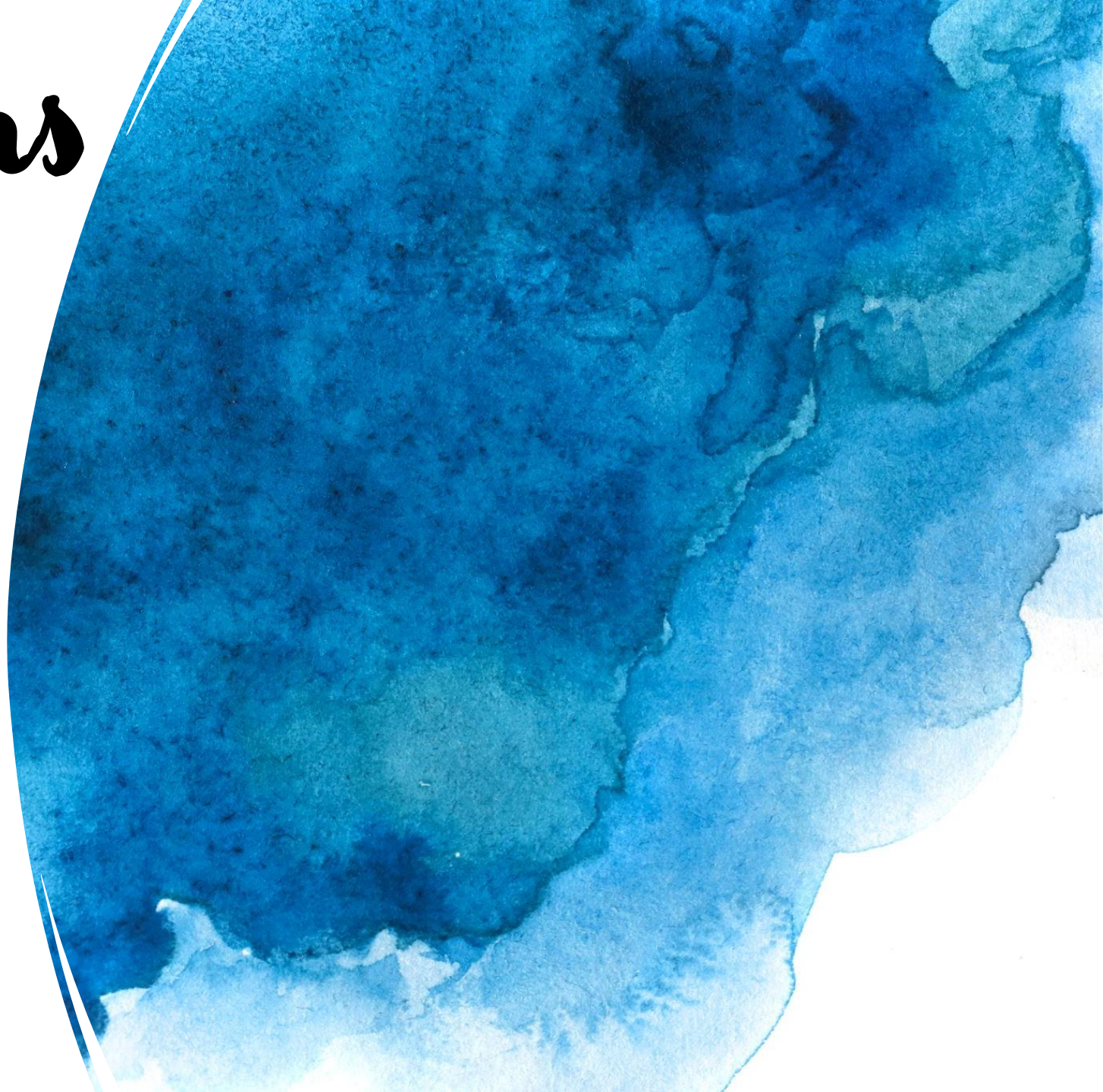
Security Tokens
The need for privacy and compliance

