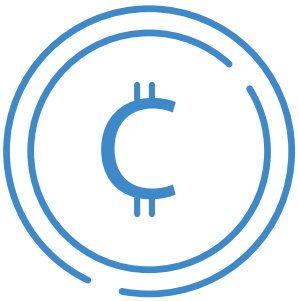
# CONTRACTNET

## WHITEPAPER

contractnet.com

# CONTENTS

# 1/ INTRODUCING CONTRACTNET



ContractNet is a new public, permissionless blockchain which is purpose built with the storage, sharing and analysis of IoT data streams. The ContractNet technology company is based in Hong Kong, and is registered in both Hong Kong and the USA.

We believe that a systemized framework for sharing IoT data, and a platform for developing distributed apps & smart contracts, could benefit all industry sectors for the better. The ContractNet is positioning itself at the intersection of these exciting technologies - Blockchain, the Internet of Things and Smart Contracts.

It has been designed and optimized specifically for IoT solutions, where IoT device owners can share their data streams in a secure, incentivized manner, and application developers use this data to develop the next generation of apps and contracts. External devices (called data providers or “Oracles”) will interface directly with the ContractNet network, providing time-series data from the physical world, to the walled garden that is a smart contract (or distributed app) within a Blockchain, in a safe, secure manner.

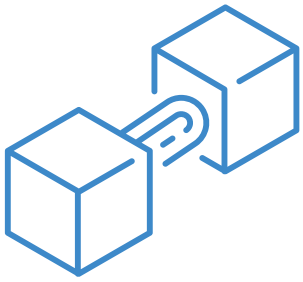
The platform uses a base currency (CNET) to act as a store of value, and also as the unit of exchange for payment, computation and storage.

ContractNet plans to garner support and grow a community in the following ways:

- Miners can provide computing power to the network in exchange for “gas” and the opportunity to find the next block which is rewarded.
- Storage Miners can provide storage capacity to the network in exchange for “gas”.
- IoT device owners can sell data streams to developers or other users/services
- 3rd party developers can create new Oracles and sell these on our Oracle Hub. These Dapps provide physical input into the Blockchain
- Smart Contracts can be used to fundraise through Crowdsales on the platform in exchange for tradeable tokens.

ContractNet is at the cutting edge of a technology wave that promises to transform the way many industries and businesses function.

# 2/BLOCKCHAIN



While Bitcoin continues to dominate the headlines, breaking records and defying predictions of bursting bubbles, there is a quieter but equally powerful move in the background to find new uses for blockchain, the technology behind Bitcoin.

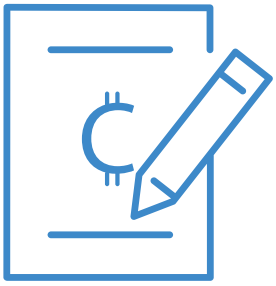
Where there was, originally, a “wild west”, anti-establishment flavor to blockchain, with proponents wanting independence from central control, it is now fast becoming part of the establishment. Companies such as IBM and Microsoft are selling it, and major banks and stock exchanges are running Proof of Concepts.

In essence, a blockchain is a public ledger. It is like a narrow, deep spreadsheet that registers transactions and makes them visible to the public. Once data is written, it is immutable, which means it cannot be modified. In addition, multiple copies are written around the world which makes data highly redundant and available. What makes it different to traditional databases is that it has a consensus mechanism that allows multiple parties who do not know or trust each other to have a shared database. Everyone has the same view of the state of and changes made to the database, without the need for a third-party intermediary.

One of the key new areas for the application of blockchain technologies is in IoT – the Internet of Things. Jerry Cuomo, vice president of blockchain technologies for IBM, predicts that shipping companies could have information about goods on the move, including the condition of the contents, and whether they’ve been damaged. Sensors in refrigerated containers could track temperatures and tampering with contents. Every step a food product takes from field to supermarket can be tracked, so users can be sure products are safe. As self-driving and self-parking cars take to the roads, blockchain could be “a shared single source of truth” to establish fault in the event of an accident or damage to a vehicle.

This view is supported by Professor David Lee of Singapore Management University. According to him, we have now moved beyond having to provide user education on how Blockchain works, and now must demonstrate its uses. He believes that “the key ingredient is M2M (machine to machine) and IoT (Internet of Things). This needs to take off for Blockchain to take off in a big way”. If this is true, then this is the place for developers and professionals to direct their attention.

