Open Source Foundries

Blockchain of Things

Tyler Baker

tyler@opensourcefoundries.com

Disclaimer

The information provided in this session is for informational purposes only. It should not be considered legal or financial advice. Please do not make any investment decisions based on this content without first consulting your financial adviser and or conducting your own research and due diligence.

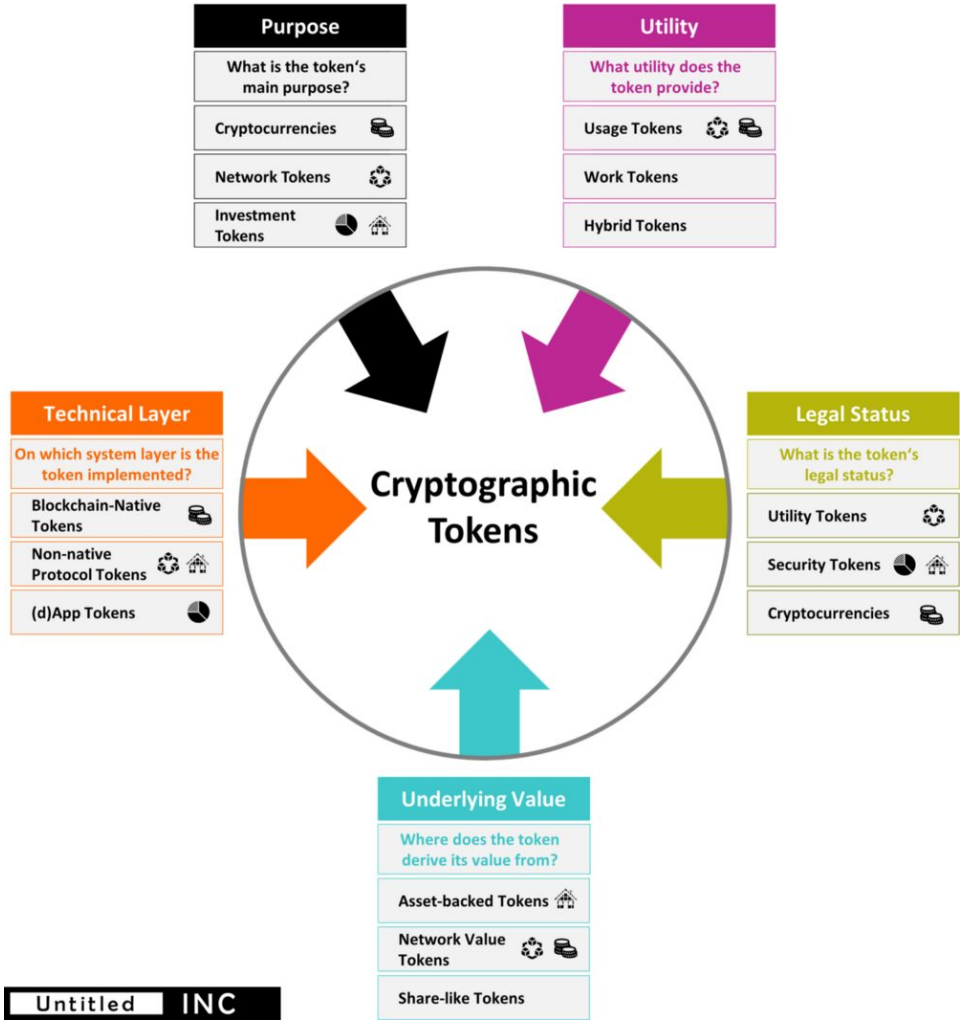
Cryptographic Tokens

OPEN SOURCE
FOUNDRIES

It’s not all about Lamborghini’s

Real world use cases

- Currency
  - Store of value
- Investment
  - Asset value
- Network
  - Provides functionality on a network
- Work
  - Shows contribution
- Security
  - Identification


Purpose
What is the token's main purpose?
Cryptocurrencies
Network Tokens
Investment Tokens
Utility
What utility does the token provide?
Usage Tokens
Work Tokens
Hybrid Tokens
Technical Layer
On which system layer is the token implemented?
Blockchain-Native Tokens
Non-native Protocol Tokens
(d)App Tokens
Cryptographic Tokens
Legal Status
What is the token's legal status?
Utility Tokens
Security Tokens
Cryptocurrencies
Underlying Value
Where does the token derive its value from?
Asset-backed Tokens
Network Value Tokens
Share-like Tokens
Untitled INC

- Critical to operate the blockchain
- Integral component of the blockchain's consensus mechanism
- Part of the blockchain's incentive mechanism for block validators/other nodes

