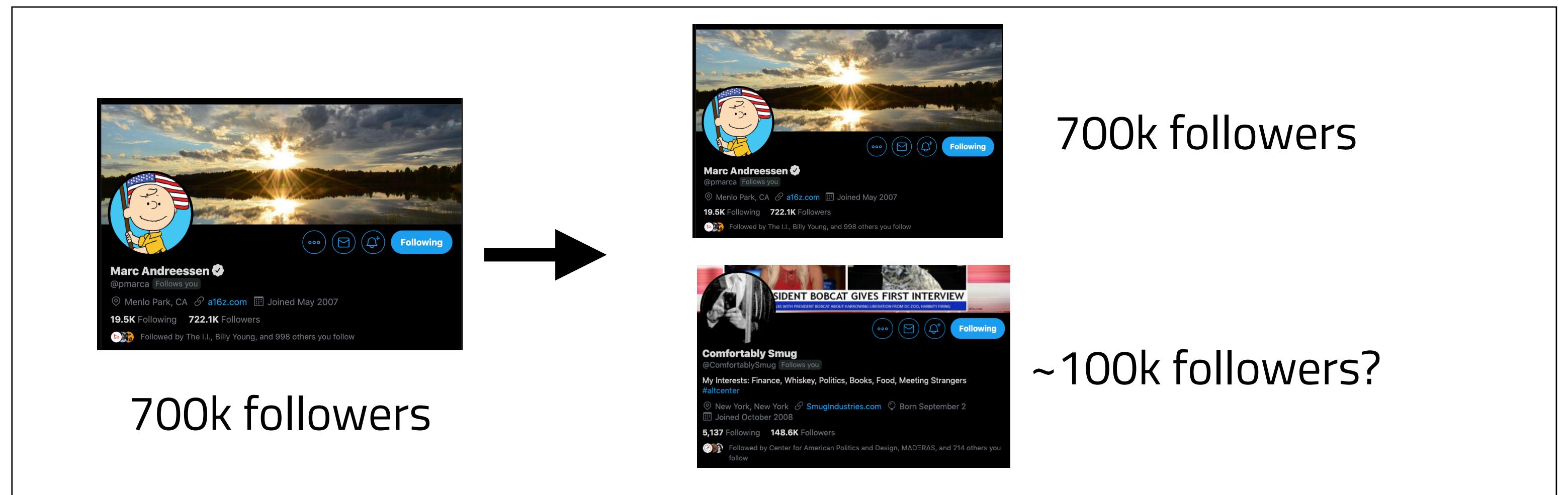
How might it work?

How could we build it?



**We can move wealth
to a pseudonym.
Can we move
reputation too?**

If so, we could one-click set up a new pseudonym.



Transfer reputation to a pseudonym?

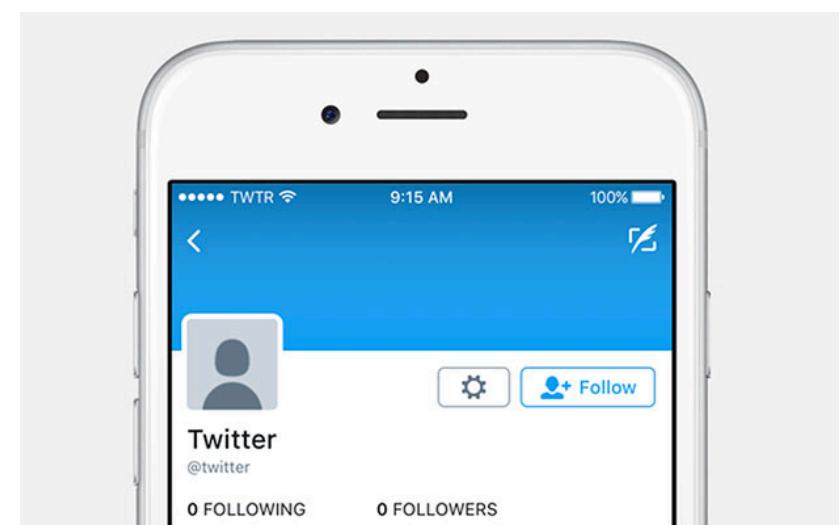
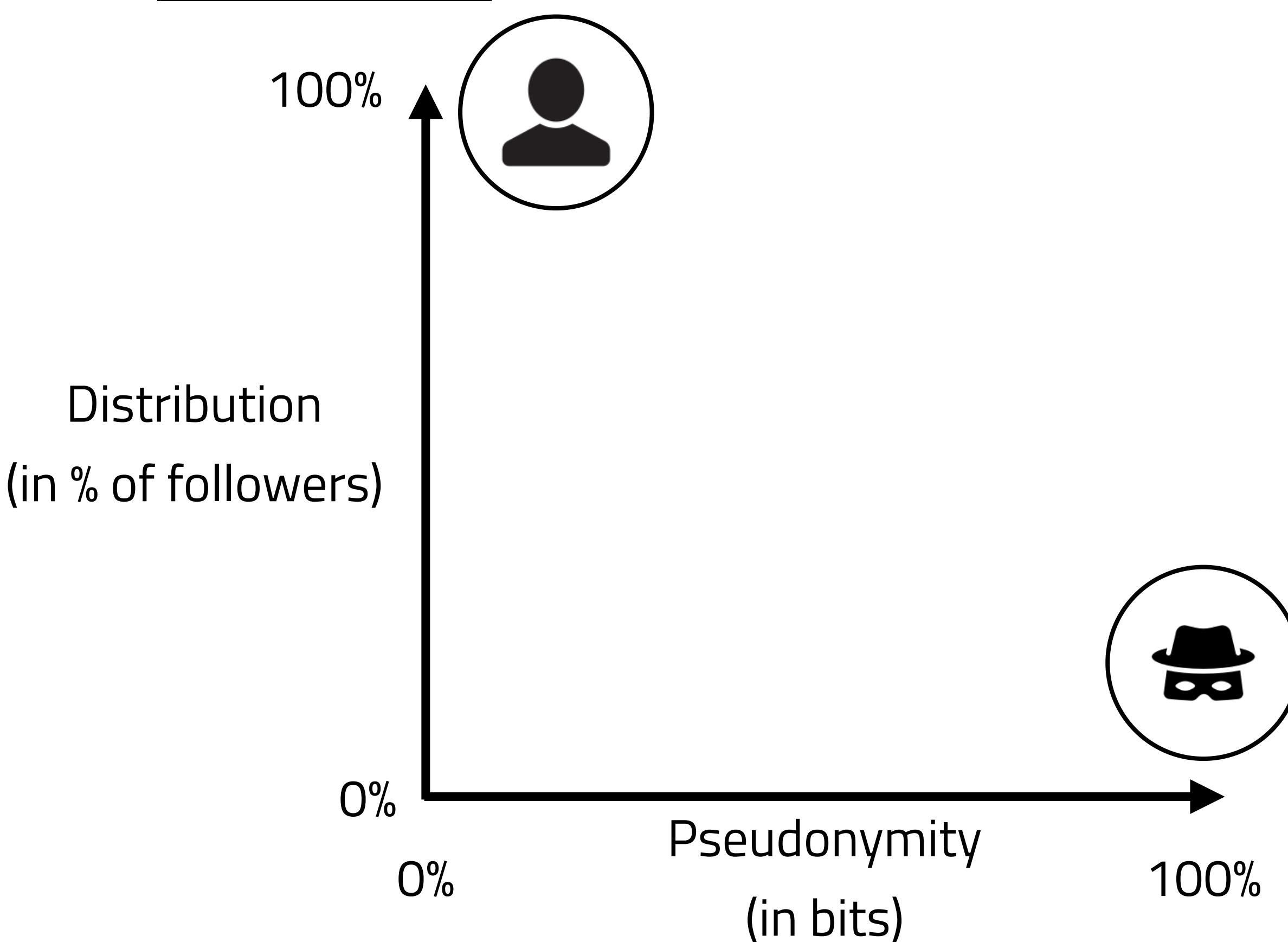
Let's take the special case of Twitter.

We can now decentralize much of the Twitter backend. So this is more feasible.



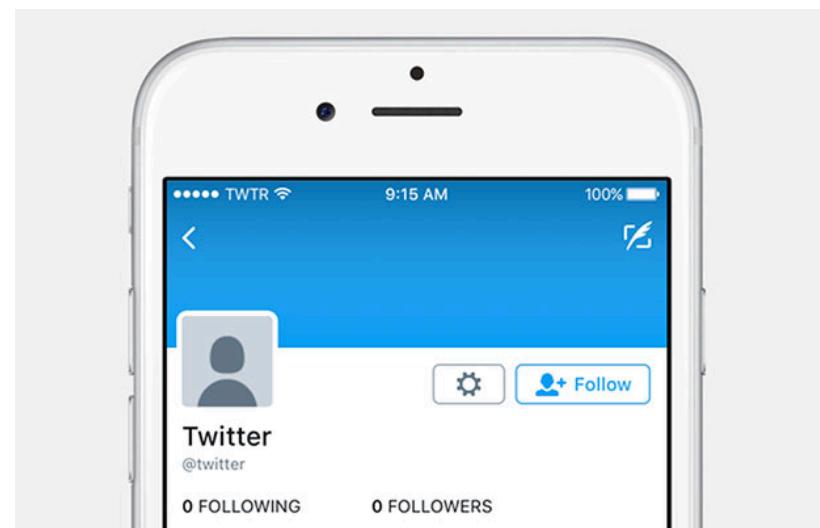
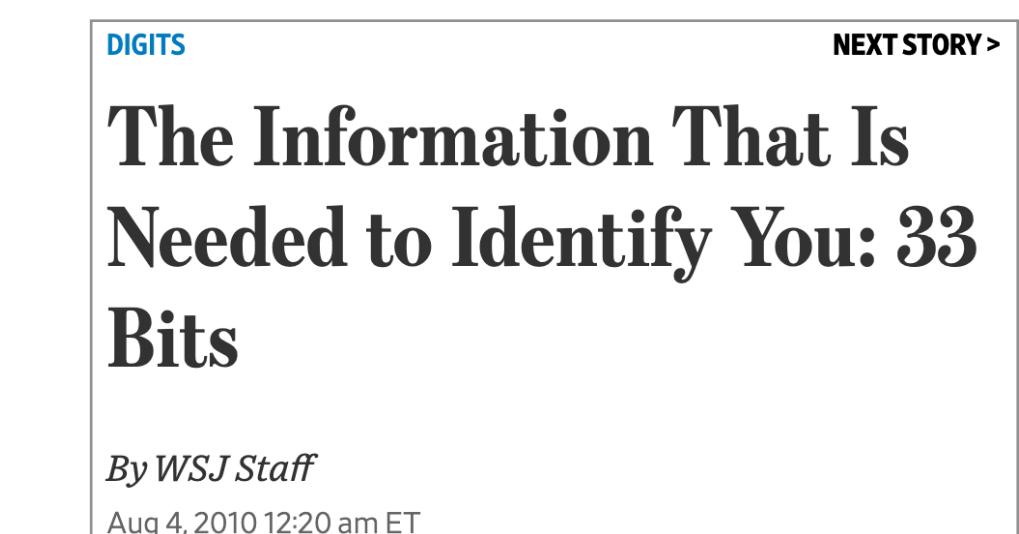
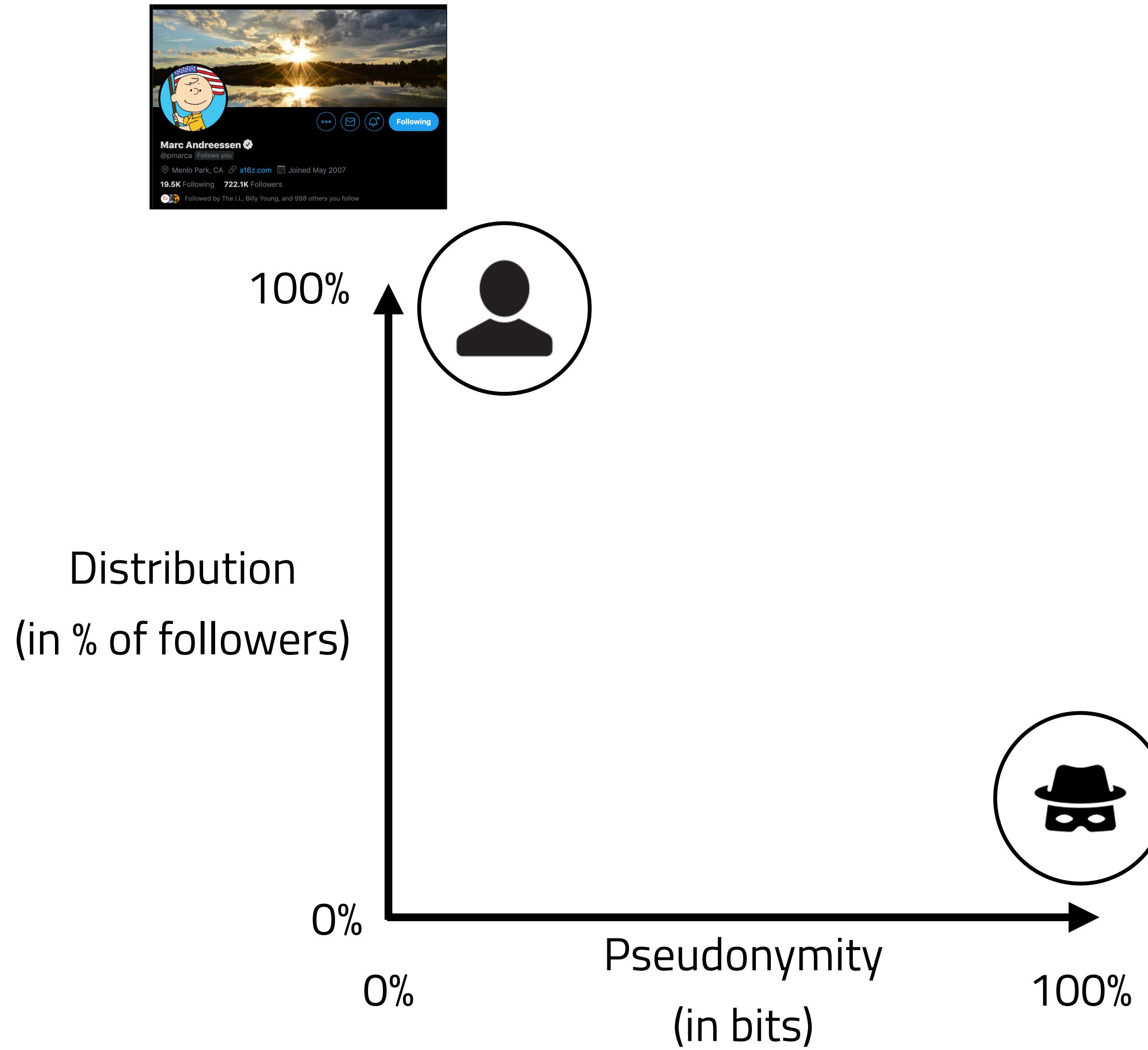
**Right now only two choices:
100/0 or 0/100.**

All your distribution and no pseudonymity, or
vice versa.