# 3/ SMART CONTRACTS



## 3.1 WHAT IS A SMART CONTRACT?

A smart contract is ***not*** autonomous, intelligent software. It is simply a piece of code that is stored on a blockchain, that automatically implements the terms of an agreement between partners.

It is triggered by transactions on the blockchain, and it reads and writes data in that blockchain's database. The code can be in Pascal, Python, PHP, Java, Fortran, C++, Go, Solidity and a multitude of other languages. It can be compared to stored procedures written in an extension of SQL. It is deterministic, in that the same input will always produce the same output.

To quote Martha Bennett, a principal analyst at Forrester Research:

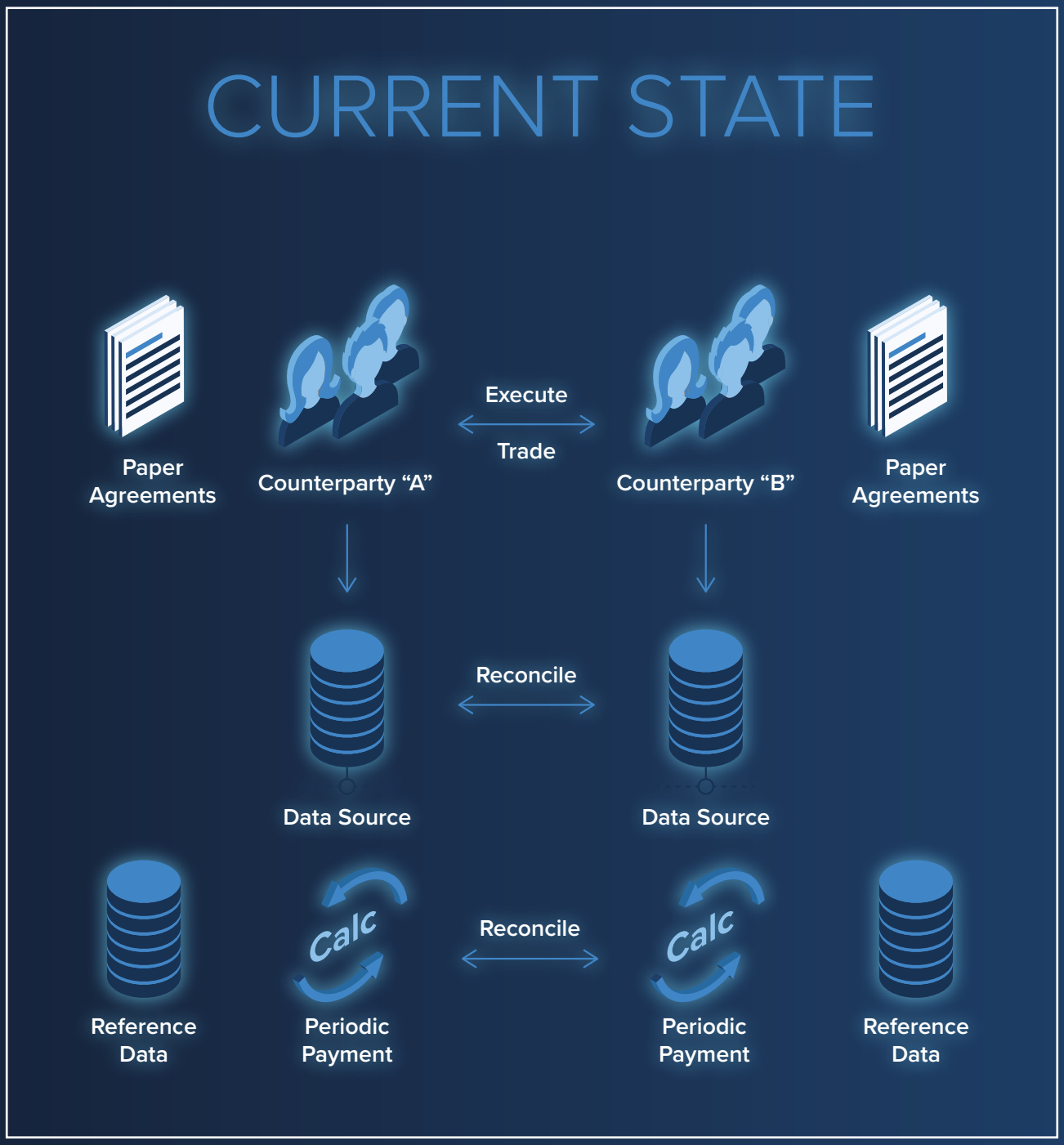
> "IF YOU STRIP AWAY ALL THE ASPIRATIONAL LANGUAGE, A SMART CONTRACT IS A SET OF BUSINESS RULES ENCODED IN SOFTWARE."