Examples: BTC (Bitcoin, Bitcoin); ETH (Ether, Etherum), STEEM (Steem, Steem)

exchange
- Functions as a store of value

Examples: BTC (Bitcoin), ZEC (Zcash), KIN (Kin, Kik)

actually having to move the underlying asset
- The issuer is responsible to hold the underlying asset
- Introduces counterparty risk

Examples: USDT (Tether USD, Tether), GOLD (GOLD, GoldMint), Ripple IOUs (Ripple)

- Grants holders access to exclusive functionality of the service

Examples: BTC (Bitcoin), STX (Stacks, Blockstack)

- Closely tied to the functionality of the issuing network or application
- Internal network/app currency but not necessarily attempting to be a currency
- Grants owners the right to actively contribute to the system vs. passive investor role
- Avoids security-like features

Examples: GNO (Gnosis), STEEM (Steem)

Non-native Protocol Tokens

Description: A token that is implemented in a cryptoeconomic protocol on top of a blockchain

Characteristics:
- Integral component of the protocol's consensus mechanism
- Part of the protocol's incentive mechanism for nodes
- Tracked on an underlying blockchain to which it is not integral (e.g. ERC20 Tokens on Ethereum)

Examples: REP (Decentralized Oracle Protocol, Augur)

Network Tokens

Description: A token that is primarily intended to be used within a specific system (e.g. network, application)

Characteristics:
- Token has functionality within the issuers system
- Not intended as a general cryptocurrency

Examples: GNO (Gnosis), STX (Stacks, Blockstack)

Network Value Tokens

Description: A token that is tied to the value and development of a network

Characteristics:
- Tied to the value generated and exchanged on the network (e.g. transaction fee volume)
- Closely intertwined with key interactions of network participants

Examples: ETH (Ether, Ethereum) STEEM (Steem)

Work Tokens

Description: A token that provides the right to contribute to a system

Characteristics:
- Owning Tokens is the precondition for contributing to the system
- Contributions are either incentivized with a rewards system or holders get utility from the system/decentralized organization

Examples: REP (Reputation, Augur), MKR (Maker, Maker DAO)

Security Tokens

Description: A token that behaves like a security

Characteristics:
- Showcases security-like features, e.g. voting on decisions regarding the issuing entity, dividends, or profit shares
- Holders are regarded as owners
- Little or insufficient utility

Examples: SPiCE (SPiCE VC), Bitwala (tba)

(d)App Tokens

Description: A token that is implemented on the application-level on top of a blockchain (and potentially protocol)

Characteristics:
- Integrated within the application
- Part of the app's incentive mechanism for nodes and/or users
- Tracked on an underlying blockchain to which it is not integral (e.g. ERC20 Tokens on Ethereum)

Examples: WIZ (Wisdom, Gnosis), SAFE (Safecoin, SAFE Network)

Investment Tokens

Description: A token that is primarily intended as a way to passively invest in the issuing entity or underlying asset

Characteristics:
- Promises owners a share of asset value or in (future) success of the issuing entity
- No or little significant functionality

Examples: Neufund Equity Tokens (Neufund), DGX (Digix Gold, DigixDAO)

Share-like Tokens

Description: A token with share-like properties

Characteristics:
- The issuer promises token owners a share in the success of the issuing entity (e.g. dividends, profit-shares)
- May or may not come with voting-rights
- Mostly on no/weak legal basis

Examples: DGD (DigixDAO), LKK (Lykke)

Likely to be classified as a security token

Hybrid Tokens

Description: A token featuring traits of both usage and work tokens

Characteristics:
- Grants access to system functionalities
- Allows owners to contribute to the system

Examples: ETH (Ether, Ethereum, after Casper), DASH (Dash)

Cryptocurrencies

Description: A token that is a pure cryptocurrency

Characteristics:
- Acts as a store of value and medium of exchange
- Not emitted by a central authority against which owners have claims

In Germany (according to BaFin):
- currently not regarded as lawful, functional currency
- not regulated by e-money laws

Examples: BTC (Bitcoin), ZEC (Zcash), LTC (Litecoin)

*details dependent on respective jurisdiction

Security of Things

OPEN SOURCE
FOUNDRIES

Don’t trust people on the world wide web

Trustless Consensus

- Distributed consensus for validating transactions
  - Mining or Staking
- Decentralized ledger for recording transactions
  - Entire history of validated transactions exist on all nodes of the network
- Combining IoT and blockchain
  - Provides digital identities
  - Removes centralized transaction model

Proof of X

OPEN SOURCE
FOUNDRIES

PoW (Proof of Work)

Provides security for the blockchain network

- Data payload that is difficult to produce, but easy to verify
  - Miners use PoW to verify each transaction in a block
- Computationally expensive to create many transactions
  - Mitigates DDoS attacks, however most blockchains are vulnerable to the 51% attack
- “Hello World” Example
  - Find a variation of it that SHA-256 hashes to a value beginning with '000'
  - Append incrementing integer to string called a noonce

```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9
```