Right now only two choices: 100/0 or 0/100.

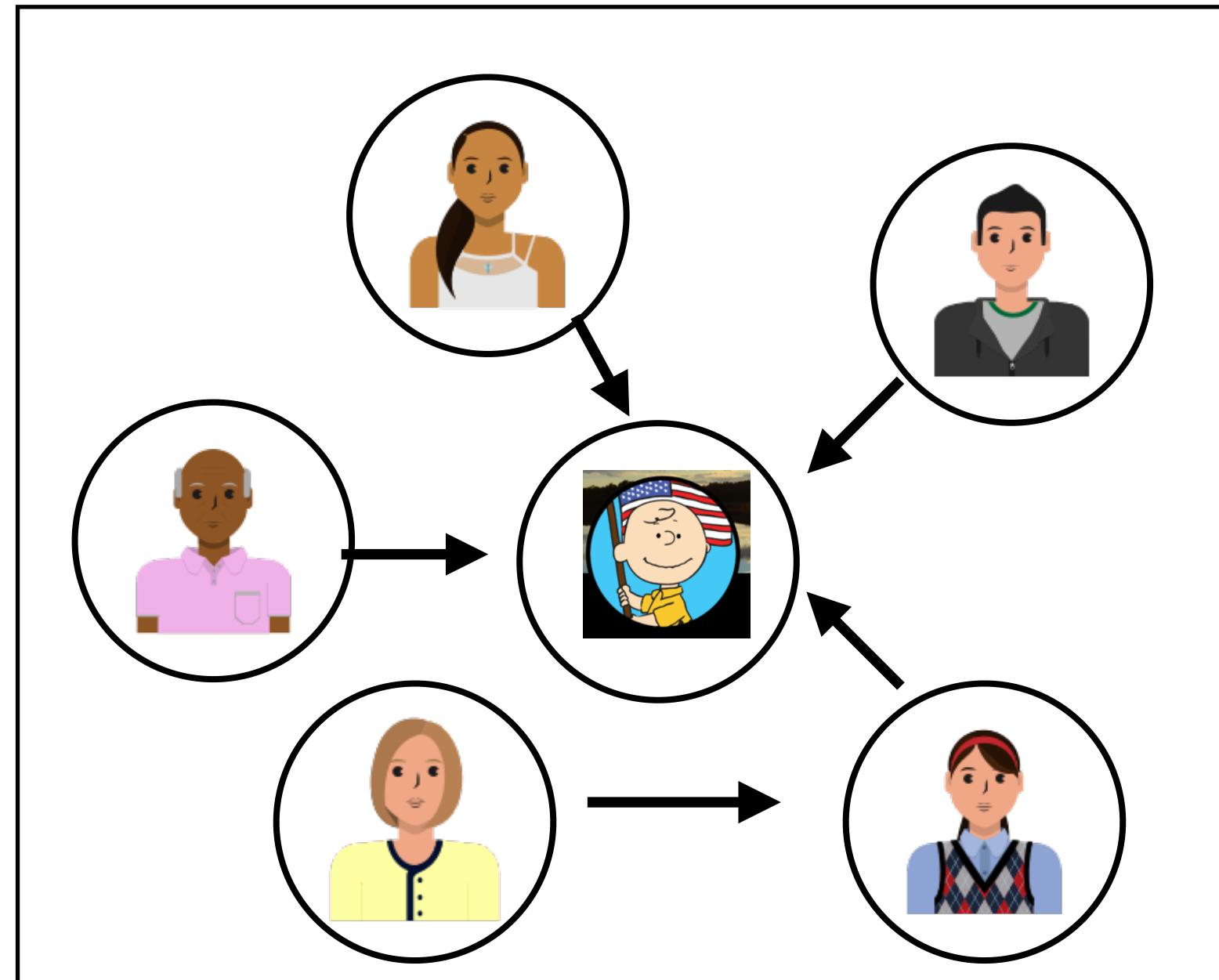
All your distribution and no pseudonymity, or vice versa.



Can we trade off some pseudonymity for some distribution?

Naive approach: transfer all followers

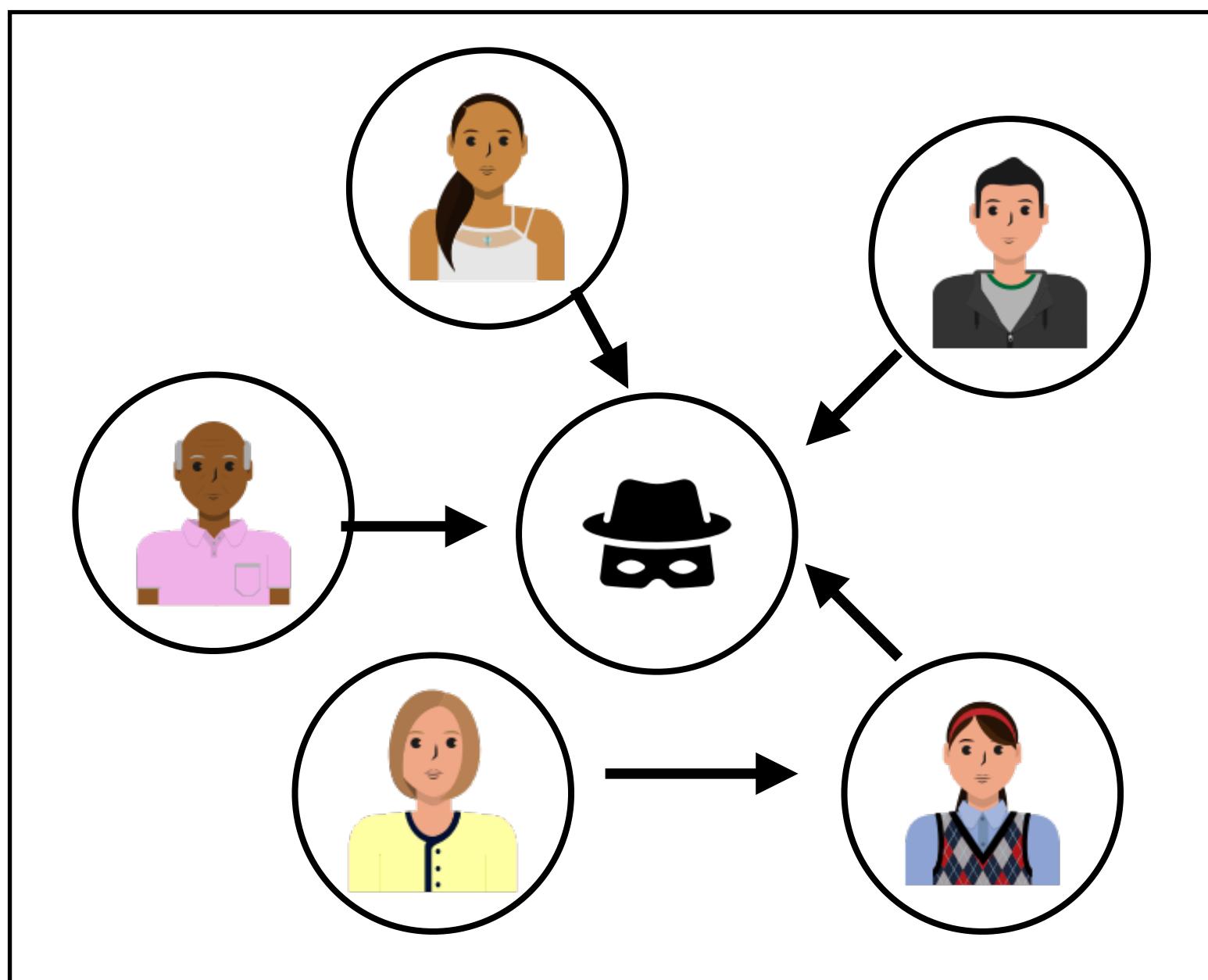
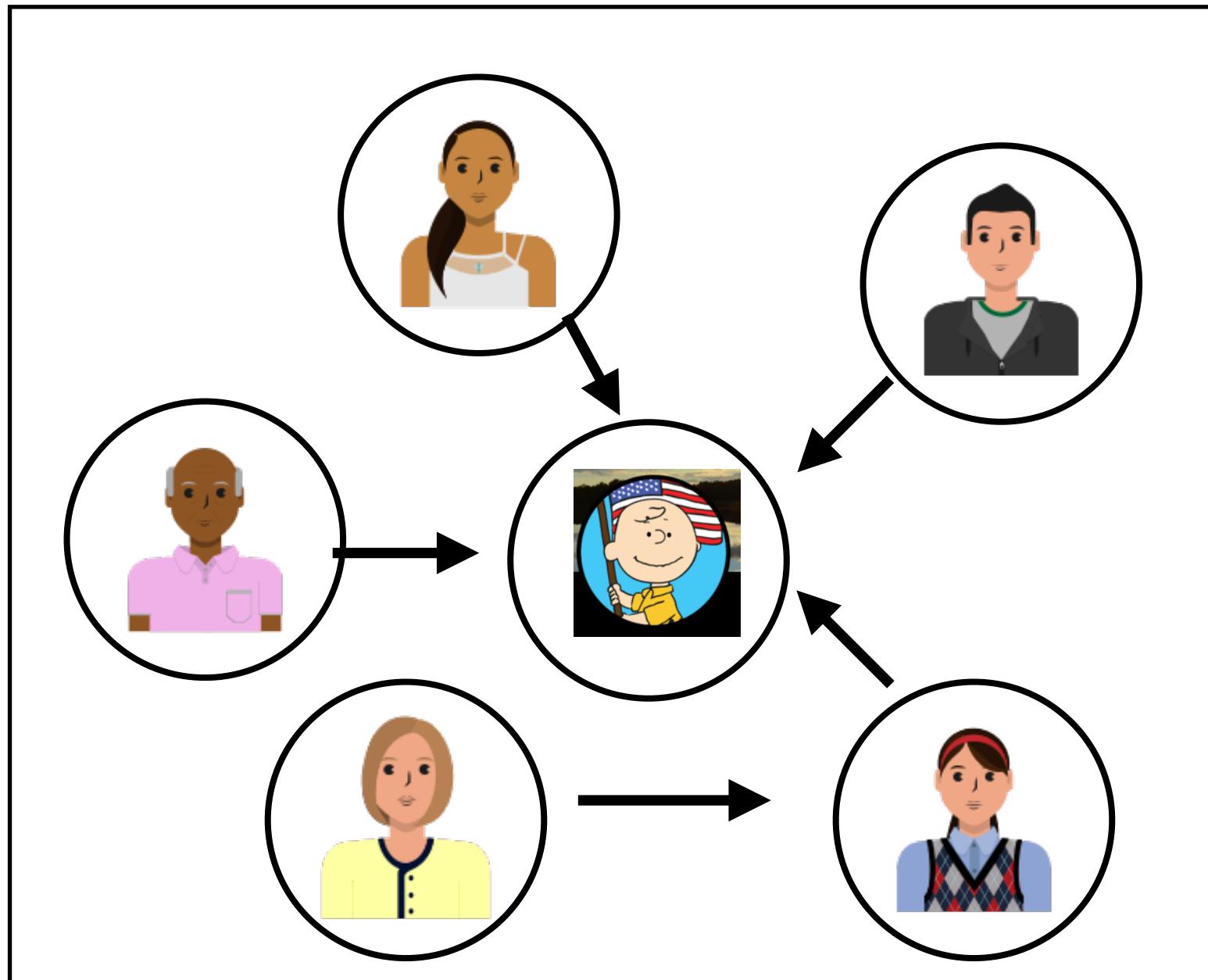
Suppose we just set up a new Twitter pseudonym and transfer all followers to that pseudonym.



0	1	1	0	1	1
0	0	0	0	0	0
0	0	0	1	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

Naive approach: transfer all followers

Suppose we just set up a new Twitter pseudonym and transfer all followers to that pseudonym.

