

Platforma Blockchain dla Rynku Kapitałowego

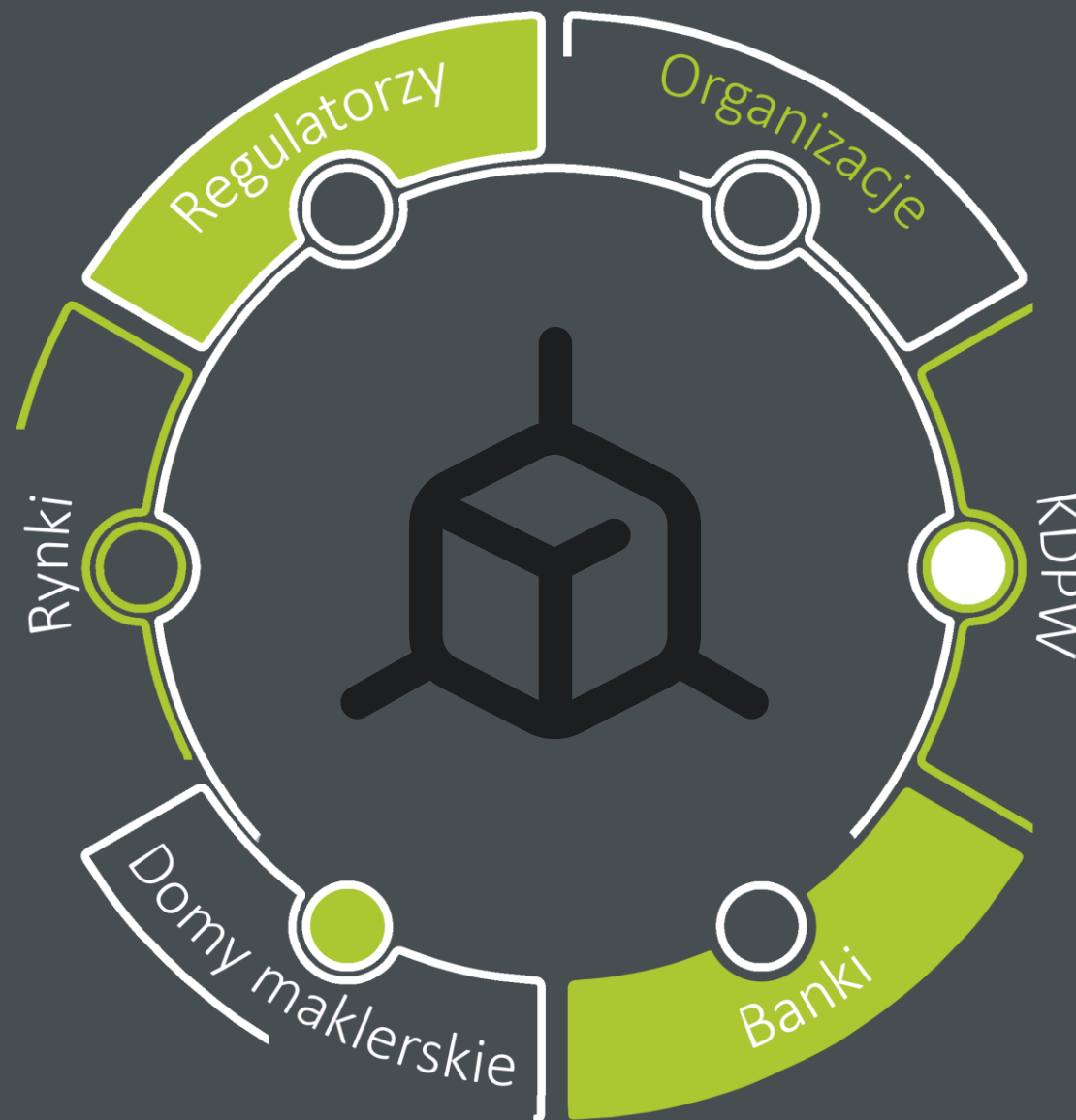
Spojrzenie technologiczne

Spotkanie
23 stycznia 2019

Innowacyjna, otwarta i w pełni
bezpieczna infrastruktura dla rynku
kapitałowego wspierająca rozwiązania
w obszarze usług posttransakcyjnych



Jako rozwiązanie sektorowe zapewnia wyższy poziom bezpieczeństwa i wzajemnego zaufania, co otwiera możliwości rozwoju innowacyjnych i efektywnych linii biznesowych.



Platforma jest otwarta dla różnych, zidentyfikowanych podmiotów, które mogą pełnić różne role w usługach biznesowych działających we współużytkowanym ekosystemie blockchain.

Klienci

Podmioty korzystające
z usług biznesowych

Procesy utrzymania

Standardowe zasady i
procedury zarządzania



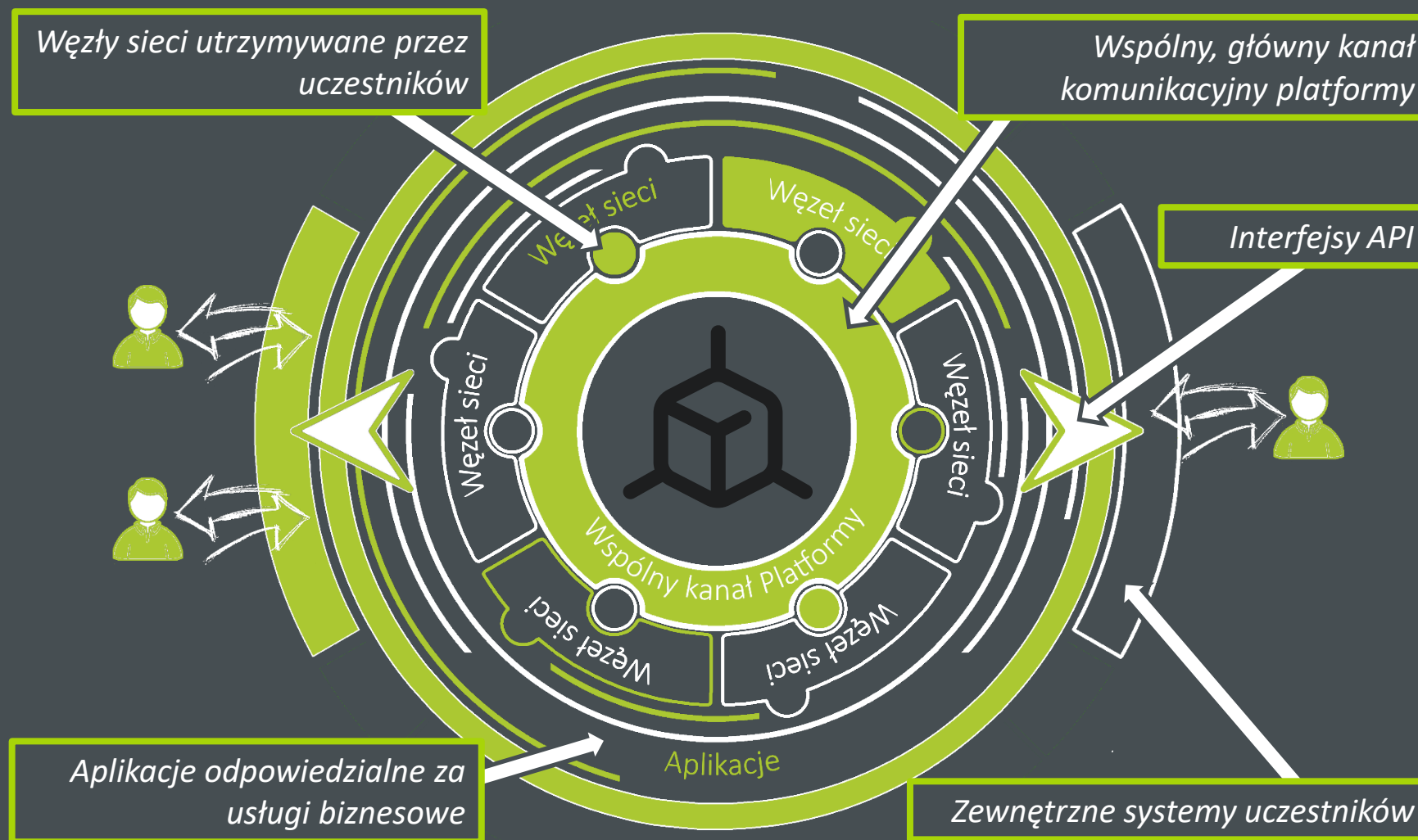
Aplikacje

Usługi biznesowe na
platformie

Uczestnicy platformy

Podmioty utrzymujące
infrastrukturę platformy

Infrastruktura platformy...



