



SGH

Szkoła Główna
Handlowa
w Warszawie

II Kongres Informatyka dla Ludzi Lasu
Rogów, 8 września 2022 r.

Blockchain

Dr Grzegorz Sobiecki
Szkoła Główna Handlowa w Warszawie





O mnie



Dr Grzegorz Sobiecki

- doktor nauk ekonomicznych (ekonomia, finanse, zarządzanie, blockchain)
- blockchain i kryptowaluty **od 2011 roku**
- kierownik **studiów podyplomowych „Blockchain: biznes, prawo, technologia”**
- prezes i współzałożyciel **Stowarzyszenia Ekspertów Blockchain (SXB)**
- **konsultant** w projektach biznesowych (DLT w systemie płatniczym, Billon)
- publikacje & wystąpienia: blockchain, kryptoaktywa, DeFi, DAO, CBDC, NFT
- kierownik B+R projektu platformy emisji i obrotu tokenami w Polsce (2021)
- grant NCN (OPUS) z prof. W. Srokoszem (DLT i kapitałochłonne inwestycje)
- promotor pomocniczy doktoratu dr Antona Bubiela, opiekun 5 doktorantów
- ekspert: NCBIR, PARP, analizy finansowe
- biegły ad hoc Prokuratury
- członek strumienia “Blockchain / DLT i cyfrowe waluty”

Agenda

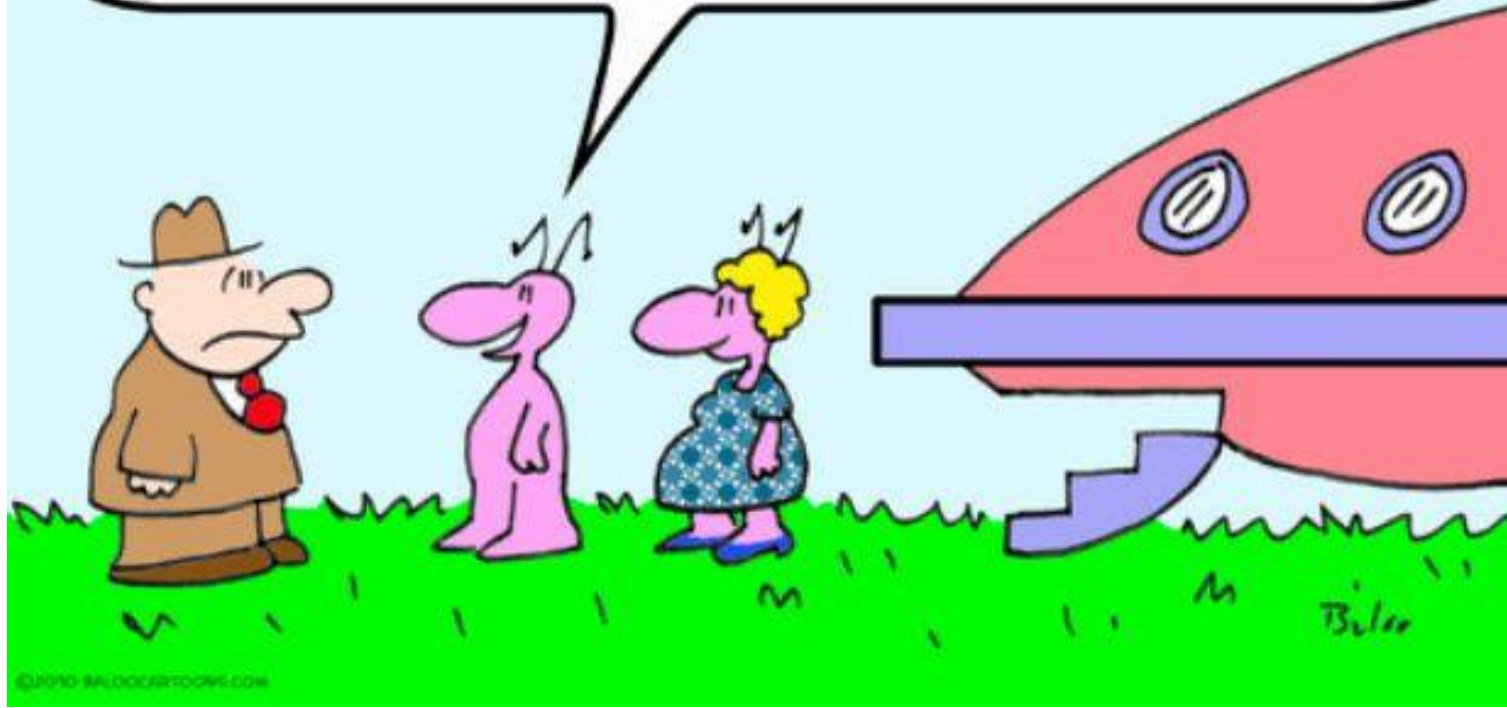
1. **Czym jest** blockchain (DLT), inteligentne kontrakty?
2. Jakie są **rodzaje blockchaina**?
3. Z czego wynika fenomen i wartość blockchaina, tokenów?
4. Jakie są główne **zastosowania blockchaina**?
5. **Blockchain dla lasu**?



