1729

Lecture 12: The Pseudonymous Economy

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

6529
@punk6529

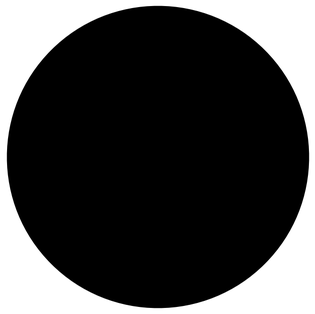
I still can't believe how right @balajis was on avatars/pseudo identity.

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?

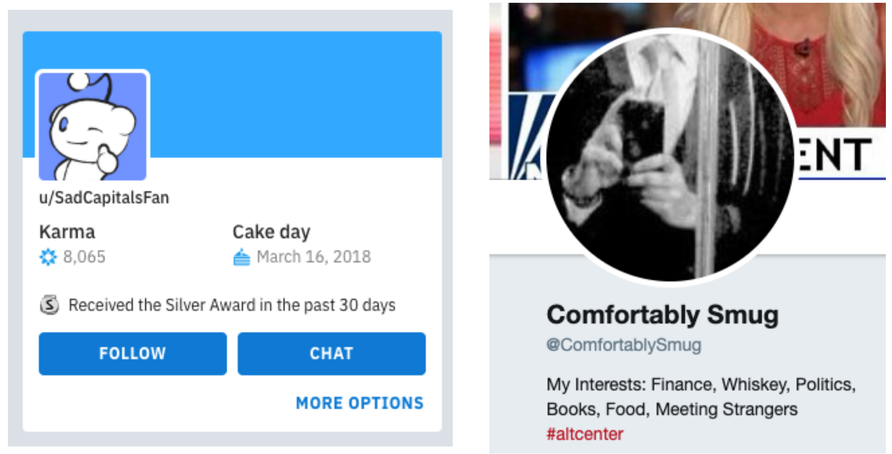
What is pseudonymity?
Why a pseudonymous economy?
How might it work?
How could we build it?

Pseudonymity is not anonymity

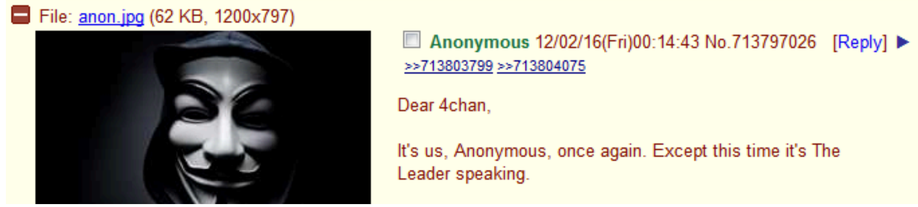
Let's distinguish real names, pseudonyms, and anonyms.

Real names

Pseudonyms



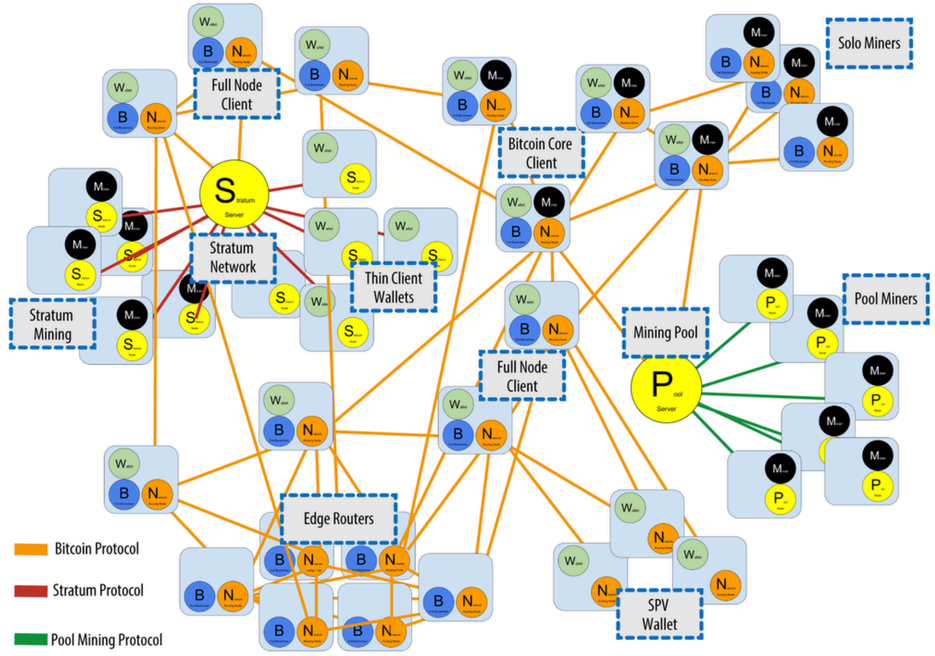
Anonyms



Pseudonymity is as important as decentralization

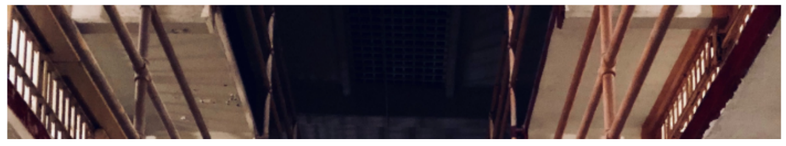
Satoshi's pseudonymity was as important as Bitcoin's decentralization.

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



Should Satoshi Nakamoto Go to Jail?

October 14th 2019 TWEET THIS



Pseudonymity is a continuum

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

DIGITS NEXT STORY >

The Information That Is Needed to Identify You: 33 Bits

By WSJ Staff

Aug 4, 2010 12:20 am ET

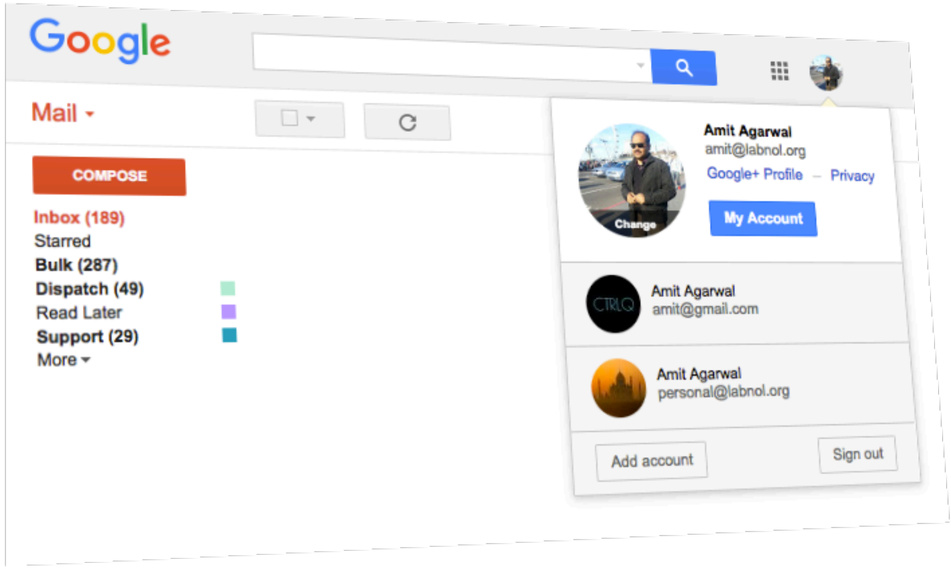
2^33	8.6B	33 bits
World population	7.5B	32.8 bits
Twitter MAUs	330M	28.3 bits
Twitter verified	330K	18.3 bits

Pseudonymity is already mainstream

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

Pseudonymity is where society is going

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



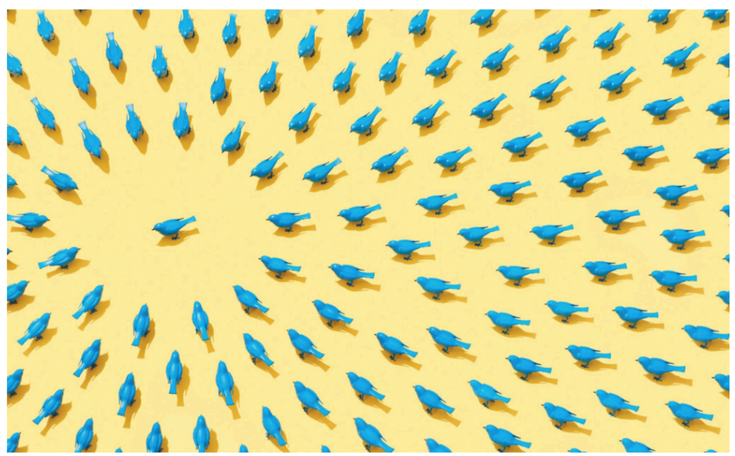


Photo illustration by Andrew B. Myers. Prop stylist: Sonia Rentsch.

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

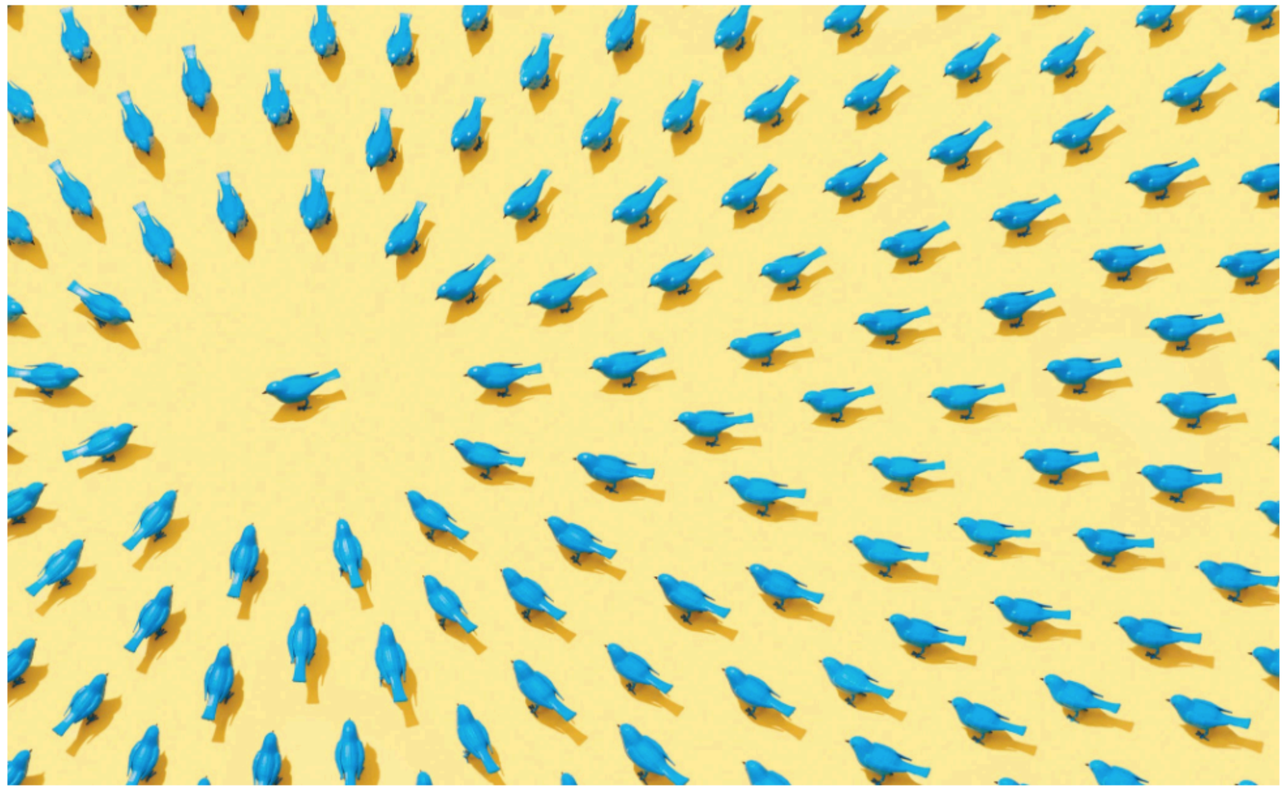
> In Soviet Russia, we too have freedom of speech. But in America, you have freedom after speech!
>
> *Yakov Smirnoff*

