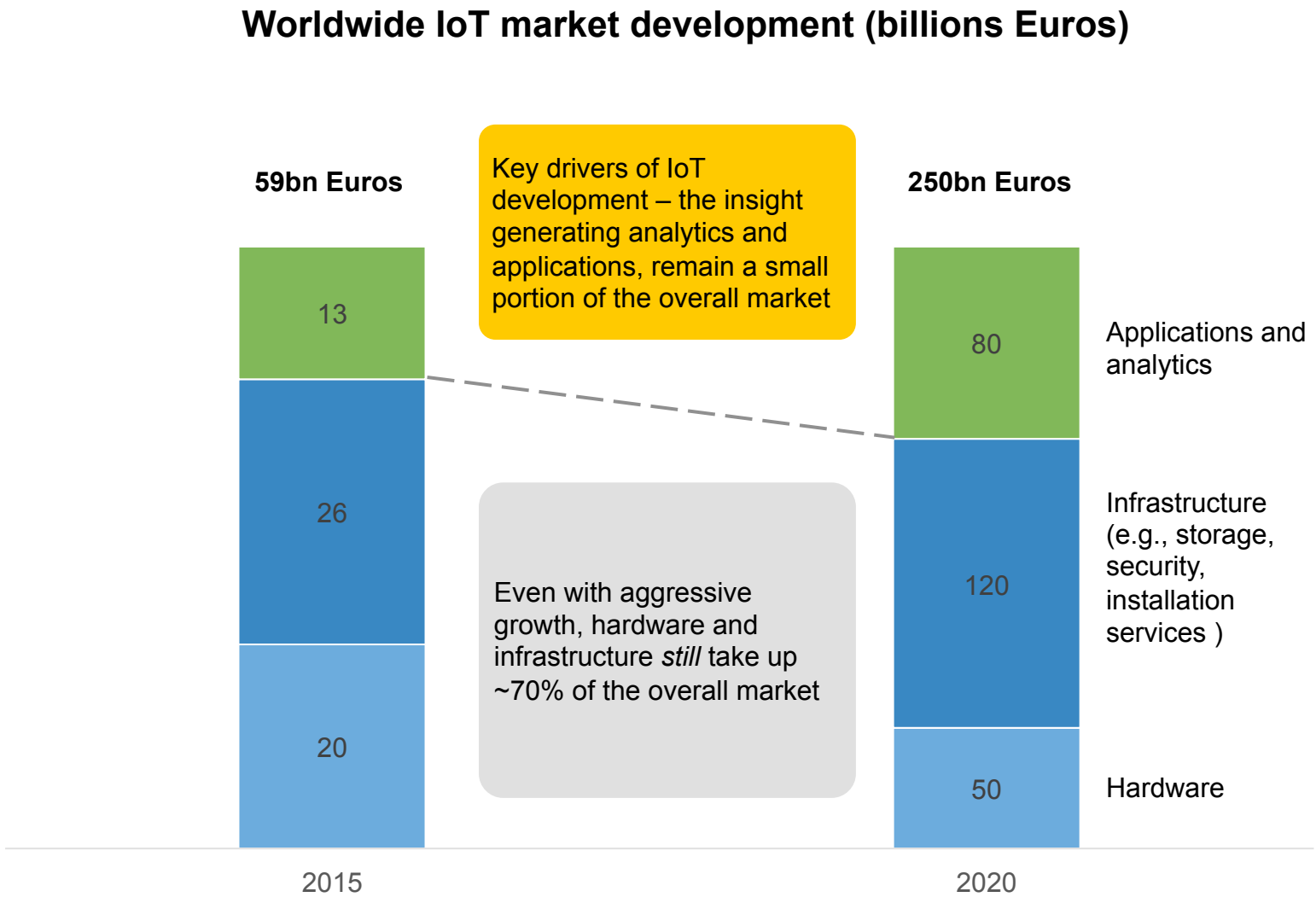

Democratizing IoT data with lightning-fast concurrent smart contracts

# The Taraxa Protocol

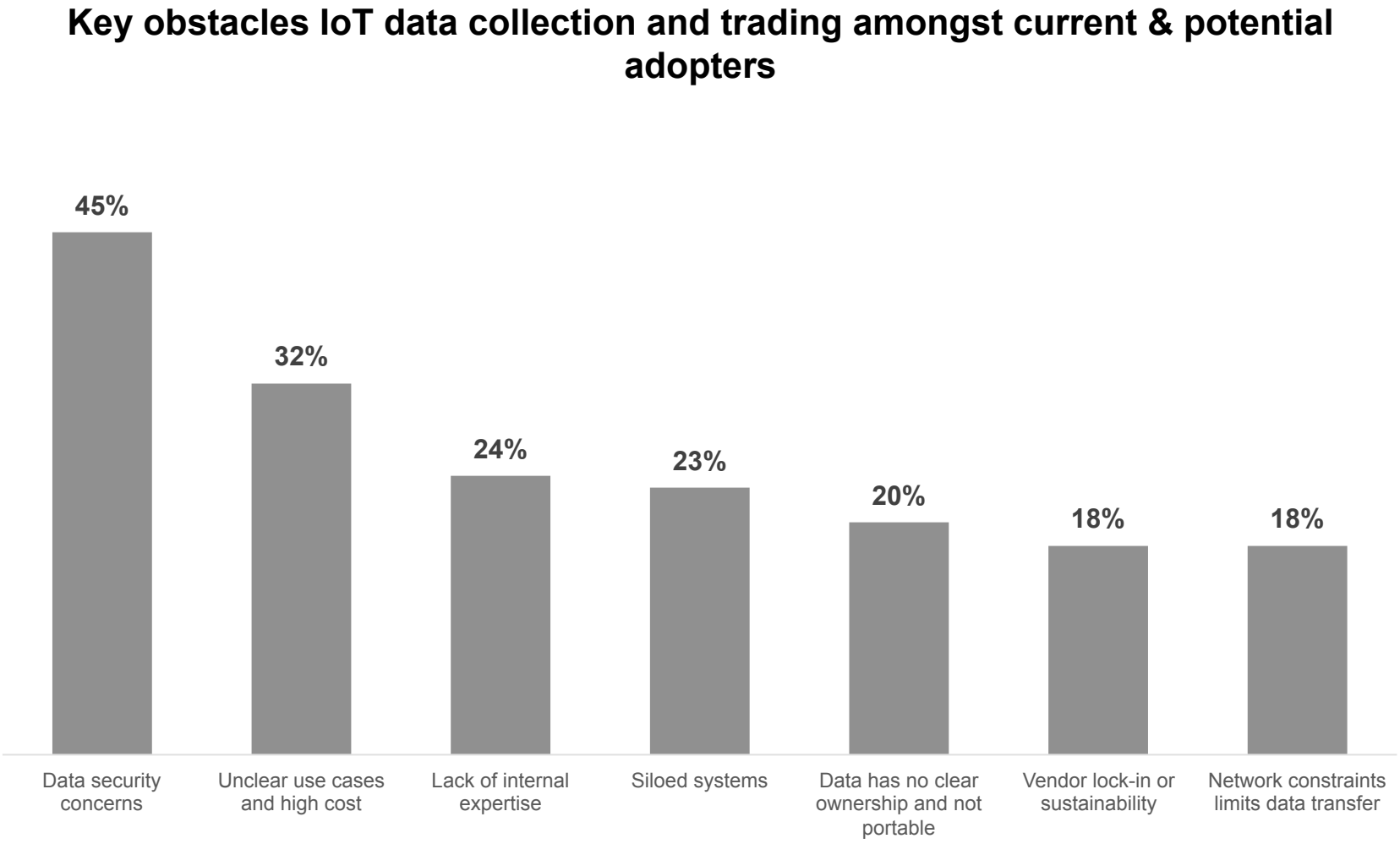
April, 2018
contact@taraxa.io

# The IoT sector's full potential is held back by a lack of applications, largely driven by insufficient sharing and trading of collected data




Source: BCG, internal analysis

# Data collection and sharing are held back by a set of obstacles amongst current and potential IoT adopters




Source: Bain, internal analysis

# The emergence of blockchain and decentralized ecosystems could alleviate many of these obstacles and help to accelerate IoT's growth

**Obstacles to IoT data sharing**

- Data security
- Ownership & data portability
- Vendor risk
- Network constraints
- Lack use cases and high cost
- Siloed systems
- Lack internal expertise

**How blocchain technology & ecosystems could address these concerns**

### Decentralized Operating Model

- A decentralized model guarantees that no single person or entity controls the ecosystem
- Transparency amongst all dealings minimizes the risk of foul play
- Decentralized resources and services are leveraged to provide a host of services

### Open Source, Open Innovation

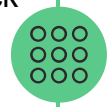
- An open innovation model leverages a global open source community's expertise to create innovative use cases
- IoT data could easily become a profit center as they're traded

### Cryptographically Secure

- Blockchain ecosystems have proven to be highly resistant to attacks, ensuring that the data is secure and anonymous if need be
- Ownership is easily defined and enforced through blockchain