Wartości generowane przez Platformę



Niezaprzeczalność



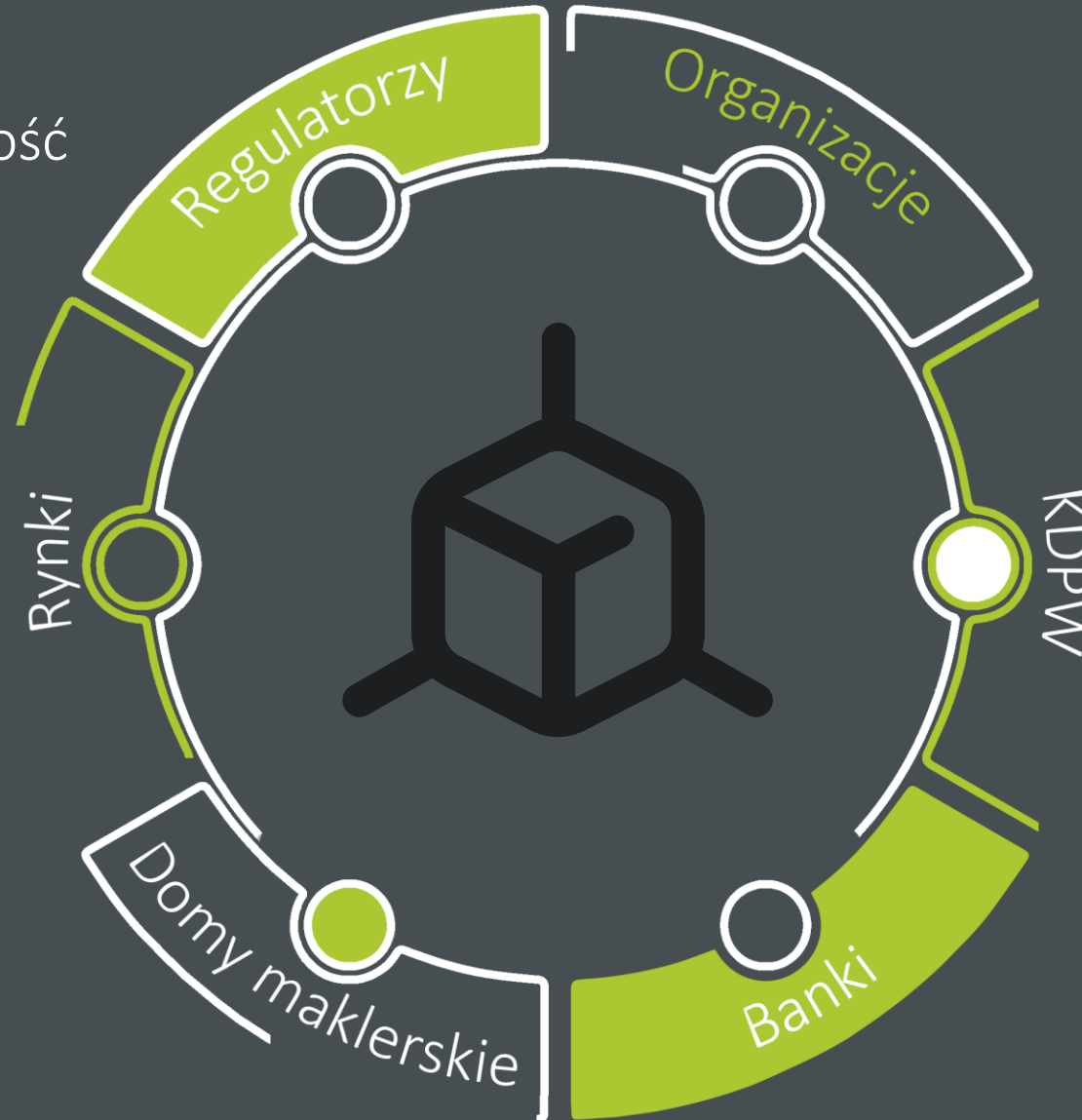
Zaufanie



Otwartość



Zarządzanie



Dostępność



Skalowalność



Poufność



Bezpieczeństwo



Wartości generowane przez Platformę



Niezaprzeczalność

Notaryzacja zdarzeń następuje w czasie rzeczywistym. Rejestry zdarzeń są chronione kryptograficznie przed wprowadzaniem późniejszych zmian.



Zaufanie

Wyeliminowana zostaje możliwość wpływu jednej ze stron na zawartość rejestru transakcji. W ramach sieci działają tylko zidentyfikowane i uwierzytelnione podmioty, które pełnią określone role według nadanych im uprawnień dostępu.



Otwartość

Stosowanie rozwiązań Open Source gwarantuje transparentność i swobodę doboru infrastruktury. Możliwość integracji z własnym systemem informatycznym.



Zarządzanie

Wspólny fundament konstrukcji systemu określa zasady funkcjonowania nowych aplikacji i upraszcza ich implementację.

Wartości generowane przez Platformę



Dostępność

Przechowywanie niezbędnych informacji w wielu lokalizacjach zapewnia stały dostęp do usług, nawet w przypadku awarii pojedynczych komponentów systemu.



Skalowalność

Możliwość szybkiego i skutecznego przyłączania nowych podmiotów. Im więcej węzłów, tym bardziej niezawodny staje się cały system.



Poufność

Wbudowane metody kryptografii, odizolowane kanały komunikacji oraz kontrola dostępu pozwalają na ograniczenie zasięgu informacji wyłącznie do podmiotów współpracujących w ramach danej usługi.



Bezpieczeństwo

Model rozproszony zwiększa poziom bezpieczeństwa przez szyfrowanie danych, odporność na awarie węzłów i uwierzytelnianie podmiotów na etapie przyłączania.

Platforma Blockchain dla zaawansowanych

(spojrzenie na techniczne aspekty dotyczące infrastruktury)



Logiczna architektura węzła sieci



Peer funkcjonujący w roli potwierdzającego transakcję – endorsing peer.



Peer funkcjonujący w roli utrzymującego kopię rejestru – committing peer.



Logiczna architektura węzła sieci



Bezpieczny kanał komunikacyjny, zapewniający komunikację pomiędzy wybranymi węzłami w ramach danej logiki biznesowej.



Logika biznesowa aplikacji – smart kontrakt. Komponent zawierający uruchomienie kodu w środowisku rozproszonym



Aktualny stan rejestru, tzw. World State, wykonany na podstawie ostatniej zmiany zarejestrowanej w systemie.



Pełny rejestr blockchain z transakcji oraz zdarzeń.



Logiczna architektura węzła sieci



Silnik API, służący do definiowania i uruchamiania interfejsów REST API służących integracji z systemami uczestników w kontekście danej aplikacji.



Aplikacja udostępniana klientowi. W zależności od rozwiązania komponent może reprezentować własne systemy uczestników platformy.



Komponent CA zarządza rolami i dystrybucją kluczy dla danej organizacji.



Oprogramowanie pozwalające na graficzną reprezentację stanu rejestru w ramach dostępnego kanału komunikacji.