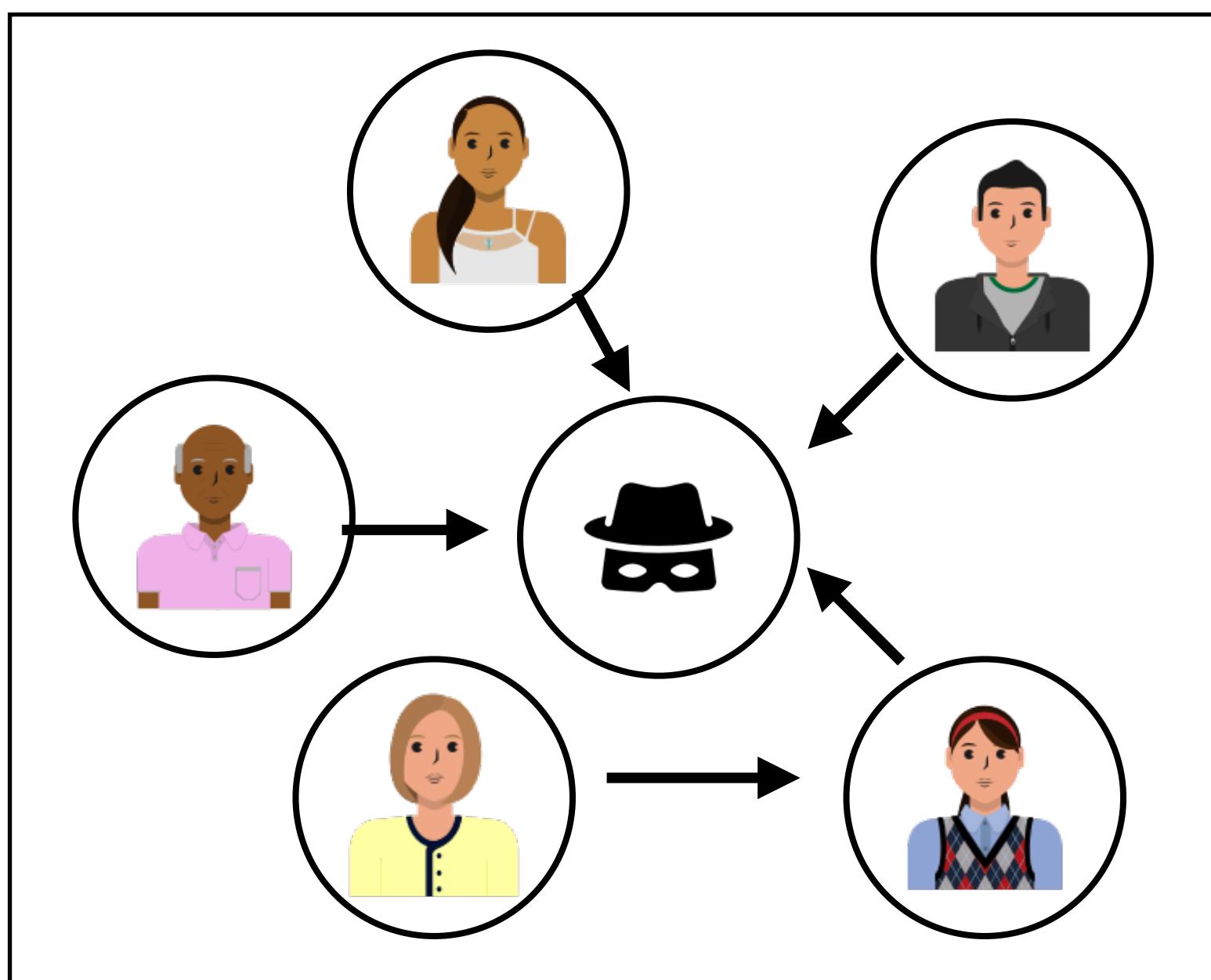
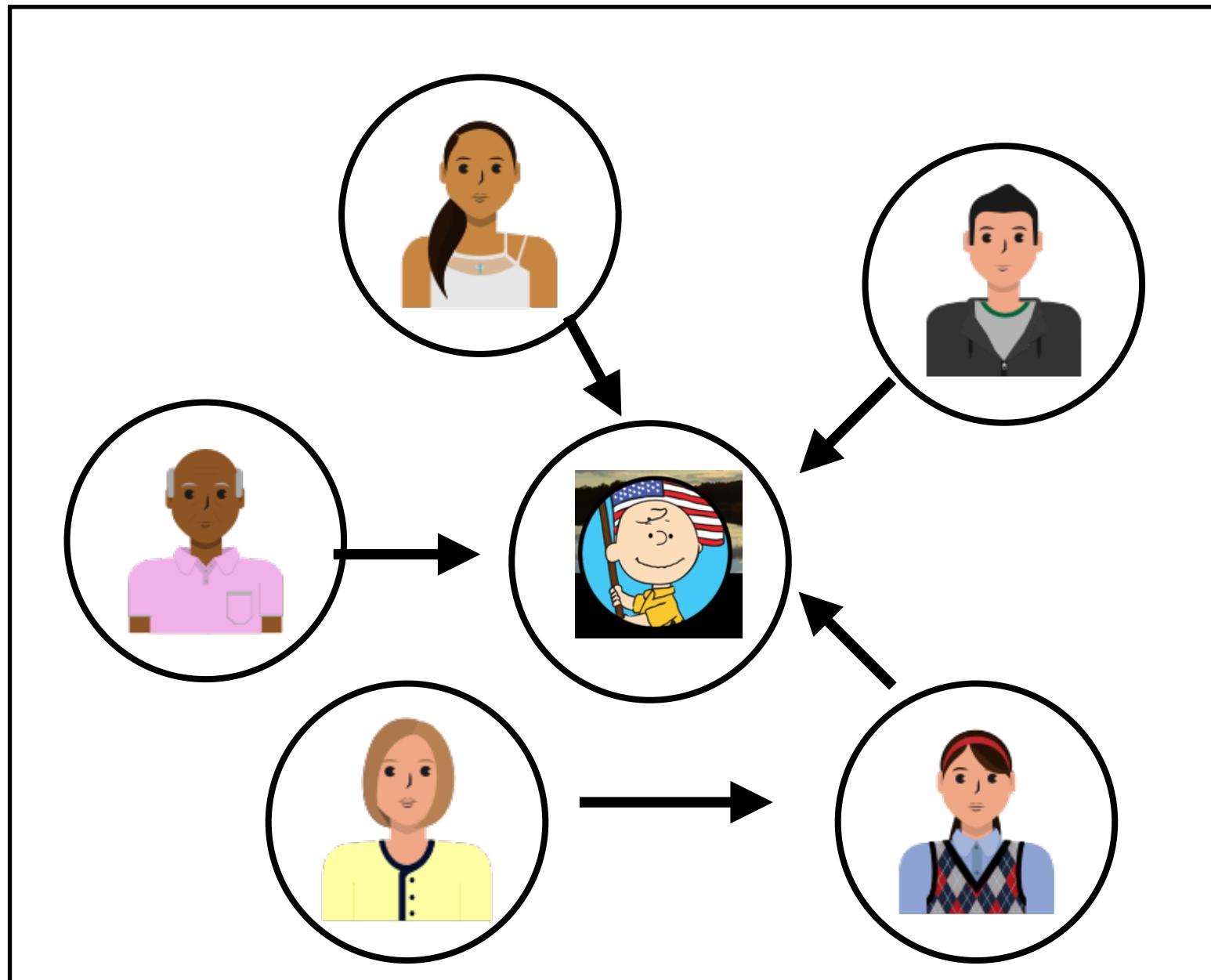


0	1	1	0	1	1
0	0	0	0	0	0
0	0	0	1	0	0
0	0	0	0	0	0
0	0	0	0	0	0
0	0	0	0	0	0

The table illustrates the follower matrix. The columns represent the original users and the rows represent the new pseudonym. A value of 1 indicates that a user is a follower of the pseudonym, while 0 indicates they are not. In the first row, User 1 is a follower (value 1). In the second row, User 2 is a follower (value 1). In the third row, User 3 is a follower (value 1). In the fourth row, User 4 is a follower (value 0). In the fifth row, User 5 is a follower (value 1). In the sixth row, User 6 is a follower (value 1).

Naive approach: transfer all followers

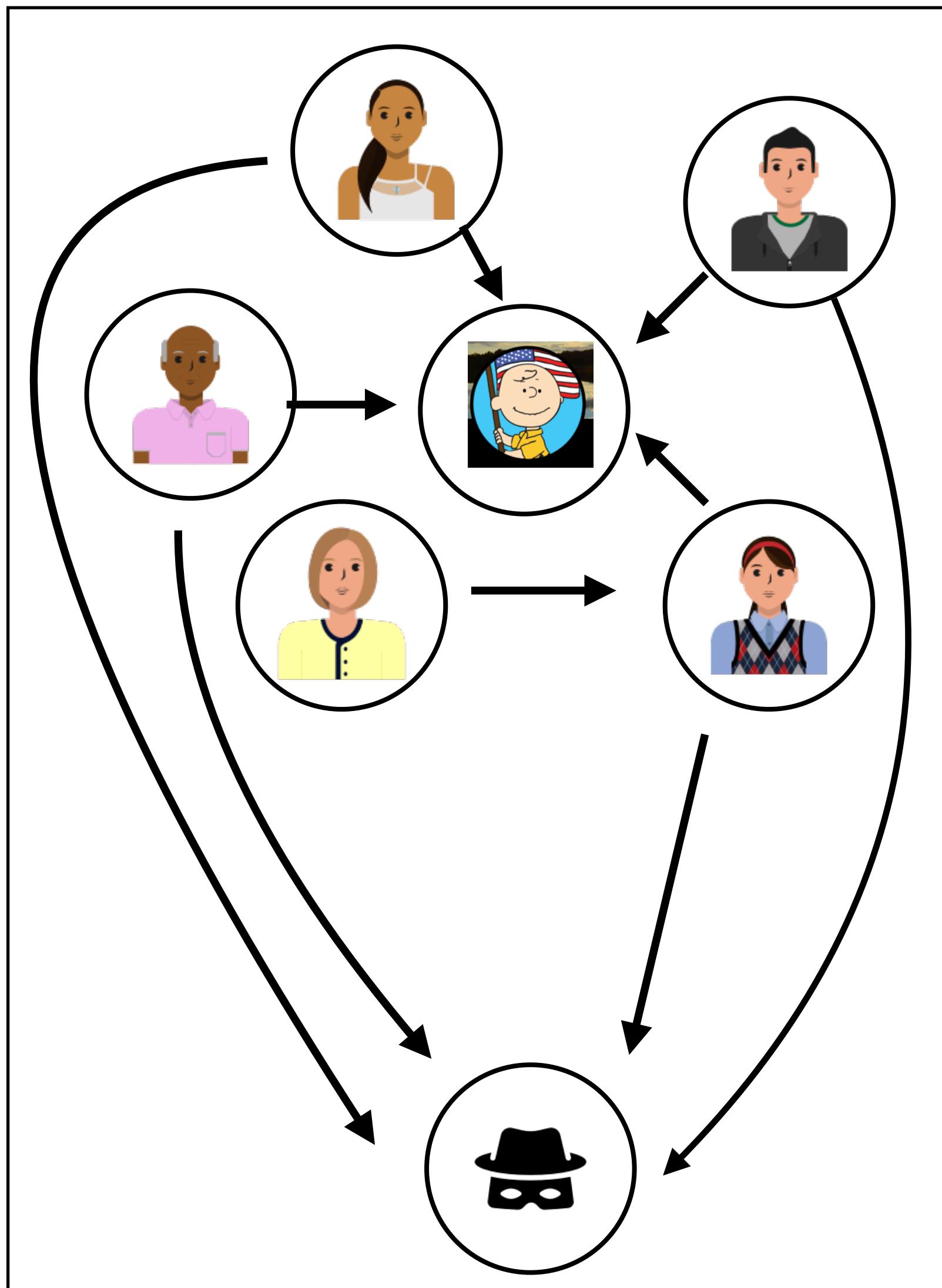
Suppose we just set up a new Twitter pseudonym and transfer all followers to that pseudonym.



0	1	1	0	1	1	0	0
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	1	1	0	1	1	1	0

Naive approach: transfer all followers

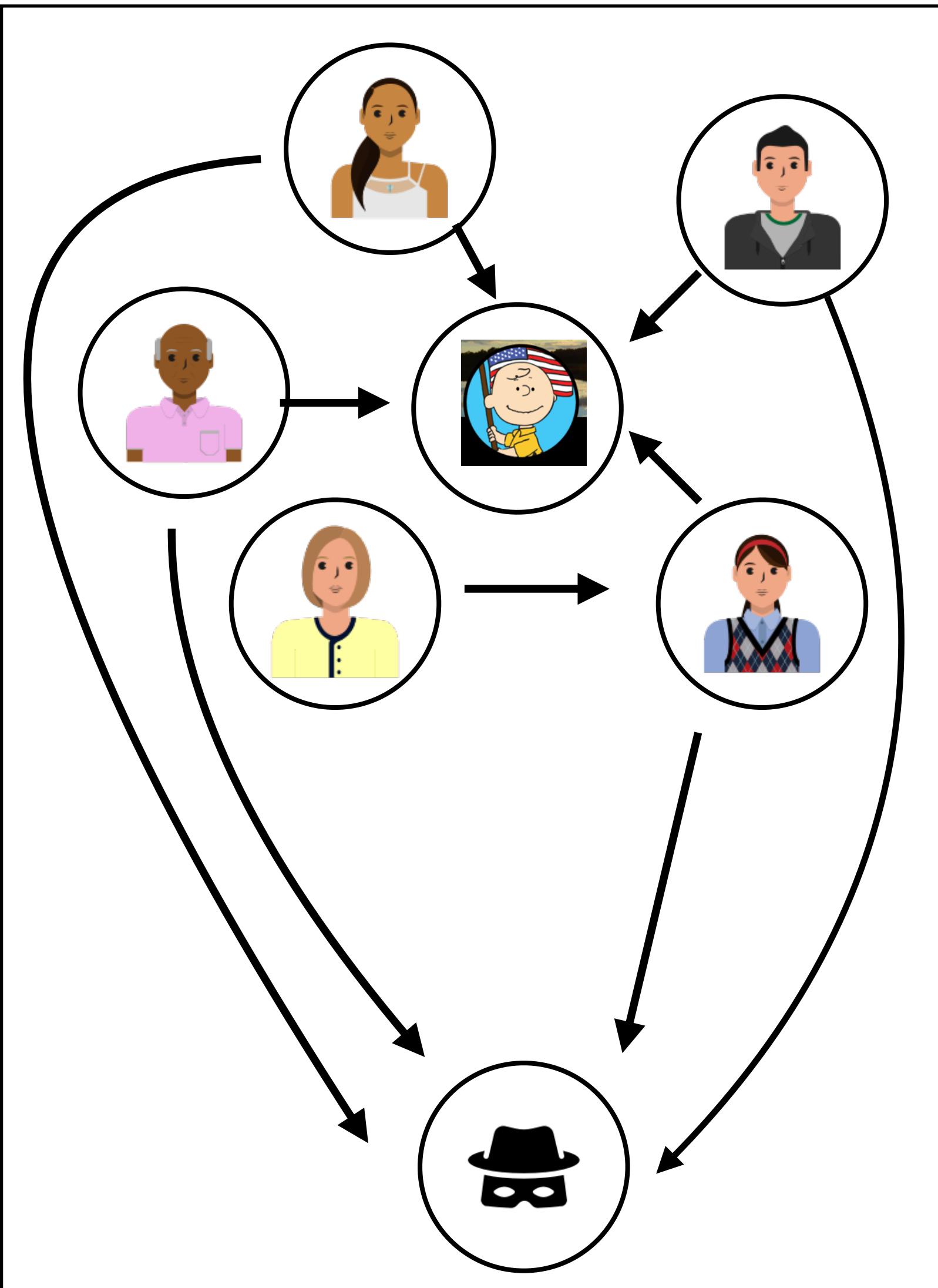
Suppose we just set up a new Twitter pseudonym and transfer all followers to that pseudonym.