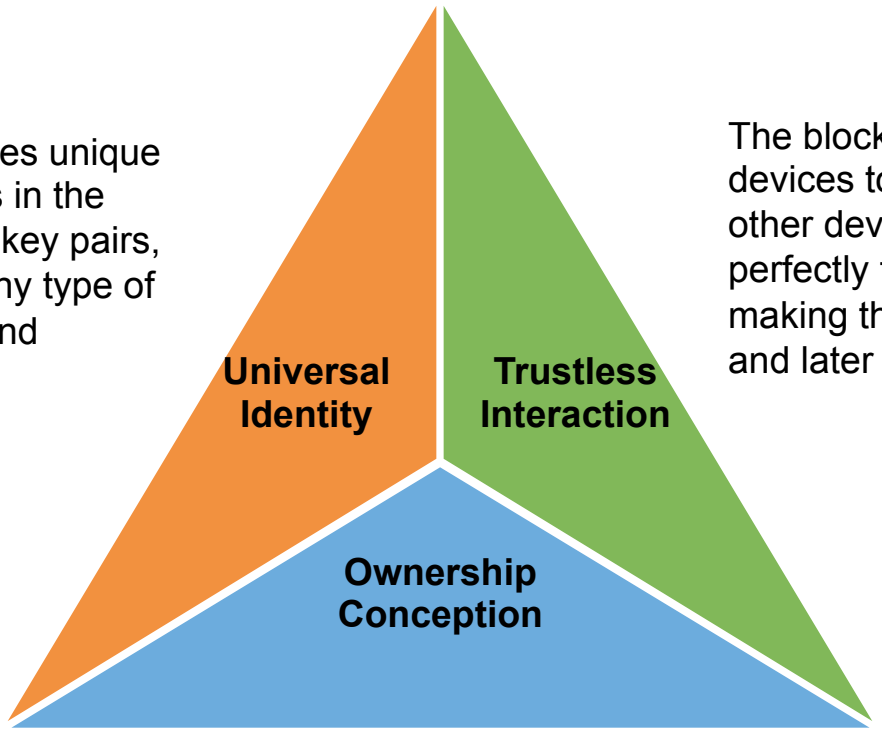
### Fractionalized Resources

- Blockchain helps to both unlock underutilized resources and fractionalize storage and processing to pay-as-you-use units



# Blockchain can help give IoT devices universal and persistent identities, instill concepts of ownership, and enable trustless interactions

Blockchain gives devices unique and universal identities in the form of public / private key pairs, forming the basis for any type of network participation and authentication




The blockchain ledger allows devices to freely interact with other devices and humans in a perfectly trustless manner, making them fully independent and later autonomous entities

By hosting a node, devices now have a platform through which it can claim ownership to crypto-tokens as well as data sets

# Decentralized IoT data markets are the most likely application in the short term – we're in close negotiation with partners in these verticals

## Internet of Cars

Each vehicle generates reams of data through its OBD devices, much of which have compelling commercial use cases with insurers, repair shops, and auto manufacturers.

Within Taraxa, each vehicle will become an independent node that participates in data transactions on the data market.

## Crop Intelligence

With rapid adoption of drone-assisted crop protection (e.g., pesticides) delivery, hitherto non-existing crop data could now be collected via cameras and other sensors on the drone, generating intelligence on planting distribution, growth stage, and even pest (e.g., insects, weeds) growth.

Within Taraxa, each drone will become a seller of its collected data.

## Smart Parking

More widespread deployment of parking sensors could generate more income for parking operators by turning underutilized spaces into new parking lots, dynamically adjusting pricing, and with charging stations could arbitrage power pricing.

Within Taraxa, IoT gateways aggregating parking lot and charging station sensors' streaming data could offer them in a data market.

# We've designed the Taraxa protocol to address not only IoT-specific requirements, but also more general scalability challenges in blockchain

### Near Instantaneous Transactions

The block lattice asynchronous topology enables near instantaneous transactions, with preliminary test results show 300+ tps with far faster speeds possible*

### Trustless Light Node for IoT

Implemented the first practical light node, enabling resource-starved IoT devices to become a trustless and independent participant within the network

