SMART DUBAI

BLOCKCHAIN PROTOCOL ANALYSIS AND IMPLEMENTATION

TABLE OF CONTENTS

DIFFERENTIATING ETHEREUM

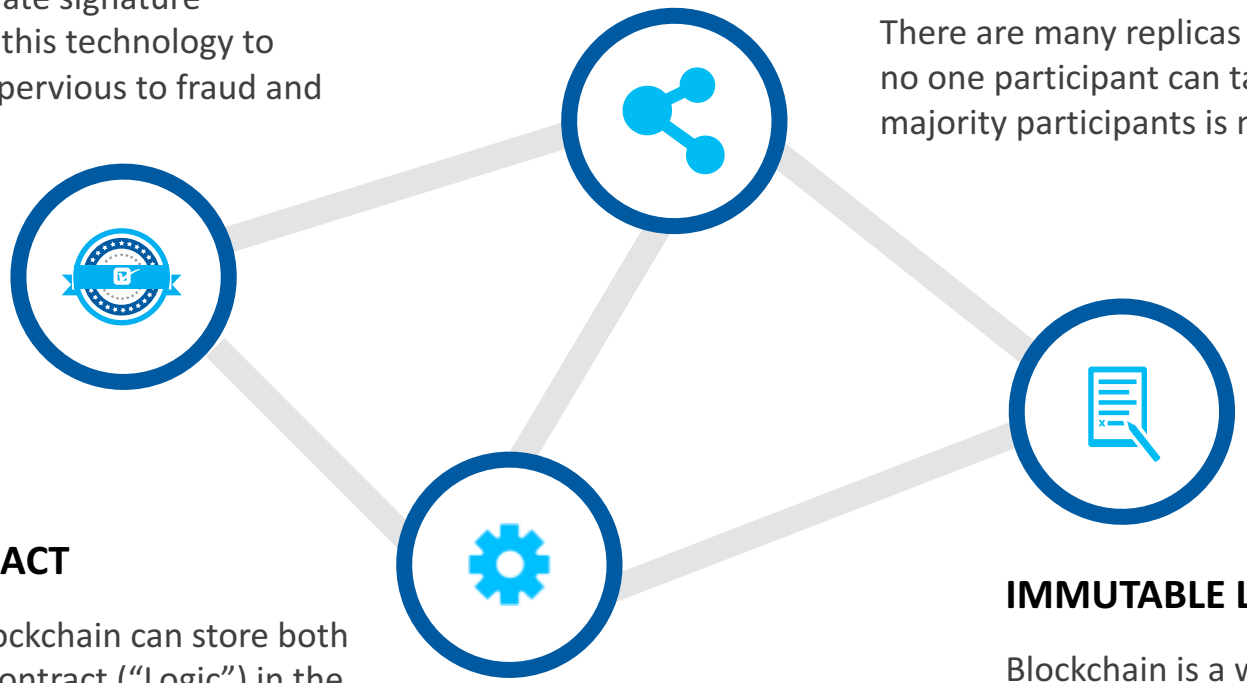
WHAT MAKES A BLOCKCHAIN DIFFERENT?

CRYPTOGRAPHICALLY SECURE

Uses tried and true public/ private signature technology. Blockchain applies this technology to create transactions that are impervious to fraud and establishes a shared truth.

DECENTRALIZED

There are many replicas of the blockchain database and no one participant can tamper it. Consensus among majority participants is needed to update the database.



SMART CONTRACT

The Ethereum blockchain can store both data and Smart Contract (“Logic”) in the blockchain

IMMUTABLE LEDGER

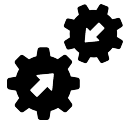
Blockchain is a write-once database so it records an immutable record of every transaction that occurs.

WHY IS ETHEREUM PRODUCTION READY?

Ethereum's unique combination of features distinguishes it as the clear leader amongst blockchain platforms

Formally specified security and smart contract capabilities

Vendor-neutral



Public – private blockchains compatibility

Private, permissioned blockchains for enterprise and government use cases

Rapidly growing community encompassing 30,000+ developers

Multi-billion dollars of value protected on the public network

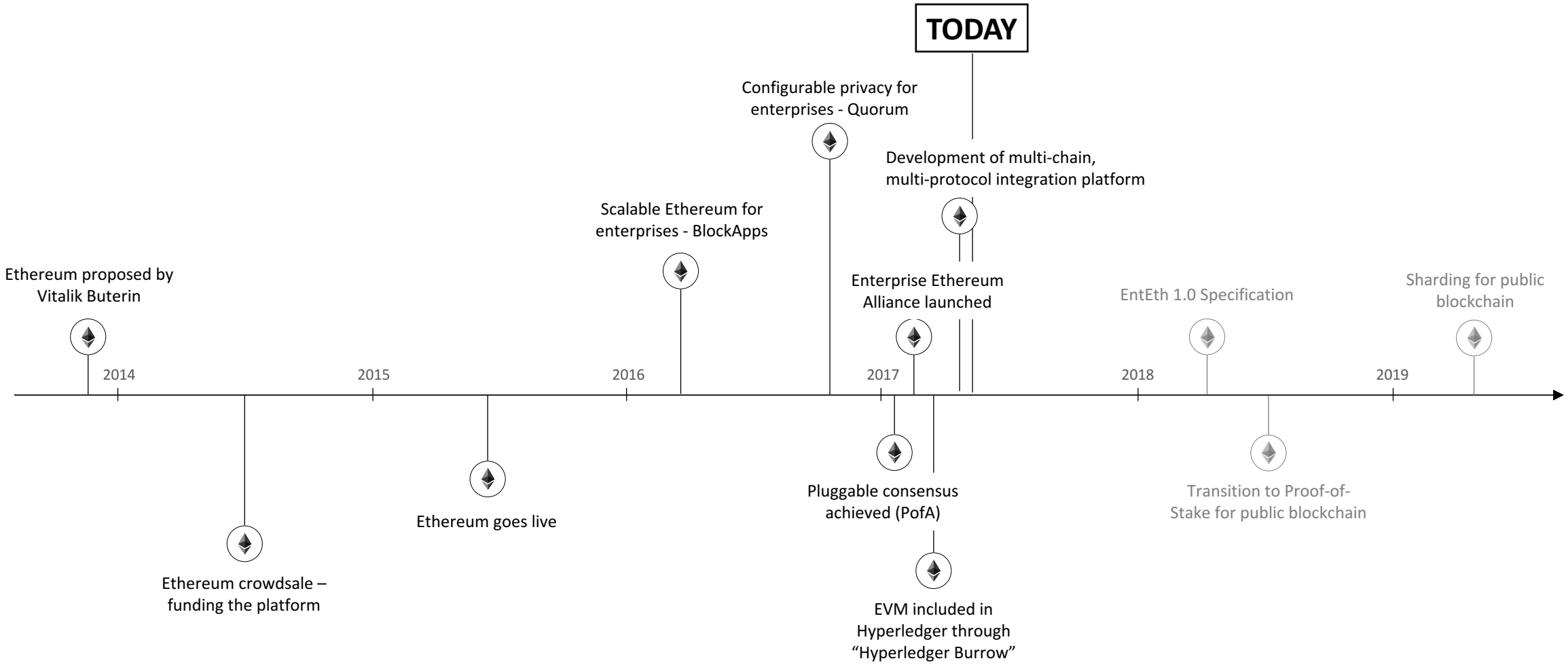
Enterprise Ethereum Alliance (EEA) is growing faster than all other blockchain consortia combined

The dominant platform for the 'token ecosystem'

In addition to its technical properties, Ethereum is developing a network effect that assures its longevity and continuing existence

