

The third wave of IT systems




Tomasz Waszczyk
Konferencja Blockchain i Finanse
January 17th, 2020 Warszawa

Introduction - Tomasz Waszczyk


- Software engineer
- Ex trader Tier 1
- Psychology (psychometrics, transactional psychology)
- History


The presentation has no bias!


BEAM - Atomic Swap



Atomic Swaps BETA

 online

 1 085,40883495 BEAM

 Connect other currency wallet to start trading



ACTIVE OFFERS

MY OFFERS

TRANSACTIONS

☐ Fit my current balance

Currency ALL

Date Time	Send	Receive	Rate	Expiration	
 1/15/20 3:24 PM	0.6 LTC	50 BEAM	0,012	1/15/20 9:26 PM	Accept offer
 1/15/20 3:23 PM	50 BEAM	0.003 BTC	0,00006	1/15/20 9:24 PM	Accept offer

First wave



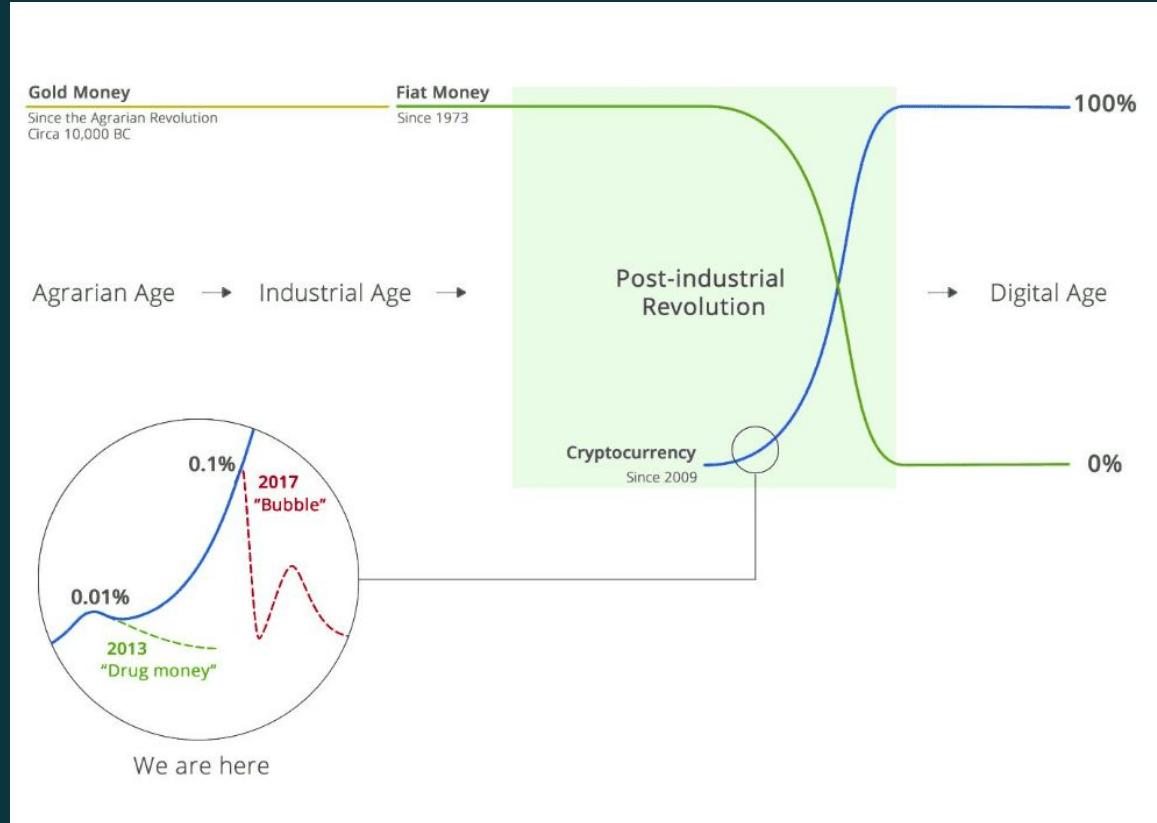
Second wave



What does third wave mean?