0	1	1	0	1	1	0
0	0	0	0	0	0	0
0	0	0	1	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	0	0	0	0	0	0
0	1	1	0	1	1	0

Naive approach: transfer all followers

Suppose we just set up a new Twitter pseudonym and transfer all followers to that pseudonym.



1 out of 1

$\log_2(1) = 0$ bits of anonymity

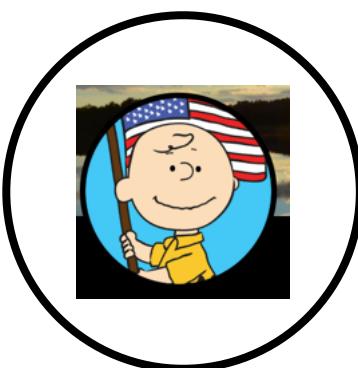
0	1	1	0	1	1	0	
0	0	0	0	0	0	0	
0	0	0	1	0	0	0	
0	0	0	0	0	0	0	
0	0	0	0	0	0	0	
0	0	0	0	0	0	0	
0	1	1	0	1	1	0	

Concept: what if we transfer *attestations* rather than everything?

Better approach: use ZK to transfer some info

What if we only transferred some info to the pseudonym, like whether the user was verified?

User profile data

Platform	Verification
	

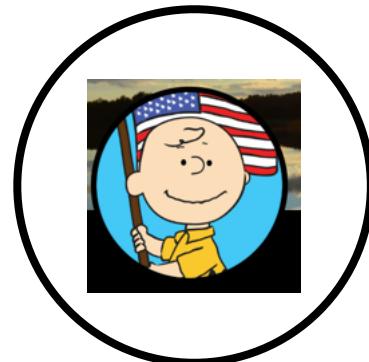


Better approach: use ZK to transfer some info

What if we only transferred some info to the pseudonym, like whether the user was verified?

User profile data

Platform	Verification
User	Name, location, bio



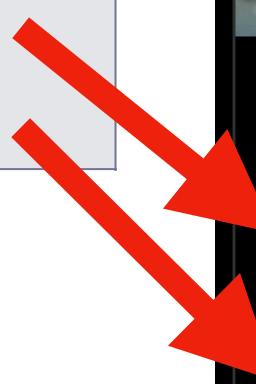
Marc Andreessen

@pmarca Follows you

Menlo Park, CA a16z.com Joined May 2007

19.5K Following 722.1K Followers

Followed by The I.I., Billy Young, and 998 others you follow

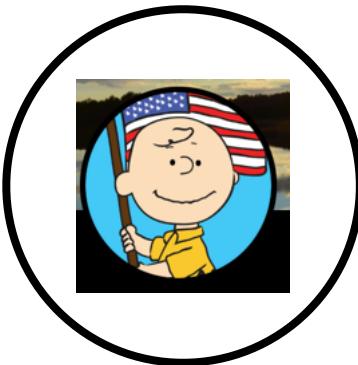


Better approach: use ZK to transfer some info

What if we only transferred some info to the pseudonym, like whether the user was verified?

User profile data

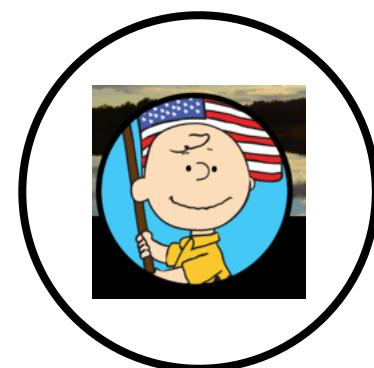
Platform	Verification
User	Name, location, bio
Others	Followers, likes, RTs



Better approach: use ZK to transfer some info

What if we only transferred some info to the pseudonym, like whether the user was verified?

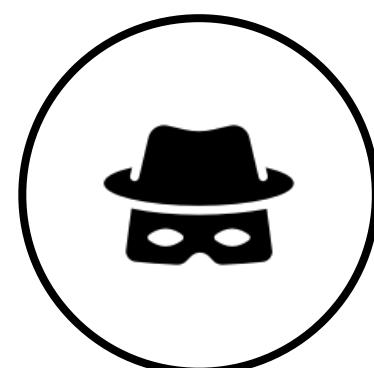
User profile data



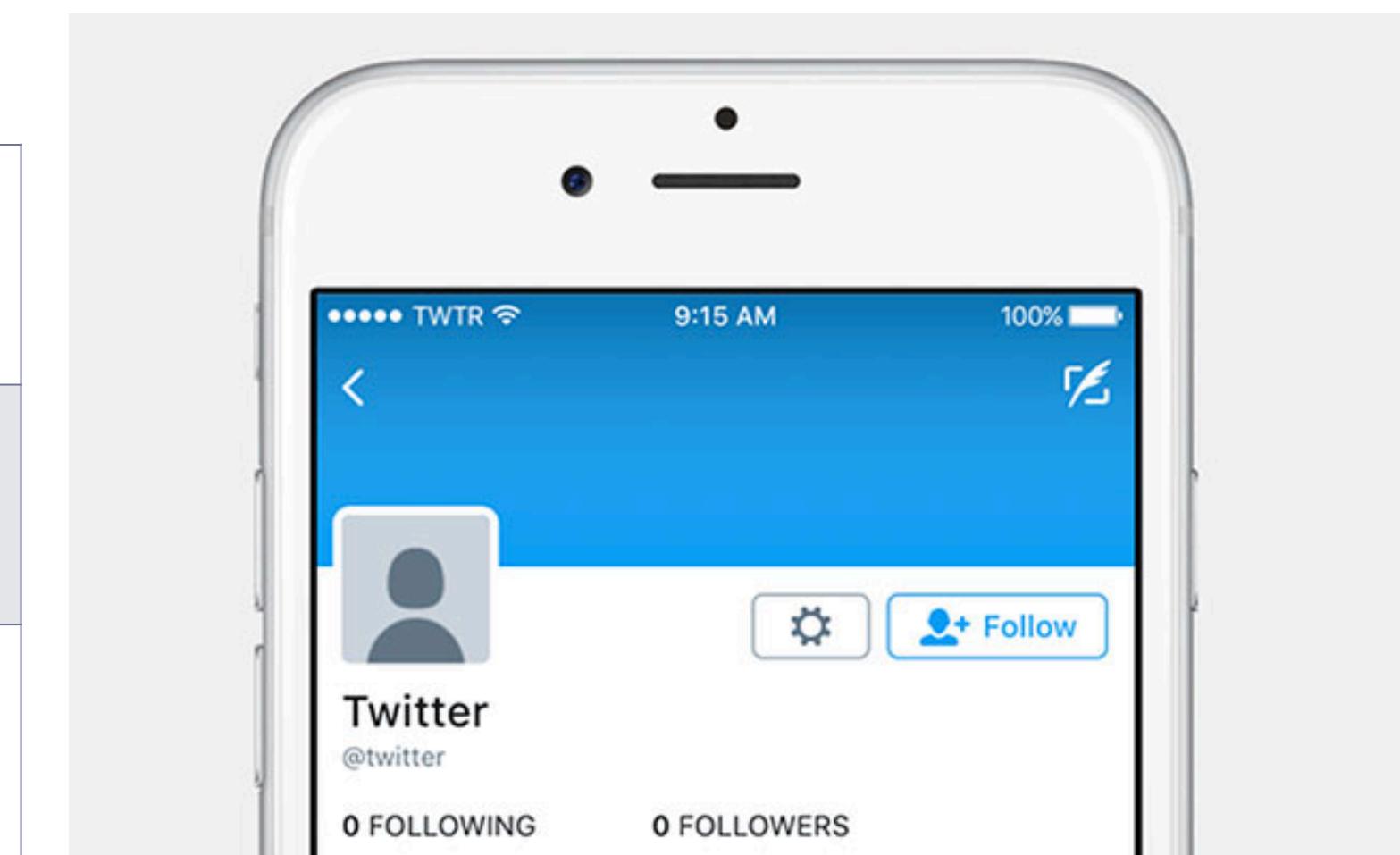
Platform	Verification
User	Name, location, bio
Others	Followers, likes, RTs



Via a zero knowledge construction
(like ZK Snarks for ZEC transfer)



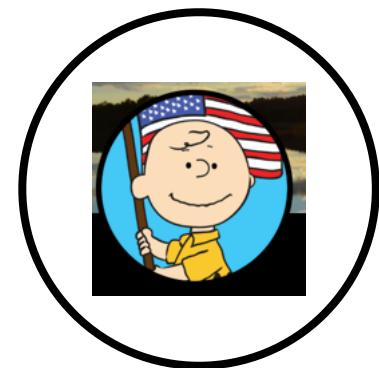
Platform	-
User	-
Others	-



Better approach: use ZK to transfer some info

What if we only transferred some info to the pseudonym, like whether the user was verified?

User profile data



Platform	Verification
User	Name, location, bio
Others	Followers, likes, RTs

Via a zero knowledge construction
(like ZK Snarks for ZEC transfer)

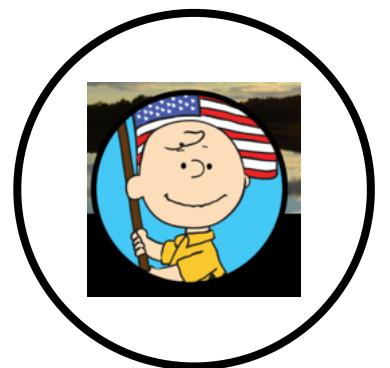


Platform	Verification
User	-
Others	-



Making progress!

Given 300e6 users & 300e3 verifieds, giving up a *quantifiable* amount of anonymity for rep.



Platform	Verification
User	Name, location, bio
Others	Followers, likes, RTs

1 out of 1
 $\log_2(1) = 0$ bits of anonymity



Platform	-
User	-
Others	-

1 out of 330M MAUs
 $\log_2(330M) = 28.3$ bits anonymity



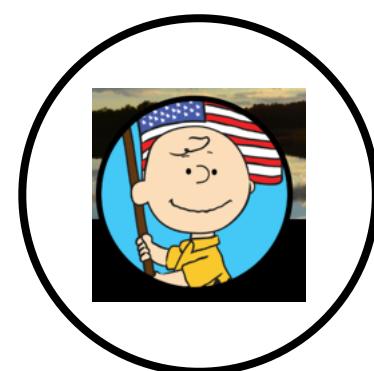
Platform	Verification
User	-
Others	-

1 out of 330K Verifieds
 $\log_2(330K) = 18.3$ bits anonymity

= **-10 bits of anonymity** to port a verification to this profile

And we could port over multiple attestations

Each one gives some reduction in anonymity.