JP Aumasson, CSO https://aumasson.jp

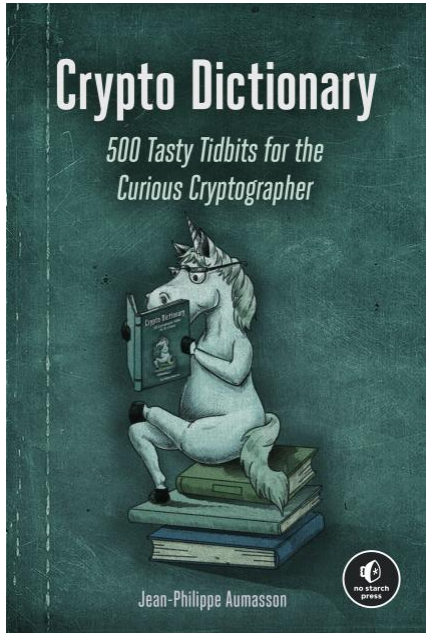
TAURUS

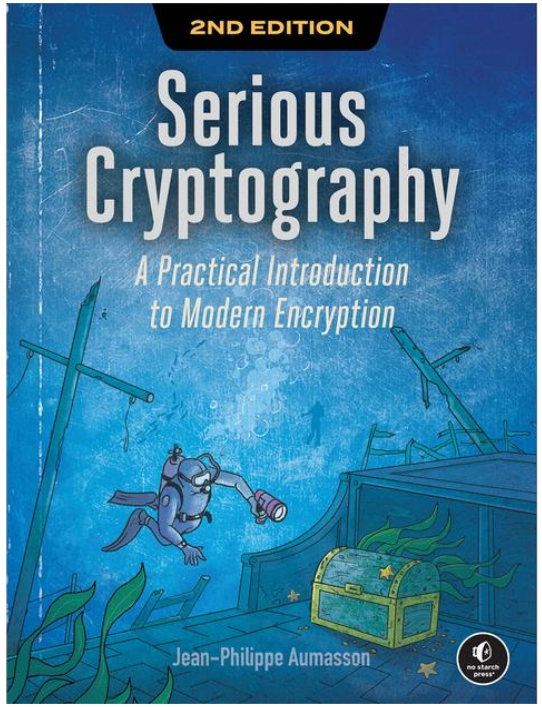
MERGE BUENOS AIRES MADRID



¿Quién soy?

- Cofounder & CSO of Taurus, the crypto custody tech for banks
- 20 years in applied cryptography
- French living in Switzerland
- x.com/veorq





Privacy

Imagine a future where anyone on Earth could see...

- Your whole Google search history
- All your LLM interactions (ChatGPT etc.)
- All your private WhatsApp messages

Should this be the "Future of Internet"?

Privacy

Imagine a future where anyone on Earth could see...

- All the bank accounts you have, your salary, your savings
- The investments you made (funds, stocks, ETFs, etc.)
- Who you transfer money to

Should this be the "Future of Finance"?

