Not-So-Fungible Crypto:

Privacy vs Social Integrity

020 BLOCK

Hong Kong Blockchain Week.

Anatoly Ressin
BLOCKCHAIN ARCHITECT AT PARSIQ
CEO AT BLOCKVIS

parsiq.io
https://parsiq.io
POWERED BY blockvis.com

Preface

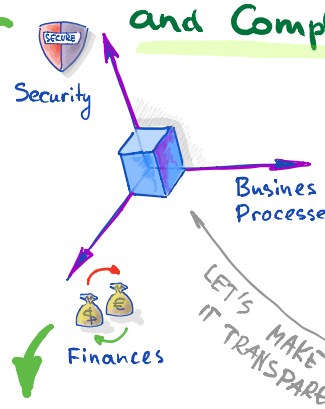
Cryptography.

PROVABLY FAIR
- Merkle Proofs
- Zero-Knowledge Proofs

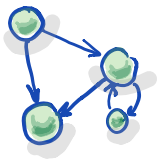
PROTECTED
- Asymetric cryptography (PKI)

Future of Audit and Compliance

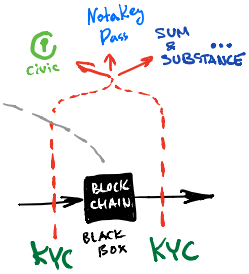
The new generation of auditors SHOULD be capable to audit digitalized dimensions of the business.



Smart Contracts DAO/DAPPS
- Business rules in Blockchain



LET'S MAKE IT TRANSPARENT



TRADITIONAL AUDITORS PREFER TO BLACKBOX BLOCKCHAIN PART OF THE PROJECT AND CHECK ONLY INPUT/OUTPUT GATES
it is a WRONG APPROACH!

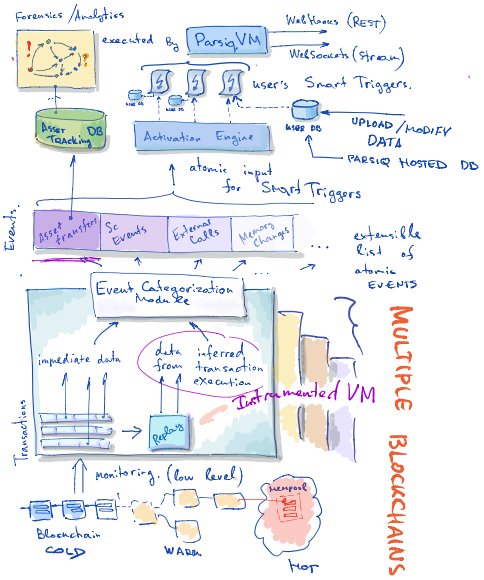
SOME TIME AGO THIS PICTURE WAS PRESENTED BY
Blockvis
TO A BIG AUDITOR ENTITY...

IT WAS A vision...

Crypto-Currencies
- Transaction Traceability.
- Graph audit
- Deals and Taxes on BLOCKCHAIN

parsiq.io

Now it's parsiq.io [under development]



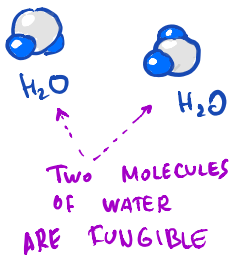
- system for an in-depth analysis of multiple blockchains
  - EVEN AT THE LEVEL OF SUB-TRANSACTION ASSET MOVEMENTS
- Realtime notification engine, that allows continuous Busines Logic Audit via SMART TRIGGERS

NOW EVERYBODY IS ASKING ABOUT ANONYMOUS / TRULY FUNGIBLE COINS AND OUR POSITION ON PRIVACY.

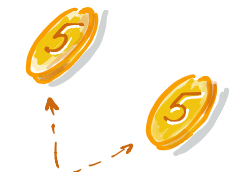
[WE RESPECT PRIVACY] OK...