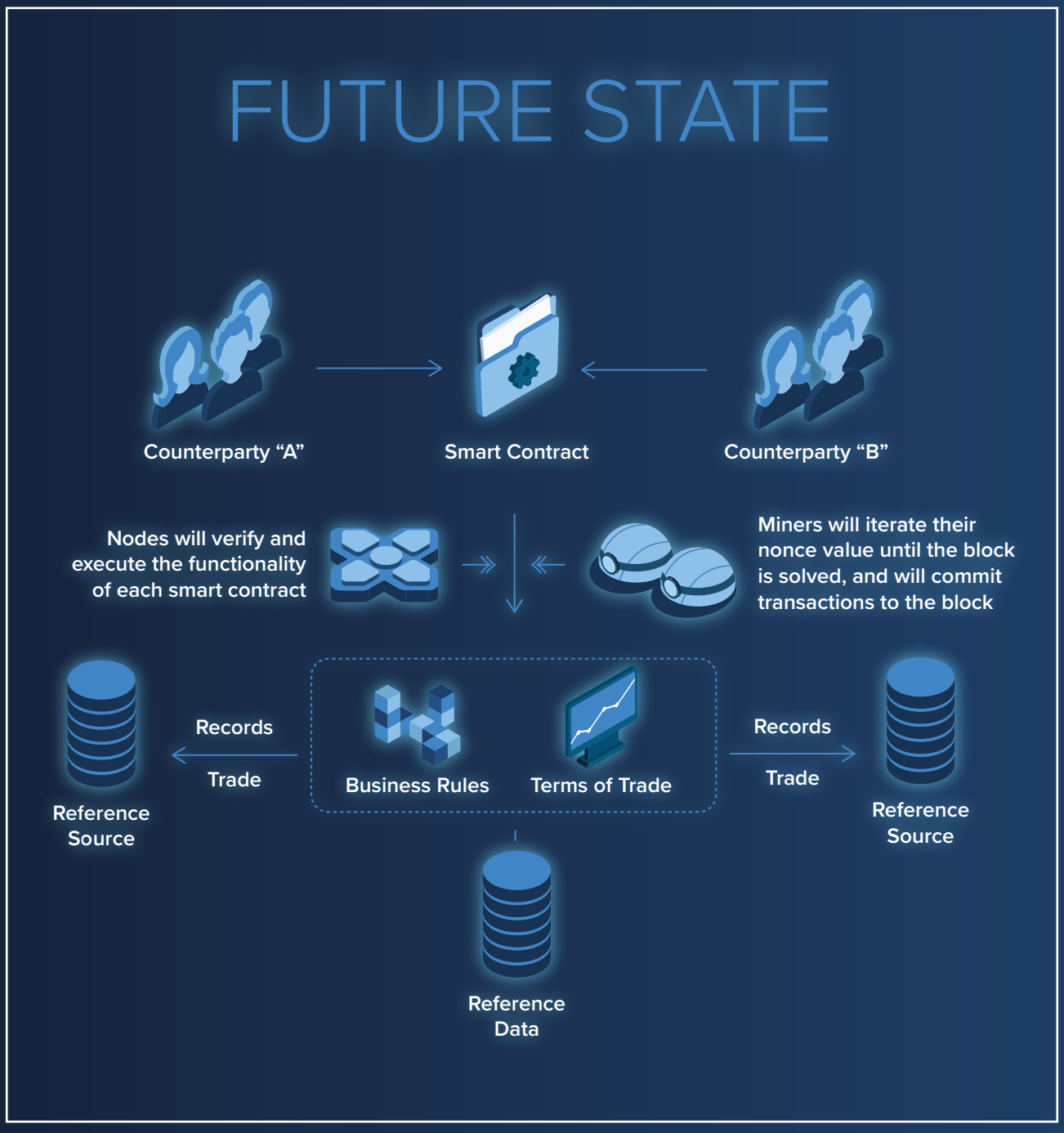
Ethereum is a platform that's built specifically for creating smart contracts. The Ethereum Virtual Machine (EVM) is "Turing complete", which means that the EVM code can perform most computations associated with modern programming languages. Smart contracts run on the EVM, which is like a distributed global computer. The most popular language for writing smart contracts in Ethereum is Solidity.