ETHEREUM'S TIMELINE

Innovation is happening at a much faster pace as the ecosystem grows

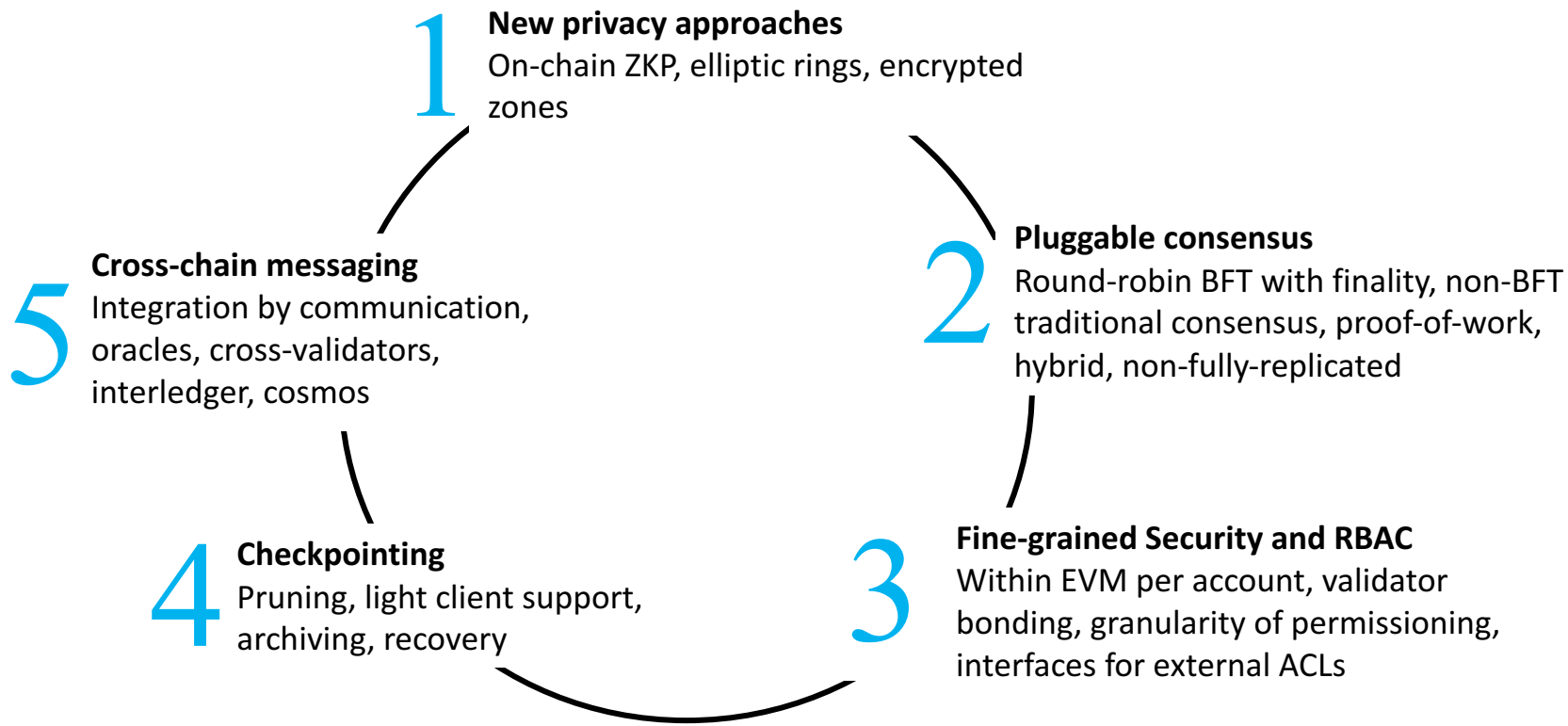


ETHEREUM'S ROADMAP

Ethereum continues to innovate at great pace and with a materially increased focus on enterprise requirements. Currently available, production Ethereum clients such as Parity and Geth support high performance consensus algorithms, while the core Ethereum roadmap includes adoption of proof-of-stake, sharding, and state channels

ENTERPRISE ETHEREUM ALLIANCE

The EEA is exploring next generation approaches to privacy, throughput and scalability including:



REAL WORLD EXAMPLES OF ETHEREUM IN ENTERPRISE PRODUCTION

PROVENANCE

BHP Biliton, the world's largest mining firm, is using blockchain to record movements of wellbore rock and fluid samples and better secure the real-time data that is generated during delivery. This will enable benefits for its internal efficiency while allowing it to work more effectively with partners.

OIL TRADING

ING and Société Générale built a platform, called Easy Trading Connect, designed for paperless trading and aims to digitize and standardize commodity transactions in order to increase speed and efficiencies in the trade process. The prototype is being used in a real trades.

CROSS-BORDER PAYMENTS

Santander has developed a cross-border payments application that is being piloted in production. The app connects to Apple Pay, where users can confirm payments securely using Touch ID. It lets users transfer between £10 and £10,000, and payments can be made from British pounds to euros and U.S. dollars

PRIVACY

JP Morgan has developed and deployed Quorum, an Enterprise-ready distributed ledger and smart contract platform. It is ideal for any application requiring high speed and high throughput processing of private transactions within a permissioned group of known participants.

THE BROADER ETHEREUM ECOSYSTEM

An Open-Source Platform for Innovation

oraclize

IPFS

uport

STABL

GNOSIS

BoardRoom

WeiFund

OTONOMOS

PROJECT OAKEN

INFURA

A Growing Global Talent Community

TRUFFLE

Ethereum Development Framework

60k downloads

as of April 25th, 2017

Expanding Catalog of

Online Ethereum Courses

udemy

Blockgeeks

B9lab Academy

DIGINOMICS

Increasing Developer Mindshare

Meetup

3.2k London	**2.3k** New York City	**2.0k** Silicon Valley
1.3k Zurich	**1.1k** Berlin	**1.3k** Singapore

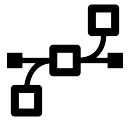
IMPLEMENTING BLOCKCHAIN IN DUBAI

RECOMMENDATIONS FOR DUBAI'S BLOCKCHAIN PRODUCTION ENVIRONMENT

When providing a specific recommendation for the Dubai Production Blockchain, we must consider the nuances in:

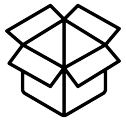
1. Timing considerations, based on the POC, Pilot, and Production model for the program
2. Trade-off between technology available today vs the roadmap
3. Availability of production infrastructure designed for blockchain deployments
4. Dubai specific requirements that we have discussed previously

With that in mind, we propose the following recommendations:



No Single Protocol

- It is highly unlikely that within Dubai or any other state we will see only a single protocol adopted because of risk mitigation, application availability, talent management and systems integration.
- Ethereum is one of a very small number of protocols capable of delivering Dubai's requirements

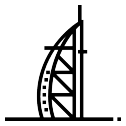


Use Available Software for POCs and Pilots

- Immediate POCs and Pilots should be developed using 'stock', generally available software, hosted on 'cloud sandboxes'.
- In the case of Ethereum, we would recommend clients such as Parity and Geth, which are frequently used to host public nodes and are also capable of running private, permissioned networks

Leverage Existing Cloud Infrastructure

- Leveraging the existing cloud infrastructure such as Microsoft Azure or IBM Bluemix, which already provide robust infrastructure for blockchain deployments, whether cloud, on-premise or hybrid.



A Dubai-specific, production blockchain infrastructure

- For the production system, a Dubai-specific, production blockchain infrastructure, which we will develop over 2017-2018.
- We will likely need to develop certain custom infrastructure, middleware and services to meet Dubai's multi-protocol interoperability, scalability, specific permissioning and identity requirements

INFRASTRUCTURE FOR BUILDING A PRODUCTION BLOCKCHAIN IN DUBAI

The infrastructure requirements and tools will vary and evolve as a blockchain solution moves from proof of concept to production and reaches its final stage of multi-protocol interoperability

Proof of Concepts

Centralized Governance & Op Model

- Clickable prototype that proves the idea/concept
- Deployed on external infrastructure, kept separate from existing systems

Production Pilots

Decentralized Governance & Op Model

- Limited release of a production system
- Focused Minimum Viable Product (MVP) that can be expanded into a full scale production system

Live Production Systems

Consortium Governance & Op Model

- Operational, enterprise-grade system with no critical defects
- Standalone or parallel system with integration to legacy systems

Interoperability - Dubai Blockchain

Consortium Governance & Op Model

- Multi-platform interoperability to allow for collaboration, connectivity and ecosystem expansion
- Full integration to legacy systems

INFRASTRCTURE

- Blockchain Sandboxes
- Development tools: Truffle, INFURA, etc.
- One-click deploy

- Production-grade blockchain infrastructure: tools for security, resilience, scaling, authentication, etc.
- Development tools: Truffle, INFURA, etc.
- Cloud platforms: Azure, AWS, Fabric, etc.

- Cross-chain multi-protocol Dubai-specific chain for long-term growth

APPLICATION DEVELOPMENT – SIMILARITIES AND DIFFERENCES IN THE STACK

Blockchain is just one piece of an application's technology stack. A great majority of existing popular frameworks and tools can be leveraged for development, with added customizations to harness the full power of a decentralized platform

Technology Stack	Traditional Stack	Ethereum Stack
	• UI layout and device specific design considerations	• Optional plugins for decentralized key management and identity management (e.g. Metamask, uPort)
Web Application / UI	• UI frameworks and tools like React, Redux, Angular, JQuery etc.	• Need for web3.js to interface with blockchain via RPC
Application / Business Logic	• Standard frameworks for business logic development	• Logic that needs to be in a trustless environment needs to be deployed as on-chain smart contracts
Data and Storage	• Traditional data modeling and stored procedures for logic • Application data and logic	• Logic and data programmed via smart contracts on chain • On-chain data and logic, off-chain data

APPLICATION DEVELOPMENT – FAMILIAR DEVELOPMENT ENVIRONMENT

Blockchain applications are developed using a great majority of existing popular tools, along with blockchain-specific tools that connect to the Web3.0 ecosystem

Technology Stack	Traditional Tools	Additional Ethereum Tools
		
Web Application / UI		• Web3.js  • Optional: 
Application / Business Logic		
Data and Storage		