Why? Because social media mobs are now routine

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

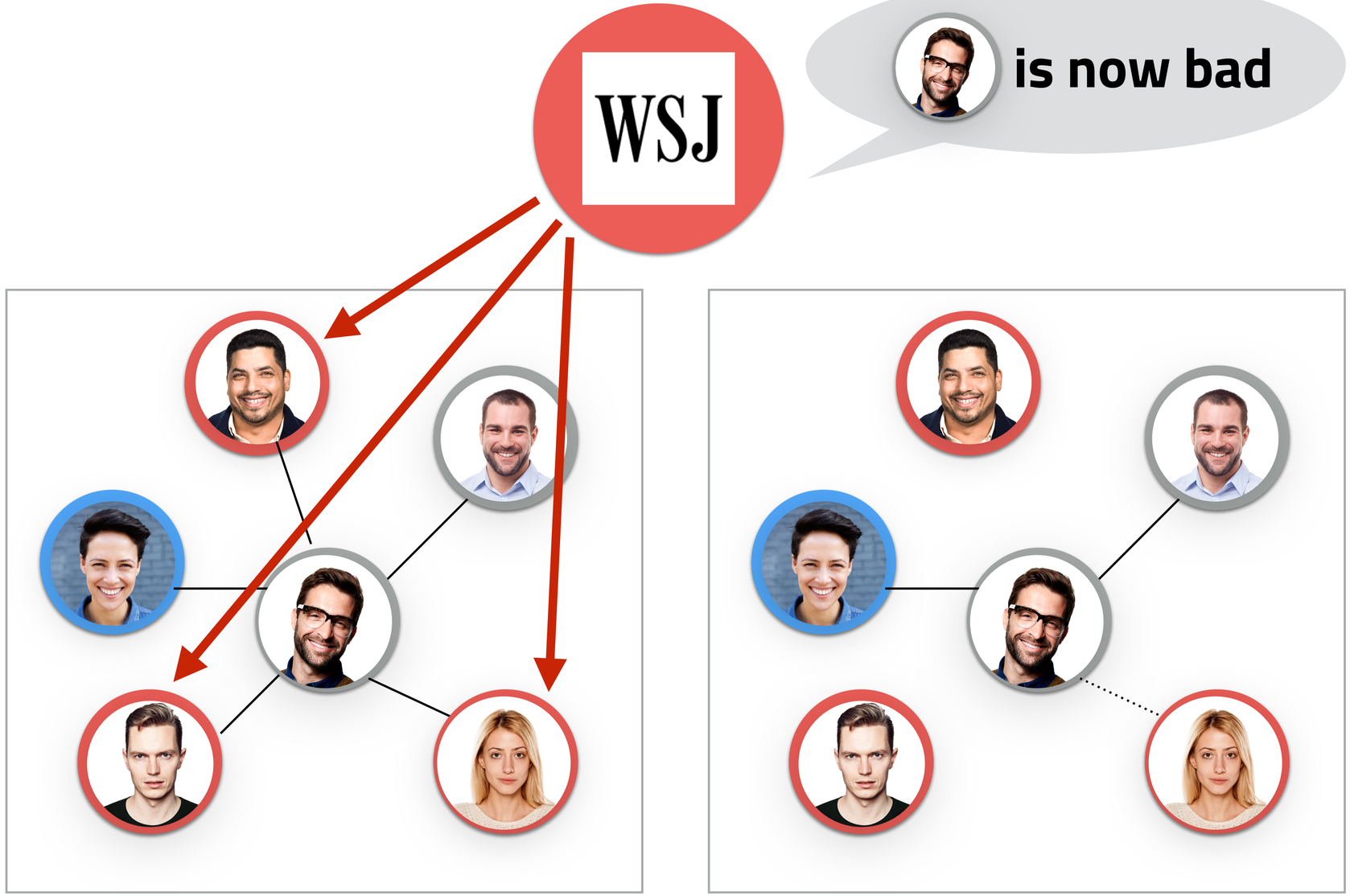
How One Stupid Tweet Blew Up Justine Sacco's Life

By JON RONSON FEB. 12, 2015



And negative press is an attack on your social network

Call this a social network supply chain disruption.

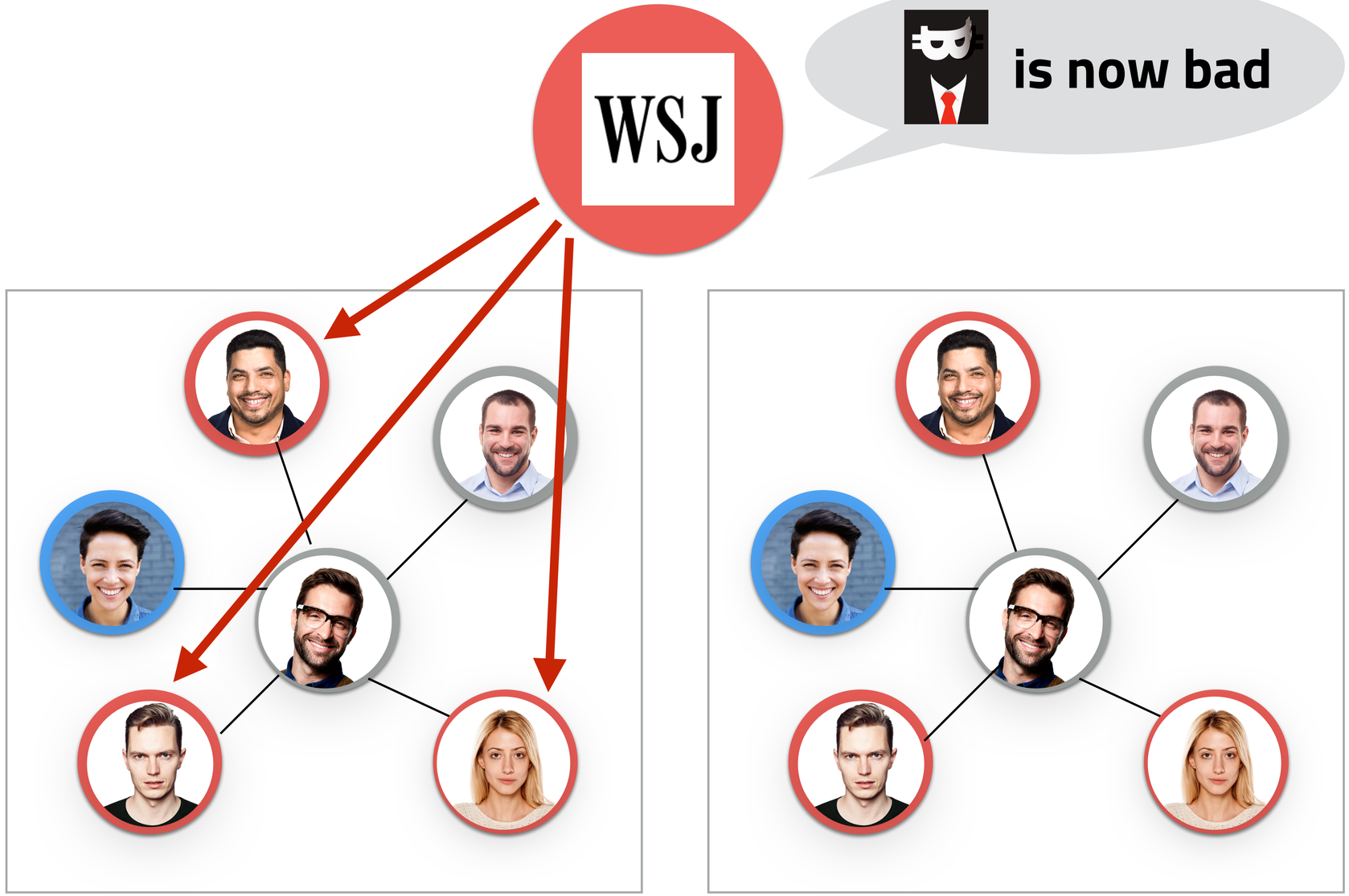


before

after

Pseudonymity defends against social supply chain disruptions

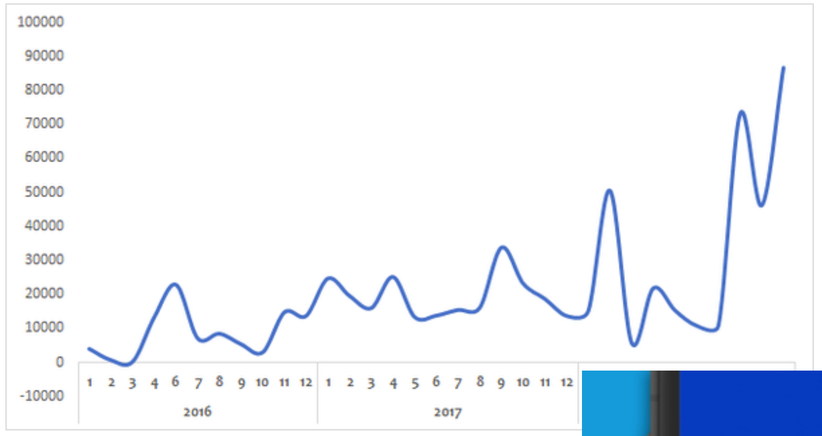
There are others, like maximizing personal runway / financial independence, or maintaining multiple options for each supply chain node.