Smart contracts solve one of the "messiest" parts of any contract – deciding whether all the terms have been satisfied and if payments should be made. A key task of the smart contract is "arbitration". An arbitrator (adjudicator) settles disputes. In the case of blockchain, the data written to the blockchain is used to adjudicate whether the terms of the contract have been met.

Smart contracts have a place in many business and organisational activities where some form of automation would either simplify processes, increase efficiency or cut costs.

The following diagram illustrates how a smart contract removes the need for people to institute action and perform multiple reconciliations. It automates the action, matches it against the terms of the contracts, keeps everyone informed, and retains a single set of reference data, that cannot be altered.






Smart contracts allow for automation of complex multi-step processes. Applications that previously required a trusted intermediary can achieve the same functionality in a decentralized manner, without the need for a central authority.

## 3.2 CHALLENGES FACING SMART CONTRACTS

The challenges hindering Smart Contracts from greater adoption are:

- Legal Status
- Security
- Accessing External Information
- Difficulty in Rolling Back Errors

### 3.2.1 LEGAL STATUS

There is no real clarity about whether smart contracts are legally binding under current legislation in different countries.

Most countries are adopting a “regulation will follow innovation” stance on this and hopefully a clear path will be proposed soon.

### 3.2.2 SECURITY

Most transactions on a blockchain are single actions (a transfer of funds), however, a smart contract requires processing and it therefore is persisted for the duration of the blockchain’s existence time. During this time, it is vulnerable to attacks of various sorts, and especially those on the “CIA” list:

- **Confidentiality** (leaking of information to non-approved parties)
- **Integrity** (intentional or unintentional changes to the internal state of the code, leading to incorrect execution)
- **Availability** (where one party in the agreement affects the availability of one of the parts that makes up the smart contract)

Smart contracts, if poorly designed, can be riddled with bugs and security vulnerabilities. A recent analysis of over 19,000 smart contracts deployed on the Ethereum blockchain, found 8,333 contracts with at least one security issue. Many of these can lead to cyber theft or the deadlocking of smart contracts.

*FSolidM* a proposal by *Anastasia Mavridou & Aron Laszka,* seeks to resolve these issues by implementing *locking* and *transition counter* plugins which prevent reentry and unpredictable state vulnerabilities.

### 3.2.3 ACCESSING EXTERNAL INFORMATION

Smart Contracts inherently cannot access data outside their network. An *oracle* is a data provider designed for use in smart contracts on the blockchain. An oracle could be software (eg a website or desktop app) or hardware (eg a smart sensor). The oracle creates a transaction, that is verified by all the nodes, and pushes data into the blockchain. Inbound oracles provide external data and trigger smart contract executions when pre-defined conditions are met. Such conditions could be any data, like weather temperature, successful payment, price fluctuations, etc. Outbound oracles allow smart contracts to send data to the outside world.

The main challenge with oracles is that people need to trust these sources of information. Different trusted computing techniques can be used as a way of solving these issues, but in general, current oracle solutions rely on data from centralized services, and so remove the smart contract's ability to be trustless and tamperproof.

ContractNet will leverage the power of oracles and will create a marketplace for 3rd party developers to create and share oracles with the greater community.

### 3.2.4 DIFFICULTY IN ROLLING BACK ERRORS

Immutability, in our opinion, is a core tenant of a blockchain. Without it, a system cannot claim that its code is law. As a next generation platform for the internet-of-contracts, our system must maintain this principle in order to maintain confidence in an autonomous platform. All data on the ContractNet and the terms under which it executes is an immutable state which can never be altered or censored.

However, while immutability is part of the strength of a smart contract, it is also a potential weakness. The technology itself is immature, and if there is a mistake in code logic, the outcome is irrevocable. The Ethereum DAO vulnerability showed what can happen if code is not exhaustively tested for every potential outcome.