METHODOLOGIES AND TOOLS FOR POCs

CREATING THE ETHEREUM SANDBOXES FOR POCs

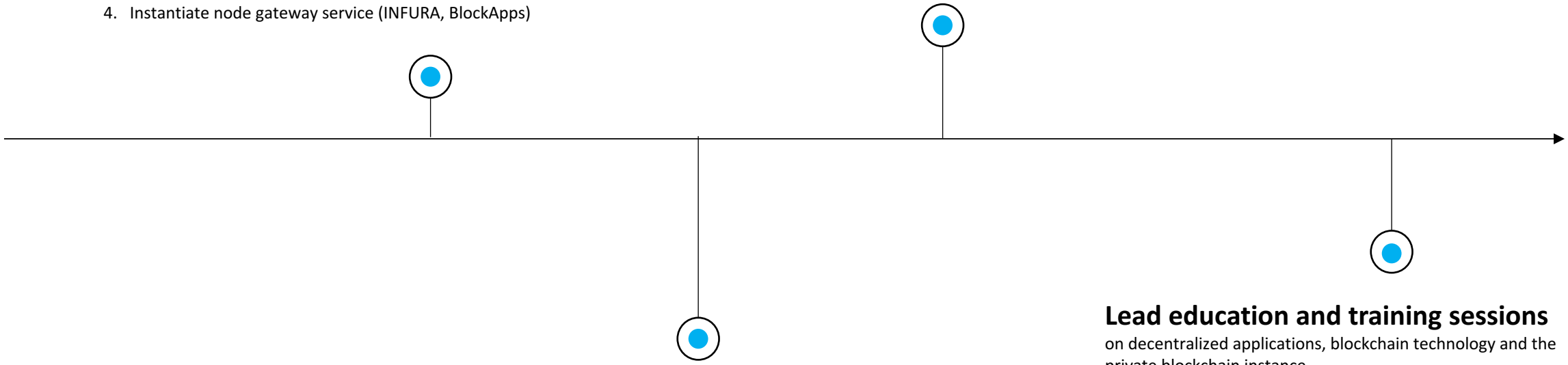
Creating blockchain sandboxes for the Proof of Concept stage will allow for rapid prototyping of ideas/concepts on both private and public chains through node hosting gateways and user-friendly development tools

Stand-up a single node private Ethereum based blockchain:

1. Initialize and configure cloud instance for building and running of Ethereum code
2. Initialize and build Ethereum client code on cloud instance node
3. Initialize and build compilers for smart contract languages (Solidity)
4. Instantiate node gateway service (INFURA, BlockApps)

Initialize the genesis block on the private Ethereum node:

1. Determine the initial amount of native tokens to be generated by genesis for clients' use based upon expectations for accrual heuristics; and
2. Create genesis JSON file mapping addresses from to their initial balances



Create private and public key pairs on the private node:

1. Generate initial set of client master keys for genesis issuance; and
2. Store private/public key pairs via Node gateway Key Server for ease of development

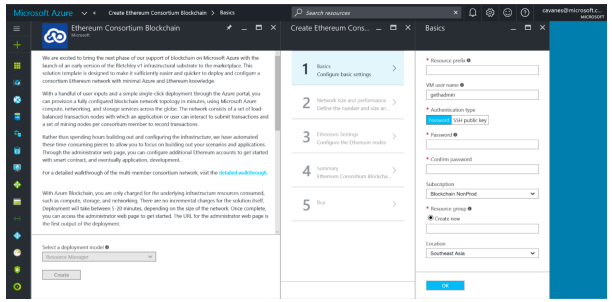
Lead education and training sessions

on decentralized applications, blockchain technology and the private blockchain instance

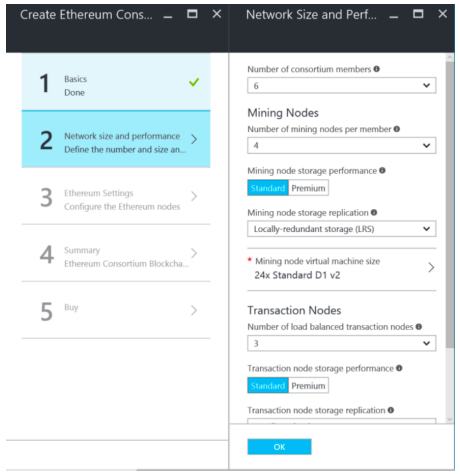
ONE-CLICK CLOUD DEPLOY

Launching an Ethereum blockchain sandbox is easy through the one-click deploy tools on cloud providers

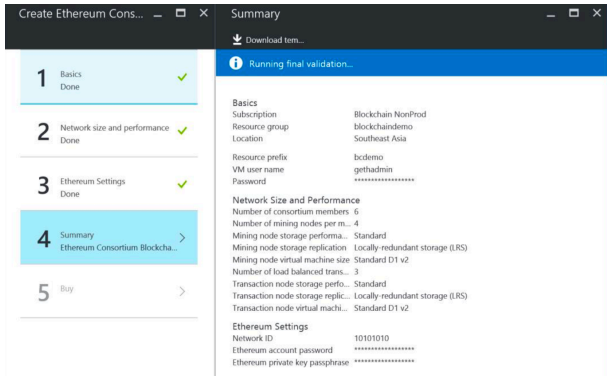
1 Create Ethereum template



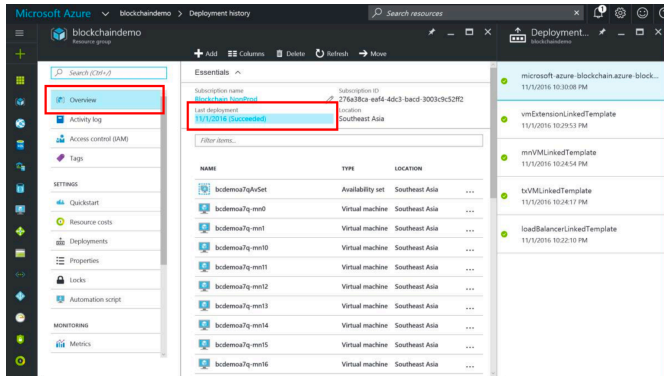
2 Fill out parameter details



3 Confirm configuration



4 Sandbox Deployed



PRODUCTION BLOCKCHAIN INFRASTRUCTURE – TRUFFLE

The Truffle dev-ops framework and development environment is used by Ethereum developers worldwide to write, test and deploy smart contract decentralized applications.

TRUFFLE

Ethereum Development Framework

Largest Blockchain Development Community Worldwide

60k downloads
as of April 25th, 2017

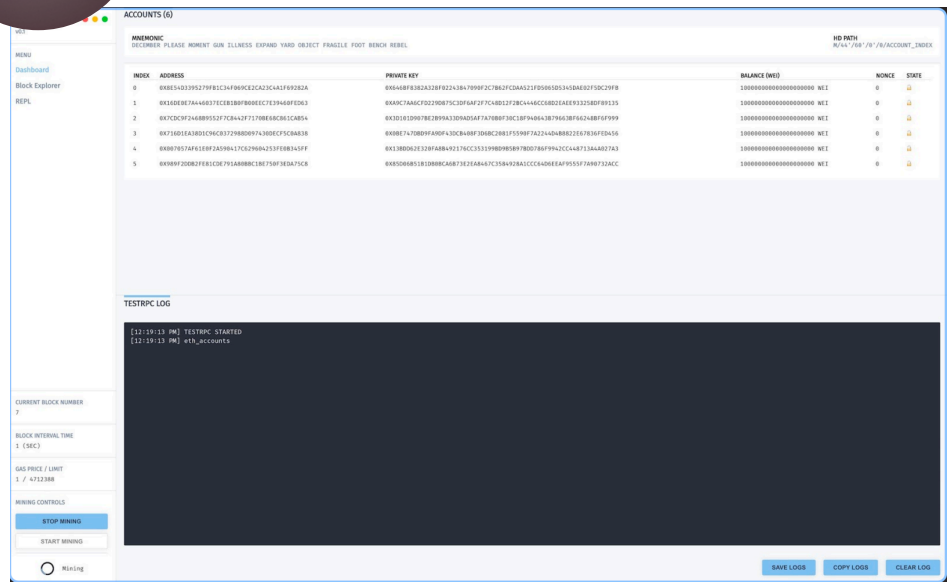
Mission

- Help developers build their decentralized vision by providing tools, practices, community and support.
- Make Ethereum development synonymous with Truffle

Core Features

- Professional-grade workflow and deployment tools for building complex smart-contract applications.
- Marriage of tools, community, documentation and support