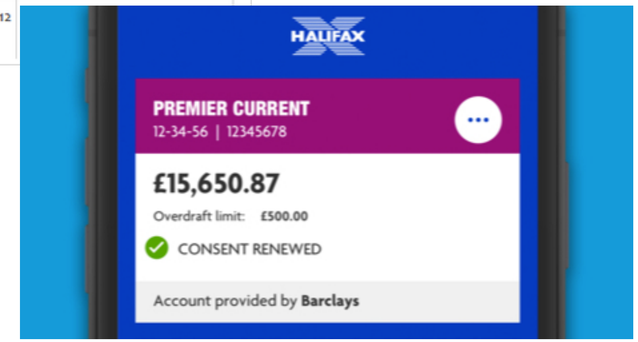


before

after

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

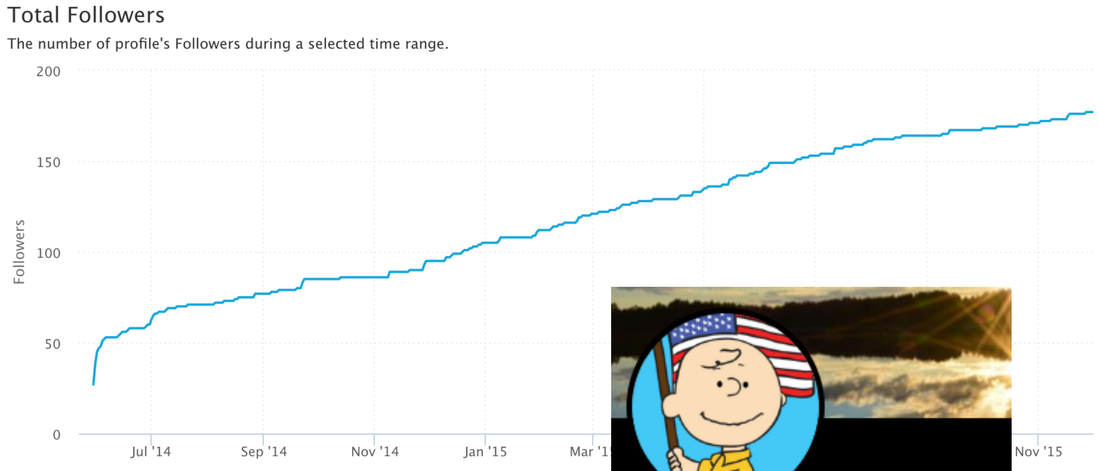


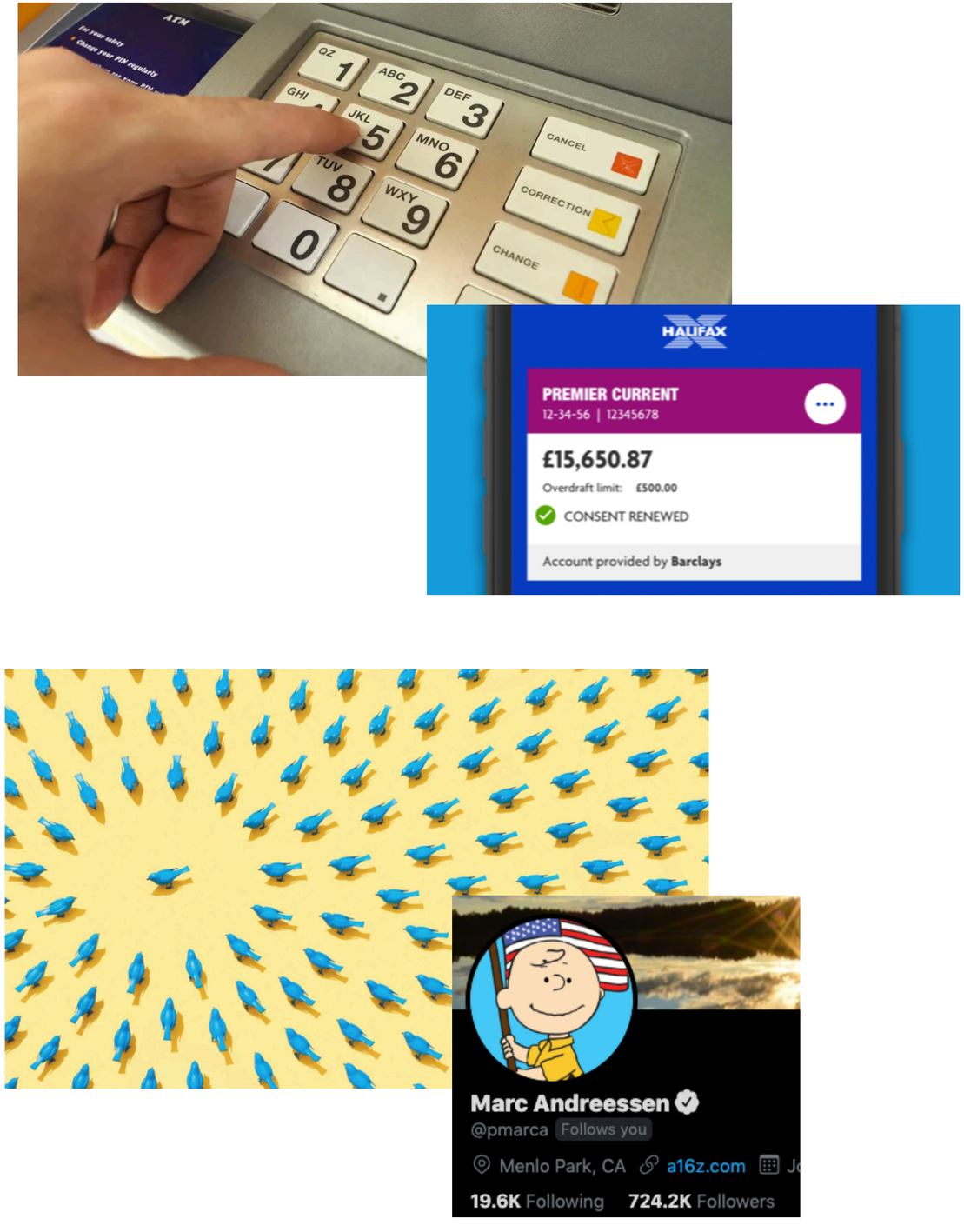


Your bank account is stored wealth.

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

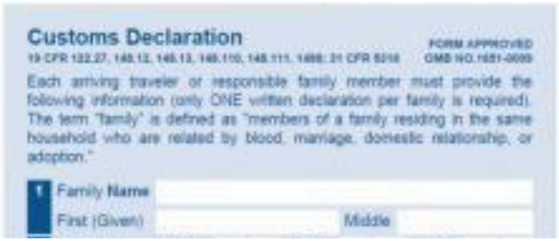
Zcash

Speaking

Comfortably Smug
@ComfortablySmug

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

"Real" name



Customs Declaration

FORM APPROVED OMB NO.1651-0009

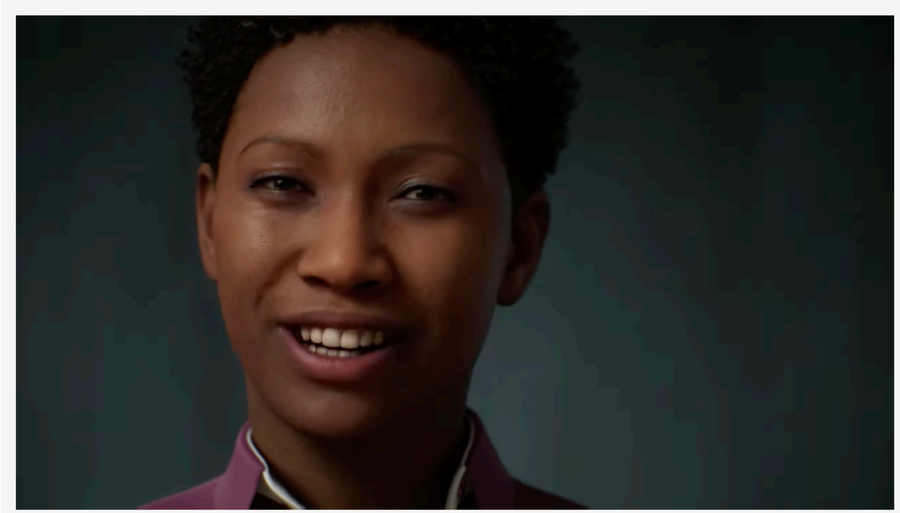
19 CFR 122.27, 148.12, 148.13, 148.110, 148.111, 148.6; 31 CFR 5316

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."

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
362 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.

23 61 482

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.

6 18 186

balajis.com
@balajis

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

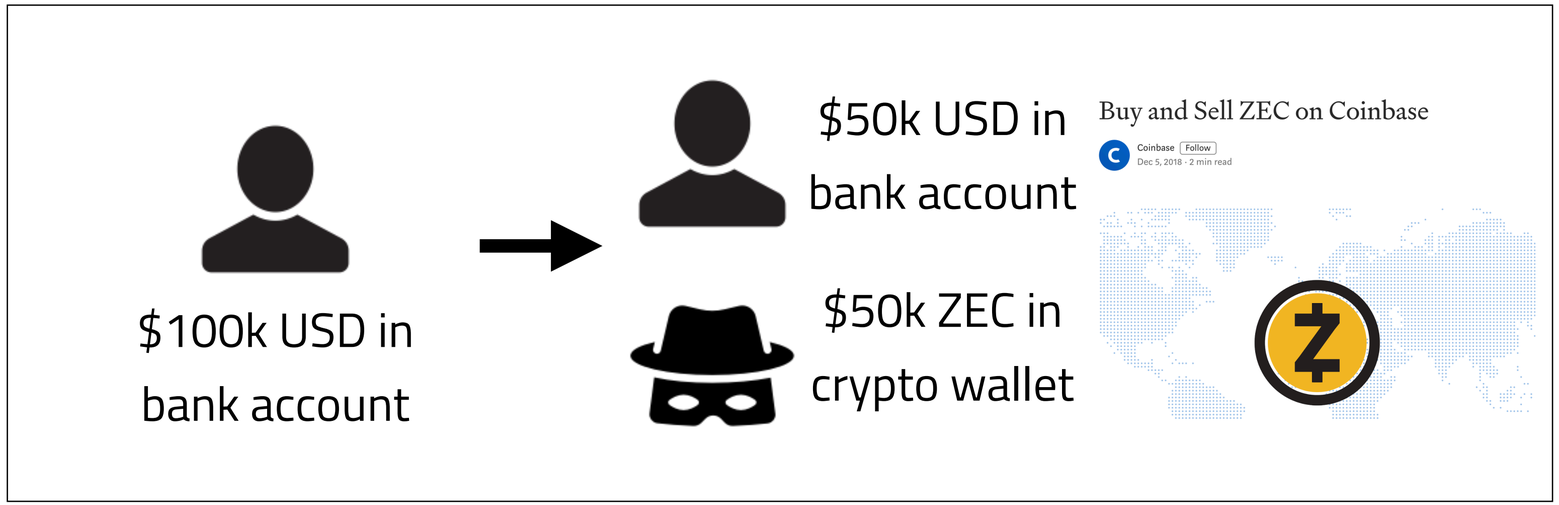
3:12 AM · Dec 15, 2020 · Twitter for iPhone

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?

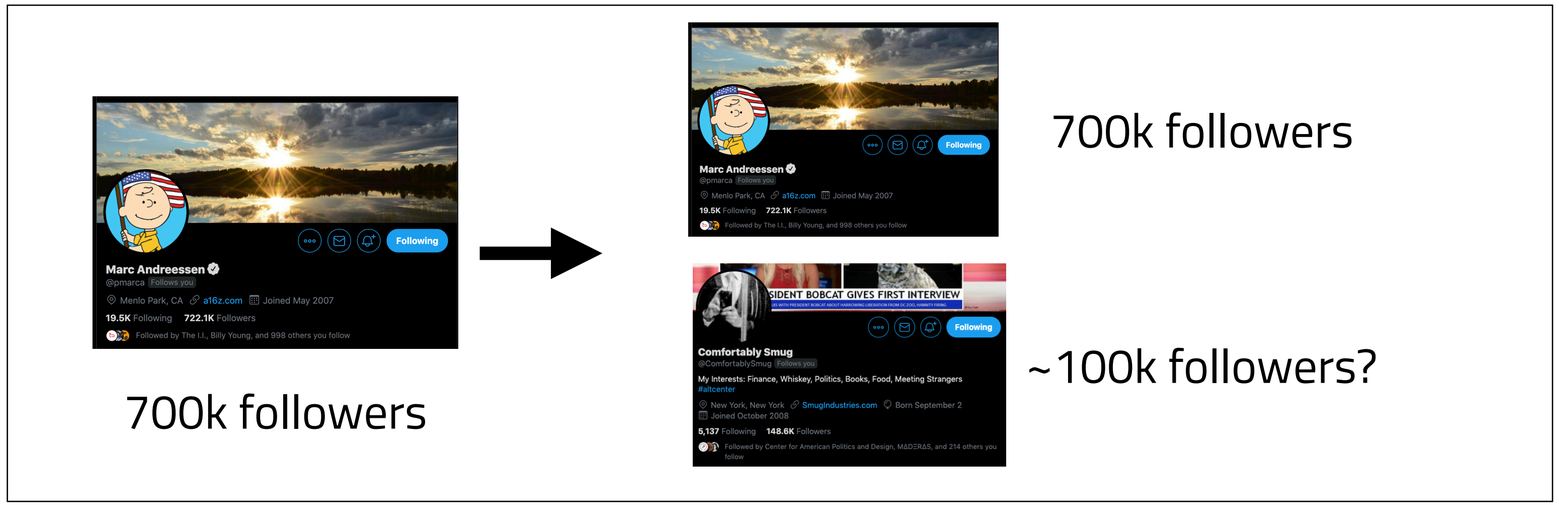


Transfer wealth to a pseudonym

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?

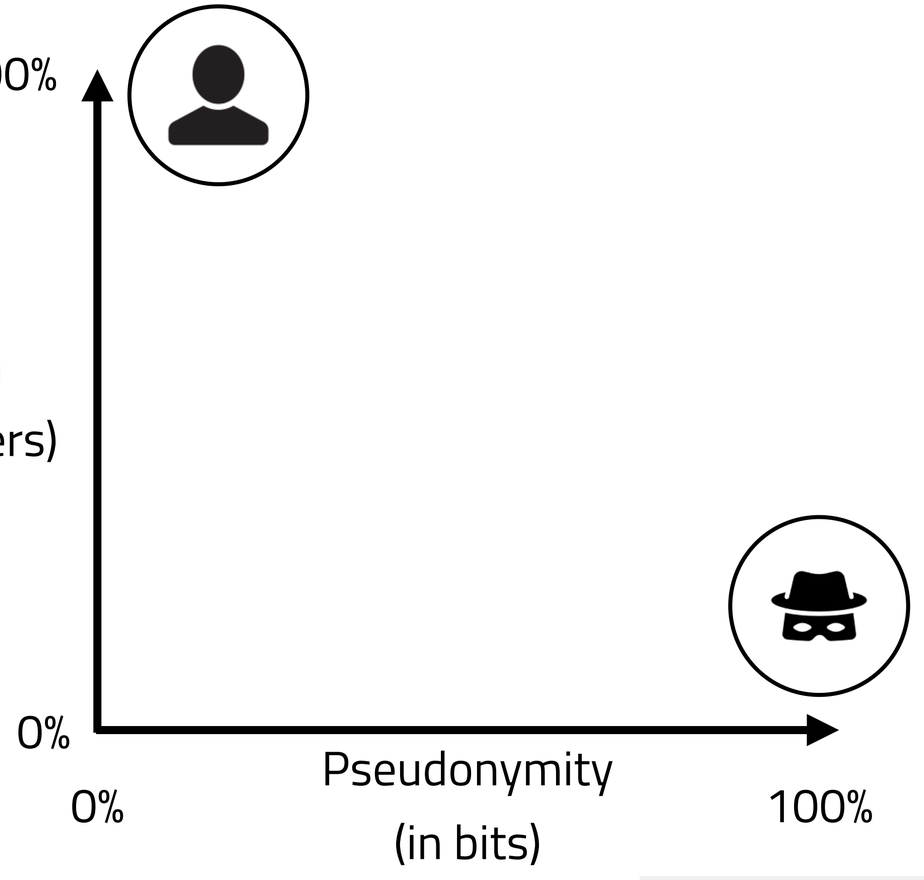
Let's take the special case of Twitter.