parsiq.io

Fungibility

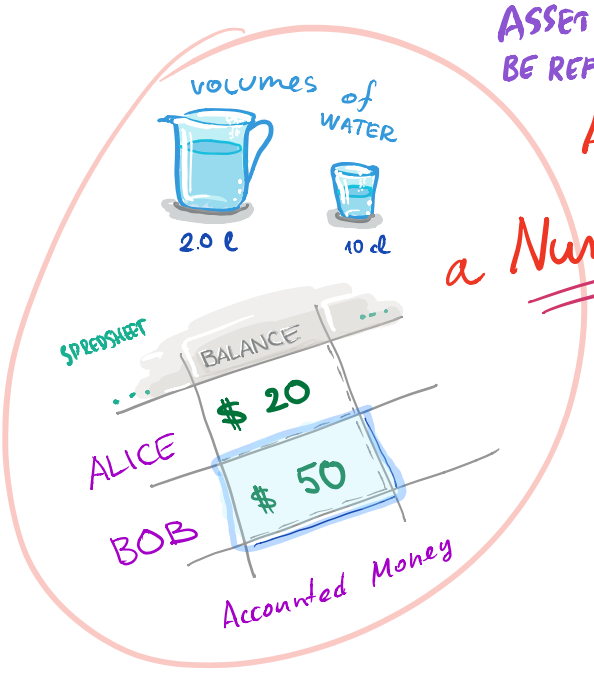


TWO MOLECULES OF WATER ARE FUNGIBLE



TWO Coins ARE FUNGIBLE AS WELL

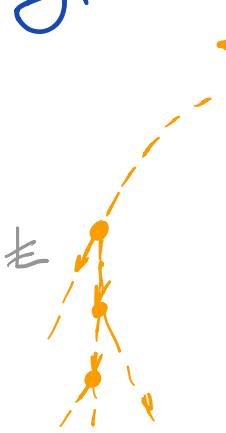
Amount of the fungible ASSET COULD BE REPRESENTED AS A a Number!



parsiq.io

Crypto :

Main Concern : fungibility of BTC



Bitcoin WAS BORN TO BE Fungible

But IT IS NOT

AT LEAST AS IT EXISTS NOW

AND THE PLETHORA OF IT'S DESCENDANTS

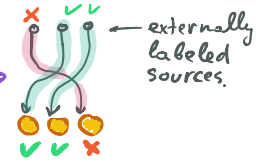
THE SAME FOR ETHEREUM

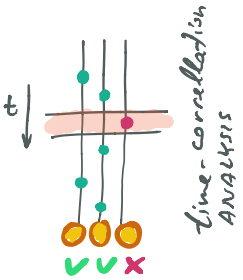
parsiq.io

WHY ?

with appropriate game-theoretic incentivisation based

- IF THE PATH OF THE COIN IS TRACEABLE...
- IF TRANSACTIONS ARE TIMESTAMPED...
- IF TRANSACTIONS ARE STORED... IN A REPLAYABLE FORM
- IF YOU CAN PROVE TO SOMEBODY OTHER THAN THE RECIPIENT THAT YOU'VE PAID GIVEN AMOUNT IN PARTICULAR DIRECTION...





!!! ...

A LOT of other properties

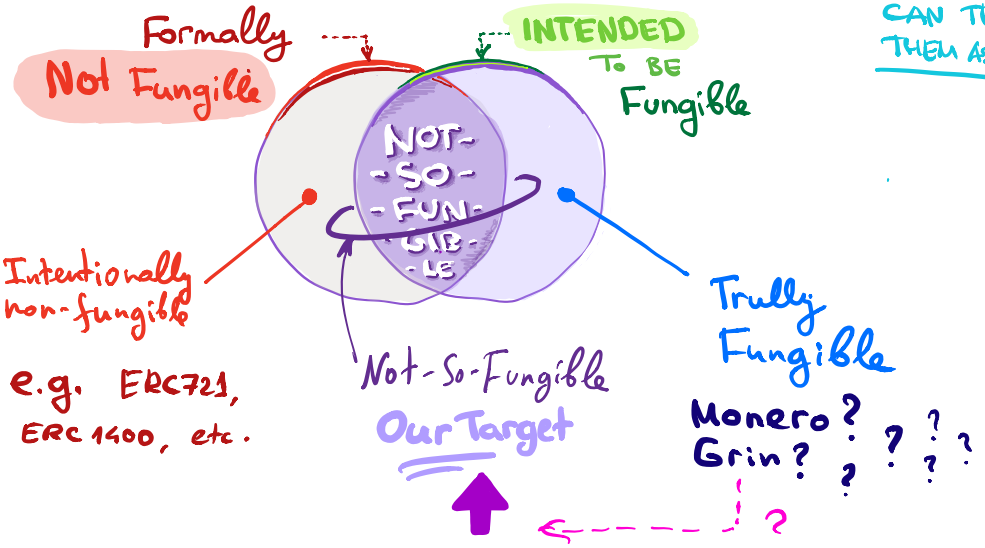
then the coin is NOT formally FUNGIBLE

parsiq.io

In this context we don't speak about

[identifiable assets distinct] **ERC721**, and other Crypto-Kitties

Yet WE CAN TRACK THEM AS WELL



parsiq.io

True Fungibility

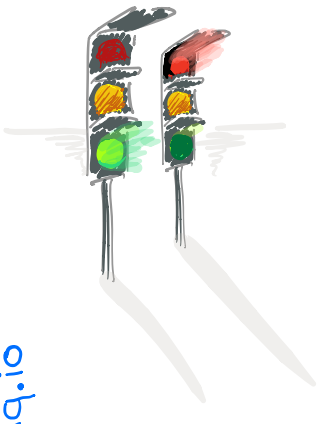
is NECESSARY for implementing MONEY → 21th CENTORY

