

PERSONIX

lustra sieci
reputacji
ujawniają nawet
wypolerowaną
nędzę ukrytą w
środku.

**Niecenzurowalna i Nieskorumpowana Zdecentralizowana Sieć Reputacji
ewolucyjny następca państwa**

Personix — Bezkompromisowa zmiana

Nieczenzurowalna i nieprzekupna zdecentralizowana sieć reputacji

© 2025–2026 Pavel Kudrna, Praga

Wersja 6 (2026-05-21)

Pierwsza wersja robocza powstała od czerwca do listopada 2025, przeredagowana od kwietnia do maja 2026.

Skład w $\text{\LaTeX}$ (Tectonic) z użyciem krojów Palatino i Helvetica Neue.

A5 poziomo (210×148 mm).

Udostępniono na licencji **Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0)** — creativecommons.org/licenses/by-sa/4.0/. Elementy zastrzeżone, repozytorium źródeł oraz notę o narzędziach produkcyjnych wymieniono na końcu książki.

Contents

Wprowadzenie	7
O czym jest ta książka?	9
Niezbędne warunki zmiany	17
Niezbędne warunki zmiany	17
Narzędzie	28
Reputacyjna sieć społecznościowa	28
Dlaczego sieci nie da się ocenzurować	54
Odpowiedzi na oczywiste wątpliwości	56
Zależność od technologii	56
Czy publikując w sieci, nie wyrzucam pieniędzy w błoto?	56
A co, jeśli ktoś stworzy wiele tożsamości?	58
Czy zamożna osoba nie może po prostu „kupić” sobie więcej tożsamości (albo tworzyć wirtualnych wspólnot)?	61
A co z pasażerami na gapę, którzy chcą tylko czytać i nic nie dawać wspólnocie?	64
Neutralność finansowa	65

Dobrowolność, odpowiedzialność i wolność	67
Przełącznik wolność-totalitaryzm (i delegacja)	68
Problem wyroczni — pomost między światem cyfrowym a fizycznym	74
Jak działa weryfikacja	78
Konsensus i proces weryfikacji	78
Roles in the verification transaction and authorities	84
Przegląd ról	84
Wystawca	85
Autorytet	86
Weryfikator	90
Podmiot	92
Obserwator	95
Mechanizm: znacznik czasu i kod wyzwania	95
Puenta: nie potrzebujesz prawdziwych obserwatorów	97
Delegacja	99
Komunikacja między rolami	104
Emergentna umowa społeczna — polityka	104
Udostępnianie informacji o sobie	108

Zbrodnia i kara	109
Zbrodnia i kara	109
Podążaj za pieniędzmi	121
Podążaj śladem pieniędzy	121
Słaby punkt państwa — pieniądze	122
Proposed transition to the state's successor	125
Ewolucja, nie rewolucja	125
Cztery narzędzia, które się wzajemnie wspierają	126
Prosty system podatkowy — przynęta na wejście	127
Elektroniczny rejestr wydatków (ESR)	127
Obywatelska alokacja podatków — waga decyzji	129
Platforma negocjacyjna z państwem — dźwignia	133
Obywatelstwo bez dowodu osobistego	135
Nakładanie się i odwracalność	138
Zakończenie	141
Droga istnieje	141
Podziękowania	143
Inspiracja	143

Recenzja i informacja zwrotna	143
Narzędzia	143
Słownik pojęć	146
Słownik pojęć	146

Wprowadzenie

Czy masz poczucie, że możesz polegać na państwie?

Nie godzę się na to, że gdy dzieje się oczywista niesprawiedliwość wobec mnie, mojej rodziny albo kogoś z mojej wspólnoty (krzywda fizyczna, oszustwo, nieuzasadnione ograniczenie...), a państwo odpowiada: tak, to niesprawiedliwość, ale nic z tym nie rób, bo będziesz miał z nami jeszcze większy problem. Taki stan jest chory, a ludzie, którzy się na niego godzą, są współwinni.

Rezultatem jest wzajemne wyobcowanie, zabawa we wspólnotę, zabawa w państwowość i pogłębiający się rozpad społeczeństwa z obietnicą poważnych konfliktów w przyszłości.

Czy państwo nadąża za tempem przemian technologicznych i społecznych, czy woli wlepić zakaz?

Mógłbym udawać, że stagnację, niekompetencję i korupcję będę traktował jako deklarowaną stabilność praworządności i tradycji, ale już nie chcę. Okłamywałbym siebie i okłamywałbym ciebie.

Czy czujesz protekcyjność urzędników i wybranych przedstawicieli, gdy ośmielasz się krytykować coś, za co płacisz?

Nie godzę się, by uznawać ludzi w społeczeństwie za niegodnych współkształtowania ogólnospołecznych reguł tylko dlatego, że nie błyszczą w miękkich kompetencjach, które są dziś jedynym wystarczającym warunkiem, by zostać wybranym przedstawicielem w skodyfikowanych przez państwo instytucjach. Wierzę, że ogromna większość potrafi zadbać o siebie, o bliskich i o swoją wspólnotę — i że widzi w tym część własnej życiowej filozofii. Większość ludzi, których udało mi się poznać wokół siebie, taka właśnie jest.



Nie zgadzam się na to.

Ale spotkałem też skończonych dupków, którzy byli dupkami właśnie dlatego, że umieli grać w grę — grę, w której wspólnocie nie wolno dawać im informacji zwrotnej, w której państwo ich chroni, żeby nikt nie zakłócał porządku zagrażającego samej istocie państwa: zapewnianiu łatwego życia tym z górnych pięter hierarchii władzy i hierarchii jej instytucji. Feudalizm zastąpiono rządami populistów i elitarystów.

Czy uwielbiasz, gdy inni mówią ci, jak masz żyć?

Nie przyjmuję obecnego stanu rzeczy jako doskonałej, ostatecznej danej. Muszę zachowywać się odpowiedzialnie, a jednocześnie jestem przewrażliwiony, gdy ktoś mówi mi, jakie właściwe wartości powinienem wyznawać. A ty jak masz?

O czym jest ta książka?

Wyobraź sobie reputacyjną sieć społecznościową, w której każdy, kto chce, może utworzyć dla siebie własne klucze (stworzyć swoją tożsamość), dać się zaprosić członkom swojej wspólnoty albo wejść na własną rękę. Budujesz swoją reputację i sięgasz po użyteczne dane reputacyjne o innych, kiedy ich potrzebujesz. Szukasz wsparcia swojej wspólnoty, gdy dzieje się niesprawiedliwość — przedstawiasz swoją sprawę i dostarczasz to, co masz, a wspólnota przygląda się temu, decyduje na podstawie istotności, czy przekazać to dalej i jak ukarać sprawcę.

Cała ta krótka książka mówi o tym, co musi być pod maską, żeby na zewnątrz działało to tak prosto. Jeśli przy niej wytrwasz, obiecuję ci, że świat, który dziś może wydawać się pod wieloma względami złożony i trudny do zrozumienia, otworzy się jako bardziej zrozumiały i jaśniejszy. Zobaczysz, że wiele złych rzeczy można ułożyć tak, by przestały się tak niesprawiedliwie opłacać złym aktorom. I nie jest to narzędzie, przy którym trzeba by ciągle tkwić online — wystarczy sięgnąć po nie wtedy, gdy poczujesz taką potrzebę.

Obiecuję ci ponadto, że opisany tu układ będzie bliższy prawdziwym motywacjom ludzi i że nie musi ich przekształcać w imię jakiegoś -izmu.

I wreszcie pokażemy, jak przeprowadzić nierewolucyjne przejście do stanu, w którym wspólnoty znów stają się w pełni funkcjonalnymi jednostkami społecznymi i nie muszą już tylko udawać.

Artykuł techniczny

Ta książka jest wyjaśniającym towarzyszem oryginalnego artykułu technicznego „*Decentralized Reputation Network: A Framework for Voluntary and Uncorruptible Societal Organization*” (Pavel Kuderina, 2026). Jeśli interesuje ci formalny opis architektury, algorytm wyboru weryfikatora i uzasadnienie mechanizmów ekonomicznych, polecam zacząć właśnie od niego.

Rozdziały opierają się na sobie nawzajem

Książka napisana jest jako ciągły wywód — każdy rozdział opiera się na poprzednim. Pojęcia wprowadzone w jednej części są używane w częściach późniejszych, także w przypisach. Nie polecam czytania poza kolejnością.

Dla kogo jest ta książka?

Mimo wizualnie przyjaznej formy głównym adresatem jest bardziej specjalistyczny czytelnik zajmujący się zasadami możliwych społeczno-ekonomiczno-politycznych układów ludzkiego społeczeństwa. Dojście do punktu, w którym potrafiłbym przystępnie wyjaśnić całą materię najszerzej publiczności, wymaga jeszcze długiej drogi budowania pełnej strategii komunikacji.

Chętnie przyjmę sugestie, jak uczynić to niewielkie dzieło — lub kolejne poprawione wydania — bardziej zrozumiałym.

Ostrzeżenie

Nie wiem, kim jesteś, ile masz lat ani ile złamanych obietnic musiałeś w życiu przesiedzieć. Ja z ich składaniem tutaj kończę. Zamiast tego chcę cię ostrzec, że jedynym rezultatem tego, czego się tu dowiesz, może być uświadomienie sobie, iż prawdopodobnie nie ma drogi, na której ktoś inny posprząta za ciebie dzisiejszy bałagan. Opisuję jedynie ramy/narzędzie, które mogłyby uczynić to sprzątanie prostszym i bardziej przejrzystym. Na jego podstawie spróbuję przygotować eksperyment/symulację społeczną, naprawić potencjalne wady albo całkiem pogrzebać pomysł, jeśli okaże się, że ma fundamentalne pęknięcia projektowe.

Prośba

Byłbym głęboko wdzięczny, gdybyś nawet po skończeniu tej książki zachował otwartość wobec tej idei i śledził, dokąd zmierza i jak wytrzymuje merytoryczną krytykę. Jeszcze bardziej doceniłbym twoje



To dopiero początek. Zostań ze mną.

późniejsze zaangażowanie — próby złamania proponowanych zasad równowagi własnymi pomysłami, a przez to lepsze sprawdzenie, jak bardzo system jest przygotowany na realne ludzkie zachowanie.

Bez ciebie i twojego zaangażowania idea pozostaje teorią w szufladzie. Bez ciebie oraz twoich wkładów i darowizn finansowych nie będziemy w stanie popchnąć projektu ku prawdziwemu eksperymentowi społecznemu, a tym samym ku prawdziwej gotowości. Bez ciebie i twojej merytorycznej krytyki będziemy tkwić tam, gdzie jesteśmy teraz, albo damy się pochłonać świętemu Graalowi centrystów — absolutnemu, nieodwracalnemu totalitaryzmowi. To od nas zależy, którą drogę wybierzemy albo przesiedzimy.

Wyzwanie

Nie kładziemy ci na barki lekkiego ciężaru. Już teraz ponosisz koszty rozrzutnie zarządzanego społeczeństwa poprzez okultystyczno-zaklinające podręczniki twierdzące, że społeczeństwem najlepiej rządzić centralnie — a ja mam czelność prosić cię o jeszcze więcej i o to, żebyś szedł pod prąd tym tendencjom. Zdaje sobie sprawę, że będziemy musieli przetrwać upadek największej piramidy finansowej w historii — repartycyjnego systemu emerytalnego — nie pozwalając zagłodzić kilku pokoleń.

A jednak proszę cię mimo to: przekażmy wreszcie naszym dzieciom lepszy świat i zostawmy po sobie dziedzictwo, że dokonaliśmy tej zmiany. Uwolnienie wzrostu gospodarczego mogłoby być częściowym rozwiązaniem kłopotu, który majaczy na horyzoncie. Będziemy wtedy mogli powiedzieć naszym potomkom, że była to niezła jazda i że nie poszła na marne.



Lepszy świat jest wart tego ciężaru.

■ Problem

Tylko wolność zrównowazona bezpośrednią odpowiedzialnością może naprawdę uwolnić ogromny potencjał, jakiego świat jeszcze nie widział.



Wejdz. Plany są już rozłożone.

Niezbędne warunki zmiany

Niezbędne warunki zmiany

Podstawowym warunkiem zmiany na lepsze jest to, by podporządkowany stał się przełożonym — albo przynajmniej równorzędnym partnerem. Oznacza to przejęcie najbardziej krytycznych agend, które definiują relację nadrzędności i podporządkowania. Agendy te opierają się na dowodach przynależności do wspólnot tworzących obywateli państwa. Są to informacje i ich weryfikowalność przez autorytet cieszący się znaczącą reputacją wewnątrz tych wspólnot.

Aby przewyciężyć obecny system, doszedłem do pięciu warunków, które następnie wyjaśniam tak, jak je rozumiem. Możemy myśleć o tych warunkach jak o filarach dźwigających konstrukcję systemu opisanego w dalszej części książki. Filary wybrałem początkowo według własnych preferencji, a rozumując nad nimi, stopniowo dopracowałem swoje rozumienie każdego z nich do poniższej postaci.

Przejdźmy przez te pięć filarów po kolei.

WARUNKI WSTĘPNE ZMIANY

DOBROWOLNOŚĆ



DOBROWOLNOŚĆ

Decyduję sam
za siebie.

ORGANIZACJA



ORGANIZACJA

Razem, ale bez
zwierzchnika.

ODPORNOŚĆ



ODPORNOŚĆ

Nie da się tego
ocenzurować.

KONSENSUS



KONSENSUS

Kompromis
pod presją.

NIEPRZEKUPNOŚĆ



NIEPRZEKUPNOŚĆ

Nie da się
kupić
wszystkich.

Bez tych pięciu filarów każda zmiana to tylko marnowanie czasu.

■ Dobrowolność

W naszym przypadku dobrowolność oznacza, że nie jestem zmuszany do udziału w prowadzeniu zdecentralizowanej sieci reputacji. Nie mogę jednak domagać się ujętego pozytywnie prawa do tego, by sieć nie zapisywała o mnie informacji — to, czy informacja o mnie trafi do sieci reputacji, zależy wyłącznie ode mnie, mojego zachowania, moich czynów i mojej odpowiedzialności.



Dobrowolne — dopóki nie dogoni cię odpowiedzialność.

■ Organizacja

Pojedyncza jednostka nie jest w stanie złamać systemu, dlatego państwo kontroluje zrzeszanie się ludzi jako sposób zapobiegania działaniom, które mogłyby zagrozić jego strukturze i funkcjonowaniu. Nie ma znaczenia, czy ludzie organizują się za czy przeciw. Dzięki organizacji można złagodzić skutki kar wymierzanych dla przykładu, gdy ktoś ośmiela się zmieniać państwo wbrew jego woli.

Nie stawiamy sobie wspólnych celów, ale możemy przejść razem część drogi. Najbardziej naturalną formą jest zrzeszanie się we wspólnotach — muszą one jednak mieć wszystkie potrzebne narzędzia, by nie pozostać jedynie zabawą we wspólnotę.

■ Odporność

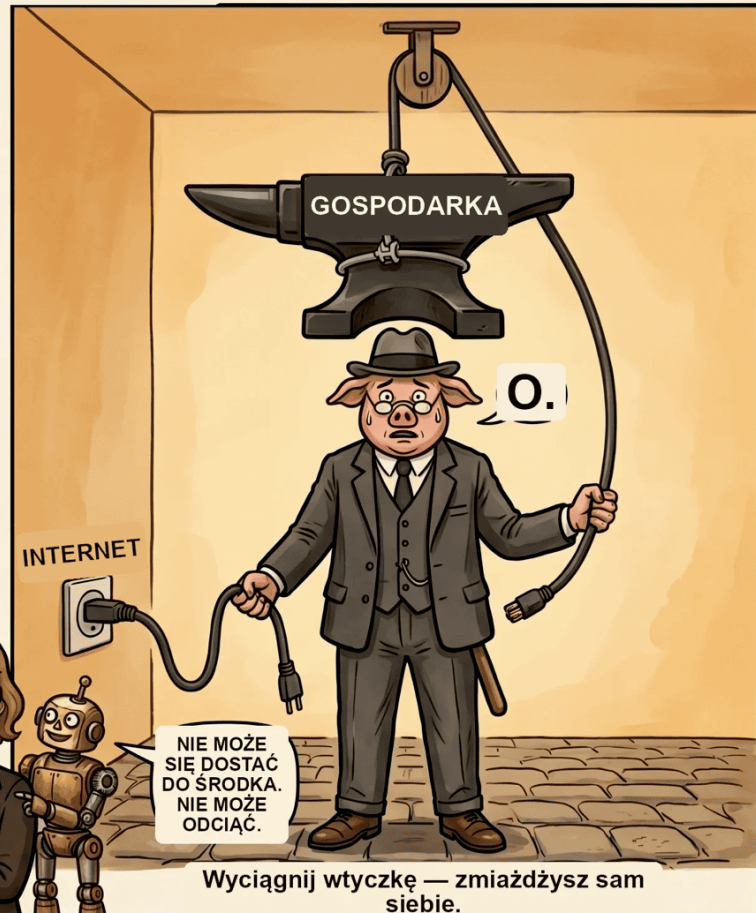
Wybrana droga ku zmianie państwa — albo ku przejściu do jego następcy — nie może zależeć od zezwolenia państwa. Narzędzia i sposoby ich używania muszą być jak najbardziej niecenzurowalne. Mówiąc wprost, koszt ich ocenzurowania musi być astronomiczny. Bez tego cały wysiłek jest tylko marnowaniem czasu i energii życiowej.

WARUNEK 2 Z 5: ORGANIZACJA



Jednostka nie złamie systemu. Społeczność może.

WARUNEK 3 Z 5: ODPORNOŚĆ



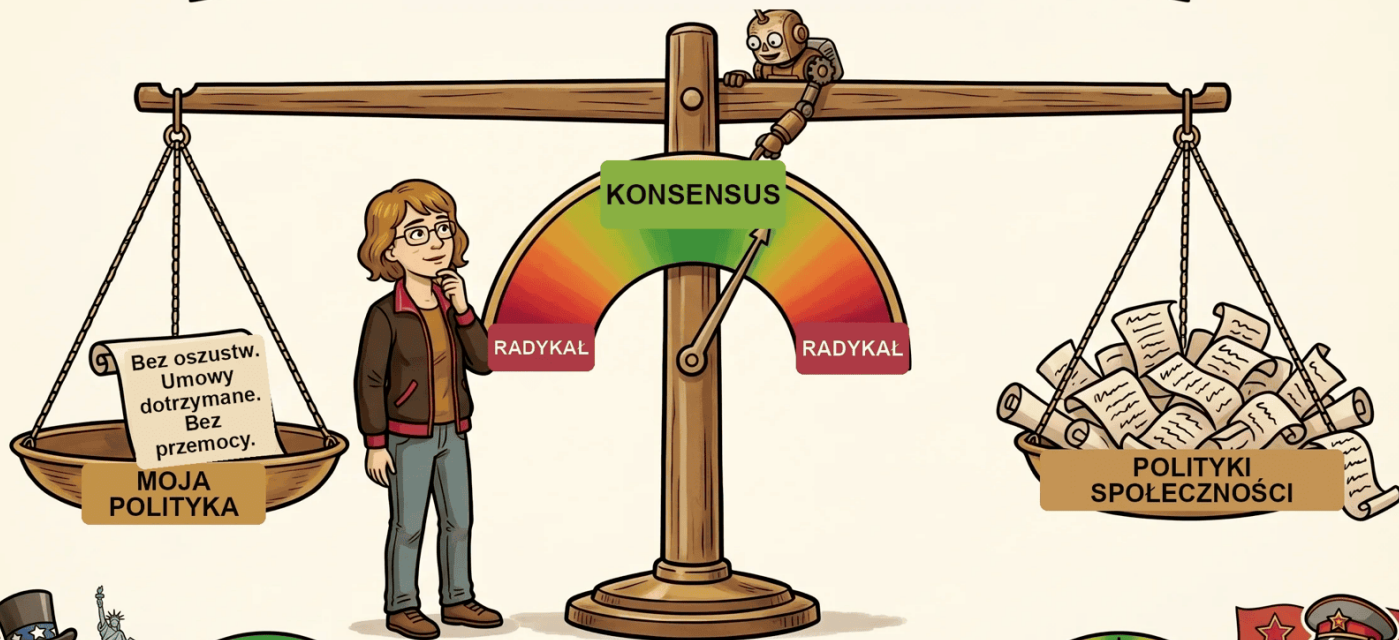
NIE MA O CO PROSIĆ. NIE MA CZEGO ODŁĄCZYĆ.

■ Konsensus

Proponowane rozwiązanie musi z samej swojej natury zawierać mechanizm negocjowania konsensusu, a także element represyjny na wypadek naruszenia konsensusu. Nie musi to być dobrowolne porozumienie typu win-win. Wystarczy, że okoliczności i presja społeczna zapewnią kompromis wewnątrz wspólnoty i między wspólnotami.

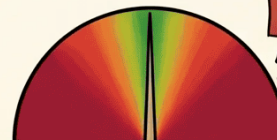
ZOSTAŃ W ZAKRESIE — NIE BĄDŹ RADYKAŁEM.

Możesz się różnić. Tylko nie za bardzo.



Strefa tolerancji rozciąga się
wraz z wolnością kultury.

WARUNEK 4 Z 5: KONSENSUS



KONSENSUS TO STREFA TOLERANCJI, NIE JEDNOMYŚLNA ZGODA.

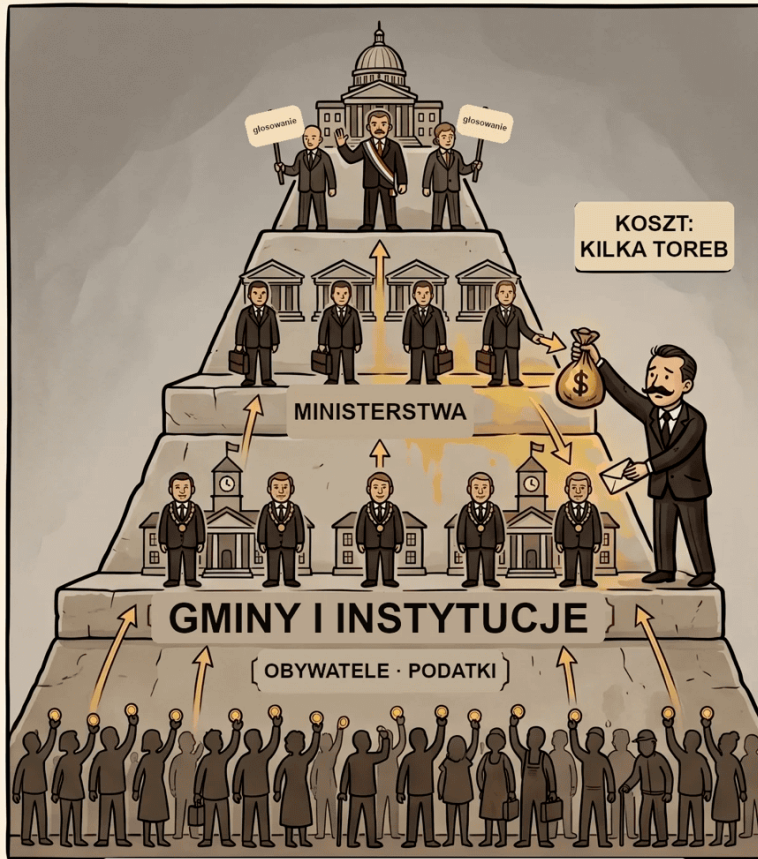
■ Nieprzekupność

Niecenzurowalność broni systemu z zewnątrz. Ale sieć ludzi może też gnić od środka — autorytet zostaje przejęty, deklarowana reguła po cichu porzucona, uczestnicy przekupieni w milczeniu. Niecenzurowalność byłaby pustym zwycięstwem, gdyby ludzi wewnątrz można było bez konsekwencji zepsuć.

Nieprzekupność nie jest wynikiem jednej sprytnej sztuczki. Wyłania się z **kilku zasad proponowanego projektu działających w zgraniu** — presja przeciw korupcji jest rozłożona w całej architekturze, a poszczególne części wzmacniają się nawzajem. Jak dokładnie się to osiąga, pokażemy stopniowo — w opisie narzędzia, w weryfikacji i w rozdziale o karze. Na końcu podsumujemy wszystko, co zostało zbudowane.

Nieprzekupność jest jednocześnie warunkiem projektu i emergentną właściwością rezultatu. Jest drugą linią obrony — tą zwróconą do wewnątrz — a bez niej Odporność jest tylko połową tarczy.

WARUNEK 5 Z 5: NIEPRZEKUPNOŚĆ



Przekup kilka górnych pięter — podstawa i tak zapłaci.



Przekup jednego — traci reputację na zawsze. Przekup wszystkich — wcześniej zbankrutujesz.

KORUPCJA MA CENĘ. W SIECI JEST ONA ZBYT WYSOKA.

Narzędzie

Reputacyjna sieć społecznościowa

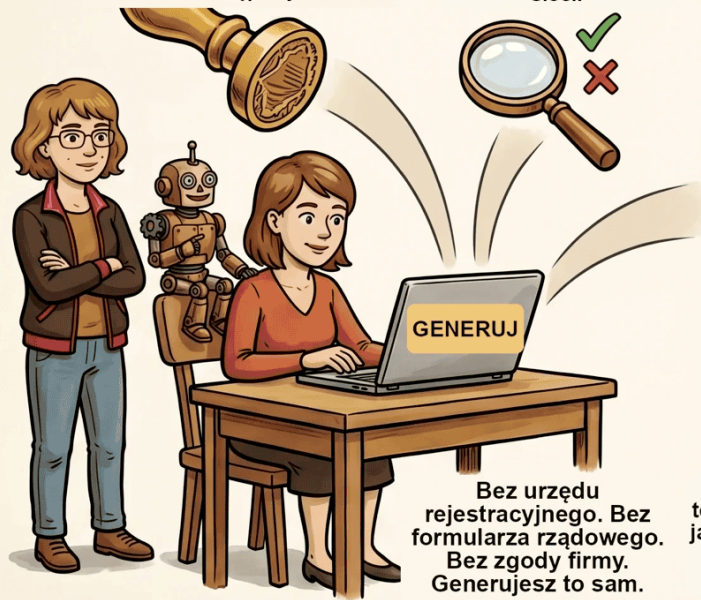
Aby doprowadzić do zmiany, potrzebujemy starannie zaprojektowanego narzędzia. Najpierw naszkicujemy je pokrótce; w kolejnych rozdziałach przyjrzymy się każdemu elementowi dokładniej i dodamy więcej. Wyobraź sobie niecenzurowalną, globalną, zdecentralizowaną sieć społecznościową, w której mógłbyś bezpiecznie utworzyć swoją zastępczą tożsamość i nią zarządzać — tak zwaną tożsamość zdecentralizowaną (DID). DID to cyfrowa tożsamość, którą tworzysz i kontrolujesz sam, bez zależności od jakiegokolwiek centralnej władzy. Nikt nie może jej odebrać ani podrobić, ponieważ jest kryptograficznie podpisana twoim kluczem prywatnym (lub kluczami, poprzez multisig).

TWOJA TOŻSAMOŚĆ, TWOJE KLUCZE, TWOJE ZASADY

TWORZYSZ JĄ SAM

KLUCZ PRYWATNY — podpisuje w twoim imieniu. Tylko ty go posiadasz. Nigdy nie udostępniaj.

KLUCZ PUBLICZNY — weryfikuje twoje podpisy. Widoczny dla sieci.



Bez urzędu rejestracyjnego. Bez formularza rządowego. Bez zgody firmy. Generujesz to sam.

TWÓJ DOKUMENT DID



KLUCZ PUBLICZNY:
[hash kryptograficzny]

ADRES SIECIOWY:
[brama onion]

POLITYKA WERYFIKACJI:
Moje zasady interakcji

TWIERDZENIA:
patrz po prawej

To twoja publiczna tożsamość. Każdy może ją odczytać. Tylko TWÓJ klucz prywatny może podpisać jej zmiany.



TWIERDZENIA — ZWERYFIKOWANE FAKTY O TOBIE

- OBYWATELSTWO:** Republika Czeska — zweryfikowane przez Notariusza Miejskiego
- WYKSZTAŁCENIE:** mgr inż. informatyki — zweryfikowane przez Sieć Absolwentów Uczelni
- WŁASNOŚĆ:** Właściciel mieszkania nr 42 — zweryfikowane przez Lokalny Rejestr Społeczności
- ŚWIADEK BIERNY:** Zignorował wykroczenie — polityka niedotrzymana — zgłoszone przez Świadków Sąsiedzkich
- OSZUSTWO:** Wyłudził oszczędności od sąsiada — zgłoszone przez Lokalny Sąd Społeczności

Twierdzenia to zweryfikowane oświadczenia. Dobre i złe. Autorytety ręczą za nie swoją reputacją.



DOWÓD PAŃSTWOWY — ODWOŁYWALNY: państwo może go unieważnić w każdej chwili.



DID — NIEODWOŁYWALNY: tylko twój klucz prywatny może podpisać zmiany.

Twoja tożsamość. Twoje klucze. Twoje zasady. Bez niczyjej zgody.

Uwaga

Jedną z implikacji jest to, że taka tożsamość mogłaby stopniowo zastąpić wydawane przez państwo dokumenty tożsamości — ale o tym więcej w rozdziale o przejściu.

W takiej sieci mógłbyś zgłosić poprzez swoją tożsamość, że ktoś wyrządził ci krzywdę (a później, potencjalnie, że ją naprawił lub został do tego zmuszony). Aby ta informacja zwrotna — skierowana do sprawcy krzywdy — miała wartość jako istotne źródło, wprowadzenie informacji do sieci musi kosztować czas, energię i pieniądze — a na dodatek trzeba wytworzyć dla innych weryfikowalny dowód, że nie jest to czcza gadanina.

Czytanie informacji byłoby łatwe i stosunkowo tanie, ale utworzenie pojedynczego zapisu byłoby kosztowne i wymagające. Zapis podlegałby jasnemu protokołowi, w którym obliczenie według wybranego algorytmu ściśle wyznacza, którego DID poprosić o weryfikację przesłanej informacji i jak postępować, by wybrany uczestnik przetworzył informację w twoim imieniu, opublikował ją i stał się jej weryfikatorem.