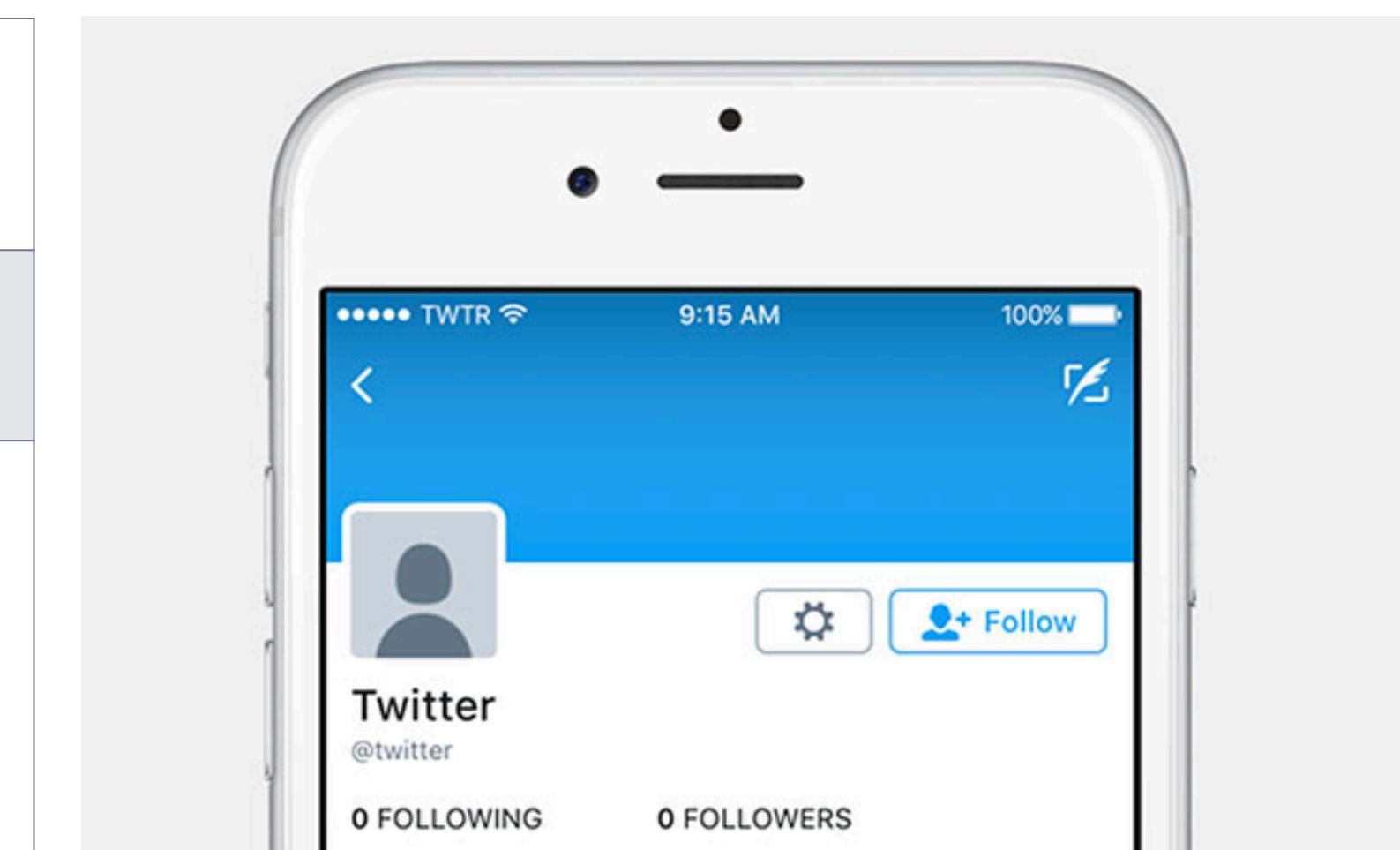


Platform	Verification
User	Name, location, bio
Others	Followers, likes, RTs

Via a zero knowledge construction
(like ZK Snarks for ZEC transfer)



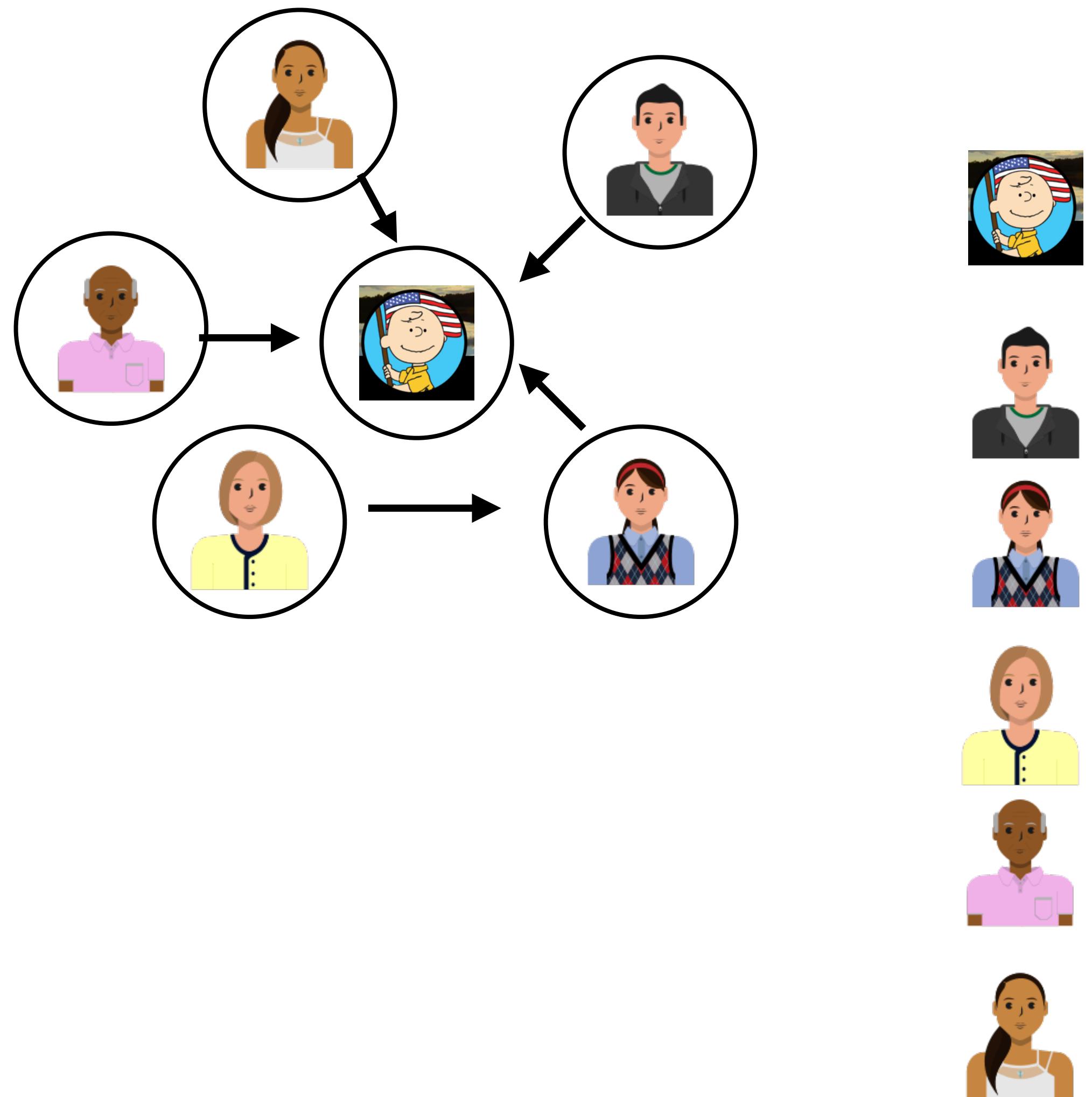
Platform	Verification
User	
Others	>100k followers, followed by @jack, etc



But how do we ensure folks still follow?

What about reputation? Autofollow.

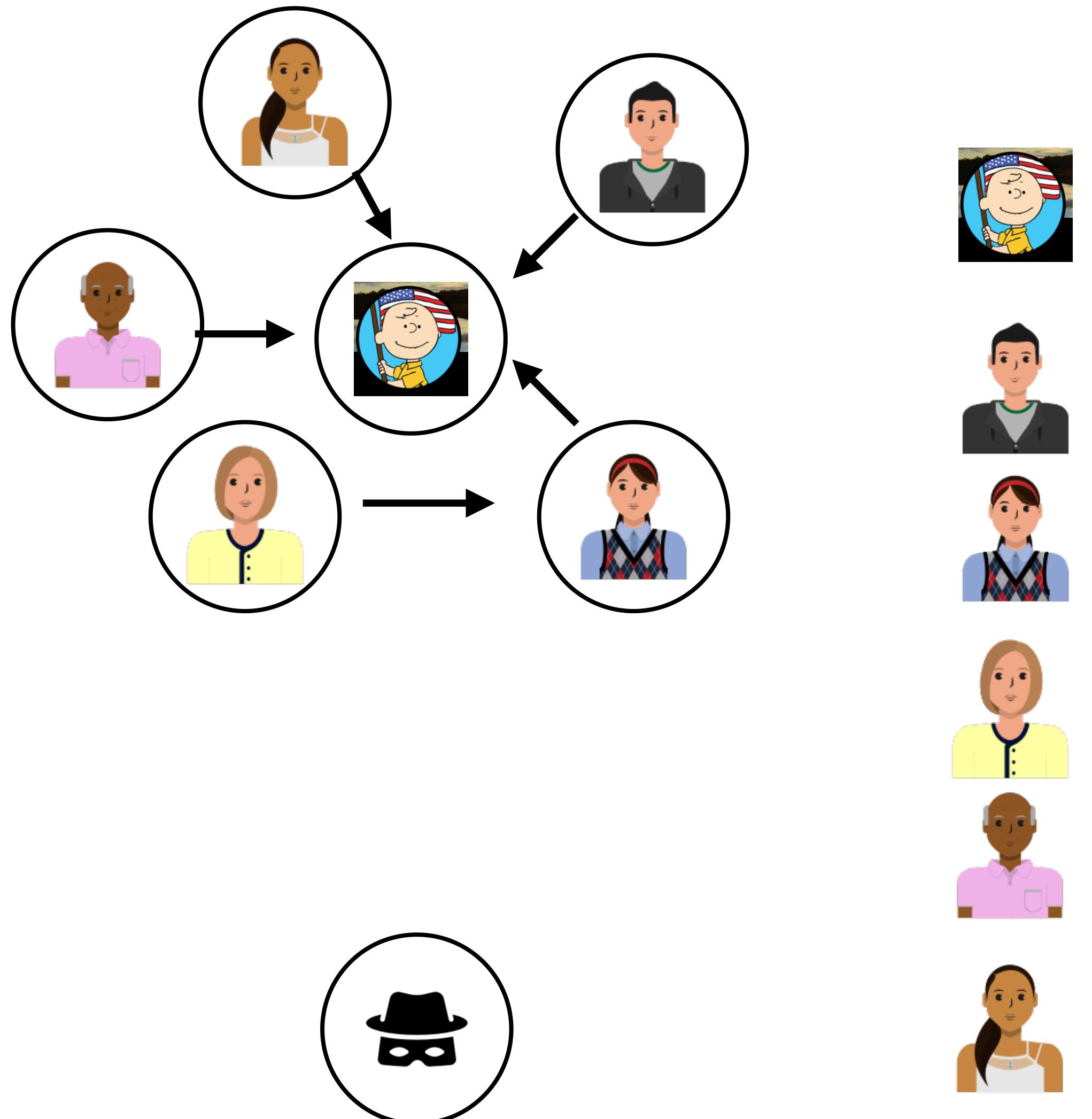
One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.



Autofollow if verified?	Autofollow if >10k followers?	Autofollow if @jack follows?
0	1	1
1	0	1
1	0	1
1	1	1
0	1	0
0	1	1

What about reputation? Autofollow.

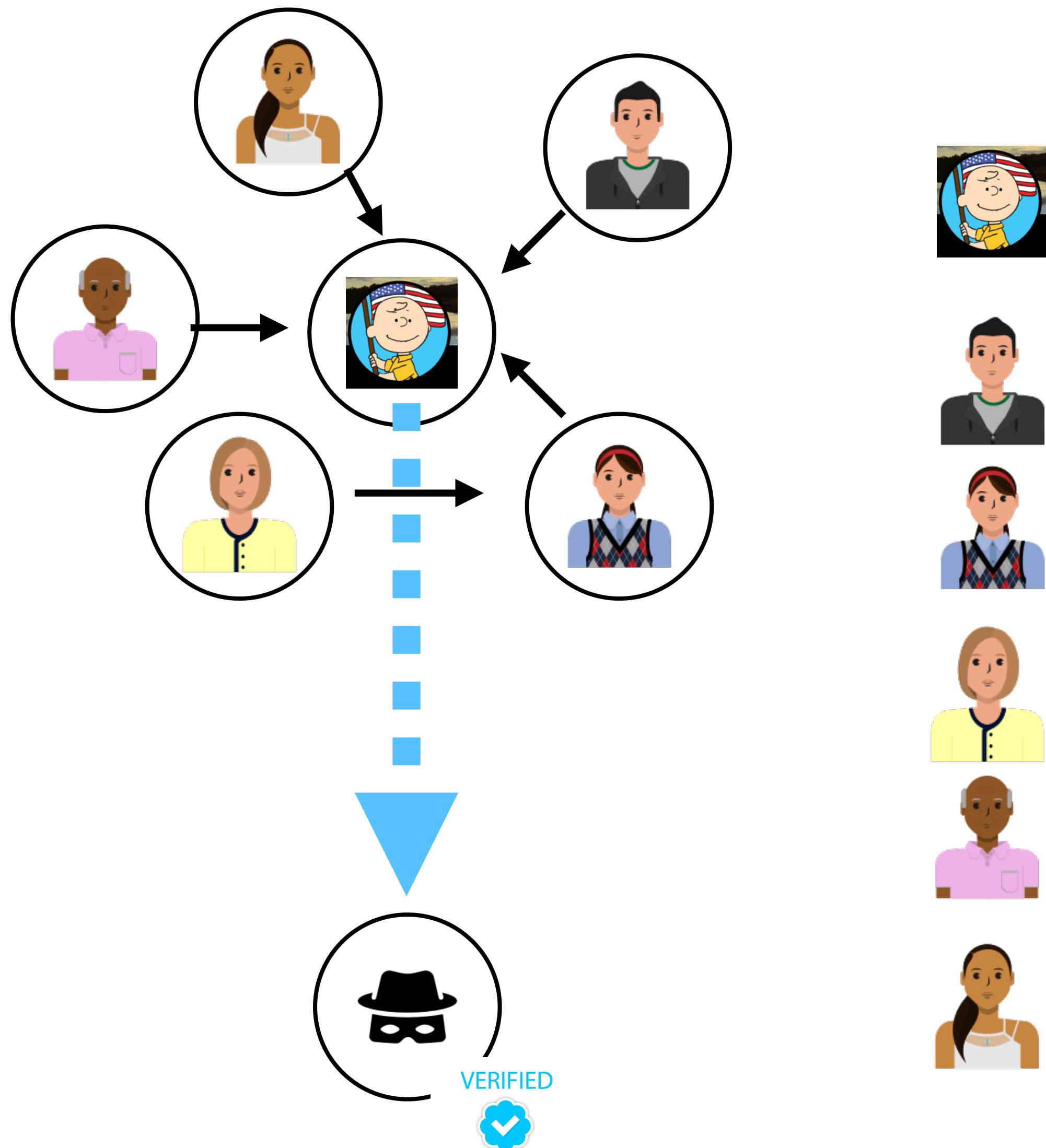
One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.