PoW for IoT

Computationally expensive operations

- Hashcash with double iterated SHA256
  - Wouldn’t be feasible on a small footprint MCU
  - A larger application processor with AES extensions or OpenCL support is a better fit
- Hashcash Lite
  - Created for IoT applications (IOTA)
  - Proof of concept
- Storage
  - Storing entire blockchain on a small footprint MCU isn’t feasible either
  - Needs to offloaded or a different solution developed entirely

PoS (Proof of Stake)

Staking tokens provides network security

- Staking provides transaction validation without massive resources
  - Validators stake tokens in an attempt to solve block
- Expensive to attack
  - Mitigates DDoS attacks, as attacker would need to control 51% of all circulating tokens
- Storage still an issue for IoT
  - Each staking node needs a blockchain locally
  - Much less resource intensive than PoW

Many other consensus algorithms

- Delegate proof of stake
- Proof of importance
- Proof of existence
- Proof of capacity

Digital Identities

OPEN SOURCE
FOUNDRIES

Create an identity for your device

Storing data on the blockchain allows you to create a tamper proof digital identity

- Wallet addresses are hashed versions of public key
  - Transactions from a specific wallet address are searchable
- Private key enabled access to wallet
  - These need to be secured like any other key or certificate
- Services can use wallet addresses to consume transaction data
  - Trust is established through public/private key encryption
  - i.e. Only consider transactions from a known set of wallet addresses

Use Cases

Asset Tracking

- Automotive History
  - Service
  - Ownership
    - Transfer of ownership
  - Accident
- Supply Chain
  - Tracking assets
  - Verification of delivery
- Lending
  - Creating debt and settlement layers

Automated Machine Economy

OPEN SOURCE
FOUNDRIES

Machine to Machine payments

The problem set

- Payments need to happen fast
- How to do you accurately assess value
- How are payments requested
- Where do the token go

Use cases

- Parking meter detects car, requests payment. Car receives payment request, and creates a transaction. Parking meter receives payment, and starts meter.

Proof of Concept

OPEN SOURCE
FOUNDRIES

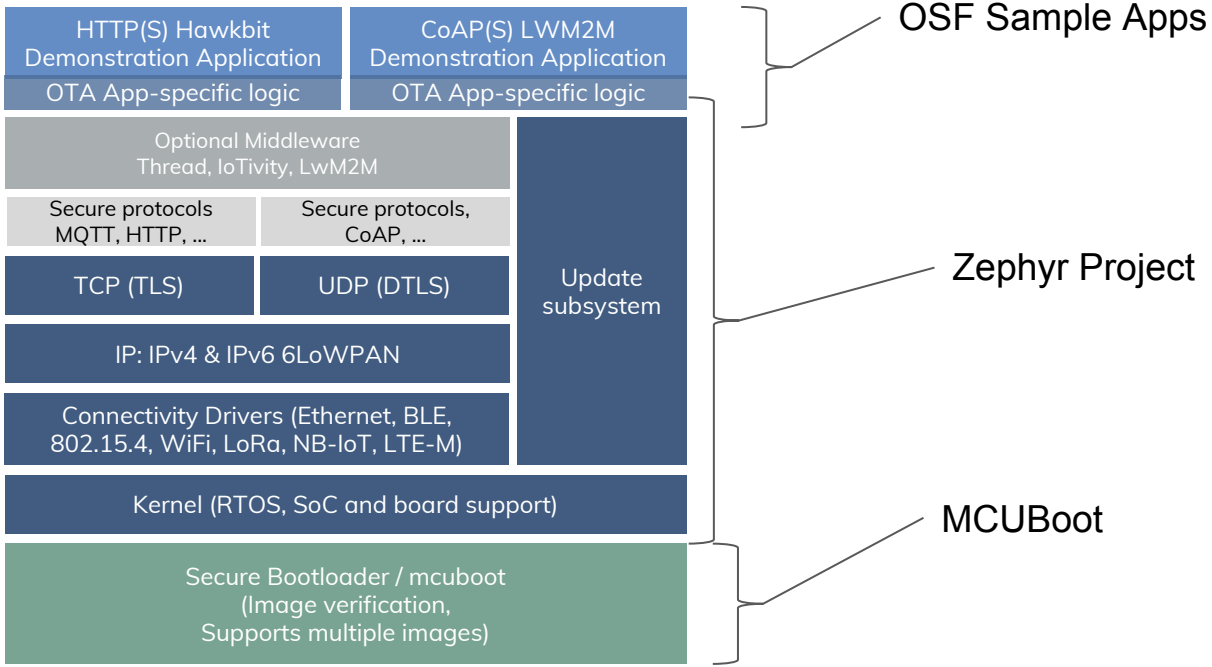
Demo

Marshalling sensor data to the IOTA distributed ledger (Tangle)