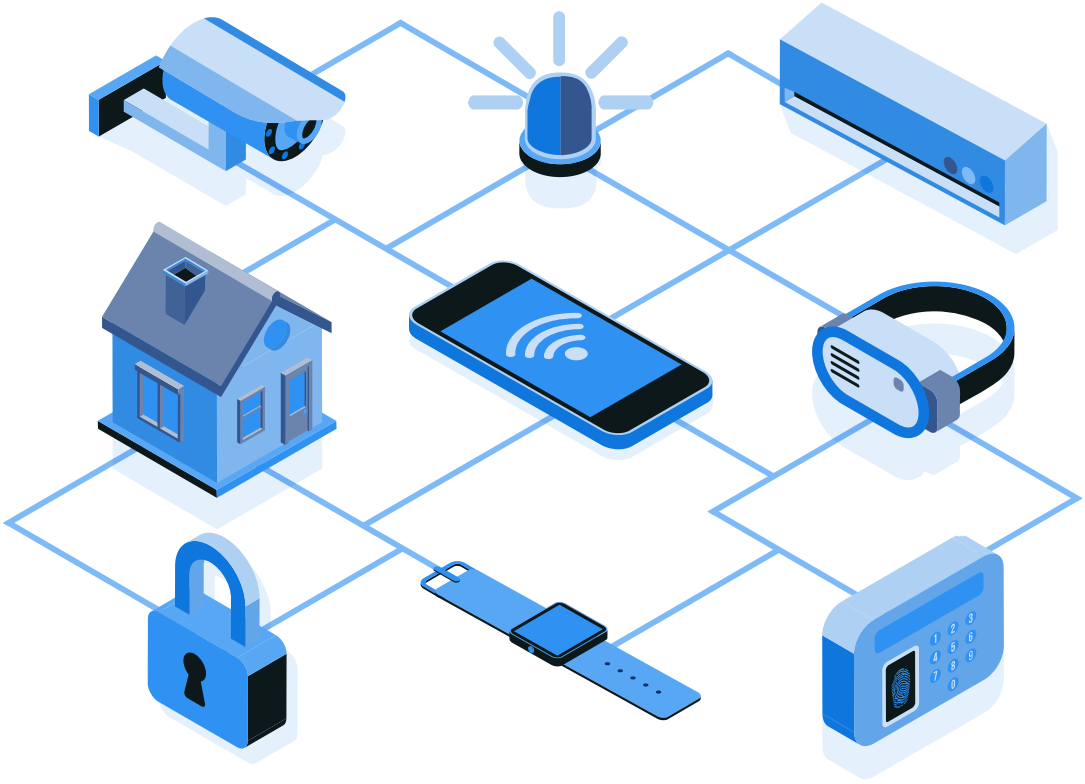
ContractNet aims to resolve this challenge by implementing the FSolidM proposal (*Anastasia Mavridou & Aron Laszka)*, which aims to address common vulnerabilities in the Solidity language (and the greater EVM ecosystem) by designing contracts as Finite State Machines (FSM). This solution will aim to eliminate errors in contracts from the outset by implementing safe coding patterns in the form of plugins to prevent rather than try to cure.

# 4 / INTERNET OF THINGS (IOT)

## 4.1 WHAT IS IOT?

The Internet of Things is a giant network of everyday devices connecting with other devices, servers or platforms on the Internet. This includes everything from mobile phones to washing machines, coffee makers to wearable devices for health and fitness, machine components like jet engines of an airplane to drills on an oilrig. The projection from the analyst firm Gartner is that by 2020 there will be over 26 billion connected devices – others are talking about 100 billion.

The current 32-bit address system (IPv4) used on the world wide web, has a limit of 4,294,967,296 concurrent devices. This has necessitated a new standard to be introduced - IPv6 - which has a 128-bit length and therefore could facilitate a maximum of 3.4x1038 unique addresses.



Why would we want devices to communicate with each other? It might be something simple like having your alarm clock switch on your coffee machine in the morning. Or it might be much bigger, like the development of smart cities, with connected devices managing traffic flow, reducing waste or improving energy usage.

IoT has evolved from machine-to-machine communication (M2M), which is about networked devices exchanging information and performing actions without manual input from humans. IoT is the convergence of M2M with big data analytics.

The value of the IoT is in the data – its manipulation and representation. Enterprise IT architects will be looking for off-the-shelf components and will want them to fit with their current IT infrastructure. Data integrity, privacy and security will be primary concerns.