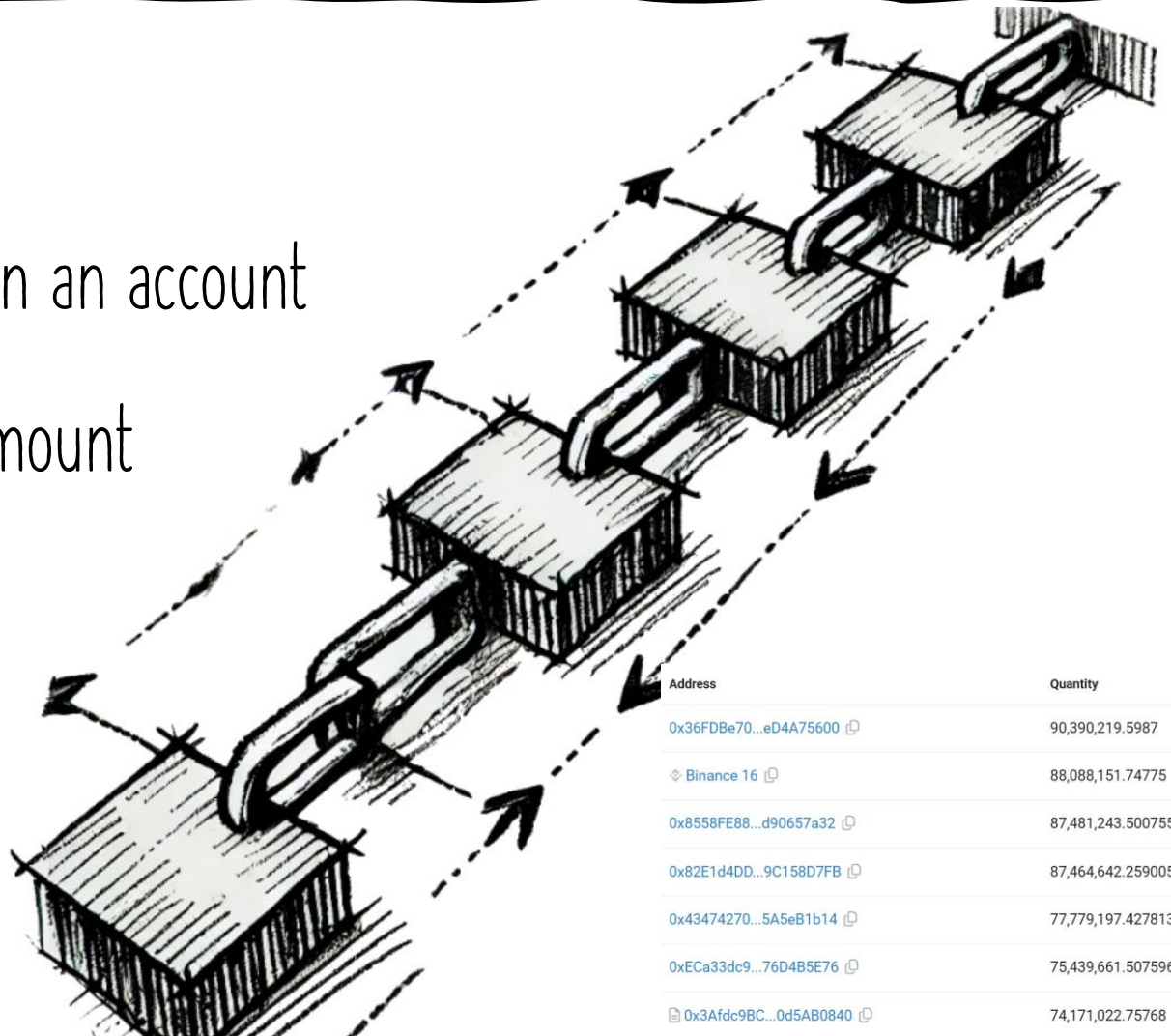
Blockchain tokens NOW

Anyone can trivially see

- Balances: how many tokens on an account
- Transfers: sender, recipient, amount

OK for scam tokens

Not OK for real finance



Address	Quantity
0x36FDBe70...eD4A75600	90,390,219.5987
Binance 16	88,088,151.74775
0x8558FE88...d90657a32	87,481,243.500755
0x82E1d4DD...9C158D7FB	87,464,642.259005
0x43474270...5A5eB1b14	77,779,197.427813
0xECa33dc9...76D4B5E76	75,439,661.507596
0x3Afdc9BC...0d5AB0840	74,171,022.75768

Blockchain tokens NOW

Anyone includes...

- Organized crime

- Any foreign entities
- Any government agencies
- Business partners, clients
- Friends, neighbors, colleagues

Address	Quantity
0x36FDBe70...eD4A75600	90,390,219.5987
Binance 16	88,088,151.74775
0x8558FE88...d90657a32	87,481,243.500755
0x82E1d4DD...9C158D7FB	87,464,642.259005
0x43474270...5A5eB1b14	77,779,197.427813
0xECa33dc9...76D4B5E76	75,439,661.507596
0x3Afdc9BC...0d5AB0840	74,171,022.75768

"Security" token?