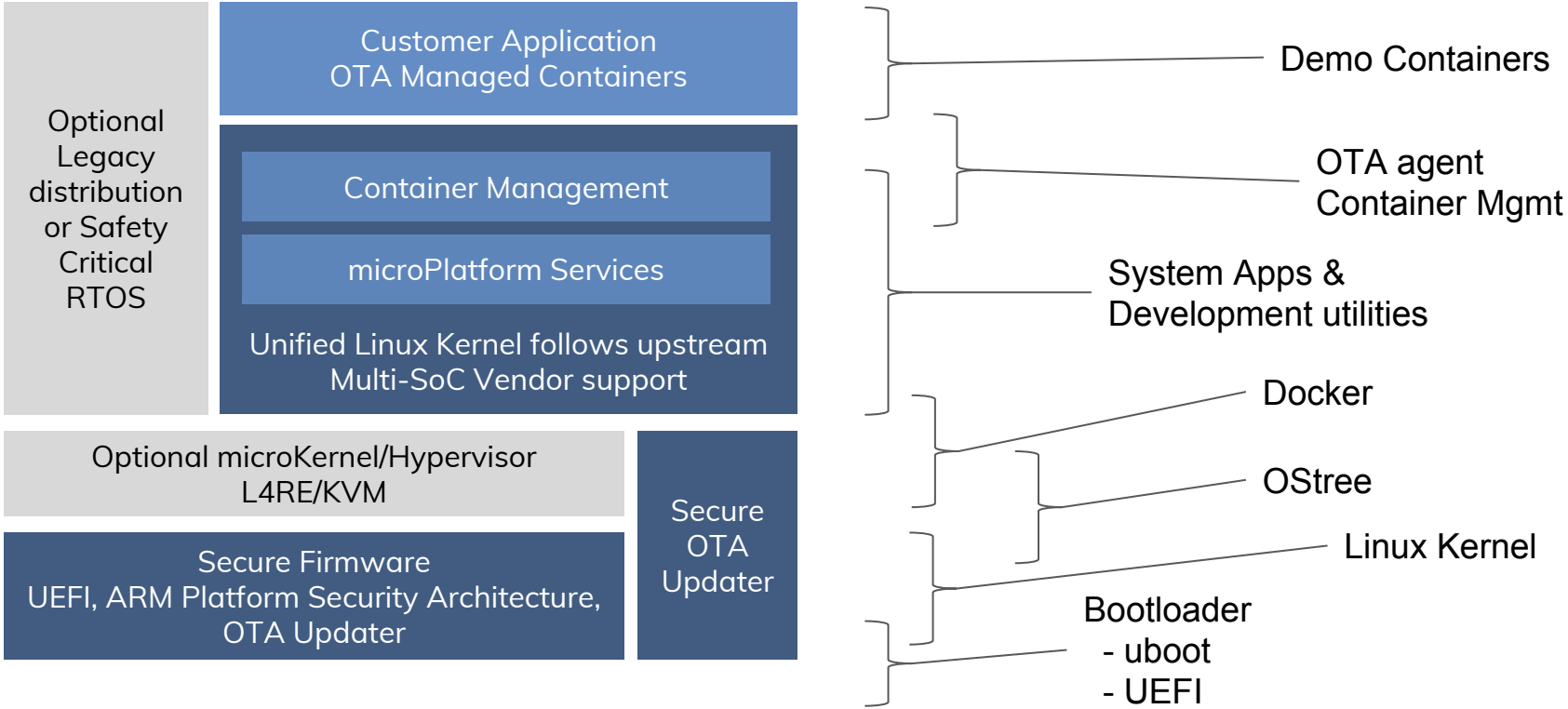
- End devices
  - Nordic NRF52 BLE Nano2 producing MQTTS temperature data
  - Connected to gateway using 6lowpan over BLE
  - Running on CR2032 coin cell batteries
  - Devices are not blockchain/ledger aware
- Edge Gateway
  - Minnowboard Turbot running the Linux microPlatform
  - Containerized microservices provide proxy services to end devices
  - MQTTS messages will be brokered by service, and attached to the tangle
  - Proxy service provides proof of work computation on gateway
- Cloud
  - Reads sensor data from tangle, and display device sensor data

http://opensourcefoundries.com

Zephyr microPlatform - OS for microcontrollers



Linux microPlatform - OS for embedded systems



Thank you


OPEN SOURCE
FOUNDRIES


Embedded Linux
Conference


OpenIoTSummit

Questions

- Why Blockchain, instead of other data lakes?
  - Snowflake
- Blockchain / decentralized today, what’s tomorrow
- Why shouldn’t you roll your own Crypto Currency
- How do you chose the appropriate blockchain currency
-