Każdy komponent typu peer:

- Jest przyłączony do jednego lub większej liczby kanałów komunikacyjnych.
- Utrzymuje kopie rejestru blockchain dla każdego z kanałów komunikacyjnych.
- Utrzymuje zainstalowany kod smart kontraktu dla każdego z kanałów komunikacyjnych.
- Odpowiada za zarządzanie kontenerami dla zainicjowanych smart kontraktów dla każdego z kanałów.
- Utrzymuje lokalną kopię MSP (Membership Services Provider) zawierającą kopię materiałów kryptograficznych (certyfikatów).



Smart kontrakt – logika biznesowa

Każdy smart kontrakt tworzony w ramach Platformy reprezentuje logikę biznesową. Jest on:

- Instalowany w ramach komponentu typu peer oraz inicjowany w kontekście kanału komunikacyjnego.
- Uruchamiany w bezpiecznym kontenerze Docker niezależnym od kontenera, w ramach którego funkcjonuje sam peer.
- Posiada własną kopię bieżącego stanu rejestru (Worldstate)
- Implementuje dwie podstawowe metody:
 - `Init()`
 - `Invoke()`

Smart kontrakty mogą być tworzone w oparciu o następujące języki programowania:

- Golang
- Node.js
- Java (Future FAB-8063)



World State

World State stanowi rejestr ostatniej zmiany stanu w systemie odwzorowując aktualny stan rejestru

W ramach tworzonych rozwiązań może być stworzony przy wykorzystaniu baz danych levelDB lub CouchDB.

Pozwala na tworzenie zapisu danych w postaci publicznej, zaszyfrowanej (Chaincode Encryption) i poufnej (Private Data Collection)



Prywatne kolekcje danych - RODO

Dane zapisane w ramach prywatnej kolekcji są współdzielone z komponentami typu peer, które są wskazane w odpowiedniej polityce prywatności skojarzonej z daną kolekcją danych.

Peer, który nie jest wskazany w polityce nie ma dostępu do danych. Dane z prywatnej kolekcji nie trafiają także do usługi Orderer.

Są wyłączone z danych bezpośrednio zapisywanych z transakcjami i zastępowane są odpowiednią funkcją skrótu już na etapie przekazywania transakcji do potwierdzenia.

Stany rejestru głównego oraz prywatnych kolekcji utrzymywane są przez peer w sposób rozłączny.



Silnik API dla eVoting

Silnik API służy do definiowania i uruchamiania interfejsów REST API odpowiedzialnych za integrację z systemami uczestników w kontekście danej aplikacji.

Rodzaje API dla eVoting

- Meeting : Rejestracja i przebieg WZ
- Agenda : Agenda WZ
- Question: Pytania inwestorów i pełnomocników
- ISIN: Pobranie kodów ISIN
- Resolution: Uchwały WZ
- Voting: Głosowanie na WZ
- Eligibility List: Zarządzanie listą uprawnionych



Usługa szeregowania transakcji

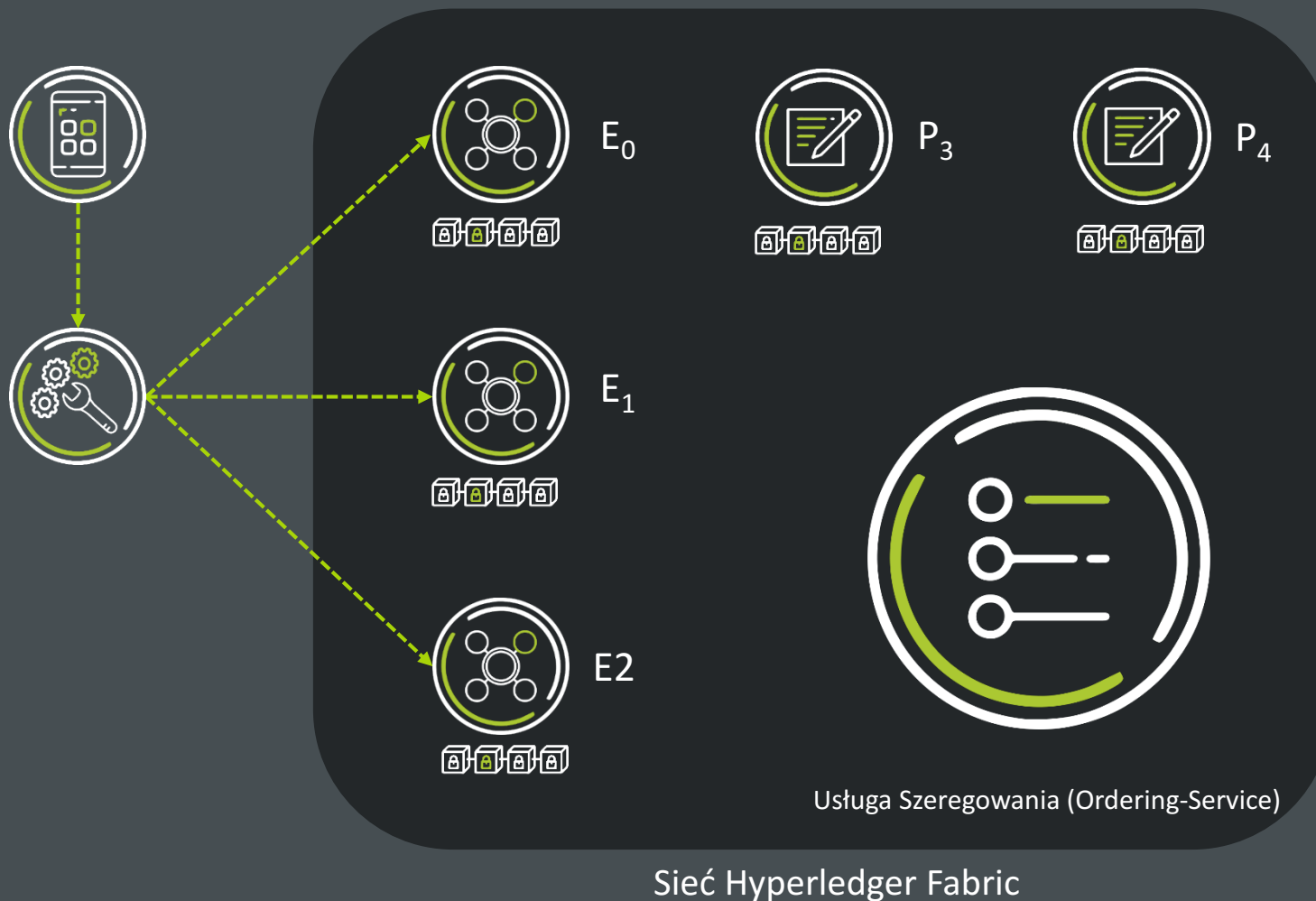
Usługa szeregowania (OSN) służy do porządkowania i sortowania przychodzących transakcji oraz odrzucania duplikatów.