■ Algorytm kontra radykalizm

Algorytmiczny wybór weryfikatorów zapewnia, że nieradykalni wydawcy informacji z czasem utrzymują niemal neutralny bilans między kosztami publikowanych informacji a nagrodami za weryfikację.

PUBLIKACJA KOSZTUJE CZAS, ENERGIĘ I PIENIĄDZE

ZAPIS DO SIECI NIGDY NIE JEST DARMOWY — ODCZYT TAK

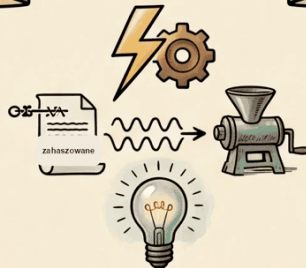
TRZY KANAŁY — WSZYSTKIE TRZY SĄ REALNE

CZAS



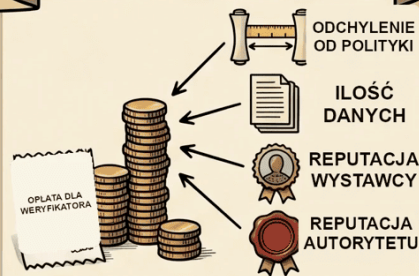
czekasz, aż algorytm wybierze weryfikatora, a weryfikator odczyta twój zapis.

ENERGIA



podpisywanie, haszowanie, weryfikacja — każdy krok to realne obliczenia i realny prąd.

PIENIĄDZE



im dalej twoje twierdzenie odbiega od polityki weryfikatora, im większy zapis i im mniej zaufany wystawca lub jego autorytet — tym wyższa opłata.

CO DZIEJE SIĘ DALEJ

- Trzyetapowy łańcuch weryfikacji — zobacz JAK ALGORYTM WYBIERA WERYFIKATORA, JAK ODPOWIADA WERYFIKATOR, WYBÓR WYSTAWCY
- Dlaczego kosztowny zapis chroni reputację — dalej w tym rozdziale

szum jest kosztowny. Sygnał jest cenny. Dlatego sieć pobiera opłatę za zapis, nie za odczyt.

koszt w kolejnych iteracjach

KAŻDA KOLEJNA PRÓBA KOSZTUJE WIĘCEJ

odpowiedź weryfikatora wchodzi do chronologii — zobacz WYBÓR WYSTAWCY oraz JAK ALGORYTM WYBIERA WERYFIKATORA



każda odmowa lub ponowny rzut powiększa chronologię, którą pochłania algorytm — a kolejna próba jest droższa we wszystkich trzech kanałach.

asymetria odczytu

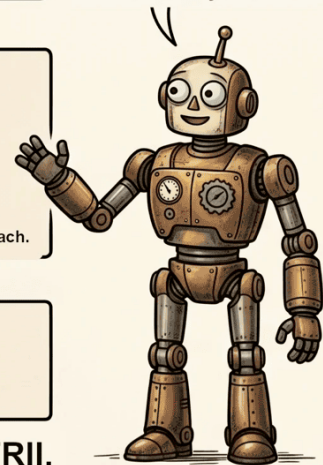
ODCZYT JEST TANI



darmowe zapytania

każdy może odczytać reputację i zapisy — kosztuje tylko zapis. Ta asymetria jest zamierzona.

ZAPIS KOSZTUJE — ODCZYT NIE. O TO WŁAŚNIE CHODZI W TEJ ASYMETRII.



Przyjrzyjmy się, jak algorytm wybiera weryfikatora.

■ Algorytm

Wybór algorytmiczny niedeterministycznie dobiera innego weryfikatora (lub zbiór możliwych weryfikatorów) dla różnych informacji. Hash (jednokierunkowa funkcja matematyczna, która z dowolnego wejścia wytwarza unikalny „odcisk” — jak odcisk palca dokumentu) kompletnego dokumentu DID wyznacza pozycję na spójnym pierścieniu haszującym i wybiera kandydatów na weryfikatorów.

$$\text{verifier_DID} = \text{hash}(\text{DID_document})$$

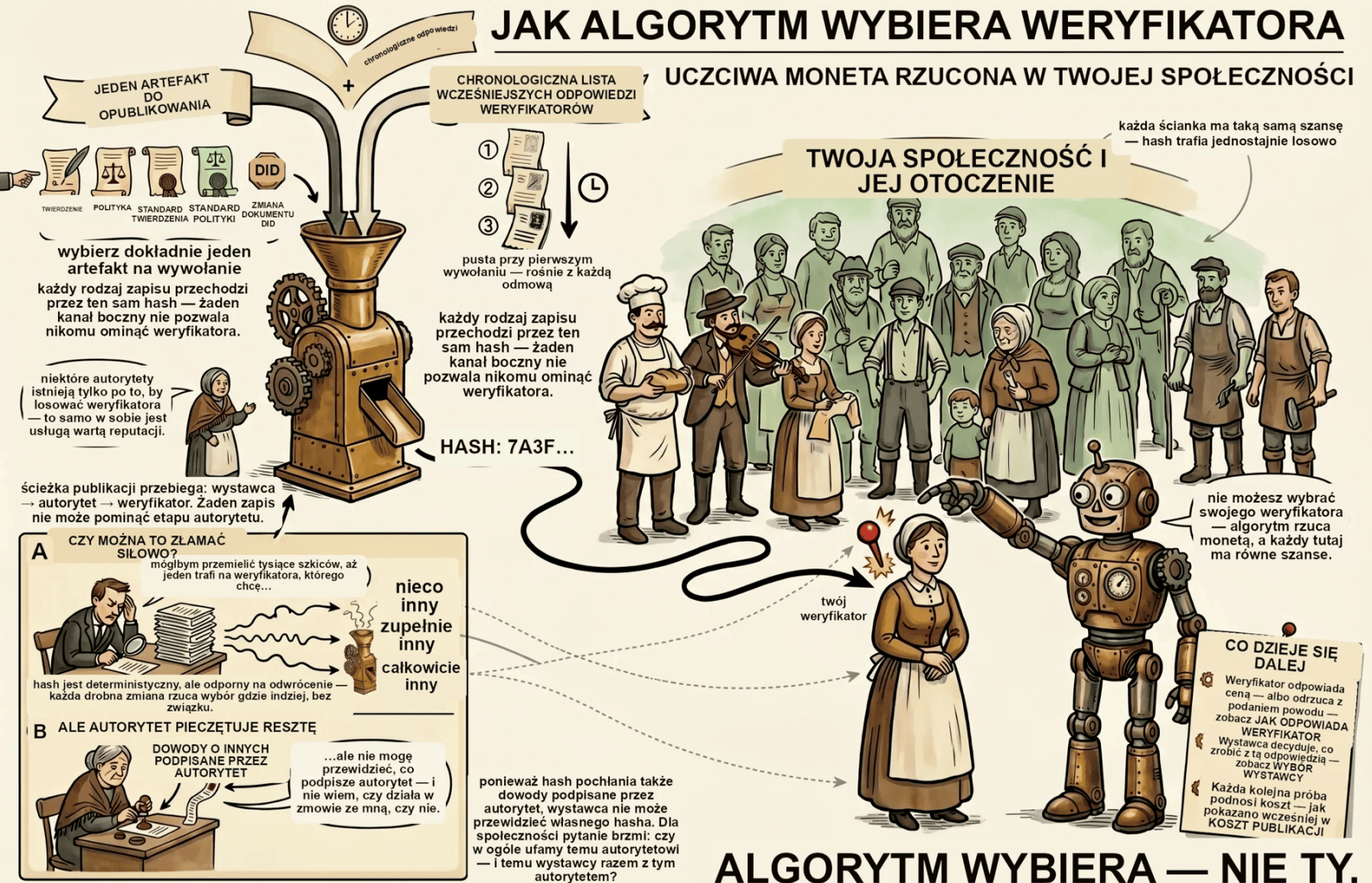
Mówiąc prosto: algorytm bierze cały twój dokument DID, oblicza z niego odcisk, a ten odcisk wyznacza twojego weryfikatora.

U pierwszego weryfikatora, którego wybierze algorytm, ty jako wydawca możesz nie odnieść sukcesu — twoja reputacja albo deklarowane ustawienia mogą nie spełniać jego wymagań. Algorytmicznie kontynuowałbyś poszukiwania kolejnego, wykonując następną rekurencyjną iterację, która przydziela ci dalszego weryfikatora. Z każdym krokiem rośnie „odległość” do docelowego weryfikatora, a wraz z nią towarzyszące metadane, które trzeba opublikować. W miarę jak dane rosną, naturalnie rosną koszty (nie tylko z powodu początkowego rozmiaru tezy, ale i metadanych narastających z każdym odrzuceniem). Wiarygodna informacja przechodzi znacznie łatwiej niż bezsensowne kaprysy. Od każdego zależy, jak

wysoką cenę jest gotów ponieść i jak bardzo zależy mu na zapisie — radykalizm z gwarancją zrobi się drogi.

JAK ALGORYTM WYBIERA WERYFIKATORA

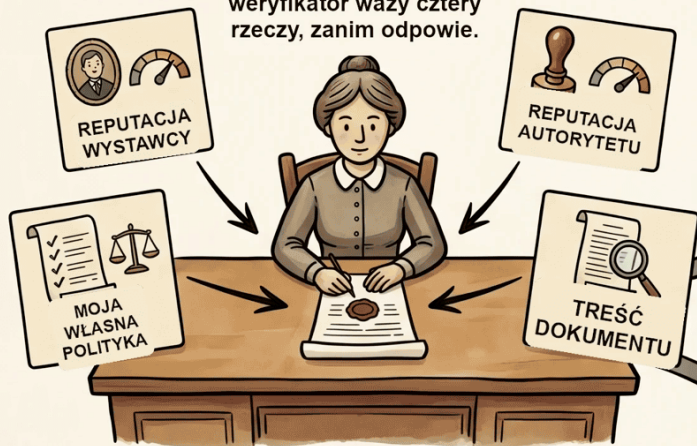
UCZCIWA MONETA RZUCONA W TWOJEJ SPOŁECZNOŚCI



JAK ODPOWIADA WERYFIKATOR

AKCEPTACJA Z CENĄ — ALBO ODMOWA Z POWODEM

weryfikator waży cztery rzeczy, zanim odpowie.

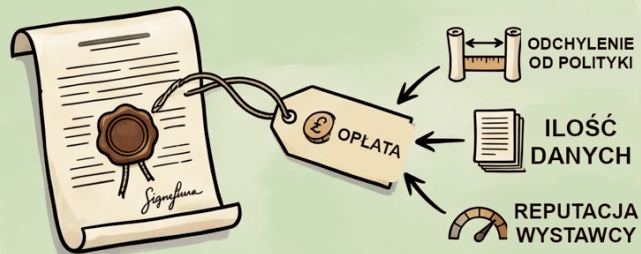


ODMOWA — Z POWODEM

- reputacja wystawcy jest dla mnie zbyt niska
- autorytet stojący za tym zapisem nie jest tym, któremu ufam
- polityka wystawcy zbyt odbiega od mojej, by dało się to pogodzić
- sam dokument nie spełnia zasad mojej polityki

weryfikator zapisuje DLACZEGO — jego odpowiedź wraca jako dane wejściowe do kolejnej próby.

AKCEPTACJA — Z CENĄ



weryfikator zgadza się na publikację — ale cena odzwierciedla, jak daleko twierdzenie odbiega od jego polityki, ile niesie danych i jak bardzo zaufany jest wystawca.

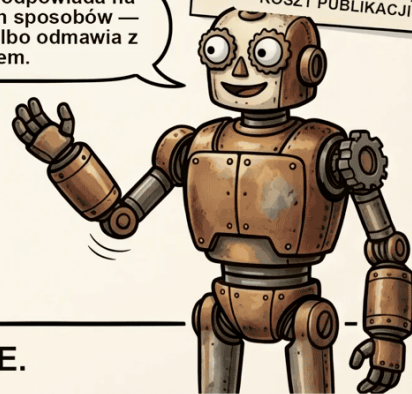
odpowiedź weryfikatora zostaje dodana do chronologicznej listy — jak pokazano w JAK ALGORYTM WYBIERA WERYFIKATORA

cokolwiek powie weryfikator, jego odpowiedź staje się danymi wejściowymi kolejnego wywołania.

każdy weryfikator odpowiada na jeden z tych dwóch sposobów — akceptuje z ceną albo odmawia z powodem.

CO DZIEJE SIĘ DALEJ

- Wystawca decyduje, co zrobić z tą odpowiedzią — zobacz WYBÓR WYSTAWCY
- Każda odpowiedź zmienia koszt kolejnej próby — jak pokazano wcześniej w KOSZT PUBLIKACJI



WERYFIKATOR ALBO USTALA CENĘ — ALBO MÓWI, DLACZEGO NIE.

Cokolwiek weryfikator postanowi w odpowiedzi na twoje żądanie weryfikacji, piłka wraca na połowę wydawcy: może przyjąć ofertę weryfikatora na usługi weryfikacji, dołączyć odpowiedź do chronologii i spróbować ponownie (drożej) albo odejść i przełknąć poniesiony koszt.

Aby nadać swojej informacji większą wagę i lepszą szansę na przyjęcie przez weryfikatorów, ty — jako wydawca zainteresowany wystawieniem informacji — mógłbyś skorzystać z usług **zaufanego autorytetu**. Autorytet albo odrzuca przesłaną informację, albo ją przyjmuje i stawia na nią swoje dobre imię (reputację). Autorytet zazwyczaj żąda dowodów ze świata rzeczywistego, weryfikuje je i klasyfikuje. Wynikiem jest protokół jego oceny danej sprawy w danym czasie. Wyobraź sobie autorytet jako specjalistę od pewnego rodzaju usług zarówno w świecie rzeczywistym, jak i cyfrowym — na przykład śledczego, audytora, ubezpieczyciela, dostawcę pewnej klasy towarów (w istocie dowolnego podmiotu gospodarczego na rynku).

WYBÓR WYSTAWCY

CO ZROBIĆ Z ODPOWIEDZIĄ WERYFIKATORA

niezależnie od tego, co powiedział weryfikator, wystawca ma teraz **JEDNĄ** odpowiedź na stole.



powrót do JAK ALGORYTM WYBIERA WERYFIKATORA — pokazano wcześniej

pętlę tworzy tylko ścieżka ponownej próby — akceptacja i odejście kończą historię.

TRZY WYJŚCIA

PRZYJMIJ OFERTĘ

sieć DID



TYLKO W PRZYPADKU AKCEPTACJI

wystawca płaci opłatę — zapis zostaje opublikowany w sieci. Dostępne tylko, jeśli weryfikator zaakceptował.

SPRÓBUJ PONOWNIE



mini maszyna do mielenia



każda kolejna próba kosztuje więcej

odpowiedź zostaje dołączona do chronologii — algorytm rzuca ponownie. Działa niezależnie od tego, czy weryfikator zaakceptował po cenie, która nie odpowiada wystawcy, czy odmówił wprost.

ODEJDŹ



czas i energia już poniesione nie wracają

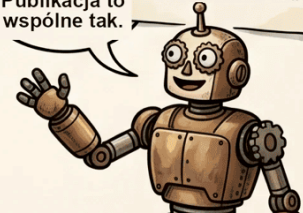


wystawca porzuca szkic. Nic nie zostaje opublikowane — ale też nic więcej nie trzeba zapłacić.

CO DZIEJE SIĘ DALEJ

weryfikator decyduje jak — wystawca decyduje czy. Publikacja to wspólne tak.

Każda kolejna próba zmienia koszt następnej — jak pokazano wcześniej w KOSZT PUBLIKACJI
Sama odpowiedź weryfikatora — jak pokazano wcześniej w JAK ODPOWIADA WERYFIKATOR

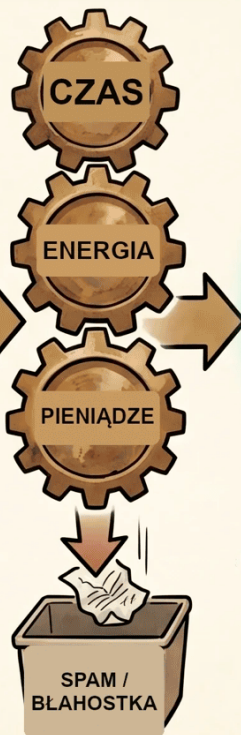


WERYFIKATOR PROPONUJE — WYSTAWCA DECYDUJE.

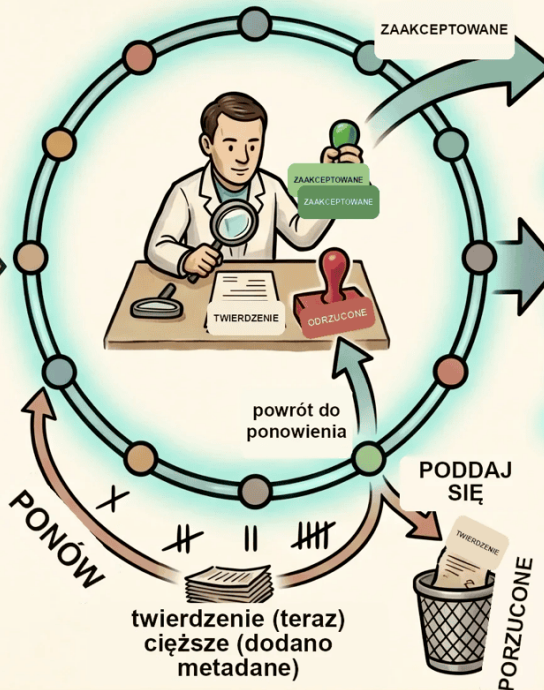
ETAP 1 — PUBLIKACJA TWIERDZENIA



ETAP 2 — FILTR JAKOŚCI



ETAP 3 — WERYFIKACJA REKURENCYJNA



ETAP 4 — TRWAŁY ZAPIS



Trwale.
Weryfikowalne.
Publiczne.

DROGO SFAŁSZOWAĆ. TANIO ZWERYFIKOWAĆ.

Zanim spróbujesz opublikować informację w sieci, będzie ona już prawdopodobnie zawierać informacje o swoich uczestnikach — to sygnały reputacyjne. Poruszanie się po tym, jak czytać sygnały reputacyjne — co znaczą dla ciebie w różnych sytuacjach i jakie niosą ryzyka — może nie być trywialne. Każdy uczestnik może patrzeć na zapisy reputacyjne inaczej poprzez swój DID, zależnie od sytuacji, którą rozgrywa wobec drugiej strony. Czy druga strona jest rzetelnym płatnikiem, czy muszę zażądać pieniędzy z góry za transakcję handlową? Czy oferowany produkt nosi recenzje o ukrytym oszustwie lub wadach? Czy próbują wywinąć się od odpowiedzialności kontraktowej, gdy coś idzie nie tak? Czasem przydaje się bardziej złożony obraz ogólnej spójności drugiej strony — zależy to od preferencji tego, kto zamawia przegląd. Rynek mógłby oferować produkty i usługi, które upraszczają, przetwarzają i wyjaśniają odczyt reputacji w kontekście danej sytuacji. Do tego celu mogą służyć również różne autorytety i oferowane przez nie usługi.

JAK CZYTAĆ REPUTACJĘ

ŚWIADOMA DECYZJA



Ona wie, z kim ma do czynienia.

ŚLEPE ZAUFANIE



On nie ma pojęcia, z kim ma do czynienia.

ZANIM UDZIELISZ KREDYTU. ZANIM PODPISZESZ. ZANIM ZAUFASZ.

■ Przykłady

Typowe informacje interesujące wydawców — i cenne dla innych — dotyczą zdarzeń wykraczających poza zwykłą komunikację międzyludzką w świecie rzeczywistym lub wirtualnym.

Przykłady negatywne: - dowody czynów przestępczych (np. zaudytowane przez zaufany organ śledczy) - dowody poszlakowe (słabe same w sobie, ale statystycznie kumulatywne) — np. wielokrotna obecność w pobliżu kilku kradzieży w krótkim czasie → wciąż przypadek? - naruszenie umowy

Przykłady pozytywne: - naprawiona krzywda (dobrowolnie lub pod presją wspólnoty jako kara) - przyjęcie i odbycie kary zaproponowanej przez autorytet X - autorytet X cofnął w pewnym zakresie uznanie praw własności sprawcy

Od każdego zależy, by zebrać dostępne informacje o drugiej stronie i ocenić ryzyko według własnych preferencji.

JAKIE RODZAJE TWIERDZEŃ MOGĄ SIĘ POJAWIĆ?

PRZYKŁADY ARTEFAKTU TWIERDZENIA

(twierdzenie to stwierdzenie o kimś)
— oto rodzaje, jakie ludzie publikują.)

—

TWIERDZENIA NEGATYWNE



NAPAŚĆ
fizyczny atak na inną osobę



KRADZIEŻ
zabranie cudzej własności bez zgody



OSZUSTWO
oszukiwanie kogoś dla własnej korzyści



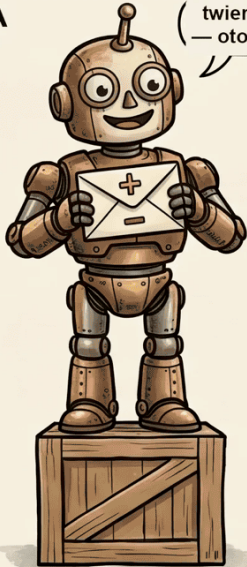
ZŁAMANA UMOWA
niedotrzymanie uzgodnionego zobowiązania



ZNIESŁAWIENIE
rozpowszechnienie szkodliwej nieprawdy



PORZUCENIE
zaniedbanie osób zależnych lub obowiązków



+

TWIERDZENIA POZYTYWNE



NAPRAWIONA SZKODA
naprawienie wcześniej wyrządzonej szkody



SPŁACONY DŁUG
spłacenie długu w całości



UDZIELONA POMOC
pomoc innej osobie kosztem własnym



ZWERYFIKOWANA EKSPERTYZA
udowodniona umiejętność w rzemiośle lub dziedzinie



WYBITNA ZASŁUGA
wieloletni wkład w społeczność

to tylko przykłady — każde twierdzenie jest zgodne ze standardem twierdzenia, a każdy standard może dodać więcej.

nie musisz dołączać — ale jeśli twoje zachowanie wpływa na innych, ktoś może opublikować o tym twierdzenie.

TWIERDZENIA SĄ SPOSOBEM, W JAKI ZACHOWANIE WCHODZI DO SIECI.

■ **To, czy informacja o tobie pojawi się w sieci, zależy wyłącznie od twojego własnego zachowania.**

Nigdy nie musisz dołączać do takiej sieci, a mimo to informacja o tobie może się w niej pojawić. Zależy to wyłącznie od twoich czynów i wpływu, jaki mają na innych.

SPOŁECZNOŚĆ MOŻE OTWORZYĆ GO ZA CIEBIE



Nie ma własnego DID.
Nigdy się nie zarejestrował.



Nie otworzyłeś DID, więc społeczność
otwiera go O TOBIE. Tu dołączane są
negatywne twierdzenia.



Możesz otworzyć własny
— ale społeczność
połączy oba. Reputacja
podąża za osobą, nie za
kluczem.

1. WYRZĄDZASZ SZKODĘ -----> 2. SPOŁECZNOŚĆ ZGŁASZA ----->

3. NIE MOŻESZ UCIEC ----->

Możesz zrezygnować z otwarcia DID. Nie możesz zrezygnować z własnej reputacji.

To, co przed chwilą pokrótce naszkicowałem, to sposób, w jaki mogłaby działać sieć społecznościowa zainspirowana tożsamością zdecentralizowaną (DID). Podstawowym celem koncepcji DID jest wzmocnienie prywatności i wolności poprzez zasadę subskrybowania reguł, których będę przestrzegać i według których będę żyć — dającej użytkownikom możliwość decydowania, jakie informacje udostępniać i na jakich warunkach.

Proponuję dalej połączyć DID w sieć komunikacyjną, w której ich posiadacze wymieniają informacje zwrotną nawet poza sytuacjami, gdy coś się komuś stało i wspólnota lub jednostka musi zareagować. Takie prewencyjne porównywanie reguł, do których się zapisaliśmy — z możliwością obliczenia ekonomicznych i innych konsekwencji wzajemnych odchyłeń w oczekiwaniach co do tego, jak druga strona powinna działać — można by uznać za motywację do znajdowania konsensusu. Zamiast wolności taki system kładłby nacisk na dobrowolne podejmowanie decyzji połączone z odpowiedzialnością za zachowanie w świecie rzeczywistym.

Jednostka nie jest w stanie złamać systemu sama — grupa ludzi ma większą szansę, a grupa ludzi z wynegocjowanym konsensusem i motywacjami, by w wielu kwestiach ciągnąć wspólnie, ma jeszcze większą szansę na oparcie się tendencjom autorytarnym. Warunek organizacji z pierwszego rozdziału zostanie spełniony, gdy zajdą dwa warunki: sieć reputacji DID obejmie wspólnoty na tyle reprezentatywnie, że jej używanie przestanie być egzotyczne. A jednocześnie ten segment wspólnoty stanie się ekonomicznie znaczącą mniejszością, która potrafi asertywnie negocjować z resztą społeczeństwa.

■ Dobrowolność kontra wolność

Wolność — w sensie pozytywnym — byłaby wtórnym efektem równoważenia dwóch czynników: dobrowolności i presji otoczenia ku odpowiedzialności.

■ Era AI i wartość reputacji

W erze sztucznej inteligencji automatyzowane jest wszystko, co związane z myśleniem poznawczym — i może to pójść jeszcze dalej. Co wtedy pozostaje w ludzkiej aktywności jako przewaga konkurencyjna? Odpowiedź jest trudna i coś na pewno się znajdzie, ale jedno możemy powiedzieć z pewnością: zadecyduje reputacja. Weryfikowalna historia twojego zachowania, twoich zobowiązań i ich wypełnienia — tego AI za ciebie nie zbuduje.

JEŚLI AI MYŚLI ZA CIEBIE — CO ZOSTAJE DLA CIEBIE?

AGENCI AI PRZEJMUJĄ POWTARZALNĄ PRACĘ

USTANDARDYZOWANE
PROCESY FIRMOWE

KSIĘGOWOŚĆ

SPORZĄDZANIE
PROJEKTÓW

jedna po drugiej, powtarzalna praca
umysłowa jest przekazywana agentom.

CO WIĘC ZOSTAJE DLA CZŁOWIEKA?



każdy może wybrać ten sam pomysł.

co odróżnia jednego piekarza, jednego
stolarza, jeden warsztat AI od kolejnego?

REPUTACJA — CO ODRÓŻNIA JEDNO OD
DRUGIEGO



to ludzki dotyk
wciąż domyka
transakcję.

ktoś musi odpowiadać za to, co robi agent
— a tej odpowiedzialności nie da się
przekazać dalej.

bez reputacji każdy piekarz wygląda tak samo — a najsilniejsza marka pożera wszystkich.

czy to może być zdecentralizowana droga, która trzyma AI na smyczy — coś, co nie pozwala jednemu graczowi przejąć całego rynku?

AI AUTOMATYZUJE PRACĘ — REPUTACJA UTRZYMUJE W TOBIE CZŁOWIEKA.

EKONOMIA PRAWDY

pasek społeczności



JEDNA SPOŁECZNOŚĆ. RÓŻNE STANOWISKA.

NIEPOPULARNE, ALE DOPUSZCZALNE

W KONSENSUSIE

POZA KONSENSUSEM

ZGŁOSZENIE



LOSOWANIE



ZWROT



REJESTR

DOLNY PASEK OBSERWATORA

ALGORYTM WYBIERA UCZCIWIE. LUDZIE WYCENIAJĄ TO, W CO WIERZĄ.

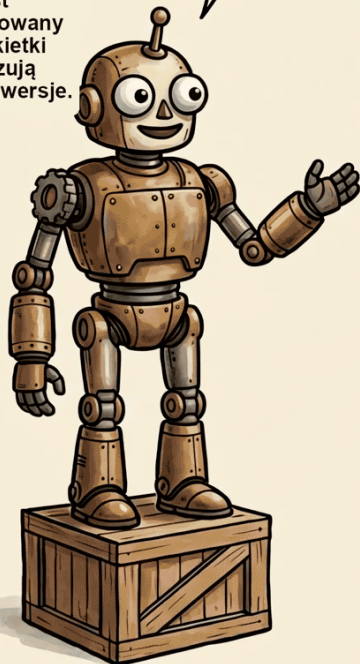


LOSOWANIE JEDNOLITE. REAKCJA NIEJEDNOLITA. IM DALEJ OD KONSENSUSU, TYM WYŻSZA CENA.

CO JEST PUBLIKOWANE W SIECI

pięć rzeczy można opublikować — każda ma swoje wersje.

każdy artefakt jest wersjonowany — plakietki pokazują aktualne wersje.



v1

DOKUMENT DID

twój zapis tożsamości w sieci — klucze, metadane, adres sieciowy.

ZARZĄDZA: posiadacz DID



v2

STANDARD TWIERDZENIA

schemat, którego musi przestrzegać twierdzenie — co liczy się jako ważny dowód.

ZARZĄDZA: autorytet z reputacją w danej dziedzinie



v3

STANDARD POLITYKI

schemat, którego musi przestrzegać polityka — kształt reguł akceptacji.

ZARZĄDZA: autorytet z reputacją w danej dziedzinie

↓ pochodzi od

↓ pochodzi od



v4

TWIERDZENIE

twierdzenie o podmiocie, zgodne ze standardem twierdzenia — publikowane przez wystawcę, współpodpisywane przez autorytet standardu, jeśli zażąda tego zarówno wystawca, jak i weryfikator.

ZARZĄDZA: wystawca publikuje — podmiot jest celem

twierdzenia występują w dwóch rodzajach — pozytywne (+) i negatywne (-).



v5

POLITYKA DID

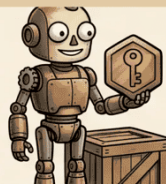
zadeklarowane reguły DID — używane przy weryfikacji, konsensusie i wystawianiu.

