

Zrównoważony rozwój systemu Blockchain.



Grzegorz Cenkier

*PTI, ISSA and
SEEBLOCKS.eu*

STANDARDISATION
CONFERENCE

SHAPING THE FUTURE OF EUROPEAN STANDARDISATION



TURNING ^{NEW} LEGISLATION
**CYBER
RESILIENCE
ACT**

INTO
STANDARDS

EU
COMMISSION

**OUR
STRATEGY**
FOR IMPLEMENTATION

**COLLABORATION
IS
CRUCIAL**



THOSE WHO
THREATEN OUR
SECURITY ARE
COLLABORATING

AS
TECHNOLOGY
HAS GOTTEN MORE
COMPLEX,
STANDARDS ARE
INCREASINGLY
IMPORTANT

SUPPORT
INNOVATION
& BOOST
SKILLS

MIND THE
GEOPOLITICAL
ENVIRONMENT

PRIORITISE
STANDARDS

INVOLVE ALL
STAKEHOLDERS

**INTERNATIONAL
FIRST** PRINCIPLE



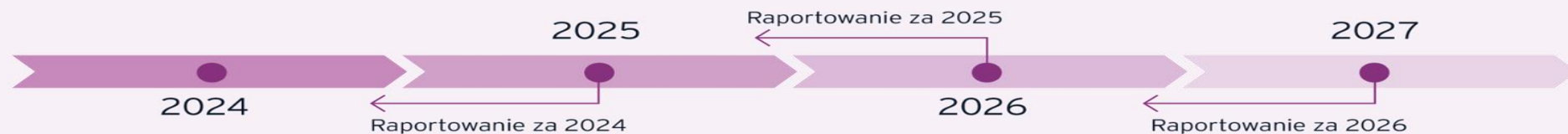
WE MUST
TOO!

Zrównoważony rozwój systemów informatycznych odnosi się do projektowania, wdrażania i zarządzania technologiami w sposób **minimalizujący negatywny wpływ na środowisko**, społeczeństwo i gospodarkę. Obejmuje to **efektywne wykorzystanie zasobów, redukcję emisji CO₂, optymalizację zużycia energii oraz wdrażanie ekologicznych technologii.**

Współczesne organizacje IT coraz częściej integrują strategie ESG (Environmental, Social, Governance), które pomagają w budowaniu odpowiedzialnych i zrównoważonych modeli biznesowych. Firmy technologiczne wdrażają rozwiązania takie jak chmura obliczeniowa, automatyzacja procesów oraz zarządzanie energią w centrach danych, aby zmniejszyć ślad węglowy i poprawić efektywność operacyjną

Zrównoważony rozwój blockchain odnosi się do wykorzystania technologii w sposób minimalizujący negatywny wpływ na środowisko i społeczeństwo. Obejmuje to redukcję **zużycia energii, przejrzystość łańcuchów dostaw, weryfikację energii odnawialnej oraz zastosowanie ekologicznych mechanizmów konsensusu.**

Rozwój raportowania niefinansowego w Polsce



Kto

2025

Podmioty raportujące do tej pory na gruncie NFRD, czyli tzw. jednostki zainteresowania publicznego, np. spółki publiczne

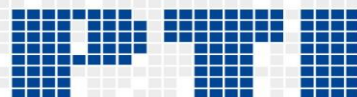
2026

Duży przedsiębiorcy, czyli zarówno przedsiębiorcy notowani, jak i nienotowani, spełniający 2 z 3 poniższych kategorii:

- zatrudnienie powyżej 250 pracowników
- 25 mln EUR sumy aktywów
- 50 mln EUR przychodów netto

2027

Między innymi notowane małe i średnie przedsiębiorstwa



POLSKIE TOWARZYSTWO INFORMATYCZNE

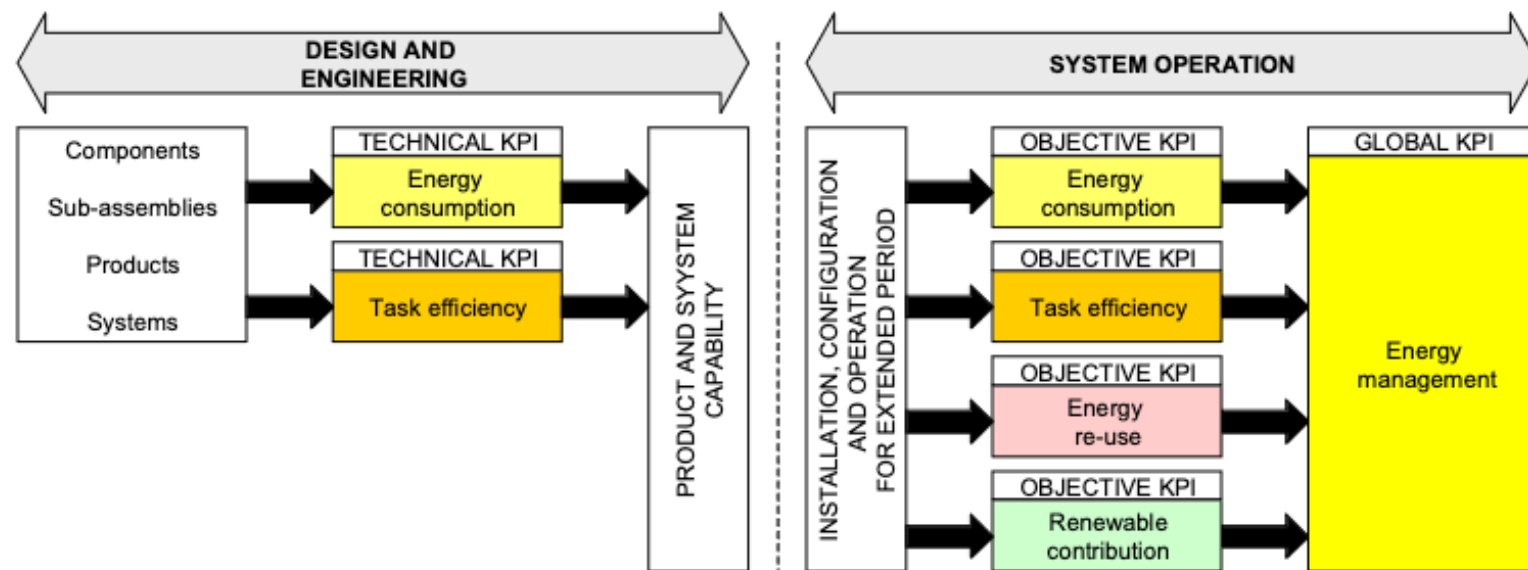
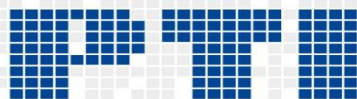


