HOW CRYPTO IS BROKEN

…and why we need open silicon to fix it

WHERE ARE THE USERS?

WIRED

Weaknesses in bitcoin's underlying technology slow processing times, and spawn big fees.

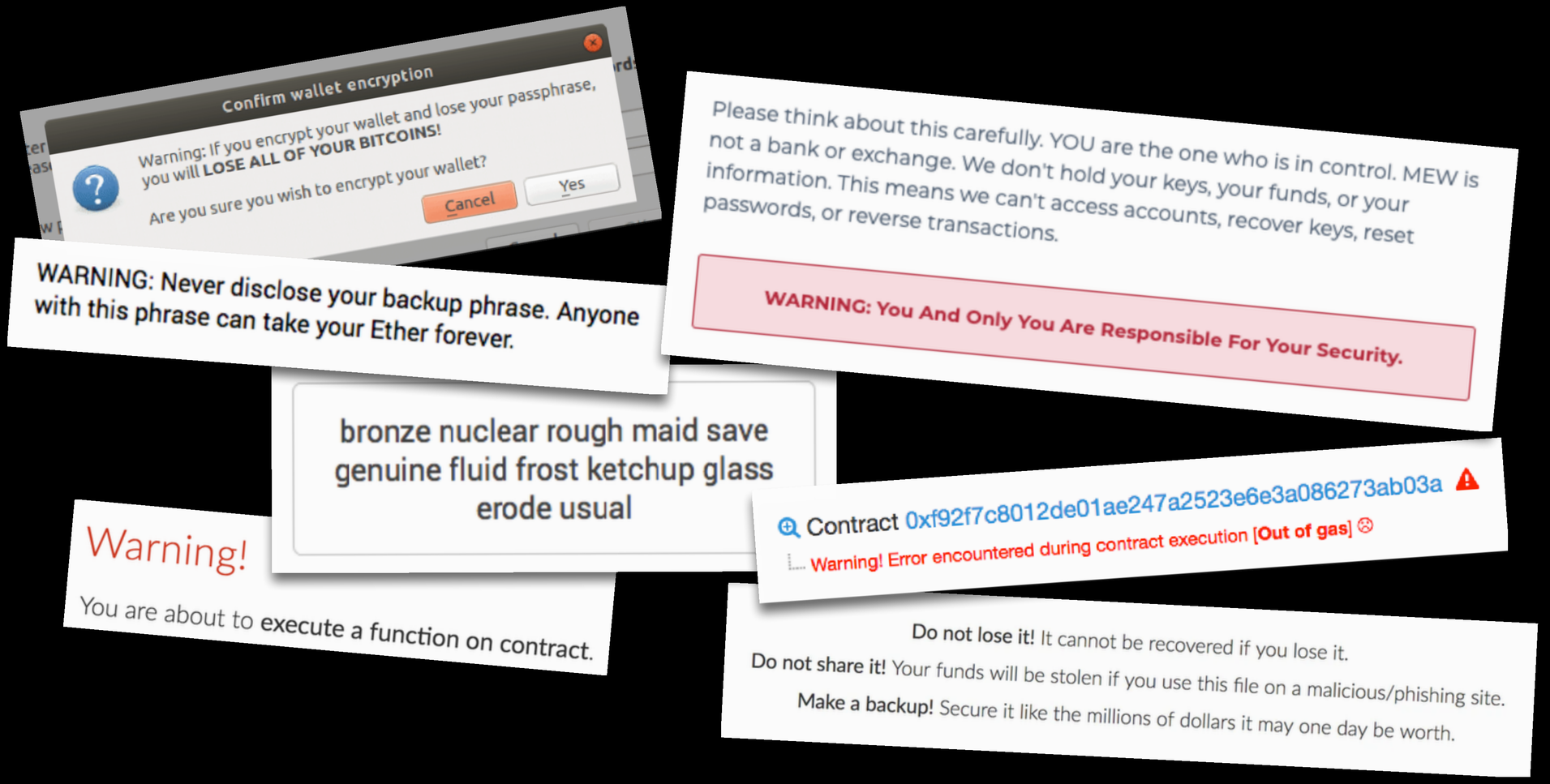
FINANCIAL TIMES

It’s expensive to use and getting ever more so. It can be slow and unpredictable.

Forbes

There are two big problems with bitcoin: Its value is unstable and its transaction processing is too slow.

