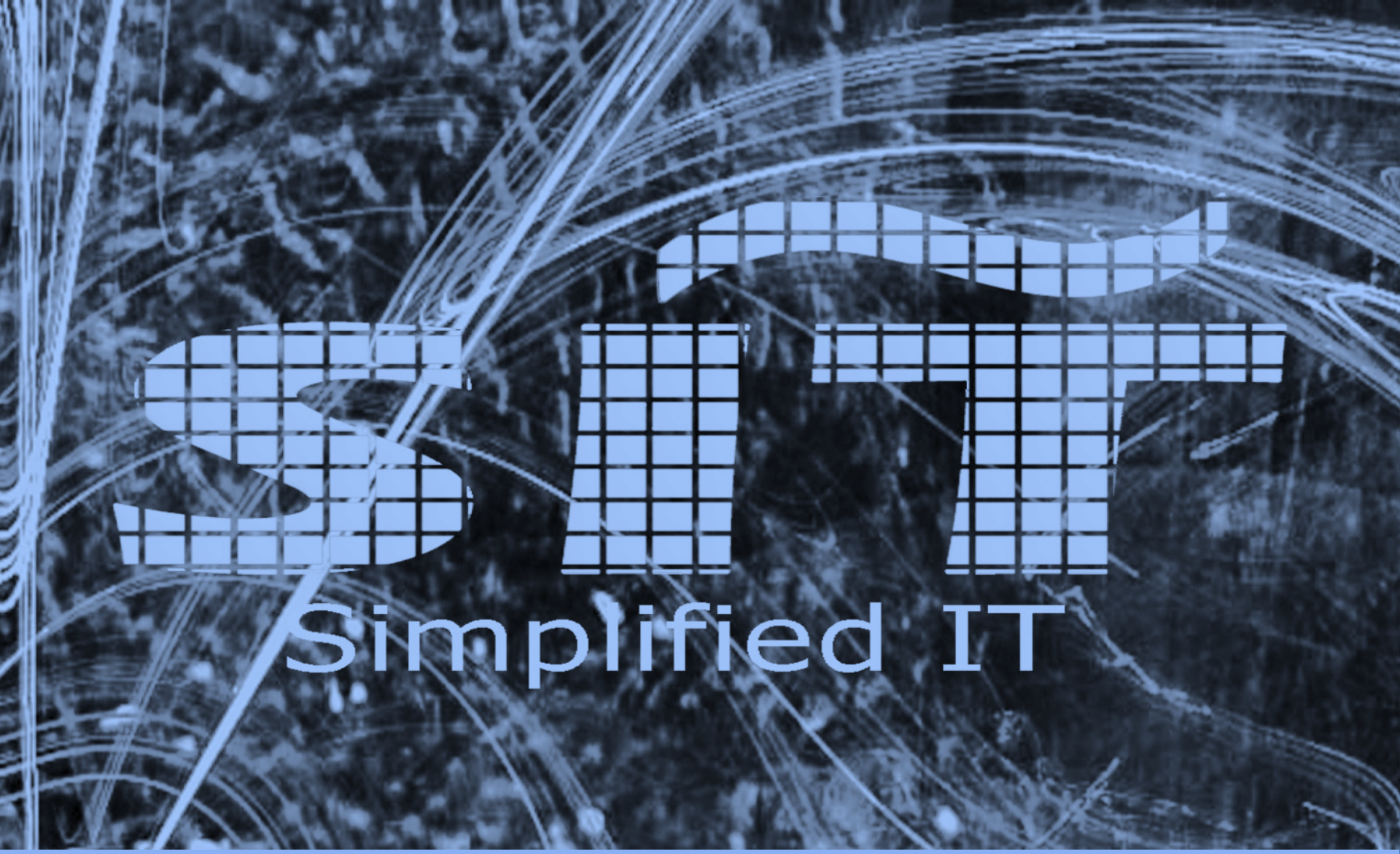
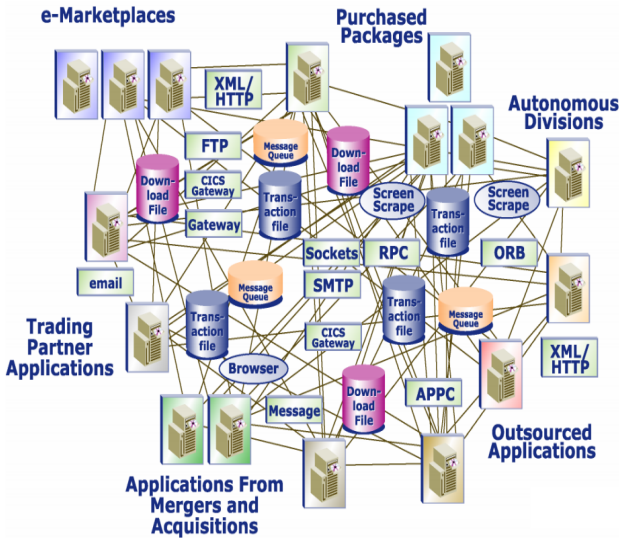