BLOCKCHAIN

Istota łańcucha bloków

WE HAVE COME FOR YOUR
BLOCKCHAIN TECHNOLOGY



Blockchain to rozwiązanie integrujące kilka koncepcji

1

struktura danych

2

zdecentralizowana sieć p2p

3

mechanizm konsensusu

4

mechanizm identyfikacji i uwierzytelniania

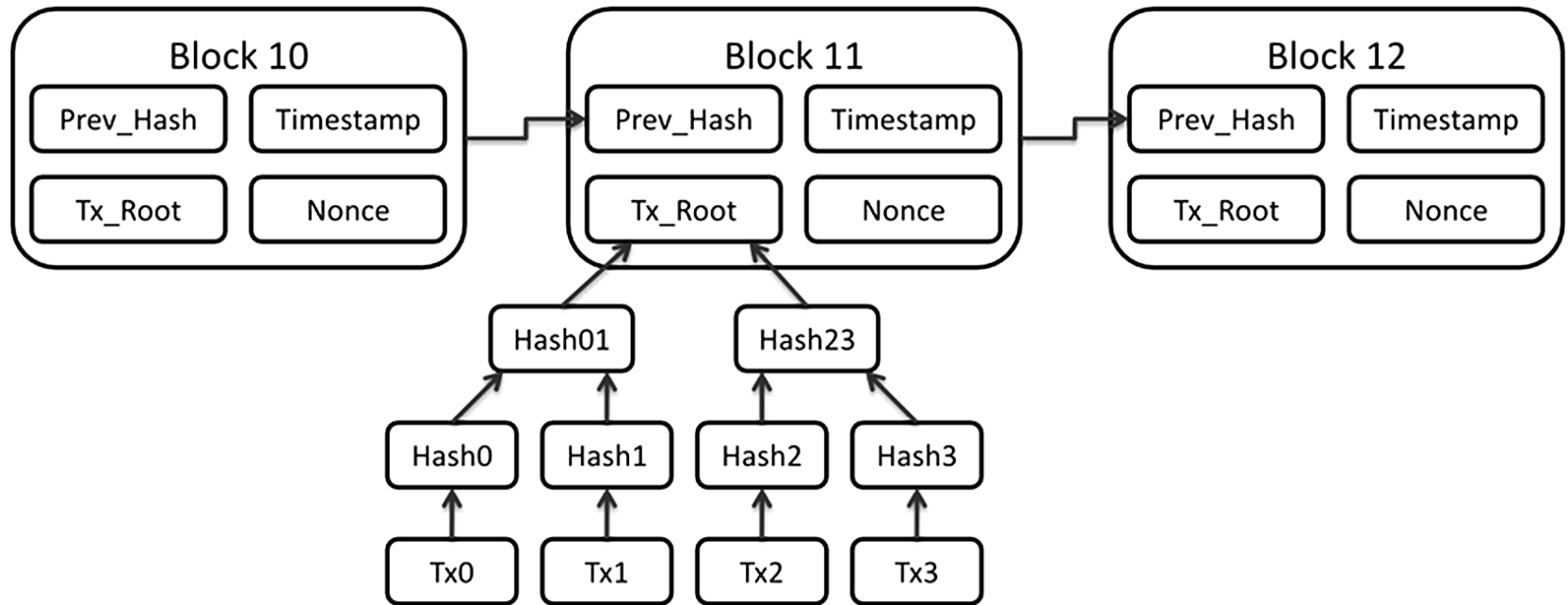
5

mechanizm incentywizacji

6

wirtualna maszyna (zdecentralizowana)

łańcuch bloków (nagłówki bloków)



- Tx: transakcja
- Prev_Hash: skrót poprzedniego nagłówka bloku danych
- Tx_Root: „korzeń” drzewa skrótów transakcji
- Timestamp: znacznik czasowy
- Nonce: inne dane (w Bitcoinie: pewna liczba o szczególnym znaczeniu)

[2] Sieć P2P

- Sieć można budować na wielu poziomach stosu technologicznego
- W blockchainie
 - sieć wirtualna (nie fizyczna)
 - sieć blockchain osadzona na istniejącej sieci fizycznej (hardware: kablowej i bezprzewodowej)
 - węzłami sieci są aplikacje (w tym firmware)
 - sieć **P2P**: węzły dostępne bezpośrednio dla innych
 - sieć rozproszona geograficznie
 - sieć **zdecentralizowana (rozproszona w sensie Barana)**
 - sieć tworzą węzły suwerenne postępujące wg określonego protokołu sieci blockchain

Rodzaje sieci blockchain wg uprawnień

		Uprawnienia użytkownika (odczytu, zlecenia transakcji)	
		KAŻDY*	OGRANICZONE
Uprawnienia infrastrukturalne (zapis, walidowanie transakcji, weryfikacja, relay)	PERMISSIONLESS (każdy)	Bitcoin, Ethereum	Monet, Holochain
	PERMISSIONED (ograniczone)	Ripple, Enterprise Ethereum, EOS	Hyperledger Fabric

*) występują określenia: prywatny / publiczny, otwarty / zamkniętym ale czasem są sprzecznie używane!

[3] mechanizm konsensusu

- Opisany w ramach protokołu sieci
- Mechanizm synchronizacji węzłów w warunkach
 - ciągłego napływu danych
 - niezależności decyzji węzłów
 - braku centralnego koordynatora
- Powszechna zasada realizacji
 - co pewien czas **jeden** węzeł dopisuje nowe dane, pozostałe akceptują
 - różne mechanizmy konsensusu \leftrightarrow zasady wyboru węzła zapisującego
- Korzyści
 - Niezaprzeczalność
 - Niezmiennność (trwałość) zapisu danych i historii
 - Demokratyzacja sieci

[4] mechanizm identyfikacji i uwierzytelniania

- W ramach protokołu
- Użytkownicy usług sieci blockchain są identyfikowani wg **adresu** sieci
- W usłudze rejestru stanów posiadania (np. Bitcoin) do adresu przypisane są środki (tokeny)
- Adres jest elementem mechanizmu **uwierzytelniania** użytkowników usługi wykorzystującej blockchain
- Korzyści
 - bezpieczeństwo (uwierzytelnienie)
 - integracja poziomu usługi i infrastruktury
- Analogia: jakby numer konta bankowego
 - Identyfikował docelowy rachunek do którego przypisane są środki
 - identyfikował posiadacza środków
 - był elementem procesu uwierzytelniania posiadacza

[5] mechanizm incentywizacji

- suwerenne węzły zużywają zasoby
- aby sieć przetrwała niezbędne są korzyści dla interesariuszy
- warunek: realna ekonomiczna wartość ich korzyści
- w sieciach otwartych, publicznych: **węzły dopisujące kolejny blok (walidatorzy, górniczy) otrzymują**
 - nagrodę (tokeny danej sieci) wg polityki
 - opłaty transakcyjne
- w sieciach zamkniętych, prywatnych
 - rozliczenia wewnętrzne lub korzyści niematerialne
- korzyści
 - kapitalizm rynkowy

[6] Inteligentny kontrakt uruchamiany na wirtualnej zdecentralizowanej maszynie

- Komputerowy protokół / aplikacja, który sprawdza i egzekwuje wykonanie umowy
- To umowy, których warunki są rejestrowane w języku komputerowym zamiast w języku prawnym
- Umożliwiają realizację wiarygodnych transakcji bez osób trzecich.
- Uzupełniły i rozszerzyły funkcjonalność blockchainów kryptowalut, m.in. o budowanie aplikacji umieszczanych i uruchamianych w rozproszonym środowisku *wirtualnych maszyn* (tzw. Dapps)
 - Distributed Virtual Machine (DVM) łączy logikę z rejestrem by osiągnąć rozproszoną automatyzację procesów biznesowych

Możliwości i ograniczenia IK

- Program komputerowy
 - Zapisany w łańcuchu bloków
 - Uruchamiany jednakowo przez węzły sieci
 - Działający w maszynie wirtualnej
 - Do działania wymaga tokena danego łańcucha
- Może wywoływać inne kontrakty
- Może wysyłać token danego łańcucha

