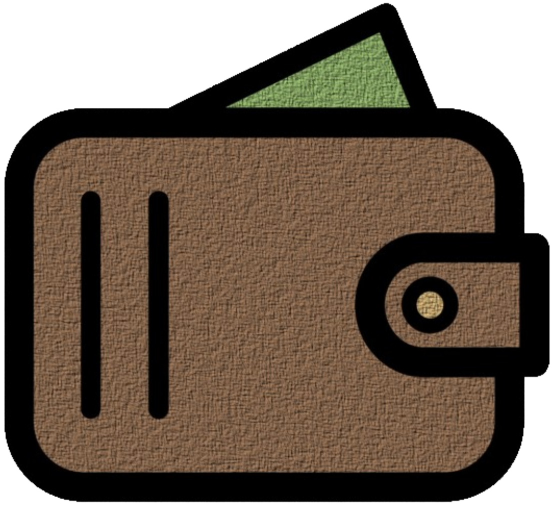
BLOCKCHAIN ADDRESSES, ACCOUNTS, AND WALLETS



(let’s start using those words correctly)

by Keir Finlow-Bates
#blockchaingandalf

BLOCKCHAIN HAS A TERMINOLOGY PROBLEM

In an attempt to make it more accessible to the public, words from banking have been borrowed to provide an analogy between finance and blockchain.

✉️ *Address*

💳 *Account*

💼 *Wallet*

But the analogies are not perfect, and they can lead to misunderstandings.

Let’s start unpacking them...

ADDRESSES

A blockchain **address** is a string of numbers and/or letters that are used to record specific ownership of assets (crypto or tokens) on a blockchain.

For example, here is a Bitcoin address holding 50 Bitcoin:
`12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX`

And here is an Ethereum address owning 5149.6 ETH and over $1M in tokens:
`0xd8dA6BF26964aF9D7eEd9e03E53415D37aA96045`

Who	What			
	ETH	DAI	USDT	BAT
0xd8d...045	5,149.6227201	27,182.12588	70.23	17.4672

In both cases, the blockchain is functioning as a ledger, with the address acting as a key (the “who” column of the ledger), and values being recorded against that key (the “what” and “how much” columns of the ledger).

ADDRESSES (an analogy)

You can think of a blockchain **address** as a bank **account number**.

You can use a bank account number to look up a balance (if you work at the bank or it’s your account), or you can send money to a bank account number.

And blockchains are like banks where anyone can examine the ledger of balances[1].

[1] Except for privacy blockchains like Monero and Zcash, but that’s a different story for another day

ACCOUNT

I have been unable to find a clear definition of what a **blockchain account** is, so I'm going to provide one.

In banking people use "account" and "account number" interchangeable – when they say:

"Can you transfer 50€ to my bank account",

what they mean is

"Can you transfer 50€ to this bank account number, which belongs to me."

I like to think of a blockchain **account** as the collection of your private key, public key, and blockchain address.

Which means I have to briefly explain asymmetric key cryptography...

ASYMMETRIC KEY CRYPTOGRAPHY

1️⃣ You generate a large random number. That’s your private key (keep it secret).

2️⃣ Using a cryptographic algorithm, you derive the public key from the private key.

3️⃣ Using a blockchain address algorithm, you derive the address from the public key.

Or rather, your blockchain **wallet** software does all this for you.

Private Key ⇨ Public Key ⇨ Blockchain Address

Each derivation is one-way: you can’t compute the private key from the public key, and you can’t compute the public key from the blockchain address.

Through digital signing with the private key you can prove you own the public key, and hence the blockchain address, and therefore the things recorded on the blockchain as being owned by that blockchain address.

WALLET

A wallet is some software (and perhaps some hardware too) whose primary purpose is to generate, store, manage, and protect your private keys.

It also derives your corresponding public keys and blockchain addresses.

Which means it “holds” your accounts.