Platforma Blockchain będzie wykorzystywać protokół konsensusu oparty o klaster Kafka/Zookeeper:

- 2 kontenery Orderer do przyjmowania i przetwarzania transakcji
- 6 kontenerów Kafka do zachowania fault-tolerancji
- 3 kontenery Zookeeper w roli świadka dla klastra Kafka



Potwierdzenie transakcji 1/7



Wysłanie propozycji transakcji

Polityka Endorsement:

- “E₀, E₁ oraz E₂ muszą podpisać transakcję”

Klient aplikacji wysyła propozycję transakcji z wykorzystaniem Chaincode . Propozycja musi zostać wysłana i podpisana przez peery węzłów organizacji {E₀, E₁, E₂}

Potwierdzanie transakcji 2/7



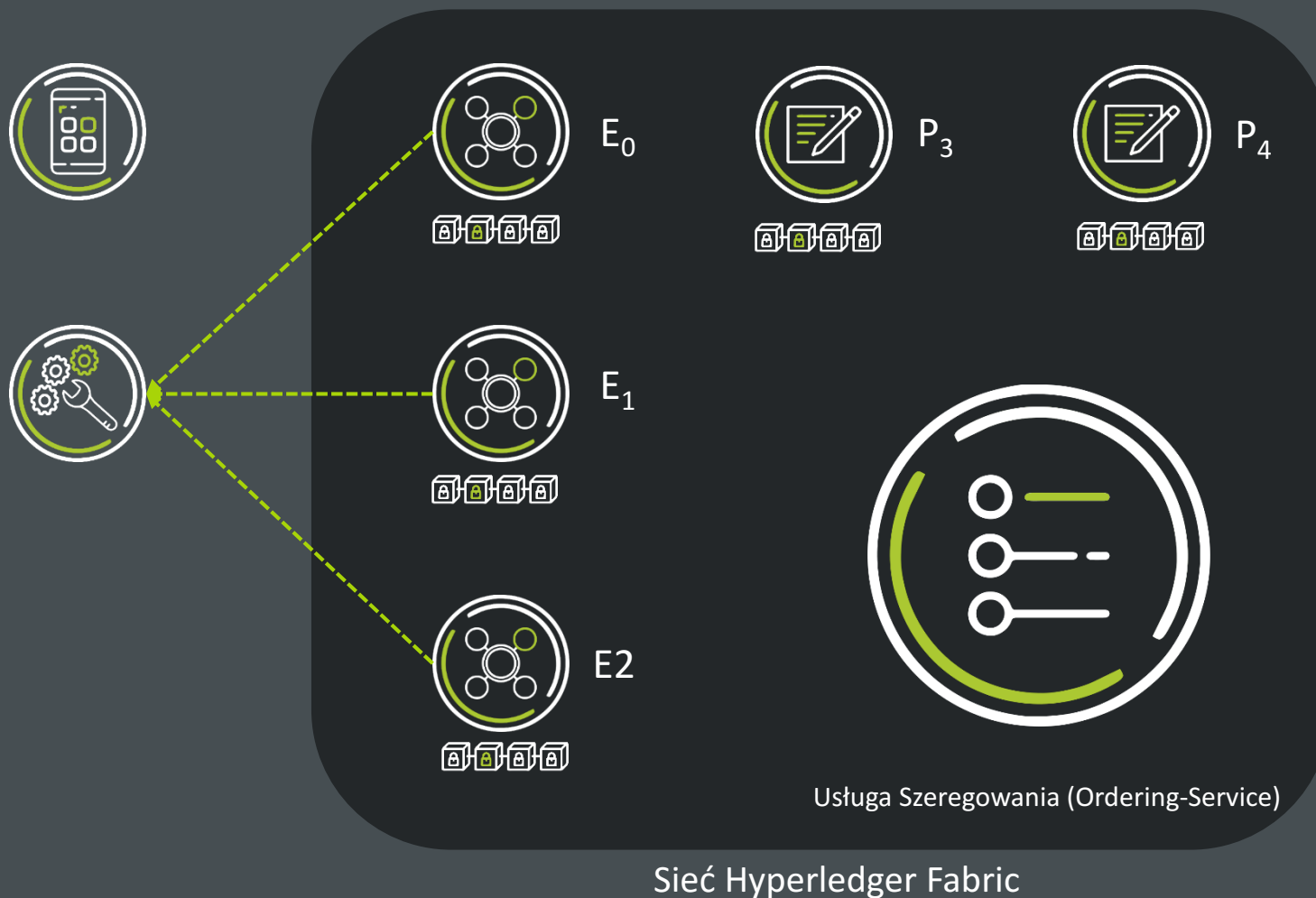
Sieć Hyperledger Fabric

Peery potwierdzające podpisują transakcję

E0, E1 & E2 indywidualnie wykonają propozycję transakcji bez aktualizacji lokalnej kopii rejestru

Każde wykonanie transakcji zarejestruje Read Sets (stan rejestru w momencie rozpoczęcia transakcji) i Write Sets (propozycja zmiany stanu rejestru w stosunku do stanu poprzedniego). Transakcje są podpisane cyfrowo.

Potwierdzenie transakcji 3/7

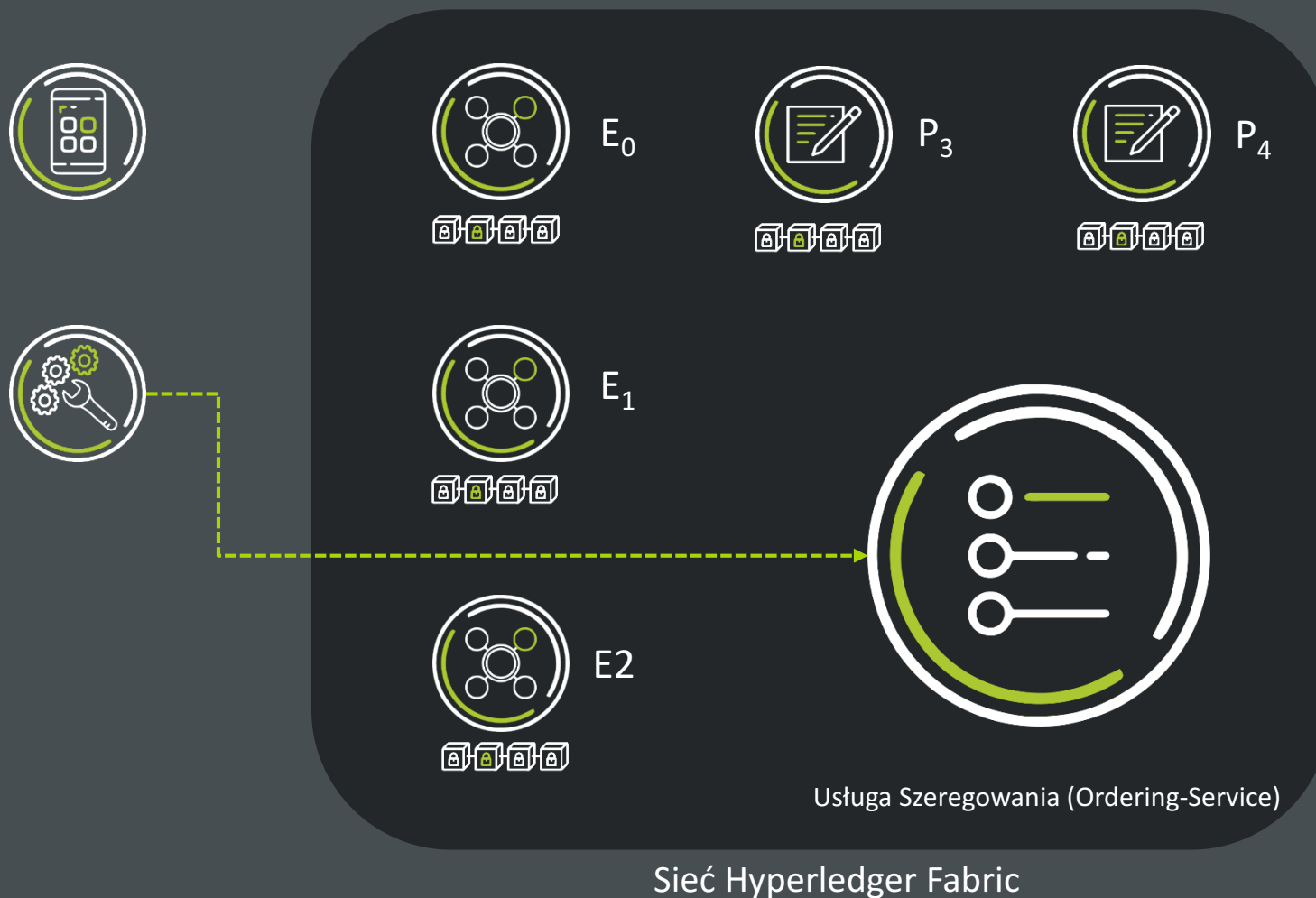


Aplikacja otrzymuje odpowiedzi

Aplikacja otrzymuje asynchronicznie Read Sets (stan rejestru w momencie rozpoczęcia transakcji) i Write Sets (propozycja zmiany stanu rejestru w stosunku do stanu poprzedniego)