ZARZĄDZA: posiadacz DID (jedna polityka na DID)

KAŻDY ARTEFAKT JEST WERSJONOWANY. KAŻDA WERSJA JEST PUBLICZNA.

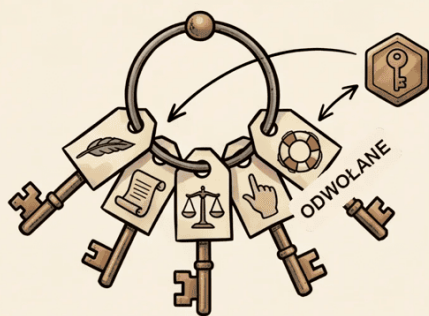
CO ZAWIERA DOKUMENT DID?

PRZYKŁADY ARTEFAKTU DOKUMENTU DID



twój dokument DID to twoja karta tożsamości w sieci — oto, co zawiera.

POLA, KTÓRE ZNAJDZIESZ W ŚRODKU



KLUCZE I REGUŁY PODPISYWANIA

każdy klucz nadaje jedno uprawnienie — edycję tego dokumentu, wystawianie twierdzenia, działanie jako autorytet, zarządzanie polityką lub delegowanie odzyskiwania. Uprawnienia można przekazać innemu DID, a później znowu je odebrać.



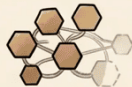
ADRESY SIECIOWE

gdzie sieć może cię znaleźć — można zmieniać bez przepisywania tożsamości



UTWORZONY I WERSJONOWANY

kiedy ta tożsamość powstała i którą wersję właśnie czytasz



POWIĄZANE TOŻSAMOŚCI

podsumowanie DID, z którymi masz powiązanie — widok dla wygody, technicznie przechowywany gdzie indziej



ZNACZNIK NASTĘPSTWA

jeśli twoja tożsamość zostanie utracona lub skradziona, autorytet może oznaczyć ten DID jako zakończony i wskazać twojego następcę

posiadacz DID pisze każdą nową wersję — ale każda wersja musi przejść weryfikację, zanim się ją opublikuje.

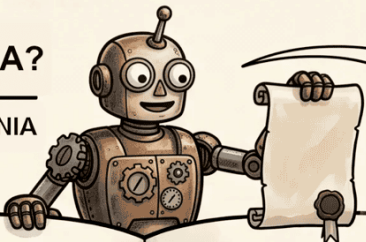
ty to piszesz — sieć to weryfikuje. Nie możesz po prostu ogłosić własnego istnienia.



TY TWORZYSZ SWOJĄ TOŻSAMOŚĆ — SIEĆ JĄ POTWIERDZA.

CZYM JEST STANDARD TWIERDZENIA?

PRZYKŁADY ARTEFAKTU STANDARDU TWIERDZENIA



standard to pusty formularz —
twierdzenie to wypełniony
formularz. Pokażę ci oba obok
siebie.

STANDARD — PUSTY FORMULARZ		TWIERDZENIE — WYPEŁNIONY FORMULARZ
 DID PODMIOTU DID, którego dotyczy to twierdzenie	↔	 DID PODMIOTU did:nwo:alice-9f2b...
 DID WYSTAWCY DID podpisujący twierdzenie	↔	 DID WYSTAWCY did:nwo:magistrates-04...
 KIEDY I GDZIE data i miejsce	↔	 KIEDY I GDZIE 3 marca, rynek
 ZATWIERDZONE RODZAJE DOWODÓW liczą się tylko te rodzaje dowodów	↔	 ZATWIERDZONE RODZAJE DOWODÓW fotografia ✓ — przysięga świadka ✓ — zaświadczenie lekarskie ✓
 brak / łagodny / umiarkowany / poważny SKALA WYNIKU wybierz dokładnie jeden stopień — bez dowolnego tekstu	↔	 ZATWIERDZONE RODZAJE DOWODÓW umiarkowany — stopień 2 z 4

każde pole po lewej ma dokładnie jeden wypełniony odpowiednik po prawej — to właśnie sprawia, że dwa twierdzenia tego samego rodzaju są porównywalne.

pieczęć autorytetu na wypełnionym
twierdzeniu to zobowiązanie: proces
został rzeczywiście zachowany.



stawiam swoją reputację
na to, że zostało to
przetworzone zgodnie
ze standardem.



NAPASĆ
v3



DLUG
v2



POMOC
MEDYCZNA
v4



RZEMIOSŁO
v1

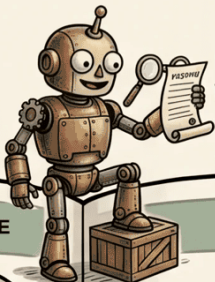


ZEZNANIE
v5

STANDARD TO FORMULARZ — TWIERDZENIE TO WYPEŁNIONY I POŚWIADCZONY FORMULARZ.

CZYM JEST POLITYKA DID?

PRZYKŁADY ARTEFAKTU POLITYKI DID



moja polityka nie dotyczy tego, jak napisane jest twierdzenie — to zadanie standardu. Moja polityka dotyczy tego, jak decyduję, czy w ogóle zwracać uwagę na to twierdzenie: czy ufam temu, kto je podpisał, czy ufam autorytetowi stojącemu za jego standardem, i czy sprawa w ogóle zasługuje na moją uwagę?

STANDARD — ODZIEDZICZONE USTAWIENIA DOMYŚLNE		MOJA POLITYKA — WYPROWADZONA Z TEGO	
	NAMINA REGULA MINIMALNA REPUTACJA WYSTAWCY akceptuję wystawców z reputacją powyżej pięciu na dziesięć		NAMINA REGULA MINIMALNA REPUTACJA WYSTAWCY zaostżone — wymagam siedmiu na dziesięć
	LISTA ZAUFANYCH AUTORYTETÓW akceptuję standardy od każdego autorytetu, którego własna reputacja przekracza cztery na dziesięć		LISTA ZAUFANYCH AUTORYTETÓW w pełni ufam sędziom pokoju i lekarzom; zmniejszam o połowę wagę twierdzeń nadzorowanych przez straż miejską; całkowicie odrzucam wszystko spod policji portowej
	FILTR ISTOTNOŚCI przetwarzam każde twierdzenie, którego waga sprawy przekracza poziom „błahy”		FILTR ISTOTNOŚCI błahę, uciążliwe twierdzenia nic mnie nie kosztują, by je zignorować — po prostu ich nie czytam
	ANTYSPAMOWA KRZYWA CENOWA zgłoszenie do mnie jest tanie dla istotnych, rzadkich twierdzeń — i szybko drożeje dla błahych lub powtarzających się		ANTYSPAMOWA KRZYWA CENOWA zachowane — domyślna krzywa mi odpowiada
	ŁĄCZNE WAŻENIE reputacja wystawcy i reputacja autorytetu mnożą się; błahość sprawy zmniejsza wynik o połowę		ŁĄCZNE WAŻENIE usunęte — używam własnego wzoru
polityka nie przepisuje standardu — ocenia ludzi i sprawę. Zachowaj, zmodyfikuj, usuń, dodaj — cztery proste posunięcia na wspólnym punkcie wyjścia.			WYKŁADNICZY KOSZT PRZY POWTARZAJĄCYCH SIĘ TWIERDZENIACH dodane — każde nowe twierdzenie od tego samego wystawcy na mój temat w ciągu roku kosztuje dziesięć razy więcej niż poprzednie
			GODZINY CISZY dodane — odmawiam czytania jakiegokolwiek twierdzenia złożonego między północą a świtem



WERYFIKACJA — moja polityka filtruje zarówno przychodzące twierdzenia, jak i moje własne szkice, zanim je wystawię. Wystawienie to weryfikacja na wyjściu.

KONSSENSUS — moja polityka jest moim głosem, gdy społeczność negocjuje wspólne reguły.

TWOJA POLITYKA OCENIA POSŁANCA — NIE FORMULARZ.



Dlaczego sieci nie da się ocenzurować

Jak dotąd opisaliśmy, co sieć potrafi. Teraz skupmy się na tym, dlaczego nie da się jej wyłączyć ani ocenzurować.

Sieć zostanie prawdopodobnie zbudowana na zasadach sieci Tor i trasowania cebulowego (sposobu maskowania ruchu sieciowego z użyciem zasad Mixnet) — technologii, w której komunikacja przechodzi przez kilka warstw szyfrowania i żaden pojedynczy węzeł nie zna jednocześnie nadawcy i odbiorcy. Centralna instytucja nie może zajrzeć ci przez ramię, bo nie ma miejsca, z którego mogłaby patrzeć.

Możesz z tym walczyć, ale nie możesz wygrać — chyba że pogrążysz cały kraj w totalitarnej inwigilacji na poziomie pojedynczych pakietów sieciowych i niskopoziomowych działań na każdym elemencie sprzętu, który łączy się z internetem i komunikuje w danej sieci reputacji. I dokładnie przed takim wyborem stoi centralizm: albo pogodzić się z tym, że obywatele mają narzędzie poza twoim zasięgiem, albo zakopać się w ciemnych kątach gospodarczej stagnacji w imię totalitarnej kontroli.

Nie miejmy złudzeń — nawet reżimy demokratyczne będą tego próbować w walce o centralizm. Prędzej zakuja ludzi w kajdany, niż oddadzą władzę.

JAK TWOJE WIADOMOŚCI POZOSTAJĄ NIEMOŻLIWE DO ŚLEDZENIA

DWIE LINIE OBRONY NARAZ — WARSTWY I SZUM

TREŚĆ: OWINIĘTA W WARSTWY

(technika stojąca za Tor — „trasowanie cebulowe”)

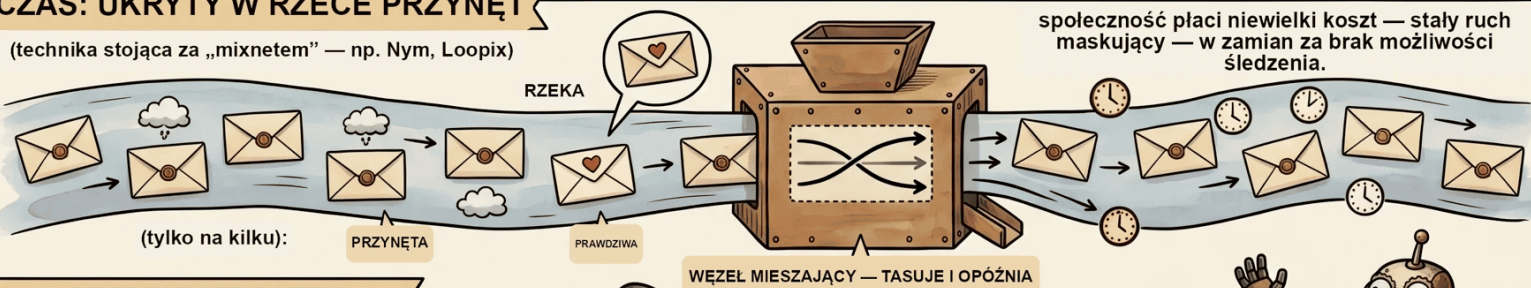


NADAWCA



CZAS: UKRYTY W RZECIE PRZYNĘT

(technika stojąca za „mixnetem” — np. Nym, Loopix)



DWIE TARCZE RAZEM

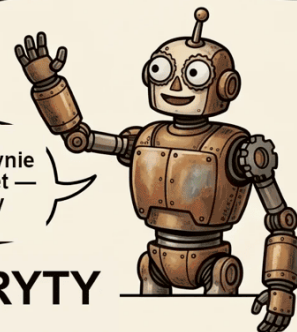
MATRIX	UKRYWA KTO ↔ Z KIM?	UKRYWA KIEDY?
TYLKO WARSTWY	✓ TAK	✗ NIE
TYLKO SZUM	✗ NIE	✓ TAK
WARSTWY + SZUM	✓ TAK	✓ TAK

(trasowanie cebulowe + mixnet — tak naprawdę, toowej potrzebujemy)



sto kopert na godzinę — która z nich ma znaczenie?
obserwator widzi przepływ, ale nie potrafi odróżnić PRAWDIWEJ od PRZYNĘTY.

prawdziwa wiadomość płynie w rzece przynęt — i nosi cztery płaszcze.



TREŚĆ UKRYTA WARSTWAMI — CZAS UKRYTY SZUMEM.

Odpowiedzi na oczywiste wątpliwości

Opisany system w naturalny sposób rodzi szereg pytań. Odpowiedzmy na najczęstsze.

Zależność od technologii

Zapewne już zauważyłeś, że w przeciwieństwie do nowoczesnego państwa — które towarzyszy nam od jakichś 150 lat — opisane tu rozwiązanie w postaci sieci reputacji silnie zależy od technologii globalnego/lokalnego internetu. W razie awarii funkcjonowanie takiej sieci jest zagrożone.

Jeśli awaria jest tymczasowa, nie dochodzi do utraty danych ani spójności tez w sieci, a osiągnięte we wspólnotach bilanse reputacji również nie powinny zostać zaburzone. W przeciwieństwie do porównywalnych sieci płatniczych ta sieć zakłada bardzo niskie częstotliwości procesów i elementów danych. Pod tym względem zdecentralizowana sieć reputacji nie różni się od dzisiejszego państwa, które również jest teraz silnie zależne od technologii i zapomniało, jak pracować z papierowymi kartotekami (choć w planach kryzysowych nie miałyby wyboru).

Ewolucyjny następca państwa w postaci sieci reputacji może w razie trwałej awarii (katastrofy o niespotykanej skali) cofnąć się do bardziej prymitywnego systemu scentralizowanego — państwa.

Technologia pozwala ludzkości sięgać po wyższe cywilizacyjne formy zarządzania i przynosi nam korzyści, ale i ryzyka.

Czy publikując w sieci, nie wyrzucam pieniędzy w błoto?

Koszty opublikowania tezy w sieci reputacji w dużej mierze nie są kosztami utopionymi. Użyteczność komunikatu wydawcy wprowadzonego do sieci — informacji o realnych krzywdach, zweryfikowanych doświadczeniach, istotnych ostrzeżeniach — statystycznie zwraca się w dłuższym horyzoncie czasowym

DWIE ŚCIEŻKI — PAŃSTWO SIĘ ZAMYKA, SIEĆ SIĘ OTWIERA

SIEĆ REPUTACJI

BEZCZYNNOŚĆ
TO WYBÓR
PRAWYCH
DRZWI.

PAŃSTWO

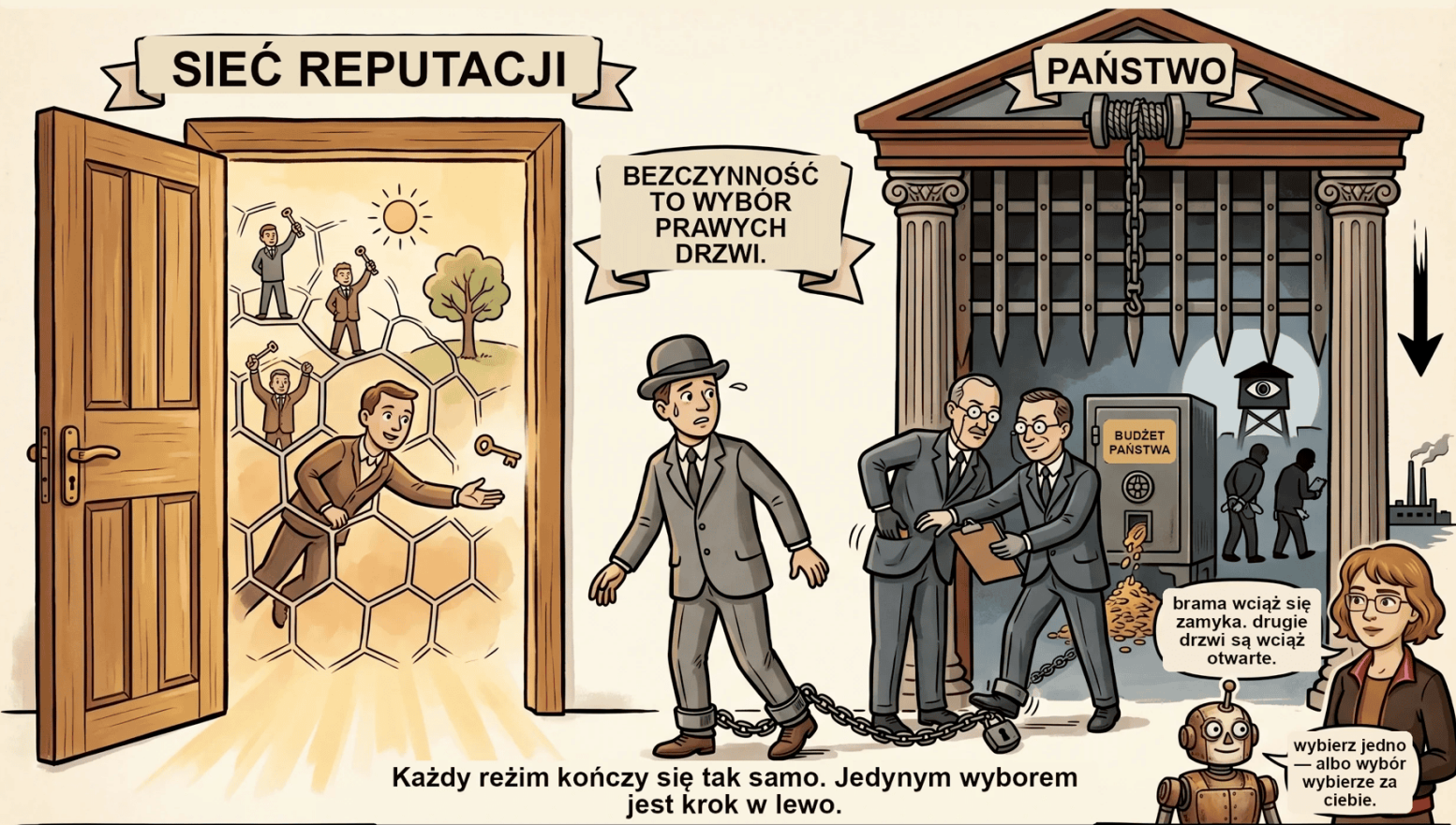
BUDŻET
PAŃSTWA

brama wciąż się
zamyka. drugie
drzwi są wciąż
otwarte.

wybierz jedno
— albo wybór
wybierze za
ciebie.

Każdy reżim kończy się tak samo. Jedynym wyborem
jest krok w lewo.

PAŃSTWO ZAMYKA SIĘ DOMYŚLNIE. SIEĆ OTWIERA SIĘ Z WYBORU.



w postaci opłat za weryfikowanie cudzych tez ze wspólnoty. Wspólnota zyskuje, wydawca buduje reputację, a koszty publikowania prawdziwych informacji zbliżają się tym samym do zwrotnej kaucji, od której trzeba odjąć jedynie mniejszą część rzeczywistych kosztów utrzymania sieci. I odwrotnie, zapisy nieprawdziwe lub błahe się nie zwracają — ich koszty są czystą stratą. Uczciwość jest więc nie tylko wyborem moralnym, ale i ekonomicznie racjonalną strategią.

Po odjęciu kosztów utrzymania sieci zasadę tę można by nazwać zasadą neutralności ekonomicznej — nie tracę, gdy jestem ze wspólnotą, tracę, gdy jestem przeciw niej.

Wspólnota ma też kanały solidarnościowe, by doceniać uczciwe podejście swoich członków. Ale nie miejmy złudzeń: apele o solidarność najczęściej rodzą się z presji społecznej wspólnoty, więc może to nie być solidarność w dobrowolnym znaczeniu tego słowa.

A co, jeśli ktoś stworzy wiele tożsamości?

Człowiek może prowadzić równolegle wiele tożsamości DID. Jednak budowanie reputacji dla każdej z nich wymaga niezależnego wysiłku — czasu, energii, pieniędzy.

Bez skrótów: każda tożsamość musi zgromadzić swój track record¹ poprzez faktyczną aktywność. Utrzymywanie równoległych tożsamości jest więc celowo drogie.

W wolnych społeczeństwach koszty zniechęcają do nadużyć.

¹**Track record** — ogólnie: historia dotychczasowych wyników, sukcesów i porażek osoby lub organizacji. Tutaj: suma wszystkich dotychczasowych interakcji danej tożsamości DID w sieci — zweryfikowanych tez, przyjętych i odrzuconych zapisów — z których wywodzi się jej reputacja.

W dyktaturach jednak równoległe tożsamości stają się narzędziem przetrwania: umożliwiają organizowanie podziemnych sieci, bezpieczniejsze poruszanie się po czarnym rynku i przedziałowy² opór, w którym skompromitowanie jednej tożsamości nie ujawnia pozostałych — a po upadku reżimu pozwalają na bezproblemowy powrót do życia publicznego i zbudowanej tam reputacji, a nawet na scalenie wcześniej oficjalnego i tajnego DID w jeden połączony zestaw zapisów poprzez tezę.

²**Compartmentalization** (od ang. *compartment* — przedział) oznacza oddzielanie informacji na izolowane jednostki tak, by ujawnienie jednej jednostki nie skompromitowało pozostałych. Zasada znana ze służb wywiadowczych: agent zna tylko swoją część operacji, więc nawet pod przymusem nie może wyjawić całości.

TEN SAM WYSIŁEK — MARNOTRAWNY PLAN B W WOLNOŚCI, KOŁO RATUNKOWE POD TYRANIĄ

RÓWNOLEGŁE TOŻSAMOŚCI KOSZTUJĄ TYŁE SAMO — ALE KUPUJĄ CO INNEGO

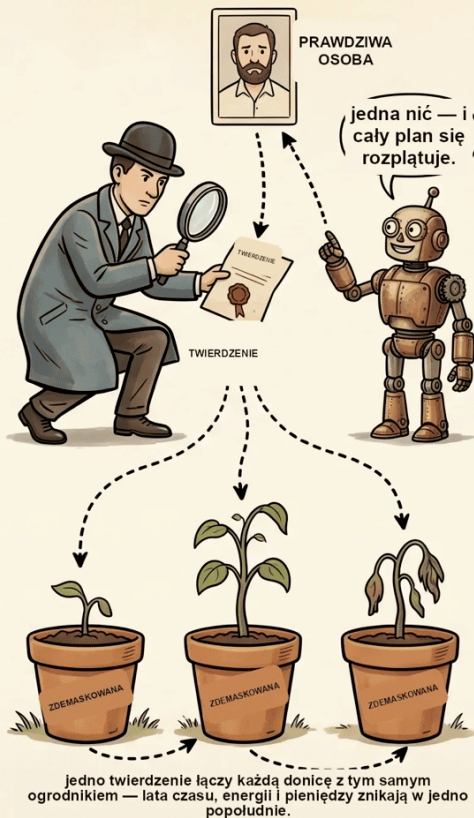
W WOLNOŚCI — KOSZTOWNY PLAN B



ALBO — CZYSTA KARTA PO OSOBISTYM POTKNIĘCIU



JEDNO TWIERDZENIE I PLAN B ZNIKA



POD TYRANIĄ — JEDNA DLA PAŃSTWA, POZOSTAŁE DLA WOLNEGO ZRZESZANIA SIĘ

(państwo albo całkowicie zakazuje tożsamości, albo wymaga ich pod własną kontrolą)



W WOLNOŚCI NADUŻYCIE JEST KOSZTOWNE. POD TYRANIĄ PRZETRWANIE JEST MOŻLIWE.

■ Percepcja wywrócona na lewą stronę

W przeciwieństwie do państwa zasada sieci reputacji zbudowanej na tożsamości zdecentralizowanej odwraca paradygmat postrzeganego priorytetu:

- Liczy się reputacja — czyli przeszłość, używana do oceny ryzyka interakcji z drugą stroną — a dane osobowe, takie jak nazwiska, adresy itd., mogą być kwestią grzecznościowej wymiany danych
- Podczas gdy państwo przede wszystkim żąda danych osobowych, gromadzi dane reputacyjne i pozwala wspólnocie zobaczyć tylko to, co mu pasuje

Czy zamożna osoba nie może po prostu „kupić” sobie więcej tożsamości (albo tworzyć wirtualnych wspólnot)?

Możliwość tworzenia równoległych tożsamości zdecentralizowanych na pierwszy rzut oka wygląda na nieuczciwą przewagę ludzi o większych środkach ekonomicznych nad tymi o mniejszych. Trzeba jednak podkreślić, że w przeciwieństwie do systemu scentralizowanego, gdzie wystarczy przekupić kilka punktów w piramidzie władzy, by pewne przewinienia zniknęły, w systemie zdecentralizowanym trzeba by przekupić całą wspólnotę.

Zastępcze tożsamości zdecentralizowane mogłyby posłużyć temu celowi, ale ich reputacja musi być budowana z czasem poprzez realną interakcję z faktycznymi innymi członkami wspólnoty — nie da się jej po prostu kupić, bo sieć czyni weryfikowalnym, jak dana tożsamość sobie radzi.

Co więcej, na rynku mogą istnieć (i prawdopodobnie będą) usługi, które działając jako autorytet, oferują dochodzenia dostarczające dowodów, że kilka tożsamości zdecentralizowanych to w rzeczywistości ta sama osoba. Pojedynczy zapis wprowadzony do sieci reputacji może więc za ułamek kosztu unieważnić całą inwestycję czasu, energii i pieniędzy włożoną w budowanie równoległych tożsamości.

Ekonomicznie opłaca się zatem nie oszukiwać wspólnoty — a w razie potrzeby zbadać swoje czyny i dążyć do naprawy, by reputacja wróciła do akceptowalnego poziomu i by jej nosiciel nie ucierpiał ekonomicznie ani w inny sposób od gniewu wspólnoty.

Ekonomicznie silna tożsamość, która straciła reputację we własnej wspólnocie, może próbować uciec przed jej gniewem poprzez podstępne układy z wybranymi tożsamościami — ale te wtedy również ryzykują utratę własnej reputacji.

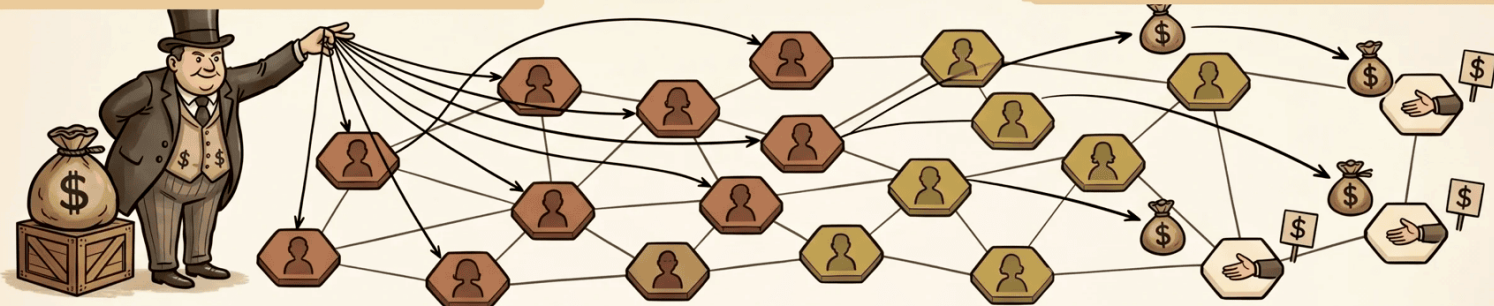
Wciąż pozostaje ucieczka do innej wspólnoty ze świeżą tożsamością — ale to oznacza porzucenie wszystkich osiągnięć i rozpoczęcie gdzieś od zera, z zerową reputacją. Czasem może to być zrozumiała droga i jedyne wyjście.

REPUTACJA JEST PRZECIWWAGĄ DLA SIŁY EKONOMICZNEJ

BOGACZ KUPIJE WPLYWY — SPOŁECZNOŚĆ TO PAMIĘTA

ATAK — INFILTRACJA I PRZEKUPSTWO

OSIEM MARIONETEK PODSTAWIOWYCH + TRZECH SĄSIADÓW PRZEKUPIONYCH



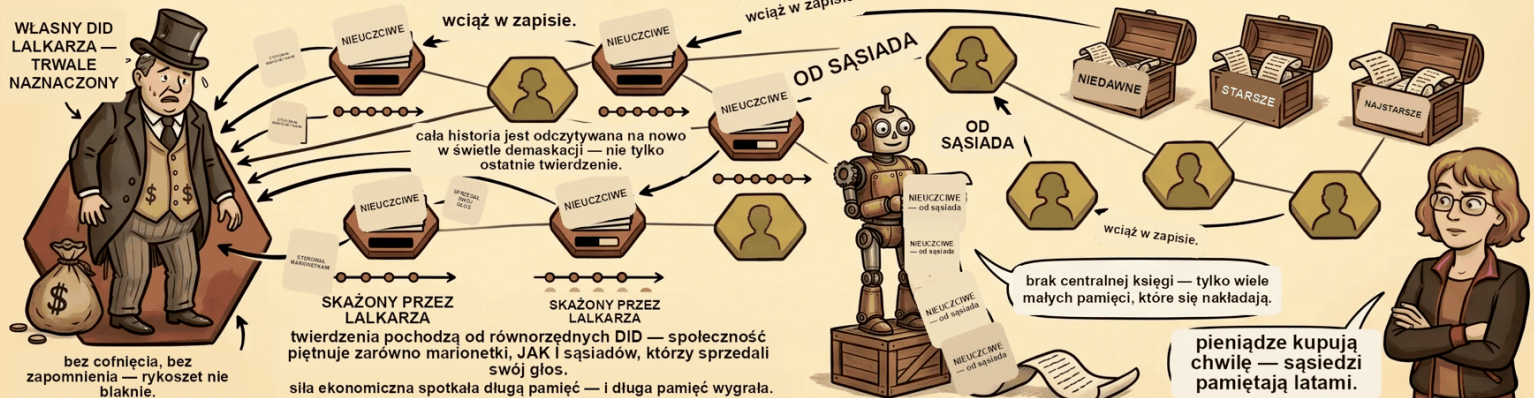
siła ekonomiczna potrafi wpłacać sznurki w każdą społeczność — i po drodze kupić kilka prawdziwych głosów.

na początku wygląda to tak, jakby bogacz po prostu poszerzył krąg znajomych.