- Easier entry to the market together with big players
- Strategic industries:
 1. Food
 2. Drugs, medicine
 3. Insurance
 4. Reinsurance
- Strong need to cooperate with politicians (law)...

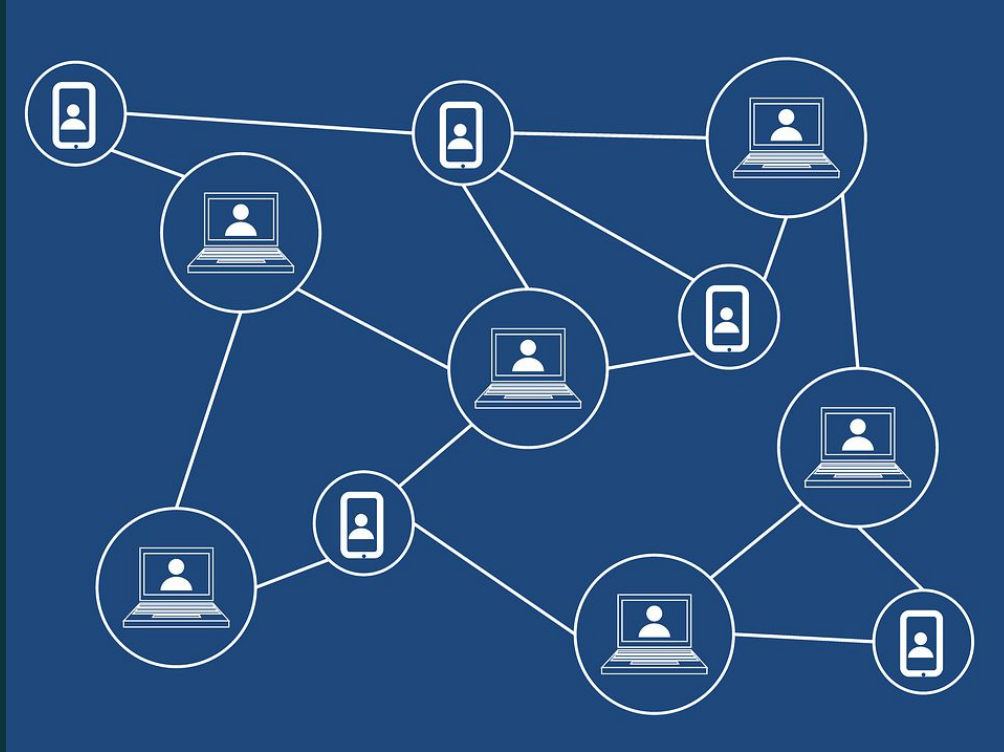
Third wave (in terms of technology and money)



Use case 1 - transformation of predictive software

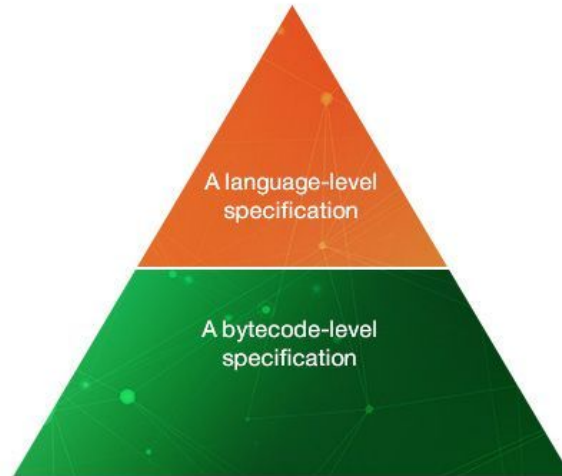


Use case 2 - reinsurance



Common issue - formal verification - (not easy!)!

A formal specification has two levels:



<https://www.apriorit.com>

Formal verification - (not easy!) - Ethereum

- EVM Level
- Solidity Level

EVM verification challenges

“Verifying the EVM bytecode is challenging, especially due to the internal byte-manipulation operations that require non-linear integer arithmetic reasoning, which is undecidable in general.”

