Blockchain @ Microsoft

Thomas Conté - @tomconte
Blockchain Geek

Agenda

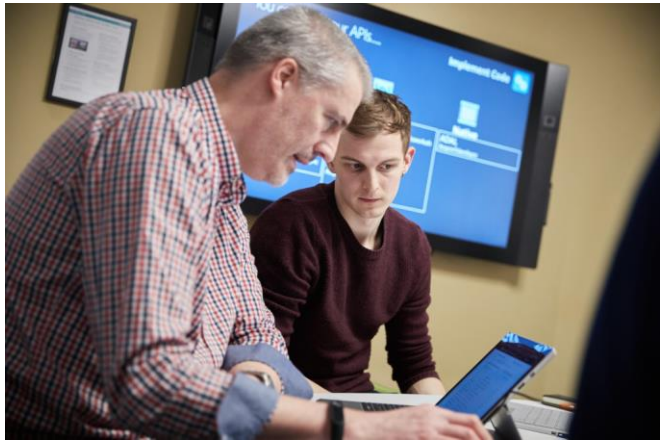
- Customer engagements
- Enterprise Ethereum Alliance
- Cryptlet Fabric
- Q&A

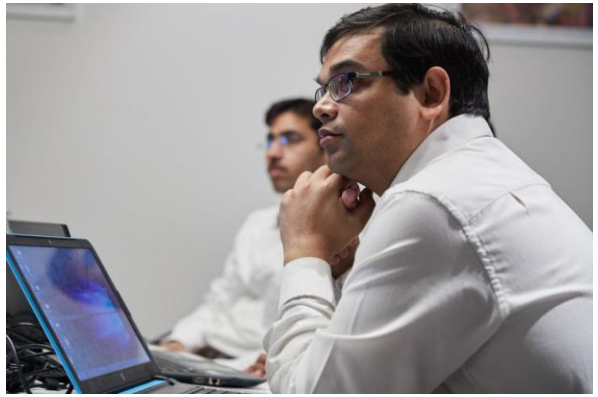
Customer engagements

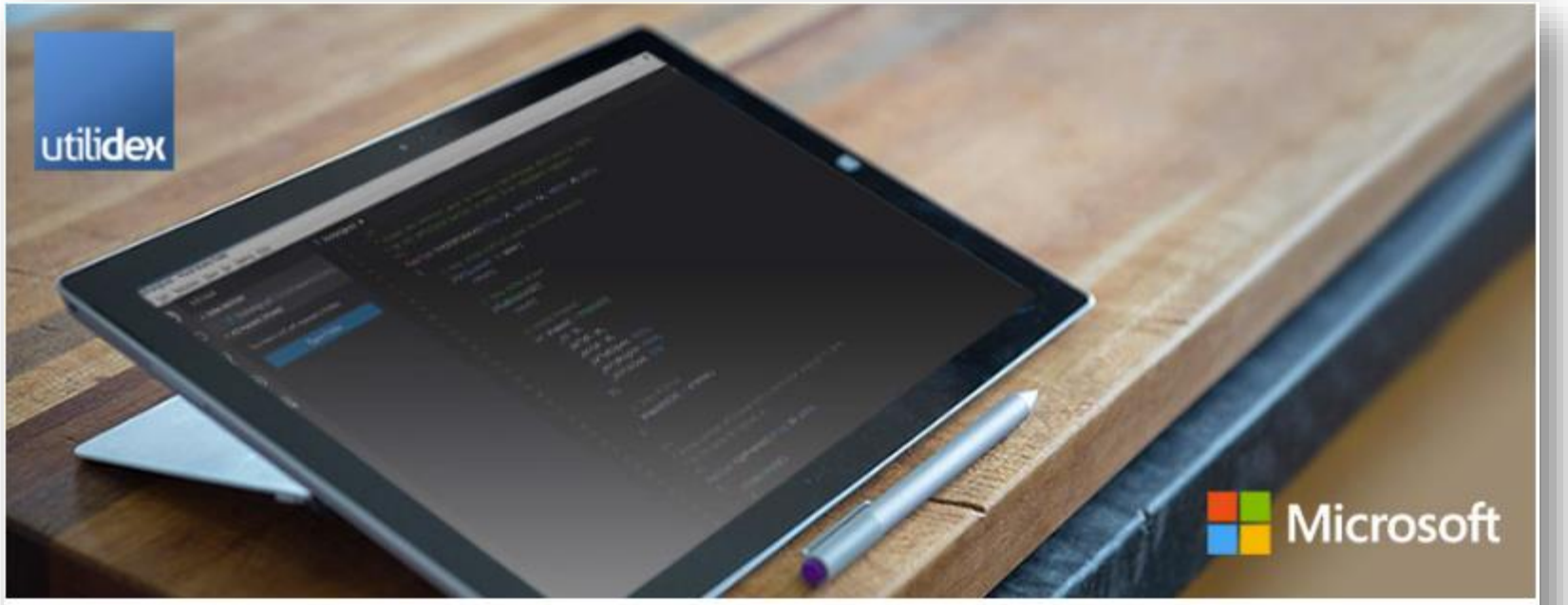
Utilidex partnership

An online platform in the energy trading sector

Microsoft helped them test the blockchain technology

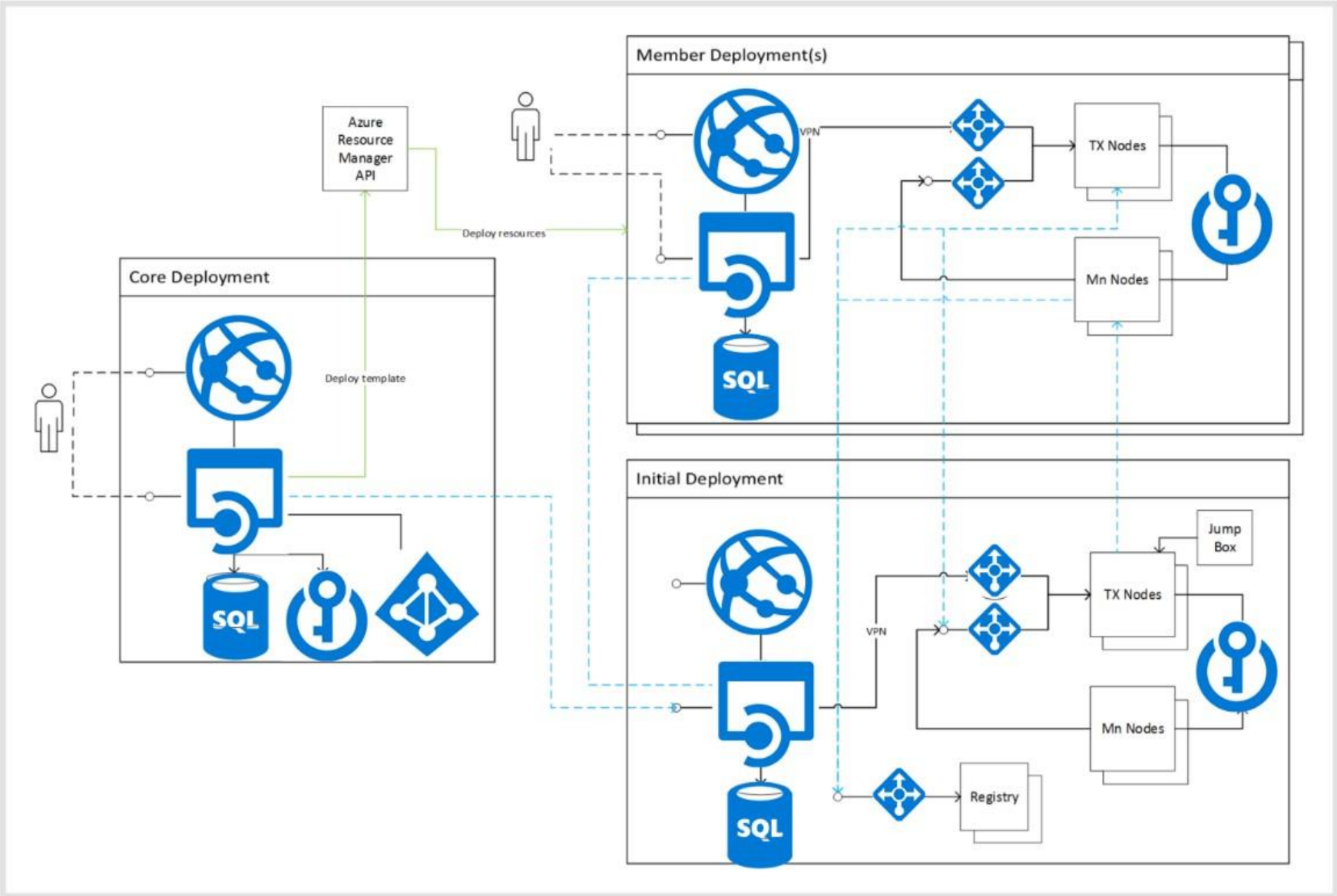






28 Jun **Utilidex announces new blockchain initiative with Microsoft**

Utilidex architecture: blockchain in context



Utilidex links

Utilidex Partnership Blog post

Utilidex Blockchain Blog post

MS News Centre article

TechNet article

Technical white paper

Source code on Github

Enterprise Ethereum Alliance

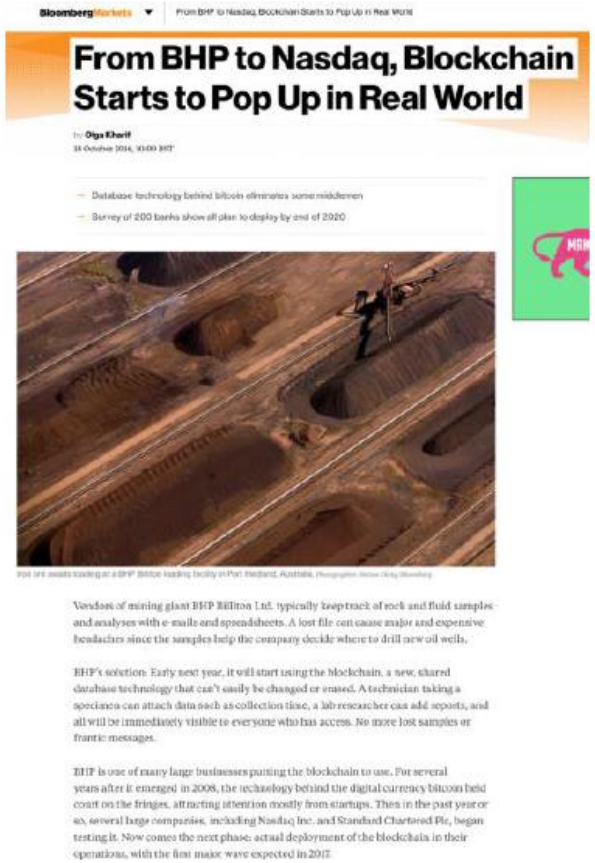
ENTERPRISE ETHEREUM ALLIANCE

accenture
AMIS
ANDUI 安兑
BBVA
BlockApps
bp
brainbot TECHNOLOGIES AG
BNY MELLON
CME Group
CONSENSYS
CHRONICLED
CREDIT SUISSE
CRYPTAPE
富邦金控 Fubon Financial
IC3 The Initiative For CryptoCurrencies & Contracts
ING
The Institutes RISK & INSURANCE KNOWLEDGE GROUP
intel
J.P.Morgan
MONAX INDUSTRIES
Microsoft
nuco
THOMSON REUTERS
Santander
string
telindus powered by tango
Tendermint
UBS
VidRoll
WIPRO Applying Thought

Ethereum: Most Popular Blockchain Globally

With a global developer community of more than 30,000 contributors, Ethereum is one of the most popular blockchains and the technology of choice for many Enterprise blockchain developments.

Enterprises are Already Deploying Ethereum Networks



Bloomberg Markets | From BHP to Nasdaq, Blockchain Starts to Pop Up in Real World

From BHP to Nasdaq, Blockchain Starts to Pop Up in Real World

by Olga Kharif
18 October 2016, 10:00 BST

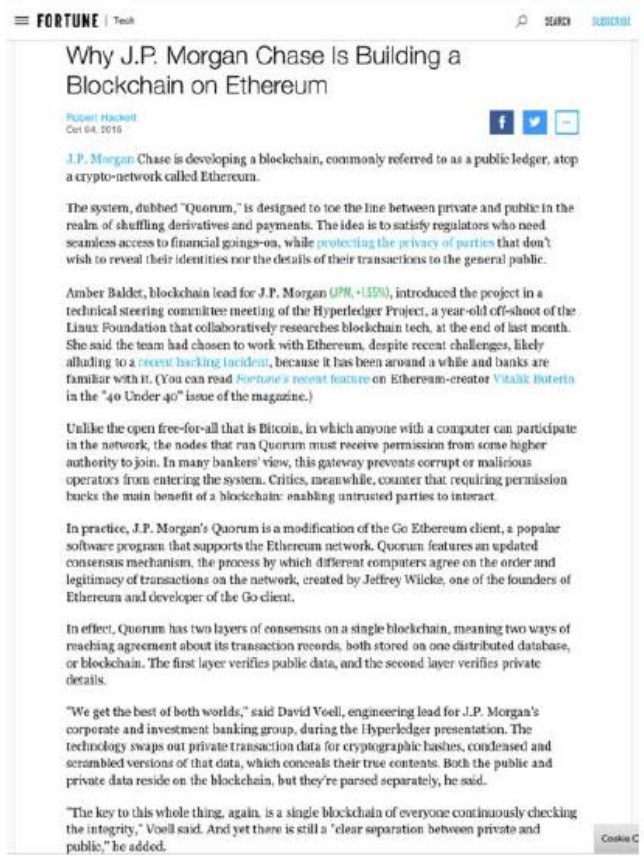
- Database technology behind bitcoin eliminates some middlemen