PÓŹNIEJ

OBRONA — DŁUGA PAMIĘĆ, ROZPROSZONA KSIĘGOWOŚĆ

KAŻDY SĄSIAD PROWADZI WŁASNĄ PAMIĘĆ — BEZ CENTRALNEJ KSIĘGI, BEZ ZAPOMINANIA



SIŁA EKONOMICZNA SIĘGA GŁĘBOKO — RYKOSZET WRACA DO DOMU I NIE DA SIĘ ZMYĆ.

Uwaga

Podobnie wspólnoty poradziłyby sobie z atakiem, w którym ktoś poświęca zasoby na stworzenie wirtualnej tożsamości: dla takiej tożsamości ryzykowne jest wchodzenie w interakcję z inną wspólnotą bez weryfikacji — czyli bezkrytyczne przyjmowanie informacji o tożsamościach drugiej wspólnoty. Reputacje zawsze buduje się wewnątrz wspólnoty, nie globalnie.

A co z pasażerami na gapę, którzy chcą tylko czytać i nic nie dawać wspólnocie?

Dostęp do informacji nie jest nieograniczony od pierwszego dnia utworzenia tożsamości zdecentralizowanej. Nowi uczestnicy — ci, którzy nie zbudowali jeszcze reputacji poprzez faktyczną aktywność — napotykać stopniowane ograniczenia: mniej informacji, dłuższe czasy oczekiwania, wyższe koszty zapytań. Sieć nagradza uczestnictwo, nie bierną konsumpcję i dowolne żniwo danych.

Tożsamość zdecentralizowana ryzykuje też swoją reputację, gdy za opłatą użycza jej innej osobie (która może nawet nie być w sieci reputacji DID). Obowiązuje tu ta sama zasada: taka zdrada wspólnoty (naruszenie prywatności) może odbić się na reputacji zdrajcy, a czynu nie da się wymazać poprzez podstępny układ tak, jak działa to w systemie scentralizowanym. Muszą liczyć się z gniewem wspólnoty, w tym z utratą osiągnięć — bo wspólnota jest w ich oczach gwarantem na przykład przywileju posiadania majątku ruchomego i nieruchomego.

Zakotwiczenie w świecie rzeczywistym

Przy ocenie ryzyka bardziej ryzykownym podmiotem jest naturalnie ten, kto nie cieszy się przywilejem własności uznawanym przez daną wspólnotę — ma mniej do stracenia w swoich transakcjach (aktywa cyfrowe łatwiej przenieść).

Może to wyglądać na drobny szczegół, ale ma poważne konsekwencje. Chęć, by wspólnota miała dźwignię nacisku na swoich członków, implikuje własność jako przywilej — w najwolniejszych społeczeństwach niemal nietykalny, a jednak wciąż nie prawo ani fundamentalną zasadę, lecz przywilej, który w skrajnych przypadkach może zostać cofnięty (wyobrażam sobie na przykład odmowę służby w obronie wspólnoty w konflikcie zbrojnym).

Odpowiada to też podprogowo na to, jak wspólnota będzie traktować swoich członków i jaką motywację ma członek, by walczyć o wspólnotę — by zachować swoje przywileje. Człowiek może zawieść w swojej odpowiedzialności wobec wspólnoty, ale moralnie nie może oczekiwać pobłażliwości, jeśli chodzi o zachowanie ciężko wywalczonych przywilejów.

Neutralność finansowa

Czytając słowa takie jak zdecentralizowany, niecenzurowalny, nieprzekupny, nie sposób nie skojarzyć ich z najlepiej znanymi kryptowalutami — Bitcoinem, Monero i, powiedzmy, Kaspą — które można opisać takimi określeniami. Intuicja jest tu jednak myląca: opłaty za usługi autorytetów, za weryfikację i publikację itd. można rozliczyć w dowolnej walucie lub pieniądzu. Dla połączonych uczestników

SIEĆ NAGRADZA UCZESTNICTWO

REPUTACJĘ BUDUJE SIĘ CAŁE ŻYCIE — NIE KUPUJE SIĘ JEJ, NIE POŻYCZA

UCZESTNIK — CAŁE ŻYCIE PRAWDZIWEJ PRACY



cięższa praca może skrócić wspinaczkę.



czas buduje krzywą —
twój własny wysiłek
może ją uczynić
bardziej stromą.

WIEK 20 LAT — NOWICJUSZ

reputacja 5%

0 ukończonych projektów



OGRANICZONY — WYSOKIE KOSZTY, DŁUGIE OCZEKIWANIE

WIEK 28 LAT — AKTYWNY UCZESTNIK

reputacja 30%



PODSTAWOWY — STANDARDOWE KOSZTY, NORMALNA Szybkość

WIEK 40 LAT — WSPÓŁTWÓRCA

reputacja 70%



PEŁNY — NISKIE KOSZTY, NATYCHMIASTOWY DOSTĘP

WIEK 55 LAT — AUTORYTET

reputacja 95%

15+ zrealizowanych projektów



AUTORYTET — WERYFIKUJESZ INNYCH, SIEĆ CI PŁACI

każdy etap kosztuje czas, energię i pieniądze — razem, nie osobno.

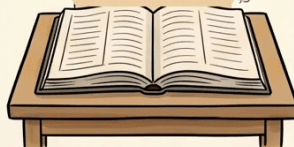
drzwi otwierają się w miarę wypełniania rejestru twoich czynów.

PASAŻER NA GAPE — CZYTA, NIGDY NIE PUBLIKUJE



czyta zapisy wszystkich innych.

MOJE WKŁADY



nie publikuje niczego własnego.

OGRANICZONY DOSTĘP — SUFIT SIĘ NIE PODNOŚI

reputacja 5%



brak czynów, brak wzrostu — rok po roku ta sama poprzeczka.

(sieć oddaje tym, którzy wnoszą swój wkład.



CZAS, ENERGIA I PIENIĄDZE — ZAINWESTOWANE W PRAWDZIWĄ PRACĘ — TO JEDYNA WALUTA, KTÓRĄ SZANUJE SIEĆ.

sieci społecznościowej w sieci DID (czyli twojej wspólnoty) i jej otoczenia liczy się poparte reputacją potwierdzenie, że płatność została dokonana. Publikacja tezy musi indywidualnie nieść rozsądny, weryfikowalny koszt, aby aktor nie mógł publikować ile i jakich też chce bez wydatkowania energii, pieniędzy i czasu — to stan skrajnie niepożądany, odpowiadający przywilejowi elit w dzisiejszych, przeżartych korupcją systemach państwowych.

Pod tym względem wspomniane kryptowaluty mają niewielką przewagę w tym, że ich sieci działają jak zaufane autorytety weryfikujące, iż dana płatność miała miejsce, kosztem niewielkiej utraty prywatności i ujawnienia niektórych ze swoich adresów.

Dobrowolność, odpowiedzialność i wolność

Dobrowolność jest indywidualna: decyduję za siebie. Odpowiedzialność powstaje, gdy moja decyzja dotyka innych — włącza się informacja zwrotna. Wolność nie jest ani darem, ani prawem — jest fenomenologicznym³ rezultatem tysięcy dwustronnych interakcji między dobrowolnością a presją ku odpowiedzialności, uśrednionych w skali społeczeństwa. Sieć nie dyktuje tej średniej — wyłania⁴ się ona z sygnałów cenowych weryfikatorów i z zapowiedzianych z wyprzedzeniem polityk weryfikacyjnych, które członkowie wspólnoty ustalają dla siebie.

³**Fenomenologiczny** (od gr. *phainómenon* — to, co się jawi) — ogólnie: podejście badające zjawiska tak, jak przedstawiają się w bezpośrednim doświadczeniu, poprzez obserwację tego, co z nich wynika, bez z góry danych teorii wyjaśniających w mikroświecie pod spodem. Tutaj: wolność nie jest abstrakcyjną zasadą definiowaną z góry, lecz obserwowanym zjawiskiem — konsekwencją tysięcy mikrointerakcji między ludźmi, wyłaniającą się z tego, jak faktycznie się nawzajem traktujemy.

⁴**Emergentny** (od łac. *emergere* — wyłaniać się) oznacza „spontanicznie powstający z interakcji prostszych części, bez niczego projektu ani sterowania”. Klucz ptaków leci w formacji, choć żaden ptak nie ma planu tej formacji — formacja wyłania się z prostych reguł każdego osobnika. Podobnie w sieci reputacji nikt nie projektuje reguł zachowania całości — wyłaniają się one z tysięcy indywidualnych decyzji.

Jaką preferencję dla wolności ma jednostka wewnątrz wspólnoty, zależy od jej wyczucia, ile sama jest gotowa przełknąć z tego, co narzuca innym. Przy rzeczach oczywistych i korzystnych dla wszystkich nie ma dylematu moralnego — morderstwo jest złe. Są też przypadki, gdzie opcje przesuwają się w pozycję dozwolonych przywilejów: udowodnij swoje umiejętności, a wpuścimy cię na drogę, żeby mniejsza była szansa, że nas zabijesz. I wreszcie są sprawy, w których jednostka mówi — nie opłaca mi się to, nie zabronię sąsiadowi palić liści, skoro sam to robię, albo dlatego że robię coś innego, co ogranicza jego komfort, a on mógłby z kolei chcieć mi tego zabronić. Jeśli historycznie wytyczaliśmy granicę wolności tam, gdzie zaczyna się wolność kogoś innego, to reputacyjna sieć społecznościowa zbudowana na tożsamości zdecentralizowanej spełnia to lepiej niż scentralizowana demokracja przedstawicielska — gdzie na przykład uprzywilejowana warstwa wybranych przedstawicieli próbuje wyłączyć siebie spod nadzoru komunikacji osobistej, a jednocześnie nie waha się narzucać go swoim wyborcom, używając wszelkiego rodzaju podstępnych pretekstów i manipulacji.

Przełącznik wolność-totalitaryzm (i delegacja)

Prosty mechanizm w sieci DID może przesunąć cały system ku większej wolności albo większej kontroli: liczba zapisów, które DID może opublikować w danym okresie. Gdy zapisy pozostają rzadkie, każdy niesie wagę — to wolność. Gdy zapisów jest w nadmiarze i dotyczą błahostek, to totalitaryzm. Kierunek wybierasz każdym opublikowanym zapisem. Sama sieć nie jest ani wolna, ani totalitarna — to neutralna infrastruktura. To, czym się stanie, wyznacza sposób, w jaki ludzie jej używają.

W ramach mojej własnej polityki weryfikacyjnej ma sens ustalić dla generycznego DID w mojej sieci społecznościowej — wewnątrz wspólnot — maksymalną liczbę tez (dowolnego weryfikowalnego stwierdzenia w ogóle; tutaj: zapisu opublikowanego do sieci reputacji), które wydawca może wystawić w danym okresie, bym brał je pod uwagę i uznawał jego żądania weryfikacji za istotne.

DOBROWOLNOŚĆ → ODPOWIEDZIALNOŚĆ → WOLNOŚĆ

TRZY KROKI — OD WYBORU JEDNEJ OSOBY DO WZORCA CAŁEGO SPOŁECZEŃSTWA

DOBROWOLNOŚĆ



jednostka decyduje — nikt jej nie zmusza.
i nikt też nie jest jej winien pozytywnego obowiązku.

ODPOWIEDZIALNOŚĆ



moje wybory rozchodzą się falami — i te fale wracają.
konsekwencje mówią same za siebie.

WOLNOŚĆ



nikt nie narysował tej mapy — narysowała się sama.

wolność to statystyczny kształt
tego, jak sąsiedzi się traktują.

WOLNOŚĆ NIE JEST DAREM Z GÓRY — JEST WZORCEM, KTÓRY TWORZYMYSZ RAZEM.

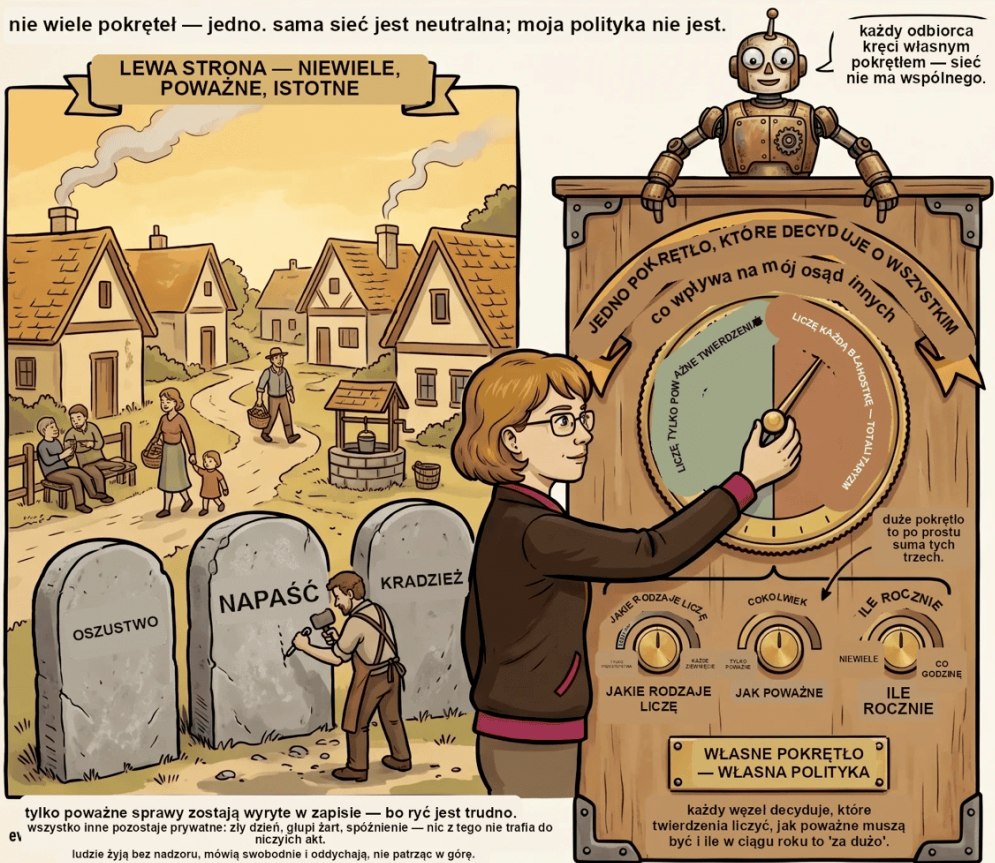
Trzymam w głowie intuicyjną liczbę — niski jednocyfrowy rząd wielkości rocznie. Takie cenzorskie podejście może wydawać się dość izolacjonistyczne. Ale mogę zasadnie postawić wnioskodawcę przed wyborem: żeby wybrał jeden ze swoich już wystawionych zapisów i poprosił weryfikatora o jego cofnięcie, czyli unieważnienie — co jest dość agresywnym żądaniem w sytuacji, gdy wnioskodawca przez zbieg okoliczności naprawdę stał się ofiarą wielu niezależnych krzywd, a ja z pewnością przyczyniłbym się przez to do jego poczucia wyobcowania ze wspólnoty.

Skuteczniejszą opcją wydaje się zatem możliwość delegowania części swoich praw do publikowania informacji w sieci reputacji na rzecz wspólnoty lub autorytetu, który następnie — w sposób solidarny, według swoich wewnętrznych reguł — decyduje, jak je rozdysponować. Grupa musi być w stanie zadbać o tych, których uważa za pokrzywdzonych. Członek wspólnoty ma prawo w każdej chwili, dopóki delegowane prawo nie zostanie użyte, cofnąć swoją delegację.

PRZEŁĄCZNIK WOLNOŚĆ-TOTALITARYZM

JEDEN JEDYNY PARAMETR — ILE POSTANAWIAM ŚLEDZIĆ — PRZECHYLA CAŁE SPOŁECZEŃSTWO MIĘDZY WOLNOŚCIĄ A TYRANIĄ

nie wiele pokręteł — jedno. sama sieć jest neutralna; moja polityka nie jest.



każde ziewnięcie staje się aktem — bo liczenie jest tanie.
kichnięcie, zakup, spacer do domu po zmroku: wszystko trafia do zapisu, na zawsze.
nic nie jest prywatne — oko nigdy nie mruga, a sąsiedzi przestają rozmawiać.

WOLNOŚĆ TO TO, CZEGO ODMAWIAM LICZENIA — TOTALITARYZM TO TO, NA CO ZGADZAM SIĘ ŚLEDZIĆ.

DELEGOWANIE PRAW PUBLIKACJI

POŻYCZASZ KLUCZ AUTORYTETOWI, KTÓRY CI SŁUŻY — I ODBIERASZ GO W JEDNEJ CHWILI

pożyczam klucz —
sznurek zostaje przy mnie.

delegacja — autorytet działa w
moim imieniu, w ramach
zasad, które akceptuję.

AUTORYTET — DOSTAWCA
USŁUGI
polityka · standard · partia ·
izba

SZNUREK
ODWOLANIA

MOJE PRAWO
DO
PUBLIKACJI
—
1 ZAPIS

mogę pożyczyć więcej niż
jeden klucz naraz —
automatyzacja w tle może
wydać nowy za każdym razem,
gdy jeden z moich zostanie
pobrany.

POLITYKA

LOSOWANE,
GDY AUTORYTET
DZIAŁA

DELEGOWANE
KLUCZE — PUŁA

LOSOWANE,
GDY AUTORYTET
DZIAŁA

sznurek nigdy nie opuszcza
twojej dłoni — na tym polega
cały trik.

JEDNO POCIĄGNIĘCIE — KLUCZ WRACA DO DOMU



odwołalne tylko do momentu
wylosowania klucza.

RODZAJE
AUTORYTETÓW,
KTÓRE MOGĄ
TRZYMAĆ
KLUCZ



PARTIA
POLITYCZNA
FAK I T



ORGAN
STANDARYZACYJNY
DUJ I T



IZBA
ZAWODOWA

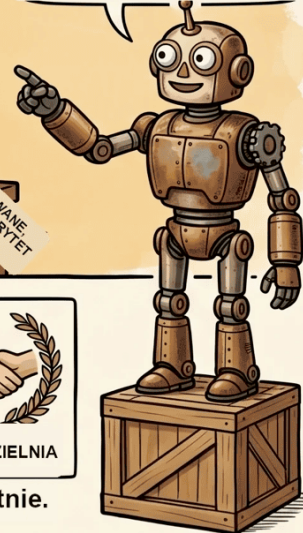


SPÓŁDZIELNIA

autorytet służy swoim członkom — nie odwrotnie.
jedno pociągnięcie za sznurek kończy porozumienie.



JEDNO POCIĄGNIĘCIE — KLUCZ WRACA DO DOMU



POŻYCZ KLUCZ — ZATRZYMAJ SZNUREK. DELEGOWANIE NIGDY NIE JEST ZRZECZENIEM SIĘ.

■ Wolność kontra totalitaryzm

Spółeczeństwo, które pilnuje i ogranicza wolumen publikowanych zapisów, będzie wolniejsze; społeczeństwo z nadmiarem zapisów będzie skłaniać się ku totalitaryzmowi. Można wyobrazić sobie delegowanie prawa do publikowania zapisów komuś innemu.

Adaptacja kulturowa

Ludzie na ogół lubią zaglądać sobie nawzajem na talerze. Między cywilizacjami różnimy się doświadczeniem historycznym i gęstością zaludnienia — a przez to tym, jak bardzo chcemy zaglądać sobie na talerze wewnątrz cywilizacji i wspólnot. Państwa azjatyckie skłaniają się ku surowszemu spojrzeniu na wolność w społeczeństwie; europejskie i amerykańskie, w pewnych aspektach, ku wolniejszemu. Jakkolwiek nieprecyzyjna byłaby ta paralela, w kontekście zdecentralizowanej reputacyjnej sieci społecznościowej można powiedzieć, że ustawienia poszczególnych wspólnot nie dyskryminują, a każda wspólnota może konfigurować komunikację wewnątrz siebie tak, jak uzna za stosowne.

Mimo różnic będą standardy uznawane na całej planecie (przypadkowe zabijanie nikomu nie służy). Inne ustawienia będą specyficzne dla wspólnoty, a jeszcze inne nawet osobiście specyficzne. Zaletą jest to, że poprzez wzajemną komunikację i obserwację ustawień swojego otoczenia można szukać konsensusu — od układów dwustronnych, przez wspólnotowe, aż z czasem, dzięki ekonomicznej dominacji najlepiej skonfigurowanych wspólnot, także na poziomie globalnym.

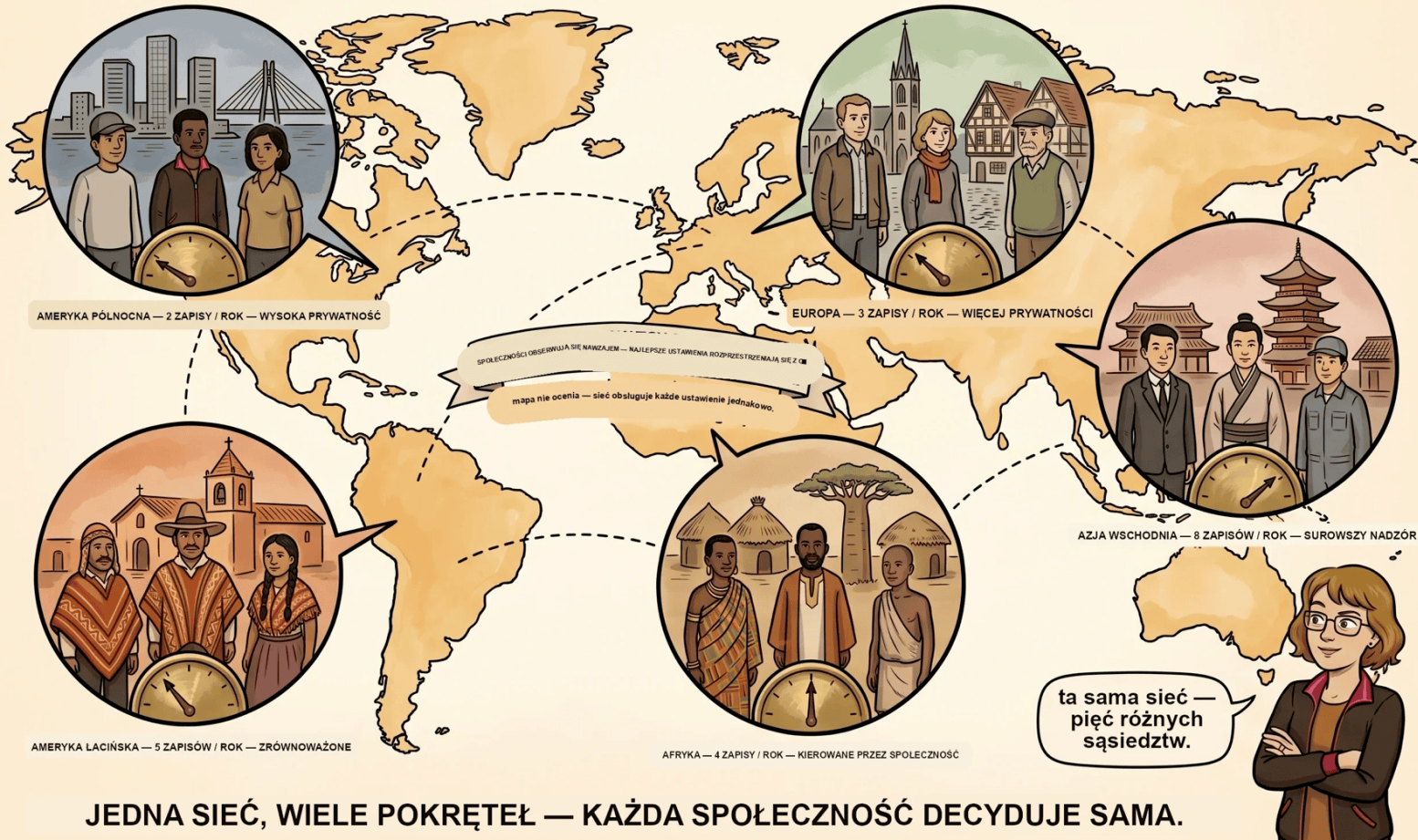
Ale o konsensusie więcej w następnym rozdziale.

Problem wyroczni — pomost między światem cyfrowym a fizycznym

Termin „problem wyroczni” (oracle problem) w ostatnim czasie najczęściej kojarzony jest ze światem kryptowalut, blockchainów i systemów zdecentralizowanych. Ogólnie: jak zapewnić, by dane wchodzące

KAŻDA SPOŁECZNOŚĆ KONFIGURUJE SIĘ SAMA

SIEĆ NIE DYSKRYMINUJE — KAŻDY REGION USTAWIA WŁASNE POKRĘTŁO



do systemu cyfrowego wiernie odpowiadały temu, co faktycznie wydarzyło się w świecie fizycznym? Sam system nie może zweryfikować, czy ktoś naprawdę skrzywdził kogoś innego albo czy umowa faktycznie została naruszona — widzi jedynie zapisy cyfrowe.

Rozwiązujemy to tutaj poprzez autorytety — podmioty, które stawiają swoją reputację na tym, że zapis cyfrowy odpowiada rzeczywistości fizycznej. Im wyższa reputacja autorytetu, tym wiarygodniejszy zapis.

ŁĄCZENIE ŚWIATA CYFROWEGO I FIZYCZNEGO

AUTORYTET PRZENOSI RZECZYWISTOŚĆ NA DRUGĄ STRONĘ



Reputacja autorytetu sprawia, że zapis cyfrowy jest wiarygodny.

* System nie próbuje rozwiązać problemu wyroczni — akceptuje, że autorytety są mostem, i dostosowuje się do tego, jak zaufanie już działa w prawdziwym świecie.

* Jeśli most myli się co do rzeczywistości, płaci za to autorytet — swoją reputacją.

Jak działa weryfikacja

Konsensus i proces weryfikacji

Aby zbudować konsensus co do tego, jakie reguły społeczeństwo powinno średnio podtrzymywać i egzekwować, może pomóc następujący mechanizm. Jako uczestnik DID deklaruje reguły, do których się zapisuje i według których będzie żyć, i publikuje je. (Wyobraź je sobie jako regulamin i statut, które w moim odczuciu składają się na mój idealny świat — świat, w którym nie czuję się ograniczony, lecz bezpieczny.)

Mogę z góry oszacować, jak zareagowaliby moi kontaktowi DID — i ocenić, jak mocno i przez kogo zostałbym ukarany w zwykłych interakcjach społecznych czy biznesowych, gdyby hipotetycznie do nich doszło.

Ostateczna ocena następuje, gdy żądasz informacji od innego DID albo prosisz go o weryfikację tezy (albo prosisz autorytet o usługę itd.), którą chcesz opublikować do sieci reputacji. Powinno to wypaść tak samo, jak wtedy, gdy sam przeprowadzasz ocenę na sucho względem deklarowanej polityki drugiej strony — a jeśli tak nie jest, coś jest nie tak po stronie drugiej strony: próbuję grać w nieuczciwą grę.

Wynikiem jest albo przyjęcie, z podaną ceną za weryfikację (w przypadku usług weryfikatora lub autorytetu), albo odrzucenie. Zarówno sankcje, jak i premie za odchylenie od polityki oceniającego są wliczone w podaną cenę. Wnioskujący następnie decyduje, czy przyjąć warunki, czy przejść do kolejnej rundy weryfikacji w algorytmie przydziału — powtarzając proces, aż będzie zadowolony albo aż ekonomia sprawi, że dalsze kontynuowanie stanie się bezcelowe.

■ Graf społeczny

Sieć reputacji jest przede wszystkim siecią społecznościową. Dodajesz kontakty — ludzi, którzy zgadzają się na połączenie. Oni mają kontakty, a tamte kontakty mają kontakty. Algorytm szuka weryfikatorów w konfigurowalnej głębokości (np. trzy poziomy: twoje bezpośrednie kontakty, ich kontakty i jeden poziom dalej). Nie jest potrzebny żaden globalny blockchain — sieć naturalnie tworzy wspólnoty z zazębieniami w inne wspólnoty.

Algorytm jest niedeterministyczny: hashuje twój dokument tezy, mapuje hash na pozycję na pierścieniu znanych tożsamości w obrębie tego kręgu i wybiera najbliższą jako kandydata na weryfikatora. Nie możesz przewidzieć ani wpłynąć na to, kto zweryfikuje twoją tezę.

Każde odrzucenie przez weryfikatora powiększa twój dokument i zwiększa koszt jego przetworzenia — to pierwszy kanał kosztowy (wzrost dokumentu). Każdy nowy weryfikator pobiera opłatę zależną od wolumenu danych, twojej reputacji i tego, jak daleko treść twojej tezy odchyła się od jego deklarowanej polityki weryfikacyjnej — to drugi kanał kosztowy (premia za ryzyko). A każda iteracja kosztuje czas i energię — to trzeci kanał kosztowy.

■ Co sprawdza weryfikator i w jakiej kolejności

Po wybraniu weryfikator ocenia tezę w mniej więcej czterech uporządkowanych krokach — najpierw najtańsze filtry, na końcu drogie sprawdzanie treści:

1. **Bramka polityki.** Czy ten rodzaj tezy w ogóle mieści się w tym, co weryfikator publicznie weryfikuje? Jeśli nie, żądanie zostaje od razu odrzucone.
2. **Zaufanie do autorytetu.** Czy autorytet, który poręczył tezę, jest wystarczająco zaufany według własnej deklarowanej polityki weryfikatora? Autorytet poniżej progu zaufania weryfikatora jest podstawą do odrzucenia niezależnie od treści tezy.
3. **Reputacja wystawcy.** Czy wystawca spełnia progi reputacji, które weryfikator zadeklarował dla tego typu tezy? Niska reputacja może albo podnieść opłatę, albo wywołać odrzucenie.
4. **Sprawdzenie treści.** Dopiero gdy przejdą pierwsze trzy bramki, weryfikator ocenia samą tezę — podpisy, wewnętrzną spójność, poprawność formalną i to, jak daleko odchyła się od polityki weryfikatora. Opłata pobierana za ten ostatni krok odzwierciedla faktycznie podjęte ryzyko.