Czego nie mogą smartkontrakty

- (Samodzielnie zainicjowany) dostęp do danych poza macierzystym blockchainem
=> wyrocznie
- Samodzielne uruchomienie – każde działanie wymaga transakcji skierowanej na funkcję smartkontraktu (kod nie „wywołuje się sam”)
- Modyfikować swojego kodu
- Problem liczb losowych

Wyrocznie (oracles)

- Bardziej złożone IK szczególnie w otwartych blockchainach publicznych, które działają na blockchain, np. takie, które *„tworzą faktury, które same się opłacają, gdy przychodzi przesyłka lub świadectwa udziałowe, które automatycznie wysyłają właścicielom dywidendy, jeśli zyski osiągną określony poziom.”* wymagają poza-łańcuchowej **wyroczni (oracle)**, aby uzyskać dostęp do „zewnętrznych danych lub zdarzeń”
- Wyrocznie łączą kontrakty ze światem realnym i dostarczają biznesowi wartości
- Wyrocznie inicjują dostarczanie danych (kontrakty nie działają „same” i nie pobierają danych samodzielnie)

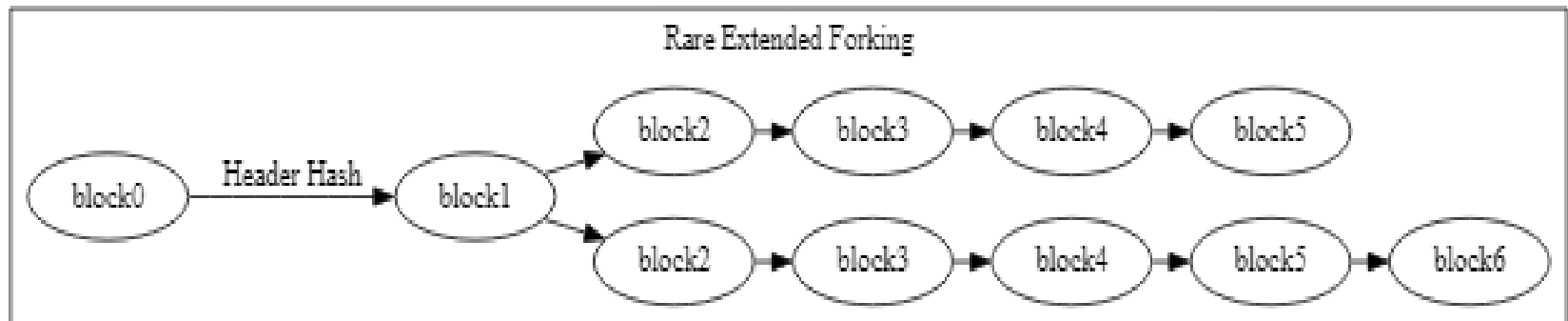
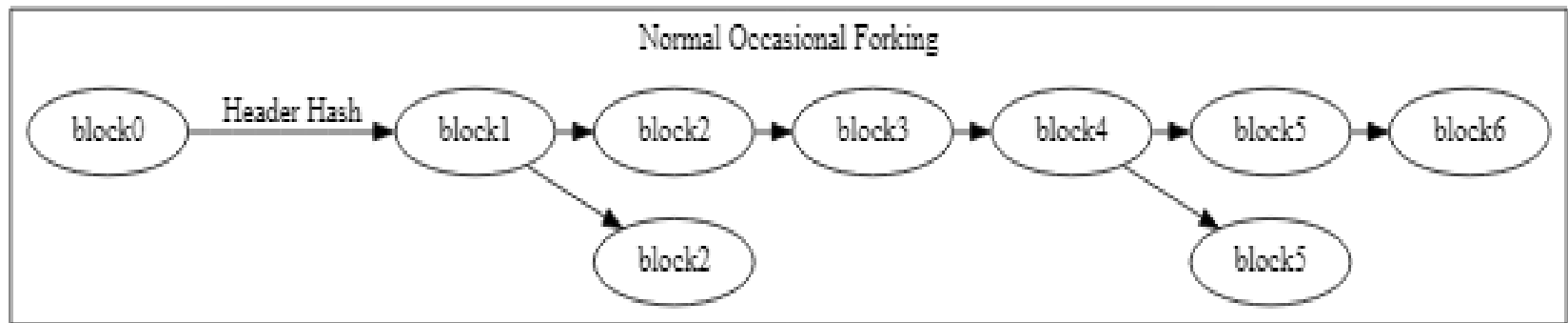
Rozwidlenia łańcucha bloków (forki)

1. Przypadkowe, okazjonalne i tymczasowe
2. Zmiany protokołu sieci blockchain nie zaakceptowane przez wszystkie węzły
 1. Rozwidlenia miękkie (softforki)
 2. Rozwidlenia twarde (hardforki)
3. Celowe rozwidlenia w celu reorganizacji bloków (atak 51%)

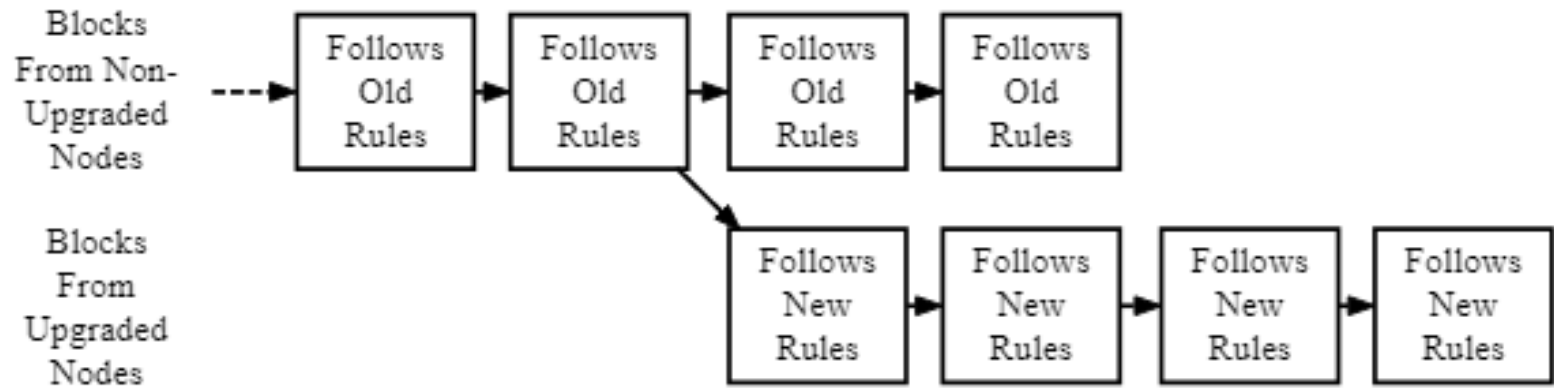
(1) Rozwidlenia przypadkowe

1. W różnych częściach sieci dwa bloki zostały prawidłowo Zdarza się, że w tym samym czasie wynajdywane są prawidłowe bloki w różnych częściach sieci – a długość łańcucha jest w nich taka sama
2. Węzły kontynuują pracę nad „własnym” blokiem, dopóki nie dotrze do nich informacja o dłuższym łańcuchu z innej części sieci – wtedy porzucają one bloki początkowo wykopane prawidłowo, a transakcje w nich zatwierdzone wracają do mempoola, chyba że zostały zatwierdzone w bloku, który ostatecznie został trwale dołączony do łańcucha