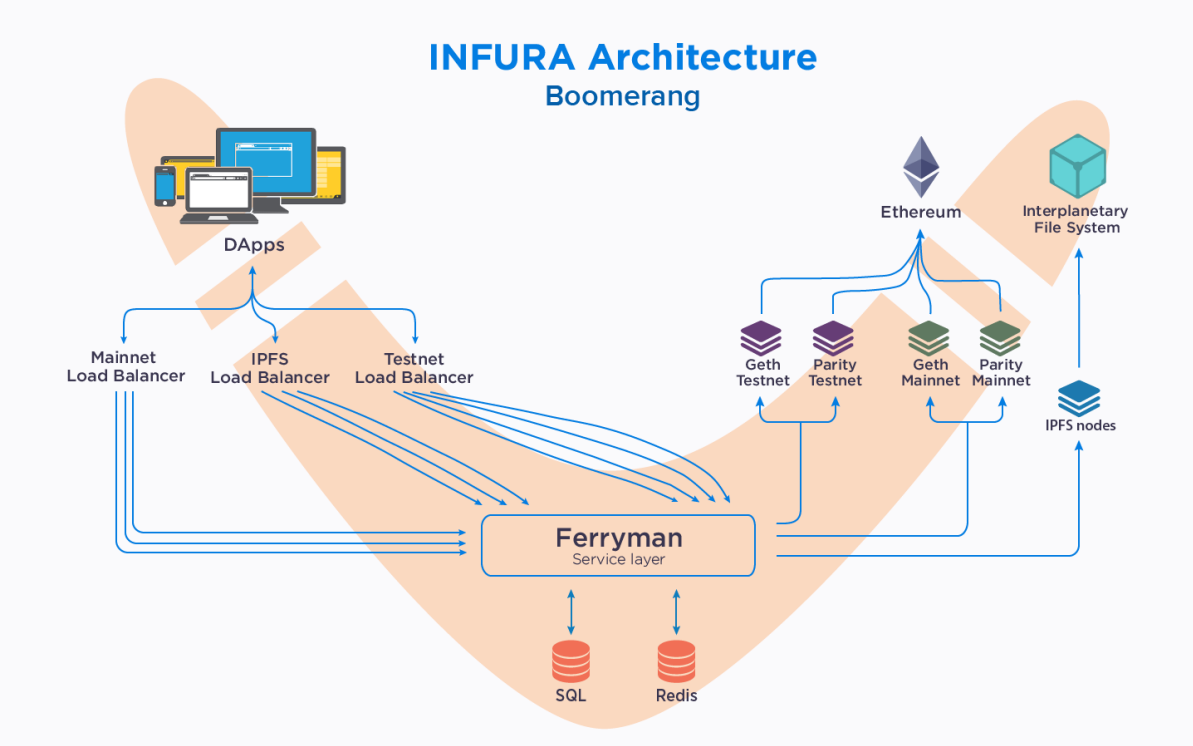
GANACHE



- A lightweight blockchain simulator with explorer and introspection capabilities
- Ability to replicate live blockchain in development environment for rapid iteration

PRODUCTION GRADE INFRASTRUCTURE – NODE HOSTING GATEWAY

INFURA provides a shared infrastructure layer that acts as a bridge to the blockchain, allowing developers to create decentralized apps and solid ecosystems to work in. It acts as a Ethereum infrastructure cluster, allowing direct access to the blockchain without the necessity of downloading a full node



CAPABILITIES	ENTERPRISE IMPLEMENTATION	REFERENCE IMPLEMENTATION
Products	Custom Blockchain Client	Geth, Parity, Python
Easily Scaled	✓	x
Secure Private Keys	✓	✓
Rapid Cloud Deployment	✓	✓
Smart Contracts	✓	✓
Enterprise Connector	✓	x
Legacy Device Support	✓	x
Out of the Box Redundancy	✓	x
Includes IPFS Nodes	✓	x
Load balancing	✓	x
Request Routing	✓	x

METHODOLOGIES AND TOOLS FOR PRODUCTION BLOCKCHAINS TODAY

BUILDING A SECURE AND SCALABLE PRODUCTION BLOCKCHAIN SOLUTION

Developing, running and maintaining a production-grade blockchain will require tools that can assure the following features:

Security

- Auditable Key Management privacy and encryption
- Detailed permissioning at a granular level
- SSL for web-based client applications
- Well-defined processes for dealing with security incidents
- Adherence to security best practices based on past production-ready enterprise deployments

Scaling

- Ability to scale up horizontal transaction processing in private implementations
- Analytics using pre-existing cloud-scale data processing platforms
- support for multiple chains and multiple protocols
- Integration with existing data repositories
- Integration with existing identity systems

Resiliency

- High speed network connection
- Deploy to multiple VMs or a hosted compute PaaS service to ensure availability
- Container orchestration and monitoring to react to changes in uptime and node recovery
- Availability of multi-zone redundant replication

API Management

- Turnkey solution for publishing APIs to external and internal consumers
- APIs secured with a key, token, and IP filtering
- Enforced flexible and fine-grained quotas and rate limits

Encryption

- Extensible encryption schemes for legal and regulatory compliance
- Key management encryption

Authentication / Authorization

- Protocol level permissions
- Contract level security and permissions
- Cloud-based roles and permissions
- Digital identity based authorization

Ease of Development

- Mature development frameworks and deployment tools to facilitate application build
- Digestible APIs and ease of integration across ecosystem

Oracle Interaction

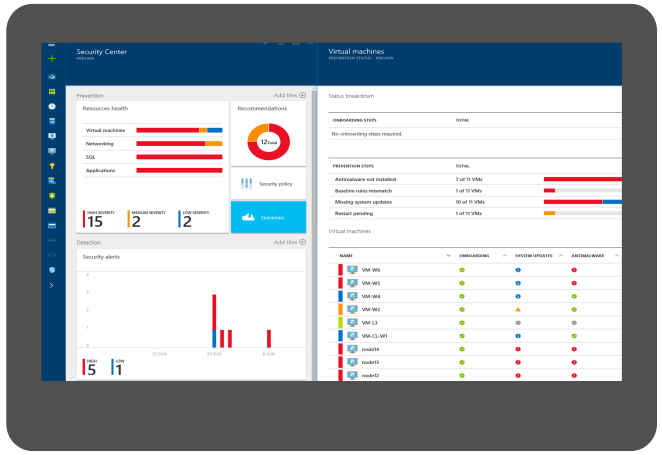
- Mature external services viewing into the blockchain that can execute logic, reading data which triggers events

Many blockchain deployment requirements are generic. Blockchain deployments can leverage existing cloud infrastructure to scale and maintain production-grade solutions.

LEVERAGING EXISTING CLOUD INFRASTRUCTURE

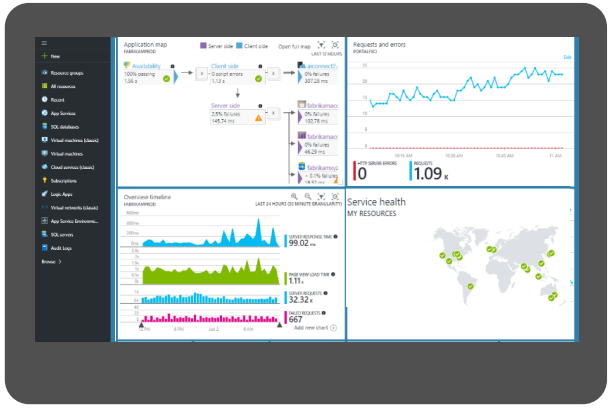
Many blockchain deployment requirements are generic. Blockchain deployments can leverage existing cloud infrastructure to scale and maintain production-grade solutions.