### Concurrent Smart Contracts

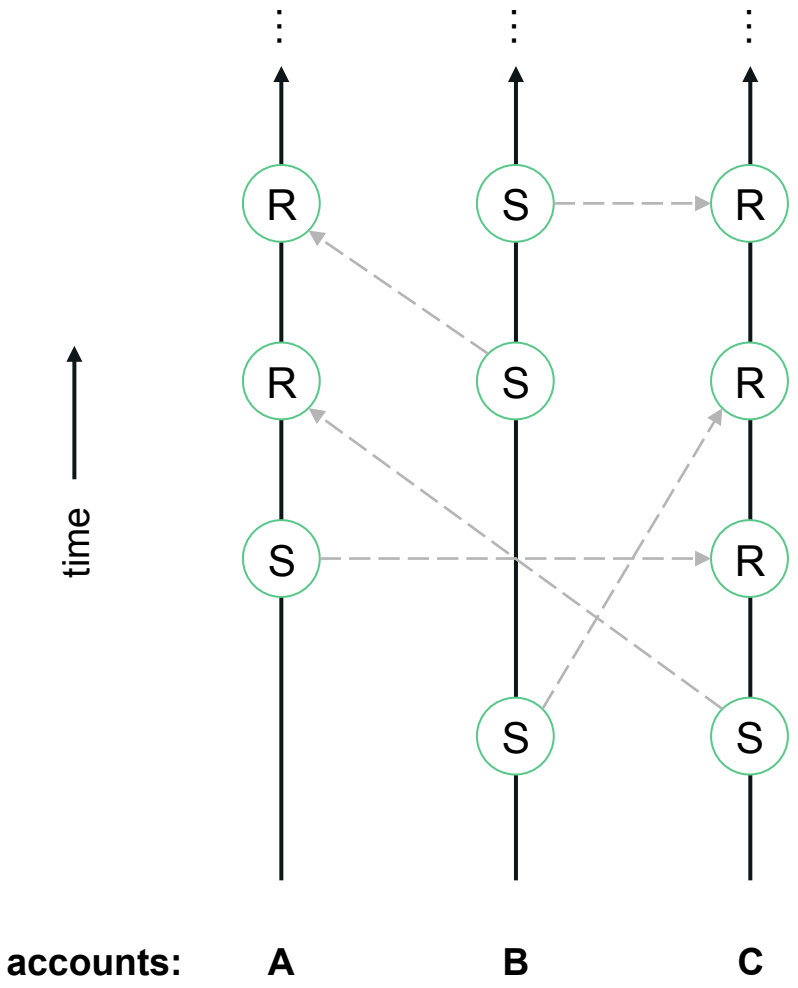
Implemented the first concurrent smart contract system inspired by STM principles, allowing for +100x speedup of contract processing throughput compared to Ethereum

### Encrypted Data Markets

Taraxa comes with a set of encryption algorithms, contracts, and concurrent data structures to enable our ecosystem partners to easily build encrypted data markets to facilitate IoT data trading

* The current anti-spam mechanism utilizes PoW, which could be replaced by a burnt-fee system which would be far faster

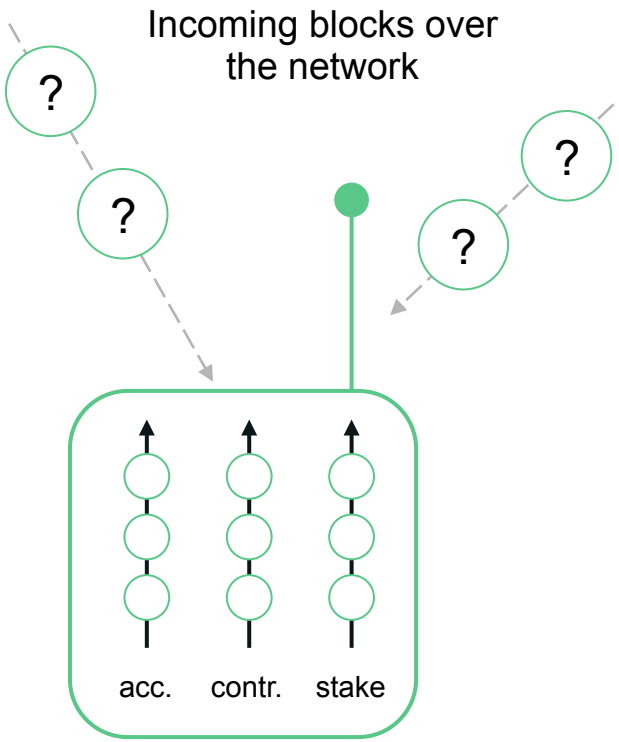
# The block-lattice ledger as pioneered by Nano enables fully asynchronous transactions with a balanced-weight vote consensus




- Each account and smart contract has its own blockchain
- A transaction begins with a send block created on the sender's chain, and is confirmed by a corresponding receive block on the recipient's chain
- Each account delegates their stake's voting power to a representative, whose voting power attached to their broadcasted blocks is used to resolve forks (e.g., double-spends) and later smart contract
- The system uses UDP instead of TCP with lower overhead, and the small packet size (under 508 bytes) minimizes network packet fragmentation

Source: Nano whitepaper, Taraxa whitepaper

# Based on the DPoS consensus and a set of voting stake distribution snapshots, light nodes are able to operate independently and trustless-ly