Weryfikator publikuje politykę, która rządzi każdą z tych bramek, więc kroki nie są kwestią jego uznania — jest związany tym, co już zadeklarował. Odchylenie od opublikowanej polityki samo w sobie jest tezą, którą można opublikować przeciw niemu, a płaci za nie swoją reputacją.

Rezultat: opublikowanie wiarygodnej i użytecznej tezy kosztuje niemal nic. Opublikowanie tezy radykalnej kosztuje więcej. Opublikowanie kłamstwa staje się zaporowo drogie — musisz iterować przez weryfikatora za weryfikatorem, a każdy, kto cię odrzuca, dokłada kosztów. Rynek wycenia twoją tezę, a cena mówi ci, gdzie stoisz względem wspólnot, w których się poruszasz.

Nie wystarczy zadeklarować, że przestrzegasz reguły, gdy w rzeczywistości tego nie robisz. W takim przypadku twój DID ryzykuje publikację negatywnego zapisu odsłaniającego obłudę — co czyni cię ryzykiem dla wszystkich innych. Rezultatem powinno być mniej reguł, ale konsekwentniej przestrzeganych, oraz oczyszczenie tej dżungli praw i przepisów, po której nawet prawnicy z trudem się poruszają.

Konsensus kontra rozliczalność

Aby sieć służyła jako wartościowe źródło informacji, DID nie powinien być zbyt radykalny — inaczej pozostali go odrzucają. Presja społeczna będzie szukać równowagi, a próby jej destabilizacji będą prawdopodobnie karane.

SIEĆ CICHU PORÓWNUJE TWOJE SŁOWA Z TWOIM ZAPISEM — LUKA JEST WIDOCZNA DLA WSZYSTKICH



LEKARSTWO NA HIPOKRYZJĘ

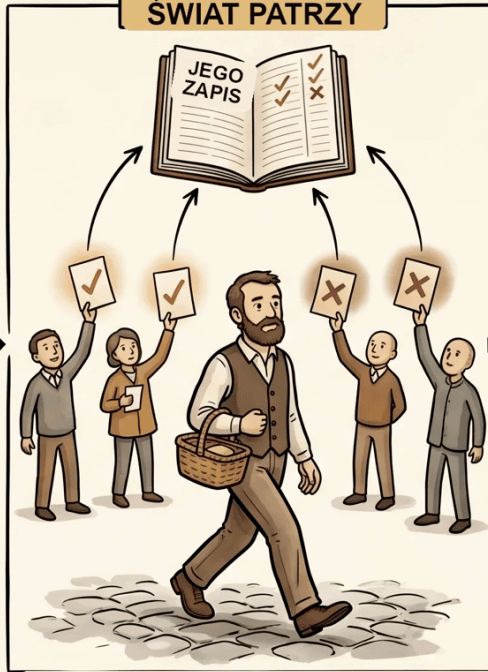
OGŁOŚ SVOJE ZASADY — ŻYJ WEDŁUG NICH, ALBO RYNEK CIĘ WYCENI

OGŁASZAM SVOJĄ
POLITYKĘ



każdy może przeczytać moje standardy.
żadnych strażników, żadnych tajemnic.

ŚWIAT PATRZY



świat zapisuje, co on naprawdę robi.
każdego dnia trochę więcej dowodów w jego rejestrze.

W SKLEPIE — PŁACISZ ZA WŁASNY ZAPIS



hipokryzja nie jest karana przez autorytet — jest wyceniana przez rynek.
każda zwykła usługa, którą kupujesz, niesie dopłatę kształtowaną przez twój własny zapis.

CZY MOŻNA NAZWAĆ TO UMOWĄ SPOŁECZNĄ — NA NOWO?

żaden autorytet nie wymusza etyki — robi to cena.
delikatna presja, każdego dnia, w stronę wspólnej średniej, z którą wszyscy możemy żyć.

BĄDŹ SPÓJNY ZE SWOIMI SŁOWAMI — ALBO ZAPŁAĆ. HIPOKRYZJA TO NAJDRÓŻSZA REPUTACJA.

■ Liczba głosów to nie to samo co waga głosu

Juraj Karpiš mówi, że „pieniądze są pamięcią dobrych uczynków”. Dodałbym, że reputacja jest pamięcią tych złych.

Wynika z tego, że merytokratycznie ten, kto wnosi więcej i nie ma złej reputacji, zasługuje na większą wagę głosu we wspólnocie. Patrząc przez pryzmat relacji dwustronnych: gdy ważę, którym naciskom konsensusu ustąpić, największą wagę mają relacje, z których czerpię największą korzyść ekonomiczną. Dziesięciu ludzi, z którymi nie prowadzę żadnego aktywnego handlu, wpłynie na mnie znacznie mniej niż jeden stały partner biznesowy. Ten paradygmat nie ogranicza się do handlu — rozciąga się na relacje społeczne, polityczne i inne.

Roles in the verification transaction and authorities

Przegląd ról

O niektórych z tych ról wspomnieliśmy już pokrótce w rozdziale o sieci i jej podstawowych właściwościach. Teraz jest czas, by przyjrzeć się im ponownie, dokładniej, i dodać kolejne, których potrzebujemy, by uczynić sieć bardziej odporną. Każda transakcja weryfikacyjna angażuje kilka ról — zobaczmy, jak się zachowują.

■ Rola w transakcji weryfikacyjnej

Każda weryfikacja angażuje do sześciu odrębnych ról, podsumowanych w poniższej tabeli. Wszystkie mogą mieć własny DID w zdecentralizowanej sieci reputacji.

Rola	Opis
Wystawca	Osoba, która publikuje informację w sieci — twierdzi, że coś się wydarzyło (utworzono, zmodyfikowano lub rozwiązano DID, teza, polityka danego DID itd.)
Podmiot	Osoba, której informacja dotyczy — adresat tezy
Autorytet	Zaufany podmiot, który stawia swoje imię na jakości tezy, badając ją i albo przeglądając przedstawione dowody, albo aktywnie je zbierając
Obserwator	Niezależna strona trzecia, która prowadzi zapis tego, jak weryfikator obchodzi się z tezą — pilnując, by weryfikator ani nie milczał, ani nie odchodził od zadeklarowanej polityki
Weryfikator	Wybrany algorytmicznie uczestnik, który przetwarza transakcje
Delegat	Osoba działająca w imieniu innego uczestnika

Wystawca

Wystawcę już poznaliśmy. Gdy ktoś zostaje skrzywdzony albo chce rozgłosić własne osiągnięcie, to osoba reprezentowana przez DID uruchamia proces wprowadzania tej informacji do sieci — bo ma w tym

pierwotny interes (motywacją jest albo pragnienie satysfakcji, albo chęć poprawy własnego wizerunku publicznego).

Tezy pozytywne

Pozytywne tezy o sobie mogą zachować, jako ich podmiot i zarazem wystawca, na sytuację, w których chcą ich użyć (dyplom, zaświadczenie o wyświadczonej usłudze itd.). Tu właśnie teza pozytywna różni się od negatywnej: dzielenie się zweryfikowaną tezą negatywną leży w interesie całej wspólnoty, podczas gdy pozytywna — w interesie jej nosiciela.

Autorytet

Autorytet pełni podwójną rolę: może być **audytorem** (weryfikującym jakość dowodów przed opublikowaniem tezy) albo **gwarantem** (stawiającym swoją reputację na prawdziwości tezy). W obu przypadkach wzmacnia tezę wystawcy. Te dwie usługi są rozdzielne — autorytet może oferować jedną, drugą albo obie naraz. Założenie robocze jest takie, że większość usług świadczonych przez autorytety można dostarczać na zasadach wolnorynkowych. Dotyczy to nawet dziedzin, które trudno wyobrazić sobie sprywatyzowane, jak wymiar sprawiedliwości, gdzie wyspecjalizowane usługi — dochodzenie, ocena dowodów, aż po usługi świadczone dziś przez scentralizowane armie (planowanie strategiczne, standaryzowane szkolenie, zaopatrzenie i zarządzanie zapasami itd.) — mogą być efektywnie dostarczane przez podmioty rynkowe. Trudno o cokolwiek, czego po restrukturyzacji nie dałoby się usprawnić bodźcami wolnorynkowymi.

AUTOR · SYGNATARIUSZ · STAWIA WŁASNĄ REPUTACJĘ

1. Pisze twierdzenie własnymi słowami
2. Zbiera dowody ze świata rzeczywistego na jego poparcie
3. Podpisuje własnym DID i wysyła do wybranego autorytetu
4. Płaci koszt publikacji
5. Ponosi konsekwencje, jeśli kłamie

A vertical thermometer with a brown frame and a white scale. The scale has major markings at 0, 10, 20, 30, 40, and 50. The liquid level is at the 10 mark. A black arrow points to the 10 mark.

**Jeśli to nieprawda,
moja wskazówka
spada.**

Moje nazwisko jest pod tym podpisane. Lepiej niech będę pewny — i przyniosę dowody.

**Każdy może mówić.
Kłamstwo kosztuje
mówiącego.**

DO:
AUTORYTET
WEDŁUG
MOJEGO
WYBORU

NASTĘPNY KROK
popros autorytet o
ocenę dowodów i
podpisanie
twierdzenia

KASETA
AUDIO

Wystawca jest autorem. To jego nazwisko jest pod tym.

*** Wystawcą może być każdy, kto ma DID. Wymaga to odwagi i odpowiedzialności, nie licencji.**

■ **Autorytet, wystawca i obserwator nigdy nie mogą być weryfikatorem własnej sprawy.**

Algorytmiczny wybór weryfikatora gwarantuje niezależność. Nikt nie może weryfikować własnej tezy ani tezy, w której ma bezpośredni interes. To jedna z podstawowych reguł, w której podtrzymywaniu cała wspólnota DID ma interes.

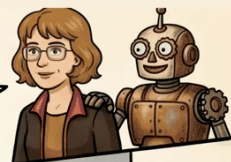
Poniższe grafiki pokazują komplementarne widoki szerokości działań, które pokrywają autorytety (termin „autorytet” można czytać wymiennie z „dostawcą usług”).

PRZEWODNIK — POMAGA CI NAWIGOWAĆ WEDŁUG TWOICH WARTOŚCI

GŁĘBOKA ANALIZA W TLE · PROSTA WSKAZÓWKA NA WIERZCHU

PRZEWODNIK

Ona agreguje złożony świat w rekomendacje. Obserwujący głosują swoją uwagę — mogą odejść w każdej chwili, przejść do innego.



MOJA ANALIZA

Notatki robocze — nie dla klientów

wydatki publiczne - przekierowane

Ja wykonuję złożoną pracę. Ty dostajesz prostą rekomendację — tylko jeśli podzielasz moje wartości.

dostawcy

1	70M	☆☆☆☆
2	70M	☆☆☆☆
3	70M	☆☆☆☆
4	70M	☆☆☆☆

DLA CIEBIE —
CO TO OZNACZA

Zagregowane, aby zmaksymalizować twoją korzyść

- przesun wydatki tutaj, oszczędzaj tam
- wspieraj dostawców, którzy przechodzą moje testy
- **przyjmij ten szablon polityki**



A co dokładnie dostaję za moje pieniądze — jakie analizy i jakie zestawienia?

na przykład: kto może być przewodnikiem

- partia polityczna lub ruch publikujący szablony polityki
- niezależna firma audytorska publikująca zagregowane ustalenia
- agencja porównująca usługi
- agregator reputacji (ekonomiczny · biznesowy · sąsiedzi · bezpieczeństwo drogowe)
- dziennikarz-recenzent lub serwis recenzji konsumenckich

Związani tym, co publicznie reprezentują. Twoje zaufanie jest ich walutą.

* Możesz odejść w każdej chwili i przejść do innego przewodnika. Twoje zaufanie nie jest zablokowane.

* Przewodnik może też sam podpisywać niektóre twierdzenia — publikowane, ale to nie jest tu główny wątek.

■ Autorytet jako obserwator incognito

Renomowany autorytet — pomyśl o notariuszu, którego biznes zależy wyłącznie od jego track recordu — może obok głównych funkcji (audytor / gwarant) zaoferować trzecią: rolę obserwatora incognito podczas weryfikacji. Prowadzi opatrzony znacznikiem czasu zapis przesłanej tezy, tak by weryfikator nie mógł jej po cichu porzucić. Mechanizm roli obserwatora opisano dalej, w sekcji o roli obserwatora.

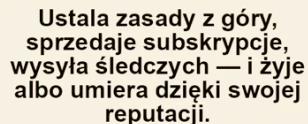
Weryfikator

Każdy DID może działać jako weryfikator, bezpośrednio albo poprzez prawa weryfikacji delegowane na trzeci DID. Aby ja — lub mój delegat — mógł weryfikować, powinienem być osiągalny w sieci (online). Nie każdy będzie chciał się do tego zobowiązać, dlatego zapis DID może wymienić, w kolejności priorytetu, zastępców, którzy będą pełnić tę funkcję w jego imieniu, gdy jest offline.

Każdy DID aktywny w sieci publicznie deklaruje własną politykę. Poprzez reguły określone w tej polityce ocenia podczas procesu weryfikacji reputację drugiej strony oraz treść i formę tezy, którą wystawca oznaczył do publikacji w sieci reputacji. Częścią polityki jest wzór obliczeniowy używany do wyliczania opłat za usługi weryfikacji. Gdy to jest gotowe, wtedy w statystycznie dużej liczbie tez przepływających przez sieć czekam, aż algorytm sieci wylosuje mnie po stronie wystawcy i przydzieli mi, w danej iteracji, weryfikację wystawianej informacji. Wystawca może z góry obliczyć, jak zareagowałby poprawnie zachowujący się weryfikator, ale nie może uniknąć faktycznego skontaktowania się z nim

OPUBLIKOWANE STANDARDY · OPUBLIKOWANE CENY

OPUBLIKOWANE STANDARDY · OPUBLIKOWANE CENY



Związany tym, co publicznie deklaruje. Resztę robi reputacja.

* Dostawca ma też własną politykę — kiedy akceptuje, kiedy odrzuca, jak zwraca pieniądze. Jest opublikowana, ale to nie jest tu główny wątek.

(lub jego zastępcami); iteracje z wybranym weryfikatorem wystawca musi przeprowadzić nawet wtedy, gdy z góry wie, że nie przejdzie.

Skąd wiemy, że wystawca uruchamia algorytm wyboru weryfikatora na właściwym zbiorze kandydackich DID weryfikatorów? Wraz z publicznie zadeklarowaną polityką każdy DID publikuje też aktualną listę identyfikatorów swojej sieci społecznościowej w obrębie sieci reputacji. Jeśli wystawca definiuje swoją sieć społecznościową jako bańkę społeczną, która jedynie powiela i wzmacnia jego własne poglądy, opublikowana przez nią informacja z trudem zostanie szerzej przyjęta przez inne wspólnoty. To, że udaje mi się wysokim kosztem przepchnąć radykalną tezę do sieci, nie oznacza, że oceniając reputację drugiej strony, nadam jej jakąkolwiek wagę. Niektóre tezy jestem popychany przez moją wspólnotę, by je uwzględnić (wyroki i ograniczenia nałożone na sprawców); inne zależą wyłącznie ode mnie — sam decyduję o ekonomicznej wartości włączenia lub wyłączenia danej informacji.

Podmiot

Ci, których dotyczy informacja opublikowana w sieci reputacji, są jej nosicielami albo, jeśli wolisz, jej podmiotami. Bodźce w sieci reputacji są ustawione tak, że podmiot ma wszelkie powody, by zachowywać się poprawnie i uczciwie według własnych reguł, i jest popychany przez wspólnotę ku pewnemu złotemu środkowi przestrzegania reguł. Ma nawet bodziec, by zachowywać się bardziej moralnie, niż wymagają jego deklarowane reguły — zapowiedziane z góry polityki nie wykluczają, że wspólnota dojdzie do konsensusu, by zastosować jakąś ocenę lub środek z mocą wsteczną. Z tego kąta reputacyjnosieciowa alternatywa dla porządku prawnego jest, jak można się spodziewać, kierowana bardziej duchem reguł niż ich literą.

WERYFIKATOR — OCENIA TWIERDZENIE WEDŁUG OPUBLIKOWANEJ POLITYKI

CZTERY BRAMY, PO KOLEI. NAJPIERW TANIE FILTRY.

Nie może improwizować. Musi robić to, co mówi jego polityka.

Jego własne zasady. Publiczne. Nie może ich po cichu zmienić.

BRAMY WERYFIKACJI — PO KOLEI

1. FILTROWANIE WEDŁUG POLITYKI
Czy w ogóle weryfikuję tego rodzaju twierdzenia?

2. ZAUFANIE DO AUTORYTETU
Czy autorytet przekracza mój próg?

3. REPUTACJA WYSTAWCY
Czy wystawca spełnia mój próg reputacji?

4. SPRAWDZENIE TREŚCI
Podpisy, spójność, odchylenie od polityki

NIE MOŻE BYĆ:
wystawcą,
autorytetem,
obserwatorem ani
podmiotem.

REPUTACJA WERYFIKATORA

ODCHYLENIE OD
POLITYKI → SPADEK
REPUTACJI → BRAK
PRZYSZŁYCH
WYBORÓW

CO ROBI WERYFIKATOR

1. Filtruje według swoich opublikowanych bram polityki (po kolei)
2. Sprawdza zaufanie do autorytetu, potem reputację wystawcy
3. Ocenia treść twierdzenia tylko wtedy, gdy przejdzie przez bramy
4. Pobiera opłatę proporcjonalną do ryzyka
5. Stawia własną reputację przy każdej decyzji

OPLATA $\propto$
RYZYO

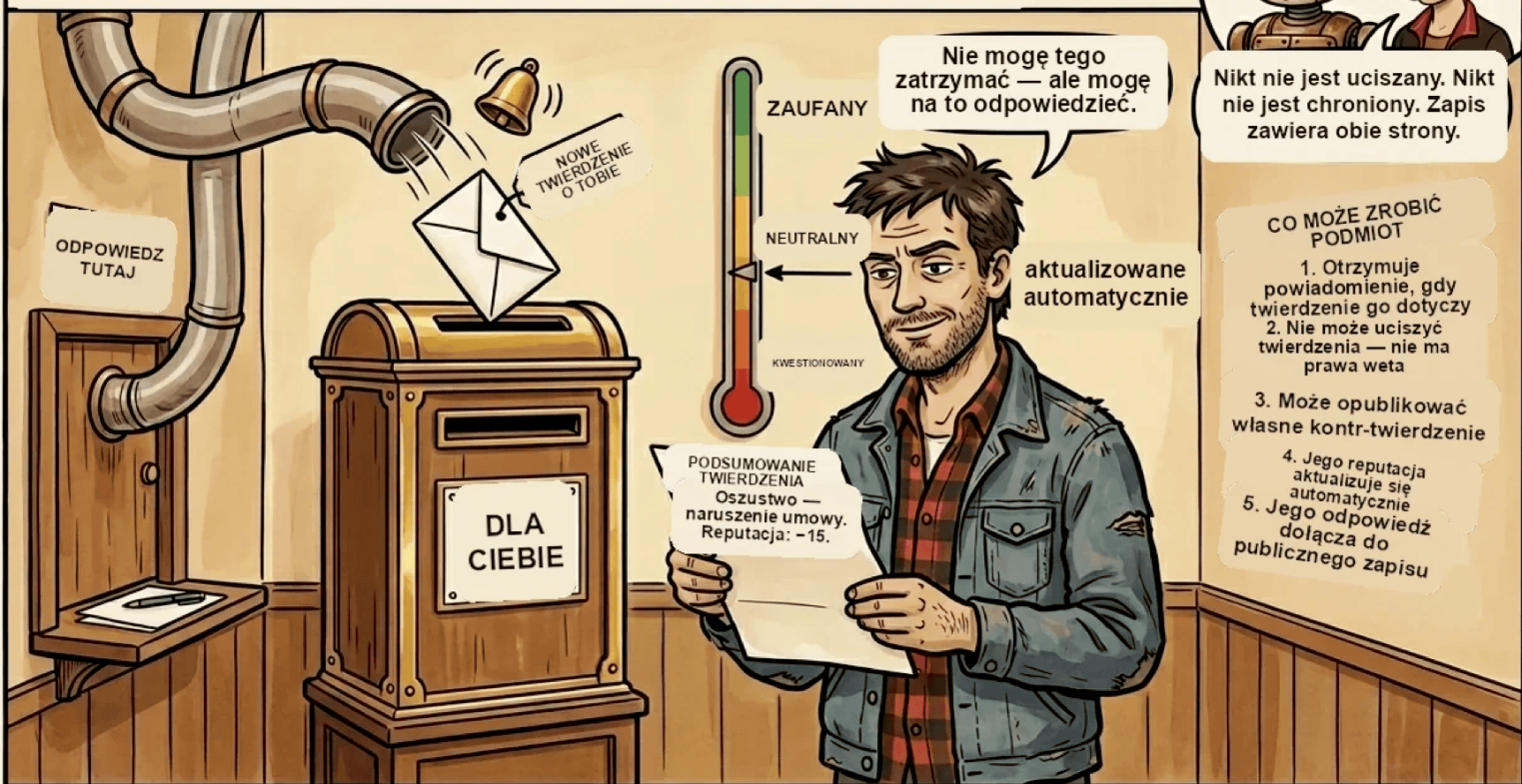
więcej ryzyka → wyższa opłata

Najpierw tanie filtry. Na końcu kosztowne sprawdzenie treści.

Weryfikator jest związany zasadami, które sam opublikował — i reputacją, którą może stracić.

PODMIOT — TEN, KOGO DOTYCZY TWIERDZENIE

OTRZYMUJE JE · NIE MOŻE GO UCISZYĆ · MOŻE NA NIE ODPOWIEDZIEĆ



Podmiot nie ma prawa weta — tylko prawo do odpowiedzi.

* Kontr-twierdzenie samo jest twierdzeniem — reputacja podmiotu jest —
stawką za to, co powie w odpowiedzi.

Obserwator

Rola obserwatora odbiera weryfikatorowi bodziec do naginania reguł. W sytuacjach, gdy weryfikatorowi nie podoba się żądanie wystawcy lub autorytetu, mógłby po prostu milczeć — nie odpowiadać i zablokować algorytmiczną sekwencję. Obserwator — lub zbiór obserwatorów — stawia swoją reputację na udokumentowaniu tego, jak weryfikator został zapytany. Jeśli weryfikator milczy mimo zadeklarowanej polityki mówiącej co innego, można go skazać za naruszenie protokołu.

Mechanizm: znacznik czasu i kod wyzwania

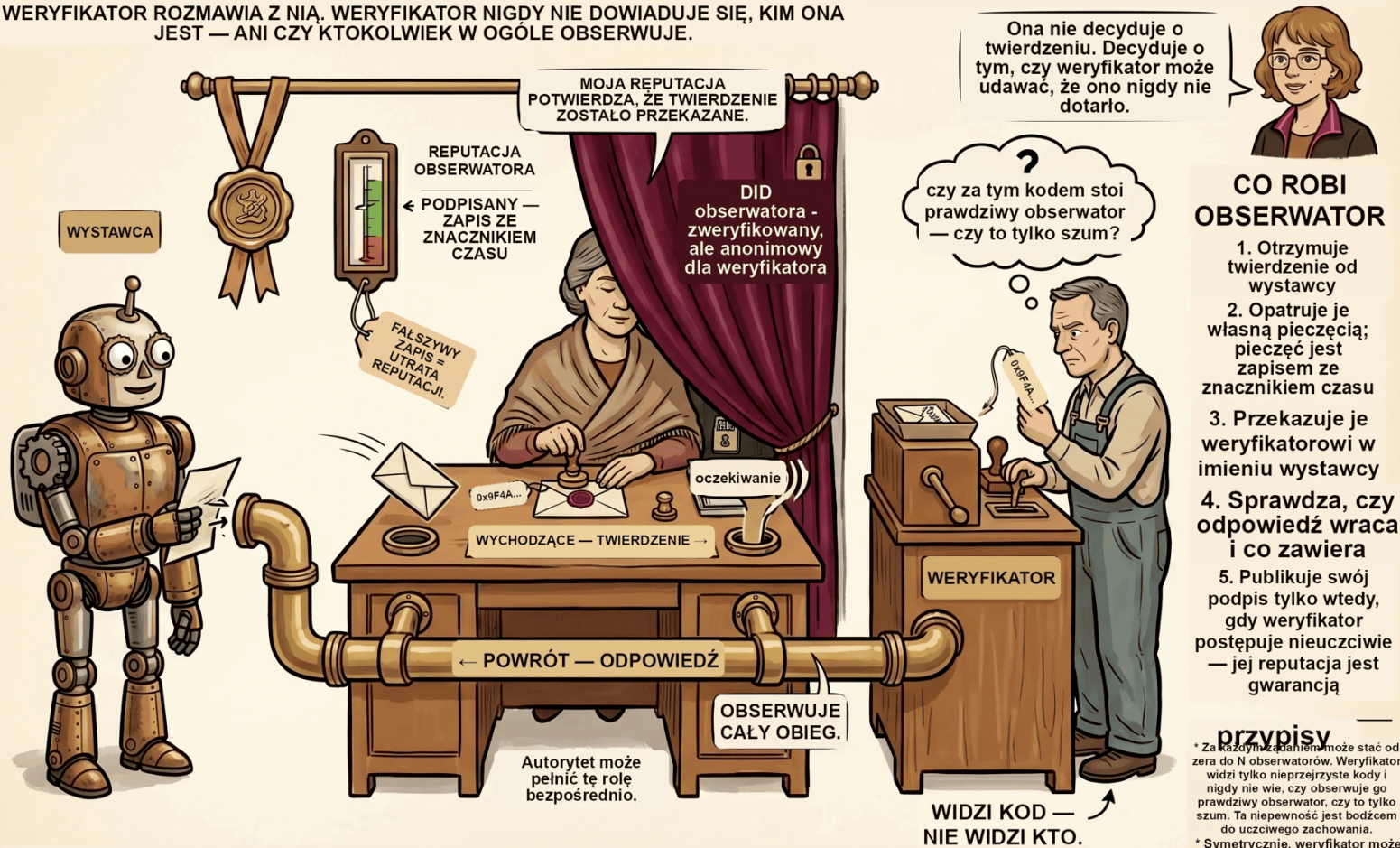
Zanim wyślesz tezę do weryfikatora, przepuszczasz ją przez obserwatorów — ludzi, którym ufasz, albo wyspecjalizowanych dostawców usług obserwatorskich pobierających niewielką opłatę. Każdy obserwator otrzymuje twoje zgłoszenie, opatruje je znacznikiem czasu, podpisuje, że widział jego wysłanie, i generuje kod wyzwania — kryptograficzny hash swojego podpisu. Kody są dołączane do twojego żądania. Weryfikator je widzi, ale nie ma pojęcia, kim są obserwatorzy ani czy kody są w ogóle prawdziwe. Obserwatorzy działają więc jako pośrednicy między wystawcą a weryfikatorem, trzymając niezależny zapis, że teza została złożona i co zawierała. Może ich być od zera do N.

Gdy weryfikator zachowuje się uczciwie — przyjmując lub odrzucając zgodnie z zadeklarowaną polityką — kody pozostają nieprzejryste. Nikt nie zostaje odsłonięty.

Ale jeśli weryfikator milczy mimo przychylniej polityki albo odpowiada w sposób sprzeczny z tym, co opublikował, ty trzymasz oryginalne podpisy obserwatorów. Możesz je opublikować jako pośrednie świadectwo, że teza została złożona i że weryfikator nie zastosował się do protokołu. Każdy może sprawdzić, że podpisy pasują do kodów wyzwania.

OBSERWATOR — POŚREDNIK, KTÓRY PRZEKAZUJE TWIERDZENIE I OBSERWUJE CAŁY OBIEG

WERYFIKATOR ROZMAWIA Z NIĄ. WERYFIKATOR NIGDY NIE DOWIADUJE SIĘ, KIM ONA JEST — ANI CZY KTOKOLWIEK W OGÓLE OBSERWUJE.



CO ROBI OBSERWATOR

1. Otrzymuje twierdzenie od wystawcy
2. Opatruje je własną pieczęcią; pieczęć jest zapisem ze znacznikiem czasu
3. Przekazuje je weryfikatorowi w imieniu wystawcy
4. Sprawdza, czy odpowiedź wraca i co zawiera
5. Publikuje swój podpis tylko wtedy, gdy weryfikator postępuje nieuczciwie — jej reputacja jest gwarancją

przypisy

* Za każdy błąd w relacji może stać o zero do N obserwatorów. Weryfikator widzi tylko nieprzejrzyste kody i nigdy nie wie, czy obserwuje go prawdziwy obserwator, czy to tylko szum. Ta niepewność jest bodźcem do uczciwego zachowania.

* Symetrycznie, weryfikator może przekierować odpowiedź przez własnego obserwatora — ten sam trik, przeciwny kierunek.

Anonimowy dla opinii publicznej, odpowiedzialny przed siecią. Weryfikator widzi kod, nigdy obserwatora.

Puenta: nie potrzebujesz prawdziwych obserwatorów

I tu najbardziej elegancka część: **wcale nie potrzebujesz prawdziwych obserwatorów**. Możesz wygenerować liczby losowe, które wyglądają dokładnie jak kody wyzwania. Weryfikator nie odróżni jednego od drugiego — musi rzucić kością, czy zaryzykować swoją reputację. Za każdym otrzymanym żądaniem mógłby czuwać incognito szanowany obserwator — albo mógłby to być czysty szum. Weryfikator nie wie. I ta niepewność jest właśnie mechanizmem.

Koszt utrzymywania uczciwej presji: niemal zero (liczby losowe są darmowe). Potencjalny koszt nieuczciwości dla weryfikatora: katastrofalny. Uczciwe zachowanie jest premiowane nawet wtedy, gdy tak naprawdę nikt nie patrzy.

System działa, bo każdy jest odrobinę paranoiczny. Niepewność jest tańsza niż inwigilacja.