According to Debra Bordgnon, CTO of Dimension Data, Australia, IoT is one of three strategic contexts where blockchain will be a game changer:

> **"BLOCKCHAIN AS AN ENABLER FOR THE INTERNET OF THINGS (IOT) -** IOT IS A DISTRIBUTED NETWORK BUT NEEDS TO HAVE MORE INTELLIGENT PROCESSING BETWEEN NODES. CURRENT CENTRALIZED IT SYSTEMS ARE INEFFICIENT, RESOURCE INTENSIVE AND CONSTRAIN THE ACHIEVEMENT OF IOT SOLUTIONS. BLOCKCHAIN PROVIDES THE NETWORK ARCHITECTURE FOR IOT, TOGETHER WITH A SECURITY FRAMEWORK TO MANAGE A MESH OF CONNECTED DEVICES."

Blockchain technology offers capabilities for tracking a vast number of connected devices. It can enable coordination and processing of transactions between devices. The decentralized approach provided by the technology eliminates single points of failure and thus creates a more resilient device ecosystem.

## 4.2 CHALLENGES FACING IOT

The application of blockchain and smart contract technologies to IoT is still in its infancy, and is therefore an ideal field for new thinking and approaches. However, there are a number of pain points to be addressed in implementing blockchain solutions for IoT:

**Technical Challenges:**

- Scalability
- Processing power and time
- Storage
- Standards for IoT

**Risks:**

- Credibility of vendors
- Credential security
- Legal compliance

ContractNet proposes to take a number of different decentralized technologies, combine them into a hybrid solution that ticks all of the following objectives:

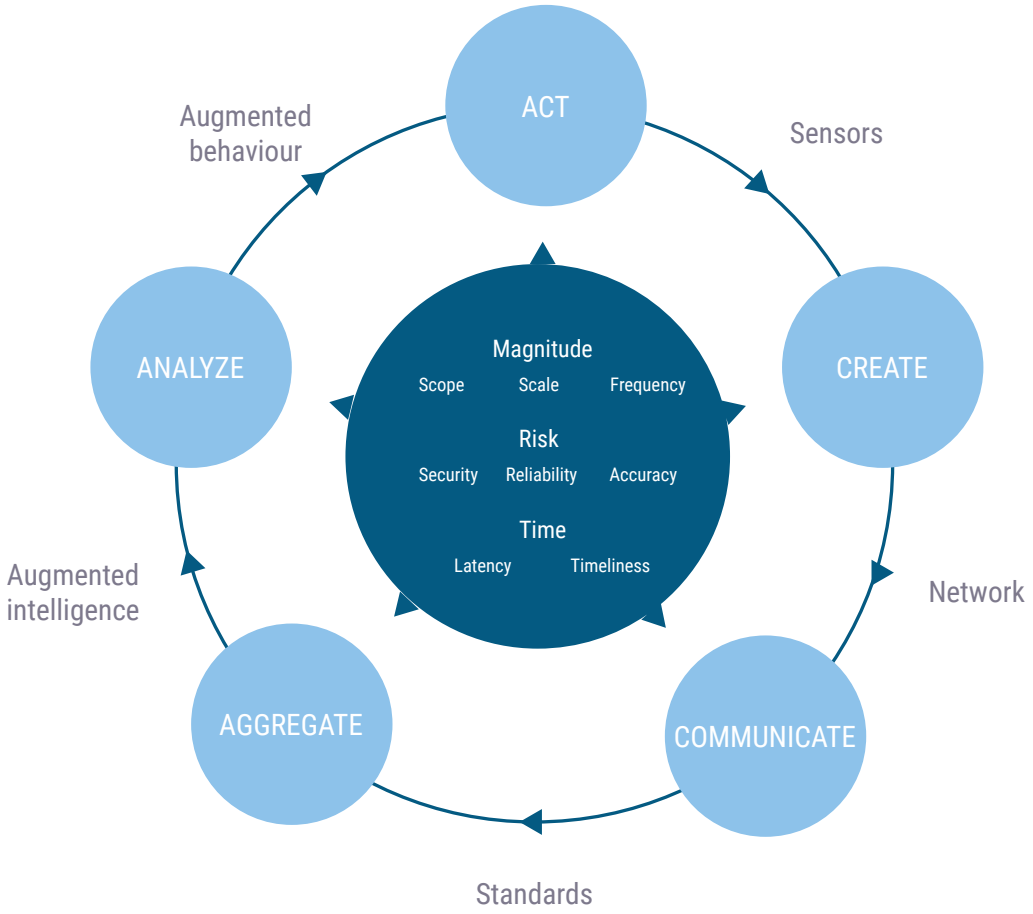
- Decentralized, resilient and auditable access control management of data streams
- Stream ownership and cryptographically secure sharing
- Secure data storage
- Confidentiality
- Authenticity
- Integrity
- Compatibility
- Single Writer
- Several Readers

ContractNet's solution to these requirements will be detailed in Section 7.