Autofollow if verified?	Autofollow if >10k followers?	Autofollow if @jack follows?
0	1	1
1	0	1
1	0	1
1	1	1
0	1	0
0	1	1

What about reputation? Autofollow.

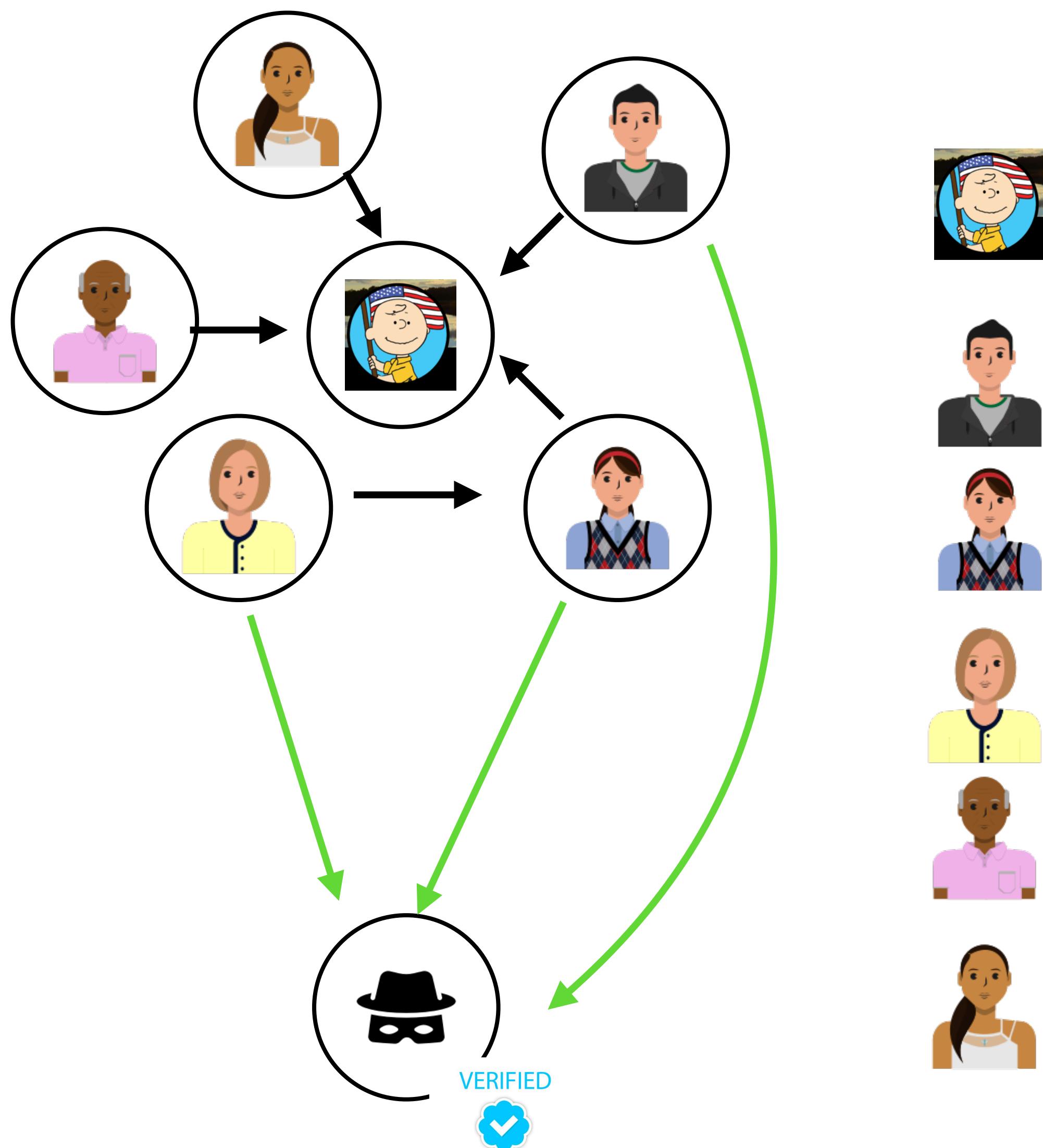
One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.



Autofollow if verified?	Autofollow if >10k followers?	Autofollow if @jack follows?
0	1	1
1	0	1
1	0	1
1	1	1
0	1	0
0	1	1

What about reputation? Autofollow.

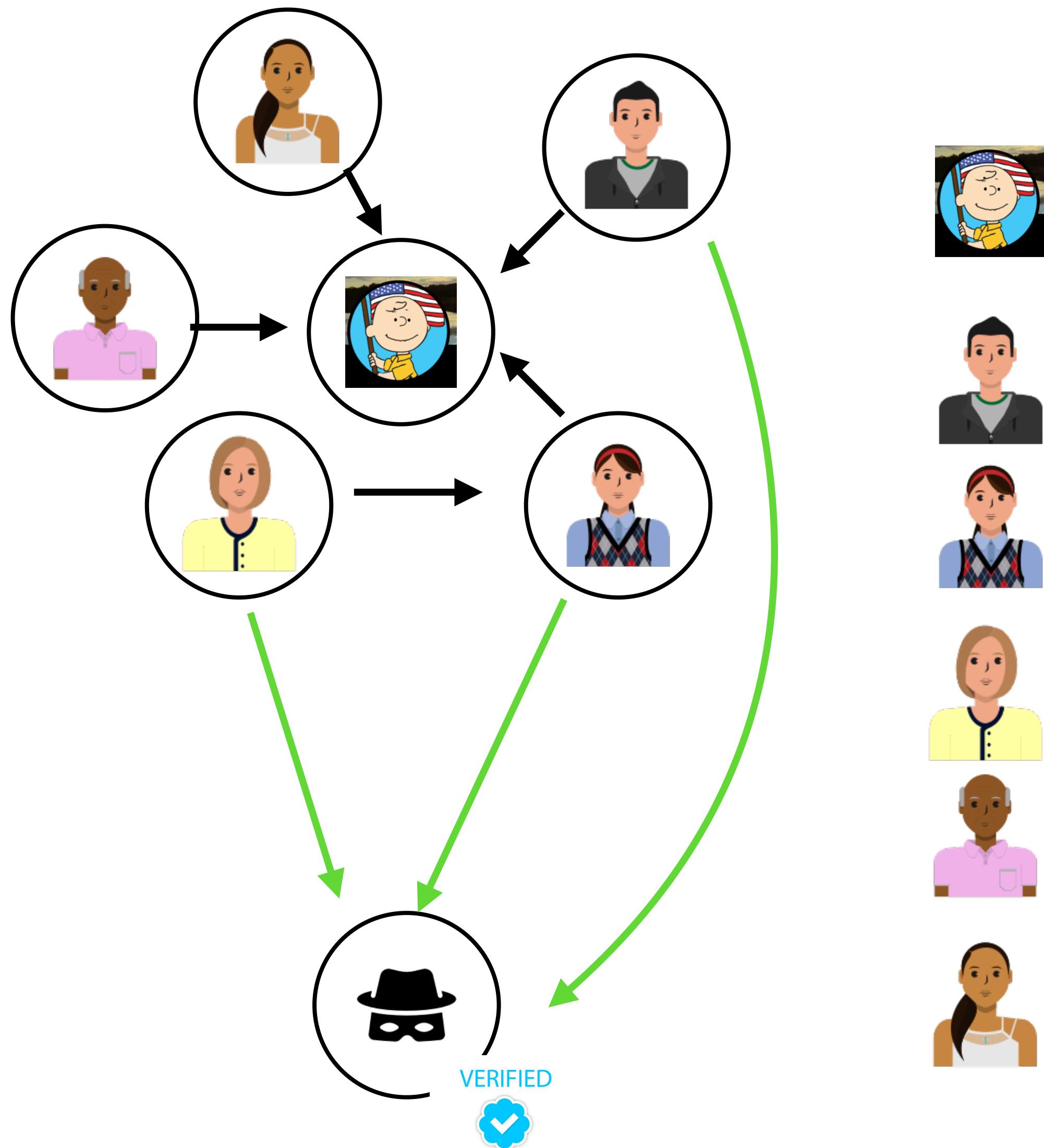
One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.



Autofollow if verified?	Autofollow if >10k followers?	Autofollow if @jack follows?
0	1	1
1	0	1
1	0	1
1	1	1
0	1	0
0	1	1

What about reputation? Autofollow.

One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.

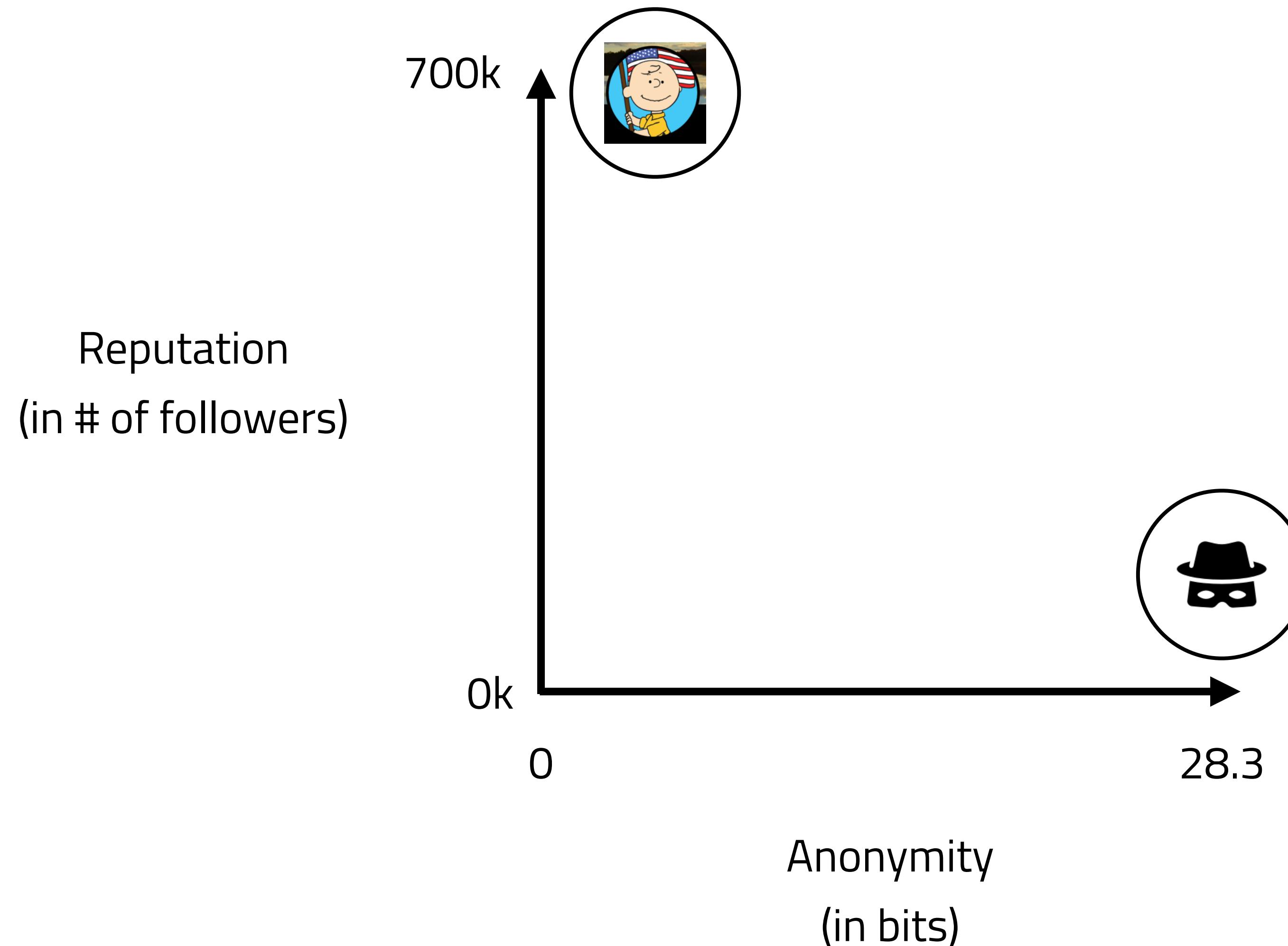


Autofollow if verified?	Autofollow if >10k followers?	Autofollow if @jack follows?
0	1	1
1	0	1
1	0	1
1	1	1
0	1	0
0	1	1