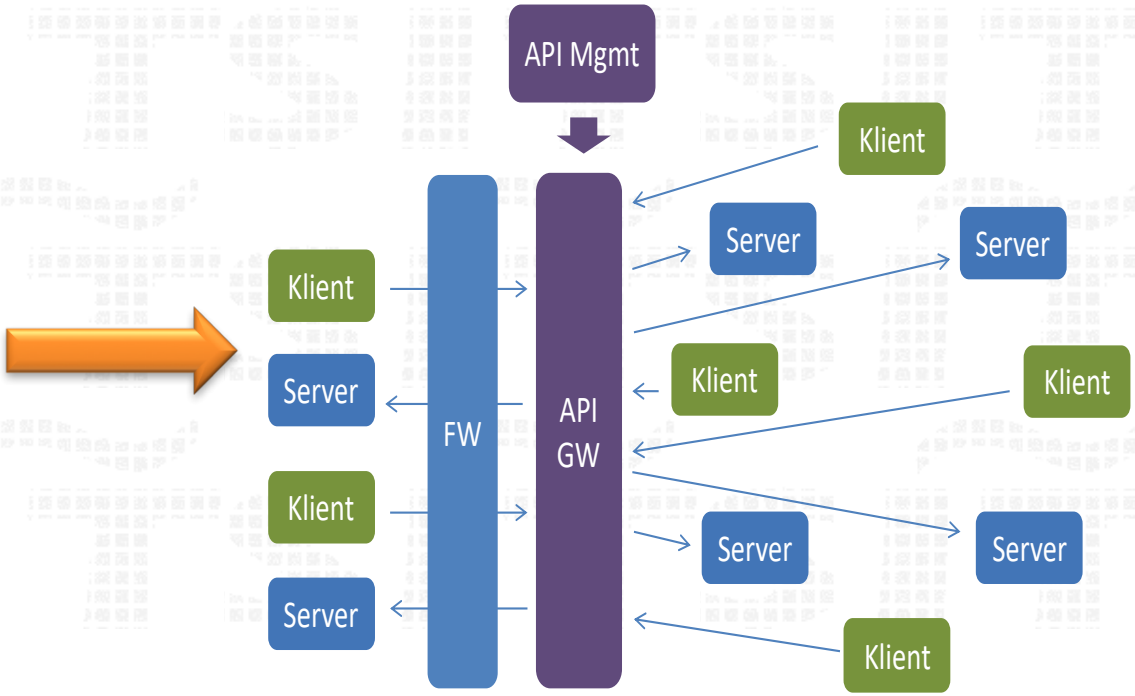
API Management a Blockchain

Proč zavádíme API ?