- Survey of 200 banks show all plan to display by end of 2020

Vast ore awaits loading at a BHP Billiton loading facility in Port Hedland, Australia. Photographer: Steve Christo/Bloomberg

Vendors of mining giant BHP Billiton Ltd. typically keep track of rock and fluid samples and analyses with e-mails and spreadsheets. A lost file can cause major and expensive headaches since the samples help the company decide where to drill new oil wells.

BHP's solution: Early next year, it will start using the blockchain, a new, shared database technology that can't easily be changed or erased. A technician taking a specimen can attach data such as collection time, a lab researcher can add reports, and all will be immediately visible to everyone who has access. No more lost samples or frantic messages.

BHP is one of many large businesses putting the blockchain to use. For several years after it emerged in 2008, the technology behind the digital currency bitcoin held court on the fringes, attracting attention mostly from startups. Then in the past year or so, several large companies, including Nasdaq Inc. and Standard Chartered Plc, began testing it. Now comes the next phase: actual deployment of the blockchain in their operations, with the first major wave expected in 2017.



FORTUNE | Tech SEARCH SUBSCRIBE

Why J.P. Morgan Chase Is Building a Blockchain on Ethereum

Robert Hackett
Oct 04, 2016

J.P. Morgan Chase is developing a blockchain, commonly referred to as a public ledger, atop a crypto-network called Ethereum.

The system, dubbed "Quorum," is designed to toe the line between private and public in the realm of shuffling derivatives and payments. The idea is to satisfy regulators who need seamless access to financial goings-on, while protecting the privacy of parties that don't wish to reveal their identities nor the details of their transactions to the general public.