Suppose 150k accounts autofollow verified

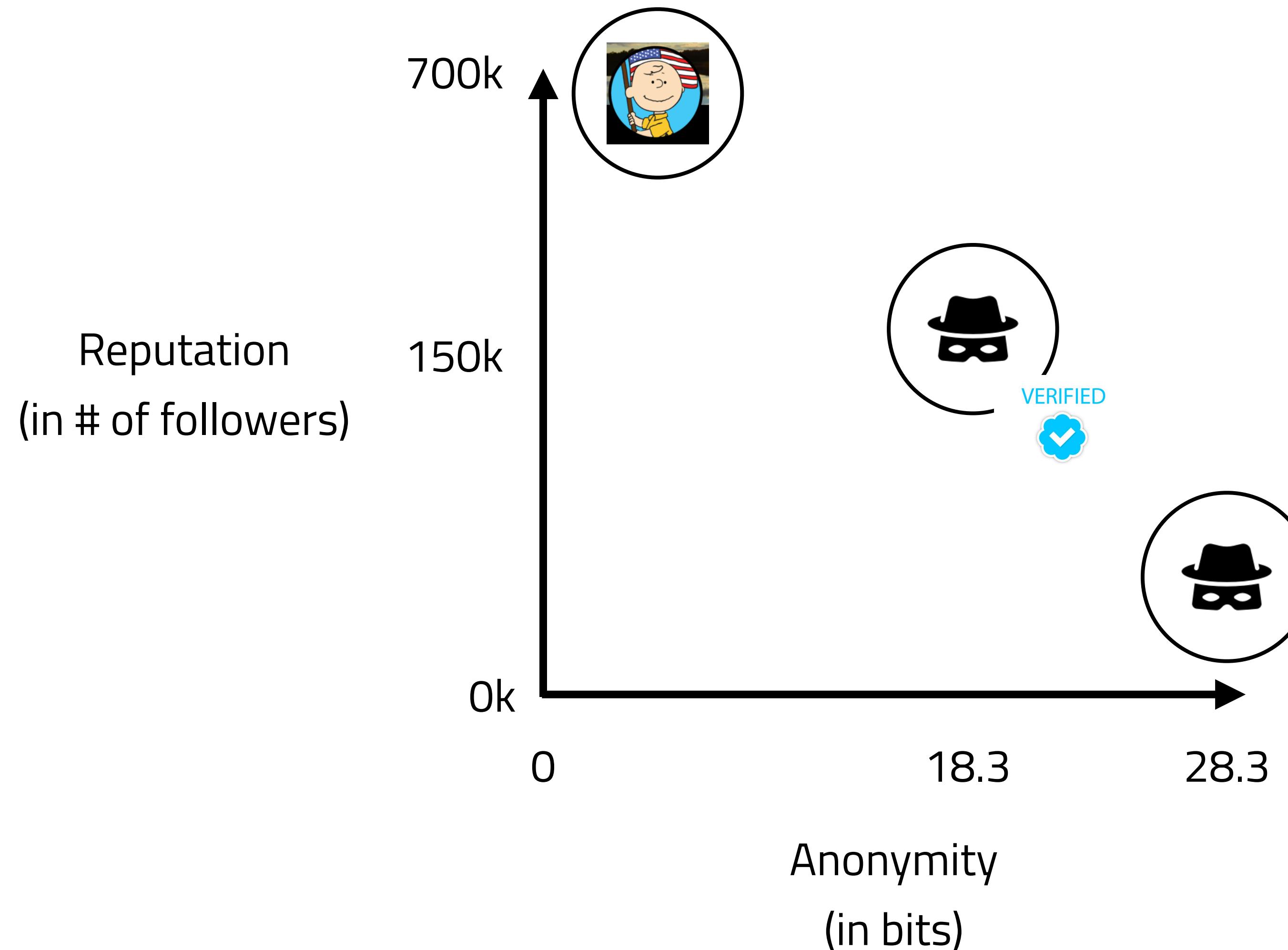
A quantifiable anonymity/reputation tradeoff

With autofollow we know how many followers we get prior to making any zero knowledge attestation(s).



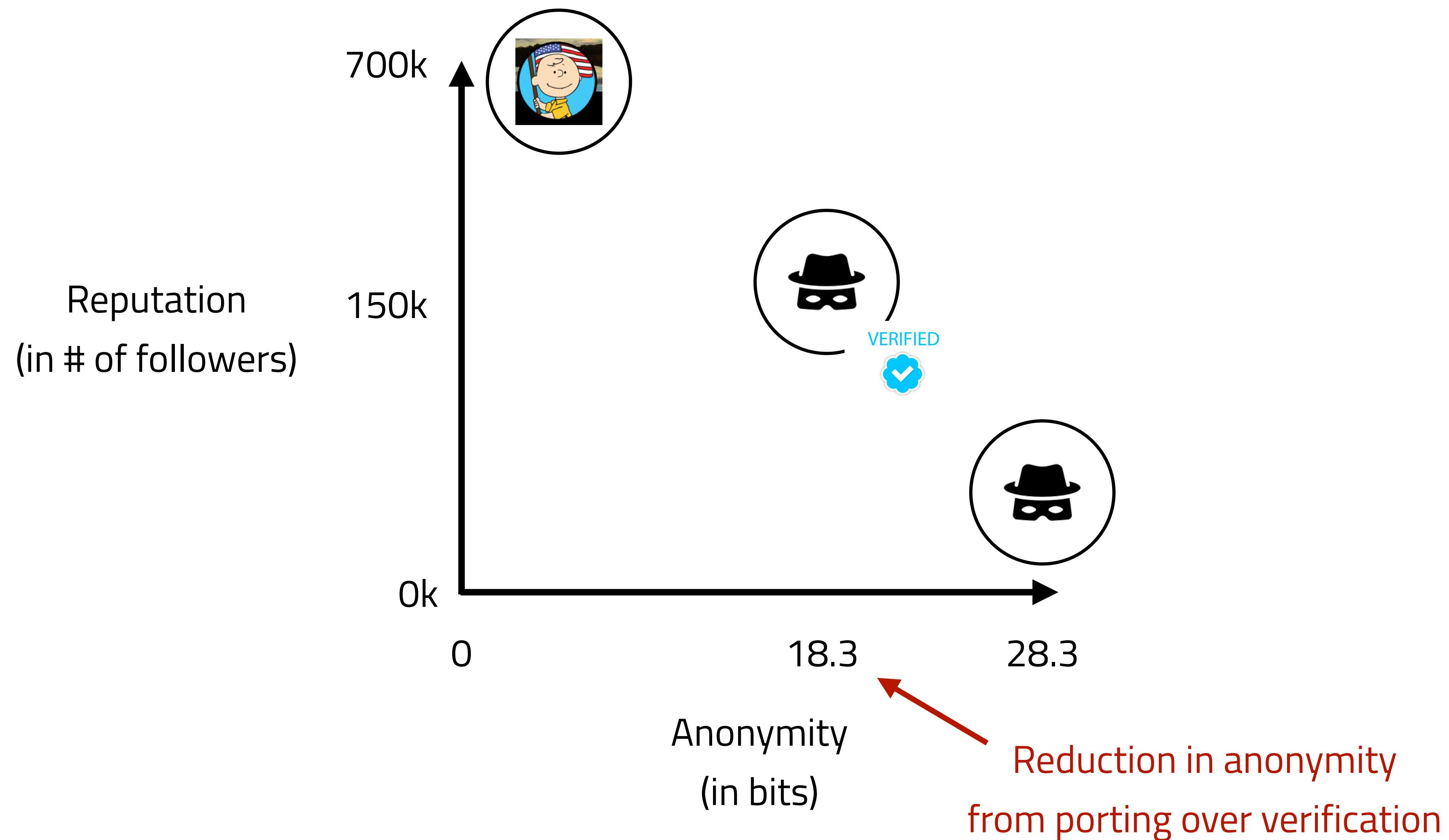
A quantifiable anonymity/reputation tradeoff

With autofollow we know how many followers we get prior to making any zero knowledge attestation(s).



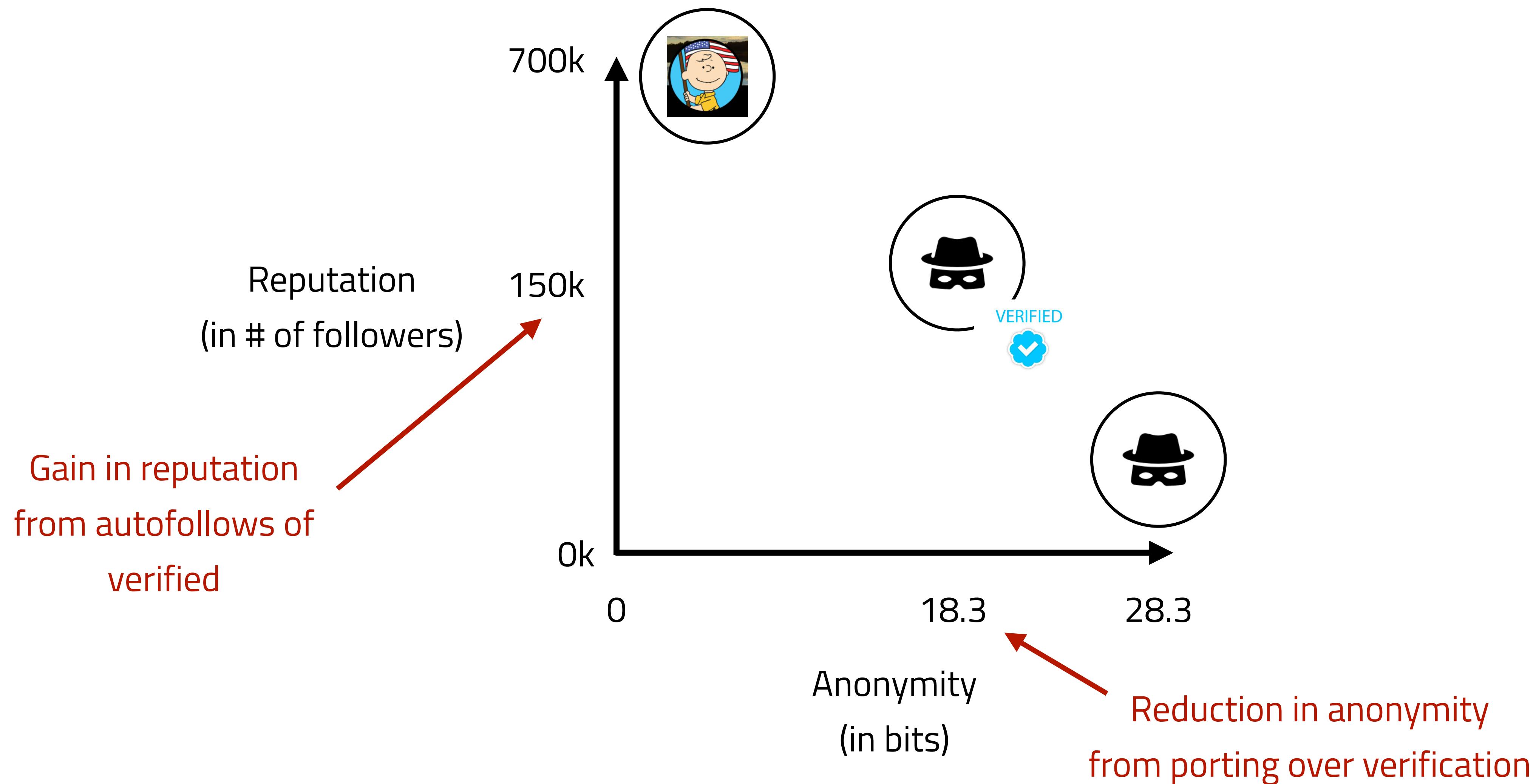
A quantifiable anonymity/reputation tradeoff

With autofollow we know how many followers we get prior to making any zero knowledge attestation(s).



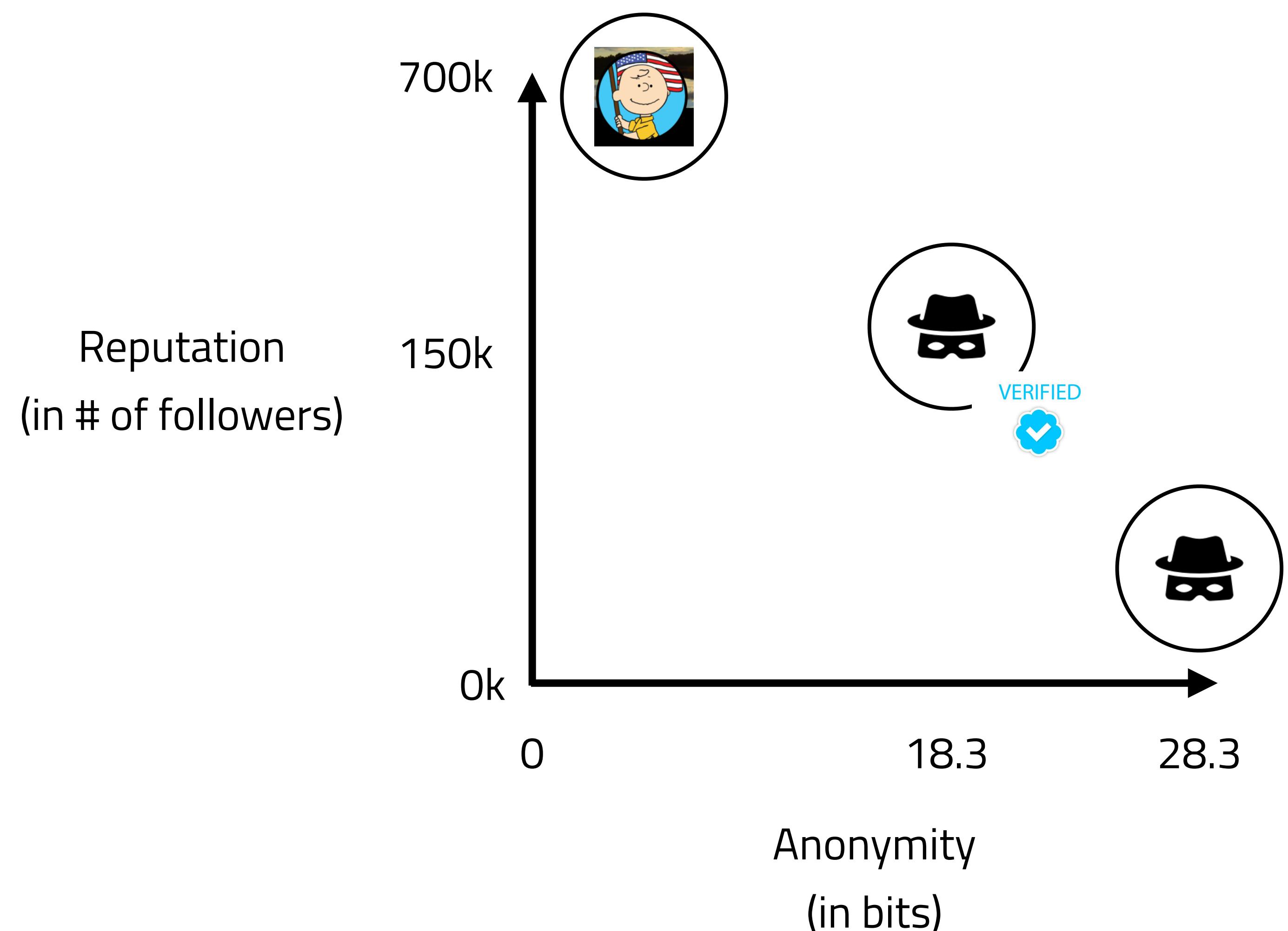
A quantifiable anonymity/reputation tradeoff

With autofollow we know how many followers we get prior to making any zero knowledge attestation(s).