“The EVM provides three types of storage structures: a local memory, a local stack, and the global storage. Of these, only the local memory is byte-addressable (i.e., represented as an array of bytes), while the others are word-addressable (i.e., each represented as an array of 32-byte words).”

Vyper (SmartPy in XTZ) as a solution?

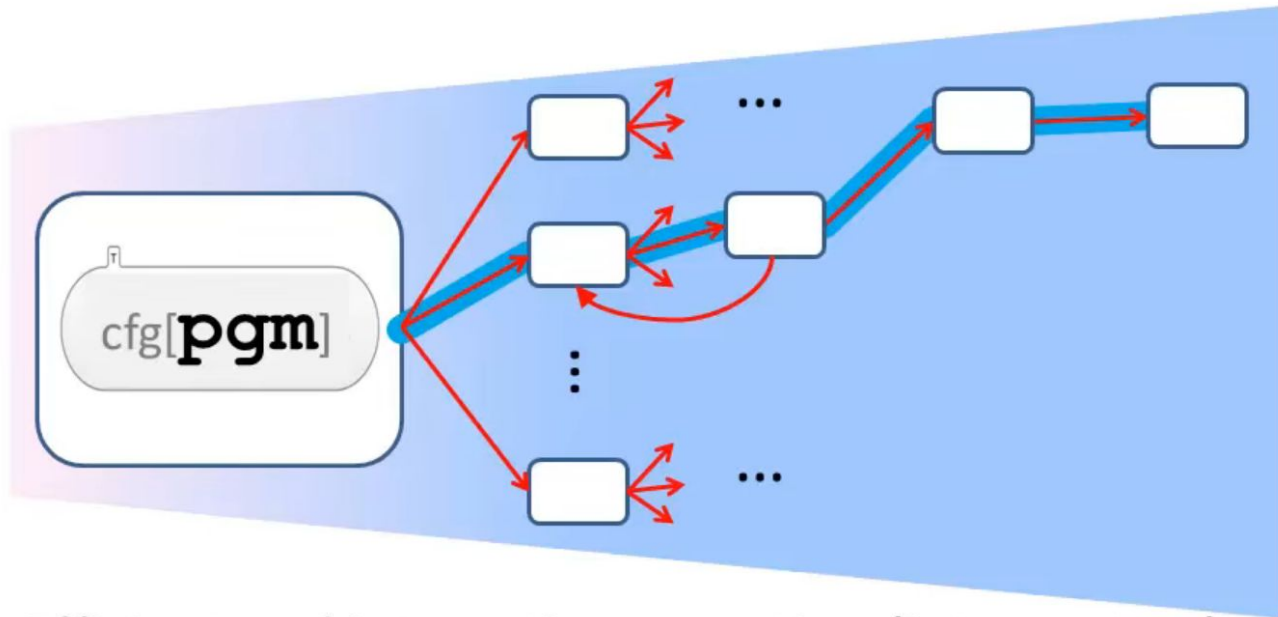
```
3  # Auction params
4  # Beneficiary receives money from the highest bidder
5  beneficiary: public(address)
6  auctionStart: public(timestamp)
7  auctionEnd: public(timestamp)
8
9  # Current state of auction
10 highestBidder: public(address)
11 highestBid: public(wei_value)
12
13 # Set to true at the end, disallows any change
14 ended: public(bool)
15
16 # Keep track of refunded bids so we can follow the withdraw pattern
17 pendingReturns: public(map(address, wei_value))
```

K framework as a solution?

“rewrite-based executable semantic framework in which programming languages, type systems and formal analysis tools can be defined using configurations, computations and rules. Configurations organize the state in units called cells, which are labeled and can be nested. Computations carry computational meaning as special nested list structures sequentializing computational tasks, such as fragments of program.”