Amber Baldet, blockchain lead for J.P. Morgan (JPM, +1.55%), introduced the project in a technical steering committee meeting of the Hyperledger Project, a year-old off-shoot of the Linux Foundation that collaboratively researches blockchain tech, at the end of last month. She said the team had chosen to work with Ethereum, despite recent challenges, likely alluding to a recent hacking incident, because it has been around a while and banks are familiar with it. (You can read Fortune's recent feature on Ethereum-creator Vitalik Buterin in the "40 Under 40" issue of the magazine.)

Unlike the open free-for-all that is Bitcoin, in which anyone with a computer can participate in the network, the nodes that run Quorum must receive permission from some higher authority to join. In many bankers' view, this gateway prevents corrupt or malicious operators from entering the system. Critics, meanwhile, counter that requiring permission backs the main benefit of a blockchain: enabling untrusted parties to interact.

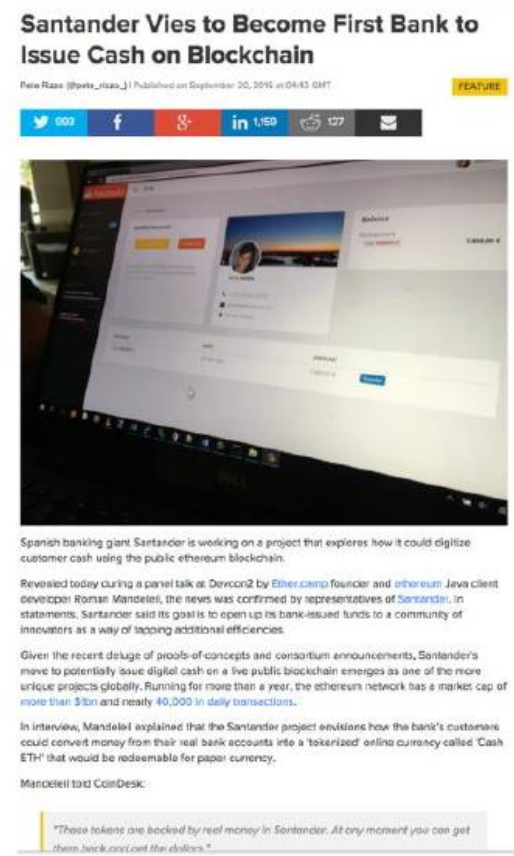
In practice, J.P. Morgan's Quorum is a modification of the Go Ethereum client, a popular software program that supports the Ethereum network. Quorum features an updated consensus mechanism, the process by which different computers agree on the order and legitimacy of transactions on the network, created by Jeffrey Wilcke, one of the founders of Ethereum and developer of the Go client.

In effect, Quorum has two layers of consensus on a single blockchain, meaning two ways of reaching agreement about its transaction records, both stored on one distributed database, or blockchain. The first layer verifies public data, and the second layer verifies private details.

"We get the best of both worlds," said David Voell, engineering lead for J.P. Morgan's corporate and investment banking group, during the Hyperledger presentation. The technology swaps out private transaction data for cryptographic hashes, condensed and scrambled versions of that data, which conceals their true contents. Both the public and private data reside on the blockchain, but they're parsed separately, he said.

"The key to this whole thing, again, is a single blockchain of everyone continuously checking the integrity," Voell said. And yet there is still a 'clear separation between private and public," he added.

Cookie C



Santander Vies to Become First Bank to Issue Cash on Blockchain

Pete Rizzo (@pete_rizzo_) | Published on September 20, 2016 at 04:43 GMT FEATURE

002 1,169 127

Spanish banking giant Santander is working on a project that explores how it could digitize customer cash using the public ethereum blockchain.

Revealed today during a panel talk at Devcon2 by Ether.camp founder and ethereum Java client developer Roman Mandeleil, the news was confirmed by representatives of Santander. In statements, Santander said its goal is to open up its bank-issued funds to a community of innovators as a way of tapping additional efficiencies.

Given the recent deluge of proofs-of-concepts and consortium announcements, Santander's move to potentially issue digital cash on a live public blockchain emerges as one of the more unique projects globally. Running for more than a year, the ethereum network has a market cap of more than $1bn and nearly 40,000 in daily transactions.

In interview, Mandeleil explained that the Santander project envisions how the bank's customers could convert money from their real bank accounts into a 'tokenized' online currency called 'Cash ETH' that would be redeemable for paper currency.

Mandeleil told CoinDesk:

> "These tokens are backed by real money in Santander. At any moment you can get them back and get the dollars."

Why Ethereum For Enterprise Blockchain

- ☑ Open Source and widely available
- ☑ Easy to learn and high development productivity
- ☑ Rapidly growing ecosystem
- ☑ Public chain provides innovation and scales developer community
- ☑ Proven ability to tokenize complex assets

Introducing Enterprise Ethereum

Enterprise Ethereum is an initiative to create a **reference standard** for private deployments of Ethereum networks, **building upon the public Ethereum** roadmap and retaining **public Ethereum compatibility**.

This initiative is driven by some of the largest corporate users of Ethereum, enterprise technology vendors and leading blockchain start-ups

http://entethalliance.org/

Short Term Technical Objectives

- Modularized Ethereum implementation with pluggable consensus.
- Benchmarked PBFT (or comparable) consensus algorithms.
- Configurable privacy implementation, including permissioning and data privacy.

How To Get Involved

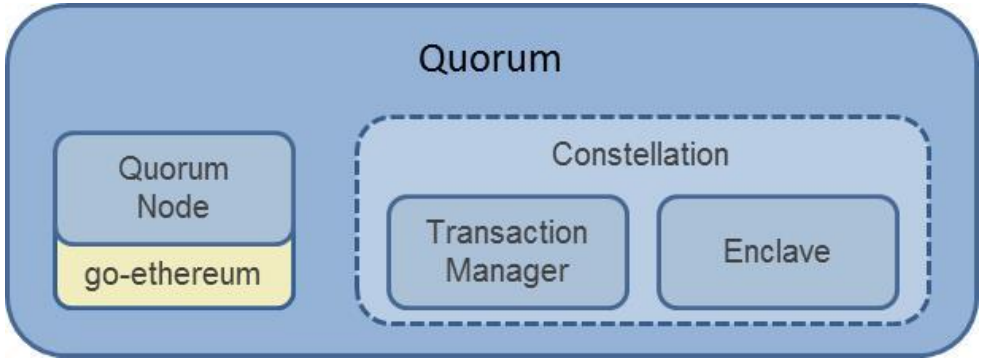
- **Enterprise Ethereum Alliance launched on February 28 2017**
- **Replay of the launch day is available on the entethalliance.org website**
- **We will be adding additional members on an ongoing basis**

Interested parties should contact **info@entethalliance.org**

We are keen to add interested corporates, enterprise technology vendors and blockchain start-ups.

Quorum

https://github.com/jpmorganchase/quorum



Highlights

- Built on Ethereum
  - In production since July 2015
  - 50K+ unit tests, security audits
  - Largest ecosystem
  - Public blockchain
- Simple Privacy Design
  - Supports both public and private transactions and smart contracts
- Single Blockchain Architecture
  - All public and private contracts derived from a single complete blockchain validated by all nodes
- High Performance
  - Able to process dozens to hundreds of transactions per second

Components

- Constellation
  - Transaction Manager: stores and allows access to encrypted transaction data, exchanges encrypted payloads with other participant's Transaction Managers.
  - Crypto Enclave: symmetric key generation and data encryption/decryption.
- QuorumChain
  - Vote-based consensus: A Smart Contract to govern consensus and manage who can partake in consensus; Ethereum Transactions to propagate votes through the network; Ethereum's signature validation to validate signatures received from Maker and Voter nodes
- Network Manager
  - Controls which nodes can connect to a given node and also to which nodes the given node can dial out to.