API představuje víc než ”Application Programming Interface”.
Je to nový způsob zavedení pořádku v datové komunikaci a způsobu jednání s klienty a partnery.

Enterprise Application “Spaghetti”





Jak zavedeme pořádek v datové komunikaci ?

API Gateway

- transparence datové komunikace, konzolidace protokolů a prostředí
- ověřování povoleného formátu dat – validace obsahu, ochrana proti hackingu
- podrobné trasování komunikačních problémů, rychlé nalezení chyby
- transformace protokolů (šetří náklady reimplementace klienta, serveru)
- arbitráž sporů mezi dodadavateli SW o chybách v datové v komunikaci
- řízení maximálního počtu požadavků, obrana před DDOS
- autentizace, autorizace, audit
- výkonnostní posílení, kešování

Podporované standardy and protokoly na enterprise API Gateway

Data format & language − JavaScript
- JSON
- JSON Schema
- REST, SOAP 1.1, 1.2
- WSDL 1.1
- XML 1.0
- XML Schema 1.0
- XPath 1.0, XPath 2.0 (XQuery only)
- XSLT 1.0
- XQuery 1.0, JSONiq

Security policy enforcement
- OAuth 2.0, OpenID Connect, Social Login
- JWE, JWS, JWT, JWK
- SAML 1.0/1.1/2.0, SAML Tkn Profile, SAML
- queries
- XACML 2.0
- Kerberos (including S4U2Self, S4U2Proxy)
- SPNEGO •
- RADIUS, RSA SecurID OTP using RADIUS
- LDAP versions 2 and 3
- Lightweight Third-Party Authentication
- Microsoft Active Directory
- FIPS 140-2 Level 3 (w/ optional HSM)
- FIPS 140-2 Level 1 (w/ certified crypto module)
- SAF & IBM RACF® integration with z/OS
- Internet Content Adaptation Protocol
- W3C XML Encryption
- W3C XML Signature
- S/MIME encryption and digital

Transport & connectivity
- HTTP , HTTP/2, HTTPS, WebSocket
- Proxy
- FTP , FTPS, SFTP
- WebSphere MQ
- WebSphere MQ File Transfer Edition
- TIBCO EMS
- WebSphere Java Message Service
- IBM IMS Connect, & IMS Callout
- NFS
- AS1, AS2, AS3, AS4, ebMS 2.0, CPPA 2.0, POP , SMTP (B2B Module)
- DB2, Microsoft SQL Server, Oracle, Sybase, IMS

Transport Layer Security
- TLS versions 1.0, 1.1, and 1.2
- SSL versions 2 and 3
- SNI, PFS, ECC Ciphers

Public key infrastructure (PKI)
- RSA, 3DES, DES, AES, SHA, X.509, CRLs, OCSP
- PKCS#1, PKCS#5, PKCS#7, PKCS#8, PKCS#10, PKCS#12
- XKMS for integration with Tivoli Security Policy Manager (TSPM)

Management
- Simple Network Management Protocol
- SYSLOG
- IPv4, IPv6

Web services
- WS-I Basic Profile 1.0, 1.1
- WS-I Simple SOAP Basic Profile
- WS-Policy Framework
- WS-Policy 1.2, 1.5
- WS-Trust 1.3
- WS-Addressing
- WS-Enumeration
- WS-Eventing
- WS-Notification
- Web Services Distributed Management
- WS-Management
- WS-I Attachments Profile
- SOAP Attachment Feature 1.2
- SOAP with Attachments (SwA)
- Direct Internet Message Encapsulation
- Multipurpose Internet Mail Extensions
- XML-binary Optimized Packaging (XOP)
- Message Transmission Optimization
- Mechanism (MTOM)
- WS-MediationPolicy (IBM standard)
- Universal Description, Discovery, and
- Integration (UDDI versions 2 and 3), UDDI
- version 3 subscription
- WebSphere Service Registry and
- Repository (WSRR)
-