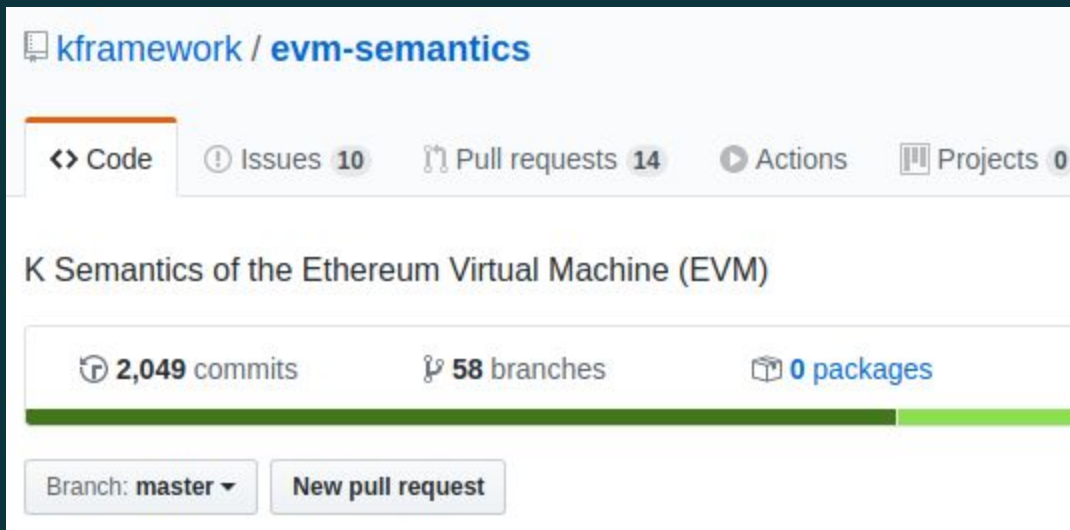
K framework

What does the K Tool Offer?



Efficient and interactive execution (interpreters)
State-space exploration (search and model-checking)

K framework as a solution?



The screenshot shows the GitHub repository page for `kframework / evm-semantic`. The repository is titled "K Semantics of the Ethereum Virtual Machine (EVM)". It has 2,049 commits, 58 branches, and 0 packages. The "Code" tab is selected, and there are 10 issues, 14 pull requests, and 0 projects. A green progress bar is visible below the statistics. At the bottom, there is a button to "New pull request" and a dropdown menu for the current branch, which is set to "master".

kframework / evm-semantic

<> Code ! Issues 10 🔗 Pull requests 14 ▶ Actions 📁 Projects 0


K Semantics of the Ethereum Virtual Machine (EVM)

🕒 2,049 commits 🔗 58 branches 📦 0 packages

Branch: master ▼ New pull request

Formal verification in XTZ

My Courses



Tezos Developer Course

Tezos Developer Course

BLOCKSTARS-TEZ-2

View Class



Academy
Blockchain education

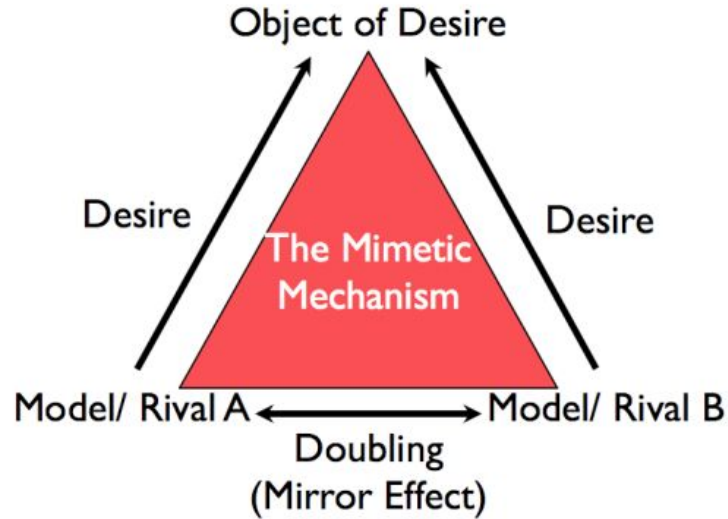
Michelson

Turing complete and **formally specified**, and can support a wide variety of different use cases.