EEA Single Member Blockchain

Enterprise Ethereum Alliance

Overview Plans

GET IT NOW

Pricing information

Cost of deployed template components

Categories

Compute
Databases
Security + Identity

Legal

License Agreement
Privacy Policy

Deploy and configure a Quorum blockchain in minutes

Quorum is an open-source, permissioned implementation of Ethereum supporting transaction and contract privacy initially created by J.P. Morgan.

Quorum is ideal for any application requiring:

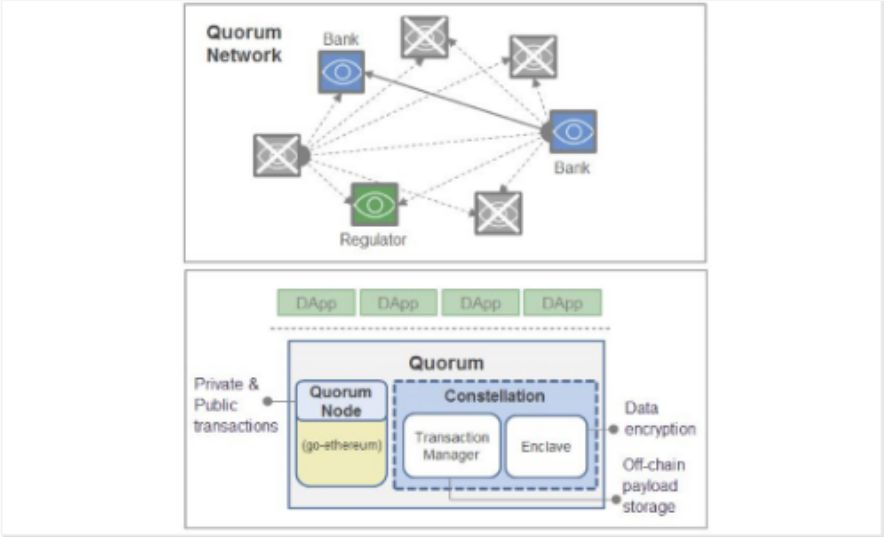
- high speed and high throughput processing of private transactions
- a permissioned group of known participants

Quorum addresses specific challenges to blockchain technology adoption within the financial industry, and beyond.

Quorum supports:

- Transaction-level privacy and network-wide transparency, customizable to business requirements
- Institutional transaction volumes
- Blockchain transactions among a permissioned group of known participants

Quorum is designed to develop and evolve alongside Ethereum. Because it only minimally modifies Ethereum's core, Quorum is able to incorporate the majority of Ethereum updates quickly and seamlessly.

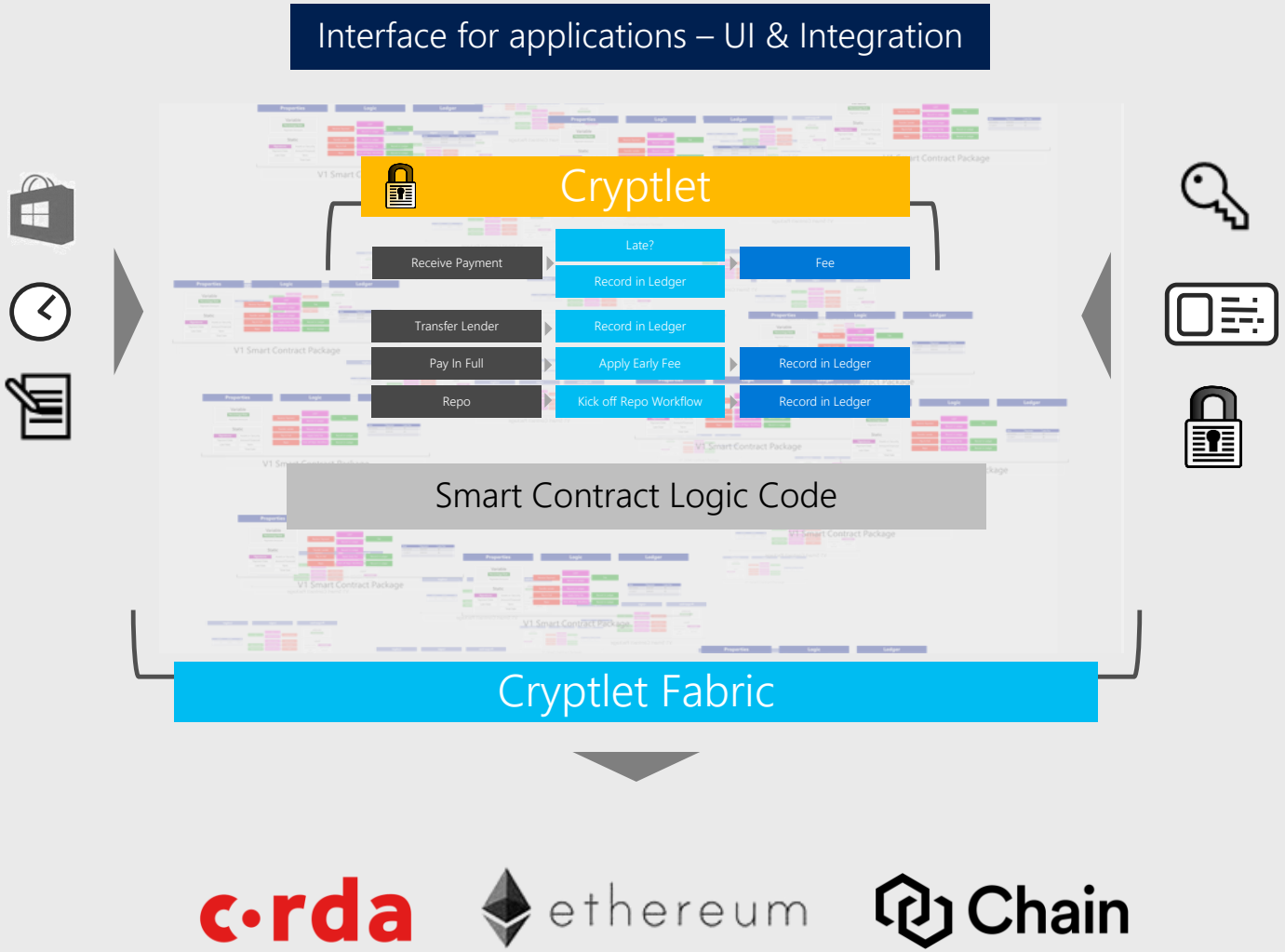


Demo: Quorum

Cryptlets

Contract as a Service

The Cryptlet Fabric



Code from smart contract business logic executes in a fabric that can bind the code to a smart contract, and provides a rich set of services including identity and key management, cryptographic services, attested data and interact with the outside world.

It also abstracts away the blockchains themselves, so the Cryptlet can write to any type of blockchain.

Platform Building Blocks

Cloud

World Wide distributed execution

Environment accessible to any distributed blockchain node.

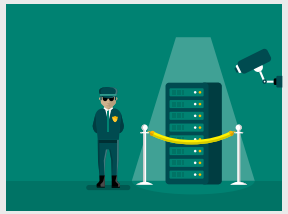
Azure Key Vault

KeyVault

Secure storage, creation and usage of secrets (keys, etc.) for Bring Your Own Key scenarios. HSM in the cloud.