USING CRYPTO IS DANGEROUS



EXCHANGES ARE THE DEFAULT


東京で MT.GOX のデモ
へ参加してください。
東京都渋谷区渋谷
2丁目11-5
MTGOX
WHERE IS
OUR MONEY
VAIO


BINANCE

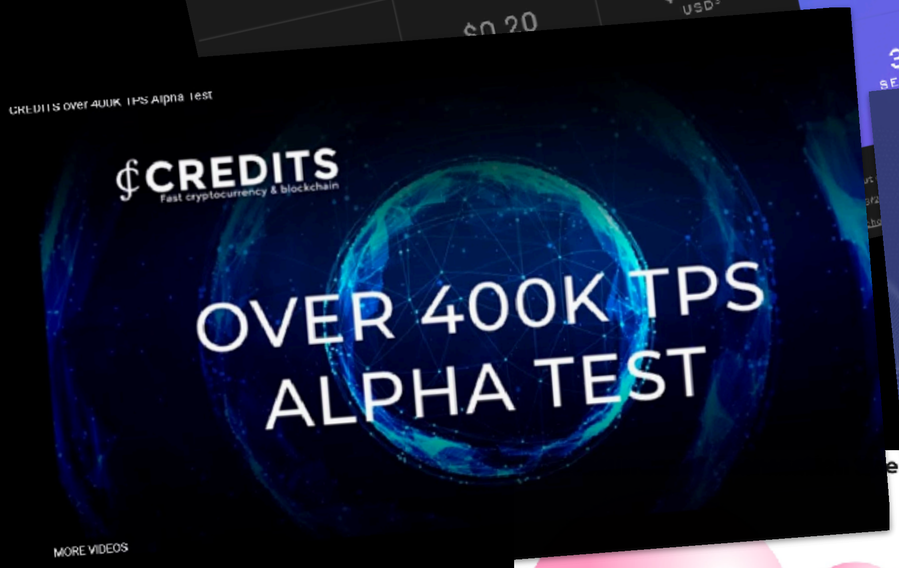
HOW HAS THIS SHAPED CRYPTO?


PEOPLE DON’T USE CRYPTO
TO BUY REAL THINGS


1ST GENERATION
BITCOIN BTC
2ND GENERATION
ETHEREUM ETH
3RD GENERATION
HEDERA HBAR
TRANSACTIONS PER SECOND
3+ TPS
12+ TPS
10,000+ TPS¹
$0.13 USD³
3-5 SECONDS


Comparisons - Performance
PoW
DPoS
Bitcoin
Ethereum
Cardano
EOS
Blocklattice
DEXON
TPS
7 TPS
20 TPS
250 TPS
100K TPS
∞ TPS
Latency
1-6 hrs
5-10 min
300 s
165 s
~1s
TX Fees
10-50 USD
1-5 USD
0.1-0.5 USD
0.1-4 USD
~0.0000001 USD