necessary for implementing

PRIVATE ANONYMOUS UNTRACKABLE MONEY }

parsiq.io

GAME-THEORETIC Result :



KNOWN AS "The Tradegy of Commons"
shows that SOMETIMES the society
without SOME INTELLIGENT REGULATION
tends to shoot itself into a leg.

E.g. Will you argue with the Traffic Lights ?

IS IT APPLICABLE
TO THE ANONYMOUS
UNTRACEABLE MONEY ?

↳ YET TO BE ANSWERED...

parsiq.io

$\int_{-\infty}^{+\infty} \frac{1}{0}$ Social Integrity

The liberty of one citizen
ends where the liberty
of anoter citezen begins

parsiq.io

Don't kill
Don't steal
Don't humiliate

« please tell me
who said that »
?

WHAT IS AT RISK ?

AML ⚡ CTF

COUNTERMEASURES BECOME INEFFECTIVE

NAIVE APPROACHE 2.

ASKING EITHER WEAKENING THE CRYPTOGRAPHY USED OR ASKING EMBEDDING THE BACKDOORS

NAIVE PROHIBITATIVE APPROACH

BAN ALL THE CRYPTO BY DEFAULT

OK, YET ITS A Progress...

NOT OK RUINS Privacy BETWEEN PEERS ! Hackers are welcome !

parsiq.io

SMARTER SOLUTIONS
The Parsiq Way

- Use any not-so-fungible crypto-currency imperfections, and status quo implementations

- To mitigate AML/CTF risks related to the accepted crypto
- To provide necessary information for investigations an fraud prevention

parsiq.io

SMARTER SOLUTIONS
The Parsiq Way

- Promote and Inegrate ZERO KNOWLEDGE proof-BASED SOLUTIONS FOR AML } AUTOMATIC RISK DELEGATION VIA BLOCKCHAIN
- Promote and Integrate cryptocurrencies with STATE-OF-THE-ART CRYPTOGRAPHY WITH SUPPORT OF OPT-IN/VOLUNTARY AUDITABILITY

MIMBLE WIMBLE + OPT IN AUDIT

=

BEAM.MW

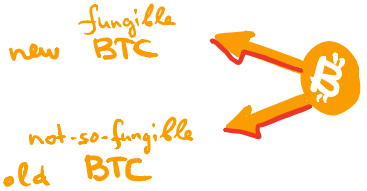
parsiq.io

IS IT SUSTAINABLE APPROACH?

? "Fungibility should be implemented"

we see TWO SCENARIOS

Adam Back [at BHB'18]



fungibility enforced W/O auditability

fungibility enforced WITH opt-in AUDITABILITY

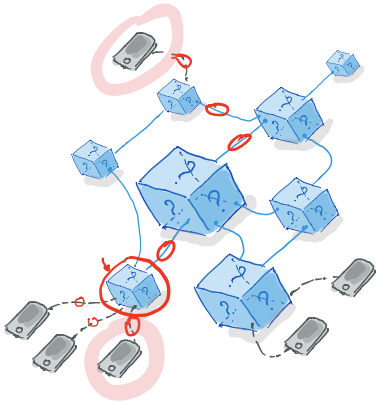
↑ YET ANOTHER BLOODY FORK

Sustainable growth

ANYWAY PARSIQ IS HERE

parsiq.io

And What About Lightning Network?



SHORT ANSWER:

2-rd LAYER IT'S A PAIN

HOWEVER

WE SEE IT'S FUTURE PROBLEMS, AND WE PROBABLY SEE HOW TO ALIGN THE NEEDS, FEARS AND HOPES OF THE SOCIETY

with the Progress, Privacy and Social Integrity

parsiq.io

Thank You! Q/A?

[probably at networking]

Anatoly Ressin
BLOCKCHAIN ARCHITECT AT PARSIQ
CEO AT BLOCKVIS

https://parsiq.io

POWERED BY blockvis.com

parsiq.io