AAD

Identity platform supporting open authentication, authorization and federation. Azure Active Directory



Enclaves

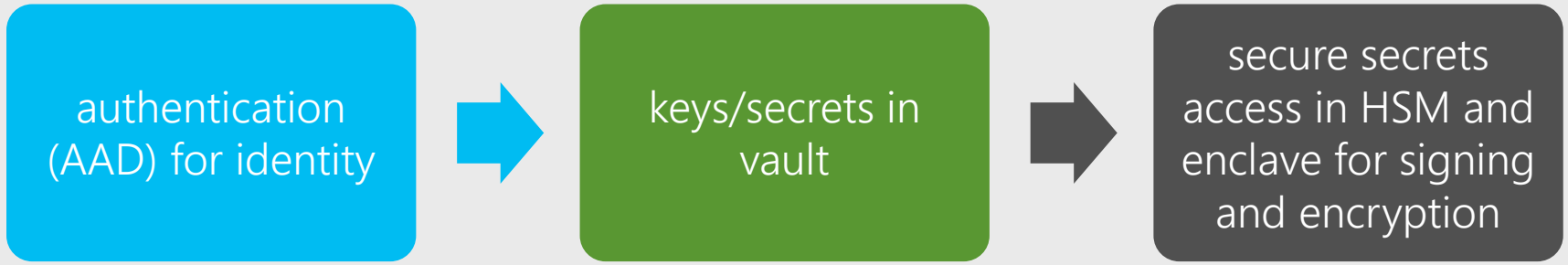
Secure, confidential, isolated compute environment that provide attested proofs of execution.

Infrastructure | Enabling Cloud

Trusted/Confidential Compute capabilities at scale:

- Pooling hardware and software resources for enclaving at WW scale
- On demand creation and secure secrets infrastructure
- Integrated Identity and Authentication platform
- HSM at scale for storage for cloud and on-premises

Working Together



Introducing Cryptlets

Utility Cryptlets

Often referred to as blockchain "oracles" these cryptlets:

- Provide attested interaction with the outside world
- Injection of market prices, external system data
- Watch for events on the blockchain to do something off chain
- Almost anything that you could normally do with middleware: queries, etc.
- Utility Cryptlets are reusable or horizontal and do not perform contract specific logic

Contract Cryptlets

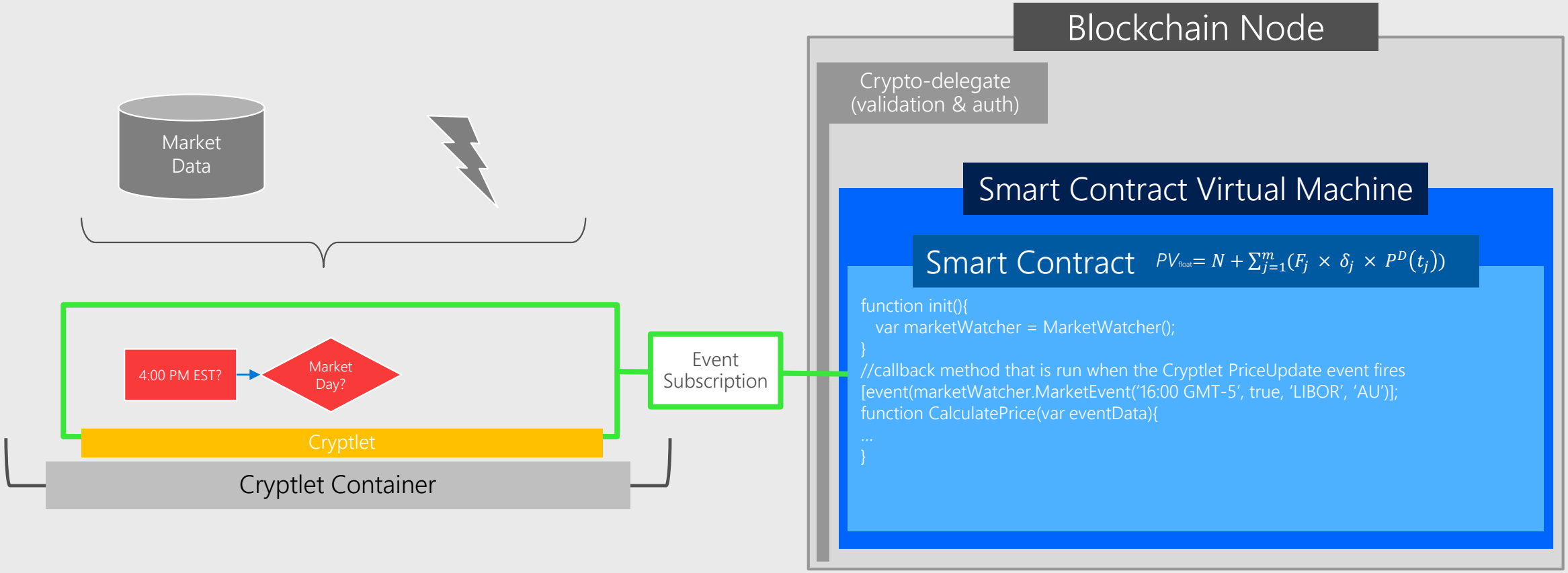
Contain the business logic for a contract:

- Provide a secure and attested execution model for contract specific logic
- Use cryptography and enclaves to perform logic that counterparties can trust
- Use Utility Cryptlets to get attested data
- Provide a strong versioning model for business logic
- Separation of concerns of data and logic allowing each to be scaled and versioned differently
- Advanced crypto features like ring, threshold and homomorphic functionality
- Vertical scale and co-location capable
- Advanced async transactions for multi-step ledger appends.

Utility Cryptlet as oracle

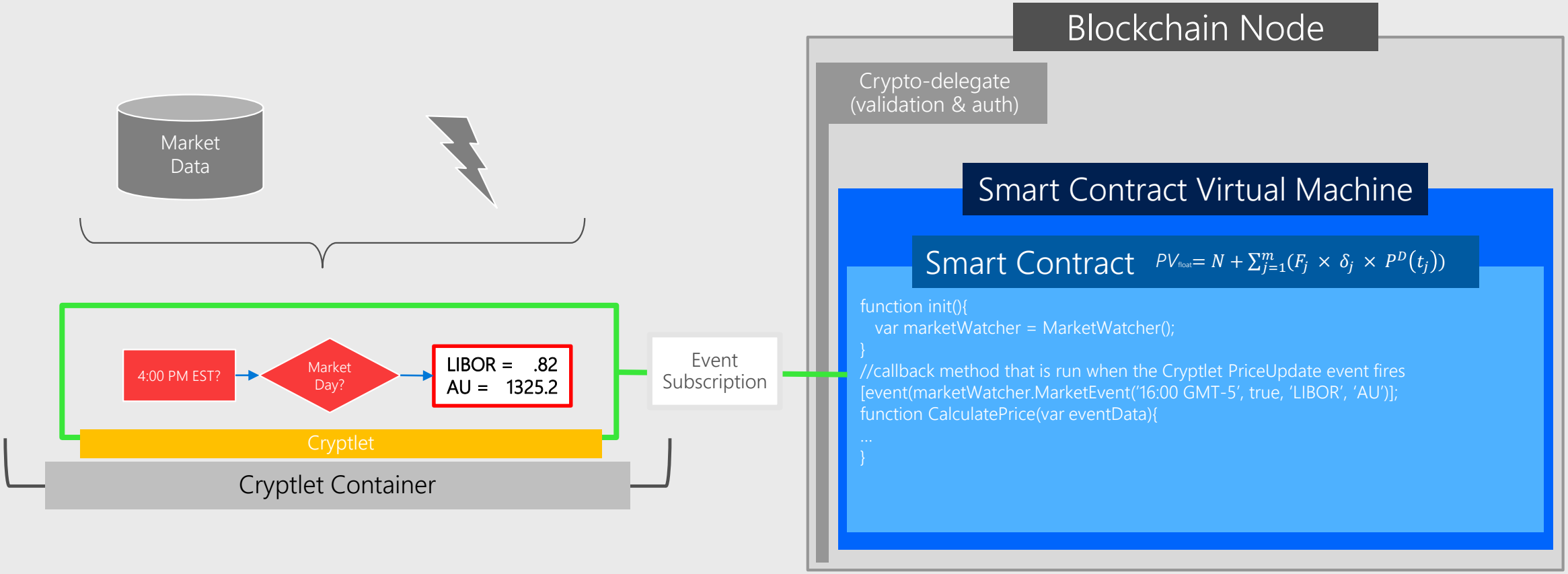
Utility | Smart Contract oracles

On chain smart contract has subscription to a Cryptlet that injects off chain data.