Formal verification - (not easy, maybe easier?) - Michelson in Tezos

```
parameter unit;  
storage (pair timestamp (pair tez (contract unit unit)));  
return unit;  
code { CDR;           # Ignore the parameter  
      DUP;           # Duplicate the storage  
      CAR;           # Get the timestamp  
      NOW;           # Push the current timestamp  
      CMPLT;         # Compare to the current time  
      IF {FAIL} {};  # Fail if it is too soon  
      DUP;           # Duplicate the storage value  
      # this must be on the bottom of the stack for us to call  
      transfer tokens  
      CDR;           # Ignore the timestamp, focusing in on the  
                      transfer data  
      DUP;           # Duplicate the transfer information  
      CAR;           # Get the amount of the transfer on top of  
                      the stack  
      DIP{CDR};       # Put the contract underneath it  
      UNIT;          # Put the contract's argument type on top of  
                      the stack  
      TRANSFER_TOKENS; # Make the transfer  
      PAIR}          # Pair up to meet the calling convention
```

Psychology - Mimetic theory

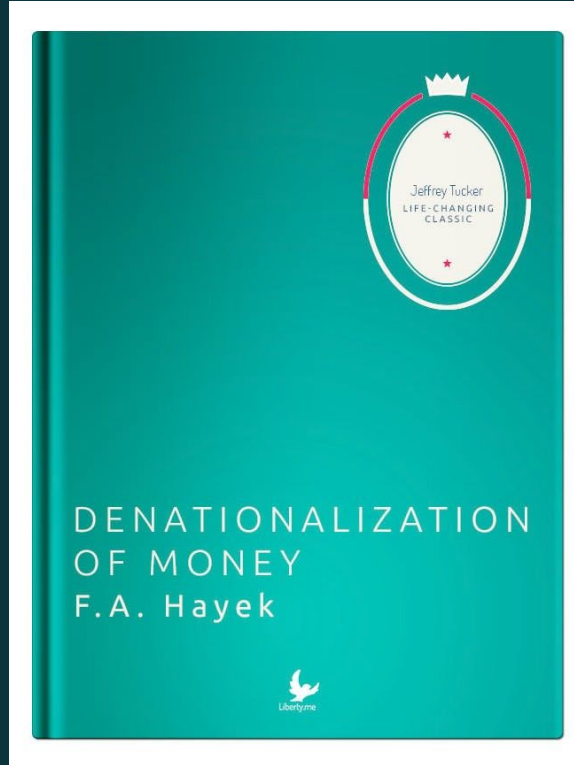


Let's conclude third wave

- Gig economy
- Deindustrialization
- Dopamine economy
- Daily life gamification
- Political correctness
- Attention economy
- Algocracy
- The end of offline, offline becoming the new luxury
- Psychology
- Virtual > Reality

IT systems from third wave will impact on psychology of every human beings, how we meet, how we communicate, WHY we communicate, how we think, WHY we think etc. etc.