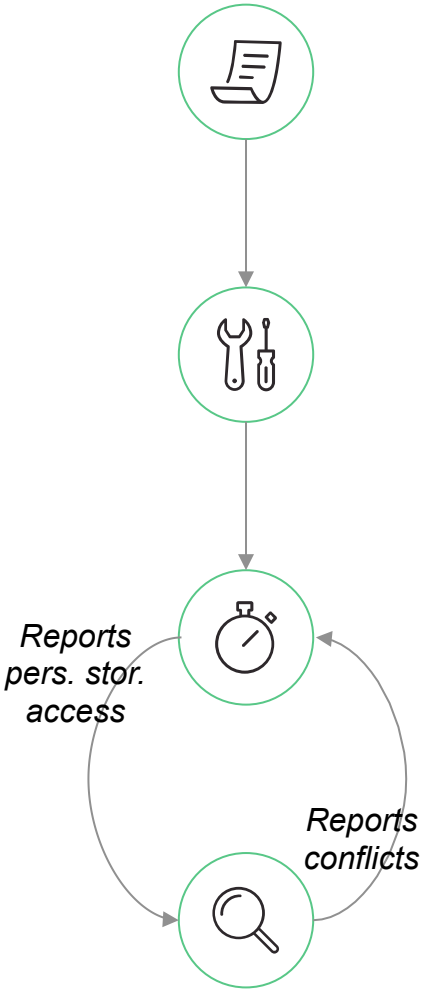



**Light node installed on an IoT device**

- IoT devices have limited processor and memory capabilities, requiring a practical light node design
- Instead of the entire ledger, each light node only stores 3 types of chains: its own account's chain, the chains of smart contracts it has deployed, and the network's stake distribution chain
- Every 24 hours the network appends a snapshot of the current voting stake distribution amongst representatives onto a stake distribution chain
- This allows light nodes to tally up votes confidently from the signed packets it hears from the network, allowing it to participate in a near-trustless manner in the network

Source: Taraxa whitepaper

# With its concurrent VM design and data structures, Taraxa can push smart contract processing throughput to over 100x compared to the EVM




**Smart contracts** written mature languages such as C / C++

**Toolchain** compiles into WebAssembly bytecode

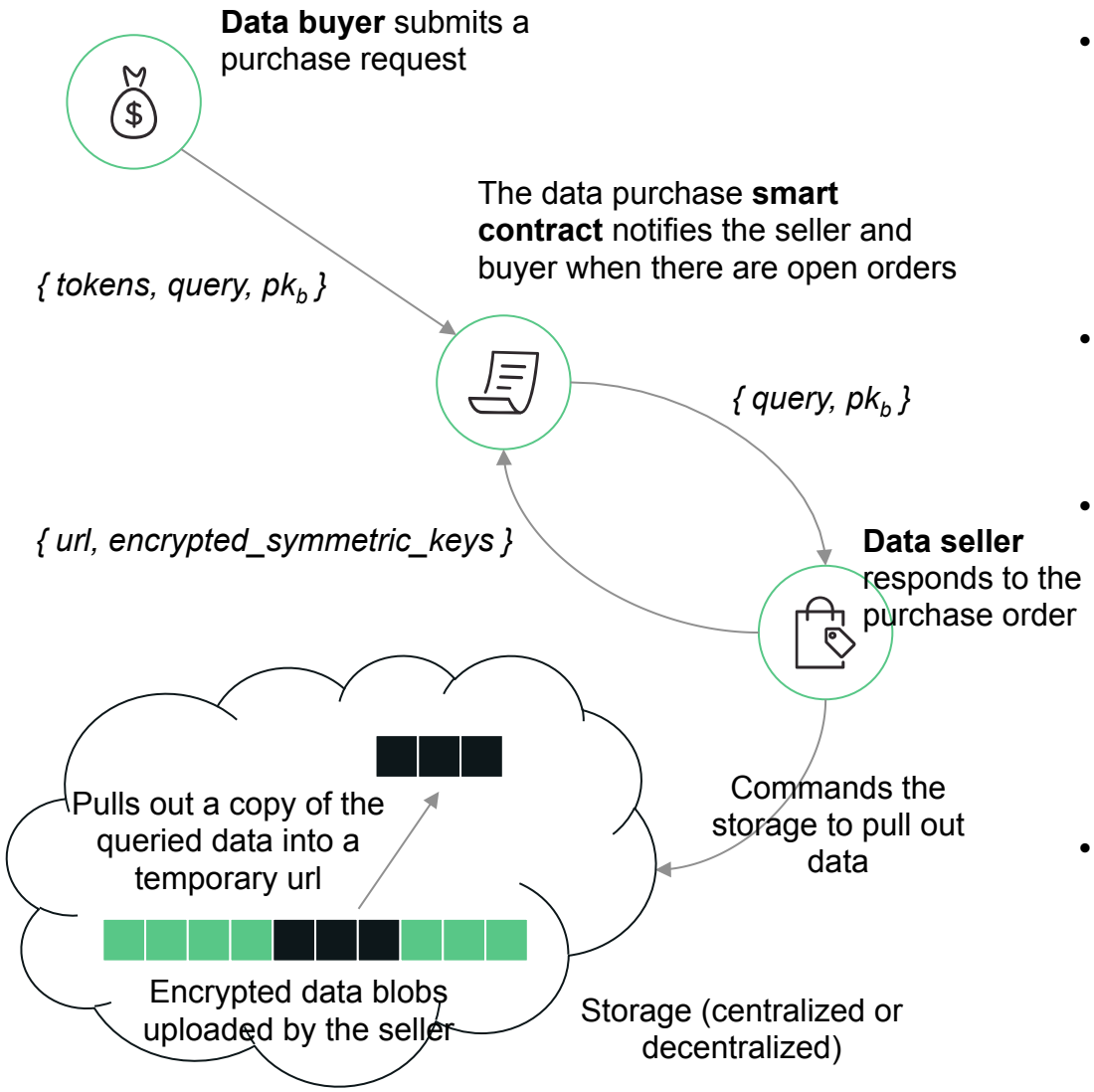
**Concurrent scheduler** creates, monitors, kills, and re-schedules sandboxed VM instances for contract calls in parallel