## 4.3 DEFINING THE LANDSCAPE

### 4.3.1 THE IOT LIFECYCLE

The IoT lifecycle is generally accepted to contain 5 components:




**Create** - where devices or sensors collect data from the physical environment around them

**Aggregate** - where data collected is aggregated by devices

**Communicate** - where the data and aggregations generated are sent through the network to a desired location

**Analyse** - sophisticated analytics are used to generate basic patterns, control and optimise processes

**Act** - suitable actions are taken based on the information created

### 4.3.2 TECHNOLOGIES

The technologies that enable the Internet of Things can be broken down into the following groups:

**Sensors** - a device that generates an electronic signal from a physical condition or event

**Networks** - a mechanism for communicating an electronic signal

**Standards** - commonly accepted prohibitions or prescriptions for action

**Augmented Intelligence** - analytical tools that improve the ability to describe, predict, and exploit relationships among phenomena

**Augmented Behaviour** - technologies and techniques that improve compliance with prescribed action

The types of sensors available are:

| Type | Description | Examples |
|---|---|---|
| **Acoustic** | Acoustic sensors measure sound levels and convert that information into digital or analog data signals. | Microphone, geophone, hydrophone |
| **Biological** | Biosensors detect various biological elements such as organisms, tissues, cells, enzymes, antibodies, and nucleic acids. | Blood glucose biosensor, pulse oximetry, electrocardiograph |
| **Chemical** | Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO2 sensor senses only carbon dioxide). | Breathalyzer, olfactometer, smoke detector |
| **Flow** | Flow sensors detect the rate of uid ow. They measure the volume (mass ow) or rate ( ow velocity) of uid that has passed through a system in a given period of time. | Anemometer, mass flow sensor, water meter |
| **Force** | Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold. | Force gauge, viscometer, tactile sensor (touch sensor) |
| **Humidity** | Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on. | Hygrometer, humistor, soil moisture sensor |
| **Light** | Light sensors detect the presence of light (visible or invisible). | Infrared sensor, photodetector, flame detector |
| **Occupancy & Motion** | Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors will generate a signal even when a person is stationary, while a motion sensor will not. | Electric eye, RADAR |

| Type | Description | Examples |
|---|---|---|
| **Position** | A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis. | Potentiometer, inclinometer, proximity sensor |
| **Pressure** | Pressure sensors are related to force sensors and measure the force applied by liquids or gases. Pressure is measured in terms of force per unit area. | Barometer, bourdon gauge, piezometer |
| **Radiation** | Radiation sensors detect radiations in the environment. Radiation can be sensed by scintillating or ionization detection. | Geiger–Müller counter, scintillator, neutron detector |
| **Temperature** | Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation. | Thermometer, calorimeter, temperature gauge |
| **Velocity & Acceleration** | Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity. | Accelerometer, gyroscope |

All of these sensor types (besides Biological perhaps) could be applied in our top four IoT adopter industries (namely, Manufacturing, Transport & Logistics, Utilities and Other).

Therefore it is extremely important to create Oracles or to create tools for developers to create Oracles that incorporate these streams into ContractNet.

The aforementioned Oracles also need to communicate on the following networks in order to interface with these IoT devices:

| | PAN (Personal Area Networks) | LAN (Local Area Network) | WAN (Wide Area Network) |
|---|---|---|---|
| **Wired Connections** | USB | Ethernet | N/A |
| **Wireless Connections** | Bluetooth, Bluetooth Low Energy, ZigBee, NFC, Wi-Fi | Wi-Fi, WiMAX | WiMAX, Weightless, Cellular Tech (2G, 3G, 4G) |

### 4.3.3 STANDARDS

Finally, it is necessary to comply with standards defined by the IEEE (Institute of Electronics and Electrical Engineers). The full table which defines all the standards that fall under the IoT "umbrella" can be viewed in the document section of our website and at http://standards.ieee.org/innovate/iot/stds.html.