Read Sets i Write Sets są podpisane przez każdego endorsera i zawierają numer wersji transakcji

Potwierdzenie transakcji 4/7

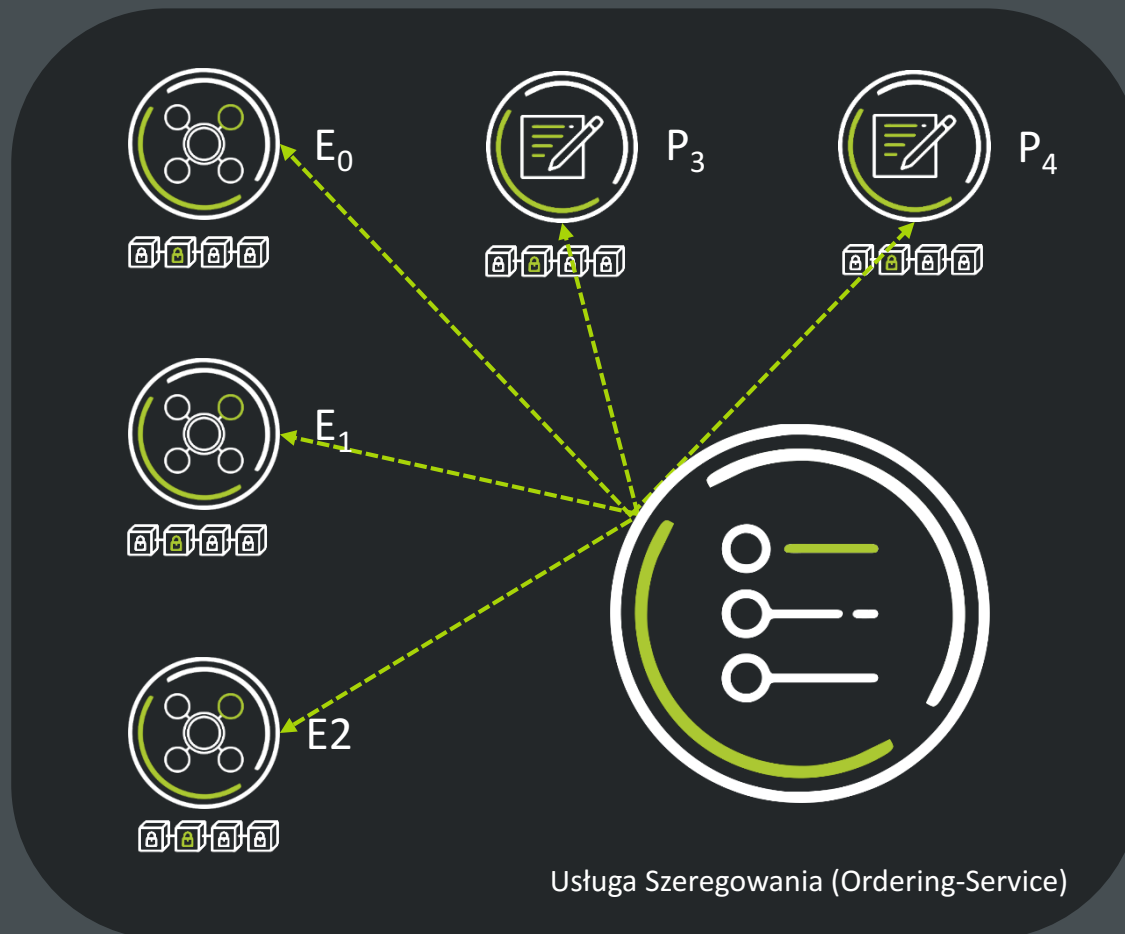


Odpowiedzi są wysyłane do Usługi Szeregowania

Aplikacja wysyła odpowiedzi w celu uszeregowania transakcji.

Uszeregowanie (ordering) odbywa się równocześnie z otrzymywaniem i przetwarzaniem kolejnych transakcji w ramach sieci opartej o Hyperledger Fabric.

Potwierdzenie transakcji 5/7

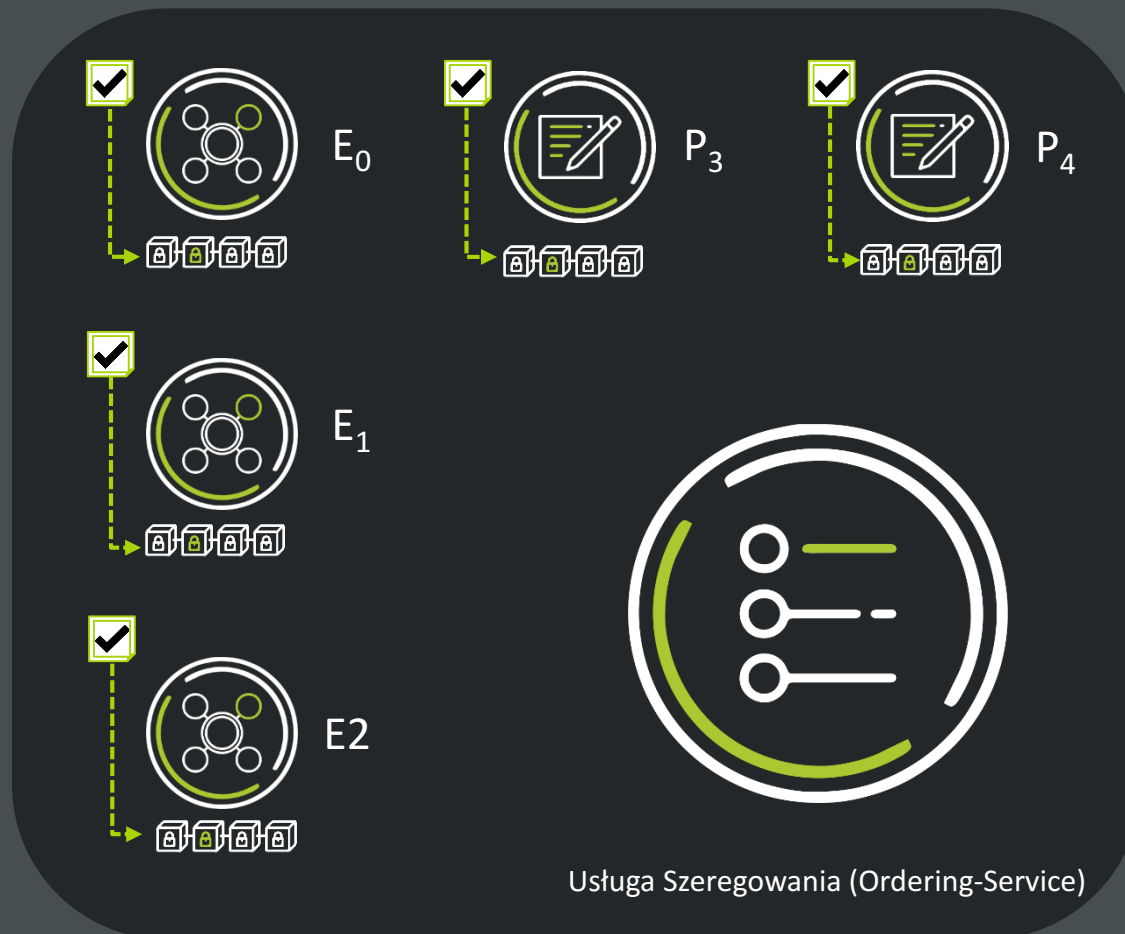


Sieć Hyperledger Fabric

Usługa szeregowania dostarcza posortowane transakcje do wszystkich Peerów

Usługa szeregowania odbiera transakcje i uporządkowuje je w bloki, w celu dalszej dystrybucji do węzłów organizacji, które są przeznaczone do roli walidatorów transakcji (committer).