API Bezpečnost

Authentizace a authorizace	Šifrování dat	Validace dat	Transport

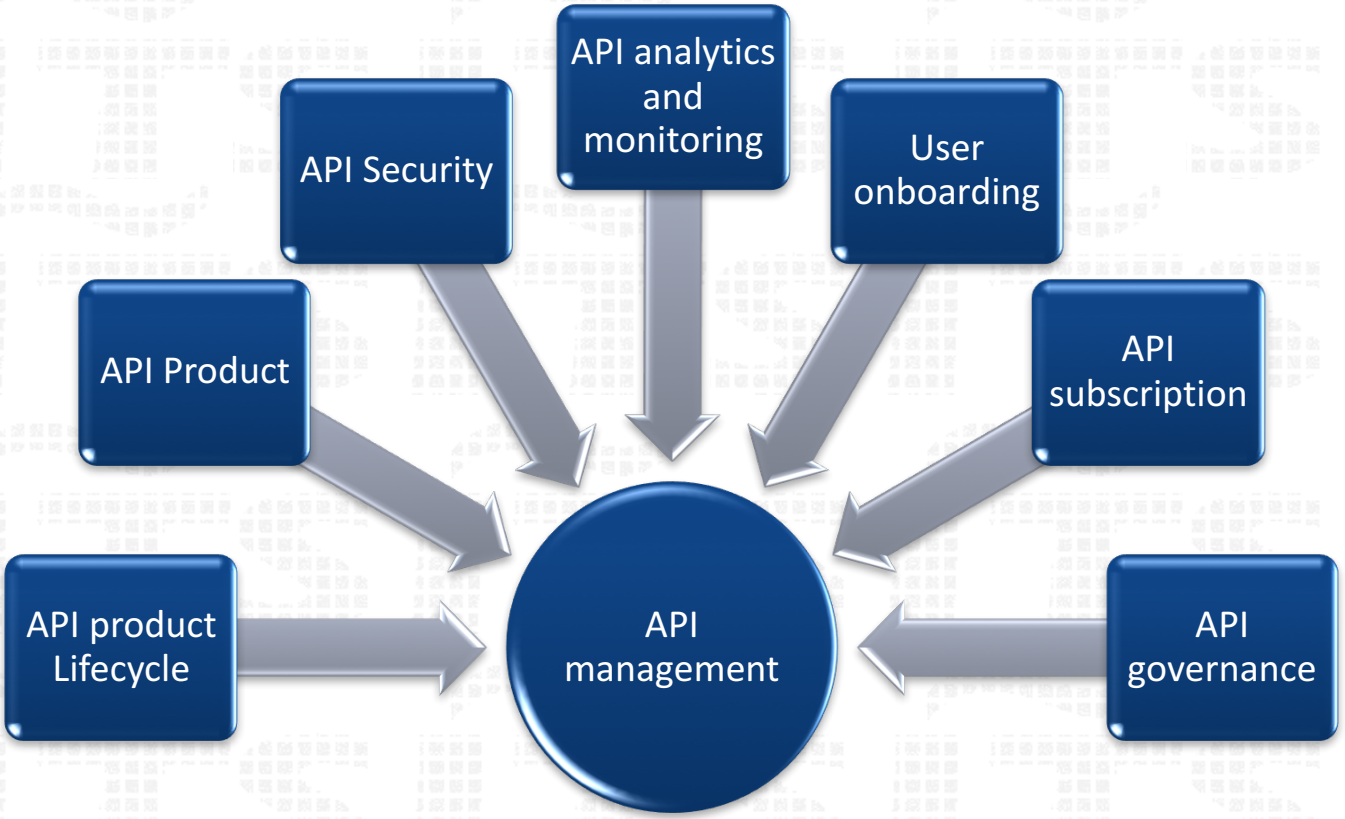
• API Keys:
  • Client id
  • Client Secret
• Klientský certifikát
• OAuth2
• WS-Security
• SAML
• Kerberos
• JWT
	• JWT	• JSON
		• XML
			• TLS v1.0, 1.1, 1.2
			• SSL v3
			• ECC Cipher
			• SNI, PFS

Jak budeme API rozhraní spravovat a monitorovat ?