Security and Resiliency

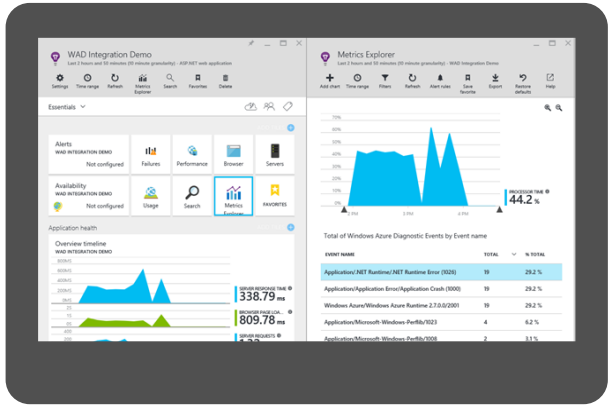


Front End Insights

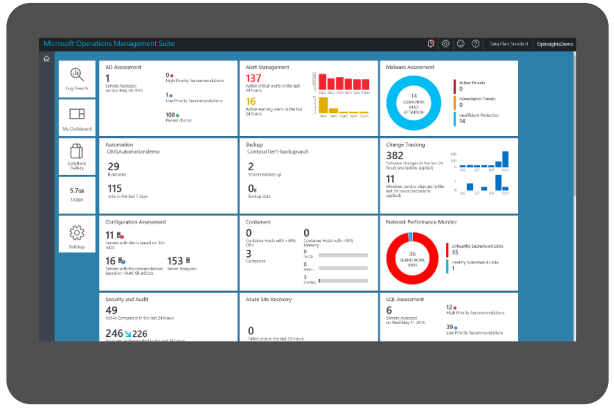
Cloud Dashboard



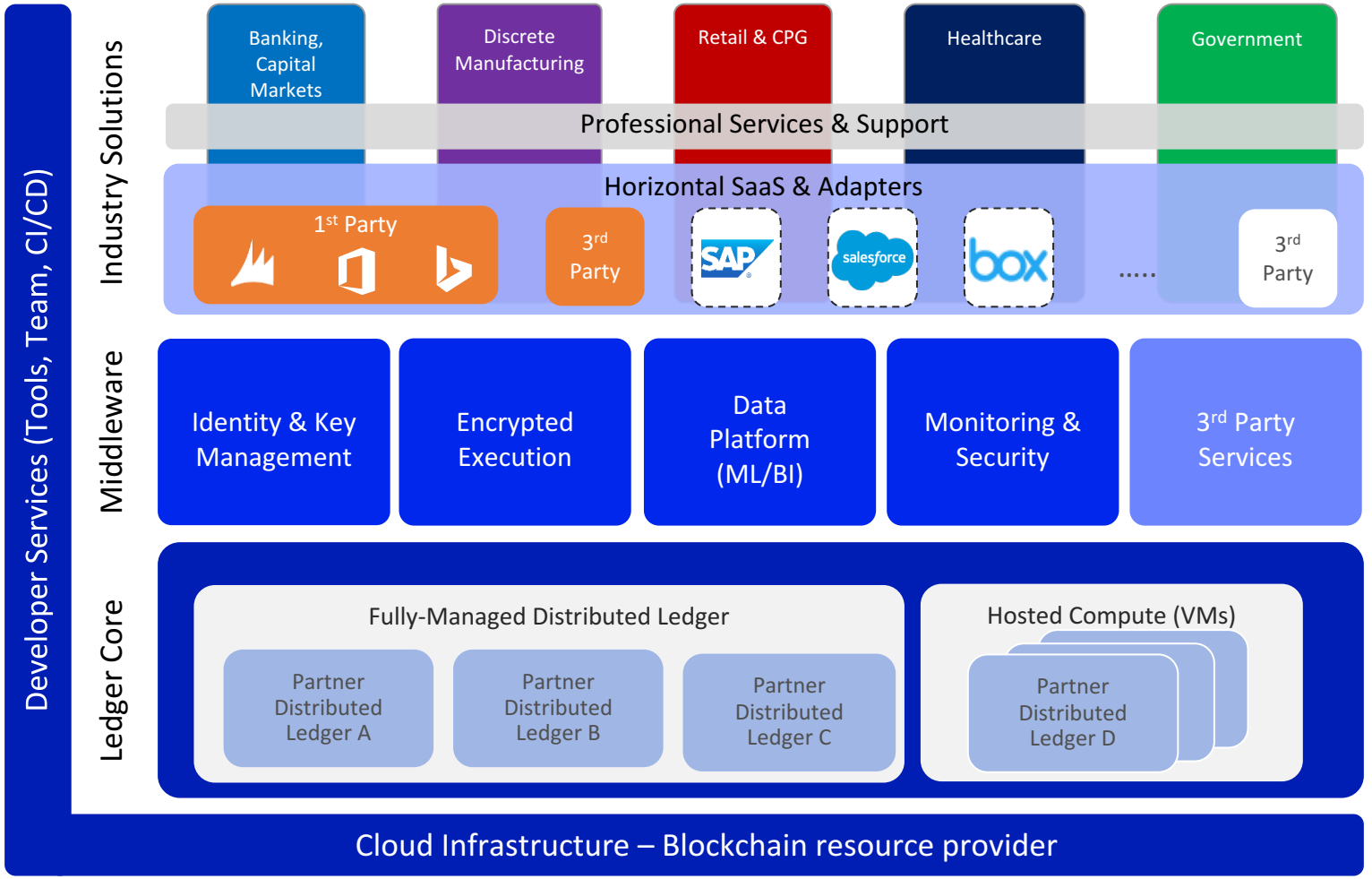
Application Insights



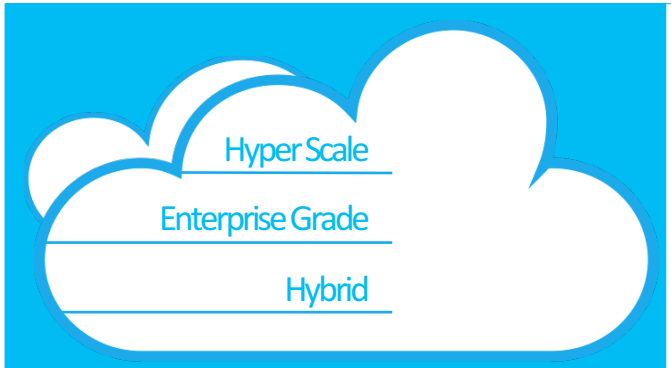
Operations Management



EXISTING PRODUCTION BLOCKCHAIN INFRASTRUCTURE – BaaS



PRODUCTION BLOCKCHAIN INFRASTRUCTURE – MICROSOFT AZURE BaaS EXAMPLE



We've delivered an open, broad, and flexible cloud across the stack

Azure BaaS

coinprism, Libra, bitpay, ETH BaaS, openchain, ripple, NETKI, Libra, factom, MultiChain, Manifold Technology

Infrastructure

ubuntu, docker, CoreOS, SUSE, ORACLE LINUX, CentOS

+Hundreds of community supported images on VM Depot

Databases

DATASTAX, Hortonworks, Couchbase, MySQL, mongoDB, redis, SQL Server, cloudera, hadoop

App Frameworks

Microsoft .NET, Java, php, eclipse, Ruby, python, IntelliJIDEA

Applications

CLOUD FOUNDRY, Drupal, SharePoint, Joomla!, Jelastic, pprenda

Web App Gallery

Dozens of .NET & PHP CMS and Web apps

Management

juju, CHEF, puppet labs, ANSIBLE, GitHub, SALTSTACK

Clients

APACHE CORDOVA, Xamarin

SDO ETHEREUM BaaS MANAGER

Management Repository

- Smart Contract Permissioning Templates
- Consensus Templates
- Genesis Templates
- Subnet Templates

Smart Contract

Authority contracts and logic

Consensus

Proof of Authority and Validators

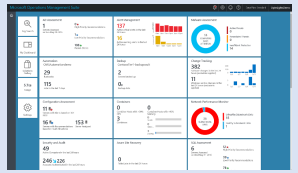
Node

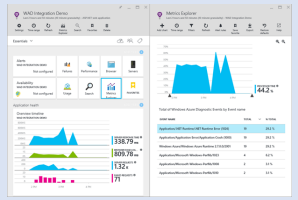
Network identifier, Peer keys, Genesis files