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

Right now only two choices:

100/0 or 0/100.

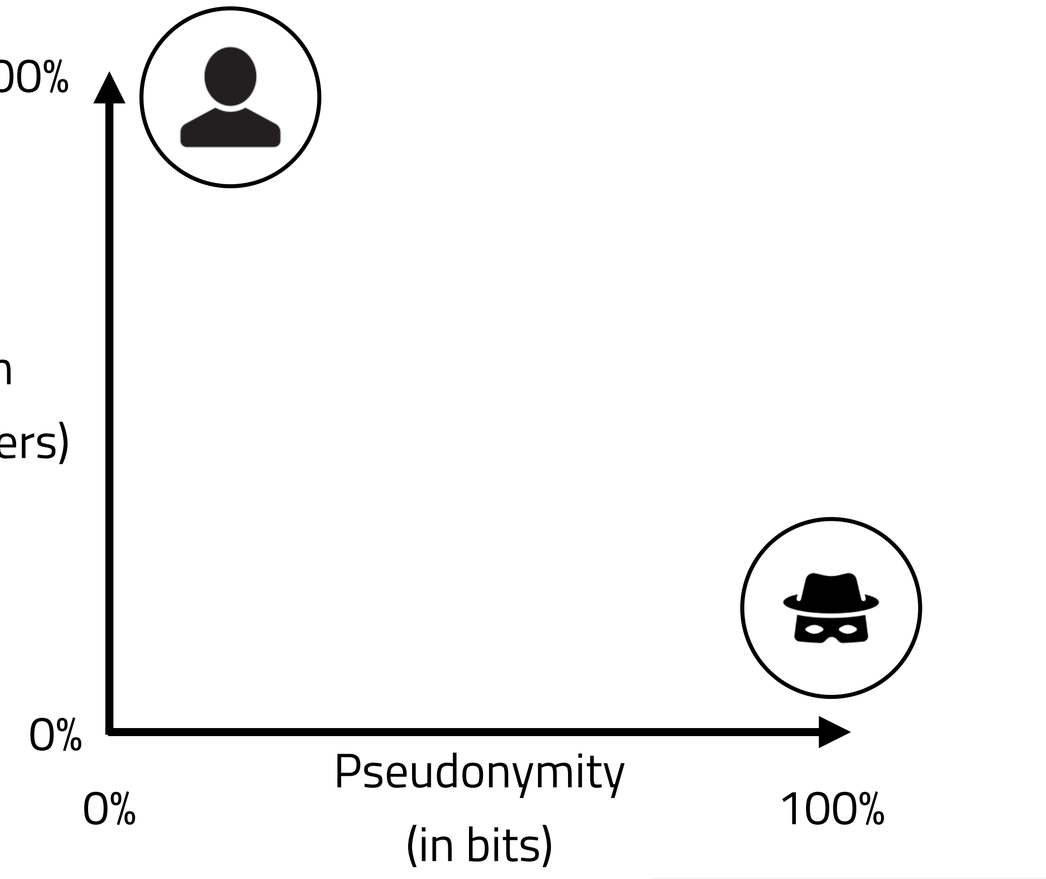
All your distribution and no pseudonymity, or vice versa.



Right now only two choices:

100/0 or 0/100.

All your distribution and no pseudonymity, or vice versa.



DIGITS NEXT STORY >

The Information That Is Needed to Identify You: 33 Bits

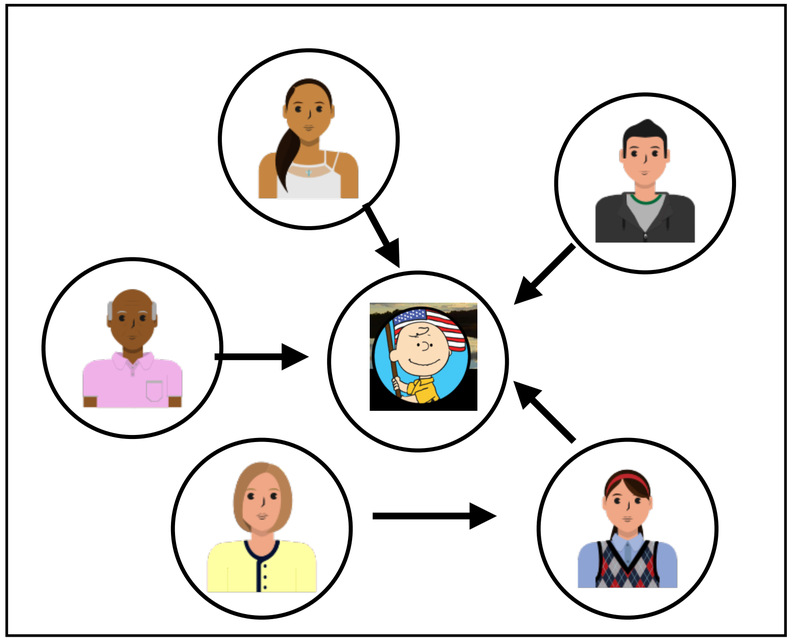
By WSJ Staff

Aug 4, 2010 12:20 am ET

Can we trade off some pseudonymity for some distribution?

Naive approach: transfer <u>all</u> followers

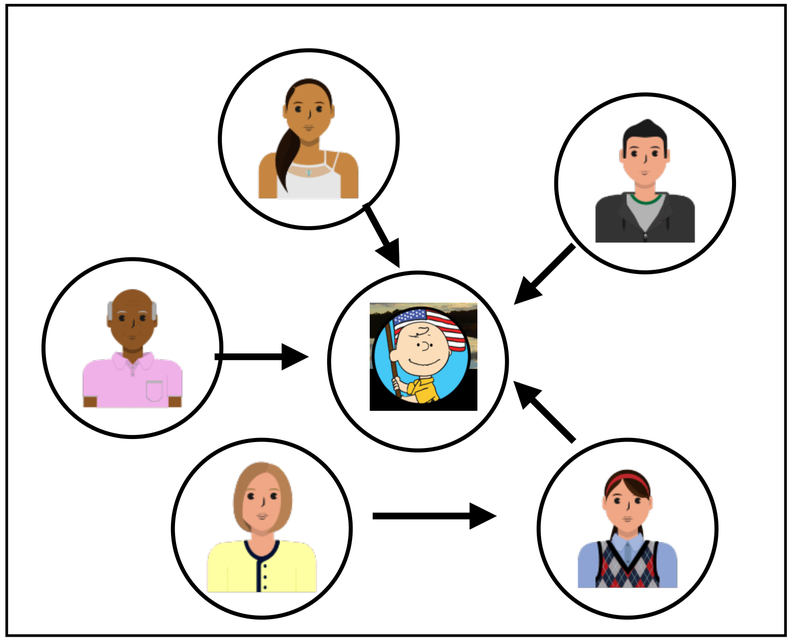
Suppose we just set up a new Twitter pseudonym and transfer all followers to that pseudonym.

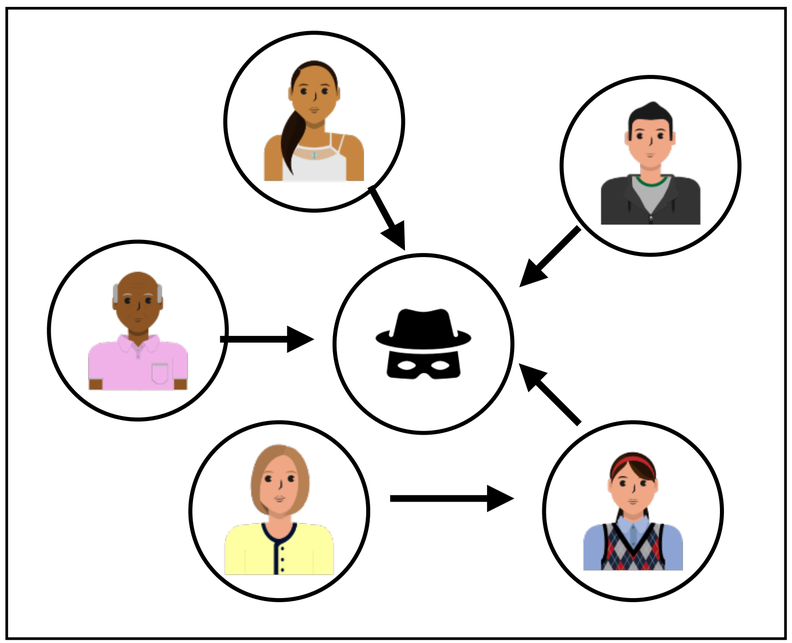


	0	1	1	0	1	1
	0	0	0	0	0	0
	0	0	0	1	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0

Naive approach: transfer <u>all</u> followers

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

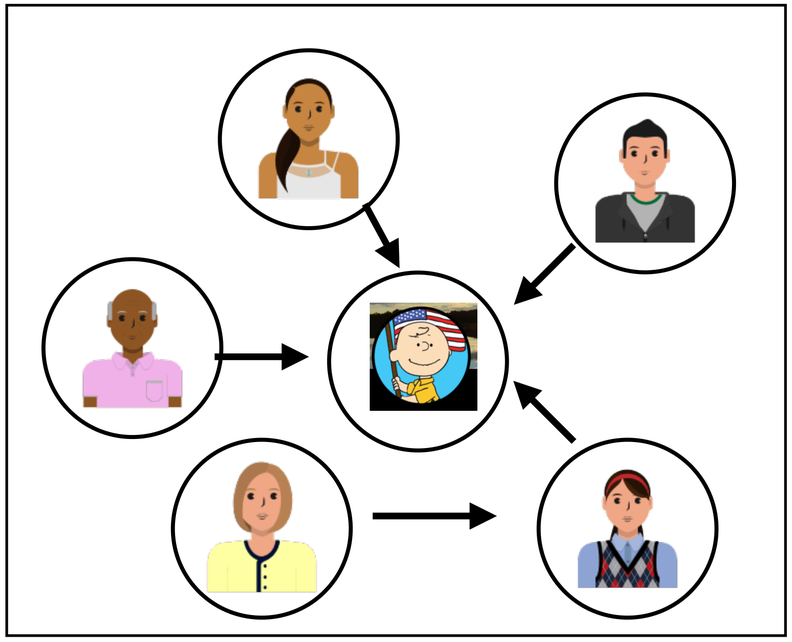


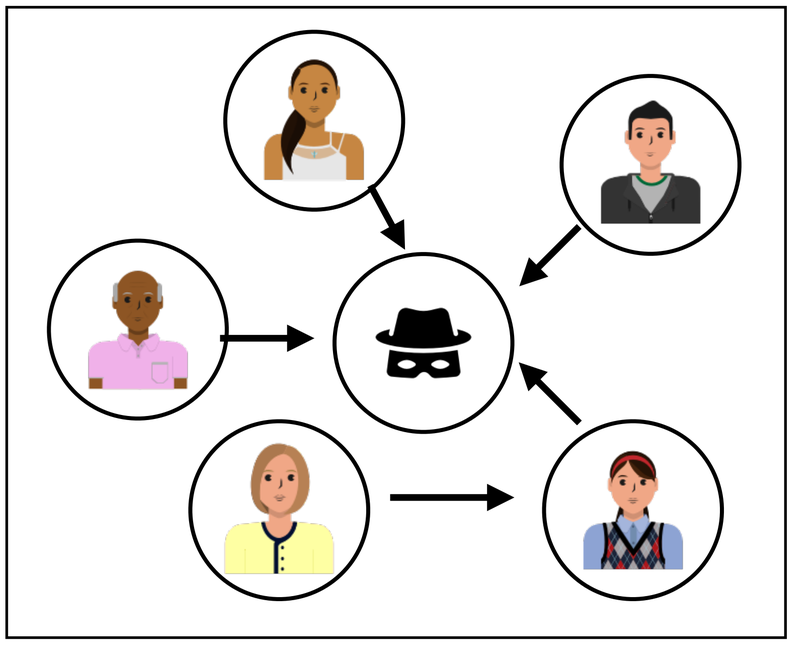


	0	1	1	0	1	1
	0	0	0	0	0	0
	0	0	0	1	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0
	0	0	0	0	0	0