Figure E.1 - The relationship of energy-related Technical, Objective and Global KPIs



POLSKIE TOWARZYSTWO INFORMATYCZNE

Historia powstania Blockchaina

Blockchain został po raz pierwszy zaproponowany przez kryptografa Davida Chauma w jego pracy doktorskiej z **1982 roku**, *„Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups”*. Dalsze prace nad kryptograficznie zabezpieczonym łańcuchem bloków zostały opisane w **1991 roku** przez **Stuarta Habera i W. Scotta Stornette**. Chcieli oni wdrożyć system, który uniemożliwiłby edycję znaczników czasu dokumentów. **W 1992 roku Haber, Stornetta i Dave Bayer dodali do projektu drzewa Merkle'a, co uczyniło go bardziej wydajnym**, umożliwiając zebranie kilku dokumentów w jeden blok.

Pierwszy zdecentralizowany blockchain był wynikiem pracy osoby (lub grupy osób) znanej jako **Satoshi Nakamoto w 2008 roku**. Nakamoto wprowadził kilka kluczowych ulepszeń do projektu, wykorzystując metodę podobną do **Hashcash** do oznaczania czasowego bloków bez konieczności podpisywania ich przez zaufaną stronę i wprowadzając parametr trudności w celu ustabilizowania tempa dodawania bloków do łańcucha.

Proof of Work (PoW) to zdecentralizowany mechanizm wykorzystywany do walidacji transakcji i zabezpieczania sieci. PoW gwarantuje, że wszyscy uczestnicy sieci zgadzają się co do stanu łańcucha bloków i umożliwia bezpieczne przetwarzanie transakcji peer-to-peer bez potrzeby korzystania z zaufanej strony trzeciej. Jest to prosty fakt, że dowód Proof of Work (PoW) jest zdecentralizowanym mechanizmem wykorzystywanym do walidacji transakcji i zabezpieczania sieci. PoW gwarantuje, że wszyscy uczestnicy sieci zgadzają się co do stanu łańcucha bloków i umożliwia bezpieczne przetwarzanie transakcji peer-to-peer bez potrzeby korzystania z zaufanej strony trzeciej. Prostem faktem jest, że proof of work na dużą skalę wymaga ogromnych ilości energii, a to tylko wzrasta, gdy więcej członków dołącza do sieci. Koncepcja ta została wynaleziona przez Moni Naor i Cynthia Dwork w 1993 roku.

Kluczowe cechy PoW:

Górnictwo: Górnicy rywalizują w rozwiązywaniu złożonych zagadek matematycznych. Pierwszy, który rozwiąże zagadkę, dodaje nowy blok do łańcucha bloków i jest nagradzany kryptowalutą.

Bezpieczeństwo: Wysilek obliczeniowy wymagany do rozwiązywania tych zagadek utrudnia złośliwym podmiotom zmianę łańcucha bloków, zapewniając jego bezpieczeństwo.

Zużycie energii: PoW wymaga znacznego zużycia energii, ponieważ górnicy używają potężnego sprzętu do rozwiązywania zagadek (PoW) jest zdecentralizowanym mechanizmem używanym do walidacji transakcji i zabezpieczania sieci. PoW gwarantuje, że wszyscy uczestnicy sieci zgadzają się co do stanu blockchaina i umożliwia bezpieczne przetwarzanie transakcji peer-to-peer bez potrzeby korzystania z systemu kontroli.

Proof of Stake (PoS) to algorytm konsensusu wykorzystywany w technologii blockchain do walidacji transakcji i tworzenia nowych bloków. W przeciwieństwie do Proof of Work (PoW), który opiera się na mocy obliczeniowej, PoS wybiera walidatorów na podstawie liczby tokenów, które posiadają i są skłonni „postawić” jako zabezpieczenie. Proof of Stake został po raz pierwszy wprowadzony w 2012 roku przez Sunny'ego Kinga i Scotta Nadala

Kluczowe cechy PoS:

Efektywność energetyczna: PoS jest bardziej energooszczędny niż PoW, ponieważ nie wymaga dużych zasobów obliczeniowych.

Wybór walidatorów: Walidatory są wybierane na podstawie ich udziału w sieci, co łączy ich interesy z bezpieczeństwem i stabilnością sieci.

Bezpieczeństwo: PoS zmniejsza ryzyko centralizacji i jest mniej podatny na niektóre rodzaje ataków, takie jak ataki 51%

Ile energii zużywają Bitcoin i Ethereum?

Porównując koszt pojedynczej transakcji w każdej sieci, różnice w zużyciu energii są wyraźne.

Sieć **Bitcoin** może obsłużyć tylko około **5 transakcji na sekundę**, co skutkuje kosztem energii wynoszącym **830 kWh** na transakcję.

Ethereum (od 14 września 2022) może obsłużyć około **15 transakcji na sekundę**, co skutkuje kosztem energii na poziomie **50 kWh** na transakcję.

Ile energii zużywają Bitcoin i Ethereum?

W celu obliczenia zużycia energii w sieciach PoW i Ethereum wykorzystywane są szacunki lub proxy. Wynika to z faktu, że oszacowanie zużycia energii przez sieć jest złożonym zadaniem. Najczęściej cytowanym szacunkiem zużycia energii Bitcoin jest **Cambridge Bitcoin Electricity Consumption Index (CBECI)**, opracowany w Cambridge Centre for Alternative Finance (CCAF).



POLSKIE TOWARZYSTWO INFORMATYCZNE



Cambridge Bitcoin Electricity Consumption Index

LIVE

Bitcoin network power demand

🕒 updated every 24 hours

Theoretical lower
bound

11.43

GW

100.17

TWh

Estimated ?

22.60

GW

Annualised
consumption ?