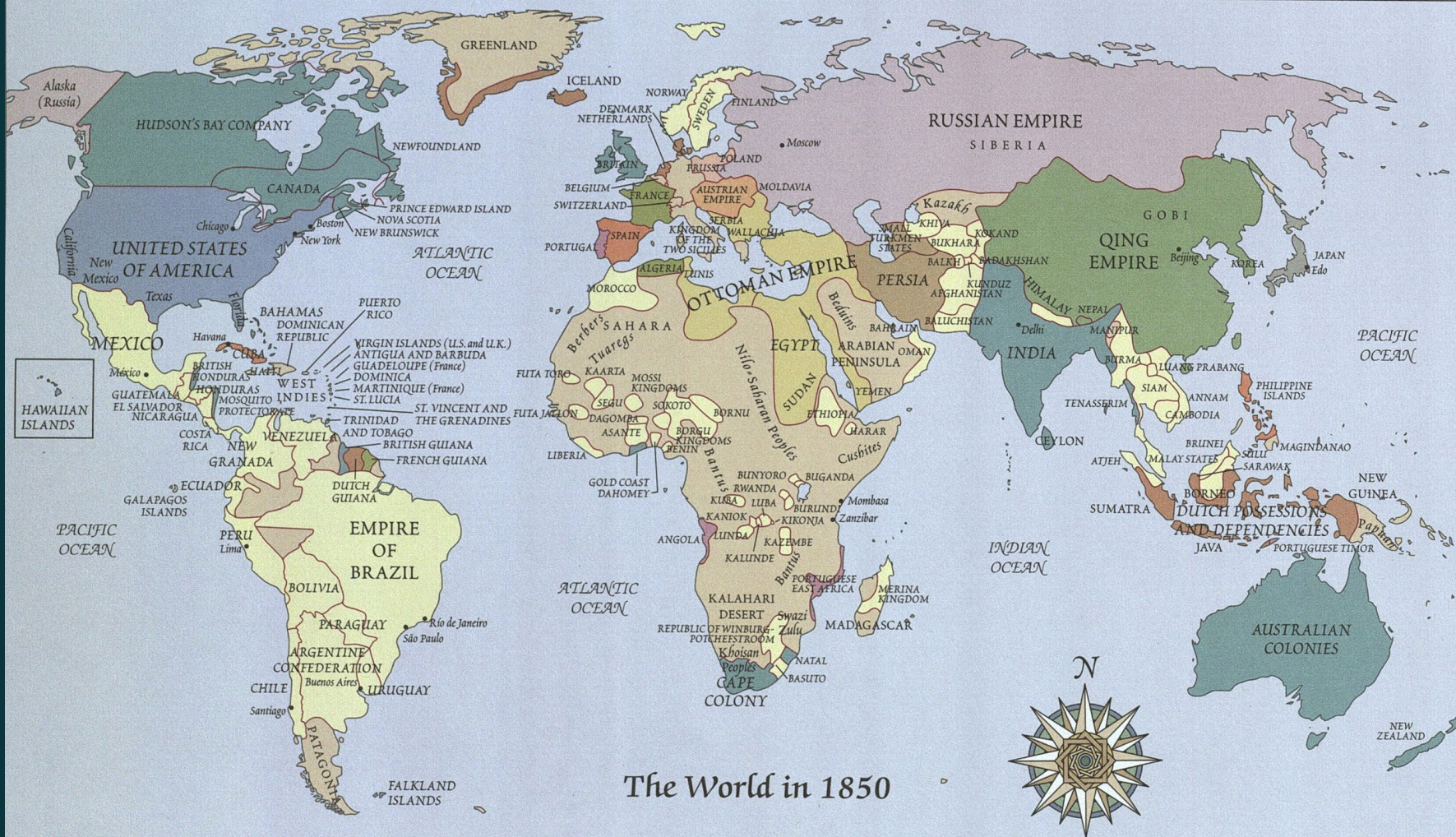
The Denationalization of Money



Return of the city-state

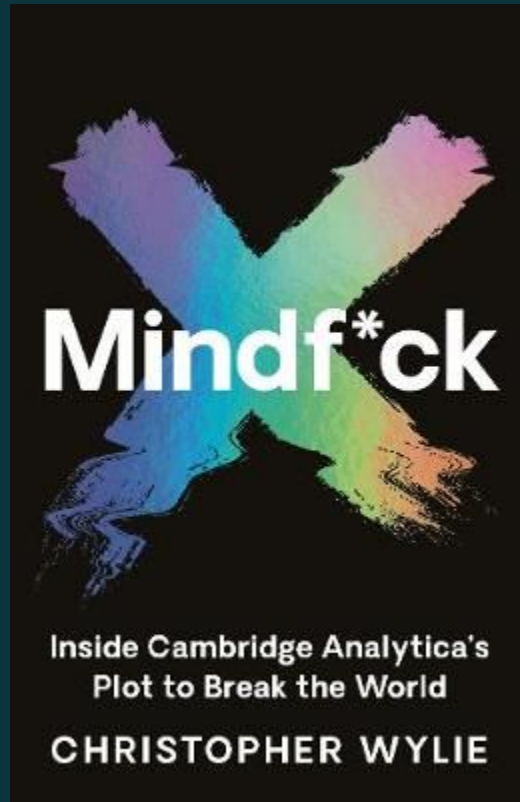
Nation-states came late to history, and there is plenty of evidence to suggest they won't make it to the end of the century.