API Management

- uživatelsky příjemná vyšší vrstva SW pro správu a řízení API Gateway
- přehlednost a konzolidace rozhraní API
- roztřídění a seskupení API na produkty, plány a katalogy
- uživatelsky komfortní vývoj API pro komunikci REST a SOAP
- online řízení dostupnosti API rozhraní
- dashboard, centrální monitoring, grafické statistiky
- řízení životního cyklu API
- jednotná autentizace, služby pro autorizaci

Management API - pojmy



Jak budeme API rozhraní dokumentovat a nabízet ?

API Developer Portál

- publikace dostupných rozhraní API
- dokumentace funkcí všech API
- vyhledávání API
- registrace uživatelů pro přístup k portálu
- registrace klientských aplikací pro užívání API
- účtování za služby

API Produkt

- Kolekce několika API:
  - Tvoří jeden související balík API
  - Společný produkt management
- Obsahuje vícero „plánů“
  - Počet příchozích volání za jednu časovou jednotku
  - Účtování za použití
- Verze produktu
  - Verze je nezávislá na verzích konkrétních API služeb.
- Viditelnost
  - Viditelnost na úrovni developer portálu
  - Kdo se může přihlásit k užívání

API Analytics and monitoring

Sběr analytik dle aplikace (client id)

Zabudovaný dashboard pro nahlížení

- Počet poslaných dotazů
- Response time
- Chyby

Napojeni na externí analytický nástroj

- Syslog
- Elasctic adapter

Monitoring

- Sběr monitorovacích a statistických událostí
- Zobrazení
- Napojeni na externí monitoring
  - Syslog
  - Elastic

Blockchain

- Blockchain je distribuované datové úložiště se zárukou nepozměnitelnosti dat a ukotvení času jejich vzniku a modifikací.
- Záruka je daná principy šifrovaného otisku dat, elektronického podpisu, časových razítek a vázaných seznamů datových bloků
- Blockchain se chová jako veřejný nebo privátní seznam (databáze, úložiště), kde jsou zaznamenány veškeré transakce a stavy evidovaných položek. Je to chronologický řetězec záznamů (bloků) o transakcích, který neustále roste a je sdílený mezi všemi uživateli – což znamená, že každý počítač zapojený do blockchain sítě dostane kopii záznamu
- základní entitou blockchain je „asset“ – evidovaná položka, dalšími jsou „transakce“ a u privátních síti „participant“ – „účastník transakce“