Naive approach: transfer <u>all</u> followers

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

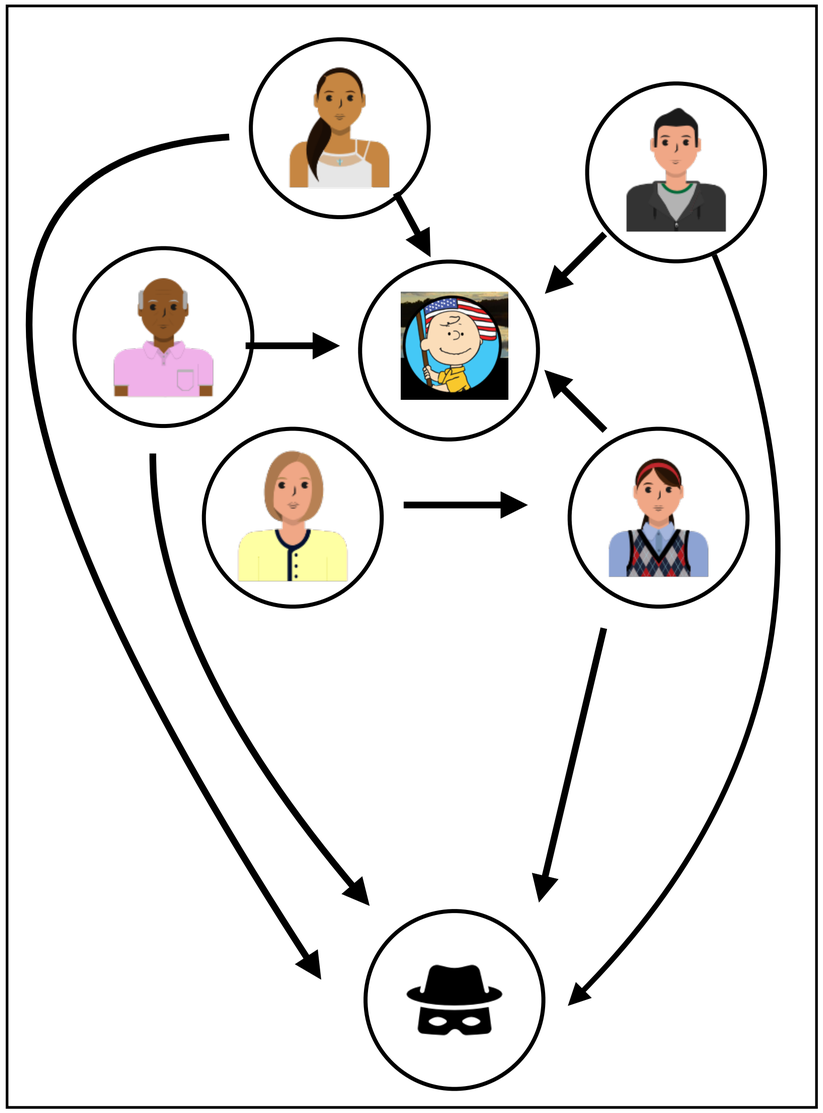




	0	1	1	0	1	1	0
	0	0	0	0	0	0	0
	0	0	0	1	0	0	0
	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
	0	0	0	0	0	0	0
	0	1	1	0	1	1	0

Naive approach: transfer <u>all</u> followers

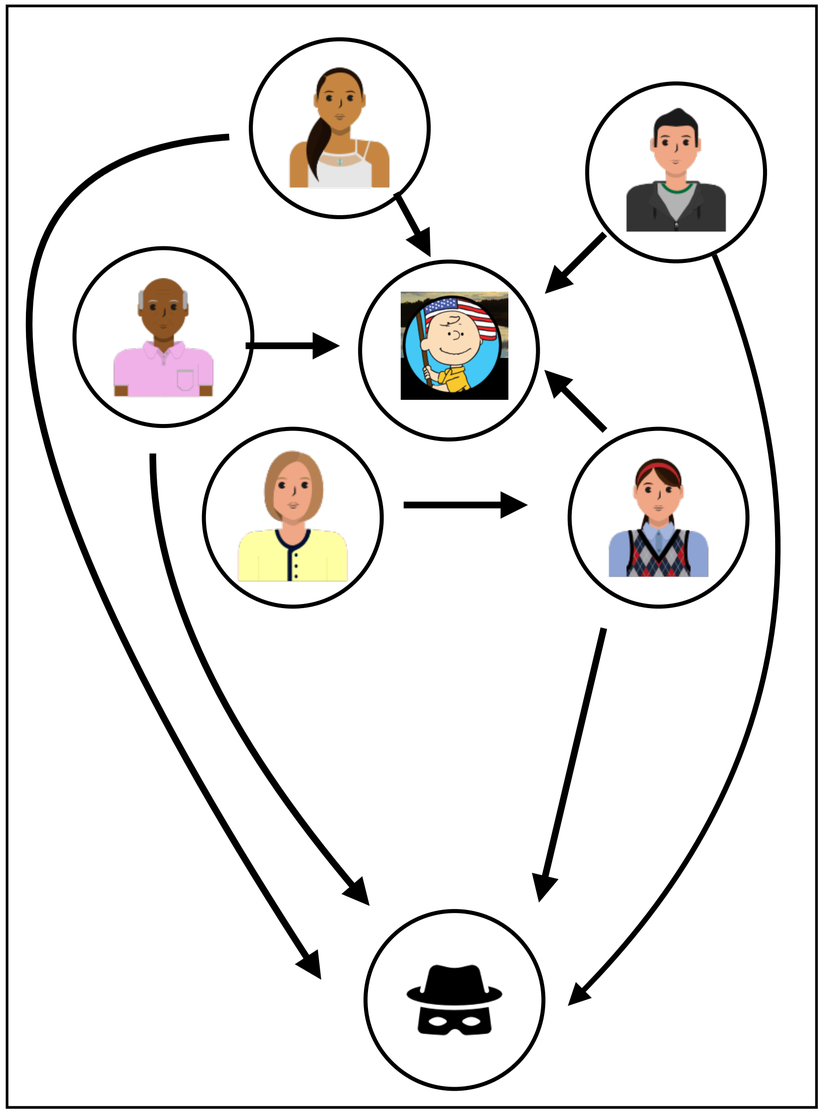
Suppose we just set up a new Twitter pseudonym and transfer all followers to that pseudonym.



	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 <u>all</u> followers

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



1 out of 1

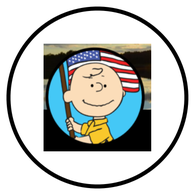
log2(1) = 0 bits of anonymity

	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?

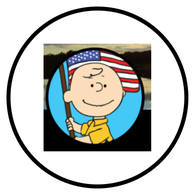


User profile data

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?

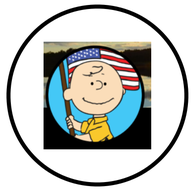


User profile data

Platform	Verification
User	Name, location, bio

Better approach: use ZK to transfer *some* info

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

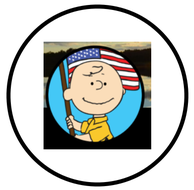


User profile data

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?

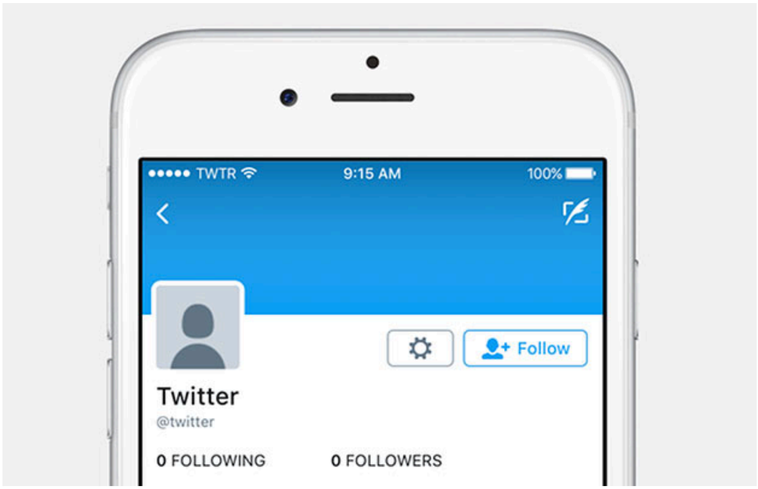


User profile data

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

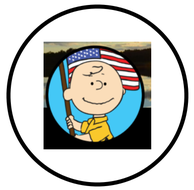
Via a zero knowledge construction
(like ZK Snarks for ZEC transfer)

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

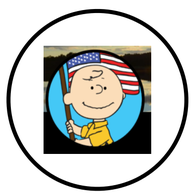
Platform	Verification
User	Name, location, bio
Others	Followers, likes, RTs

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

log2(1) = 0 bits of anonymity

Platform	-
User	-
Others	-

1 out of 330M MAUs

log2(330M) = 28.3 bits anonymity

Platform	Verification
User	-
Others	-

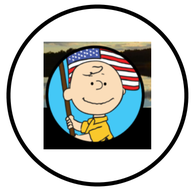
1 out of 330K Verifieds

log2(330K) = 18.3 bits anonymity

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

And we could port over multiple attestations

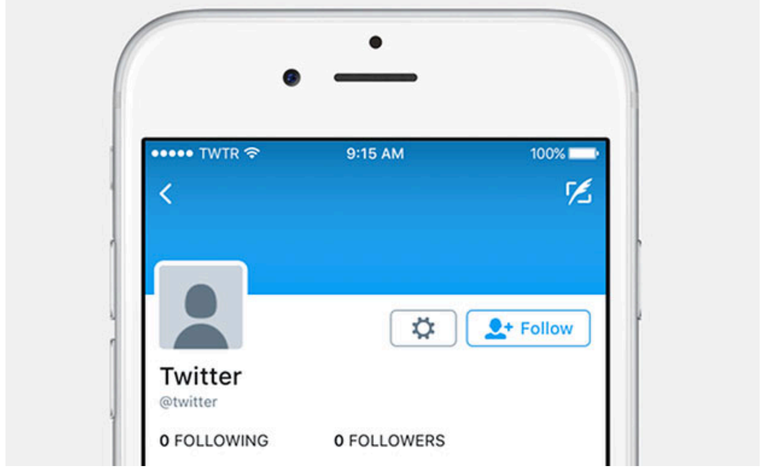
Each one gives some reduction in anonymity.



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

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

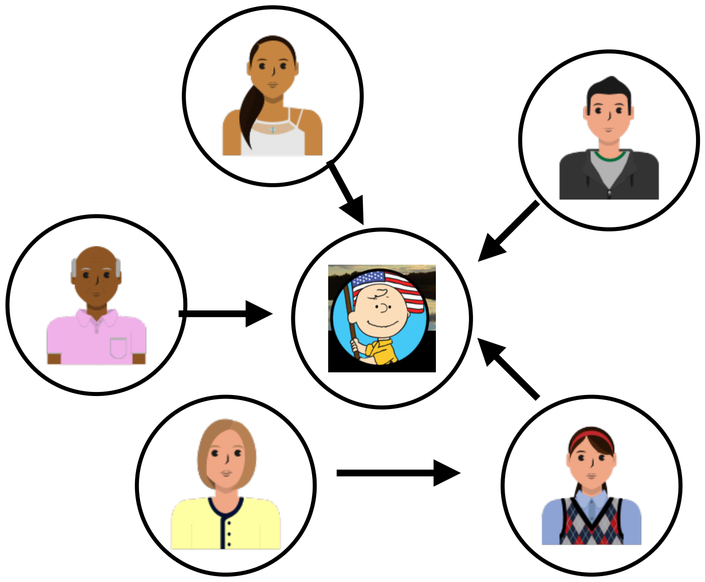
Platform	Verification
User	
Others	**>100k followers, followed by @jack, etc**



But how do we ensure folks still follow?

What about reputation? Autofollow.