198.15

TWh

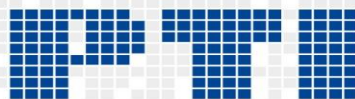
Theoretical upper
bound

47.52

GW

416.54

TWh



POLSKIE TOWARZYSTWO INFORMATYCZNE



UNIVERSITY OF
CAMBRIDGE
Judge Business School

Cambridge
Centre
for Alternative
Finance

Cambridge Bitcoin Electricity Consumption Index

LIVE

Ethereum network power demand

🔄 updated every 24 hours

Theoretical lower
bound

162.98

kW

1.43

GWh

Estimated ?

503.59

kW

Annualised
consumption ?

4.41

GWh

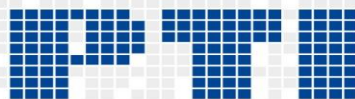
Theoretical upper
bound

1201.71

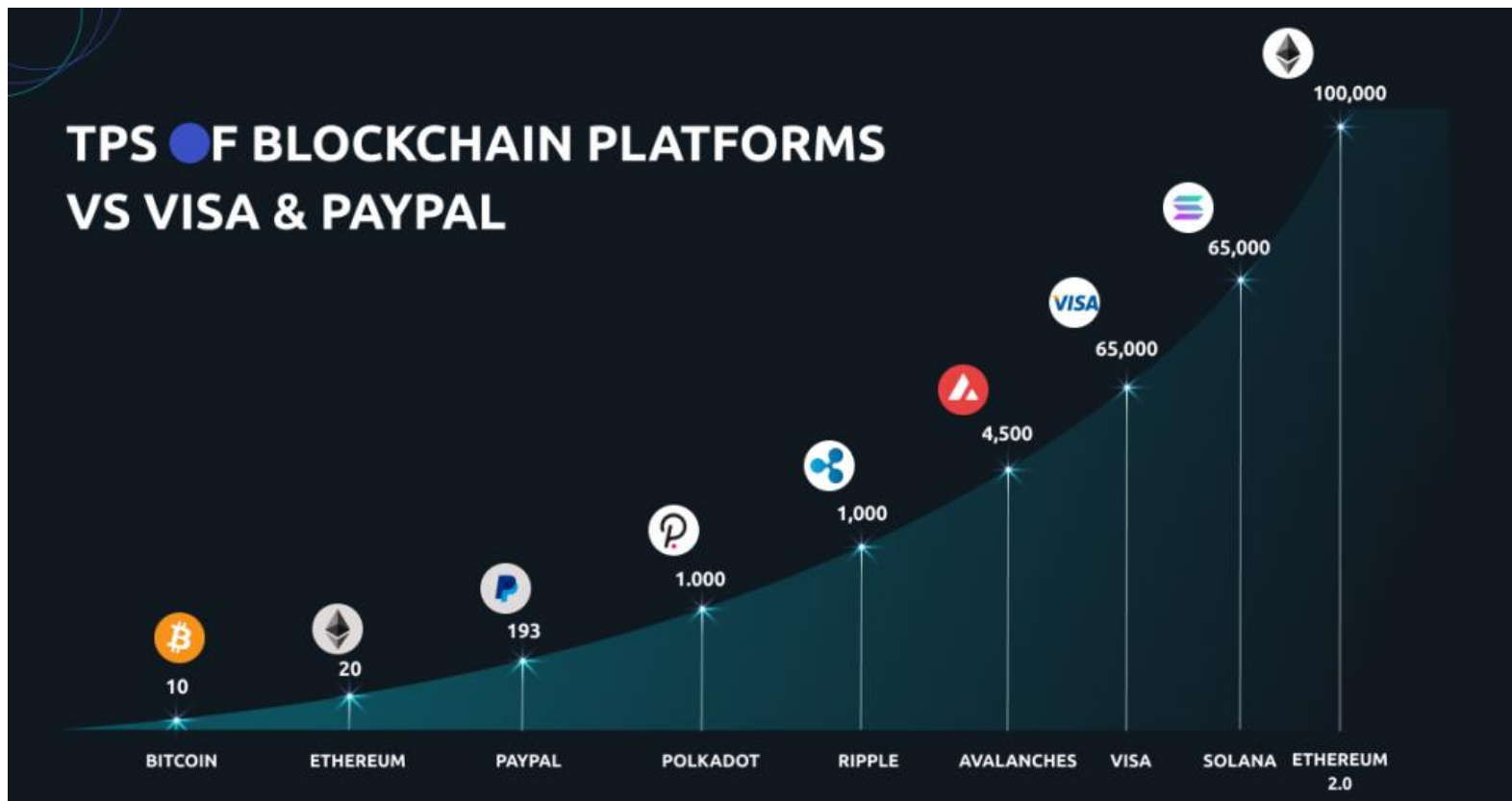
kW

10.53

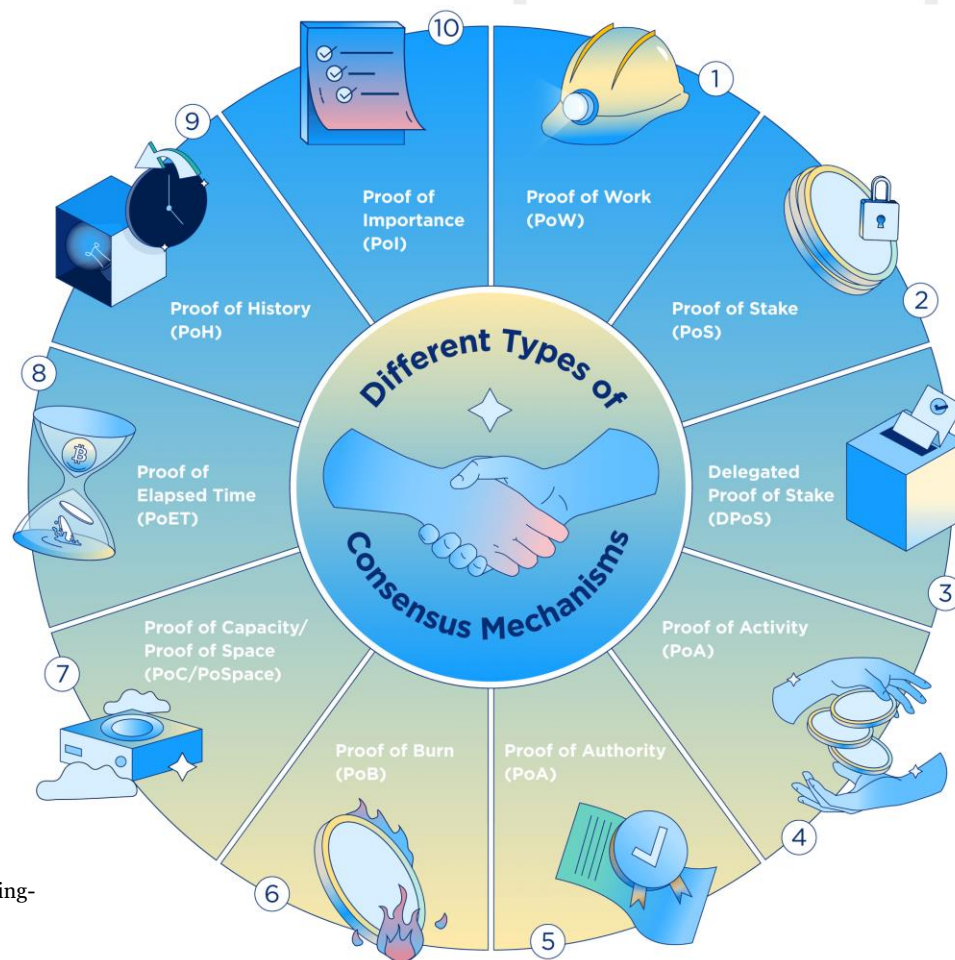
GWh



POLSKIE TOWARZYSTWO INFORMATYCZNE

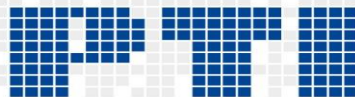


<https://www.summit.io/pl/blog-posts/understanding-proof-of-work-and-proof-of-stake>



Kluczowe punkty i najszybsza lista kryptowalut blockchain

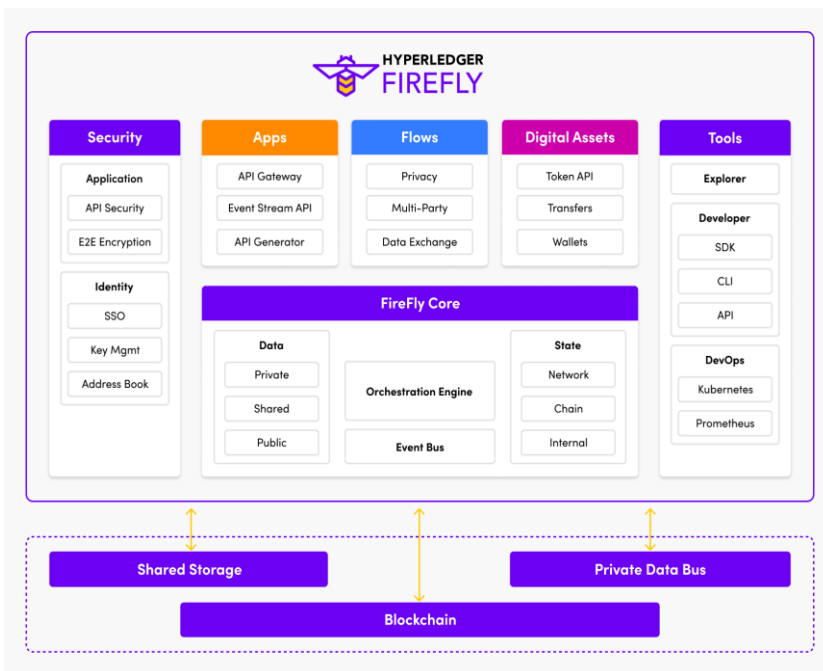
Blockchain	Key Features	Transaction Speed	Consensus Mechanism	Platform Focus
Solana (SOL)	Wysoka przepustowość, niskie opłaty, szybkie przetwarzanie, obsługuje inteligentne kontrakty i zdecentralizowane aplikacje (dApps)	65,000+ TPS	Proof of History (PoH) + Proof of Stake (PoS)	DeFi, dApps, NFTs
Avalanche (AVAX)	Wysoka skalowalność, konsensus o niskich opóźnieniach, podsieci dla konfigurowalnych łańcuchów bloków	4,500+ TPS	Avalanche Consensus	DeFi, NFTs, Enterprise Solutions
Polygon (MATIC)	Rozwiązanie do skalowania Ethereum, technologia sidechain, niskie opłaty, szybkie transakcje	7,000+ TPS	Proof of Stake (PoS)	Ethereum scaling, DeFi