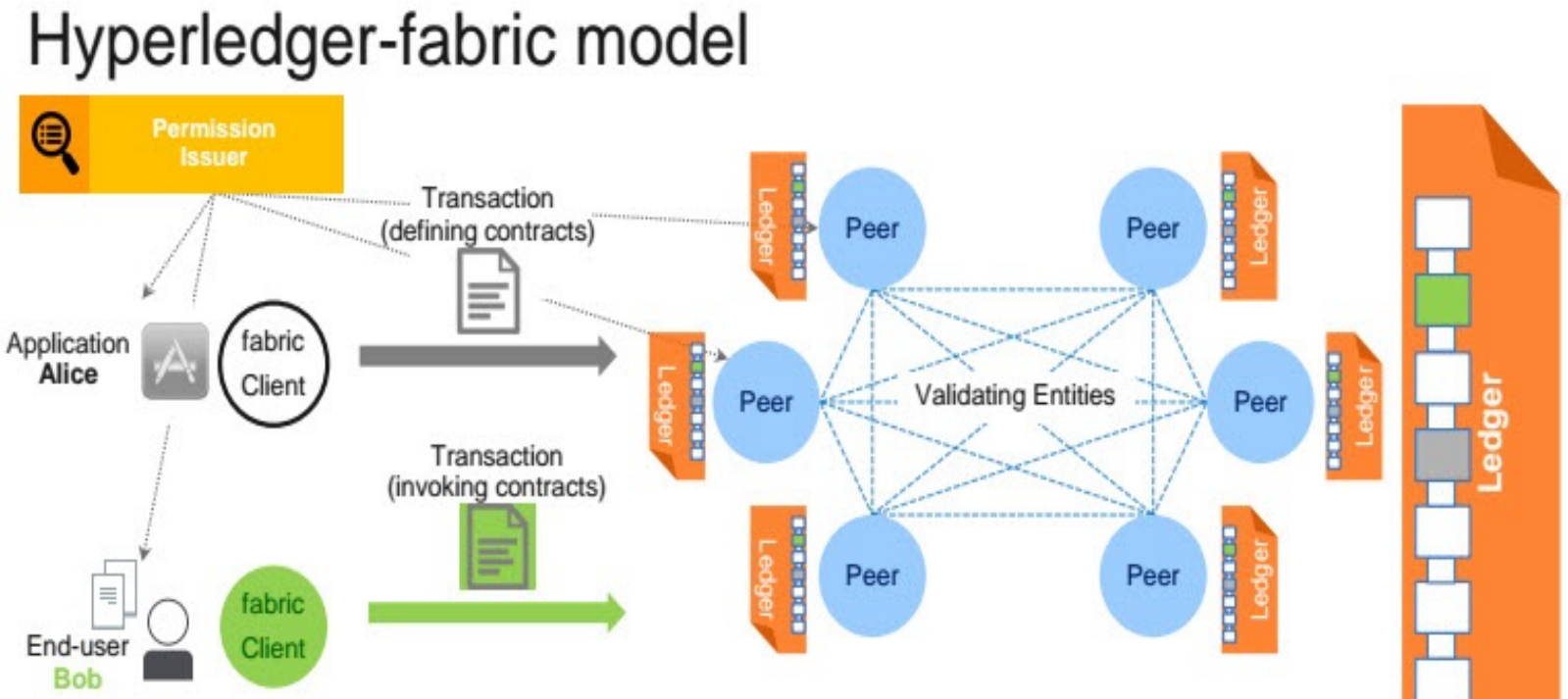
Virtuální příklad Blockchain - Zbrojnice

- Základní evidovanou položkou je „Zbraň“.
- Atributy položky : typ - „pistole, brokovnice, elektrický obušek, ..“, náboje – „počet“, dispozice „ano/ne“, sklad : „<kod_skladu>“, držitel : „<drzitel>, stav: „sklad, k vydání“, nový držitel: „<drzitel>“
- Účastníci - držitelé: „zbrojník“, „zbrojmistr“, „policista měst.“, „policista stát.“, „statistik“
- Transakce: „Výdej“, „Vrácení“, „Servis“, „Zařazení“, „Vyřazení“, „Výpis statistiky“
- Transakci manipulace provádí vždy : „držitel“, výpis může dělat „statistik“
- Blockchain má svoje uzlové servery umístěny na centrále a na skladech, všechny operace se zaznamenávají na všech serverech
- Operace výdejů a vrácení zbraně se zaznamenávají pomocí aplikace, ukládající data přes API do blockchain
- **Existují nezpochybnitelné záznamy, v jakém čase byla zbraň v čím držení. Garance jsou dány vědeckými zákony o datech, nikoliv garancemi výrobců SW či správci databází**