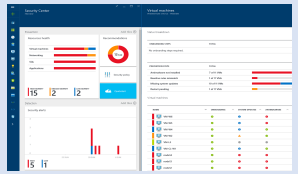
Network

VPN and Node identification

Management Console





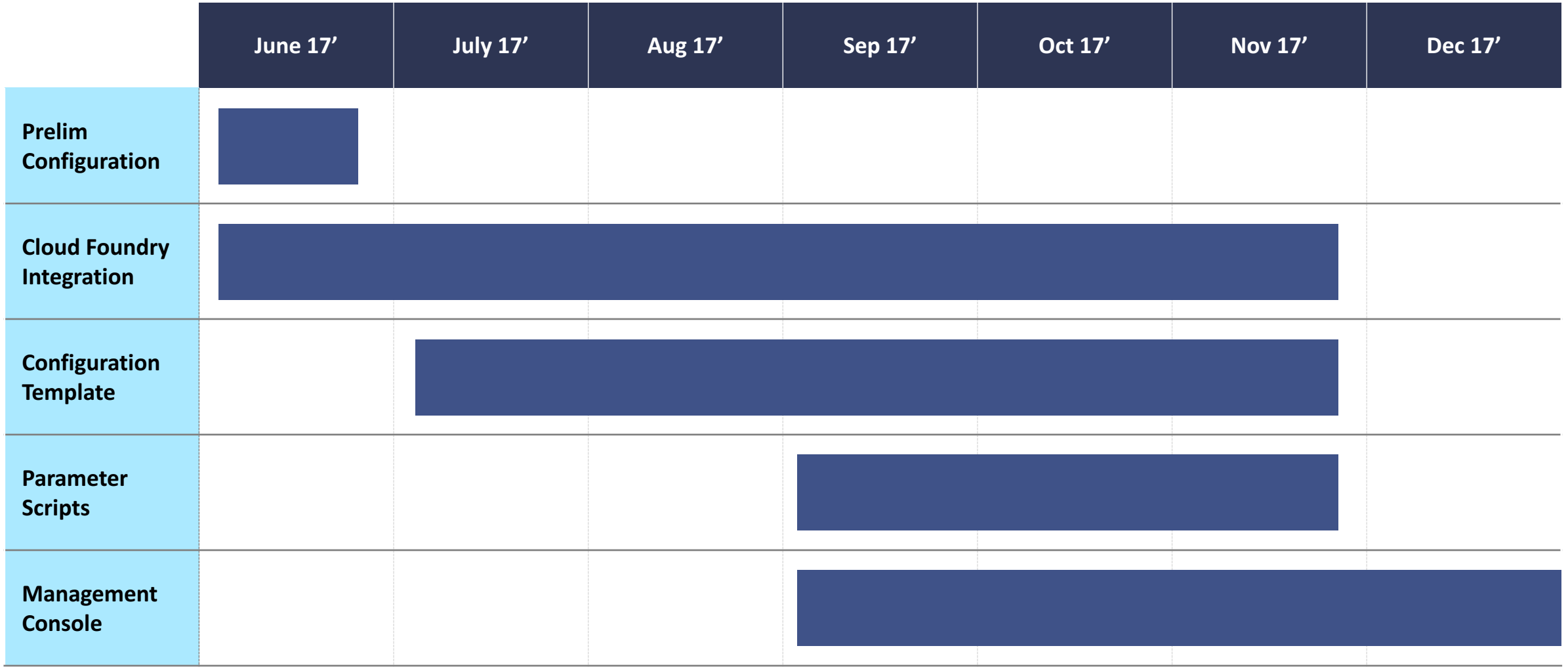


docker + INFURA + Parity

Smart Dubai Data Platform

CLOUD FOUNDRY Controller API

SDO BaaS IMPLEMENTATION TIMELINE



A PERMISSIONED PRIVATE ETHEREUM

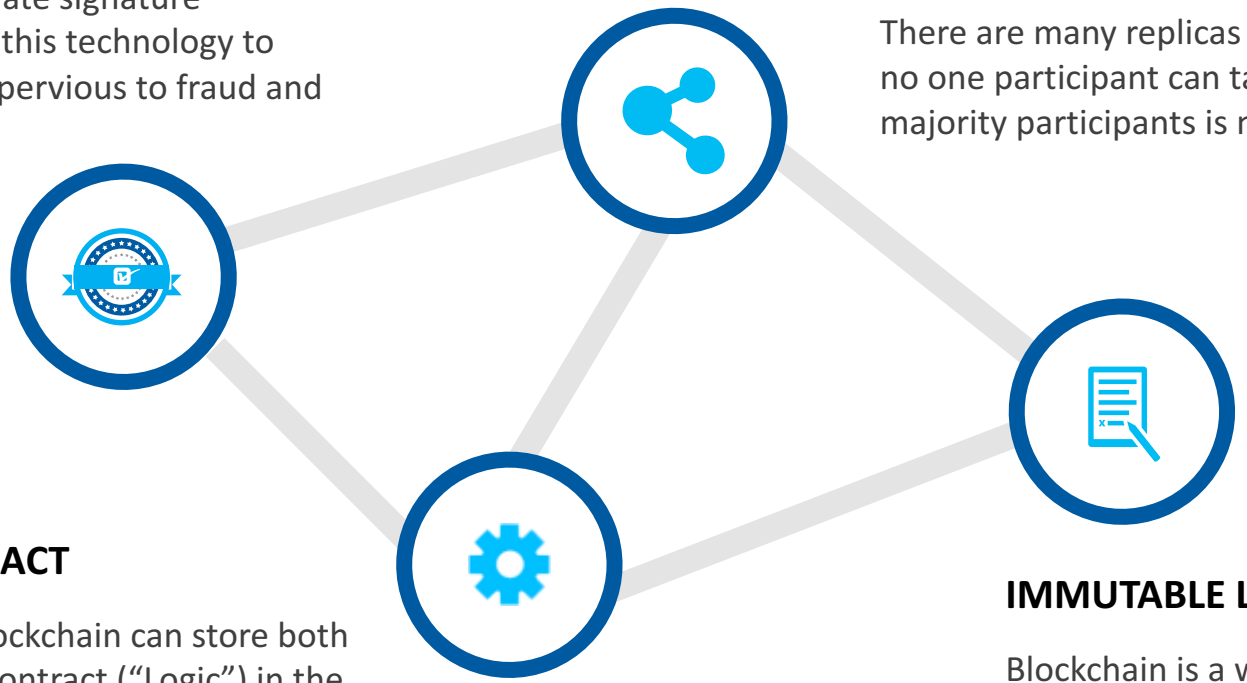
WHAT MAKES A BLOCKCHAIN DIFFERENT?

CRYPTOGRAPHICALLY SECURE

Uses tried and true public/ private signature technology. Blockchain applies this technology to create transactions that are impervious to fraud and establishes a shared truth.

DECENTRALIZED

There are many replicas of the blockchain database and no one participant can tamper it. Consensus among majority participants is needed to update the database.



SMART CONTRACT

The Ethereum blockchain can store both data and Smart Contract (“Logic”) in the blockchain

IMMUTABLE LEDGER

Blockchain is a write-once database so it records an immutable record of every transaction that occurs.

ETHEREUM PERMISSIONING FEATURES

Layer	Feature
Smart Contract	Smart contract permissioning
Consensus	Proof of Authority
Node	Node network ID, Custom Genesis file
Network	Virtual private network (VPN)

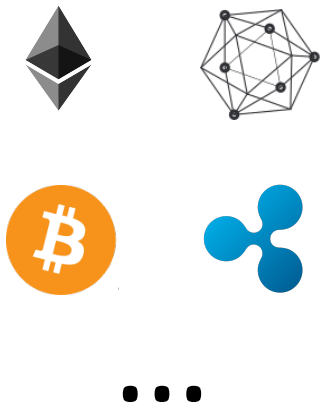
ETHEREUM PRIVACY FEATURES

Layer	Feature
Smart Contract	Quorum-style multilateral smart contracts with on-chain anchor
Consensus	Zero-knowledge proofs (Zk-SNARKS), road mapped for Metropolis release
Node	State channels
Network	Virtual private network (VPN)

CROSS-CHAIN, MULTI-PROTOCOL, DUBAI-SPECIFIC BLOCKCHAIN FOR LONG TERM GROWTH

MAKING MULTIPLE BLOCKCHAIN PROTOCOLS WORK TOGETHER

Multiple blockchain protocols exist today – each developing in silo:



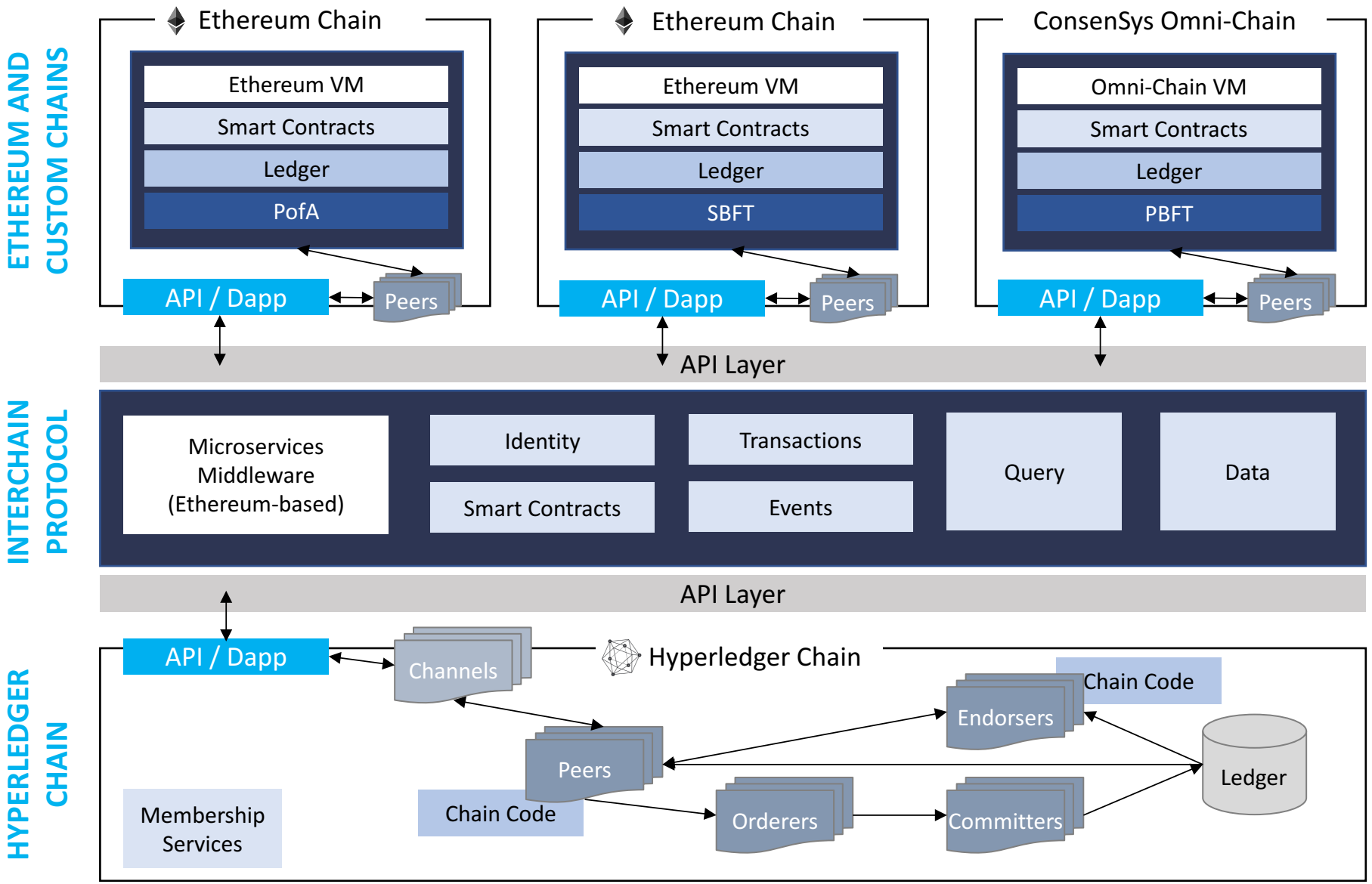
In order to develop an integration between them, we would need to consider:

Privacy	Scalability
Consensus	Developer Support
Data Layer	Pluggability
Permissioning	Governance