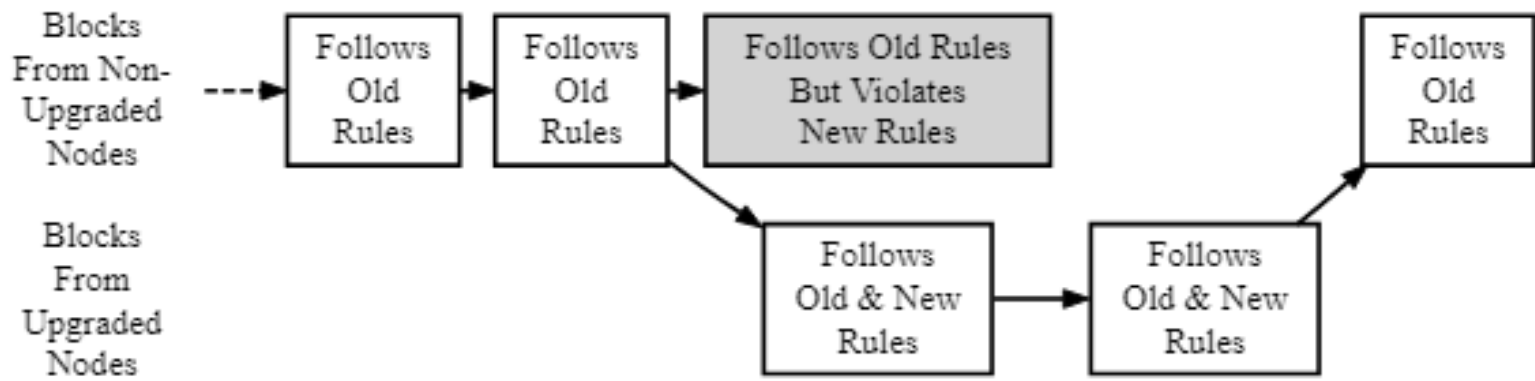
Wysokość bloku i „forki”



Hard i soft fork



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain



A Soft Fork: Blocks Violating New Rules Are Made Stale By The Upgraded Mining Majority

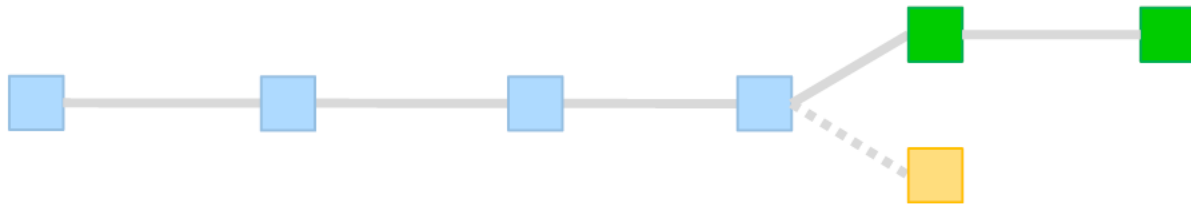
Atak 51%

- Bitcoin rozwiązuje problem generałów dopóki 51% węzłów jest uczciwych (niektórzy badacze wskazują na ok 67%)
- Jeśli pojedynczy węzeł posiada 51% mocy – może produkować dłuższe łańcuchy – zostaje centralnym kontrolującym
- Zdarzało się, że „poole” górników osiągały 40% mocy, wtedy niektóre węzły dobrowolnie się wycofywały, by zachować zaufanie do systemu
- Szacunkowy koszt ataku 51% na sieć **Bitcoina** to >10 miliardów USD (hardware only!)
<https://gobitcoin.io/tools/cost-51-attack/>

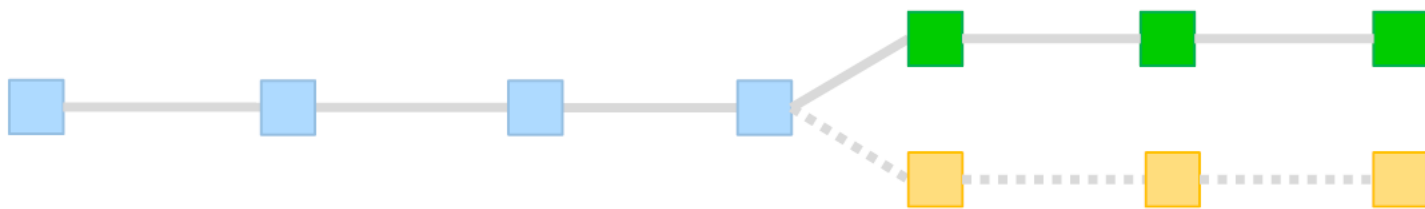
Figure 50: Illustration of Double-Spending Attack



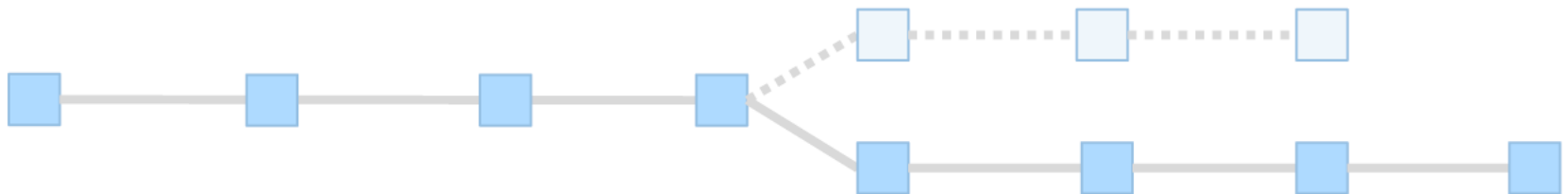
1) Initial blockchain in which all transactions are legitimate and considered valid.



2) Legitimate nodes extend the valid chain by adding green blocks, while the attacker secretly starts mining a fraudulent branch.