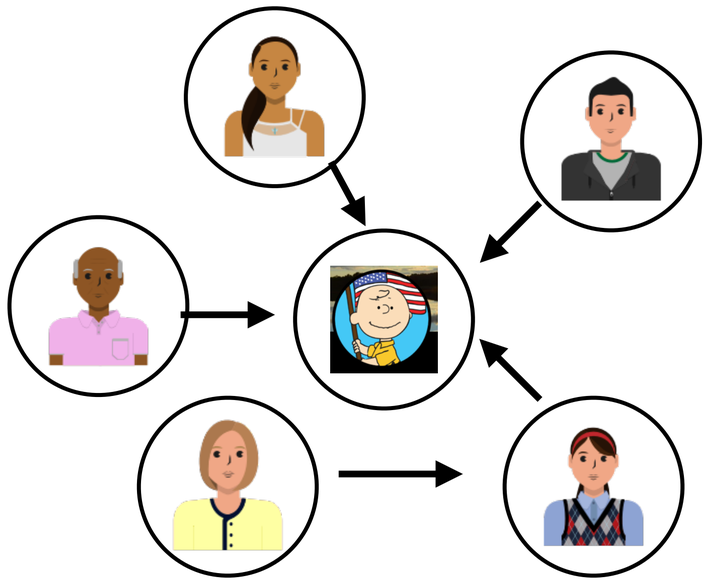
One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.



	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.

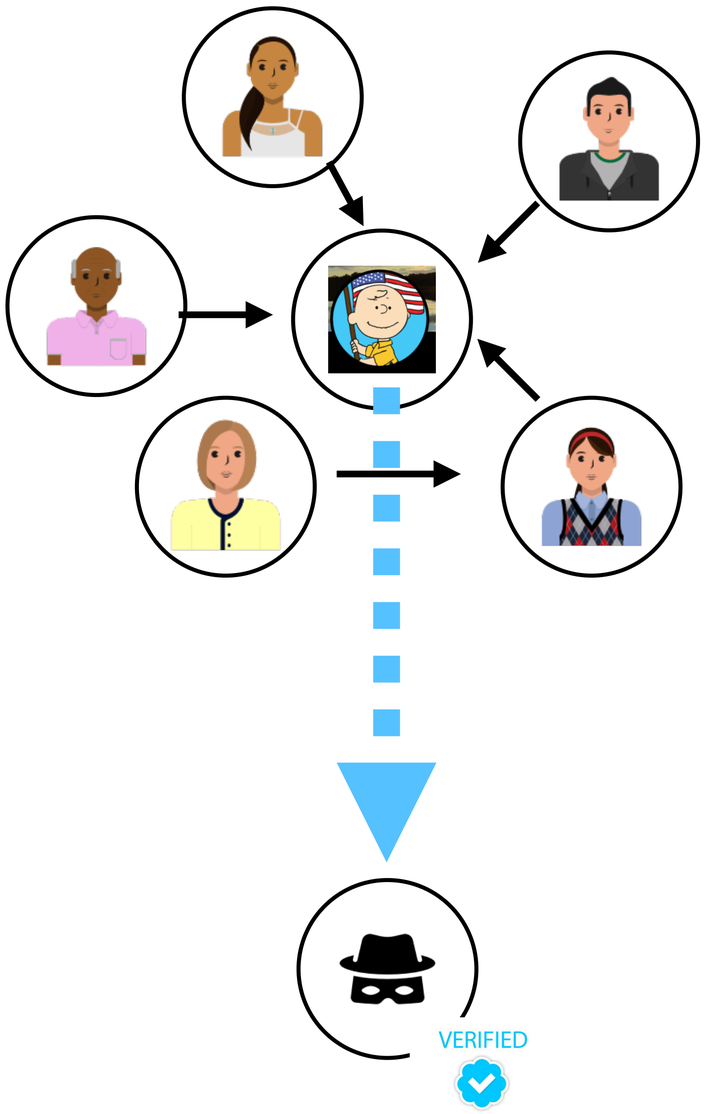
One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.



	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.

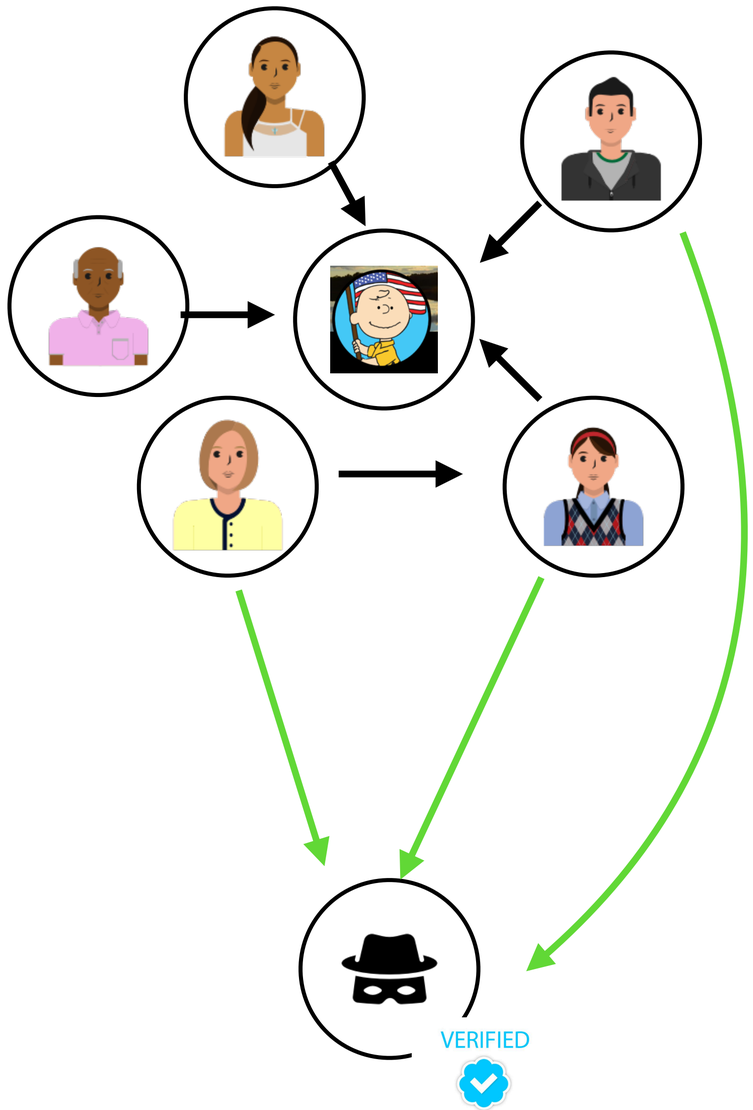
One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.



	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.

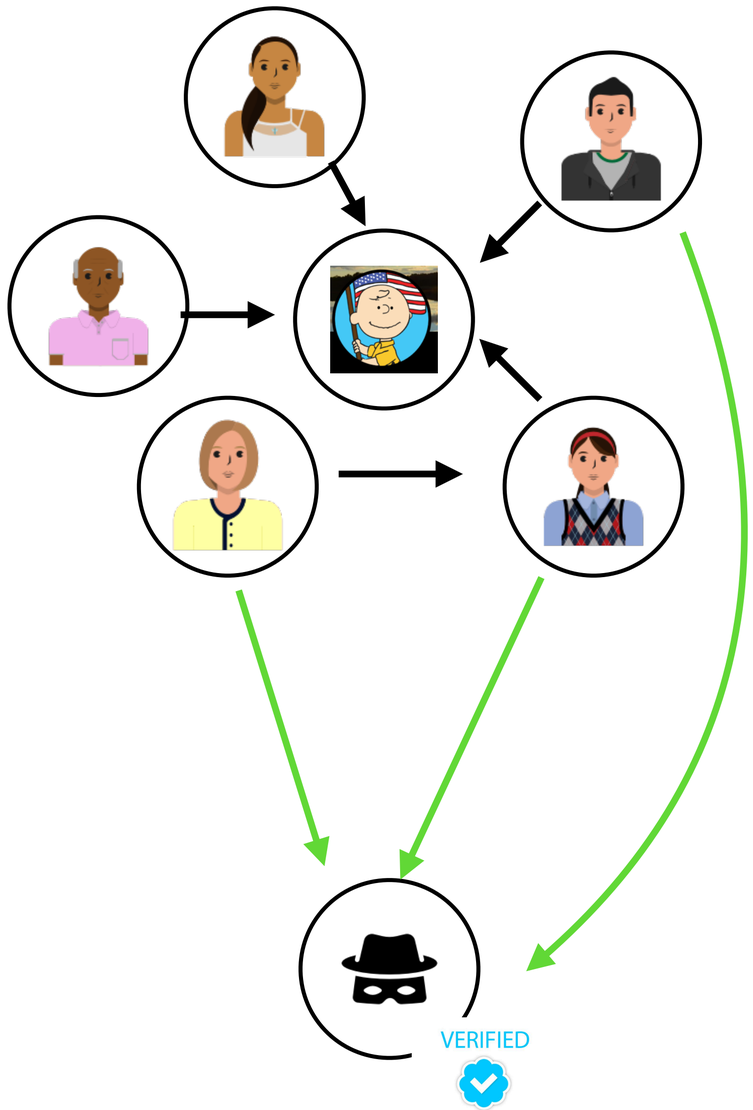
One more concept: assume that users are opted-in to *autofollowing* accounts with certain features.



	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.

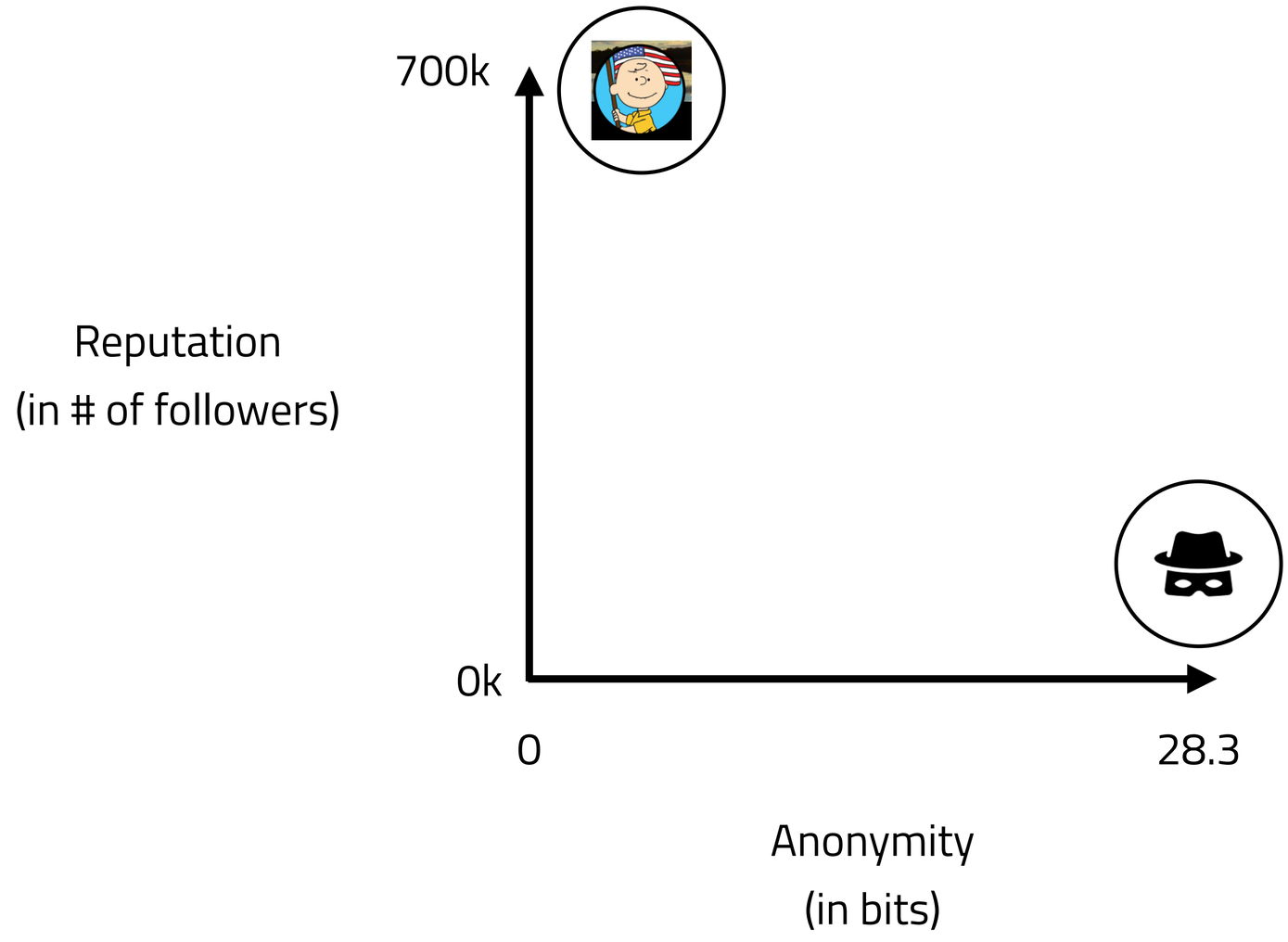


	Autofollow if verified?	Autofollow if >10k followers?	Autofollow if @jack follows?
	0	1	1
	1	0	1
	1	0	1
	1	1	1
	0	1	0
	0	1	1