Potwierdzenie transakcji 6/7



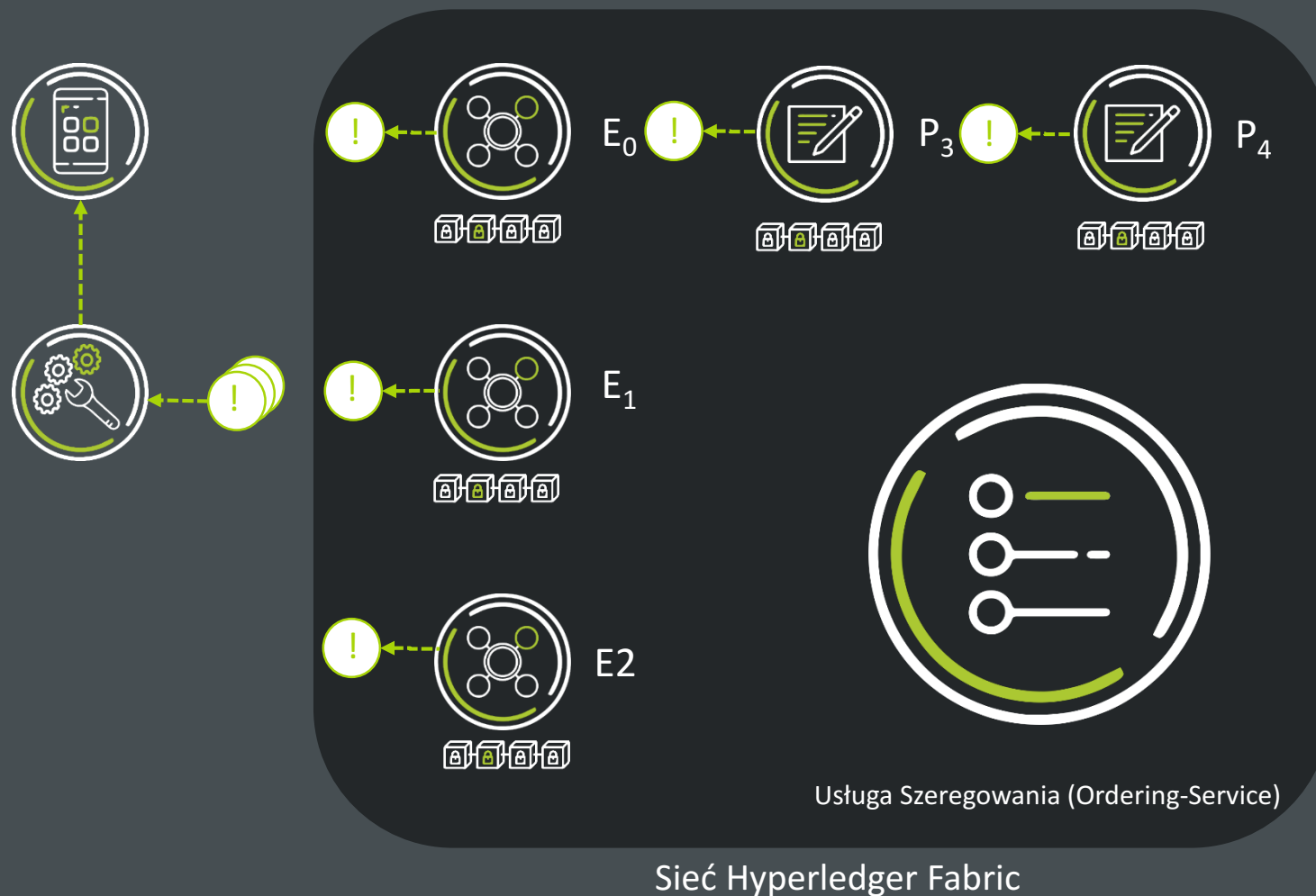
Sieć Hyperledger Fabric

Peery walidujące aprobuja transakcje

Każdy Peer posiadający status committera zatwierdza transakcję poprzez weryfikację, czy polityka endorsementu została wykonana oraz poprzez weryfikację, czy pierwotnie wykorzystanie Read Sety i Write Sety są nadal kompatybilne z aktualnym stanem rejestru.

Zaakceptowane transakcje są dodane do world state (stanu rejestru) i zapisane w lokalnej kopii rejestru (blockchain).

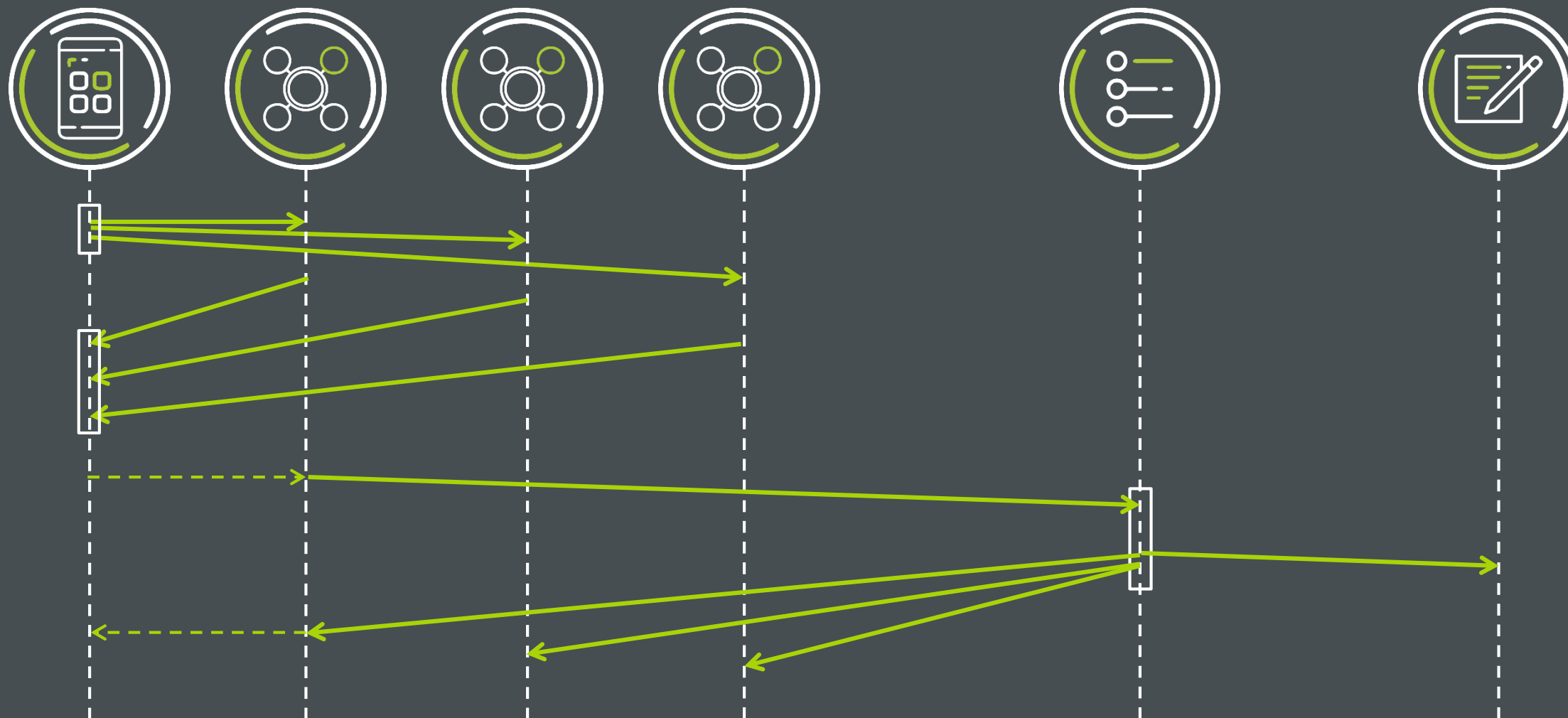
Potwierdzenie transakcji 7/7



Peery emitują zdarzenia do aplikacji

Aplikacje mogą zarejestrować informację o stanie transakcji oraz czy nowe bloki zostały dodane do lokalnej kopii rejestru.