3) The attacker succeeds in making the fraudulent branch longer than the legitimate one.



4) The fraudulent branch created by the attacker is published and now considered the valid chain.

PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

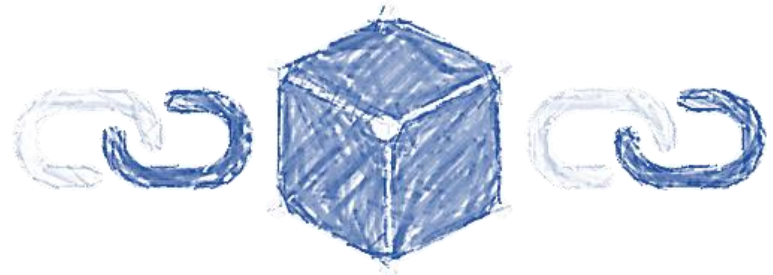
[Learn More](#)

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	\$1.08 T	SHA-256	162,595 PH/s	\$2,143,540	0%
Ethereum	ETH	\$525.42 B	Ethash	804 TH/s	\$2,393,260	7%
Litecoin	LTC	\$14.02 B	Scrypt	305 TH/s	\$169,340	14%
BitcoinCash	BCH	\$10.70 B	SHA-256	1,532 PH/s	\$20,191	40%
Zcash	ZEC	\$3.10 B	Equihash	5 GH/s	\$27,404	10%
Dash	DASH	\$1.87 B	X11	3 PH/s	\$4,810	3%
Ravencoin	RVN	\$1.12 B	KawPow	7 TH/s	\$31,889	28%
BitcoinGold	BTG	\$964.98 M	Zhash	2 MH/s	\$1,965	28%
Nervos	CKB	\$858.47 M	Eaglesong	75 PH/s	\$11,714	0%
Conflux	CFX	\$321.25 M	Octopus	4 TH/s	\$7,753	9%
Pirate	ARRR	\$319.00 M	Equihash	464 MH/s	\$2,386	118%
Ergo	ERG	\$233.68 M	Autolykos	17 TH/s	\$13,025	6%
QuarkChain	QKC	\$197.31 M	Ethash	17 GH/s	\$50	358,137%



Wartość blockchaina

Blockchain...



- **Infrastrukturalna**
 - **współdzielona / wspólna**
 - **sieciowa**
 - **ogólnego przeznaczenia**
 - **przełomowa (radykałna)**
 - **instytucjonalna**
 - **„anty-krucha”**
 - **antyintuicyjna? (*)**
 - 13 lat => wciąż początkowa faza rozwoju (!)
 - szuka zastosowań
 - wiele wyzwań (prawnych, technicznych, organizacyjnych)
- ... ALE wystarczająco dojrzała do biznesowych zastosowań i dalszego rozwoju usług DeFi

Innowacyjność blockchaina

- Sprytne połączenie znanych wcześniej technologii
- Dostarczenie rozwiązania do nieznanych jeszcze problemów
- (Eko)systemowość rozwiązań opartych na technologii
- Redundancja + bezpieczna i pewna synchronizacja
- Umożliwia zastąpienie (rozproszenie) braku zaufania i automatyzację relacji międzyludzkich (także formalnych) w Internecie
- Umożliwia powstanie dóbr cyfrowych posiadających cechę rzadkości (!) – w rozproszonym środowisku
- Umożliwia generowanie nowych modeli biznesowych wpisujących się w trend API-cyzacji
- Umożliwia zachowanie prywatności w relacjach (transferach) w nowy sposób niż „cebula” sieci Tor
- Open source, brak licencji, freeware

KRYPTOWAKTYWA, TOKENY

- *Nowa klasa aktywów*
- Jednocześnie trzy cechy
 - **Cyfrowy charakter**
 - **Rzadkość**
 - **Rozproszona wymiana**
- Dotychczas
 - **Cyfrowy charakter**: mp3, dane, artykuły online, aplikacje
 - **Cyfrowy charakter + rzadkość** – tylko scentralizowane wydawanie: podpis cyfrowy, certyfikaty elektroniczne (SSL); artefakty gier komputerowych, aplikacje i utwory z DRM



BLOCKCHAIN: ZASTOSOWANIA

Web 1.0

- Web1 to pierwsza wersja Internetu (technologii internetowych)
- Opiera się na
 - architekturze klient-serwer z komunikacją jednostronną
 - statycznych, nie interaktywnych aplikacjach webowych
 - prostej statycznej grafice

Web 2.0

- Web2 to druga wersja Internetu (technologii internetowych)
- Opiera się na
 - wykorzystaniu technologii umożliwiających interakcję z aplikacjami online
 - treściach, które tworzą sami użytkownicy
 - aplikacjach mobilnych
 - architekturze klient-serwer z komunikacją zwrotną
 - aplikacjach wykorzystujących maszynę klienta do obliczeń i przechowywania części danych
 - grafice wysokiej jakości, dynamicznej, z przejściami tonalnymi

Web 3.0

- Web3 to trzecia wersja Internetu (technologii internetowych)
- Opiera się na wykorzystaniu
 - aplikacji sieciowych
 - zdecentralizowanych protokołów (blockchain)
 - uczenia maszynowego
 - sztucznej inteligencji
 - architekturze klient-klient (P2P)
 - grafiki dynamicznej, także 3D, VR, AR
- Termin ten został stworzony przez Gavina Wooda, założyciela firmy Polkadot i współtwórcę Ethereum.

Grupy zastosowań

- Zastosowania zdecentralizowane
 - Usługi DeFi
 - Usługi DeSe (pozosące)
- Zastosowania scentralizowane



Zdecentralizowane usługi (DeSe)

DeSe = “zdecentralizowane usługi”

DeFi = “zdecentralizowane finanse”

(ang. decentralized finance)

- DeFi/DeSe to nowa branża obejmująca usługi finansowe:
 - dostarczane automatycznie w wirtualnych sieciach peer-to-peer z wysoce zdecentralizowaną kontrolą,
 - które korzystają z publicznych sieci typu permissionless (nie wymagają centralnie przyznanego zezwolenia na korzystanie z usługi, tworzenie infrastruktury usługowej lub świadczenie usługi),
 - które wykorzystują inteligentne kontrakty i technologię blockchain w procesach: świadczenia usług, tworzenia i tworzenia dóbr cyfrowych (tokenów) i jednostek rozliczeniowych (w tym stablecoinów), rozliczeń i rozliczeń, identyfikacji adresów i uwierzytelniania transakcji oraz koordynacji świadczenia usług.
- Defy - zaprzeczać