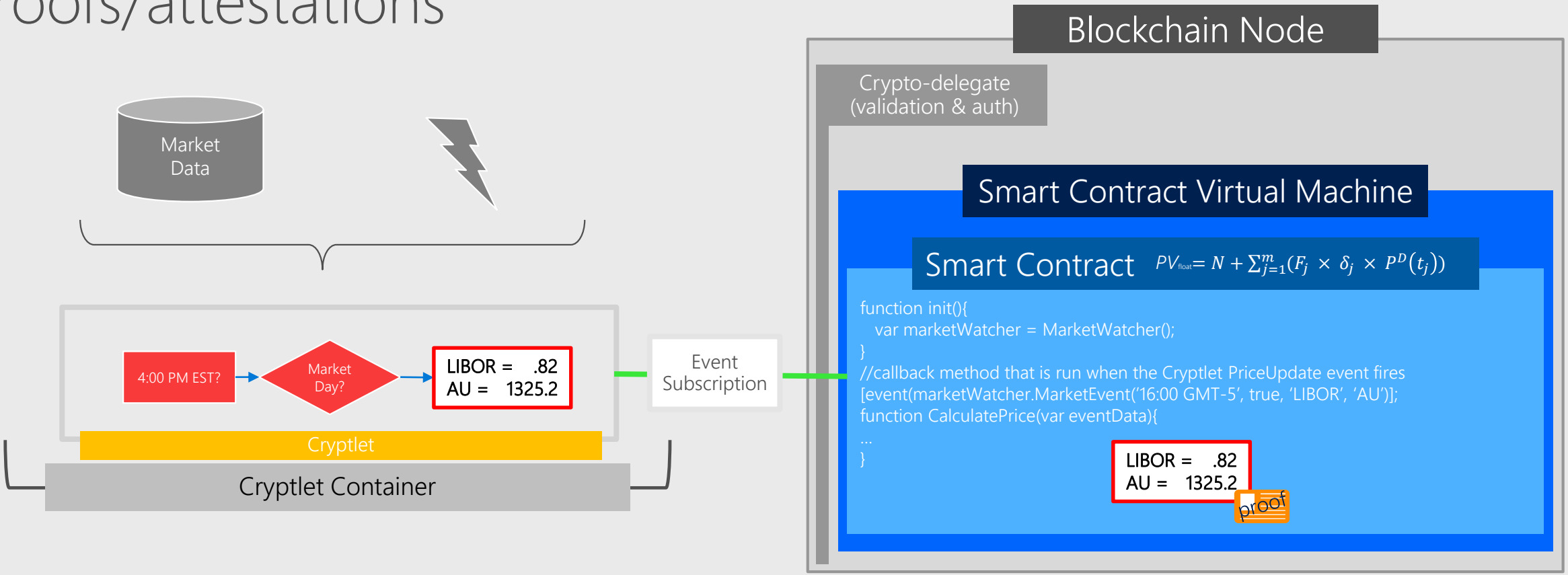
Utility| Smart Contract Oracles

If conditions are met, the Cryptlet prepares requested information.



Utility| Smart Contract Oracles

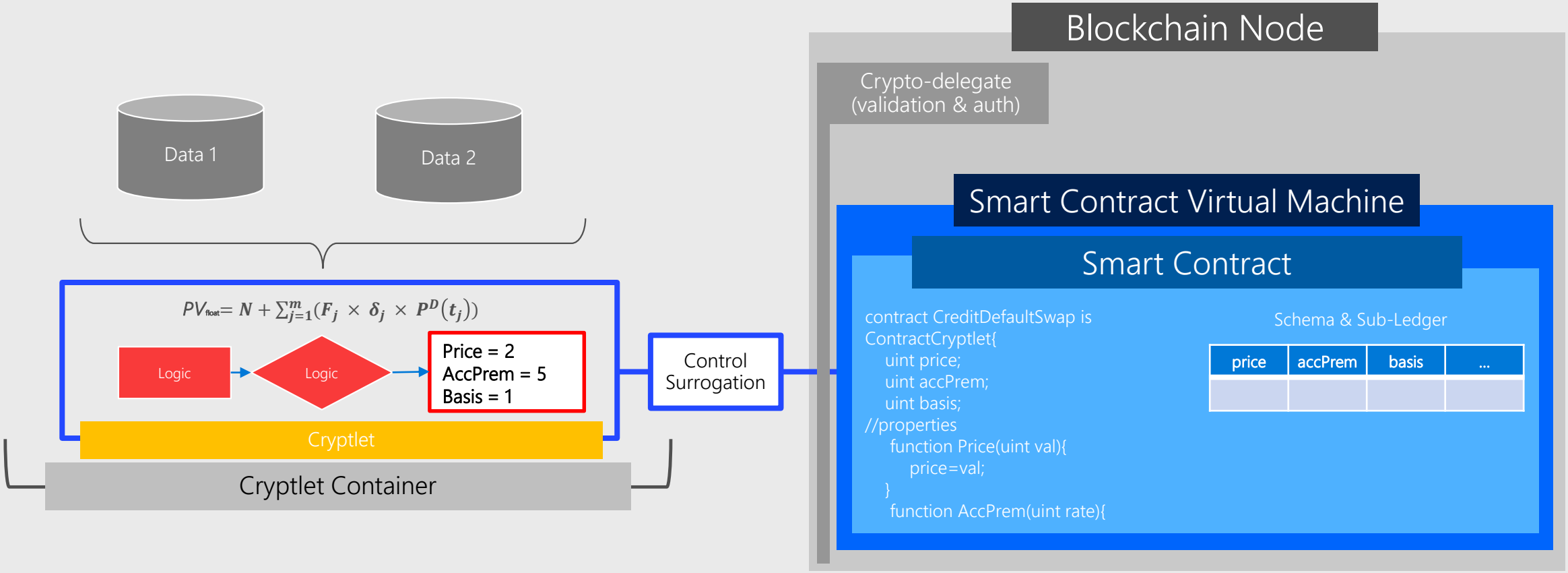
Data is then written to the smart contract on the blockchain. Only the subscribed Cryptlet can update which includes proofs/attestations