Fantom (FTM)	Szybki, skalowalny, zdecentralizowany, obsługuje dApps, DeFi, NFT	25,000+ TPS	Lachesis (aBFT)	DeFi, dApps, NFTs
Binance Smart Chain (BSC)	Szybki blockchain o niskich opłatach, zintegrowany z ekosystemem Binance, obsługuje inteligentne kontrakty	100+ TPS	Proof of Staked Authority (PoSA)	DeFi, NFTs, dApps



POLSKIE TOWARZYSTWO INFORMATYCZNE

Hyperledger Foundation

założona w 2015 r. jako część Linux Foundation, jest neutralnym miejscem dla deweloperów do współpracy, współtworzenia i utrzymywania oprogramowania w technologii blockchain dla przedsiębiorstw w modelu open source.



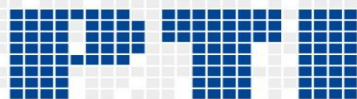
Hyperledger FireFly to pierwszy w branży Supernode o otwartym kodzie źródłowym: **platforma do tokenizacji, interoperacyjności wielu łańcuchów i tworzenia aplikacji opartych na blockchainie**. Stos nowej generacji FireFly upraszcza rozwój blockchain, ułatwiając niezawodne łączenie się w wielu publicznych i prywatnych łańcuchach oraz zarządzanie cyklem życia zasobów cyfrowych dzięki natywnej obsłudze tokenów i indeksowania. FireFly w coraz większym stopniu zasila projekty tokenizacji aktywów, które wykorzystują natywną obsługę popularnych tokenów, interoperacyjność wielu łańcuchów i zwiększoną prywatność poza łańcuchem, a także inne pojawiające się obszary, takie jak zdecentralizowana tożsamość. Algorytm konsensusu - walidator ustalonego zestawu łańcucha - najczęściej jest to **Proof of Stake (PoS)**.