Unlike most tokens, not a Ponzi token (at least in principle)

Tokenized representation of regulated, real-world financial instruments such as

- Bonds
- Equity stock
- Private credit notes
- Structured products

https://www.ft.com/content/dd020b5d-d031-4122-a488-ba7241b7f70d

Security tokens on private chains

Permissioned/private ledgers bring greater privacy and efficiency

> It is perhaps less well appreciated that these kinds of blockchains are also plagued by governance problems. We cannot simply trust in the code of the blockchain. Public permissionless blockchains are "designed by people, maintained by people, and governed by people", as one research paper put it. but we don't necessarily know who these people are, who pays them, or if they'll show up in an emergency. This is an untenable position for critical financial infrastructure.

https://www.ft.com/content/4c3ebc9f-d447-466a-8816-d4a166143029

Security tokens on public chains

Often on public chains (mostly Ethereum) for convenience and interoperability

FINANCIAL TIMES

ETF Hub Exchange traded funds + Add to myFT

Janus Henderson to follow BlackRock and Fidelity into tokenisation

Fund group's move to manage Anemoy fund means it is joining a trend that observers believe will disrupt the industry

https://www.ft.com/content/648f2249-5783-4e98-8412-4056f56ad1b0

Security token standards

CMTAT – https://github.com/CMTA/CMTAT

- Modular, powerful cross-chain token (EVM, Tezos, etc.)
- Simple and cheap to deploy, actively developed
- Permissive licensing scheme


STANDARD

CMTA Token (CMTAT)

February 20, 2025

Summary

The CMTA Token (CMTAT) is a framework enabling the tokenization of equity and debt securities, including structured products.

The CMTAT is the product of collaborative work by leading organizations in the finance and technology ecosystem.

ERC-3643 – https://github.com/TokenySolutions/T-REX

- Fixed EVM-oriented specification
- Includes identity-management
- Code GPL license

ERC-3643: T-REX - Token for Regulated EXchanges

An institutional grade security token contract that provides interfaces for the management and compliant transfer of security tokens.

Authors	Joachim Lebrun (@Joachim-Lebrun), Tony Malghem (@TonyMalghem), Kevin Thizy (@Nakasar), Luc Falempin (@lfalempin), Adam Boudjemaa (@Aboudjem)
Created	2021-07-09
Requires	EIP-20, EIP-173

Private cryptocurrencies exist

Zcash, https://z.cash

- Token ZEC: "shielded" tokens hide amounts, sender, recipient in a transfer
- "zcash sapling was the appollo project of cryptography" @hdevalence
- Based on **zero-knowledge proofs** (ZKPs)

Only ZEC token, not designed for compliance and securities tokenization

From private tokens to private programs

Principle: the program (smart contract) and its inputs are "encrypted"