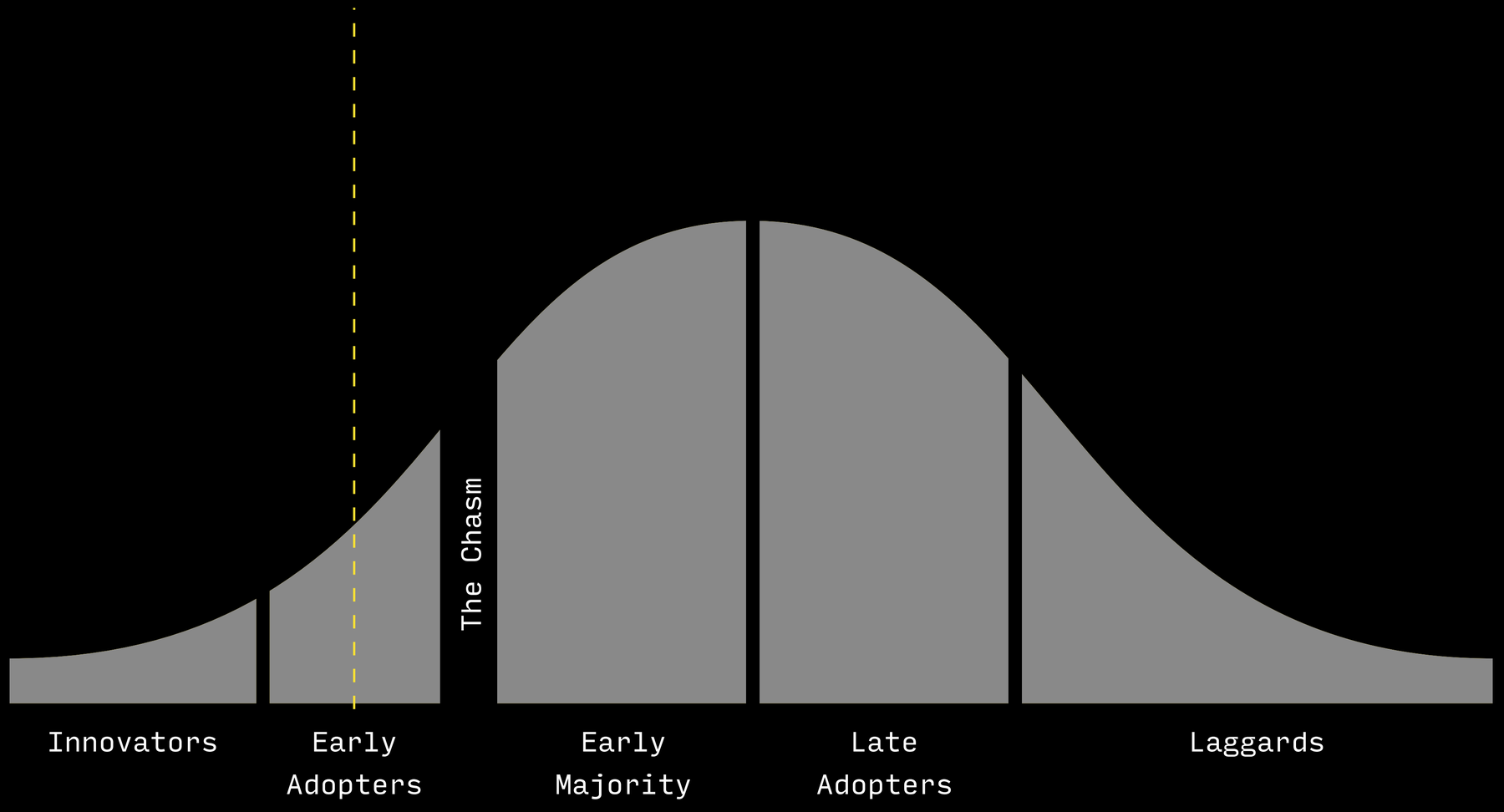

PCHAIN PEAK TPS
123,424
Sep. 13 2018


CREDITS over 400K TPS Alpha Test
CREDITS
Fast cryptocurrency & blockchain
OVER 400K TPS
ALPHA TEST
MORE VIDEOS


DURING THE LAST WE PEAKED AT
1 171 554 TPS!
RADIX


VISA
VISA
24,000
ripple
1,500
PayPal
193
60
litecoin
56
DASH
48
ethereum
20
bitcoin
7
1000 transactions
100 transactions
20 transactions
Company
Transactions per second
howmuch.net


DECENTRALIZED
HARDWARE ACCELERATED
SCALABLE
5000+ TPS
HPB
High Performance Blockchain
THIS IS ONLY THE BEGINNING


The Chasm
Innovators
Early Adopters
Early Majority
Late Adopters
Laggards

WHAT IF CRYPTO WAS LIKE CASH?

BENEFITS OF CASH

Billions of people around the world understand cash

There are no direct transaction costs

Transactions are instantly final

You can use it to buy goods and services

Transactions are (practically) anonymous

If you lose or destroy it, it’s gone

$1.7 TRILLION CASH IN CIRCULATION

WHAT IS ~~MONEY~~ CASH?

HOW DO WE MAKE PAPER CRYPTO?

- Printed private keys don’t work
- Hardware wallets are expensive and require you to trust the firmware
- Java smart cards have been broken multiple times and have dangerous APIs

HOW DO WE MAKE PAPER CRYPTO?

- Printed private keys don’t work
- Hardware wallets are expensive and require you to trust the firmware
- Java smart cards have been broken multiple times and have dangerous APIs

HOW DO WE MAKE PAPER CRYPTO?