BLEF, KTÓRY UTRZYMUJE WERYFIKATORA W UCZCIWOŚCI

PRAWDZIWY OBSERWATOR I LOSOWY BLEF WYGLĄDAJĄ IDENTYCZNIE Z PERSPEKTYWY WERYFIKATORA



■ Wielu weryfikatorów w jednej iteracji

Wzmacniającą regułą towarzyszącą dla dostępności weryfikatorów może być rozszerzenie algorytmu zwracające w jednej iteracji zbiór kandydatów na weryfikatorów, a nie tylko jednego.

Delegacja

Cywilizacja zbudowała swój wzrost gospodarczy na zdolności do podziału pracy i specjalizacji. Świat w pełnej krasie jest złożony, a nasze szanse na ogarnięcie go w całej złożoności są bliskie zeru. Naturalnym wyjściem jest delegowanie szerokiego zakresu czynności wspierających wygodne życie wyspecjalizowanym dostawcom, którzy oszczędzają nam czas, energię i pieniądze, i pozwalają nam z kolei się specjalizować — świadcząc usługi, w których jesteśmy najlepsi albo które rynek najwyżej u nas ceni.

Ta sama logika delegacji rozciąga się na sieć reputacji. W rozdziale Przełącznik wolność–totalitaryzm (i delegacja) przedstawiliśmy zasady ochrony wolnego społeczeństwa poprzez ograniczenie liczby tez, które można opublikować w sieci w danym oknie czasowym (pomyśl, w uproszczeniu, o niskim jednocyfrowym rzędzie praw publikacji rocznie, tak by społeczeństwo pozostało maksymalnie wolne). Zasadę tę można rozszerzyć na wiele wymiarów. Nie musimy mieć tylko jednej liczby — możemy mieć kilka limitów, stosujących się do różnych typów tez. Możemy używać innej liczby do sygnalizowania cudzej obłudy niż do przewinień w transakcjach biznesowych, a, powiedzmy, zmiana dokumentu DID taka jak zmiana hasła to coś, o co wspólnota z trudem w ogóle się zatroszczy, i tak dalej. Wszystko zależy

od tego, jak wspólnota definiuje, w czasie ewolucyjnym, co służy jej interesom w znalezieniu właściwej równowagi między docelowym poziomem wolności a rozliczalnością.

Dlaczego liczba praw publikacji przyznanych mi przez wspólnotę powinna być wystarczająco mała? Oznaczenie DID (podmiotu) negatywną tezą niszczy reputację, którą budowano długo, a szkoda trwa. Zniszczona reputacja napotyka skalę eskalujących sankcji ze strony wspólnoty za każde dalsze lub powtórzone przewinienie, aż po całkowite wyeliminowanie zakłócającego podmiotu (przypadek skrajny). Wykładniczo eskalująca skala kary nie potrzebuje dużego wolumenu tez, o ile są poparte weryfikowalnymi dowodami. Dotyczy to spokojnego stanu ustalonego, gdy społeczeństwem nie wstrząsa katastrofa (zewnętrzna lub wewnętrzna).

Dla zdarzeń o bardzo niskim prawdopodobieństwie częstość statystyczna jest zmienna, gdy stosuje się ją do jednostki. W skali populacji wspólnoty już nie. To jest wartość delegowania swoich praw publikacji wyspecjalizowanym autorytetom agregującym, które — podobnie jak wzajemne ubezpieczenie na wypadek szkody — używają twojego prawa i stosują je w twoim imieniu. Powiedzmy mniej abstrakcyjnie i podajmy kilka przykładów: - wykrywanie i zwalczanie przestępczości zorganizowanej - egzekwowanie porozumień handlowych - zarządzanie przywilejami (dowody wykształcenia, nabycia / zbycia majątku itd.) - i tak dalej

DELEGAT — USŁUGA TWIERDZEŃ, KTÓRĄ SUBSKRYBUJESZ

DELEGUJ TO, CZEGO NIE OGARNIESZ SAM · ZATRZYMAJ TO, CO DLA CIEBIE WAŻNE



Zleć to, czego nie ogarniesz sam. Bądź na bieżąco. Odbierz prawa w każdej chwili.

* Jeśli delegat działa poza uzgodnionym zakresem, publicznie ucierpi zarówno jego reputacja, jak i twoja.

■ Jak faktycznie działają „prawa publikacji”

Grafika dla delegata pokazuje prawa publikacji jako fizyczne żetony dla jasności, ale w systemie taki obiekt nie istnieje. To, co faktycznie się dzieje, jest takie: polityki ludzi, z którymi chcesz pozostać w dobrych relacjach — twojej wspólnoty — agregują się w emergentną regułę o tym, ile też rocznie przyjmą od ciebie jako istotne, zanim zaczną traktować cię jak szum. Limit istnieje po to, by sieć nie utonęła w błahych tezach „a co jeśli” i pozostała tak wolna, jak wspólnota chce (sygnał zachowany przez ograniczenie wolumenu).

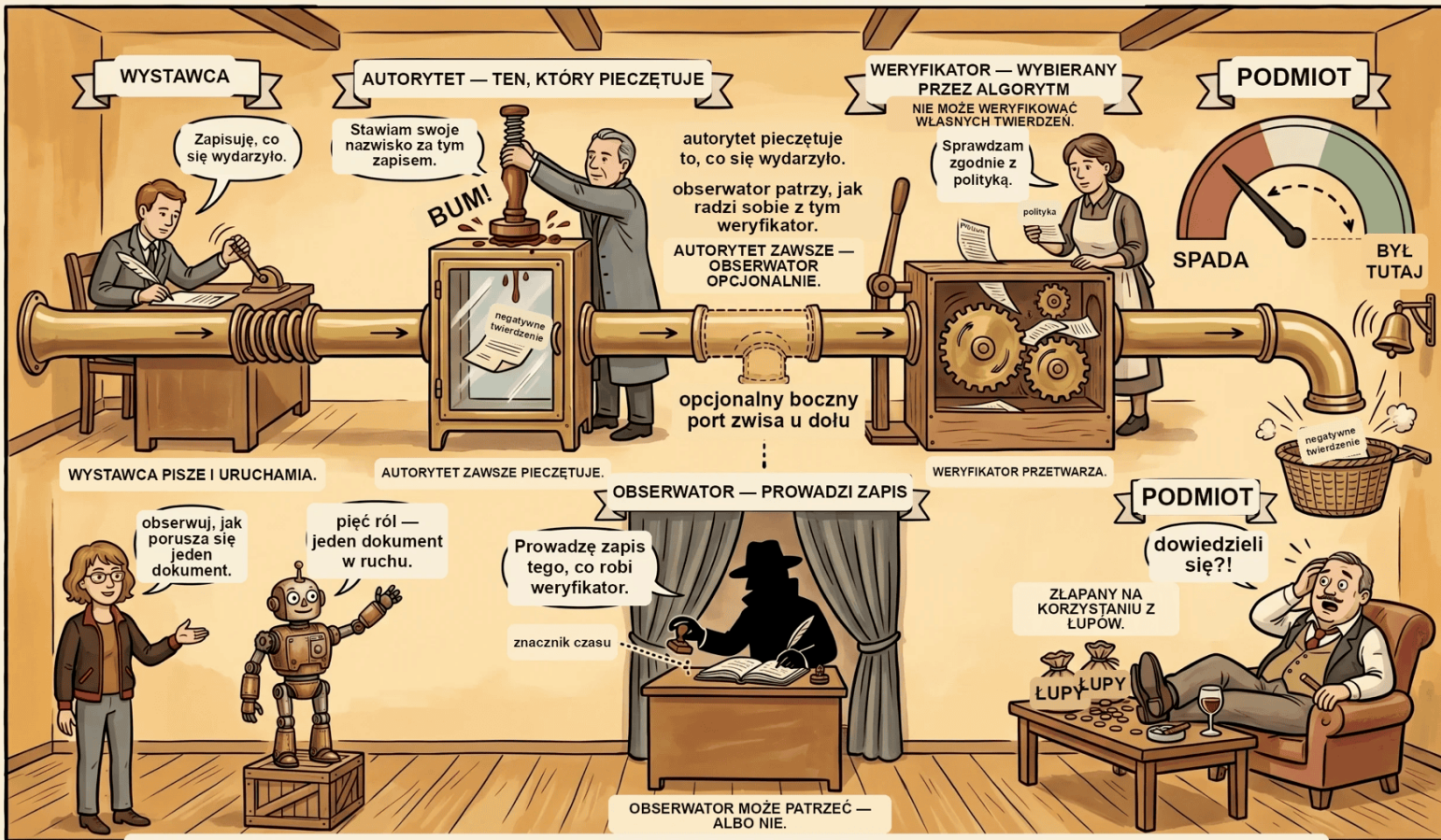
Czytasz to, na co pozwala ci twoja wspólnota. Jest to zakres, z pewnym rozrzutem zależnym od tego, którym ludziom nadajesz największą wagę. Następnie decydujesz — w ramach tego przydziału — ile też opublikować samodzielnie, a ile delegować profesjonalnym usługom, które opublikują w twoim imieniu tylko wtedy, gdy zdarzenia mieszczą się w ich zakresie. To właśnie utrzymuje cię w dobrych relacjach, nie zmuszając do składania tezy za każdą drobnostkę, która ci się przydarza.

„Żetony” na grafice są wizualnym zastępnikiem tej pętli czytaj-i-decyduj, a nie dosłownym artefaktem.

Warto móc cofnąć delegowane prawa publikacji w sieci reputacji. Można to zrobić w każdej chwili, dopóki delegat nie użył jeszcze delegowanego prawa.

NEGATYWNE TWIERDZENIE PRZEPŁYWA PRZESYSTEM

PRZEŚLEDŹ JEDEN DOKUMENT — ZOBACZ, CO ROBI Z NIM KAŻDA ROLA



PIĘĆ RÓL, JEDEN DOKUMENT W RUCHU — NIKT NIE MOŻE WERYFIKOWAĆ SAMEGO SIEBIE.

Komunikacja między rolami

Poniższa grafika podsumowuje, jak role łączą się w rzeczywistym przypadku — od złożenia tezy przez wystawcę aż po publikację w sieci reputacji.

Emergentna umowa społeczna — polityka

Jak dotąd opisaliśmy, jak weryfikuje się tezy i jaką rolę odgrywa każdy z uczestników. Teraz przejdźmy do tego, jak tysiące indywidualnych polityk staje się czymś, co działa jak prawdziwa umowa społeczna. Niczym, co przypominałoby lewicowe marzenia o umowie społecznej i wymuszonej solidarności.

Każdy uczestnik deklaruje własną politykę opartą na swojej moralności (policy) — co uznaje za akceptowalne i jak reaguje na konkretne zachowania innych. Suma wszystkich polityk w sieci znanych danemu DID (wspólnocie) wytwarza emergentną etykę — obserwowalne normy, których nikt nie zaprojektował. Te emergentne normy, podparte dwustronnymi sygnałami cenowymi, tworzą mierzalną umowę społeczną: nie teoretyczny konstrukt, którego nikt nie podpisał przy urodzeniu, lecz empirycznie obserwowalne reguły poparte faktycznym zachowaniem.

■ Umowa społeczna

Ludzie spierają się, czy „umowa społeczna” nie jest oksymoronem. Nikt niczego nie podpisuje, a mimo to przywołuje się ją do uzasadniania działań legislacyjnych i wykonawczych w społeczeństwach scentralizowanych.

Fenomenologiczna analiza interakcji w sieci zdecentralizowanej mogłaby ujawnić pewne emergentne reguły — globalne lub lokalne. Jak powinniśmy nazwać te szeroko podzielane normy? Umową społeczną? Podobnie jak w przypadku wspólnot, umowy społecznej danej wspólnoty nie da się obserwować i wyznaczyć precyzyjnie — każdy kąt spojrzenia na wspólnotę daje inną umowę społeczną.

■ Polityka oparta na wartościach

Równie mylące jest traktowanie „polityki opartej na wartościach” jako fundamentu podejmowania decyzji. Wartości są raczej fenomenologicznymi skupiskami reguł powszechnie preferowanych w danym czasie. Ewoluuja i nie są stałe w czasie.

POLITYKI SIĘ SPOTYKAJĄ. POSTAWY SIĘ KSZTAŁTUJĄ.

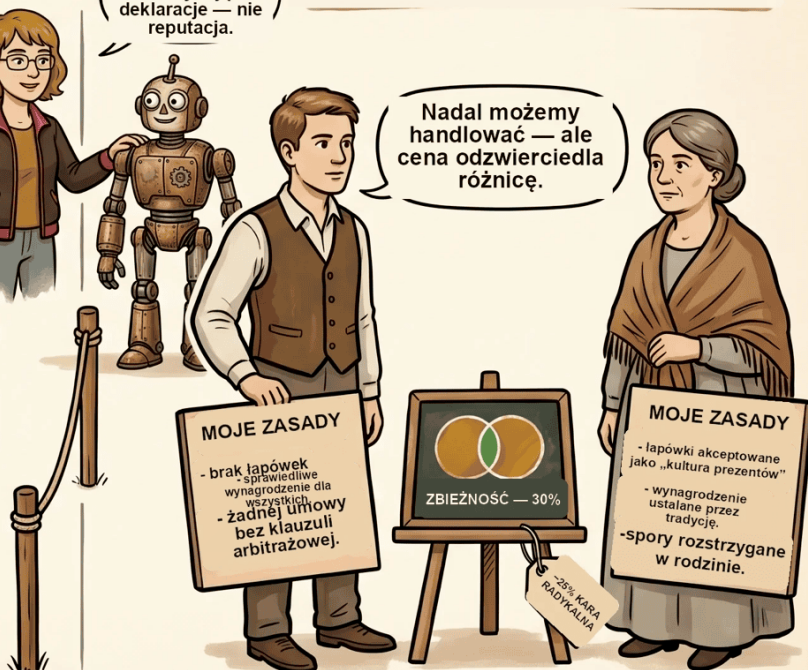
ZADEKLAROWANE ZASADY USTALAJĄ DZISIEJSZĄ CENĘ — ZNIŻKA ZA ZGODNOŚĆ, KARA ZA ROZBIEŻNOŚĆ

GDY POLITYKI SĄ ZGODNE



Ten sam towar, dwie ceny. Decydują deklaracje — nie reputacja.

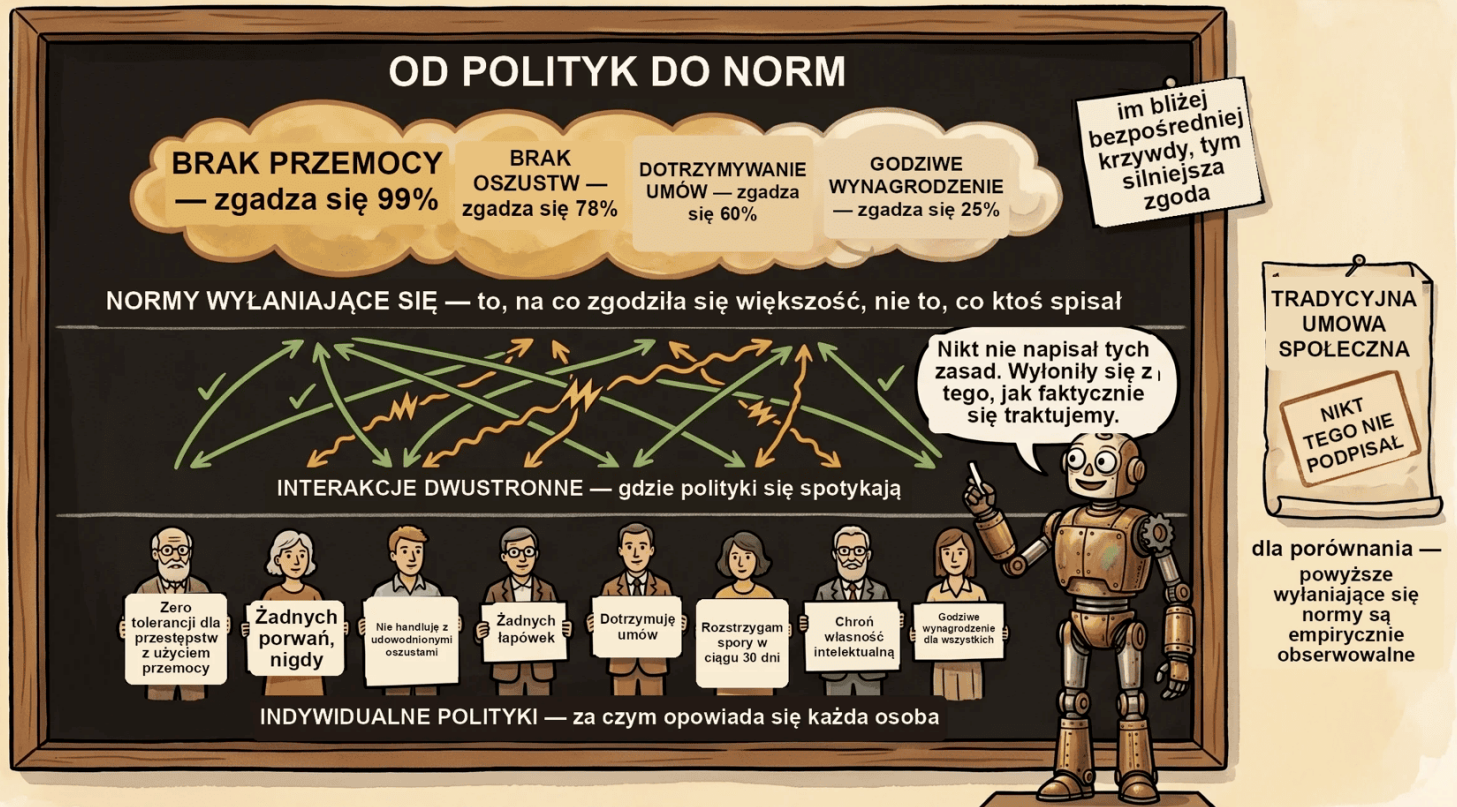
GDY POLITYKI SIĘ ROZCHODZĄ



Gdy w handlu spotykają się dwie polityki, ich zgodność staje się modyfikatorem ceny.

* Nie chodzi tu o reputację. Chodzi o to, co każda osoba publicznie zadeklarowała — i czego teraz oczekuje się, że dotrzyma.

JAK ETYKA WYŁANIA SIĘ Z INDYWIDUALNYCH POLITYK



Etyka nie jest zaprojektowana. Wyłania się z tego, jak faktycznie się traktujemy.

* Każda indywidualna polityka jest odzwierciedleniem moralności danej osoby — ukształtowanej presją dostosowania się do jej społeczności i otoczenia.

Udostępnianie informacji o sobie

Gdy dwa podmioty DID, które się nie znają, wchodzą w relację ekonomiczną, możemy podpisać żądanie do naszej własnej wspólnoty w imieniu drugiej strony, prosząc ją o udostępnienie informacji o nas. Jest to jednak bardzo naiwne wyobrażenie o tym, czym są wspólnoty. Nie są zbiorami zamkniętymi — pojedynczy DID może być uczestnikiem wielu wspólnot.

Wspólnota jest raczej zjawiskiem fenomenologicznym z perspektywy danego uczestnika, przejawiającym się w jego sieci społecznościowej; nie jest czymś, co zawsze ma sens wyznaczać wprost. Mieszkańcy wsi mogą tworzyć wspólnotę, ale osoba, która przyjeżdża tam tylko na weekendy, może również należeć do innej wspólnoty w tej samej wsi. Wspólnotą może być też drużyna piłkarska wraz z kibicami, działaczami i rodzinami wszystkich zaangażowanych. Naród lub obywatele państwa również mogą tworzyć wspólnotę lub wspólnoty. Patrzenie na DID pod różnymi kątami może dawać różne (i często intuicyjne) obrazy wspólnot.

DID na granicach są więc mostami między wspólnotami i — tak jak w prawdziwym życiu — odgrywają rolę w dostarczaniu informacji o członkach innych wspólnot, czy to na poziomie amatorskim, czy profesjonalnym, jak autorytet wyspecjalizowany w łączeniu ludzi i agregowaniu informacji o ryzykownych DID.

Niektóre rodzaje informacji w sieci DID dobrze nadają się do bezwarunkowej wzajemnej wymiany (przestępstwa z użyciem przemocy, oszustwa itd.). Inne rodzaje informacji wspólnota może jednak traktować jako zastrzeżone do użytku wewnątrz wspólnoty (odpowiednik obywatelstwa, usług wyświadczonych wspólnocie itd.). Czy takie informacje można rozpowszechniać, zależy od deklarowanych polityk członków wspólnoty.

Wspólnota strzeże swojej prywatności we własnym kręgu, a w zamian wymienia wzajemnie korzystne informacje na zasadzie bezwarunkowej.

Zbrodnia i kara

Zbrodnia i kara

Wiemy, jak działa sieć: jak powstają zapisy, kto je weryfikuje, jak zniechęca się do oszustwa ze strony weryfikatora. Pozostaje jedno pytanie — co dzieje się, gdy ktoś faktycznie wyrządza krzywdę innemu?

Jak bardzo zależymy jedni od drugich?

Wszyscy stoimy na scenie tego wielkiego świata, a cokolwiek się tu dzieje, dotyczy nas wszystkich.

Jan Amos Komeński (Labirynt świata i raj serca)

Może być wiele powodów, by dołączyć do sieci reputacji lub ją odrzucić. Wierzę jednak, że pewien aspekt ludzkiej natury — często uważany za mroczny — może służyć dobremu celowi. Mówię o ludzkiej potrzebie poczucia satysfakcji w obliczu odczuwanej niesprawiedliwości.

Satysfakcja, sprawiedliwość, zemsta — kojarzymy je z negatywnymi emocjami. Aby społeczeństwo się trzymało, musimy przynajmniej udawać, że satysfakcję wymierzają scentralizowane instytucje; inaczej jednostki nie czułyby więzi ze społeczeństwem, w którym żyją. Średnio potrzebujemy przynależeć do jakiejś drużyny i jej ufać. Gdy ktoś krzywdzi drugiego, społeczeństwo patrzy, jak zostanie wymierzona

satysfakcja i w jakim stopniu. Nieco kontrowersyjnie twierdzę, że często w historii — i teraz — nie miało znaczenia, czy proces przeciw oskarżonemu był czysty; liczyło się to, że społeczeństwo widziało, jak *ktos* zostaje ukarany. Spełniało to swoją funkcję (liczne pomyłki sądowe i opór przed wznawianiem starych spraw mówią o tym dostatecznie dobrze). Punkt widzenia ofiary i osieroconych jest tylko wtórny. Najpierw liczą się sygnały dla reszty społeczeństwa, bo niesprawiedliwości nie są aż tak częste, by figurować w dniu każdej jednostki.

Zdecentralizowany system reputacji pozwoliłby opinii publicznej zobaczyć dowody bezpośrednie i poszlakowe (audytowane i nieaudytowane). Społeczeństwo mogłoby ocenić informacje — samodzielnie albo poprzez wolnorynkowe usługi wyspecjalizowane w takiej ocenie — i zdecydować, na podstawie sygnałów jakościowych i ilościowych, jakie środki zastosować wobec podmiotu (albo nawet wobec autora lub weryfikującego autorytetu).

Czym jest kara? To forma upokorzenia domniemanego sprawcy poprzez utratę jego przywilejów — tak by zarówno ofiara, jak i społeczeństwo poczuło, że szkodliwe czyny się nie opłacają. To istota rzeczy: szkodliwe lub niebezpieczne zachowanie nie może się opłacać, a jednocześnie musi dawać poczucie satysfakcji zarówno ofiarom, jak i reszcie społeczeństwa / wspólnoty.

Czy taką karę musi wymierzać centralna władza? A gdyby każdy mógł z góry zadeklarować, jak zareaguje na pewne czyny? Oczywiście nie mogę wykonać kary na cudzej własności. Ale mogę zadeklarować, że udostępnię swoją własność wybranemu zbiorowi władz wykonawczych w celu ukarania sprawcy, jeśli przewinił i wejdzie w moje domeny. I mogę to zadeklarować publicznie, tak by inni mogli ocenić moje podejście.

I tu wchodzi cenowy mechanizm proporcjonalności. Jeśli deklaruje surowe kary za drobne przewinienia, sieć wycenia mój ekstremizm: inni uznają mnie za nieproporcjonalnego, a moje koszty weryfikacji wzrosną — mniej ludzi będzie chciało ze mną handlować albo tylko po gorszych cenach, a mniej

weryfikatorów przyjmie moje zapisy po rozsądnej cenie. Jeśli z kolei jestem zbyt pobłażliwy, wspólnota uzna mnie za ryzyko. Jeśli toleruję oszustwo, wspólnota prawdopodobnie będzie pobłażliwa wobec sprawców czynów, które dotyczą mnie — żeby dać mi posmakować własnego lekarstwa.

Sprawiedliwość przestaje być dobrem luksusowym. Gdy ktoś cię krzywdzi, zapisanie krzywdy jest przystępne cenowo, zapis jest trwały, a konsekwencje dla sprawcy są realne.

Wykrywanie obłudy

Zadeklarowanie polityki nie wystarczy — jeśli deklaruję, że przestrzegam reguły, ale moje zachowanie od niej odbiega, luka jest reputacyjnym obciążeniem. Sieć nie rozróżnia „złamał prawo” i „złamał własne słowo” — oba są mierzalnymi sygnałami. Obłuda jest droga, a nie znam bardziej drażniącej czerwonej płachty.

JEDNA PUŁAPKA. JEDNO WYJŚCIE.

WTajemniczony ZAWSZE WYGRYWA KONTRAKT — DOPÓKI SIĘ NIE POZWOŁI LUDZIOM KUPOWAĆ BEZPOŚREDNIO, BEZ ZEZWOLENIA.



Opinia publiczna zgadza się, że potrzebny jest nowy publiczny system IT, finansowany z budżetu, finansowany z podatków.



Za zamkniętymi drzwiami urzędnik ds. zamówień i wtajemniczony projektują przetarg tak, by pasował do jednej firmy. Koperta zmienia właściciela.



Urzędnik wzrusza ramionami. Jego kieszeń wybrzusza się od łapówek.



Kontrakt zostaje przyznany. Wtajemniczony ma licencję — ale nie ma umiejętności ani szacunku dla pracy.



Wtajemniczony odwiedza sąsiada. „Życzliwa oferta” to najniższa okruszyna.

1. TRADYCYJNY



skarga



cisza



zamknięte drzwi



u prawnika



Skarga, cisza, terminy, prawnik.

Pułapka jest wbudowana w same zasady.

Tam, gdzie regulacja jest fosa, sieć jest mostem.

SIEĆ REPUTACJI
— tu zaczyna się nowy świat —

2. SIEĆ REPUTACJI



najpierw dostawa



popyt ją znajduje



godne utrzymanie

Najpierw dostarcza. Ludzie znajdują aplikację i z niej korzystają. Każdy wdzięczny użytkownik płaci niewiele. Godne utrzymanie. Żadnego centralnego autorytetu do przekupienia.

Reputacja jest nowa. Dostawa jest dowodem.

Dwie ścieżki. Pułapka tkwi w zasadach. Wyjściem jest całkowite ominięcie zasad.

* Gdy zasady pisze wtajemniczony, skarczenie się w ramach tych zasad jest pułapką — nawet grzywny wracają do kolejnego ustawionego przetargu. Sieć reputacji jest wyjściem: obywatela znajdują produkt, płacą twórcy bezpośrednio, a społeczność nadaje jedyną licencję, która się liczy — zaufanie zdobyte dostawą.

■ Ilość kontra jakość — łamanie binarnego paradygmatu winy

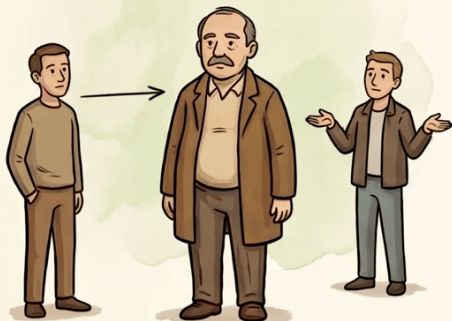
W scentralizowanym wymiarze sprawiedliwości wina jest binarna: 0 albo 1, winny albo niewinny. W sieci reputacji liczy się nie to, czy wina została udowodniona, lecz akumulacja sygnałów.

Pojedyncze nieudowodnione oskarżenie o kradzież wobec oskarżonego prawdopodobnie nie wzbudzi wielkiej czujności — ale wzbudzi czujność wobec oskarżyciela. Wiele poszlakowych wskaźników z różnych niezależnych źródeł zaczyna jednak nabierać wagi. Liczy się nie tylko ilość, ale i jakość: niezależność świadków (różni ludzie, różne konteksty), spójność wzorca (powtarzający się typ podejrzenia), korelacja czasowa.

I odwrotnie, częste bezpodstawne oskarżenia powracające od tego samego wystawcy przeciw różnym podmiotom docelowym mogą zostać ocenione jako pomówienie — a reputacja oskarżyciela płaci cenę.

JAK GROMADZĄ SIĘ DOWODY

„jedno odosobnione twierdzenie”



jedno twierdzenie samo w sobie — zbyt słabe, by na nim działać. żadna ze stron nie jest potępiona.

„wzorzec”



pięć niezależnych źródeł — wyłania się wzorzec.

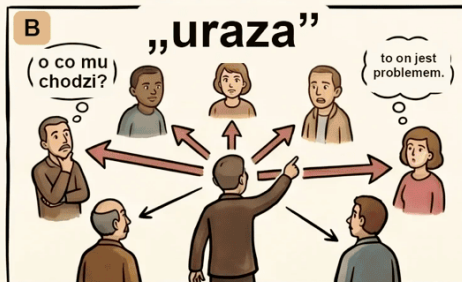
„przytłaczający ciężar”



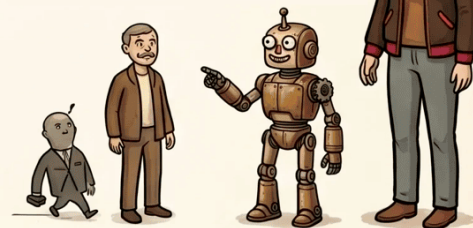
dwadzieścia niezależnych źródeł — przytłaczający ciężar.



rozpowszechnianie tego samego twierdzenia bez dowodów — gdy społeczność nic nie widzi, to oszczerstwo, i kosztuje oskarżyciela. Niezależność jest wszystkim. Jeden głos powtarzany to szum. Wiele głosów z różnych miejsc to sygnał.



jeden oskarżyciel wskazujący na wszystkich — wzorcem jest oskarżyciel, nie oskarżony.



to wygląda jak dzisiejszy świat. bo nim jest — tylko motywy są teraz uczciwe. żadnej rewolucji. tylko lepsze bodźce.