**Conflict detector** watches for persistent storage conflicts and reports to the scheduler

- Taraxa adopts the WebAssembly standard, enabling developers to use well-studied, mature languages such as C and C++ as well as their associated toolchains
- According to the principles borrowed from STM, the concurrent scheduler optimistically executes contract calls in parallel, with each parallel thread reporting persistent storage access to the conflict detector
- If the conflict detector sees a conflict, it reports it back to the scheduler which kills the conflicting threads, rolls back their changes and reschedules them for sequential execution
- At the end each parallel execution set, the scheduler publishes a concurrent schedule used when other nodes try to validate the results

Source: Taraxa whitepaper

# Taraxa comes packaged with ready-made smart contracts, data structures, and encryption libraries to enable encrypted data markets




Source: Taraxa whitepaper

- The data seller – likely an IoT device, encrypts its data by segment using a deterministic algorithm from its private key and some unique elements of the data blob
- The seller pays into a data purchase smart contract with his query and public key
- The seller pulls out a separate copy of the requested data, encrypts the symmetric keys with the seller's public key (asymmetric), then returns the url of the blob and the encrypted key set back to the smart contract
- The contract then releases the coins to the seller, and the buyer is able to read the data from the contract, completing the transaction

# Our team is made up of world-renowned academics, researchers, and engineers, most with long-standing experience in blockchain

## Core Team

**Steven Pu**
IoT entrepreneur, strategy consultant; LinkSens, Monitor Deloitte; Stanford BS & MS in EE.

**Ilja Honkonen**
Distributed computing, space weather modeling; NASA, Finnish Meteorological Inst, U. of Helsinki PhD in Physics.

**Vikram Saraph**
Distributed computing, software concurrency; Brown U. PhD in CS.

**Alexandre Rostovtsev**
Distributed computing, domain-specific languages; Google, FDA; U. of Maryland BA in Math and BS in CS.

**Justin Snapp**
Wireless chip design; Qualcomm; Stanford BS & MS & PhD in EE.

**Chris Dai**
Entrepreneur and blockchain investor; Leland Capital, Longhash Japan, blockchain incubator; Stanford BS in Management Science and Engineering.

## Advisors

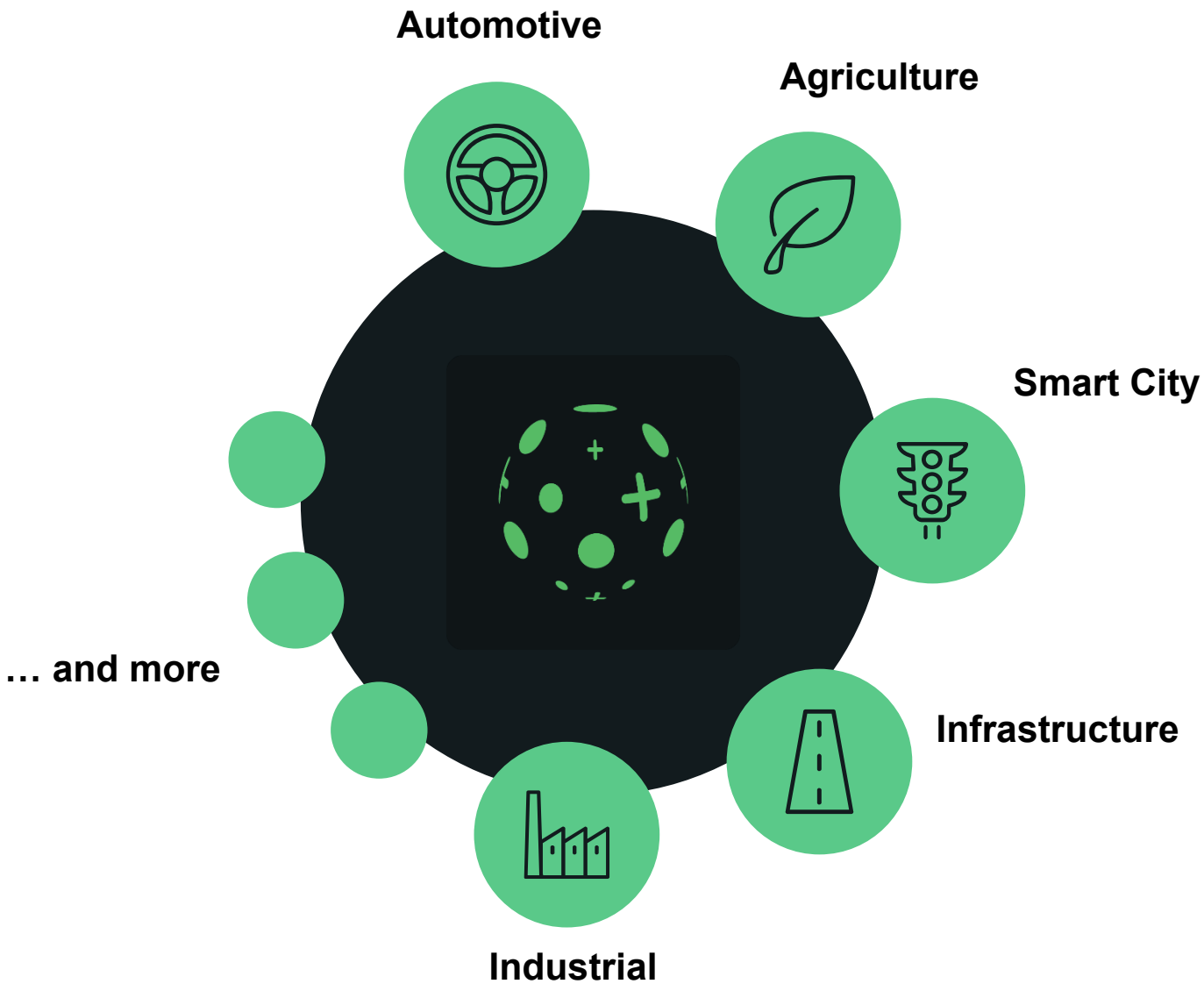
**Maurice Herlihy**
World authority in distributed computing and concurrency, professor of CS at Brown, winner of 2 Dijkstra Prizes and a Gödel Prize, fellow of the ACM, National Academy of Arts and Sciences; Harvard BA in Math, MIT PhD in CS.