Suppose **150k** accounts autofollow verifieds

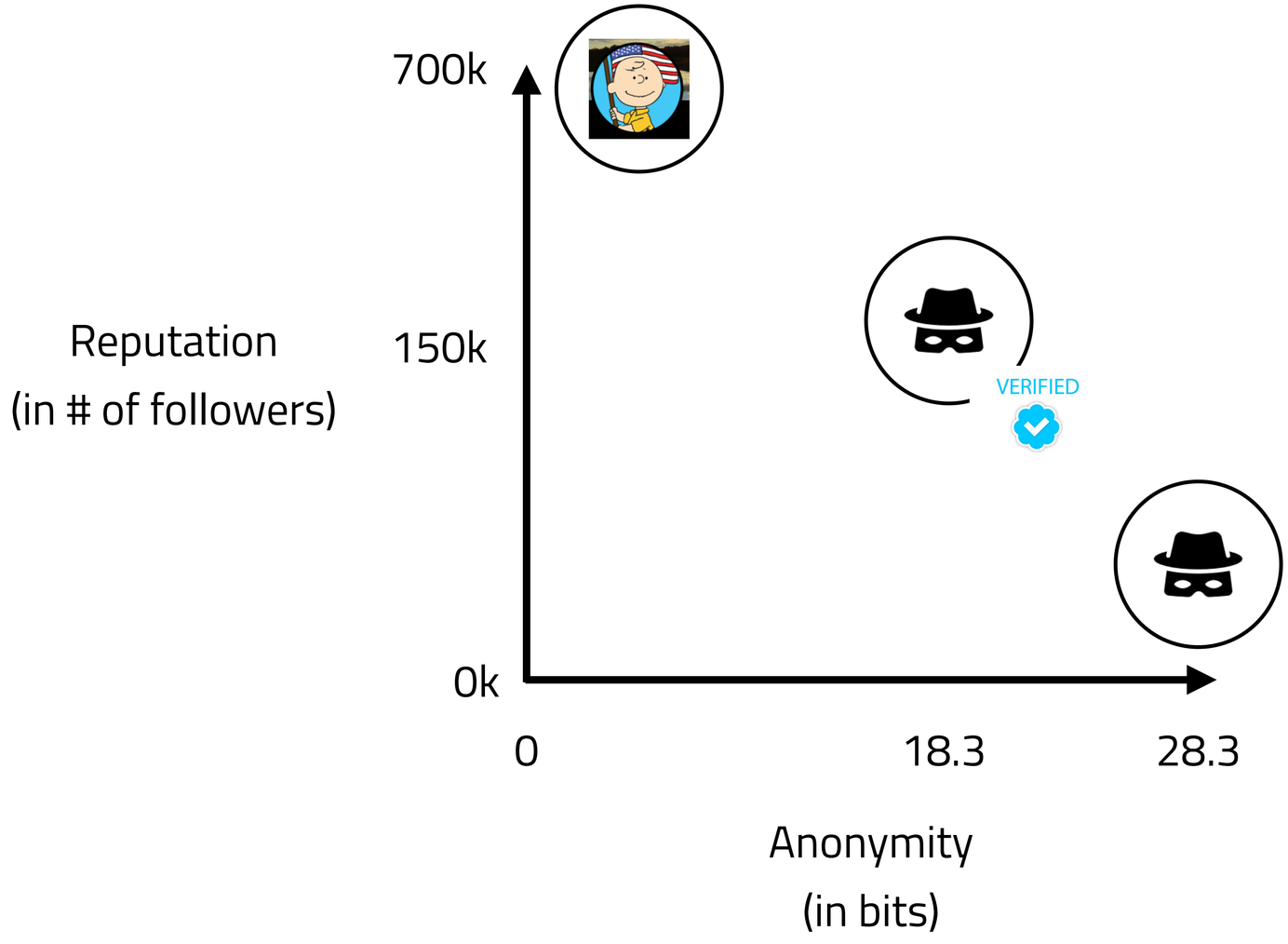
A quantifiable anonymity/reputation tradeoff

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



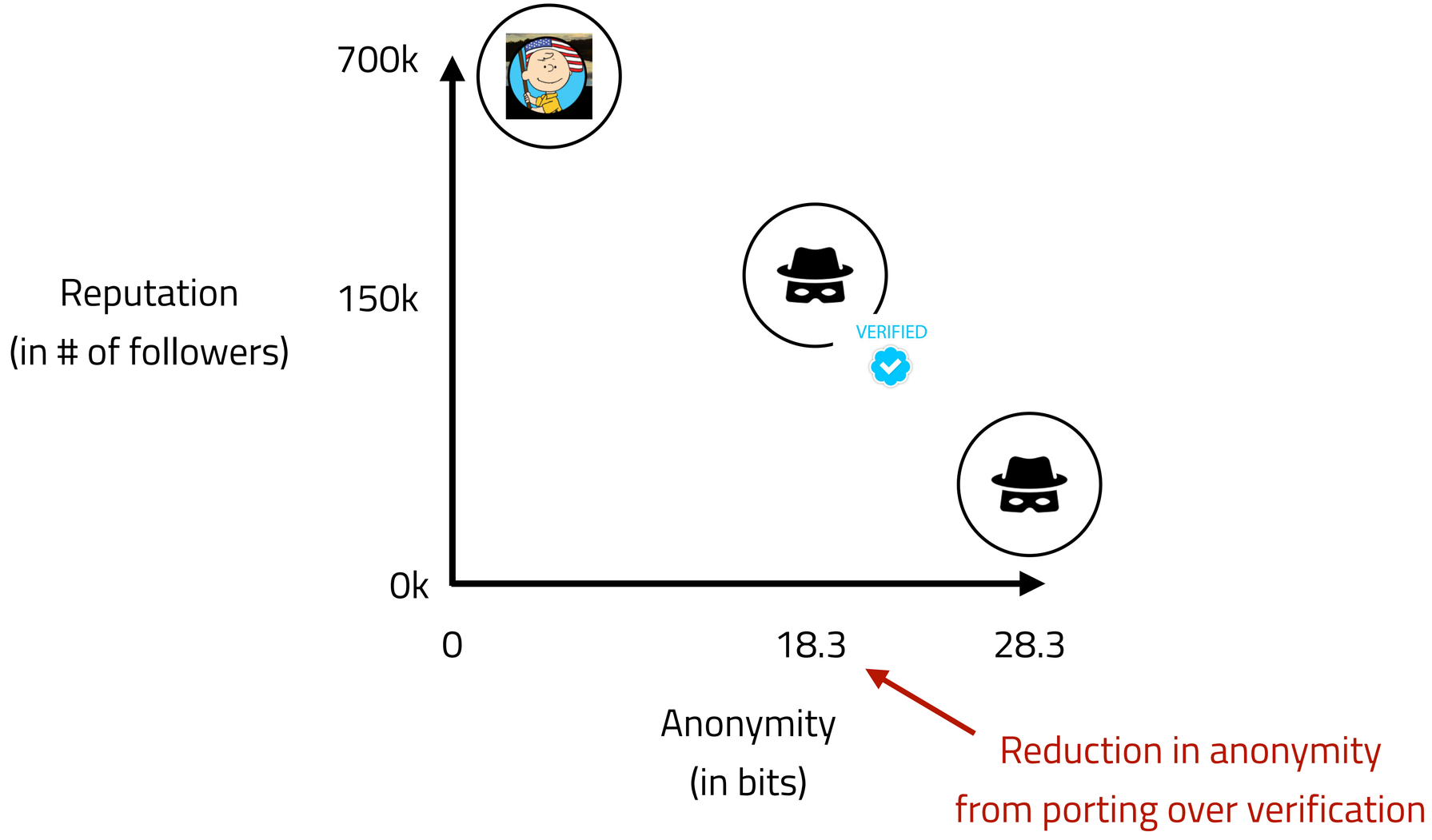
A quantifiable anonymity/reputation tradeoff

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



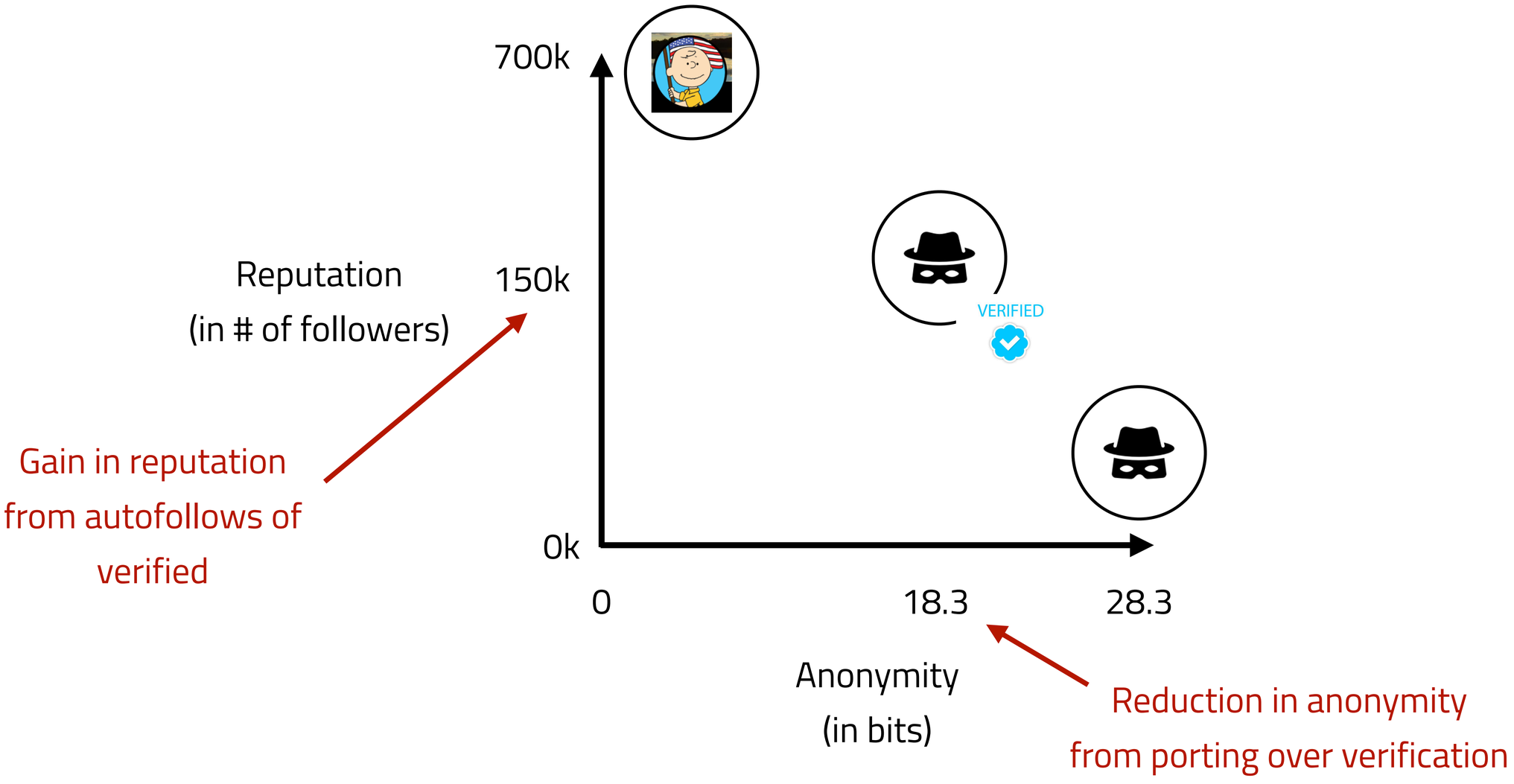
A quantifiable anonymity/reputation tradeoff