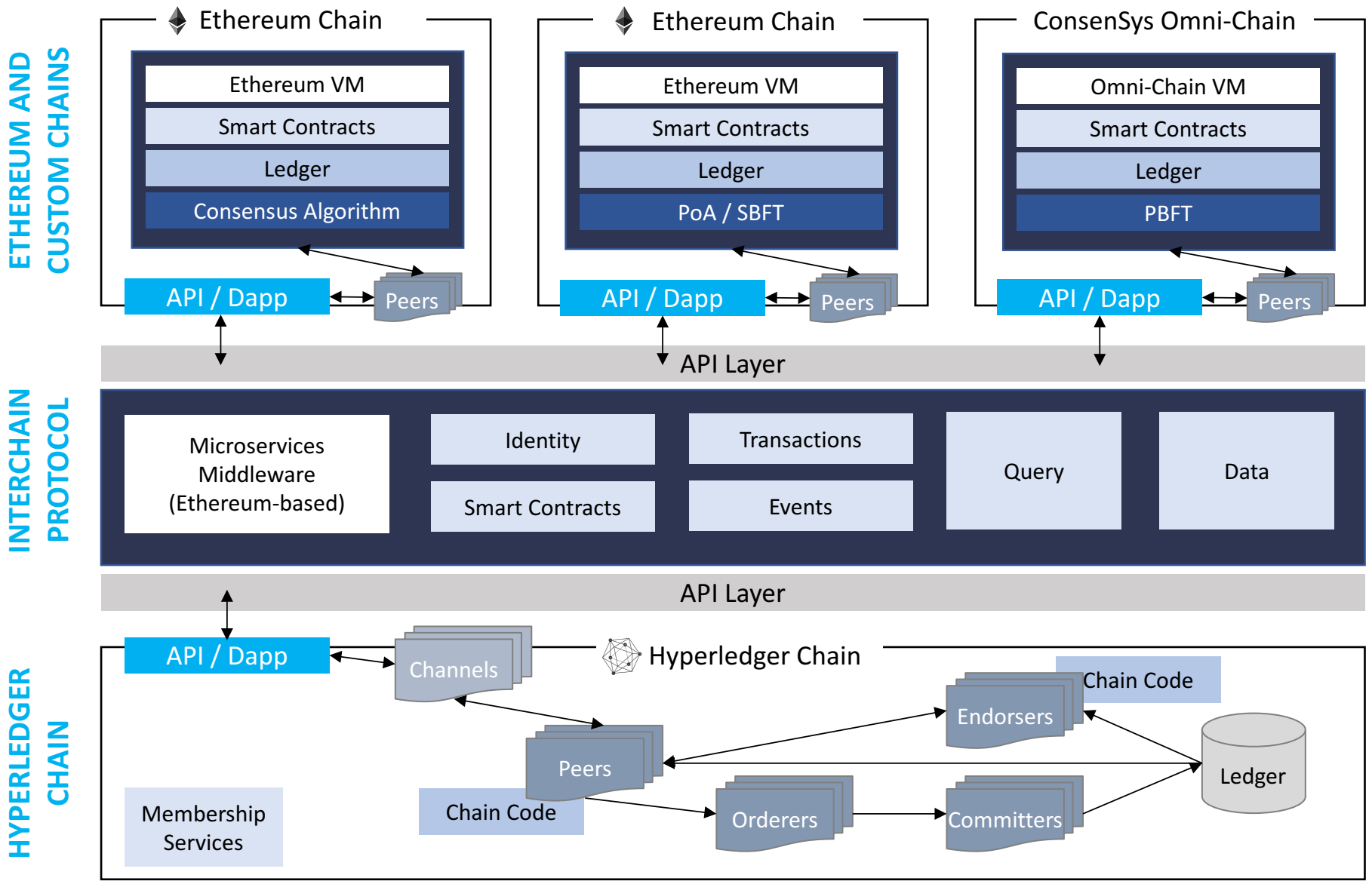
While still maintaining critical blockchain properties:

There is a clear need to develop flexible and configurable decentralized cross-chain, multi-protocol deployments

MULTI-PROTOCOL BLOCKCHAIN PROPOSED ARCHITECTURE



MULTI-PROTOCOL BLOCKCHAIN PROPOSED ARCHITECTURE

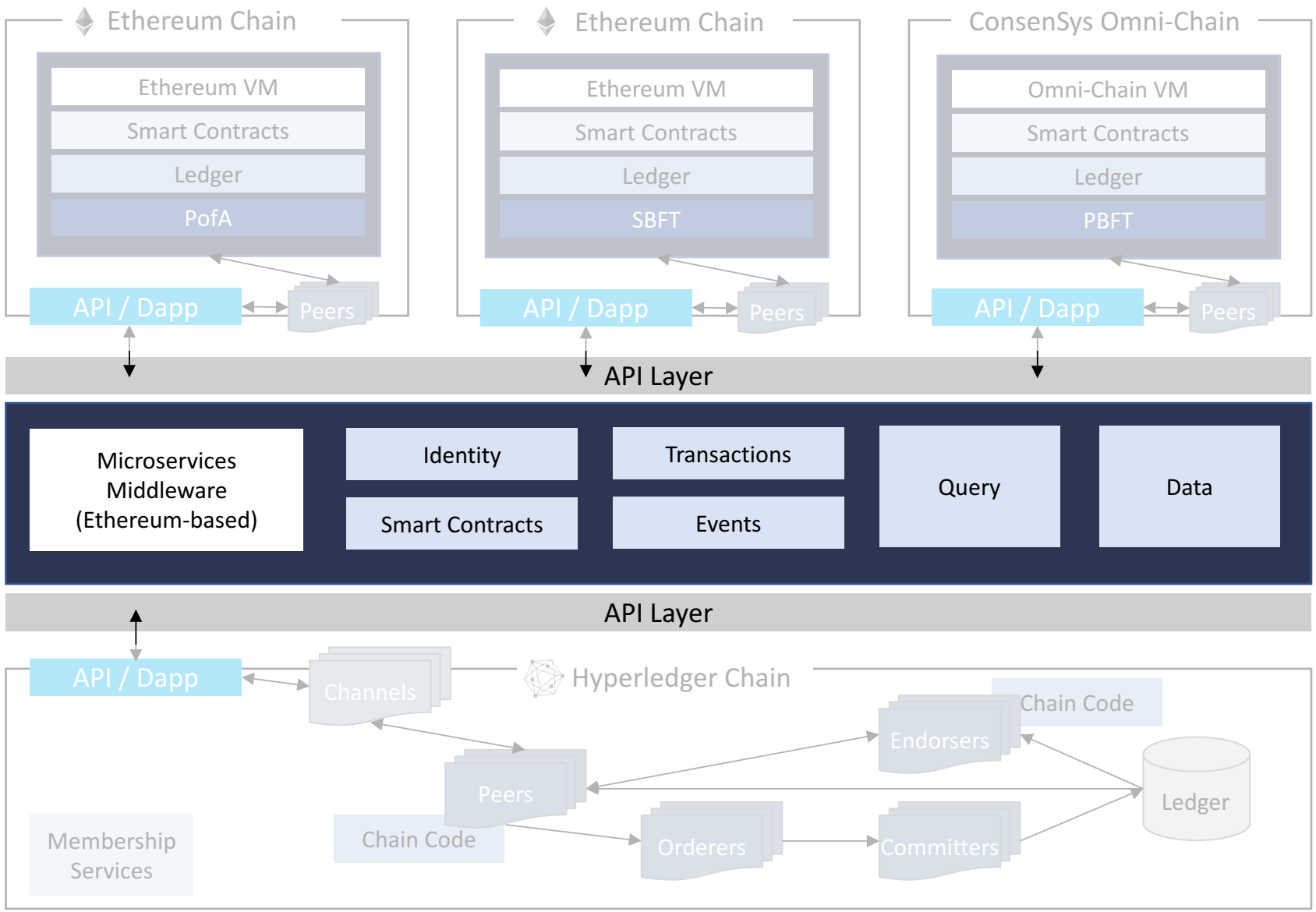


- Virtual machine processes transactions, executes smart contracts, and emits events
- Smart contracts can leverage multiple or domain-specifc languages for expressing business logic
- Scalable Ledger contains on-chain data
- Consensus layer decides transaction finality

- Support cross-chain semantics for identity, smart contracts, transactions, and events
- Has an API to enable integration of multiple chains and protocols
- Extended with relevant data and query capabilities for scalable analytics and monitoring

- Centralized account Membership Services
- Peers, orderers, endorsers, and committers work together to determine transactions,
- Centralized mutable ledger that stores state data but not code