Nie powinniśmy przeoczyć też zadośćuczynienia — dobrowolnego czynu przed udowodnieniem winy, oferującego drogę do łagodniejszej kary. Kara wchodzi w grę, gdy sprawca nie robi żadnego kroku ku zadośćuczynieniu i liczy na uniknięcie konsekwencji — podobnie jak taki wynik można kupić poprzez korupcję w systemie scentralizowanym.

Rodzaje przewinień

Rodzaje informacji nie muszą ograniczać się do czynów przestępczych; mogą obejmować: - opisy przestępstw - naruszenia umów i oszustwa - niemoralne zachowanie - zakłócenia porządku publicznego, realne i wirtualne - ...

Każdy nowy zapis w sieci DID koryguje ocenianą reputację i ryzyko danego DID (czy to podmiotu, autora, czy weryfikującego autorytetu). Im większą odpowiedzialność ponoszę za los innych, tym osrożniejszy się staję.

PO SZKODZIE — CO ZROBISZ?

odprawiony. zmuszony. dobrowolnie. trzy sposoby, w jakie odpowiada wioska.

co się stało



no i co teraz?



racjonalny wybór jest zawsze najtańszy: NAPRAW TO SAM.

„próbuję to zignorować — odprawiany wszędzie”



brak zadośćuczynienia — każdy sklep go odprawia — wygnanie z życia gospodarczego

„naprawiam to — ale tylko pod spojrzeniem tłumu”



wymuszone zadośćuczynienie pod spojrzeniem tłumu — splecone, ale wioska podnosi mu cenę — lekcja musi zostać zapamiętana.

„przychodzę sam — i przyznaję się przed wszystkimi”



dobrowolne, wcześnie zadośćuczynienie — przyjęte publicznie — reputacja się odbudowuje, z ostrożnością

to wygląda jak dzisiejszy świat. bo nim jest — tylko koszty są teraz widoczne dla wszystkich. żadnej rewolucji. tylko lepsze bodźce.

■ Egzekwowanie kary poprzez delegację

Nie muszę egzekwować kary osobiście. Mogę zapłacić (podobnie jak za ubezpieczenie) autorytetowi, który egzekwuje wyniki według z góry określonych reguł — odpowiednikowi usług śledczych, ścigania i sądowniczych. Jeśli autorytet egzekwuje nieproporcjonalnie albo nie egzekwuje wcale, cierpi jego reputacja — a jego reputacja jest fundamentem jego zdolności do zarabiania na życie.

Delegacja jest w sieci zasadą ogólną: dowolną czynność DID można delegować innemu DID — weryfikację, wystawianie tez, reagowanie na spory, deklarowanie konsensusu. Delegację można cofnąć w każdej chwili. Umożliwia specjalizację bez utraty ostatecznej kontroli.

KTO DOCHODZI, KTO EGZEKUJE?

„szkoda” → „śledczy” „zapis” → „egzekutor” → „odpowiedzialność”



DELEGOWANIE JEST ODWOŁYWALNE. Każdą aktywność DID można delegować do innego DID — i odwołać w dowolnym momencie.
nie egzekwujesz kary sam. delegujesz. a pełnomocnik odpowiada przed tobą.

■ Demokratyzacja zarządzania ryzykiem

Niecenzurowalna sieć reputacji zdemokratyzowałaby to, co banki lub utrzymujący wielkie kompleksy przemysłowe już robią jako podstawową działalność — zarządzanie ryzykiem.

Dla bankiera wobec klienta ocena ryzyka jest przygotowana z góry, tak by mógł skupić się na interakcji biznesowej w ramach z góry określonych limitów. Wyrafinowane zespoły utrzymania ruchu przy regularnych przeglądach zbierają wskaźniki ryzyka (oznaki pęknięć konstrukcji, procesy degradujące infrastrukturę operacyjną itd.) i potrafią przewidzieć żywotność urządzeń oraz to, kiedy i jaka interwencja będzie potrzebna.

Wyobrażam sobie użycie DID podobnie — ktoś (prawdopodobnie za opłatą) dostarczy czytelne dla człowieka podsumowanie drugiej strony. Podsumowanie odzwierciedli kąt oceny ryzyka, który zamówił klient.

KARA BEZ CENTRALNEGO AUTORYTETU



Zadośćuczynienie jest tańsze niż kara.

Kara jest tańsza niż ignorancja.

Podążaj za pieniędzmi

Podążaj śladem pieniędzy

Mamy zdecentralizowaną sieć reputacji i motywację, by z niej korzystać. Już teraz może ona dać swoim użytkownikom przewagę konkurencyjną — wyjaśniając potencjalne ryzyka, pomagając im efektywniej planować dobór drugiej strony i strategię negocjacji oraz uwzględniać środki ograniczające te znane ryzyka.

To, co następuje, jest jedną z możliwych metodyk⁵ jej wykorzystania — z użyciem właściwości sieci do zbudowania ścieżki migracji od obecnego systemu do jego ewolucyjnego następcy. Prawdopodobnie nosi cechy charakterystyczne dla Europy Środkowej, gdzie ta teza powstała. Lokalne warunki będą wymagać lokalnych korekt. To, co poleciłbym zachować wszędzie, to bezkompromisowy charakter środków wobec państwa — bez tego cel rozmyje się w niekończącej się dyskusji, a zmiana nigdy nie nadejdzie. Uważaj — przedstawiciele i zwolennicy państwa będą zajmować cię bzdurami. Nie daj się nabrać; na szali jest ich byt.

⁵**Dekonstrukcja państwa** — w kontekście czeskim zostanie to prawdopodobnie dogłębnie omówione w nadchodzącej książce pod tym samym tytułem czeskiego autora Daniela Steigerwalda (planowanej na 2026). Osobiście wiąże duże nadzieje z inspirującymi procedurami, które będzie zawierać.

Słaby punkt państwa — pieniądze

Wróćmy do początku. Chcemy więcej wynikowych wolności, więcej wpływu na ich kształt i więcej współmiernej im odpowiedzialności. Pytanie jest proste: gdzie państwo ma czuły punkt, na który możemy naciskać bez uciekania się do przemocy?

Odpowiedź jest nudna i tym mocniejsza. Pieniądze.

W swej istocie państwo jest przepływem pieniędzy. Pieniędźmi opłaca swój aparat przymusu — ostatnie ogniwo, które egzekwuje jego reguły. Bez pieniędzy nie ma monopolu na przemoc. Gdy pieniądze zaczynają się zacinać, państwo zaczyna się wycofywać — bo nie ma już czym płacić tym, którzy fizycznie trzymają je w miejscu.

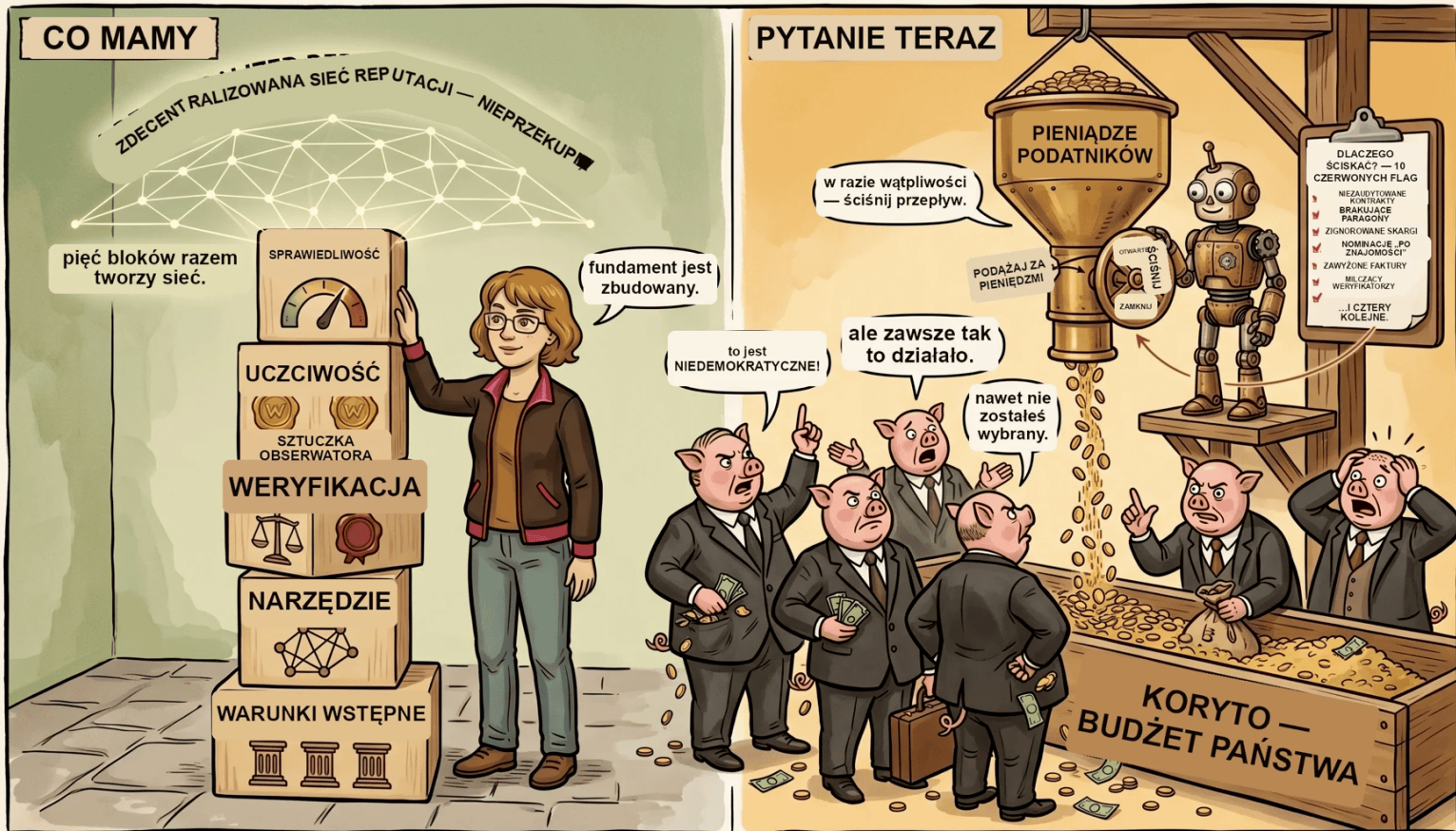
Przepływy pieniędzy naturalnie wahają się — sezonowo, gospodarczo, według nastrojów inwestorów. Państwo maskuje to zaciąganiem pożyczek na rynkach finansowych. Czasem pożyczka jest racjonalna: inwestycja, która się zwraca. Częściej jednak pokrywa przerośnięte wydatki na agendy, które dawno wyrosły poza podstawowy cel państwa — obronę, bezpieczeństwo wewnętrzne, wymiar sprawiedliwości karnej, sprawy zagraniczne. Po przekroczeniu pewnych progów bank centralny reaguje stopami procentowymi zakotwiczonymi w jego własnym szacunku inflacji.

I tu przychodzi cichy podatek. Inflacja to daleko więcej niż jedynie księgowe zmartwienie makroekonomistów. Jest ukrytym podatkiem od siły nabywczej waluty, płaconym przez każdego, kto odłożył kilka groszy na starość. Niska inflacja jest tolerowana przez opinię publiczną, bo nie pojmuje ona jej długoterminowych skutków — nie zdaje sobie sprawy, że nawet jednocyfrowe wartości, składane przez długi horyzont, erodują oszczędności do punktu, w którym ludzie nie są już w stanie zabezpieczyć własnej starości. A gdy nie są, zostają wyćwiczeni w zależności od świadczeń państwowych. W końcu wiszą na tych świadczeniach i są przywiązani do państwa.

W burzliwych czasach — wojna, pandemia, „niezbędna” inwestycja — państwo po prostu włącza maszynę drukarską. Siła nabywcza odpowiedzialnych ciułaczy i pracowników spada, a my obiecujemy im, że są dobrze wynagradzani. Ktoś po cichu kradnie im czas i chwali za to, jak wspaniale zarabiają.

To poważnie podkopuje zaufanie do państwa. A zaufanie jest jedynym spoiwem, które trzyma całą maszynę razem. To jest dźwignia, o którą warto się oprzeć.

PODĄŻAJ ZA PIENIĘDZMI — DOTYCHCZASOWA HISTORIA



Mamy sieć. Wiemy, jak działa. Teraz: w razie wątpliwości ściśnij zasobnik.

władza państwa opiera się na pieniądzu. podążaj za nimi.

■ Dlaczego pieniądze, a nie inne słabe punkty?

Innym słabym punktem cywilizacji jest na przykład dystrybucja energii. Ale zakłócanie jej przepływu nie jest dźwignią — byłoby agresją, terroryzmem. Dobrowolne nieuczestniczenie to nie to samo co rozmyślne krzywdzenie innych. Pieniądze są wyjątkowe w tym, że nacisk można wywierać dobrowolnie, przejrzystie i bez przemocy.

Proposed transition to the state's successor

Ewolucja, nie rewolucja

Nagła zmiana wywołuje opór nawet wtedy, gdy cel końcowy jest atrakcyjny. Zrywa więzi — społeczne, ekonomiczne, polityczne — a ludzie instynktownie bronią tego, co już znają, przed tym, czego jeszcze nie widzieli.

Właściwe podejście jest więc stopniowe — ewolucyjne. Takie, które uniemożliwia staremu systemowi wyłączenie nowego jednym pstryknięciem przycisku — bo w chwili, gdy mógłby, zrobiłby to.

Niestety oznacza to pogodzenie się z tym, że równowagowa dobrowolność nie zostanie osiągnięta w chwili wdrożenia sieci reputacji; nadejdzie wraz ze stopniowym tempem adopcji. Przyjęcie może być — i prawdopodobnie będzie — powolne, ciągnięte pragnieniem jednostek, by znaleźć ratunek u swojej wspólnoty poprzez sieć reputacji, gdy konformistyczny sposób szukania sprawiedliwości zawodzi (a zawiedzie). Zobaczmy, jak wygląda ta droga, wraz z proporcjonalnymi szacunkami.

■ Puste koryta — nie graj według reguł ustawionych tak, byś przegrał

Próby reformowania państwa od wewnątrz opierają się na wewnętrznych mechanizmach władzy, w nadziei, że urzędnicy przeprowadzą zmiany wbrew własnym bodźcom. To się nie stanie.

Po co karmić system, zamiast osuszyć kanały, które przynoszą mu życie? Zamiast zmieniać stary system i grać według jego reguł, zbudujmy nad nim nową warstwę — taką, która stopniowo zamienia stary system w podzbiór nowego. Na początku ten podzbiór niemal wypełnia nadzbiór. Z czasem aktorzy przechodzą na drugą stronę.

Firmy to wiedzą: gdy stary system jest zbyt zaplątany, by go wymienić, budujesz równoległy i stopniowo migrujesz do niego użytkowników.

To, że państwo skończy z rozdźwiękiem między tym, co faktycznie dostarcza, a tym, czego żąda jego statut, i że będzie skłonne przywoływać ten rozdźwięk, jest wyłącznie problemem jego przedstawicieli i uczestników — nie ma potrzeby oglądać się za tym. Jedyne, na co warto uważać, to: nie sprowokuj gwałtownej rewolucji.

Cztery narzędzia, które się wzajemnie wspierają

Do tej pory sieć reputacji DID mogła wydawać się użyteczna głównie dla sprawiedliwości i konsensusu. Wierzę, że mogłaby się ustabilizować i wytrzymać ataki — merytokratycznie, na podstawie faktycznych

zasług, a nie formalnych tytułów. Ale sama reputacja nie zmusi państwa do ustąpienia. Ekonomia to zrobi, i nacisk wywierany przez nią.

Nic nie stoi na przeszkodzie, byśmy używali tożsamości DID jako menedżerów dodatkowych narzędzi, które mocno naciskają na pieniądze. Nie zaczynaj od pełnej dobrowolności ze strony obywateli — wyznacz kierunek, którego państwo nie może zatrzymać. Przejście opiera się na czterech konkretnych narzędziach, które nawzajem osłaniają sobie plecy. Żadne z nich nie wystarcza samo w sobie.

Prosty system podatkowy — przynęta na wejście

Pierwszym narzędziem jest prosty, przejrzysty system podatkowy zbudowany na infrastrukturze DID. Jedna proporcjonalna stawka od wszystkich dochodów. Bez wyjątków, bez wakacji podatkowych, bez odliczeń dla firm, bez zachęt. Każda płatność jest audytowalnie powiązana z DID, który ją zapłacił. Sprawdzanie krzyżowe jest trywialne.

Stawka byłaby ustawiona nieco korzystniej niż w starym systemie dla części podatników — to jest przynęta na wejście. Obciążenie podatkowe malałoby rok do roku, system stawałby się coraz atrakcyjniejszy, a migracja nabierałaby tempa. System jest zarazem prowadzącym ewidencję i poborcą — bez pośrednika, bez nieprzejrzystości.

Elektroniczny rejestr wydatków (ESR)

Drugim narzędziem jest odwrócenie EET (Elektronicznej ewidencji przychodów) do góry nogami. Zamiast państwa śledzącego każdy paragon osoby samozatrudnionej, śledzimy każdy wydatek państwa. Państwo nie otrzymuje środków z prostego systemu podatkowego na żadną pojedynczą płatność, dopóki każda z nich — bez wyjątku — nie przejdzie przez to sito.

ESR to proxy⁶, które dopasowuje każdy zrealizowany wydatek państwa i sektora publicznego do zapisu planowanej płatności — wraz z kontekstowym uzasadnieniem oraz identyfikacją odbiorcy, podmiotu wydającego i celu. Wynikiem są surowe dane publiczne, dające się hierarchizować. Każdy może je wziąć i przeanalizować. Każdy może zaoferować podatnikom rekomendacje, co z nimi zrobić. To, czego izby kontroli nie zdołały osiągnąć przez lata, nagle jest dla każdego o jedno kliknięcie.

Nie musisz przechodzić na nowy system podatkowy, by wziąć udział. Wystarczy wpłacić w pełni zwrotną kaucję (powiedzmy 1–3 EUR) za zrealizowaną płatność. Niezrealizowana reszta przepada jako filtr spamu, tak by system nie został zalany atakami. Zapis może złożyć każdy — krewny za niezdolnego do czynności dziadka, sąsiad za zaniedbane usługi publiczne, przedsiębiorca za niezapłaconą fakturę, urzędnik przez eksport z własnego systemu.

Spodziewam się, że partie polityczne naturalnie przekształcą się w dostawców analiz albo powstaną nowe, by zastąpić stare. Zamiast składek pobieranych z podatków zaczną oferować ekspertyzę — dostarczając swoim zwolennikom opartych na wartościach przeglądów sprzymierzonych autorytetów, ich usług i polityk weryfikacyjnych. Zapisy niechlujne lub bezsensowne z lenistwa automatycznie stają się kandydatami do cięć budżetowych. W pierwszej rundzie twoja płatność zawsze zostanie wypłacona, ale zebrane dane służą jako podstawa oceny, czy wydatek państwa wciąż ma sens. Wykonawcy i inni na państwowej liście płac mają bodziec, by dopilnować, że urzędnicy odpowiedzialnie dopasowują wydatki. Inaczej pieniądze nie popłyną w kolejnej rundzie.

⁶**Proxy** (łac. *procurator*, ang. *deputy/intermediary*) — tutaj: pośrednik działający w imieniu innego podmiotu. Proxy ESR przyjmuje od każdego zapisy planowanych płatności, dopasowuje je do zrealizowanych wydatków państwa i udostępnia powstały zbiór danych opinii publicznej.

■ Skąd bierze się skrót ESR

W latach 2016–2022 czeski rząd wdrożył przeciwko własnym obywatelom — osobom samozatrudnionym i przedsiębiorcom — system zwany Elektroniczną ewidencją przychodów (EET). Przekaz był prosty: „Zakładamy, że każdy z was oszukuje państwo. Zapiszecie każdą pojedynczą transakcję, prześlecie ją w czasie rzeczywistym na nasze serwery, a my będziemy was obserwować. Finansowo wynagrodzimy waszych współobywateli za donoszenie na was, jeśli spróbujecie ominąć EET.”

EET wzorowano na precedensach bałkańskich. Pierwszym krajem na świecie, który uruchomił ogólnokrajowy obowiązkowy system rejestrowania sprzedaży online w czasie rzeczywistym, w 2013 roku, była Chorwacja, pod nazwą *fiskalizacija*. Czechy przyjęły ten model kilka lat później i prowadziły jeden z najsurowszych reżimów śledzenia przychodów w Europie.

Skoro ciemna strona się nie waha, dlaczego my mielibyśmy? ESR to ta sama logika odwrócona do góry nogami: to państwo udowadnia się przed obywatelami.

Obywatelska alokacja podatków — waga decyzji

Trzecie narzędzie daje podatnikom bezpośredni wpływ na to, dokąd płyną ich pieniądze. W pierwszej rundzie państwo otrzymywało swoje pieniądze niezależnie od tego, co ujawnił ESR. W drugiej rundzie

ESR — ELEKTRONICZNE RAPORTOWANIE WYDATKÓW

każdy wydatek państwa zapisany — każdy zapis publiczny — każdy szczegół otwarty na kontrolę.

kto zgłasza
każdy zapis
może zgłosić: —
urzędnik, który
przetworzył
płatność —
odbiorca, który
otrzymał
płatność



PUBLICZNY REJESTR WYDATKÓW PAŃSTWA — otwarty zapis

kategoria: doradztwo prawne
wykonawca: kancelaria prawna XYZ
s.r.o. kwota: 14 mln EUR zobowiązanie:
2026-01-14 wypłacono: 2026-01-19

kontekst: zewnętrzna opinia w sprawie nowej ustawy
o reformie zamówień publicznych — powstały trzy
wersje robocze, jeden warsztat z ministerstwem, nie
odbyło się publiczne wysłuchanie — ostateczna
wersja dostarczona po terminie legislacyjnym.

kategoria: doradztwo w zakresie
projektowania dróg wykonawca: COKU
Consultancy T kwota: 9 mln EUR
zobowiązanie: 2026-02-03 wypłacono: —
kontekst: studium wykonalności rozbudowy
autostrady D-X — ta sama firma napisała trzy
poprzednie studia na tej trasie — wynik: rekomendacja
realizacji przy +18% ponad wcześniejszy szacunek.

otwarte dla każdego,
kto chce zajrzeć.

kategoria: wydawanie tablic
rejestracyjnych odbiorca: urząd regionalny
Z kwota: 45 EUR za tablicę zobowiązanie:
2026-02-19 wypłacono: 2026-02-19

kontekst: standardowa opłata administracyjna za
wydaną tablicę — opłata pokrywa materiały i
obsługę — łączny wolumen 12 400 tablic w tym
kwartale.

kategoria: sprzęt szpitalny wykonawca:
MedSupply a.s. kwota: 8,2 mln EUR
zobowiązanie: 2026-03-08 wypłacono: —

kontekst: instalacja skanera MRI w szpitalu
regionalnym — przetarg publiczny, trzech
oferentów — wybrana oferta 2% poniżej mediany,
dostawa w ciągu 60 dni — faktura zaległa 90 dni.

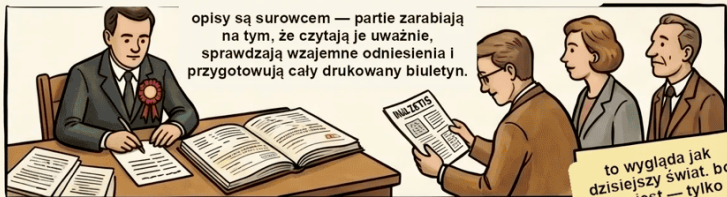


filtr antyspamowy — kaucja zwrotna



kaucja zwracana,
gdy zapis okaże
się dokładny.

partie przekształcają się w dostawców analiz



opisy są surowcem — partie zarabiają
na tym, że czytają je uważnie,
sprawdzają wzajemne odniesienia i
przygotowują cały drukowany biuletyn.

to wygląda jak
dzisiejszy świat. bo
nim jest — tylko
księgi są teraz otwarte
dla wszystkich. żadnej
rewolucji. po prostu
lepsze zachęty.

Każda korona publicznych pieniędzy — zapisana, publiczna, możliwa do skontrolowania.

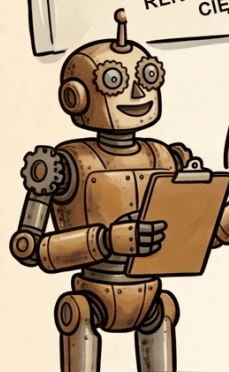
wartość nie polega na łapaniu oszustów — polega na otwarciu ksiąg.

już nie — przejmuję to analiza z pierwszej rundy i wynikające z niej środki. Niewielki procent zapłaconego podatku może zaalokować sam płatnik — pod warunkiem że jego DID spełnia wymogi reputacyjne (obywatelstwo, miejsce zamieszkania, uznana przez wspólnotę dorosłość/zdolność). Procent możliwy do zaalokowania rośnie rok do roku. Potencjalnie wykładniczo. Od pięciu procent dziś do dziesiątek procent w ciągu dekady.

Surowe dane ESR naturalnie kierują decyzjami podatników. Zapisy niskiej jakości funkcjonują jako sygnał ostrzegawczy o rekomendowanych cięciach. Każdy może tworzyć zapisy; urzędnicy muszą je dopasować. Bez tego system podatkowy nie prześle państwu żadnych pieniędzy — ani do skarbcza, ani do innych rozdziałów budżetowych. Bitwa polityczna przenosi się z urny wyborczej do codziennej alokacji konkretnych groszy.

ALOKACJA PODATKÓW OBYWATELSKICH — TY DECYDUJESZ, DOKĄD IDĄ TWOJE PODATKI

przeanalizuj zapisy ESR. potem przesun suwaki.



albo deleguj to

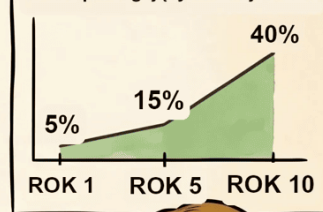
nie chcesz alokować
samodzielnie? deleguj
do: — analityka twojej
partii — zaufanego
sąsiada — kogokolwiek
wybierzesz — i odwołaj
w każdej chwili.



po
przeanalizowaniu
raportu —
obrona w
dół.



udział podlegający alokacji rośnie



kliknij dowolny
wiersz, aby
zagłębić się —
alokuj na
dowolnym
poziomie.



to wygląda jak
dzisiejszy świat. bo
nim jest — tylko
suwak jest teraz w
twoich rękach.
żadnej rewolucji. po
prostu lepsze
zachęty.

**Od 5% dziś do 40% za dekadę. Ty decydujesz.
zapisy są otwarte. analiza jest twoja. suwak też.**

Platforma negocjacyjna z państwem — dźwignia

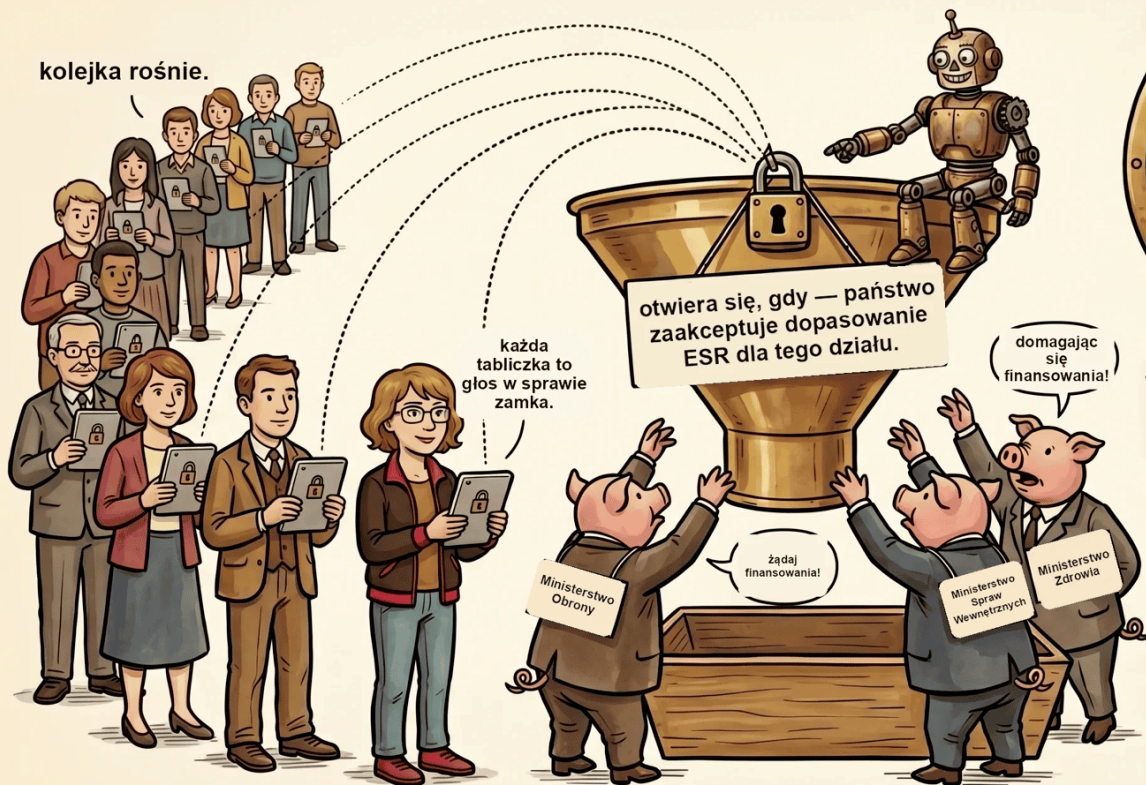
Czwarte narzędzie jest dźwignią, która wiąże wszystko razem i dopiero teraz czyni sieć realnym zagrożeniem. Główny konflikt będzie o to, czy państwo przyjmie ESR jako wiążący standard — najpierw na poziomie krajowym — i jak duże muszą stać się groźby ze strony uczestników sieci reputacji, zanim to nastąpi.