A wallet is therefore more like a password manager:

It holds your all your passwords (your private keys)

And their corresponding usernames (your public keys)

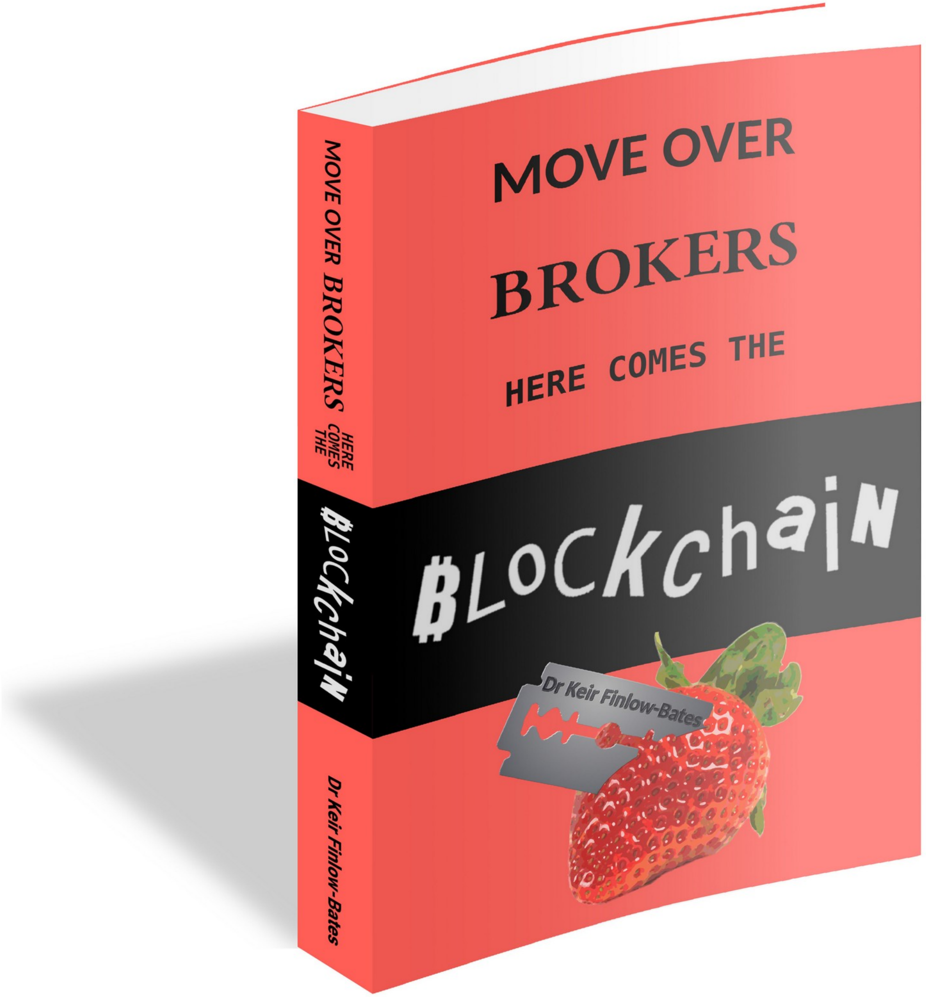
MISNOMERS

Incorrect	*Correct*
Paper **wallet** (A piece of paper does not generate private keys, nor can it send transactions.)	Paper **account** (The paper shows your private key, and usually your public key or corresponding blockchain address)
I can see my coins in the hacker’s **wallet**	I can see my coins in the hacker’s **address**
Send the funds to my **account**, which is ...	Send the funds to my **address**, which is ...
I’ll set up a new **wallet** and share it with you	I’ll set up a new **account** and share the **address** with you
I stupidly gave my seed phrase to the hacker, and now they have my **account**	I stupidly shared my seed phrase with the hacker and now they control my **wallet**
I lost the seed phrase to my **address**	I lost the seed phrase to my **wallet**, and now I don’t know what the private keys for my **accounts** are

THAT’S IT

Now you can have fun
pedantically correcting people
who use **wallet**, **account**, and **address** wrongly.

FOUND THIS USEFUL?



Why not pick up a copy of my book, which explains the rest of blockchain in a similar simple manner:

https://mybook.to/moveover

Thanks for reading!

Keir Finlow-Bates