- Printed private keys don’t work
- Hardware wallets are expensive and require you to trust the firmware
- Java smart cards have been broken multiple times and have dangerous APIs

TRUST IN CRYPTO = TRUST IN KEYS


500
KONG
要求
二零二二年十月
OCT 2022
五百塊港幣
FIVE HUNDRED KONG
实事求是
NULLIUS IN VERBA
SCAN TO VALIDATE
二十塊港幣
TWENTY KONG
一塊港幣
ONE KONG

PROPOSAL: CRYPTOCASH

A printed face value

- Looks and “feels” like money, can be sorted and counted like money

A smart contract

- Stores the crypto asset as a non-custodial wallet and grants access via signatures

A time lock

- Can’t pull the value off immediately like a prepaid card

A secure element*

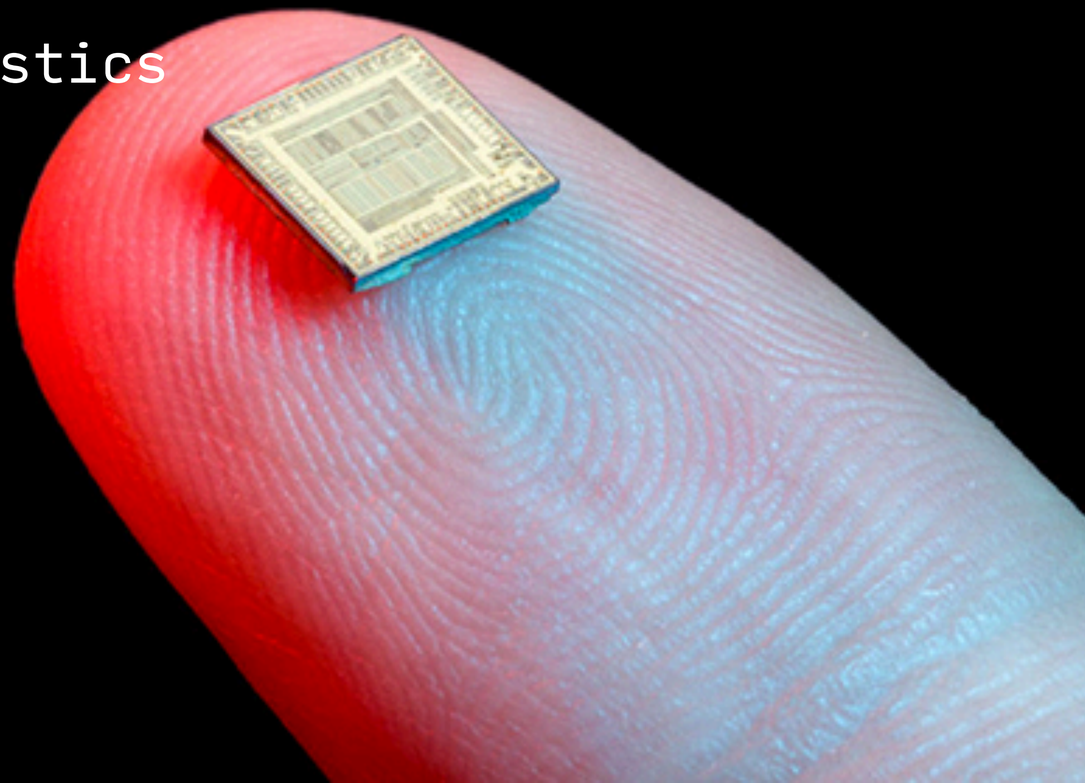
- Functionality limited to generating ECDSA key pairs, signatures


THIS CERTIFIES
THAT THERE HAS BEEN DEPOSITED IN THE TREASURY OF THE
United States
ONE
SILVER DOLLAR
B23584379
Payable to bear
Washington
B23584379


SILVER CERTIFICATE
THIS CERTIFIES THAT THERE HAVE BEEN
DEPOSITED IN THE TREASURY OF THE
UNITED STATES OF AMERICA
5
FIVE
Payable to Me
B3749663
B3749663
Five Silver Dollars
Payable on Demand.
Washington, D.C.
SILVER CERTIFICATE
FIVE
SILVER CERTIFICATE

*SECURE ELEMENT

- Secure elements today are a broad class of chips
- We need some very specific characteristics
  - NOT programmable
  - Must self-generate ECDSA key pair
- Challenge: only P256, not secp256k1