**Mamoru Taniya**
Founder of Asuka Asset Management, Mercuria Investment, founding member of Tudor Capital Japan, head of Asia trading for Salomon Brothers; Tokyo U BA in Law.

**James Gong**
Blockchain key opinion leader, serial entrepreneur; ICOAGE, Cybex, ChainB; Shanghai U. BS in Math and CS.

**Yanfeng Chen**
IoT and blockchain serial entrepreneur; National Instruments, ICOAGE, Neubla, Cybex; Jiaotong U. BS & MS in EE.

Our mission is to enable our partners to build successful ecosystems on top of the Taraxa protocol



# The Taraxa team will work with our partners to ensure every use case is grounded in sound business models and value propositions

Provides free technical & commercial consulting to ensure our partners' success

The Taraxa team holds tokens in the ecosystem and are incented to promote its health growth

## Data / insight buyer

Receive a wider range of data and analytics than available elsewhere

## App developer

Build apps & analytics to generate insights from the data on the market

Fees collected in tokens, better access to a wider range of data

## Data Market operator

Build and operate a decentralized data market to enable ecosystem players' participation

Collect fees in the form of data-market specific tokens

## Device makers

Sell / rent Taraxa-compatible IoT devices and plugins

Sales or rental revenue

## Data owner

Sell its data on the decentralized data market

Sales revenue in tokens, complete control over data

## Connectivity & storage provider

Run connectivity & data nodes for the protocol

Fees collected in tokens

What do they offer

What do they get in return

# Here's a concrete example of how Taraxa plans to work with CarBlock's transportation data alliance ecosystem

**IoT device maker**

nonda

Manufactures and sells its ZUS line of connected car devices

Provide free technical service to help develop protocol hardware integration as necessary

**Data owner**

Car owners install smart devices into their vehicles, and installs a CarBlock app, turning their phone into a light node and a data-shop

Provide free technical service to help develop client-side apps, turning vehicle into independent trustless light nodes to participate in the network

**Data market**

CarBlock

Builds and operates a decentralized data market, bringing together all relevant participants

Provides free technical services to help CarBlock develop its data market on top of the Taraxa protocol

**Data buyers**

jiffy lube

Purchases car diagnostic data to predict malfunctions, push coupons to drivers and better pre-allocate its parts & technician resources