Contract Cryptlet

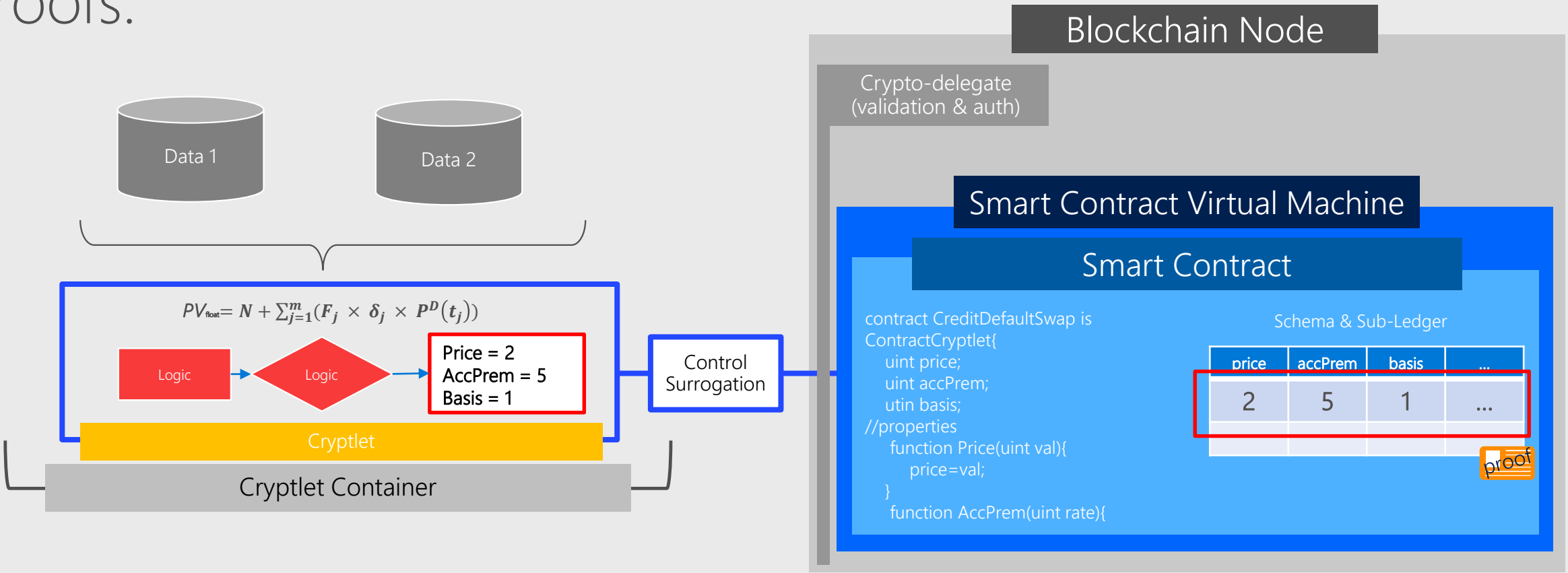
Contract| Smart Contract as Schema

Here, the calculation is done by the Cryptlet off-chain.



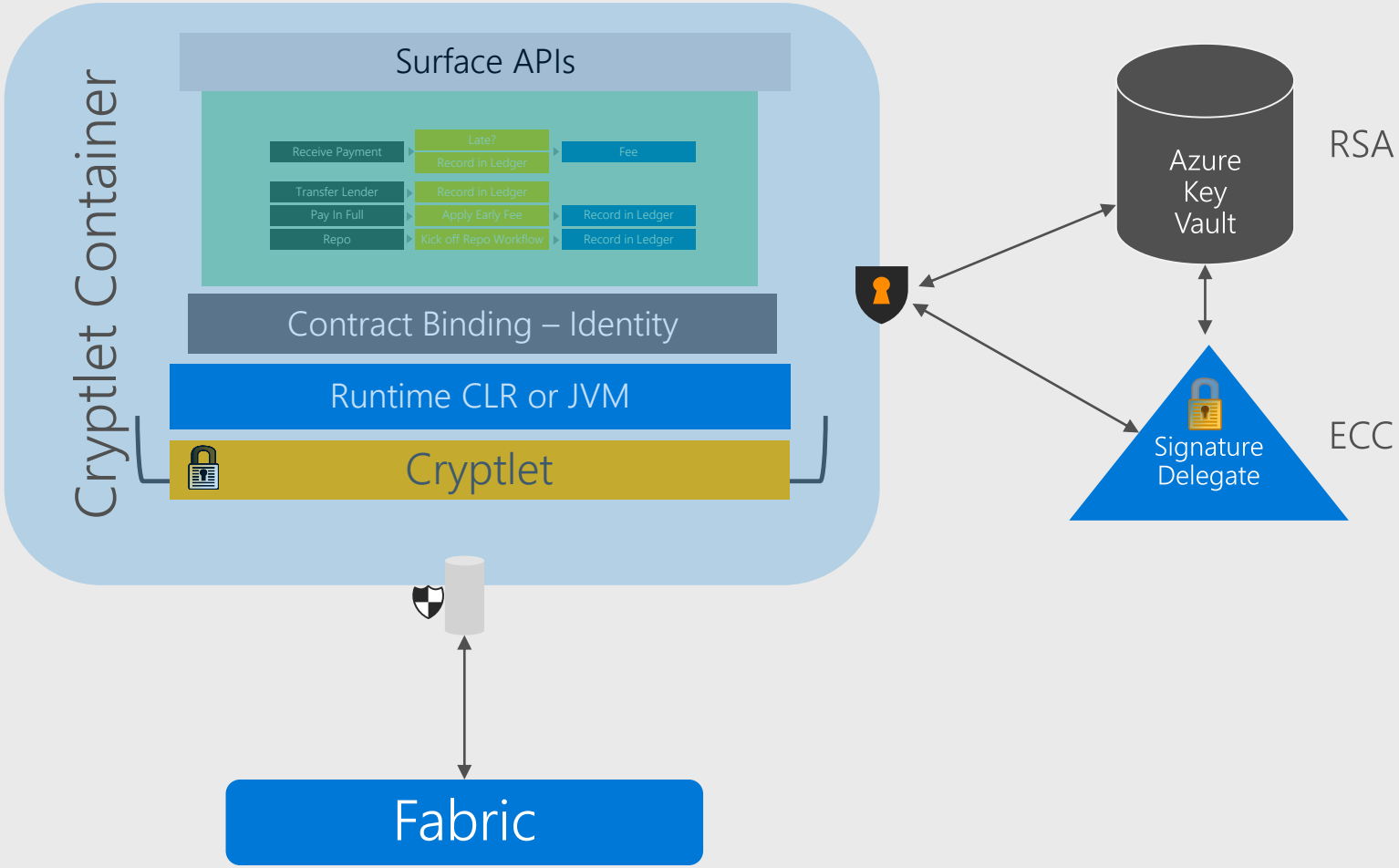
Contract| Smart Contract as Schema

The results are written to the smart contract on the blockchain itself. Only the Cryptlet can update along with proofs.

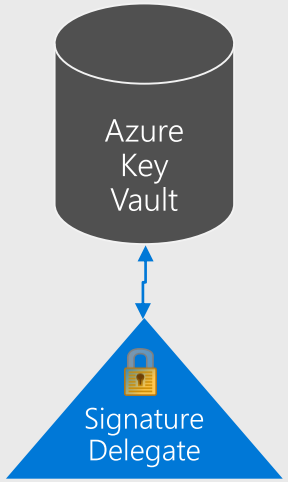


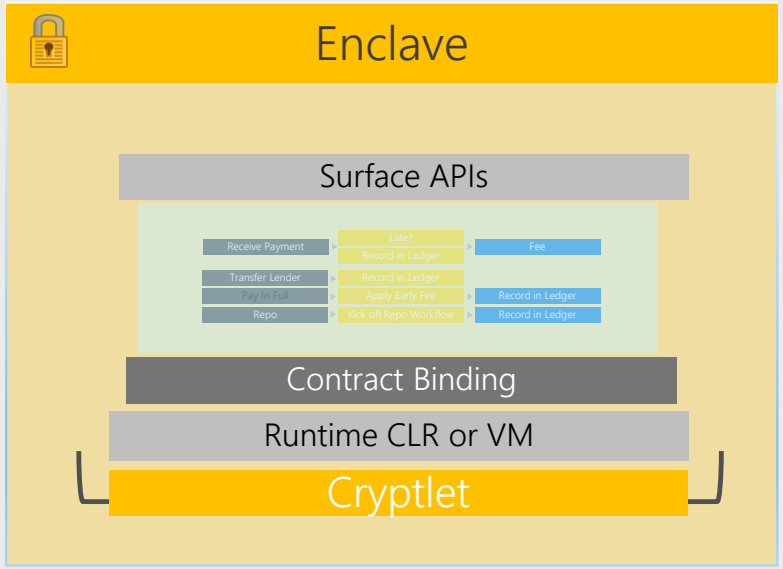
Architecture

Architecture | Key Vault and Signatures



Architecture | Cryptlet Flow

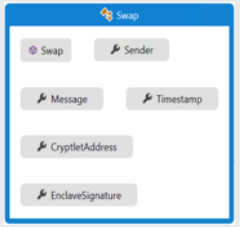




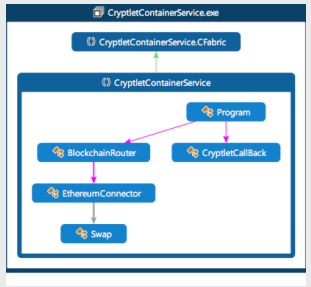
2. **Deploy Contract***: Public Key of Cryptlet wired to SmartContract call back – UpdateAsset() Function. Only msgs from Connector & Cryptlet will be accepted. CryptletBinding created.