Cechy DeFi / DeSe

- Usługi w formie platformy
- Usługi w domenie publicznej
- Cyfrowe zasoby (kryptozasoby)
- Automatyczne, autonomiczne mechanizmy świadczenia usługi i rozliczeń (rozrachunków)
- Dostępność 24/7/365
- Dostępność globalna (egalitarność)
- Otwartość kodu
- Transparentność aktywności
- Prywatność
- Trwałość zapisu historii
- Małe wsparcie prawne użytkowników
- Brak nadzoru instytucjonalnego
- Brak zabezpieczenia funduszy użytkowników
- Trudność dochodzenia roszczeń
- Samodzielność, użytkowników
- Odpowiedzialność użytkowników
- Ryzyka na wszystkich użytkownikach
- Brak właściciela
- Często brak „majątku”
- Specyficzne zarządzanie

ZASTOSOWANIA (MODELE): Usługi DeFi

Usługi DeFi (1/2)

1. Systemy płatnicze, krypto-pieniężne: generowanie i transfer tokenów
 1. Natywne tokeny sieci
 2. Owinięte tokeny do zastosowań w innych sieciach
 3. Tokeny pochodzące z ICO, STO, IEO, IDO
 4. Stablecoiny
2. Platformy obrotu cyfrowymi tokenami (DEX)
 1. oparte na tabeli zleceń (ang. Order-Book-Based, OBB)
 2. oparte na pulach płynności (ang. liquidity pool) ~kantory / automatyczni animatorzy rynku (ang. Automated Market Makers, AMM)
 3. platformy rynkowe p2p
 4. platformy tradingowe
3. Platformy pożyczkowo-depozytowe
 1. o charakterze p2p lub oparte na puli płynności
 2. zabezpieczenie (pełne, częściowe, brak)

Usługi DeFi (2/2)

4. Usługi inwestycyjne (zarządzanie aktywami)
 1. fundusze inwestycyjne oparte na wyroczniach
 2. fundusze inwestycyjne oparte na automatycznych regułach
5. Staking (Staking-as-a-Service)
6. Pule płynności (Liquidity-as-a-Service)
7. Wynajem tokenów
8. Zakłady wzajemne / rynki prognostyczne
9. Ubezpieczenia
10. Hedging i instrumenty pochodne
11. Żądanie zapłaty
12. Faktoring
13. Akredytywa
14. Optymalizacja swapowania

DeFi + CeFi

- Usługi On-ramps, off-ramps
- Giełdy jako gatekeepers, AML
- Instytucjonalne DeFi
- Custodians (ART, EMT)
- Tokenizacja

<https://www.oecd.org/daf/fin/financial-markets/Why-Decentralised-Finance-DeFi-Matters-and-the-Policy-Implications.pdf>

Inne usługi DeSe

Usługi DeSe – zdecentralizowane usługi bez charakteru finansowego

1. Tokenizacja zasobów
2. NFT
3. Metaverse
4. Wyrocznie (oracle)
5. Dozorcy (keepers)
6. Gaming (Play-to-Earn)
7. Magazyny danych
8. DAO
9. Usługi nazwowe
10. Usługi analityczne
11. Usługi identyfikacji i tożsamości (SSI)
12. Usługi bezpieczeństwa (uwierzytelnianie, podpisy cyfrowe)

