Holdfast

Solo build by Oh-Jay (jayejone), with AI coding tools



hodlfast.vercel.app

jayejone

Oh_Jay0

Holdfast

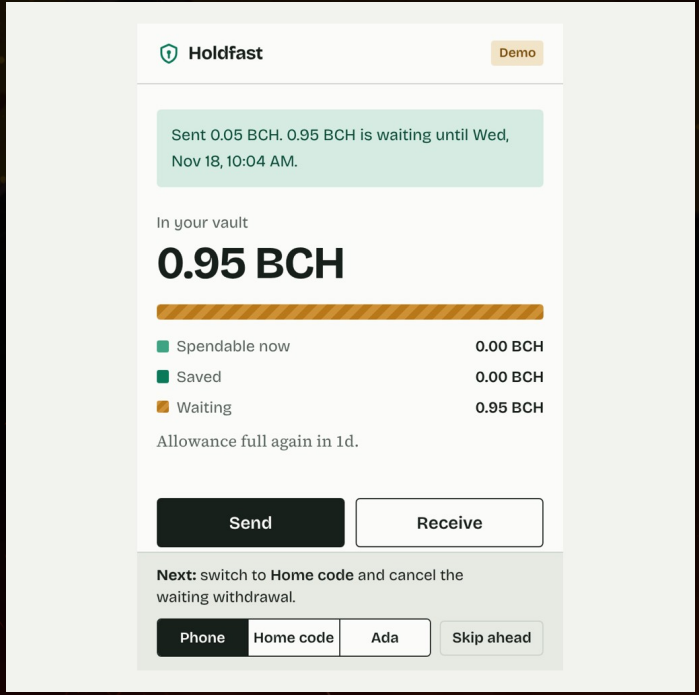
A Bitcoin Cash vault a robber can't empty

https://github.com/ohjay-official/holdfast

The Story of Holdfast

In Lagos, robbers can make you unlock your phone and send your money on the spot. Banks are adding panic PINs. Crypto has decoy wallets and some smart-wallet spending limits, but nothing on Bitcoin Cash that limits what a forced phone can send.

So I put the limit in the money itself. Whoever holds your phone gets a small allowance. The rest waits days, and you can stop it from home.



Benefits of Holdfast

- A robber with your phone gets just the allowance
  - Bigger withdrawals wait days
  - Home code or guardian can cancel
- A duress PIN freezes the vault quietly
- Lose your phone, keep your savings
  - Recover with home code and guardian



BCH Usage

The vault is a CashScript contract, signed with Paytaca over WizardConnect.
CashToken NFTs carry its state, and relative time locks enforce every wait.

```
// Anyone can release a withdrawal, but only after the wait,
// and only to the recipient recorded when it started.
function release() {
    require(this.age >= waitBlocks);
    bytes tag, bytes recipient = tx.inputs[this.activeInputIndex].nftCommitment.split(2);
    require(tx.outputs[0].lockingBytecode == recipient);
    require(tx.outputs.length == 1);
}
```

The Vision for Holdfast

- Real vaults on mainnet, inside Paytaca
  - A small one-time fee per vault
  - Telegram alerts when money starts to move
- Next: a guardian service for people without one
- Goal: a robbery limit in every phone wallet



THA
YO