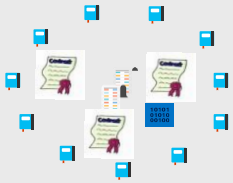
1. **Swap Contract:** Solidity SmartContract designed, referenced Cryptlet. Callback function added or referenced

CryptoSwap



SmartContract

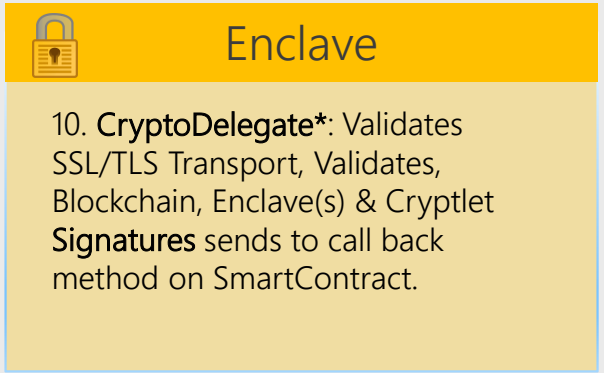




5. **Cryptlet**: Securely Executes, Fires events, builds, signs* and delivers to container

4. **CryptletContainer**: Validates cryptlet, fetch secrets and keys from vault, instantiates cryptlet with binding and provides keychain to cryptlet or Signature Delegate

3. **Cryptlet Framework Service**: Validates CryptletBinding and if active: provisions enclave* - instantiates CryptletContainer with binding information for Cryptlet

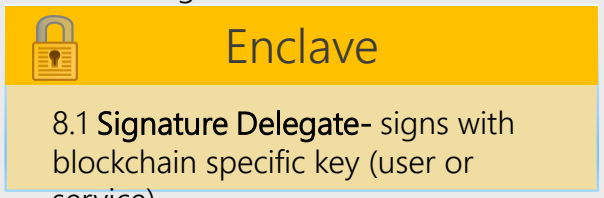


12. **SmartContract**: Validates and stores, send address, Cryptlet Addresses & proofs, executes logic and writes to blockchain

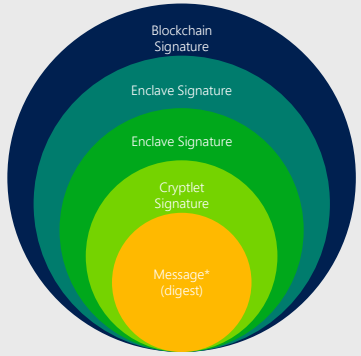
6. **CryptletContainer**: signature delegate if not signed and adds enclave attestation

7. **CryptletContainer**: Sends message to Transaction Builder, enclave signs outbound.

8. **Transaction Builder:** formats message into blockchain specific transaction, signs with blockchain key (user or service) via a signature delegate and places message with binding id on the service bus

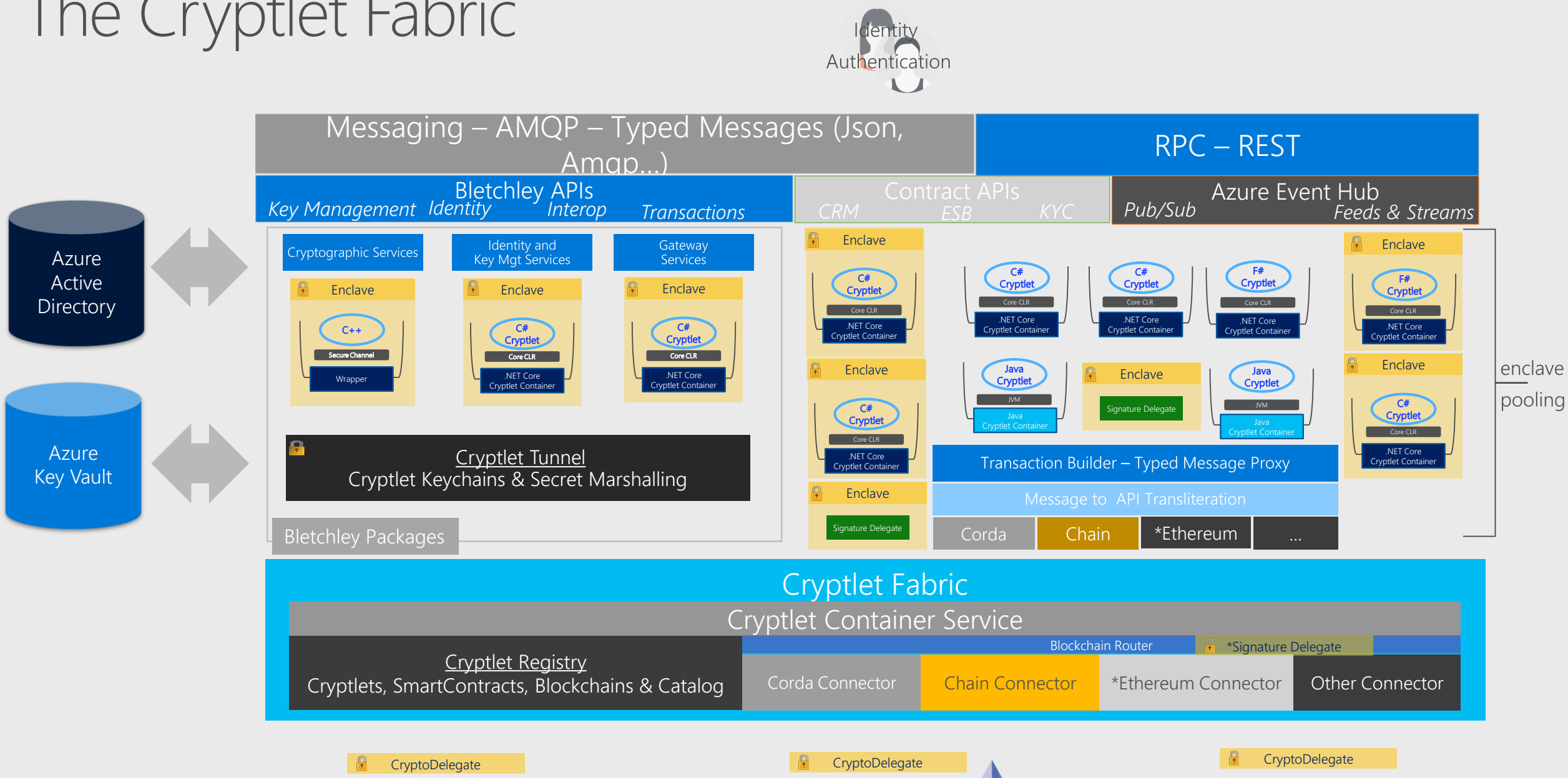


9. **BlockchainRouter**: retrieves the message from the queue, uses the binding id to determine the blockchain endpoint and delivers to a CryptoDelegate or Raw node



Signature Onion

The Cryptlet Fabric



How do you get started?

SIGN UP FOR AN AZURE ACCOUNT

- Blockchain documentation and sign up

https://aka.ms/blockchainsignup

PREVIEW PROGRAM FOR CRYPTLETFX POC FRAMEWORK

- Make an official request by filling out a simple survey

https://aka.ms/blockchainpreview

CONNECT WITH BLOCKCHAIN ENGINEERING TEAM

- Join Blockchain Azure Advisors group on Yammer

http://aka.ms/AzureAdvisors

- Join Microsoft Tech Community for Blockchain

https://aka.ms/blockchaincommunity

- Add suggestions to Blockchain User Voice

https://aka.ms/blockchainuservoice