Kluczowymi komponentami Hyperledger FireFly, platformy blockchain i tokenizacji, są:

- Multi-Protocol Blockchain Interoperability: FireFly natywnie obsługuje łańcuchy bloków Ethereum i Hyperledger Fabric z możliwością łączenia się z dowolną istniejącą siecią blockchain i obsługi przepływów do, z i między tymi łańcuchami.
- Natywna integracja zasobów cyfrowych: FireFly obsługuje popularne standardy tokenów, takie jak ERC20, ERC721 i ERC1155 z pulami tokenów, indeksowaniem i nie tylko.
- Interfejsy API Web3: FireFly oferuje pełny zestaw interfejsów API do tworzenia i zarządzania tokenami, monetami, NFT, inteligentnymi kontraktami i nie tylko.
- Interoperacyjność z wieloma protokołami blockchain: FireFly natywnie obsługuje łańcuchy bloków Ethereum i Hyperledger Fabric z możliwością łączenia się z dowolną istniejącą siecią blockchain i obsługi przepływów do, z i między tymi łańcuchami.
- Natywna integracja zasobów cyfrowych: FireFly obsługuje popularne standardy tokenów, takie jak ERC20, ERC721 i ERC1155 z pulami tokenów, indeksowaniem i nie tylko.
- Interfejsy API Web3: FireFly oferuje pełny zestaw interfejsów API do tworzenia i zarządzania tokenami, monetami, NFT, inteligentnymi kontraktami i nie tylko.
- Interfejsy API do tworzenia aplikacji: API Gateway FireFly pozwala na proste i solidne tworzenie aplikacji.
- Integracja i orkiestracja: Wewnątrz FireFly, warstwy komunikatów i zdarzeń zapewniają niezawodną integrację z istniejącymi systemami.
- Prywatność danych poza łańcuchem: FireFly koordynuje cyfrowe zasoby i przepływy, które obejmują połączenie danych „off-chain” z tokenami i zdarzeniami „on-chain”.

Hyperledger FireFly jest obecnie wykorzystywany we wdrożeniach produkcyjnych na całym świecie, w tym Synaptic Health Alliance, The Institutes RiskStream Collaborative, **Swift, CGI Federal**, Blockchain for Energy, CP Group i LACChain.

Globalne zużycie energii elektrycznej przez centra danych, sztuczną inteligencję i sektor kryptowalut ma podwoić się z szacowanych 460 terawatogodzin (TWh) w 2022 r. do ponad 1000 TWh w 2026 r., wynika z raportu badawczego Międzynarodowej Agencji Energii - International Energy Agency (IEA).



POLSKIE TOWARZYSTWO INFORMATYCZNE

Technology

Hungry for Energy, Amazon, Google and Microsoft Turn to Nuclear Power

Large technology companies are investing billions of dollars in nuclear energy as an emissions-free source of electricity for artificial intelligence and other businesses.



Google zapowiedziało, że będzie kupować energię od Kairos Power, dewelopera małych reaktorów modułowych, aby pomóc „osiągnąć postęp w dziedzinie sztucznej inteligencji”.

Microsoft podpisał we wrześniu 2024 r. umowę z amerykańską firmą energetyczną Constellation na wskrzeszenie niedziałającego reaktora w słynnej elektrowni jądrowej Three Mile Island w Pensylwanii.

Amazon Web Services inwestuje ponad 500 milionów dolarów w energię jądrową, ogłaszając trzy projekty od Wirginii po stan Waszyngton. AWS, spółka zależna Amazon zajmująca się przetwarzaniem w chmurze, ma ogromne i rosnące zapotrzebowanie na czystą energię, ponieważ rozszerza swoje usługi o generatywną sztuczną inteligencję. Jest to również część drogi Amazon do zerowej emisji dwutlenku węgla netto

Dlaczego firmy technologiczne zwracają się ku energii jądrowej ?

Znajdują się pod presją znalezienia źródeł energii do zasilania centrów danych - kluczowego elementu infrastruktury stojącej za współczesnymi aplikacjami do przetwarzania w chmurze i sztucznej inteligencji.

Wielu deweloperów wynajmuje serwery wyposażone w procesory graficzne (GPU), które zazwyczaj są zbyt drogie, aby je posiadać, od tak zwanych „hiperskalerów” chmurowych - takich jak Amazon, Microsoft i Google.

Giganci technologiczni skorzystali na wzroście zainteresowania generatywnymi aplikacjami sztucznej inteligencji, takimi jak ChatGPT firmy OpenAI. Jednak ten wzrost popytu doprowadził również do niezamierzonego efektu: odpowiednio dużych skoków w ilości wymaganej energii.

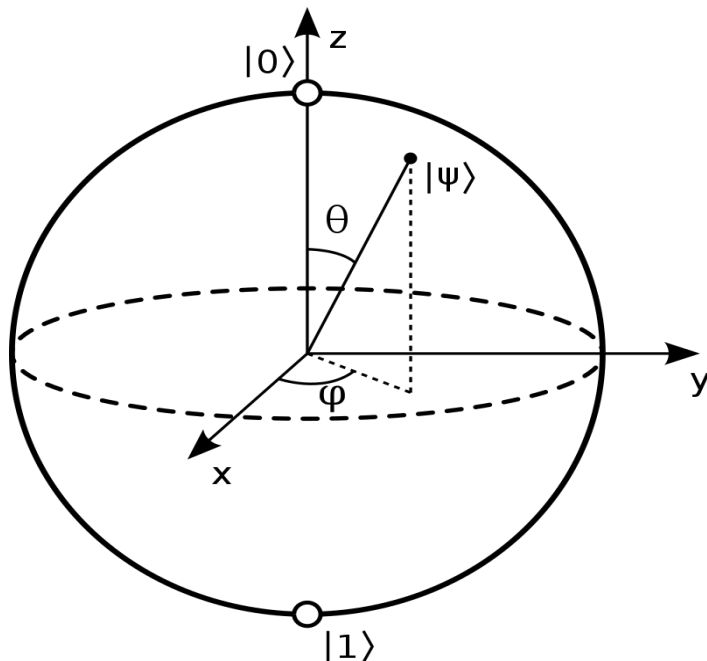
Komputery kwantowe

Komputery kwantowe w Europie mają działać od 2025 r.

