Bitcoin Basis 16 - Not your keys, not your bitcoin

"Not your keys, not your bitcoin", is a mantra often repeated by bitcoiners. It refers to private keys as protection against counterparty risk.

You'll need your private key to protect bitcoin, prove ownership, sign messages and transfer bitcoin.

In contrast, if you let a third party manage your bitcoin, you'll stop owning it. This third party, then possesses the private keys of their address, holding your formerly owned bitcoin.

Such parties all claim to be safe, secure and reliable services, until they fail you. And ..., they wìll fail you hard.

Indeed, trusting such services is a huge counterparty risk.

Many such exchanges and services have stolen funds though inside jobs, or simply vanished. Some started asking ridiculous fees holding your coins, or were hit by hacks or government seizures. On top of that they're usually a privacy nightmare.

Services often promise yield or other proceeds in order to lure you in to signing up and sending them your bitcoin. Taking such an offer is downright dumb. It's akin to grabbing a free candy bar in the middle of a minefield

Instead, take ownership. "Not your keys, not your bitcoin" promotes personal responsibility, in line with bitcoin's decentralized nature.