PROGRESSIVE

Purchases driver behavioral data to build better individualized risk models

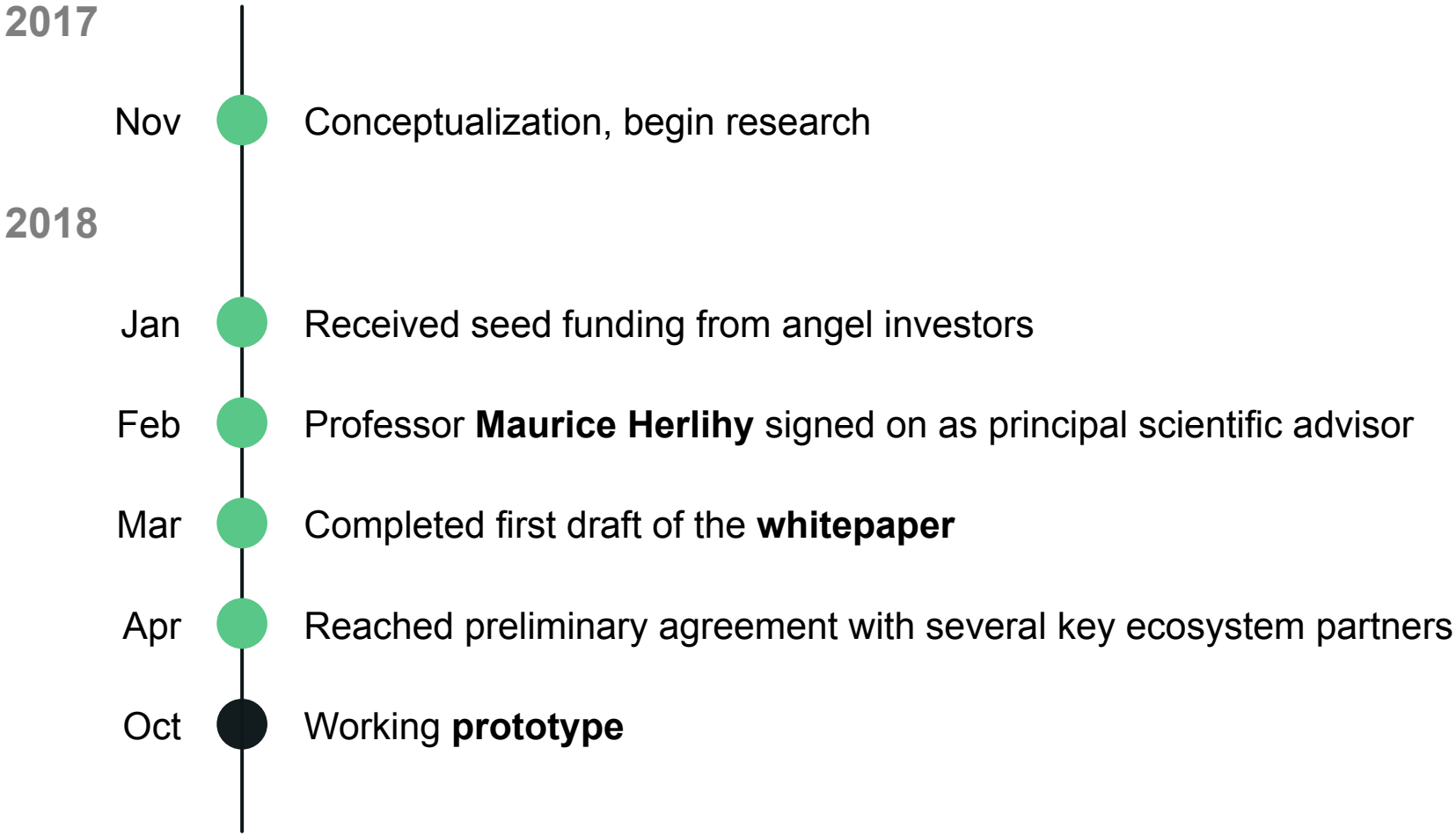
Taraxa

# Taraxa has introduced numerous market-first innovations that address IoT-specific as well as general blockchain scalability challenges

| | Brief description | TPS | Light Node | Concurrent Contracts | Encrypted data mkt |
|---|---|---|---|---|---|
| IOTA | Early IoT+blockchain project based on a DAG design. Currently the network is dependent upon a centralized coordinator to help validate transactions | 2-4 tps [1] | None | No smart contracts | None (yet) |
| IoTeX | A privacy-focused chain-in-chain topology that allows users to create private or public subchains on top of its rootchain. | (not live) | None | No smart contracts | None |
| Hdac | Based on MultiChain, a public / private chain integration project. | (not live) | None | No concurrency | None |
| IoT Chain | Protocol based on IOTA. | (see IOTA) | None | (unknown if it has smart contracts) | None |
| BAIC | Based on ByteBall but with a proposed DPOS consensus on top. | (not live) | None | No concurrency | None |
| streamr | Decentralized IoT data market built on top of Ethereum. | Same as ETH (~15) | None | No concurrency (EVM) | Has datamarket, not encrypted |
| Taraxa | Based on a block-lattice topology to enable fast asynchronous transactions and a concurrent contract system that enables parallel processing of hundreds of contract calls on a single node. | ~100-300 as tested on the Nano network[2] | First practical trustless light node | First concurrent contract sys, ~100x speed of ETH | Practical encrypted data market |

1. https://thetangle.org/live; 2. https://medium.com/@bnp117/stress-testing-the-raiblocks-network-part-ii-def83653b21f

# Our project plans to launch a prototype by the end of Q3 2018



# Thank you!