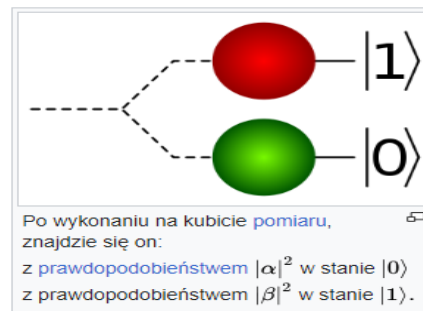
Komisja Europejska podpisała umowy z sześcioma ośrodkami naukowymi z sześciu krajów europejskich - Polski, Włoch, Hiszpanii, Francji, Niemiec i Republiki Czeskiej.

EuroQCS-POLAND będzie zlokalizowany w Poznańskim Centrum Superkomputerowo-Sieciowym (PCSS) i będzie zintegrowany z infrastrukturą Centrum.

Kubit



Kubit (ang. qubit od quantum bit, bit kwantowy) – najmniejsza i niepodzielna jednostka informacji kwantowej



Graficzne przedstawienie wartości kubitów na sferze Blocha. Nie można uogólnić sfery Blocha na więcej bitów kwantowych.

R & D

W październiku 2023 r **Fińskie Centrum Badań Technicznych VTT** oraz europejski producent komputerów kwantowych, **IQM Quantum Computers**, ukończyły budowę drugiego fińskiego komputera kwantowego. Nowy 20-kubitowy komputer kwantowy wzmacnia pozycję Finlandii wśród krajów inwestujących w obliczenia kwantowe. Finlandia ukończyła swój pierwszy komputer kwantowy, 5-kubitowy, w 2021 r.

<https://www.rdworldonline.com/>



Opis komputera kwantowego Odra 5

Pięciokubitowa maszyna waży półtorej tony i ma trzy metry wysokości, a jej charakterystyczny kriostat jest otoczony metalowym walcem zwisającym z sufitu.

Bazuje na technologii niskotemperaturowych nadprzewodzących kubitów i pracuje w temperaturze 10 mK (milikelwinów), czyli $-273,14^{\circ}\text{C}$.

Odra 5 jest przygotowana do pracy z czołowymi środowiskami obliczeń kwantowych. Będzie stanowić bazę do nauki obsługi tych technologii w większej skali.

Maszyna została opracowana i dostarczona przez firmę IQM Quantum Computers, światowego lidera w dziedzinie nadprzewodzących komputerów kwantowych.

Wraz z zakupem i uruchomieniem maszyny pięciokubitowej Politechnika Wrocławska otrzymała dostęp do większych maszyn, 20 i ponad-50-kubitowych zainstalowanych w centrum firmy IQM w Alto w Finlandii.

Algorytmy

Postęp obliczeń kwantowych otworzył możliwość przeprowadzania ataków w oparciu o algorytmy Grovera i Shora. Takie algorytmy zagrażają zarówno **kryptografii klucza publicznego**, jak i **funkcjom skrótu**, zmuszając do przeprojektowania struktur systemów informatycznych , aby wykorzystać kryptosystemy, które wytrzymują ataki kwantowe, tworząc w ten sposób kryptosystemy znane jako kryptosystemy postkwantowe, kwantowe, bezpieczne kwantowo lub kwantowo-odporne.

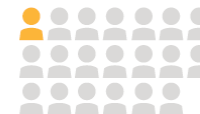
Algorytm Shora

Kryptosystemy klucza publicznego, jak i funkcje skrótu są zagrożone przez ewolucję komputerów kwantowych. Ataki mają wpływ na najpopularniejsze algorytmy klucza publicznego, w tym **RSA** (Rivest, Shamir, Adleman), **ECDSA** (Elliptic Curve Digital Signature Algorithm), **ECDH** (Elliptic Curve Diffie-Hellman) czy **DSA** (Digital Signature Algorithm), które można złamać **algorytmem Shora** na wystarczająco potężnym komputerze kwantowym.



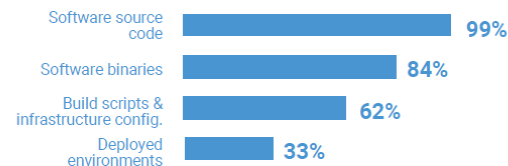
POLSKIE TOWARZYSTWO INFORMATYCZNE

Just **1 in 20** say their Digital Trust practices are extremely mature.

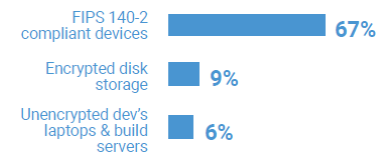


Most say just "somewhat" mature

What enterprises are code-signing:



What enterprises are storing code signing private keys:



If a code signing private key was compromised **NONE** would be able to quickly and easily discover all applications where it was used to sign.

NIST Post-Quantum Cryptography Standardization Project.

NIST ogłasza pierwsze cztery kwantowe algorytmy kryptograficzne:

Wersje robocze standardów FIPS 203, 204 i 205 określają zakres stosowania:

- ⇒ CRYSTALS-Kyber, zaprojektowany do ogólnych celów szyfrowania, takich jak tworzenie bezpiecznych stron internetowych.
- ⇒ CRYSTALS-Dilithium, zaprojektowany w celu ochrony podpisów cyfrowych, których używamy podczas zdalnego podpisywania dokumentów.
- ⇒ Protokół SPHINCS+, również przeznaczony do podpisów cyfrowych.
- ⇒ FALCON, również zaprojektowany z myślą o podpisach cyfrowych, ma otrzymać własny projekt FIPS w 2024 roku.

