The Key to Self-custody is Key Distribution

Ryan Grant, Digitial Contract Design
github.com/dcdpr
https://dcdpr.github.io/did-btc1/
2025-07-26

section: everything is fine

the custodian is doing a better job than i could

paper gold

EO-6102 (1933)

i run my own node

i have seed words

25th seed word!

i standardize

SPoF? 

"My daughter JUST dropped her phone in Puget Sound yesterday."

no, not *you* ubergeek

thesis: your digital security ==
other people's *ease of use*

section: Meatspace

what can people handle?

something you *know*

something you *have*

something you *are*

someone who *knows you*

time delay

intentional border control checkpoints

section: Meatspace Safety

what makes gold safe?

vaults, warehouses, guns, indestructibility

what scares off the normies?

highly technical scams, questioning inflation, *wrench attacks*

what makes fiat safe?

the Feds scare villains

"*Rollback!!*"

Bitcoiners use math to get a good custody result

when that math is *stifled*, wrench attacks are harder to design against

we don't really know what we're missing out on

section: What We Have

can we trust the chip makers?

enclave / TEE

intrusion detection has a knowledge problem

but combined with meatspace
you can make progress

Shamir's secret sharing

which *exact* implementation?

what is my recovery *protocol*?

Trezor released SLIP-39

wordlist...

note: assembly must be on one computer (an exfiltration SPoF)

wait, what is *my* recovery protocol?

interitance

i maintain my own complex recovery scheme

how do i communicate shards?

we already have PGP

which server do i trust to update my PGP key?

(...this question started Decentralized Identity)

section: Other Efforts

Bitkey

cosigner scheme with hardware and servers

you <-> AWS Nitro

cosigner sends SMS & email

email and SMS get hijacked all the time...

"Delay and Notify"
(7 days)

"An attacker with access to the customer's cloud account, access to the Recovery Contact's secret (either via their phone or cloud storage), a new Bitkey hardware device, and the ability to disable notifications for the Delay and Notify feature (e.g. by compelling Block or its employees) can steal funds."

however... Bitkey will replace the hardware key

.: to move funds on Bitkey, hack a cloud account, intercept communications for 7 days, trick one Recovery Contact, and intercept a package

they do not let you change those parameters

what happens when the Recovery Contact drops *their* phone in a lake?

section: Key Distribution

section: did:btc1

DCD is hiring!
Rust, C++, ML
< rgrant@contract.design >

https://dcdpr.github.io/did-btc1/