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



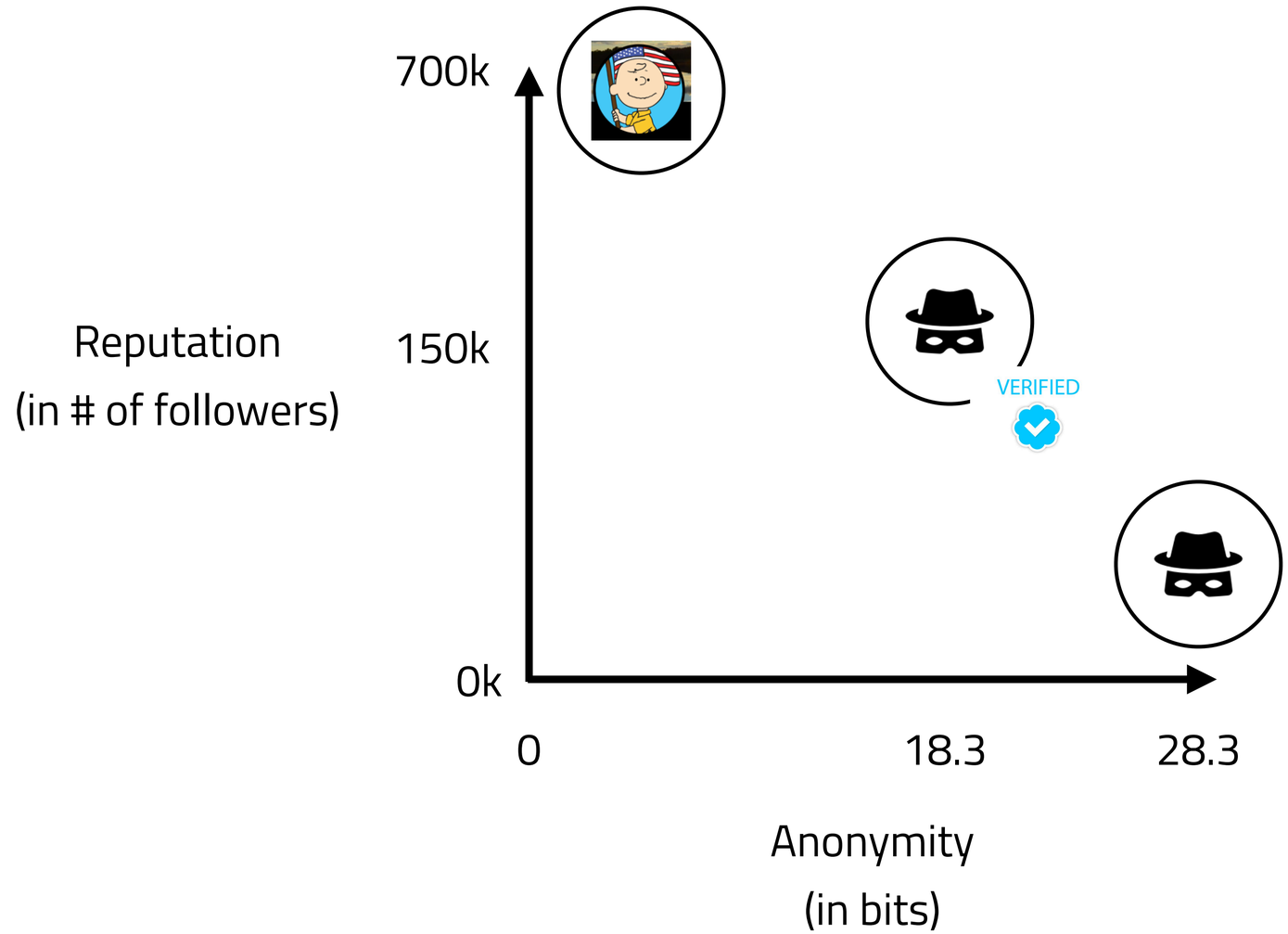
A quantifiable anonymity/reputation tradeoff

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

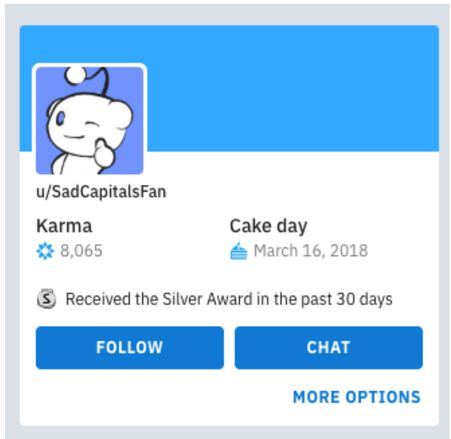
- Crypto domains, AI, ZK have all advanced
- Decentralized media exists, so can implement it there

Summary

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

Real names

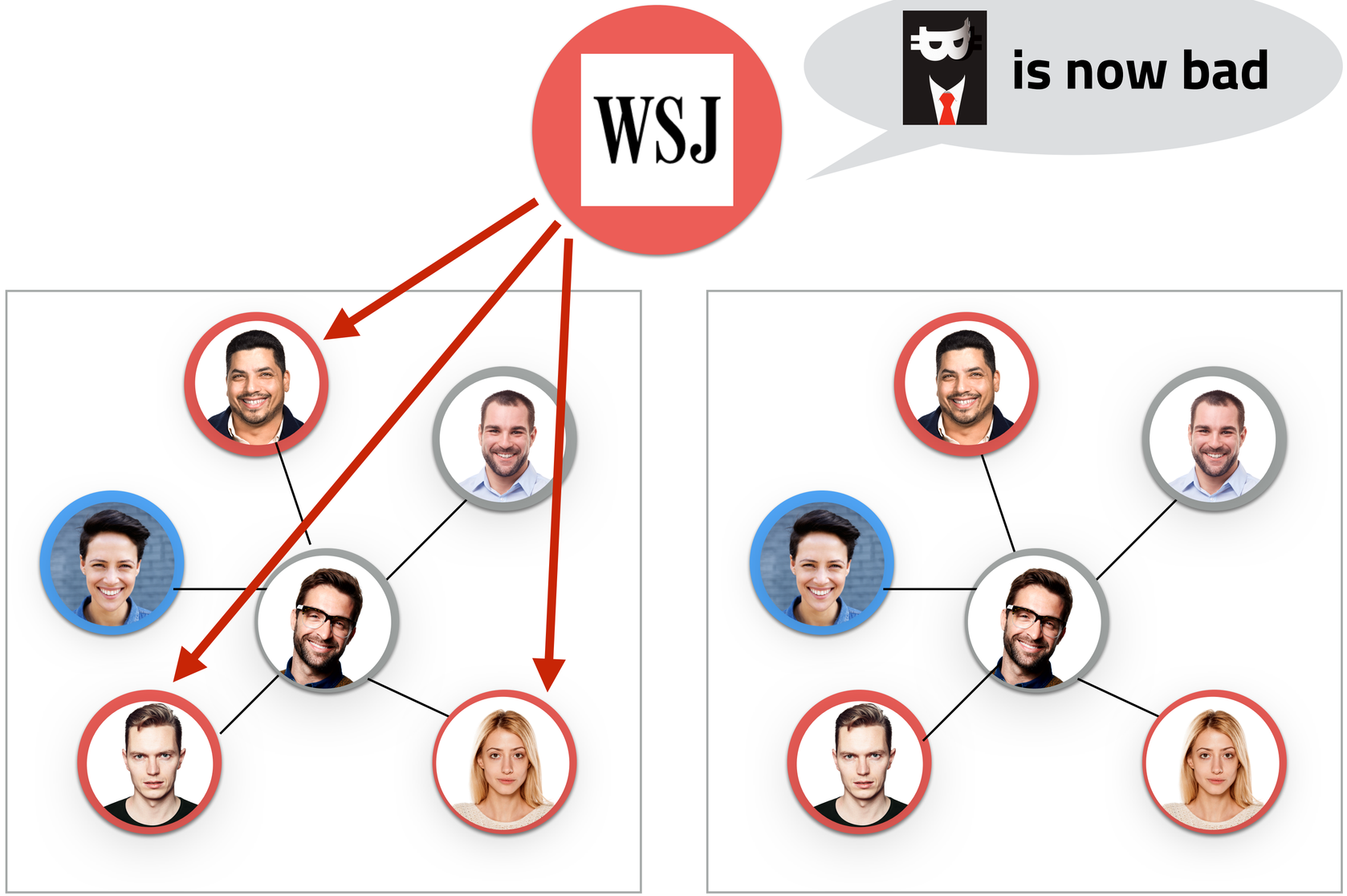
Pseudonyms



Anonyms

Summary

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



Summary

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

Earning

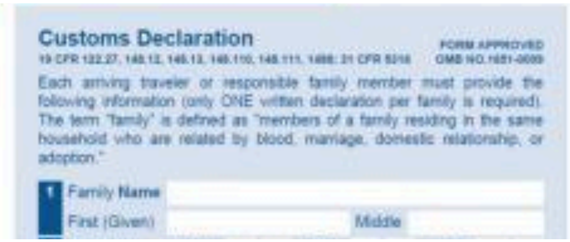
Tristan Su
foobar

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

Zcash

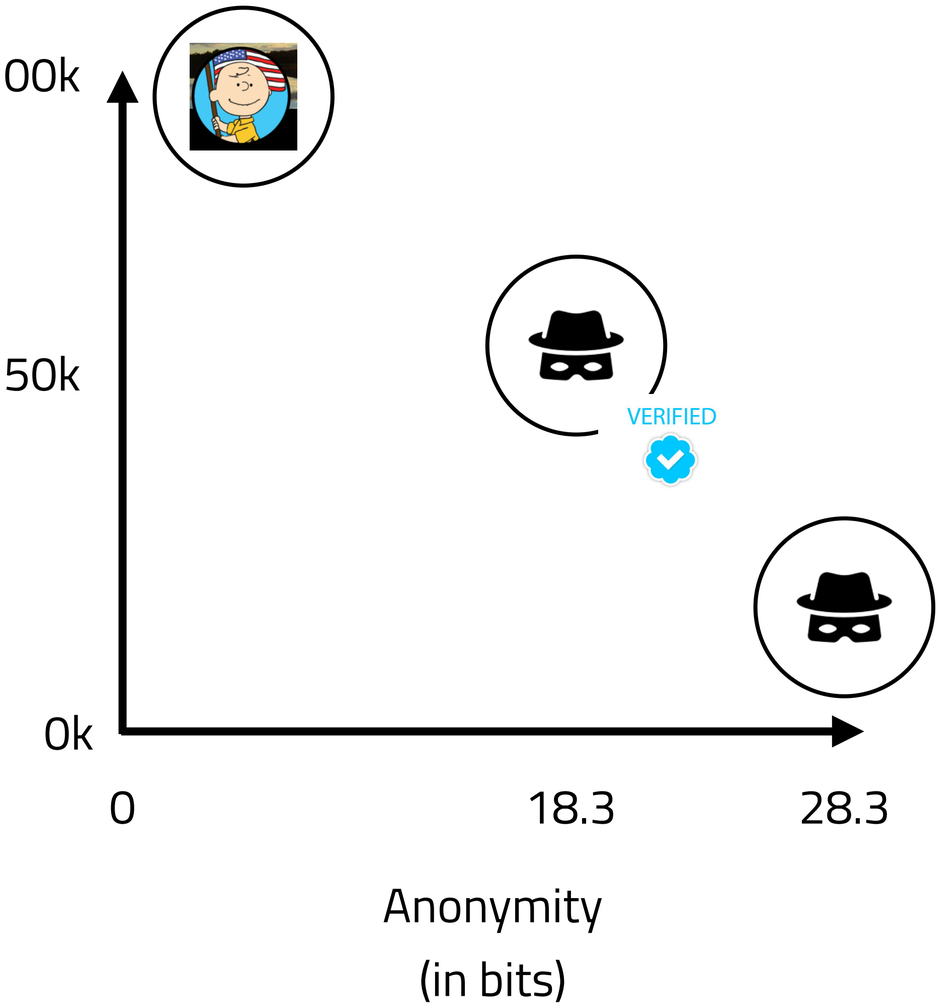
Speaking

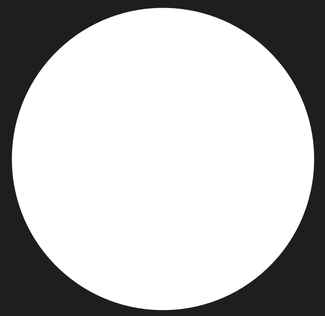
"Real" name



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/shra7mpYwTNcBfIwf