Twitter Thread by Ari Paul ■■

Ari Paul ■■
@AriDavidPaul

If you don't have firsthand experience with how traditional financial institutions (pensions, corporate treasuries etc) administratively permission the moving of assets, it's hard to understand why it's still very difficult for an institution to own bitcoin. Here's why: /1

2/ I worked at an endowment for 4 years, so I'll use the example I'm most familiar with. The Uchicago endowment had $8b and a staff of ~24 when I was there. The head of the endowment is the CIO, but he can't move money or assets by himself.

3/ when he wants to transfer cash or assets (let's say to invest endowment cash in to a VC fund), it follows a carefully controlled process to avoid theft or malfeasance.

4/ the cash itself sits with a custodian. The endowment must transmit and verify instructions to the custodian in a specific way to authorize its transfer. This is typically something like a document signed by multiple parties at the endowment and a phone confirmation.

5/ This process is not all that secure given the dollar amounts in question, but it works because of the financial infrastructure plumbing. Wire transfers are reversible (short-term), and they effectively use "whitelisting."

6/ if the bank received instructions to send $100m to some tiny russian bank, that would raise red flags and warrant extra scrutiny. It's very hard to get away with massive wire fraud since banks will only wire money to other banks that follow the same international laws and

7/ aml/kyc their customers. This produces a clear and simple chain of transfers of that $100m, and the slowness of the wire system makes it difficult to move the money fast enough to hide the trail.

8/ TLDR: it's very very hard to successfully steal and keep large amounts of fiat by wire fraud. It happens...but it's a tiny tiny % of wires. In contrast, how would this same process work with bitcoin?

9/ a successful social engineering attack could result in an instant $100m win for the thief, with no reversibility or recourse. Unlike with destination banks, a new bitcoin address isn't obviously questionable, and bitcoin addresses of users change, unlike bank accounts.

10/ Could the endowment just custody the bitcoin itself? How? Let's say $1b of bitcoin is on a hardware wallet. Who controls the wallet? The CIO gets unilateral and total control of $1b? That removes all the administrative controls and protections.

11/ you could implement an internal multisig scheme, but this introduces a long list of new risky attack vectors. For that $1b of bitcoin, what software is the endowment supposed to trust to run multisig, and why should they trust it? What hardware do they run it on?

12/ in 2017, we thought trezors were secure, then learned they could be hacked with a paperclip. It's trivial to install software or hardware keyloggers on most devices. Endowments aren't equipped to protect themselves from the most sophisticated spyware on the planet.

13/ this gets solved in two ways. A. Better authorization processes with crypto custodians and updating processes for that authorization at institutions, B. Investing in funds and third party products that hold the bitcoin for them.

14/ IMO, this is solved or close on the custodian side. We're a customer of @Anchorage for example, and they have an exceptional authorization process. Now, institutions need to get used to authorizing transfers on iphones with face ID and voice recognition.