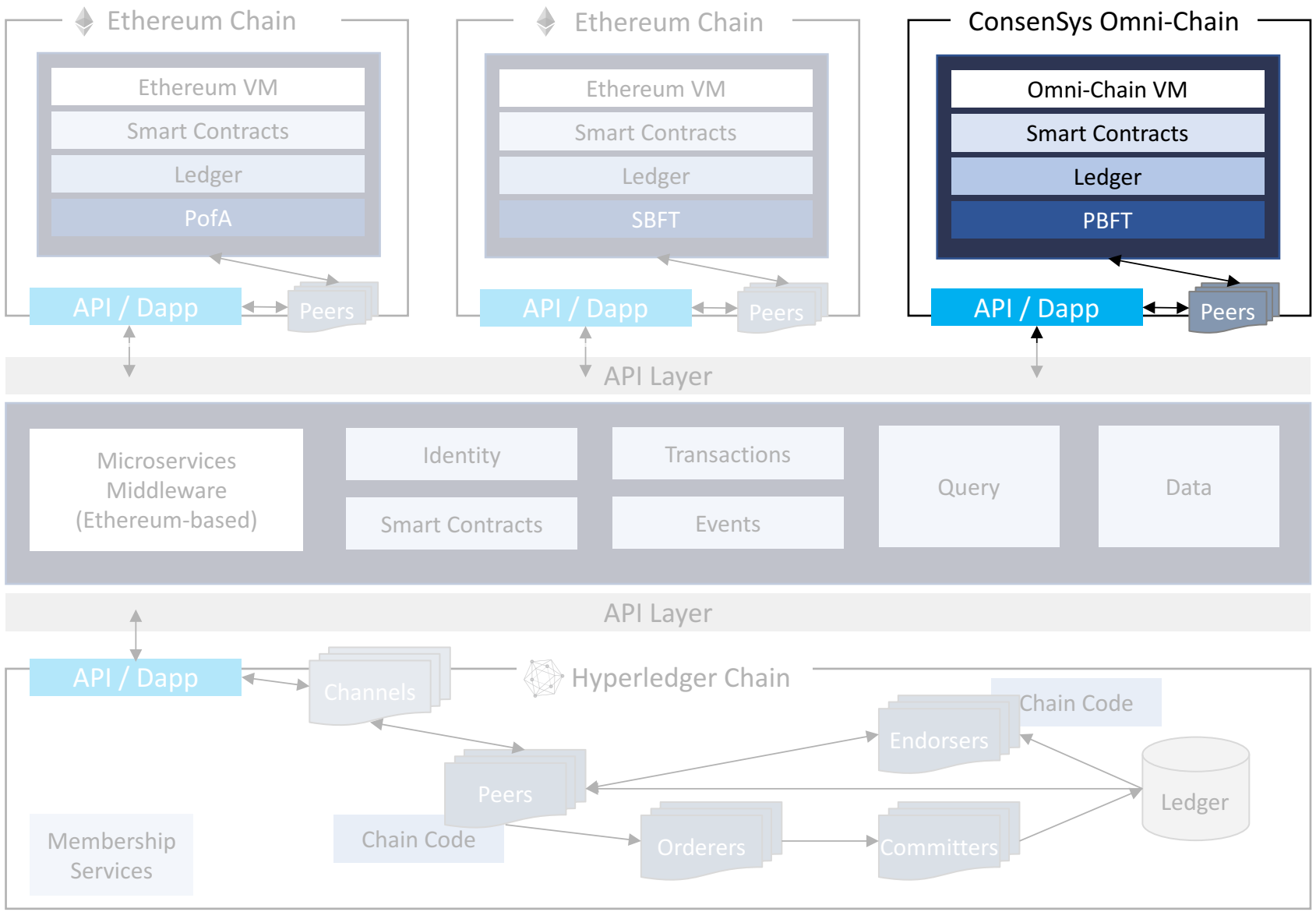
MULTI-PROTOCOL BLOCKCHAIN PROPOSED ARCHITECTURE



INTERCHAIN PROTOCOL

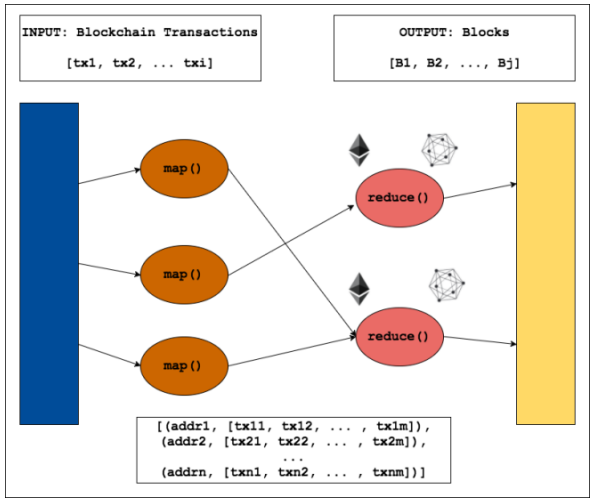
- Tracking of blocks/hashes across chains
- Multiple chains of the same protocol are easier to manage semantically since no translation is needed between hash and proof generation
- Multiple chains of different protocols can be managed via translations between hashes and proofs
- Proven semantic approaches for big data integration reusing existing unmodified databases

MULTI-PROTOCOL BLOCKCHAIN PROPOSED ARCHITECTURE

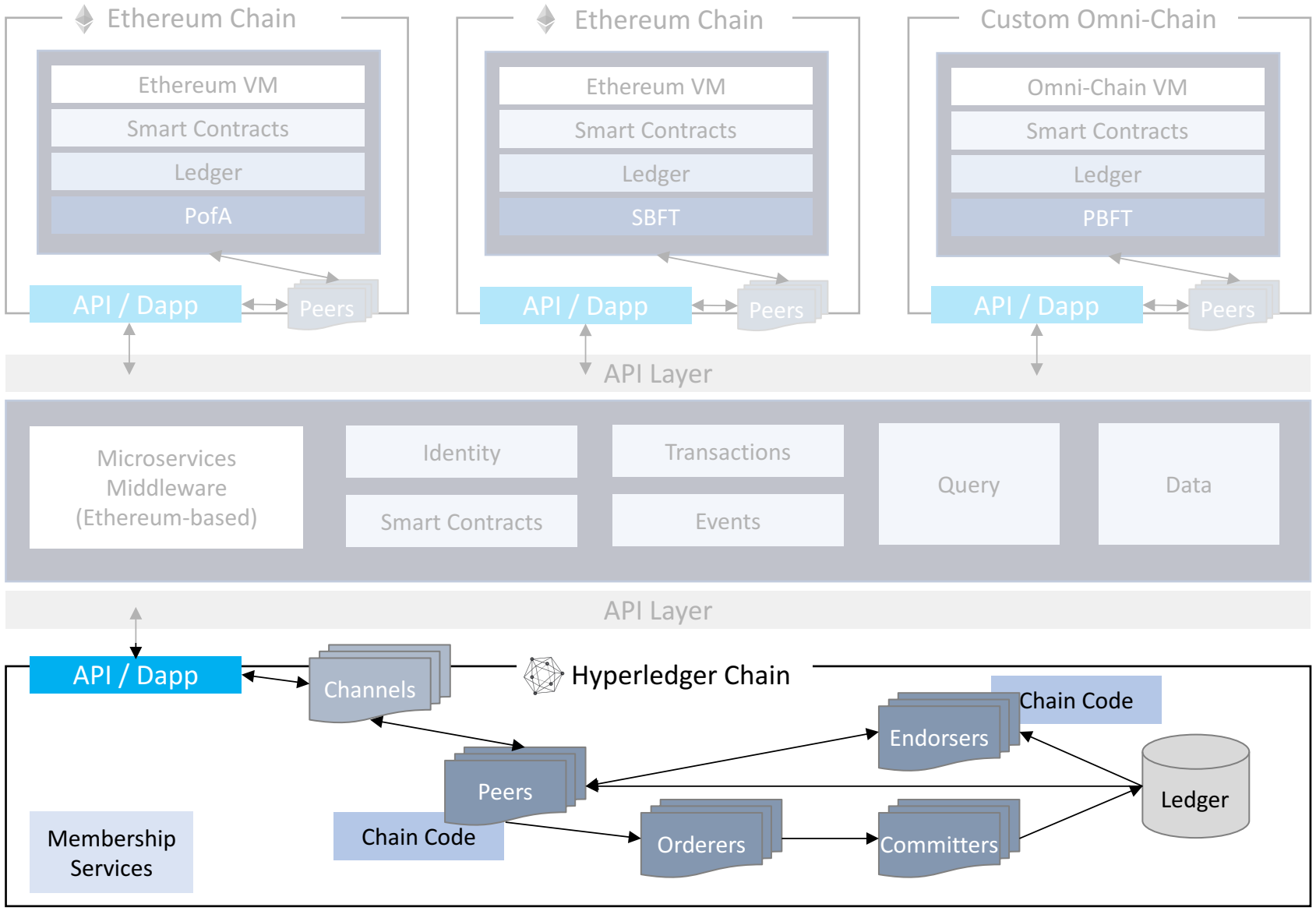


CONSENSYS OMNI-CHAIN

- Multiple language implementations
- Multiple language bindings
- Pluggable and modular components
- Support for custom implementations
- Permission Layer
- Blockchain virtual machine (BVM)
- Database and Network protocol



MULTI-PROTOCOL BLOCKCHAIN PROPOSED ARCHITECTURE



HYPERLEDGER CHAIN

- Centralized account management
- Key concepts not yet documented
- Iterative and repetitive Docker based development cycle
- Lack of consensus algorithms, also relies on centralized ledger
- Code not deployed to ledger, not immutable
- Alpha release 25 days ago

MULTI-PROTOCOL BLOCKCHAIN DETAIL

END GOAL

Deliver a cross-chain, multi-protocol, high performance Blockchain-as-a-Service platform for Smart Dubai, while respecting key blockchain properties:

- Decentralized Immutability and Security
- Maintain semantics of accounts, smart contracts, transactions, and events

WHY AN ETHEREUM-BASED MIDDLEWARE?

- Ethereum enables decentralized, multi-platform, multi-VM, multi-consensus pluggability
  - Concise and formal specification enables flexibility
  - Supports modular configurations with one protocol
- Concise and flexible Ethereum-based middleware can integrate multiple protocols
  - E.g., Automating token pegs via Ethereum smart contracts and HL Fabric chaincode
  - Support for scalable multi-protocol, multi-chain analytics of data and code (eat-our-own-dog-food approach)
- Hyperledger uses a centralized configuration
  - Does not easily support different registrations; restricted to a single, authoritative scheme
  - Not decentralized, not immutable business logic, and arbitrary smart contracts (vs. secure)
  - Not field tested

THANK YOU!

شكرا