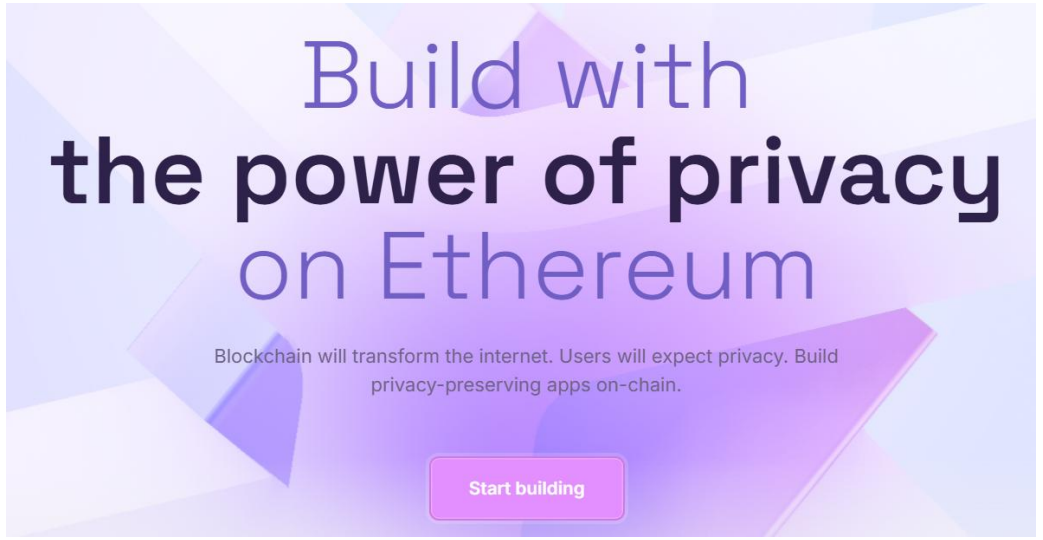
Several ongoing projects, for example by Aleo, Aleph Zero, and Aztec

"ZK rollups" are not designed for privacy, but scalability

Thus a ZK rollup layer 2 leaks transaction data

Our approach

- Start from CMTAT, the most versatile and modular security token
- Adapt it to run on Aztec, the private layer 2 https://aztec.network



From Solidity to Noir

Aztec private programs must be coded in Noir, a Rust dialect

```
fn _transfer_internal(from: AztecAddress, to: AztecAddress, amount: Field) {
    assert(!storage.enforcement_module.is_frozen(from), "Frozen: Sender");
    assert(!storage.enforcement_module.is_frozen(to), "Frozen: Recipient");
    storage.validation_module.operateOnTransfer(from, to);

    let issuer = storage.issuer_address.get_current_value_in_private();

    decrement(storage.balances.at(from),amount,from,issuer,from);
    increment(storage.balances.at(to),amount,to,issuer,from);
}
```

Features of our private token

- Private (encrypted) **transfers**, **mint**, and **burn**
- **Auditability** of transfers by the token issuer
- Transfer **restriction**, via blacklisting/whitelisting
- Public **pause** (of the contract) and **freeze** (of addresses)

Open-source at https://github.com/taurushq-io/private-CMTAT-aztec/

Testing it

- Now runs in Aztec's testing environment
- Soon in testnet, later in mainnet
- Extensive documentation

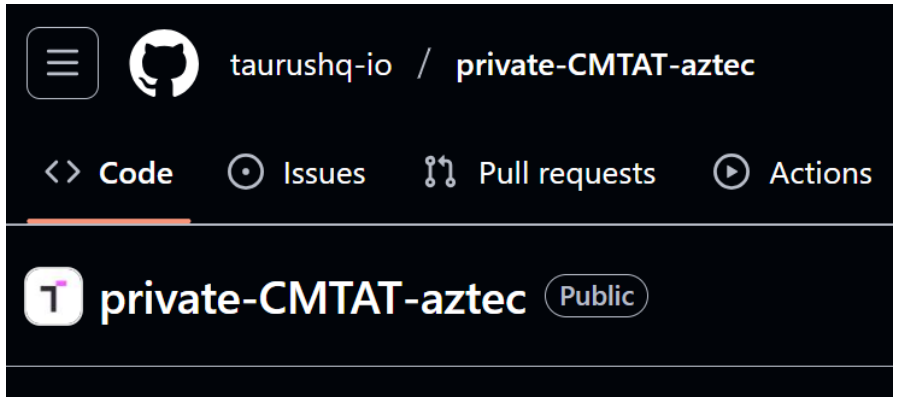


Table of contents

Conclusion

- Tokenization of securities can now be done
    1. On a public blockchain
    2. Preserving privacy and compliance
- To run our token, Aztec testnet soon, mainnet later this year
- Alternatives to public chains: private ledger systems (e.g. Canton)

¡Gracias!

Questions?

JP Aumasson, CSO https://aumasson.jp

TAURUS

https://taurushq.com