Now you can move wealth and reputation to a pseudonym

This allows people to shield themselves against attacks by separating their earning, speaking, and real names.



Next steps

- Crypto domains, AI, ZK have all advanced
- Decentralized media exists, so can implement it there

Summary

- What is pseudonymity?
- Why a pseudonymous economy?
- How might it work?
- How could we build it?

Real names

The screenshot shows Mark Zuckerberg's Facebook profile. At the top, there's a blue header with the URL "www.facebook.com/zuck?sk=wall". Below it is the "facebook" logo and a search bar. The main area features a large photo of Mark Zuckerberg smiling. To his right, his name "Mark Zuckerberg" is displayed in bold black text, followed by a short bio: "Works at Facebook Studied Computer Science at Harvard University Lives in Palo Alto, California Knows English, Mandarin Chinese From Dobbs Ferry, New York Born on May 14, 1984". Below the bio is a "Wall" section with a post from him: "I like dangerous thoughts." on Samuel W. Lessin's status, posted on January 17 at 11:43am via iPhone. The post has 150 likes. Navigation links "Wall" and "Info" are visible, along with options to "Share Profile" and "Report/Block This Person".

Pseudonyms

The screenshot shows a Reddit user profile for "u/SadCapitalsFan". The profile picture is a white cartoon character. The username is "u/SadCapitalsFan". Below the username, "Karma" is listed with a value of "8,065". A "Cake day" badge indicates the user's birthday is March 16, 2018. A note says "Received the Silver Award in the past 30 days". There are three buttons at the bottom: "FOLLOW", "CHAT", and "MORE OPTIONS". To the right of the profile is a circular image of a person with blonde hair, and the word "ENT" is partially visible.

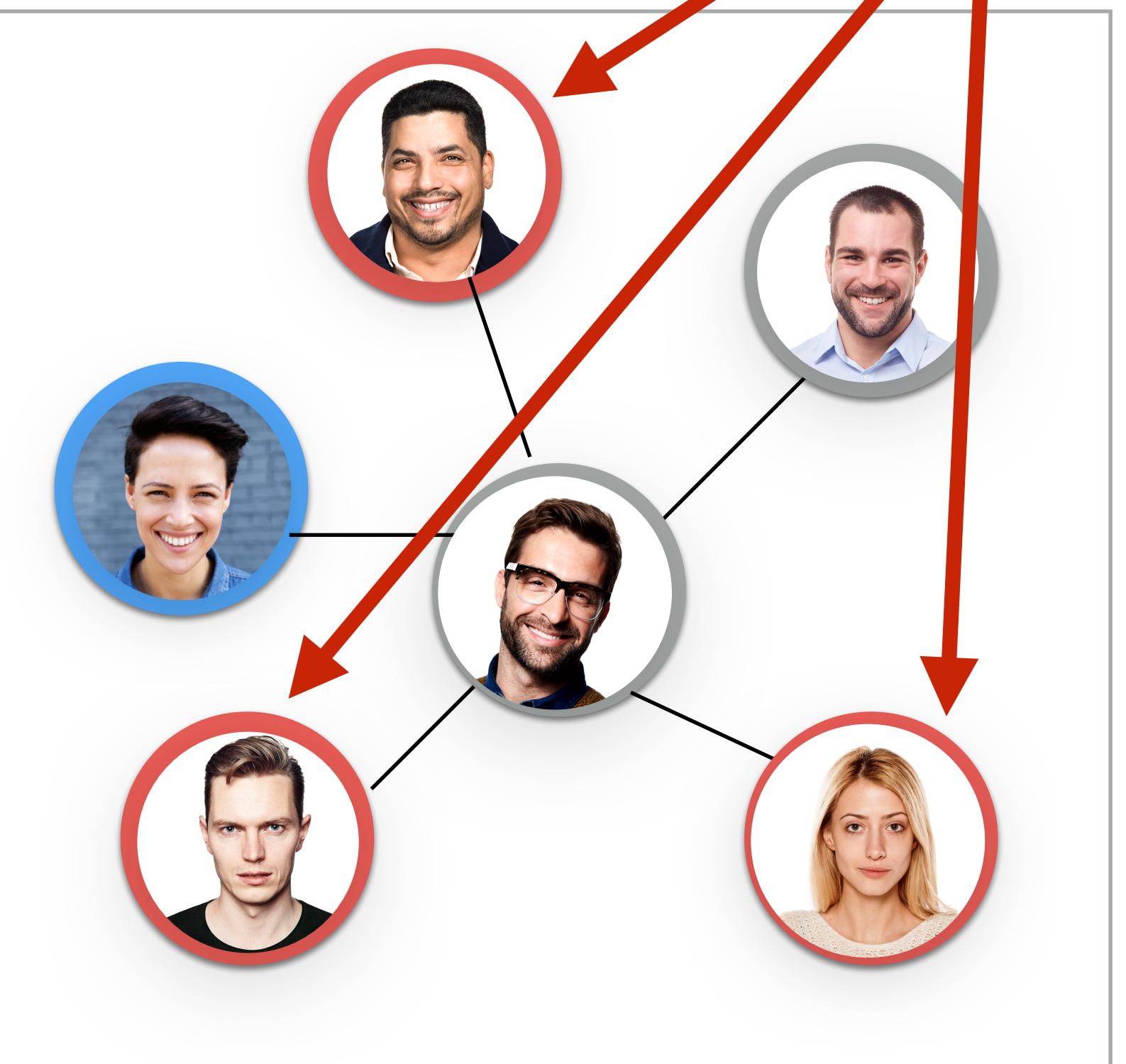
Comfortably Smug
@ComfortablySmug
My Interests: Finance, Whiskey, Politics, Books, Food, Meeting Strangers
#altcenter

Anonyms

The screenshot shows a post from the "Anonymous" account on 4chan. The post was made on December 2, 2016, at 00:14:43, with ID No. 713797026. The file attached is "anon.jpg" (62 KB, 1200x797). The post includes a link to the file and a reply link. The text of the post is: "Dear 4chan, It's us, Anonymous, once again. Except this time it's The Leader speaking." The background of the screenshot is yellow.

Summary

- What is pseudonymity?
- Why a pseudonymous economy?
- How might it work?
- How could we build it?



before



after



is now bad

Summary

- What is pseudonymity?
- Why a pseudonymous economy?
- How might it work? **Yellow Box**
- How could we build it?



Earning



Tristan Su
foobar

📍 China
✉️ Sign in to view email
🔗 http://foobar.github.io



Zcash

Speaking



Comfortably Smug
@ComfortablySmug

My Interests: Finance, Whiskey, Politics, Books, Food, Meeting Strangers
#altcenter

"Real" name

Customs Declaration

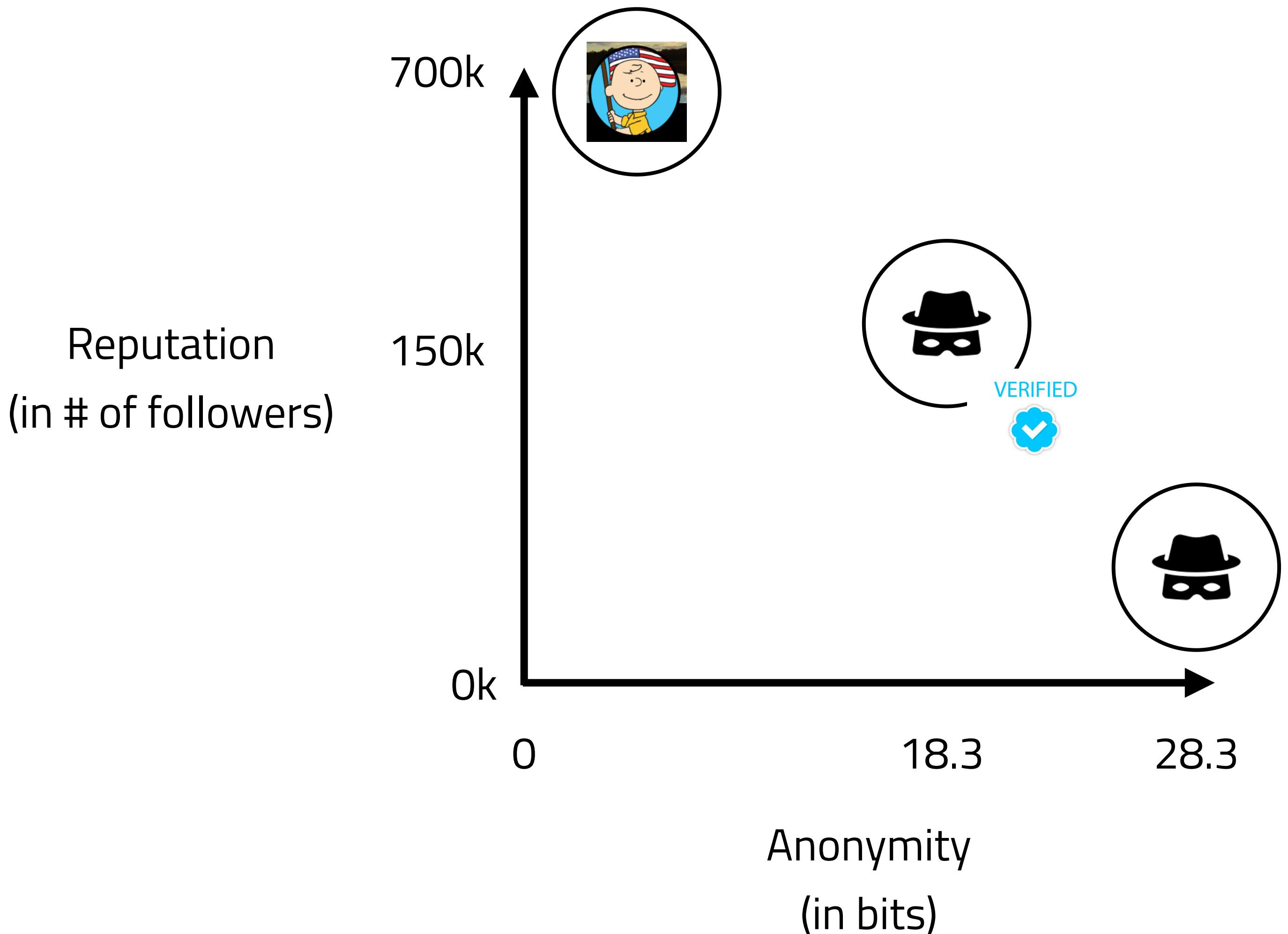
FORM APPROVED
19 CFR 122.27, 148.12, 148.13, 148.150, 148.111, 1488.21 OPR 83-16
OMB NO. 1625-0009

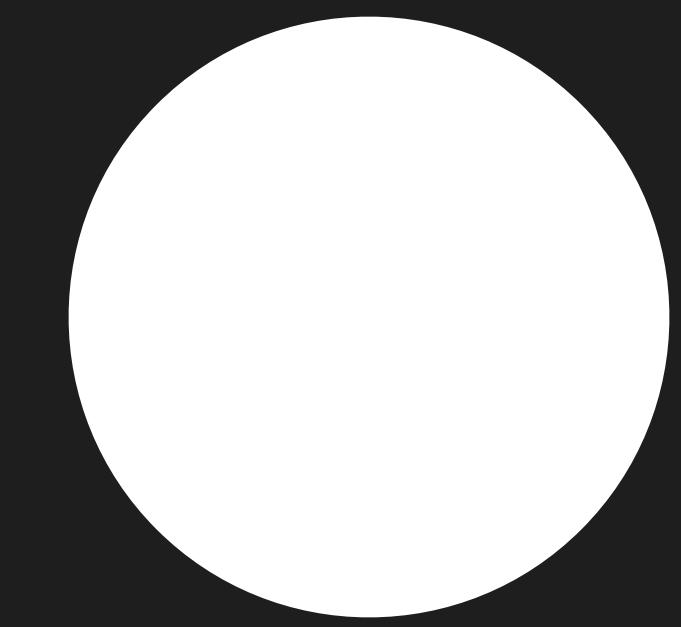
Each arriving traveler or responsible family member must provide the following information (only ONE written declaration per family is required). The term "Family" is defined as "members of a family residing in the same household who are related by blood, marriage, domestic relationship, or adoption."

1 Family Name
First (Given) _____ Middle _____

Summary

- What is pseudonymity?
- Why a pseudonymous economy?
- How might it work?
- How could we build it?





Thank you
@balajis

Next Steps

Please fill out the feedback form here:

<https://airtable.com/shra7mpYwTNcBflwf>