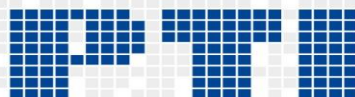
Schematy kryptograficzne

FIPS 203 standardowy mechanizm hermetyzacji kluczy oparty na siatce modułów

Module-Lattice-Based Key-Encapsulation Mechanism
Standard

FIPS 204, standard podpisu cyfrowego oparty na sieci modułów
Module-Lattice-Based Digital Signature Standard

FIPS 205, bezstanowy standard podpisu cyfrowego oparty na skrótach
Stateless Hash-Based Digital Signature Standard



POLSKIE TOWARZYSTWO INFORMATYCZNE



Lattice-based KEMs



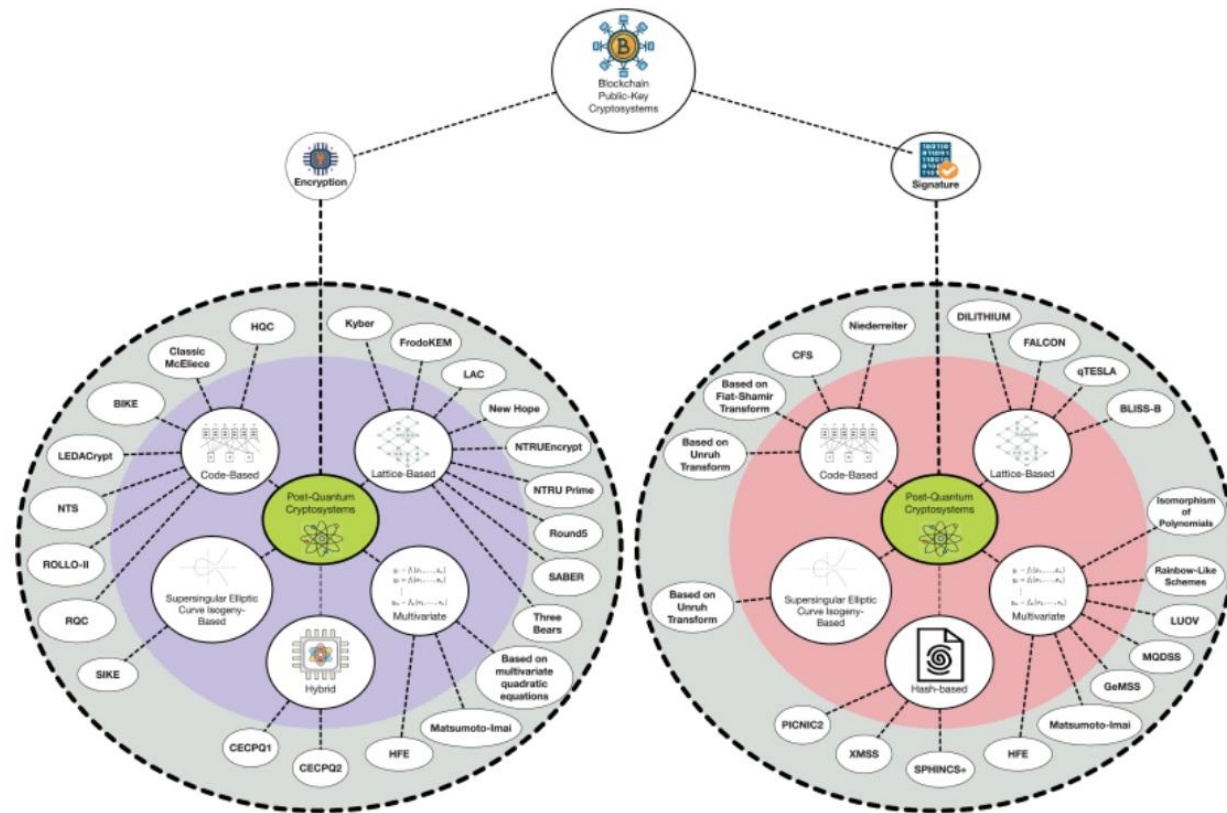
Crystals-Kyber

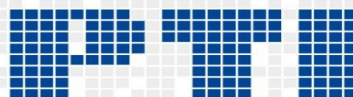
- competitive performance, relevant for many use cases
- based on structured lattices problems
- relatively simple design

FrodoKEM

- more conservative variant (based on an unstructured lattice problem)
- simple design as well

Postkwantowa taksonomia kryptosystemu klucza publicznego i główne praktyczne implementacje





POLSKIE TOWARZYSTWO INFORMATYCZNE

Country	PQC Algorithms Under Consideration	Published Guidance	Timeline (summary)
Australia	NIST	CTPCO (2023)	Start planning; early implementation 2025-2026
Canada	NIST	Cyber Centre (2021)	Start planning; impl. from 2025
China	China Specific	CACR (2020)	Start Planning
European Commission	NIST	ENISA (2022)	Start planning and mitigation
France	NIST (but not restricted to)	ANSSI (2022, 2023)	Start planning; Transition from 2024
Germany	NIST (but not restricted to)	BSI (2022)	Start planning
Japan	Monitoring NIST	CRYPTREC	Start planning; initial timeline
Netherlands	AES, monitoring NIST, SPHINCS-256 and XMSS	NCSC (2023)	Draft action plan with timeframes
New Zealand	NIST	NZISM (2022)	Start planning
Singapore	Monitoring NIST	MCI (2022)	No timeline available
South Korea	KpqC	MSIT (2022)	Start competition First round (Nov. '22-Nov. '23)
United Kingdom	NIST	NCSC (2023)	Start planning; impl. from 2024
United States	NIST	CISA (2021, 2022, 2023) NIST (2023) NSA (2022, 2023) White House (2022)	Implementation 2023-2033

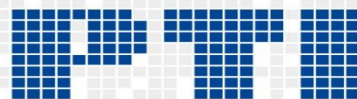
GSM Association. Post Quantum Cryptography – Guidelines for Telecom Use Cases Version 1.0 22 February 2024

Krypto zwinność

W miarę zbliżania się czasu na wdrożenie nowych algorytmów należy ustanowić wysoki poziom zwinności kryptograficznej w organizacji. Takie rozwiązanie będzie można wy/korzystać w klasycznej kryptografii, nawet jeśli kwantum nie stanie się uzasadnionym zagrożeniem