Blockchain – Hyperledger fabric

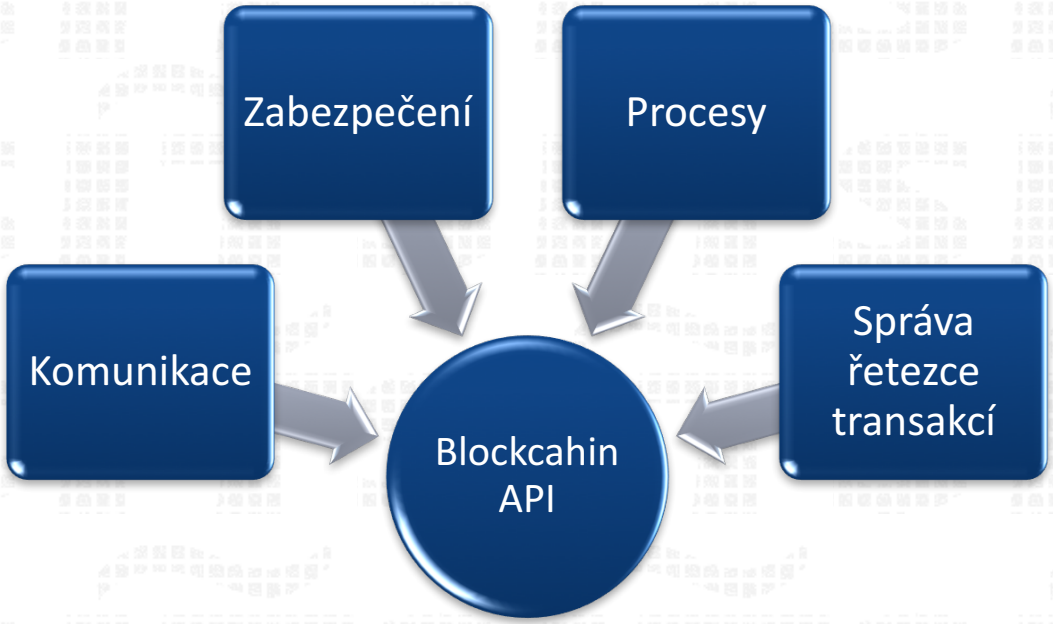
- Hyperledger fabric je otevřený framework pro zabezpečenou síť (permission network blockchain) s řízeným přístupem které transakce jsou viditelné pro každého člena
- Reprezentuje druhou generaci blockchain:
  - Škálovatelnost
  - Interoperabilita (společná součinnost)
  - Udržitelnost
  - Soukromí
  - Správa
  - Podpora smart contract (chaincode in hyperledger)

Hyperledger fabric



- **Permissioned** system; strong **identity management**
- Distinct roles of **users**, and **validators**
- Users **deploy** new pieces of code (chaincodes) and **invoke** them through **deploy** & **invoke** transactions
- Validators evaluate the effect of a transaction and reach consensus over the new version of the **ledger**
- **Ledger** = total order of transactions + hash (global state)
- **Pluggable consensus** protocol, currently PBFT & Sieve

Blockchain a API



Blockachain aplikace je obalena vrstvou API, které umožňuje vytvářet různé klientské aplikace pro práci s blockchain.

Blockchain API

- API management se z pohledu blockchain velice důležitou součástí.
- API vytvořené pro účely blockchain jsou dokumentované a dostupné přes developer portál.
- API gateway tvoří bezpečnostní bránu k blockchain databáze a k transakční logice.
- Tím že blockchain se rozšiřuje do různých lokací je nutné zvážit dostupnost API gateway.
- Hyperledger je administrován centrálně. Prostřednictvím administrativního API je možné vytvářet změny jako je přidání nové organizace.

Bezpečnost blockchain přístupné z API

- Blockchain představuje distribuovaný řetezec transakcí. Existuje několik **nezávislých** ale **stejných** reprezentací transakčního řetězce
- Znehodnocení či napadení jednoho řetězce neznamená ztrátu – nahradí se z jiné kopie
- Nicméně není dobré spoléhat na náhradu z jiného zdroje, ale měli bychom zabezpečit aby napadení bylo minimální