Private Key, Signatures

Secure Element

P256 Pub Key, Tokens

Smart Contract

P256 Elliptic Curve

Smart Contract

SILO: SILICON LOCKED CONTRACT

We can imagine other assets tied to their digital representation

Crypto Identity

Cheap, secure identities that can provide sybil resistance

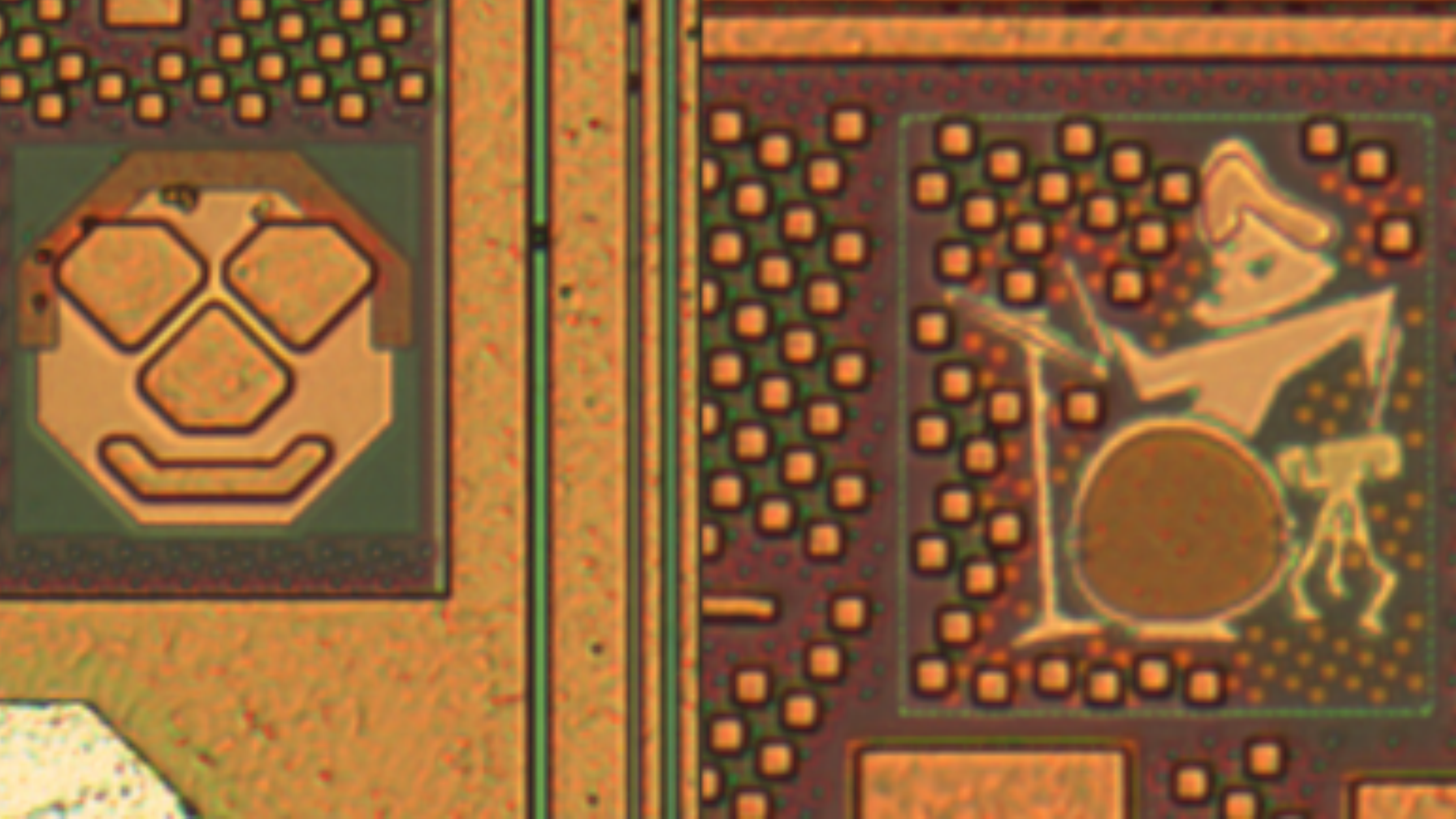
Crypto Art

You can verify the art on chain, but you cannot split off the NFT

Asset Tracking

Any asset tracking where open/public tracking is important for end users

WE NEED OPEN TRUSTWORTHY CHIPS



- An experiment: can we quantify trustworthiness in secure elements through cryptoeconomic incentives?
- A bounty program for secure elements with one primary challenge: extract the private key
- The ARX project is focused on this challenge (arx.org)

SECURING CRYPTO IS THE FIRST STEP TO SECURING THE DECENTRALIZED WEB

2009 → 2019

We are experiencing a breakdown in centralized services and trust in the web in the same way trust broke down in the banking system in 2009

1 We need usable, self-sovereign crypto

2 To achieve this we need to anchor crypto to open secure chips

3 KONG is crypto cash, the first silicon locked crypto

THANK YOU

HTTPS://KONG.CASH
@KONGISCASH

CAMERON ROBERTSON
@CCAMROBERTSON