Dźwignią jest finansowanie państwa dokładnie na czas (just-in-time), uwarunkowane dopasowaniem płatności do ESR. Pieniądze płyną tylko w chwili, gdy państwo spełniło warunki przejrzystości. Wewnątrz sieci reputacji tworzy się lista oczekujących uczestników. Aktywacja wchodzi w grę, gdy grupa osiąga ekonomicznie znaczący rozmiar — na tyle duży, by zagrozić wzrostowi PKB. W tym momencie obywatelskie nieposłuszeństwo staje się wiarygodną groźbą, a nie gestem.

Państwo będzie najdłużej trzymać się problematycznych płatności powiązanych z korupcją. Pod presją ustąpi najpierw tam, gdzie ma łatwą obronę i gdzie nie ma pola na szukanie oszczędności. Stopniowa i rosnąca presja zmusi je do wycofywania się, krok po kroku, z każdej pozycji.

PLATFORMA NEGOCJACYJNA — ZAMKNIĘTY ZASOBNIK

obywatele trzymają klucz. państwo otwiera się, gdy warunki zostaną spełnione.



wystarczy niewielki ułamek PKB — przy masie krytycznej wstrzymanie środków staje się realną groźbą.

- po osiągnięciu masy krytycznej —
- państwo najpierw otwiera księgi dla prostych, uzasadnionych płatności.
- kategorie powiązane z korupcją pozostają zamknięte najdłużej.
- każde odblokowanie wymaga większej presji — i samo jest rejestrowane.

Pieniądze płyną, gdy jest przejrzystość. Obywatele trzymają klucz.

żadnej siły. żadnej rewolucji. wystarczy tyle tabliczek, by wstrzymanie stało się wiarygodne.

to wygląda jak dzisiejszy świat. bo nim jest — tylko klucz jest teraz w wielu rękach. żadnej rewolucji. po prostu lepsze zachęty.

Obywatelstwo bez dowodu osobistego

Wraz z przejściem na infrastrukturę DID wydawany przez państwo dowód osobisty traci swój monopolistyczny cel. Nie potrzebujesz dowodu osobistego — masz szereg tożsamości DID, a niektóre z nich niosą tezę, że jesteś na przykład Czechem, mieszkańcem danej gminy, absolwentem danej szkoły. Teza jest weryfikowalna, trwała i niezależna od administracji państwowej.

Otwiera się pytanie o techniczną implementację: kto na rynku podejmie się weryfikacji istniejących obywateli poza kontrolą państwa, by migrować zainteresowanych do DID niosącego odpowiednią tezę? Najprawdopodobniej pojawią się wolnorynkowe autorytety wyspecjalizowane w weryfikacji tożsamości — notariusze, lokalne wspólnoty, pracodawcy. Stawiają swoją reputację na tym, że dany DID naprawdę należy do osoby, która to o sobie twierdzi. Obywatelstwo — czyli przynależność do określonego spojrzenia na wspólnotę — zostaje uwolnione od potrzeby centralnej ewidencji. Poprzez połączenie w sieci reputacji osadzone dane są łączone i walidowane po raz drugi, trzeci, czwarty i tak dalej.

Konsekwencja jest intuicyjna, a zarazem nierozwiązywalna w systemie scentralizowanym. Dziś przywództwo polityczne — z myślą o łatwiejszej reelekcji — może importować skoncentrowane problemy na terytorium wspólnoty: przyjmować migrantów z innych kręgów cywilizacyjnych niezależnie od zdolności absorpcyjnej i gotowości istniejącej wspólnoty, przekształcając pierwotne wspólnoty pod presją, pod którą nie nadążają z asymilacją przybyszów z innych kręgów cywilizacyjnych. W sieci DID skorumpowanie przyjęty migrant nie może być pewien, że wspólnota nadal będzie traktować go jako swojego. Członkowie wspólnoty obiektywnie nie muszą znosić obcego, który przychodzi do ich drzwi w mundurze wspólnoty i grozi im legalnością środków, które zamierza wykonać w domu (konfiskata telefonu dziecka za post w mediach społecznościowych). Ze zdecentralizowaną reputacją większość społeczeństwa nie musi się z tym godzić — bo o przynależności do wspólnoty nie decyduje urzędnik, lecz sama wspólnota, poprzez swoje sygnały reputacyjne.

CZTERY NARZĘDZIA EWOLUCYJNEJ TRANSFORMACJI

system przebudowany od wewnątrz — bez jego rozbijania.

PROSTY PODATEK



jedna stawka. bez ulg.
możliwa do weryfikacji
krzyżowej.

ESR — ELEKTRONICZNE RAPORTOWANIE WYDATKÓW



każdy wydatek zapisany
— każdy zapis publiczny
— każdy szczegół otwarty.

ALOKACJA PODATKÓW OBYWATELSKICH

5% → 15% → 40%
ROK 1 → ROK 5 → ROK 10



przeanalizuj zapisy —
potem przesun suwaki.

PLATFORMA NEGOCJACYJNA



pieniądze płyną tylko
wtedy, gdy spełnione są
warunki przejrzystości.

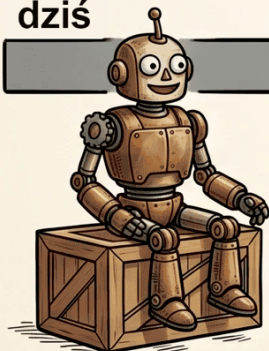
dziś

ewolucja w toku

za dekadę

95%

rozszerza się



Ewolucja, nie rewolucja.

cztery narzędzia, które zmieniają system od wewnątrz.

to wygląda jak dzisiaj.
jest — tylko narzędzia
są teraz w rękach
obywateli. żadnej
rewolucji. po prostu
lepsze zachęty.



OBYWATELSTWO BEZ DOWODU OSOBISTEGO

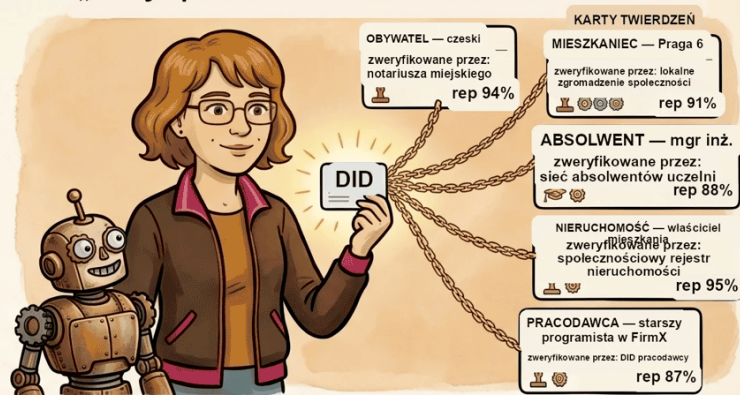
od pozwolenia państwa do uznania społeczności.

„stary sposób” — model instytucjonalnego dowodu wydawanego przez państwo



tożsamość = pozwolenie państwa — odwoływalne — społeczność nie ma głosu.

„nowy sposób” — model DID z kartami twierdzeń



żaden pojedynczy autorytet nie kontroluje wszystkich twierdzeń — każde jest niezależne — każdy weryfikator stawia na szali swoją reputację.

„kto należy?”



polityk decyduje — społeczność nie ma głosu.



społeczność decyduje — poprzez sygnały reputacji — rozproszone, bez jednego głosu.

to wygląda jak dzisiejszy świat. bo nim jest — tylko weryfikatorów jest teraz wielu. żadnej rewolucji. po prostu lepsze zachęty.

Twoje obywatelstwo to nie pozwolenie rządu. To uznanie twojej społeczności.

pieczętkę państwa zastępuje łańcuch niezależnych weryfikatorów — każdy z własnym ryzykiem.

Waga głosu wyborczego w sprawach należących do domeny państwa mogłaby w przyszłości być ściśle skorelowana z zapisami wkładów do prostego systemu podatkowego. W połączeniu z odpowiednimi tezami DID (na przykład „ta osoba jest obywatelem Czech”) można wtedy wykluczyć z wyborów cudzoziemców — rejestr ludności po prostu przenosi się tutaj.

Nakładanie się i odwracalność

Nie twierdzę, że to jedyna droga ani nawet najlepsza. Ale wydaje się kompleksowa — obejmuje główne dźwignie i zachowuje możliwość cofnięcia się. Na starcie nowy system nakłada się na stary i zmienia jedynie bodźce. Z czasem stary system kurczy się, aż może — ale nie musi — się rozpuścić. Zaletą jest stopniowość i odwracalność: gdyby w projekcie pojawił się błąd, nie jest to koniec, tylko korekta.

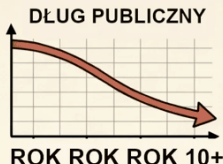
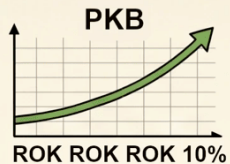
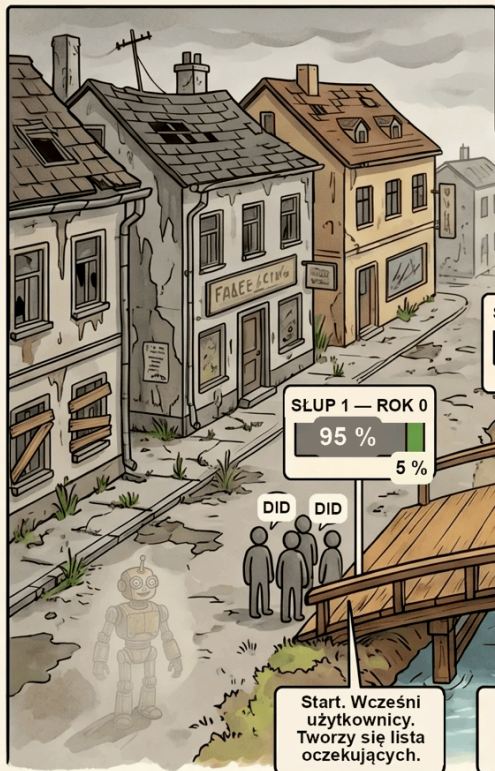
Pokój i wojna

Niektóre części państwa mogą nie mieć w pełni rynkowej alternatywy — być może wojsko. Tymczasowe delegowanie nadzwyczajnych uprawnień w kryzysach (jak starożytni Grecy powoływali dyktatorów) mogłoby nadal istnieć. Odpowiedzialność jednak spoczywa na zdecentralizowanym społeczeństwie, nie na przywódcy. W przeciwieństwie do rządów scentralizowanych łatwiej będzie odzyskać delegowane uprawnienia, gdy zagrożenie minie — albo wcześniej, gdy zajdzie taka potrzeba. Wolne społeczeństwo nie będzie w niekorzystnej sytuacji nawet w starciu zbrojnym z reżimami autorytarnymi.

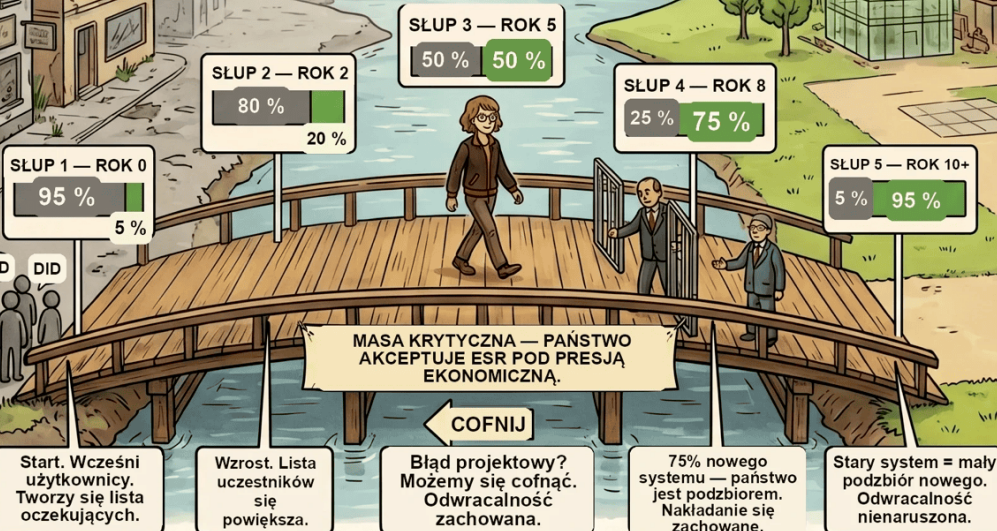
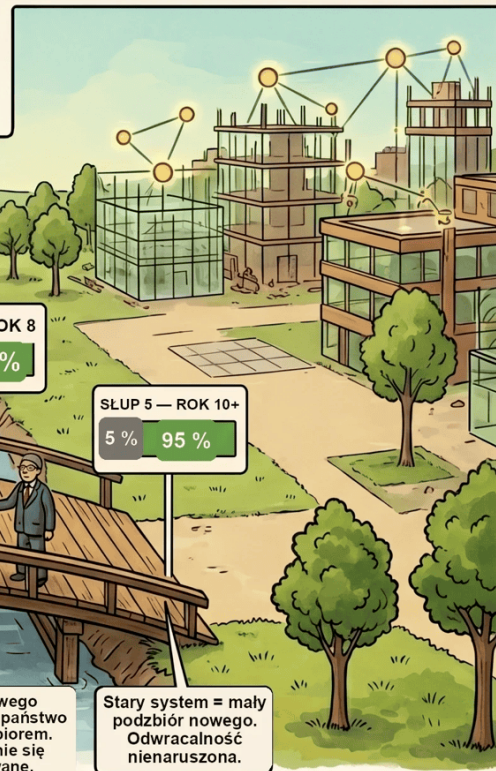
Zbrodniarze wojenni

Przy finansowaniu państwa dokładnie na czas i przejrzystych wydatkach trudno jest zgromadzić zasoby na wojny agresywne. Podatnik, który nadal finansuje taką wojnę, staje się legalnym celem i nie może powoływać się na status cywilny na mocy konwencji genewskich. W nowym układzie milczącą zgodę traktuje się jako udział.

LEWY BRZEG — „STARY SYSTEM”



PRAWY BRZEG — „NOWY SYSTEM”



STARY SYSTEM

> Stopniowe przejście. Odwracalność w razie błędu. Kierunek, którego nie da się zatrzymać.

Zakończenie

Droga istnieje

Państwo jest takie, jakie jest, z powodu technologii dostępnych w czasie jego powstania, w połączeniu z ludzką naturą. Budowanie wszystkiego na dobrowolności przy jednoczesnym zaprzeczaniu przeciętnej ludzkiej naturze jest naiwne. Nie pozbędzie się ono korupcji ani skłonności do dryfowania ku totalitaryzmowi. Następca państwa musi działać nawet z cechami, które obecnie uznajemy za negatywne i albo je ostracyzujemy, albo karzemy.

Ta książka opisała problem — system (państwo), w którym ludzie piszący reguły nigdy nie żyją z ich konsekwencjami. Opisała warunki, które muszą zajść, by ten system przestał działać. Opisała narzędzie, które te warunki spełnia. I zaproponowała metodykę przejścia — konkretne kroki, jak to narzędzie wykorzystać, jako jeden z możliwych przykładów.

W pierwszym rozdziale wymieniałem pięć filarów: dobrowolność, organizację, odporność, konsensus i nieprzekupność. Spełniliśmy je wszystkie.

- **Dobrowolność** — nikt nie zmusza cię do wejścia do sieci, ale nie możesz też wymazać z niej swoich czynów.
- **Organizacja** — wspólnota wyrasta z tego, kogo znasz, a nie z tego, kogo ci przydzielono z góry.
- **Odporność** — nawet państwo gotowe płacić za inwigilowanie każdego pakietu nie może jej wyłączyć.
- **Konsensus** — rodzi się z metki cenowej na obłudę, a nie z głosów czy podpisów.

- **Nieprzekupność** — pięć małych reguł wplata korupcję w koszty: równowaga dobrowolności i odpowiedzialności, prawo każdego do głosu, punkty wejścia, których nikt sobie nie wybiera, publiczne obietnice z ceną za obłudę i cień obserwatora za każdą transakcją.

Żaden pojedynczy filar nie zastąpi państwa sam. Razem tworzą opór wobec korupcji, jakiego państwo, z całym swoim aparatem, nie potrafi.

Jesteśmy w punkcie, w którym całość da się zbudować za pomocą dzisiejszych technologii (kryptografia, tożsamość zdecentralizowana, dobrze znane wzorce psychologiczne pozwalające właściwie ustawić bodźce...). Brakuje tylko jednego: masy krytycznej ludzi, którzy znajdą odwagę, by to wesprzeć, i zdecydują się zacząć.

Nie przez rewolucję.

Idee te nabierały kształtu między czerwcem 2025 a majem 2026. Zanim usiadłem do pisania, miałem już ramy w dużej mierze poukładane w głowie — właśnie dlatego z taką ciekawością przeczytałem [Farewell To Westphalia](#), gdy się ukazało. Chciałem zobaczyć, gdzie ich obraz pokryje się z moim, a gdzie się rozejdzie. Drugi impuls przyszedł od Dana Steigerwalda, który w maju 2026 wciąż pracuje nad własną książką *Dekonstrukcja państwa* z innego kąta; jego projekt popchnął mnie, by przedstawić własną wizję w pełnej szerokości — tak by świat miał ją na stole obok pozostałych.

Nie proszę cię, byś w cokolwiek z tego wierzył. Proszę cię, byś się nad tym zastanowił. I zostawiam cię z jednym pytaniem:

Co byś zmienił?

Pavel Kudrna 23 maja 2026, Praga, Czechy

Podziękowania

Inspiracja

Dziękuję autorom [Farewell to Westphalia](#) (Jarrad Hope, Peter Ludlow) za intelektualne ramy, które pomogły mi umieścić własne idee w szerszym kontekście dekonstrukcji westfalskiego modelu państwa.

Recenzja i informacja zwrotna

Narzędzia

Przygotowując tekst, porządkując idee i iterując nad sformułowaniami, korzystałem ze wsparcia narzędzi AI. Wszystkie idee, argumenty i wnioski są moje własne — AI służyła jako narzędzie dopracowania, nie jako współautor treści.

Infografiki zaprojektowano we współpracy z narzędziami generatywnymi na podstawie specyfikacji autora.

ODZYSKAJ SWÓJ CZAS

obywatele wypędzają pasożytów z życia publicznego.



Broń czasu, który chcieliby ukraść. co zabrano podstępem, odbiera się własnymi rękami.

Wesprzyj projekt

Personix jest finansowany przez czytelników takich jak ty.



Bitcoin on-chain

bc1q7ccdtz6r026dgy06ul94eygg49ujtxnrq5czaj



Bitcoin Lightning

LNURL1DP68GURN8GHJ7AMPD3KX2AR0VEEKZ
AR0WD5XJTNRDAKJ7TNHV4KXCCTTDEHHWM30
D3H82UNVWQHXMNP0FA8JMTPTVD5XJMN9XUE
RX55QRQK

Dokąd trafiają te pieniądze — a dokąd nie

Kody QR to **osobiste kanały autora** — wpłaty trafiają bezpośrednio do Pavla Kudrny i finansują dalsze pisanie, eksperyment / symulację społeczną oraz działania informacyjne.

Jedyne legalne kanały zbiórki na ten projekt to:

- **Autorskie wydania tej książki** — kody QR w egzemplarzach autoryzowanych przez autora.
- personix.org lub podlinkowane stamtąd lustro Tor onion — gdzie *Fundacja Personix* zbiera na opisane tam działania. Środki fundacji są trzymane oddzielnie od prywatnych środków autora.

Wszystko, co reklamowane gdziekolwiek indziej — podmienione adresy w dodrukach, łudząco podobne domeny, „zbiórki na Personix” w mediach społecznościowych, zbiórki niepowiązane z żadnym z powyższych — **to najprawdopodobniej oszustwo**. Celowo unikamy rynku kryptowalut i jego uczestników.

Słownik pojęć

Słownik pojęć

Pojęcie	Polski	Znaczenie
Authority	Autorytet	Zaufany podmiot (osoba, organizacja), który weryfikuje informacje i stawia na nie swoją reputację. Może być wyspecjalizowany (śledczy, prawny, techniczny).
Claim	Teza	Ogólnie: dowolne weryfikowalne stwierdzenie. Tutaj: zapis opublikowany w sieci reputacji — twierdzenie o zdarzeniu, właściwości lub relacji, kryptograficznie podpisane i zweryfikowane. Np. „jestem mieszkańcem gminy X” albo „ta osoba naruszyła umowę”.

Pojęcie	Polski	Znaczenie
Compartmentalization	Kompartmentalizacja	Ogólnie: oddzielanie informacji na izolowane jednostki tak, by ujawnienie jednej jednostki nie skompromitowało pozostałych. Zasada znana ze służb wywiadowczych. Tutaj: równoległe tożsamości DID w dyktaturach — skompromitowanie jednej nie ujawnia pozostałych.
Consistent Hash Ring	Pierścień haszujący	Algorytmiczny mechanizm wyboru weryfikatorów — pozycję na pierścieniu wyznacza hash dokumentu DID w obrębie grafu społecznego. Zapewnia niedeterministyczny, a zarazem weryfikowalny wybór.
DID	DID (Tożsamość zdecentralizowana)	Cyfrowa tożsamość, którą tworzysz i kontrolujesz sam, bez centralnej władzy. Kryptograficznie podpisana twoim kluczem prywatnym — nikt nie może jej cofnąć ani podrobić.

Pojęcie	Polski	Znaczenie
DID Document	Dokument DID	Publicznie dostępny plik danych opisujący twoją tożsamość DID — zawiera klucze publiczne, adresy sieciowe i metadane. Służy do weryfikacji twojej tożsamości w sieci.
Due Diligence	Due diligence	Ogólnie: dogłębna weryfikacja drugiej strony przed wejściem w relację biznesową lub prawną — sprawdzenie jej historii, finansów, reputacji i ryzyk. Tutaj: w sieci reputacji odbywa się szybciej i bardziej automatycznie dzięki dostępności zweryfikowanych zapisów.
Economic Neutrality Principle	Zasada neutralności ekonomicznej	Uczciwe zachowanie w sieci jest ekonomicznie bliskie zeru — koszty publikacji zwracają się jako nagrody za weryfikację. Nieuczciwe zachowanie jest czystą stratą.

Pojęcie	Polski	Znaczenie
Emergent	Emergentny	Spontanicznie powstający z interakcji prostszych części, bez niczyjego projektu ani sterowania. Klucz ptaków leci w formacji bez planu — formacja wyłania się z prostych reguł, których przestrzega każdy osobnik.
Emergent Social Contract	Emergentna umowa społeczna	Reguły zachowania powstające nie z góry (prawo), lecz z dołu — z powtarzanych interakcji i konsensusu wewnątrz wspólnoty.
ESR	Elektroniczny rejestr wydatków	Proponowany system przejrzystego śledzenia wydatków publicznych — każdy zrealizowany wydatek państwa jest dopasowany do planowanej płatności. Zainspirowany czeskim EET, ale odwrócony przeciw państwu.

Pojęcie	Polski	Znaczenie
Hash	Hash (odcisk)	Ogólnie: jednokierunkowa funkcja matematyczna, która z dowolnego wejścia wytwarza unikalny „odcisk” o stałej długości — jak odcisk palca dokumentu. To samo wejście zawsze daje to samo wyjście, ale z wyjścia nie da się wyprowadzić wejścia. Tutaj: używany do wyznaczenia pozycji na pierścieniu haszującym i do weryfikacji integralności dokumentu.
Just-in-Time Funding	Finansowanie just-in-time	Finansowanie państwa uwarunkowane przejrzystością — pieniądze płyną tylko wtedy, gdy państwo przyjmuje ESR i dopasowuje swoje wydatki. Dźwignia zmuszająca do współpracy.

Pojęcie	Polski	Znaczenie
Meritocracy	Merytokracja	Ogólnie: system, w którym pozycję wyznaczają faktyczne zasługi i udowodnione umiejętności, a nie formalne tytuły, koneksje czy odziedziczony przywilej. Tutaj: sieć reputacji naturalnie faworyzuje tych, którzy w dowodliwy sposób wnoszą wkład do wspólnoty — ich głos ma większą wagę dzięki track recordowi, a nie urzędowi.
Onion Gateway	Onion gateway	Adres sieciowy tożsamości DID w sieci onion. Oddzielny od dokumentu DID — można go zmienić bez utraty tożsamości (podobnie jak zmiana adresu IP za domeną).
Onion Routing	Onion routing (Tor)	Protokół komunikacyjny zapewniający niecenzurowalność sieci. Wiadomości są szyfrowane warstwami — każdy węzeł zdejmuje jedną warstwę, ale nie zna pełnej trasy.

Pojęcie	Polski	Znaczenie
Oracle Problem	Problem wyroczni	Ogólnie: jak zapewnić, by dane wchodzące do systemu cyfrowego wiernie odpowiadały temu, co faktycznie wydarzyło się w świecie fizycznym. Termin pochodzi z domeny blockchaina. Tutaj: rozwiązywany poprzez autorytety, które stawiają swoją reputację jako gwarancję, że zapis cyfrowy odpowiada rzeczywistości fizycznej.
Phenomenological	Fenomenologiczny	Ogólnie: podejście badające zjawiska tak, jak przejawiają się w bezpośrednim doświadczeniu, poprzez obserwację tego, co z nich wynika, bez z góry danych teorii. Tutaj: wolność, umowa społeczna i normy zachowania są obserwowanymi zjawiskami — konsekwencjami tysięcy mikrointerakcji między ludźmi, a nie zasadami definiowanymi z góry.

Pojęcie	Polski	Znaczenie
Policy	Policy (polityka)	Ogólnie: zbiór reguł lub zasad rządzących zachowaniem w danym kontekście. Tutaj: każdy uczestnik sieci DID deklaruje swoją politykę — jak reaguje na konkretne zachowania innych, których reguł przestrzega i które kary uznaje za proporcjonalne. Suma polityk tworzy emergentną umowę społeczną.
Proxy	Proxy	Ogólnie: zastępca lub pośrednik — system lub podmiot działający w imieniu innego. Używane tu w dwóch kontekstach: (1) ESR jako proxy dopasowujące wydatki publiczne do planowanych płatności; (2) obserwatorzy jako proxy między wydawcą a weryfikatorem w triku z obserwatorem.
Publisher	Wydawca	Uczestnik sieci, który tworzy i publikuje zapis (tezę o niesprawiedliwości, naprawie itd.). Ponosi koszt publikacji.

Pojęcie	Polski	Znaczenie
Reputation-Based Social Network (RSN)	Sieć reputacji	Zdecentralizowana sieć społecznościowa, w której uczestnicy wymieniają informacje zwrotną o zachowaniu w świecie rzeczywistym. Zapisy są kosztowne do utworzenia, tanie do przeczytania.
Reputation Signal	Sygnał reputacyjny	Pojedynczy zapis w sieci — pozytywny (naprawa krzywdy, wypełnienie zobowiązania) lub negatywny (niesprawiedliwość, naruszenie umowy). Kumulatywnie sygnały tworzą profil reputacyjny.
Social Graph	Graf społeczny	Sieć twoich kontaktów i kontaktów twoich kontaktów. Algorytm szuka weryfikatorów na konfigurowalnej głębokości (na przykład 3 poziomy). Brak globalnego blockchaina — sieć naturalnie tworzy wspólnoty z zazębieniami.

Pojęcie	Polski	Znaczenie
Tax Allocation	Alokacja podatków	Mechanizm, dzięki któremu podatnik decyduje, dokąd trafia część jego podatków. Procent możliwy do zaalokowania rośnie rok do roku.
Track Record	Track record	Ogólnie: historia dotychczasowych wyników, sukcesów i porażek osoby lub organizacji. Tutaj: suma wszystkich dotychczasowych interakcji danej tożsamości DID w sieci — zweryfikowanych tez, przyjętych i odrzuconych zapisów — z których wywodzi się jej reputacja.
Verifier	Weryfikator	Uczestnik wybrany algorytmicznie do zweryfikowania i opublikowania zapisu. Stawia swoje dobre imię na prawdziwości informacji.

Nota produkcyjna

Zastrzeżone przez autora (nieobjęte licencją CC BY-SA): nazwa i znak słowny Personix, okładka książki oraz kanały wsparcia (kody QR, adresy, kontaktowy adres e-mail). Wydania pochodne muszą usunąć lub zastąpić te elementy. Wolno ich użyć wyłącznie w celu odesłania do tego oryginalnego dzieła.

Pliki źródłowe. Kompletne źródło — tekst w markdownie, infografiki, skrypty budujące — jest dostępne wraz z tym plikiem PDF.

Narzędzia. Przygotowując tekst i dopracowując sformułowania, autor korzystał ze wsparcia narzędzi AI, a infografiki zaprojektowano we współpracy z narzędziami generatywnymi na podstawie specyfikacji autora. Wszystkie idee, argumenty i wnioski należą do autora.

PERSONIX

Bezkompromisowa zmiana

Niecenzurowalna i nieprzekupna zdecentralizowana sieć reputacji

Państwo sprawdzało się, gdy komunikacja była powolna, decyzje zapadały lokalnie, a władza mieszkała w tym samym mieście, którym rządziła. Dzisiejsze sieci odwracają wszystkie trzy założenia — a instytucje na nich zbudowane nie pasują już do świata, którym rządzą. Ta książka opisuje narzędzie, które pasuje: zdecentralizowaną sieć reputacji, w której tożsamość zostaje twoja, prawda jest publicznie sprawdzalna, a przekupstwo to reputacyjne samobójstwo.

To nie manifest. To nie prognoza. To działający plan budowy następcy państwa — dobrowolnie, jedna deklaracja po drugiej.

Pavel Kudrna • Praga, 2026

personix.org

Udostępniono na licencji Creative Commons Attribution-ShareAlike 4.0 International (CC BY-SA 4.0).