Aplikację będą poinformowane przez każdego Peera, z którym mają połączenie.



Potwierdzanie transakcji – przykłady polityk.

Wymagane jest potwierdzenie od przedstawicieli wszystkich organizacji

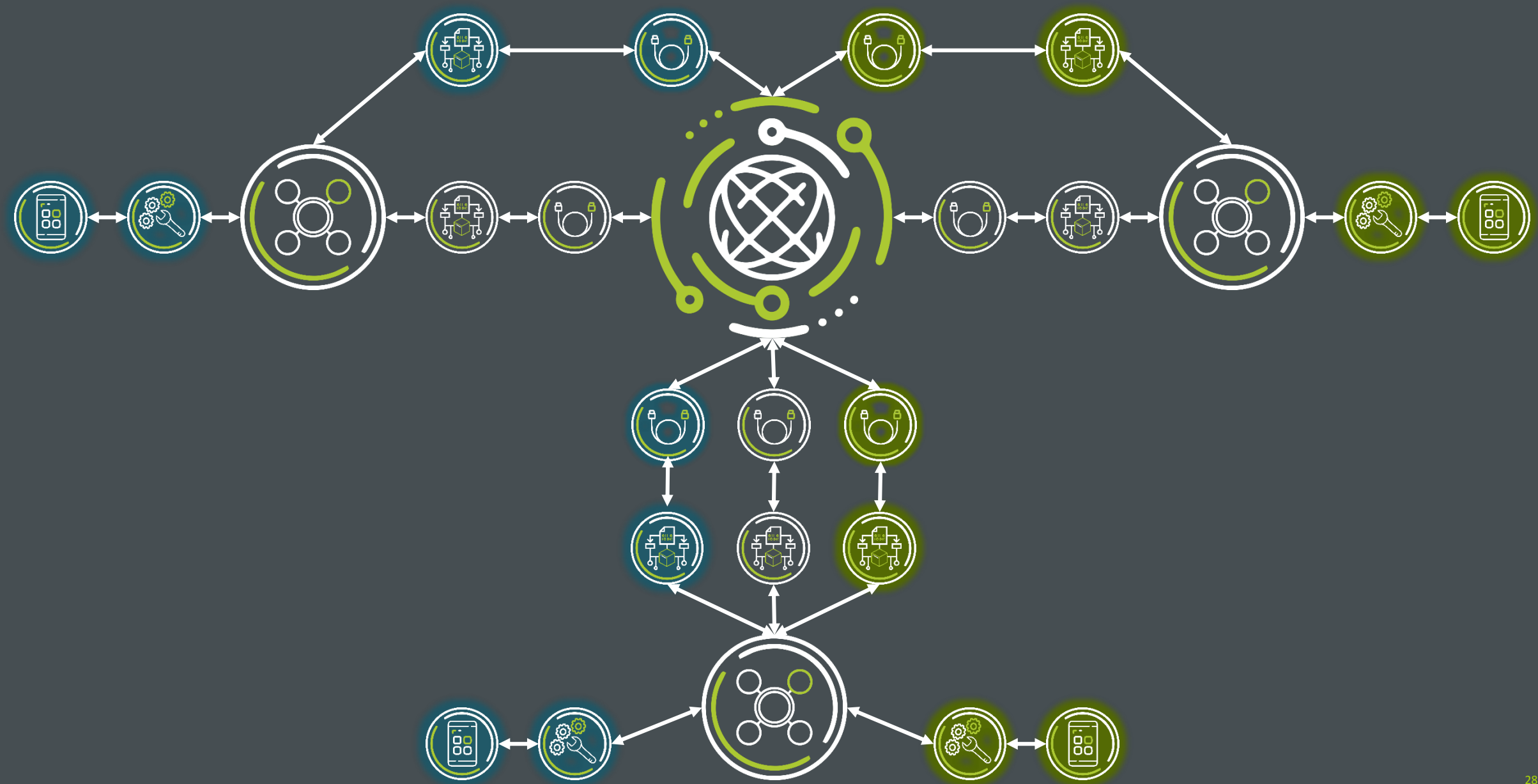
- `AND('Org1.member', 'Org2.member', 'Org3.member')`

Wymagane jest potwierdzenie od przynajmniej jednego z przedstawicieli spośród Organizacji 1 oraz Organizacji 2

- `OR('Org1.member', 'Org2.member')`

Wymagane potwierdzenie od przedstawiciela Organizacji 1 lub przynajmniej jednego potwierdzenia od przedstawiciela którejkolwiek z dwóch Organizacji spośród (Org2 i Org3)

- `OR('Org1.member', AND('Org2.member', 'Org3.member'))`



Centrum Certyfikacji Platformy

Serwer udostępniający usługę Centrum Certyfikacji dla komponentów Organizacji, dostosowaną do potrzeb Hyperledger Fabric:

- Możliwość konfiguracji ról Root CA i Intermediate CA
- Możliwość wykorzystania LDAP i HSM
- Możliwość wycofywania certyfikatów (CRL)

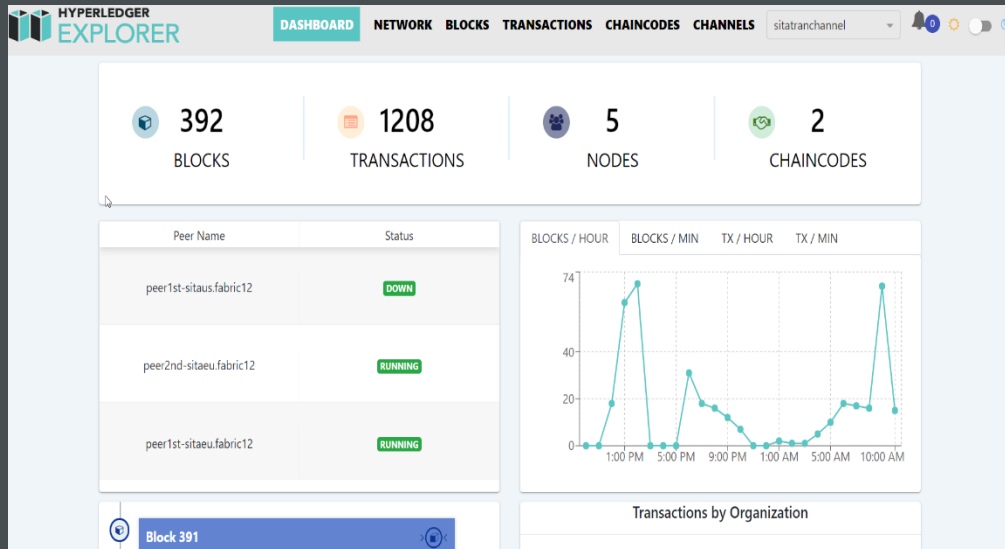
Wykorzystanie CA w sieci:

- Każdy komponent i uczestnik sieci posiada swój własny klucz prywatny oraz publiczny certyfikat (x509)
- Każda transakcja w Hyperledger Fabric jest podpisywana cyfrowo



Monitoring węzła

- Serwer udostępniający usługę Eksploratora Bloków
- Możliwość sprawdzenia aktualnego stanu rejestru, listy podłączonych organizacji, historii transakcji oraz zawartości bloków