<i>CURRENCY</i>	<i>DEVIATION FROM</i>	
	<i>ANNOUNCED STANDARD</i>	<i>OUR TEST STANDARD</i>
	<i>%</i>	<i>%</i>
Ducats (SGB)	−0.04	−0.04
Florins (FNB)	+0.02	+0.03
Mengers (WK)	+0.10	+0.10
Piasters (DBS)	−0.06	−0.12
Reals (CNB)	−1.02	−1.01
Shekels (ORT)	−0.45	−0.45
Talents (ATBC)	+0.26	+0.02



The World in 1850

The end of democracy

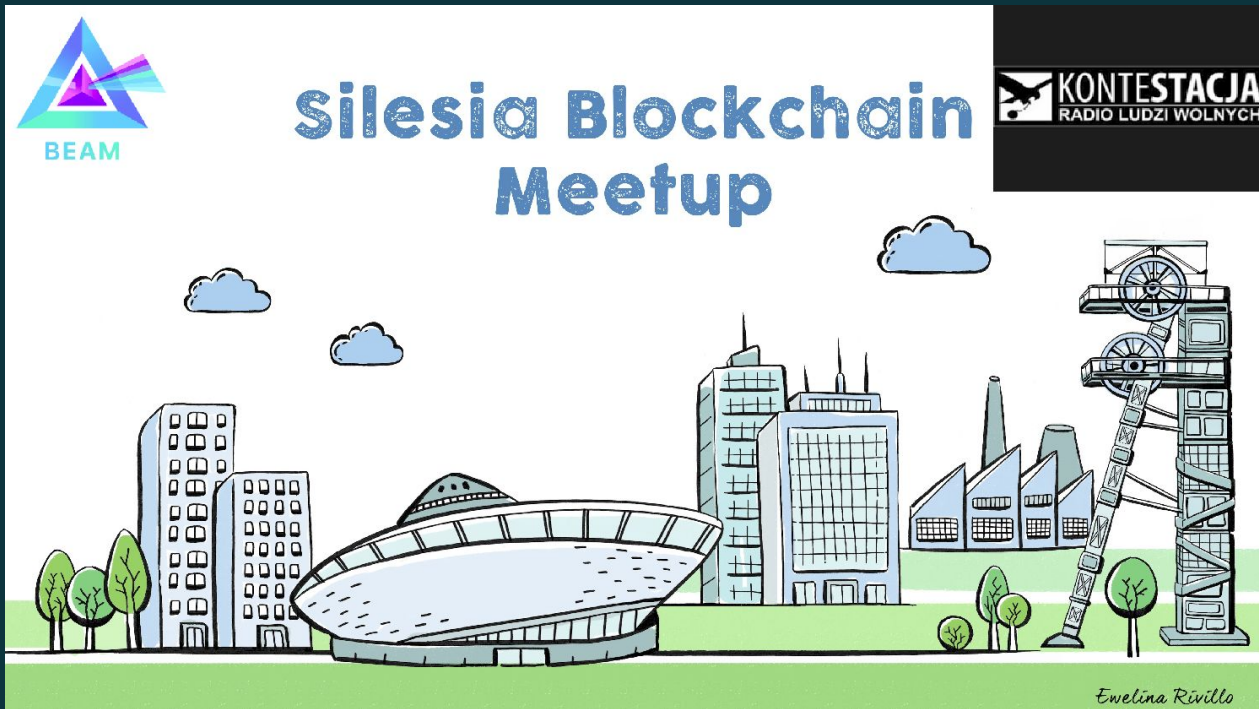


“People don't have ideas. Ideas
have people.” — Carl Jung

Smart contracts =? Government

“bonds of words are too weak to bridle men’s ambition, avarice, anger, and other passions, without the fear of some coercive power”
(Leviathan, p. 69).

Silesia Blockchain Meetup



Thank you for attention, for invitation!

Any questions?!

Feedback and hints are welcome!

Fast contact with me: <https://tlk.io/kbif>