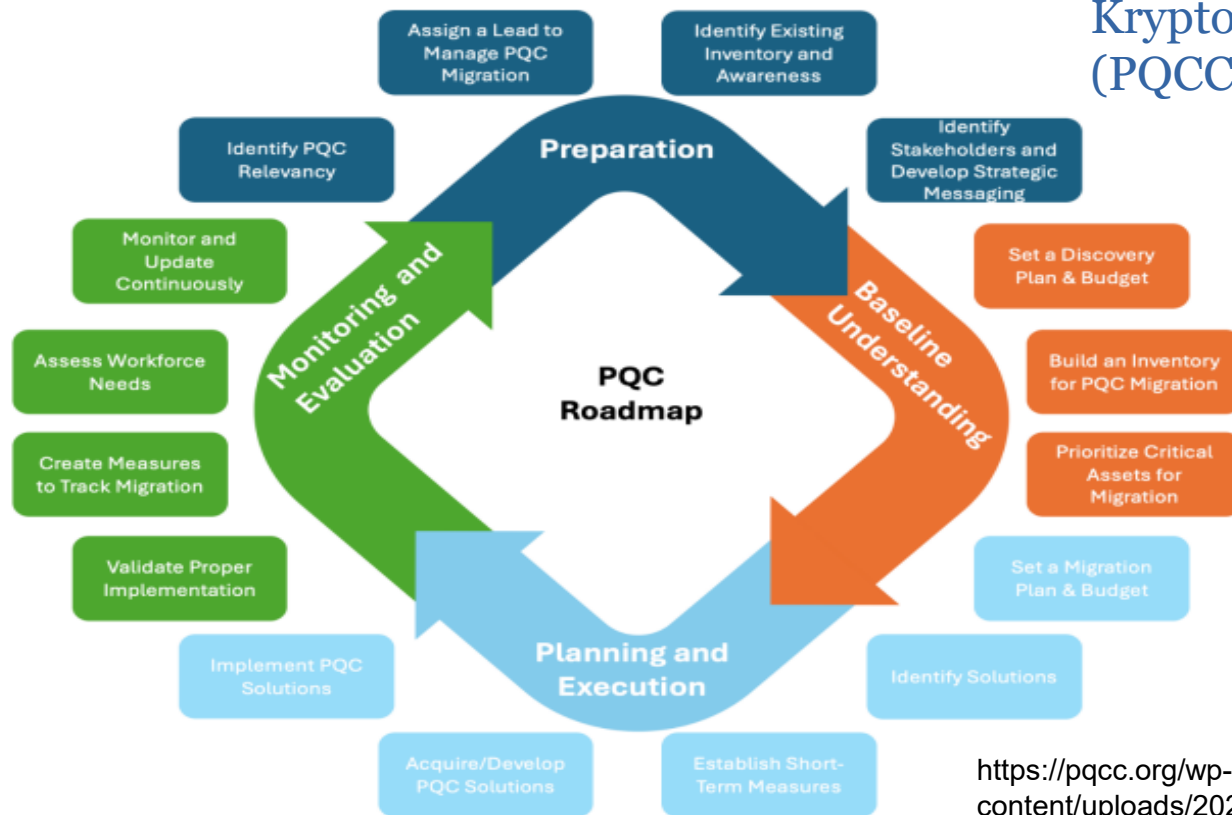
Skuteczna "zwinność kryptograficzna" obejmuje takie czynniki, jak:

- ▶ Posiadanie spisu kluczy, certyfikatów i algorytmów w użyciu.
- ▶ Automatyzacja i podział - aby lepiej móc wprowadzać zmiany i redukować skutki uboczne.
- ▶ Krótszy okres ważności - wymaganie elastyczności w produktach i rozwiązaniach.



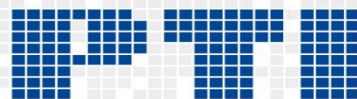
POLSKIE TOWARZYSTWO INFORMATYCZNE

Figure 1. PQC Roadmap Categories.



Koalicja na rzecz
Kryptografii Kwantowej
(PQCC)

<https://pqcc.org/wp-content/uploads/2025/05/PQC-Migration-Roadmap-PQCC-2.pdf>



POLSKIE TOWARZYSTWO INFORMATYCZNE



Examples of related programmes

- PKI evolution
- Crypto agility
- Hardware/software refresh cycles
- Technology refresh cycles and retirement of legacy capabilities
- Identity management refresh



Bardzo ważne jest, aby rozpocząć planowanie wymiany sprzętu, oprogramowania i usług wykorzystujących algorytmy klucza publicznego już teraz, aby informacje były chronione przed przyszłymi atakami.

Co należy zrobić?

Zidentyfikować wszelkie zastosowania potencjalnie podatnych na ataki algorytmów, którymi zarządzasz oraz ustalić, czy chronią one długoterminowe dane.

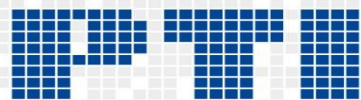
Oznacza to, że musisz zbadać czy stosujesz:

- algorytmy podatne na ataki: RSA, DSA, ECC, DH;
- protokoły zależne od tych podatnych algorytmów: TLS, SSH, S/MIME, PGP, IPSEC;
- VPN, Kerberos – protokoły, które mogą zależeć od tych podatnych algorytmów

Przeglądarki, poczta elektroniczna, szyfrowane wiadomości, szyfrowanie dysków, schematy uwierzytelniania – aplikacje, które (potencjalnie) wykorzystują te protokoły i podatne algorytmy

Zadania do wykonania:

- ✓ Upewnij się, że użytkownicy nie próbują chronić danych długoterminowych.
- ✓ Stwórz plan zastąpienia podatnych algorytmów algorytmami postkwantowymi, gdy tylko staną się dostępne. Priorytetowo traktuj te systemy, które przechowują lub przesyłają najbardziej poufne dane. Prawdopodobnie będzie to oznaczać aktualizację starych systemów operacyjnych, a może nawet starego sprzętu.
- ✓ Zidentyfikuj systemy, które nie są pod Twoją kontrolą (strony internetowe osób trzecich itp.) i zaplanuj, w jaki sposób możesz ograniczyć narażenie na ich systemy.



POLSKIE TOWARZYSTWO INFORMATYCZNE





gcenkier@proton.me