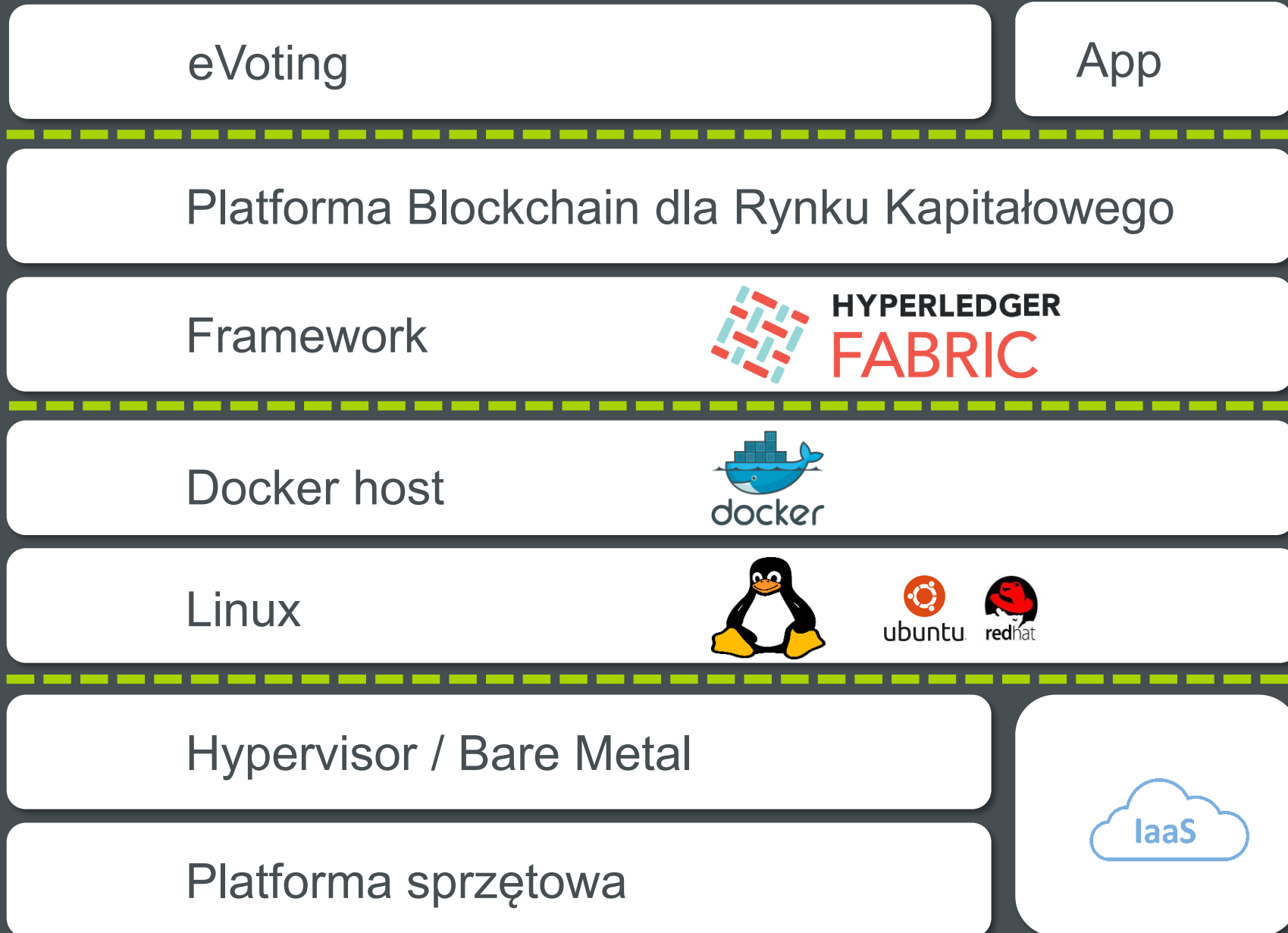


Platforma Blockchain

Infrastruktura fizyczna



Stos infrastruktury



Topologia sieci - Gwiazda

Etap I budowy sieci – topologia Gwiazdy

- Węzeł KDPW stanowi centralny punkt sieci.
- Wszystkie węzły połączone są jedynie z węzłem KDPW.
- Połączenie może być ustanowione jako P2P VPN.

Konsekwencje:

- Z uwagi na brak bezpośrednich połączeń pomiędzy poszczególnymi węzłami, KDPW może być jedyną instytucją potwierdzającą transakcje.



Topologia sieci – model rozproszony

Etap II budowy sieci – topologia rozproszona

- Węzeł KDPW nie stanowi centralnego punktu sieci.
- Wszystkie węzły połączone są wzajemnie ze sobą z wykorzystaniem sieci internet.
- Połączenie realizowane jest z wykorzystaniem TLS.
- Ruch wewnątrz sieci każdej z organizacji nie wymaga szyfrowania (decyzja o szyfrowaniu ruchu wewnętrznego może być podjęta niezależnie w każdej organizacji).



Parametry techniczne dla produkcyjnego Węzła Organizacji

Informacja	vCPU	CPU Ratio	RAM (GB)	HDD (GB)	Ilość (VM)
Sandbox	4	12	8	30	1
Stage-Standard-HTTP	2	12	4	20	2
Stage-Standard-API	8	8	8	20	2
Stage-Standard-CA	1	12	2	10	1
Stage-Standard-Peer	4	4	8	50	2
Prod-Standard-HTTP	2	8	4	20	2
Prod-Standard-API	8	8	8	20	2
Prod-Standard-CA	1	8	2	10	1
Prod-Standard-Peer	4	4	8	50	2

Parametry techniczne dla testowego Węzła Organizacji

Informacja	Opis	Uwagi
Hostname	VM-DLT-Prod-Org-Starter	---
OS	Dystrybucja Linux kompatybilna z Docker-CE 17.x i wyższym	---
vCPU	4	---
RAM	8	---
HDD	50	thin-provisioning
Wersja HLF	1.4 LTS	
Ilość organizacji	1	
Ilość węzłów per organizacja	1	
Ilość kanałów	2	
Rodzaj OSN	---	
Rodzaj CA	Fabric-CA	
TLS	Wyłączony (wewnątrz sieci)	Szyfrowanie TLS przez serwer Proxy organizacji
Firewall	out ALL / in 22, 443, 3000:3010, 5984, 6084, 8080/tcp.	

Węzeł Testowy vs Węzeł Produkcyjny

Cechy	Węzeł Testowy	Węzeł Produkcyjny
Ilość VMs	1	7
Ilość vCPUs	4 (vCPU:pCPU - 12:1)	15 (vCPU:pCPU - 4:1)
Ilość RAM	8 GB	22 GB
Ilość HDD	50 GB (HDD)	100 GB (SSD)
Redundancja	Brak	Klaster wysokiej dostępności, anti-affinity rules
Przeznaczenie	Testy funkcjonalne i symulacje testów pozafunkcjonalnych	Sandbox, Staging do pełnych testów pozafunkcjonalnych, wydajnościowych i przygotowania aplikacji, Prod pod rollout produkcyjny

Zapraszamy do Współpracy

- Możliwość tworzenia nowych usług biznesowych
- Zwiększony poziom wzajemnego zaufania oraz bezpieczeństwa i niezawodności infrastruktury Rynku
- Partnerstwo we wspieraniu innowacyjnych modeli usług biznesowych



Zapraszamy do Współpracy

Uruchomienie Platformy Blockchain wraz z pierwszą aplikacją zapewniającą obsługę Walnych Zgromadzeń wraz z eVoting.

połowa roku 2019

W przypadku chęci rozpoczęcia współpracy w fazie tworzenia infrastruktury testowej oraz chęci integracji z systemem eVoting (a także w obszarze tworzenia rozwiązań w innych obszarach) przed uruchomieniem produkcyjnym, zapraszamy do kontaktu.

blockchain@kdpw.pl

Szczegółowe informacje przed uruchomieniem rozwiązania będą przekazane z odpowiednim wyprzedzeniem.





Dziękuję za uwagę

<https://blockchain.kdpw.pl>

Rafał Wawrzyniak



rafal.wawrzyniak@kdpw.pl



www.linkedin.com/in/wawrzyniakrafal/