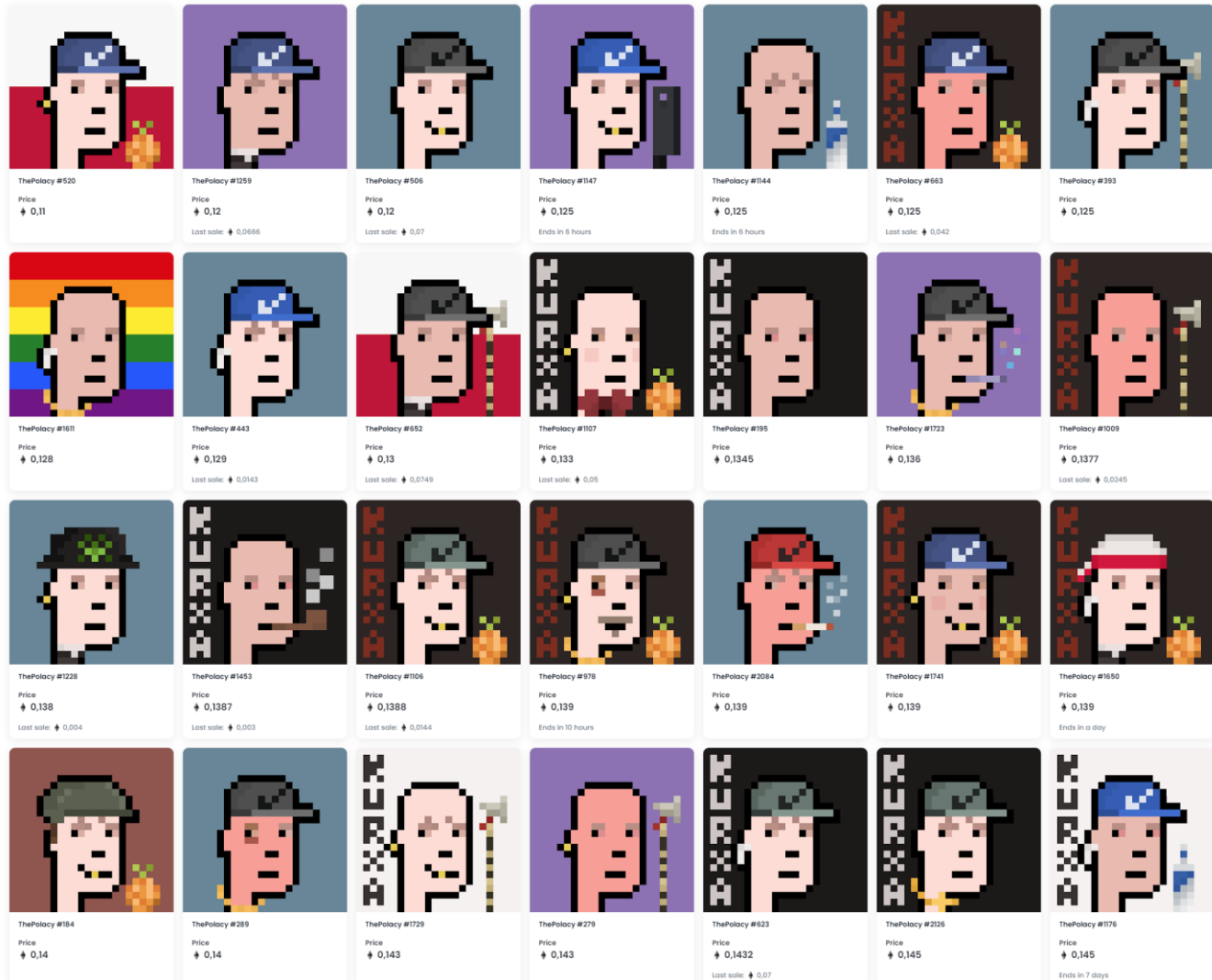
NFT 1.0

- NFT = Non-Fungible Token
- Dobro cyfrowe o złożonej strukturze
 - W rejestrze blockchainowym
 - Identyfikator dobra, odnośnik do zdecentralizowanego systemu plików
 - W zdecentralizowanym systemie plików
 - Ustrukturyzowany opis dobra
 - Poza zdecentralizowanym systemem
 - Wygenerowana cyfrowa materializacja dobra
- Każda jednostka dobra
 - indywidualna (nawet, jeśli identyczny zestaw cech, zwykle różny)
 - niepodzielna (co do zasady)
 - niezamienna - niezależnie transferowana i obracana na rynku
 - niesumowalna z innymi
 - niezależnie wyceniana

NFT 1.0 - rodzaje

- PFP (profile picture)
- Kolekcjonerskie
- dzieła sztuki cyfrowe
- Bilety
- wirtualne artefakty gier
- mody
- tokenizowane dobra i wartości (instrumenty finansowe)

ThePolacy (opensea.io/collection/thepolacy)



NFT 2.0

- Zaawansowane, złożone pod względem funkcjonalności tokeny NFT
- Cechy NFT 2.0
 - **Rozszerzalność własności**
 - Łańcuch własności: NFT jest w stanie połączyć się z innymi NFT lub projektami w użyteczny sposób: połączyć z innym NFT, NFT może „trzymać” wymienne tokeny (NFT może być „właścicielem” innych NFT); brak limitu zagnieżdżania;
 - NFT DAO: NFT może też samo być podzielne i mieć wielu właścicieli
 - **Możliwość aktualizacji** — szaty graficznej, wyboru metadanych, dodania nowych zasobów, przełączanie się między nimi (książka NFT może mieć 3 zasoby w różnych formatach — pdf, audiobook i okładkę jpeg); możliwość renderowania warunkowego: NFT zmienia swoje zasoby na podstawie spełnienia określonych kryteriów
 - **Dynamizm** — mogą wydawać polecenia, wyposażać inne NFT, zmieniać ich wygląd i wiele więcej, zgodnie z ustaleniami projektanta lub właściciela.

<https://medium.com/coinmonks/a-brief-overview-of-nft-2-0-e7bff4155533>

Metaverse

- Metaverse = wirtualna przestrzeń istniejąca poza światem rzeczywistym
 - Technologia 3D
 - Technologia VR
- Kiedyś niezależnie
 - Gry MMORPG
 - Gry FPP
 - Facebook
- Ale rynki – albo centralnie kontrolowane przez dostawcę gry (podaż artefaktów lub podaż waluty) albo poza grą
- Dzięki blockchainowi (NFT i cyfrowym walutom) – które potwierdzają „obiektywnie” własność, możliwe jest dodatkowo m.in.
 - nadawanie wartości artefaktom
 - handel nimi, bez centralnej kontroli
 - realizacja usług wewnątrz świata
 - realizacja konferencji, spotkań wymagających biletu lub opłaty
- Cyfrowe dobra:
 - Nieruchomości (działki)
 - Artefakty
 - Moda
 - Sztuka
- Masa nowych problemów prawnych



E

every

3d9d



Heineken
SILVER



Pascal#4b6c

an#cf52

Me#6b08

Brown#fd1c

nickolas#275b

Manouk#e6ed

Laura#584e

Madicu#716

Malty#8b0f

Nat#6010

icclo#2320

Zofia#ce6b

dauidsanper#7521

vassilis85#e21
Lambym

Vivian#enatsyou#29

97

ZASTOSOWANIA (MODELE):
PRYWATNY BLOKCHAIN

Wartość blockchaina

Przez funkcje i właściwości techniczne, które dostarcza blockchain, czyli

- **bezpieczeństwo** zapisu, przechowania, transferu (fundament)
- redundancja + bezpieczna i pewna **synchronizacja**, spójność danych
- **niezaprzeczalność** i ciągłość historii, dostęp do niedawnej historii w czasie rzeczywistym
- **decentralizacja** i elastyczność kontroli
- **automatyzacja** i programowalność, elastyczność reguł (protokołu) wymiany i synchronizacji
- **transparentność** (opcja),
- **kontrola** procesów wgrzywania, dostępu, zatwierdzania, utrzymywania... (opcja)

BLOCKCHAIN UMOŻLIWIA

utrzymanie trwałej relacji w rozproszonej sieci suwerennych jednostek, czyli np..

Zastosowania scentralizowane (1/2)

1. Płatności

1. system płatniczy
2. system podatkowy
3. usługi rozliczeniowo-rozrachunkowe
4. usługi płatnicze
 1. pieniądz elektroniczny
 2. zamknięte systemy z własną jednostką płatniczą (rozliczeniową)
5. CBDC
6. stokenizowane instrumenty finansowe (swapy, forward, futures, dłużne)
 1. Pozyskiwanie finansowania
 2. Hedging

2. Funkcja trwałego nośnika (PKO BP, KIR)

1. dokumenty publiczne
2. dokumenty prywatne
3. inne rejestry (akcjonariuszy, nieruchomości; medyczne, certyfikaty)

Zastosowania scentralizowane (2/2)

