

THOU MUST CUSTODY



FOR THINE LIBERTY

Why identity matters in web3

Arthur Gousset - Product at cLabs

READ + WRITE + OWN



cdixon.eth
@cdixon

web1: 1990-2005

read

web2: 2005-2020

read + write

web3: 2020-

read + write + own

6:43 AM · Dec 30, 2021 · Twitter for iPhone

BUT **WHO** OWNS WHAT

AND **HOW** ARE THINGS OWNED



private key = random 60 hexadecimal characters

fffebaaedce6af48a03bbfd25e8cd036415f

public key = generated using **private key** and Elliptic Curve Digital Signature Algorithm

public address = last 40 characters of keccak-256 hash of **private key** + 0x at beginning

keccak_256(public_key) =
ddd12d393dc462f92f8308ddba81d46535125b590cee325c0c62b9122fa48f3b

0x + ~~ddd12d393dc462f92f8308dd~~ ba81d46535125b590cee325c0c62b9122fa48f3b

0xba81d46535125b590cee325c0c62b9122fa48f3b

THIS IS YOU

THIS IS YOU TOO → **+44 79 8756 4578** (maybe?)

(Celo TLDR:

- *mobile phone focus*
- *payment focus*
- *environmental focus*

)

SMART CONTRACT REGISTRY

+44 79 8756 4578	0x4737f30dC6...
+254 732 054 829	0x6b6cd1D6D...
+55 955 214 2955	0x7a8019887...
+1 202 555 0156	0xd8C68eBeC...
+234 7067 4229	0x1f1788b096...
+33 93 867 8347	0xdff75a3b93f...
...	...

private key = random 60 hexadecimal characters

Ffffffffffffffffffffffffffffffffffffffebaaedce6af48a03bbfd25e8cd036415f

24-word mnemonic phrase to recover the private keys:

shallow fine six jaguar cricket width aspect topic mystery east
erase path taxi sample undo thought neutral peasant quality mango
truth canvas test great



DON'T LOSE THIS

If you own something, you might want a say about how it should be **governed**

- **1-token 1-vote**: weighted by **wealth** (maybe suboptimal?)
- **1-person 1-vote**: weighted by **individual** ← **BUT WHO IS AN INDIVIDUAL?**

0xba81d46535125b590cee325c0c62b9122fa48f3b

(remember, this is you)

Sybil attack

From Wikipedia, the free encyclopedia

A **Sybil attack** is a type of attack on a computer [network service](#) in which an attacker subverts the service's reputation system by [creating a large number of pseudonymous identities](#) and uses them to gain a disproportionately large influence. It is named after the subject of the book *Sybil*, a case study of a woman diagnosed with [dissociative identity disorder](#).^[1] The name was suggested in or before 2002 by Brian Zill at