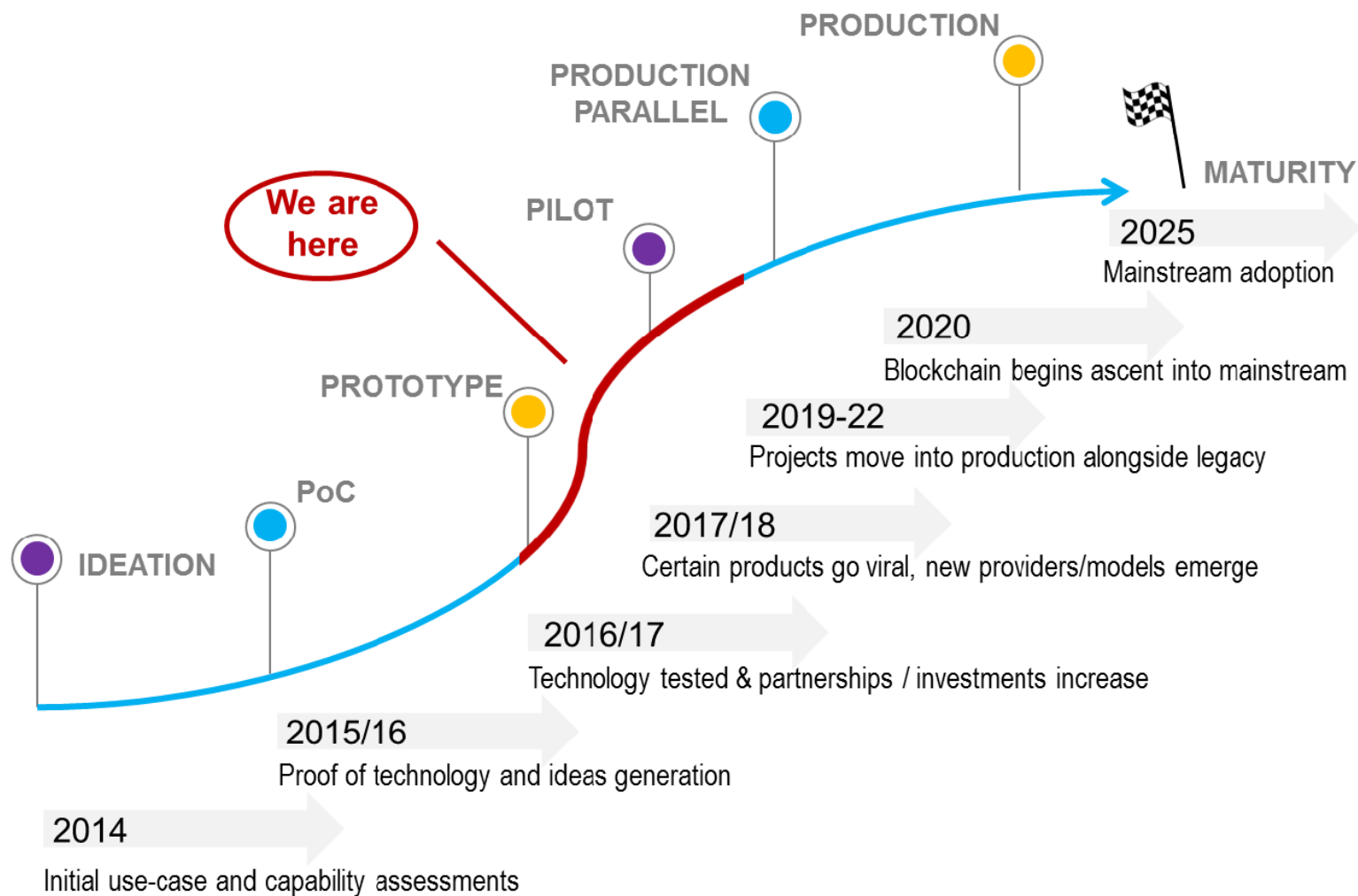
3. Blockchain-as-a-Service (BaaS)
4. Logistyka: integracja łańcucha dostaw
 1. Kontrola przepływu dokumentów
 2. Kontrola przepływu dokumentów
5. Rozproszone platformy wymiany
 1. rozproszone usługi tzw. gospodarki wymiany (jak Uber, Allegro, pożyczki p2p)
 2. rozproszone giełdy (energii dla prosumentów, papierów wartościowych)
6. Zarządzanie prawami autorskimi dzieł cyfrowych
7. Systemy głosowania i wyborów
8. Internet of Things (IoT)
9. Audyt, controlling finansowy

The background is a dark blue space filled with numerous glowing, semi-transparent blue cubes of various sizes and orientations. These cubes are interconnected by a network of thin, bright blue lines, some of which resemble lines of computer code or data streams. The overall effect is a sense of a complex, multi-dimensional digital or data environment.

Przyszłość?

Przyszłość

Figure 45: Development timeline – where are we now?



Blockchain w lesie?



TAK!

- Śledzenie pochodzenia produktów drewnianych
- Zarządzanie lasem
- Wsparcie wykrywania zagrożeń pożarowych

**„Blockchain Applications in Forestry: A Systematic Literature Review”
(2022): <https://www.mdpi.com/2076-3417/12/8/3723/pdf>**

Śledzenie produktów

Main Focus	Purpose(s) of the Use of Blockchain
A blockchain-based technical solution	To provide a blockchain-based technological solution to prevent illegal logging
Azure Blockchain Workbench	To trace and validate wood from standing tree to the final user
A tamper-proof digital system	To combine blockchain with digital protocols for physical verification and authentication in timber tracking
LogLog: A Blockchain Solution for Tracking and Certifying Wood Volumes	To trace wood volumes in the timber supply chain
A Tamper-Proof Volume Wood Tracking System	To validate certified wood and record the origin of wood
Ethereum decentralized application (Dapp)	To trace and validate teak wood in the supply chain via Ethereum DApp
Image Identification of blockchain-based Wood traceability system	To improve wood product identification in blockchain-based wood traceability system by using AKAZE method replace the traditional image-based methods
Blockchain-based contract management platform	To control and manage the documents and permits to reduce complexity of contract management

Zarządzanie lasem

Main Focus	Purpose(s) of the Use of Blockchain
A blockchain-based web application on forestry nurseries (inventory) management	To monitor the forest plants and record information of each plant for further validation
The use of blockchain on carbon trading market	To address the key concerns to REDD+ projects
A blockchain solution for REDD+	To improve the reliability of carbon sequestration monitoring and protecting global forests
Blockchain on forestry carbon sink projects	To optimize forestry carbon sink trading and reduce emissions
Participatory forest management with blockchain (blockchain-based governance)	For governance purposes
Image processing and blockchain for forest management	To save species of tree varieties and avoid overexploited by identifying the number and type of trees

Wykrywanie zagrożeń pożarowych

Layers of Architecture	Purpose(s) of the Use of Blockchain
IoT layer (with sensors) Fog layer Cloud layer	To detect forest fire and validate the information
IoT layer (with drones) Edge layer Cloud layer	To detect forest fire and validate the information

O czym nie powiedzieliśmy (m.in.)

- Szczegóły technologiczne
- Problemy prawne
- Problemy ekologiczne
- Ryzyka
- Analiza i inwestowanie
- Finanse (podatki, księgowość)
- Ekonomia ekosystemu
- Relacje z innymi technologiami

DZIĘKUJĘ

- [linkedin.com/in/gsobiecki/](https://www.linkedin.com/in/gsobiecki/)
- gsobie@sgh.waw.pl
- gsobiecki@gmail.com
- +48 696 440 725
- ETH: grzegorzsobiecki.eth



WIZYTÓWKA