## 4.4 OPTIMAL BLOCKCHAIN CONFIGURATION FOR IOT

The current ContractNet codebase (https://github.com/ContractNetLabs/go-ContractNet) configurations, which were forked from Ubiq, would generally be a good fit for IoT. As Ubiq was originally an Ethereum fork, one of the main changes made was reducing the targeted block time as seen in the table below.

| Characteristic | Ubiq | ContractNet |
|---|---|---|
| Targeted blocktime | 88 seconds | 12-19 seconds |

Due to the nature of committing and requesting streams from the chain, a blocktime of 88 seconds may be too long. If additional latency is incurred when writing and reading information from the decentralized file system, users could be waiting in excess of 2 minutes for confirmation that an operation has been completed. ContractNet lowered the block time to overcome this latency.

Contrary to Ethereum the goal of ContractNet is to build a platform for Smart Devices, a marketplace for IoT streams and a hub for Decentralized applications of Internet of Things.

Smart Contract coded in the ContractNet blockchain are better secured than Ethereum as the confidentiality level of the Smart contracts will be increased by deploying permission-based storage and Encryption.

## 4.5 A SHALLOW DIVE INTO ORACLES

An “Oracle” is a data provider which allows a smart contract to communicate with the physical/outside world. This data provider is a translation between a Blockchain node and our sensors.

It is at this point that ContractNet will need to pay close attention to which IoT vendors are selling the most products (a measure of market adoption) and which IEEE standards or SDKs need to be integrated into as a matter of priority.

In addition, these Oracles should not only connect to IoT sensors, but to create a truly global platform should have interfaces to:

**Payment Providers**

- Visa
- Mastercard
- Paypal

**Other Blockchains**

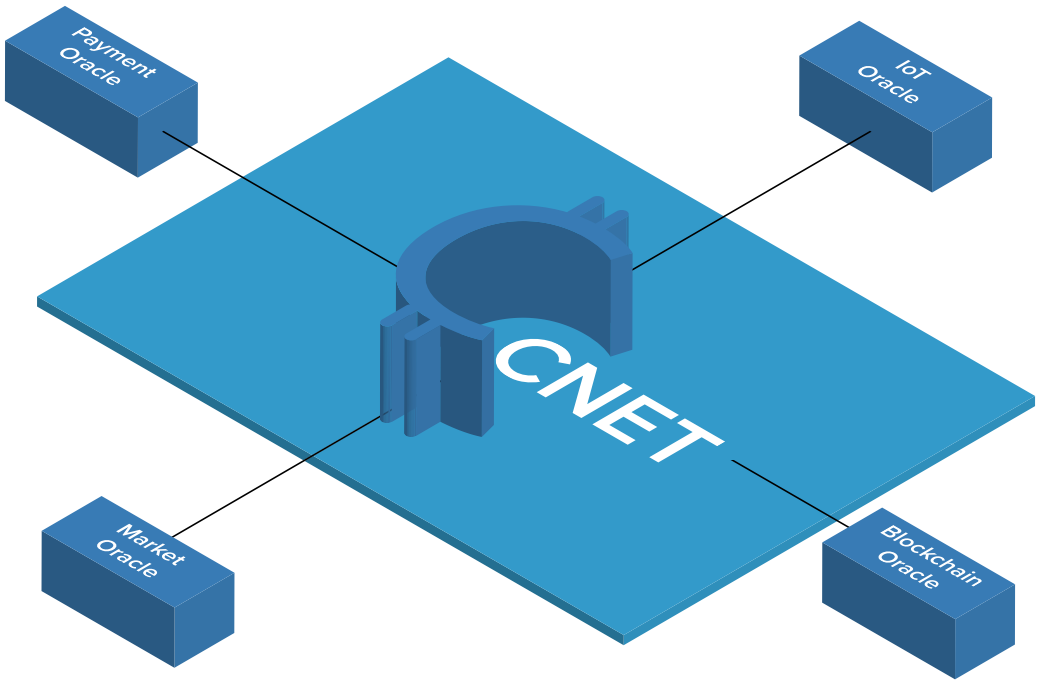
- Ethereum
- Bitcoin

**Backend systems**

- SAP
- Salesforce

**Market Data**

- New York Stock Exchange
- Bloomberg



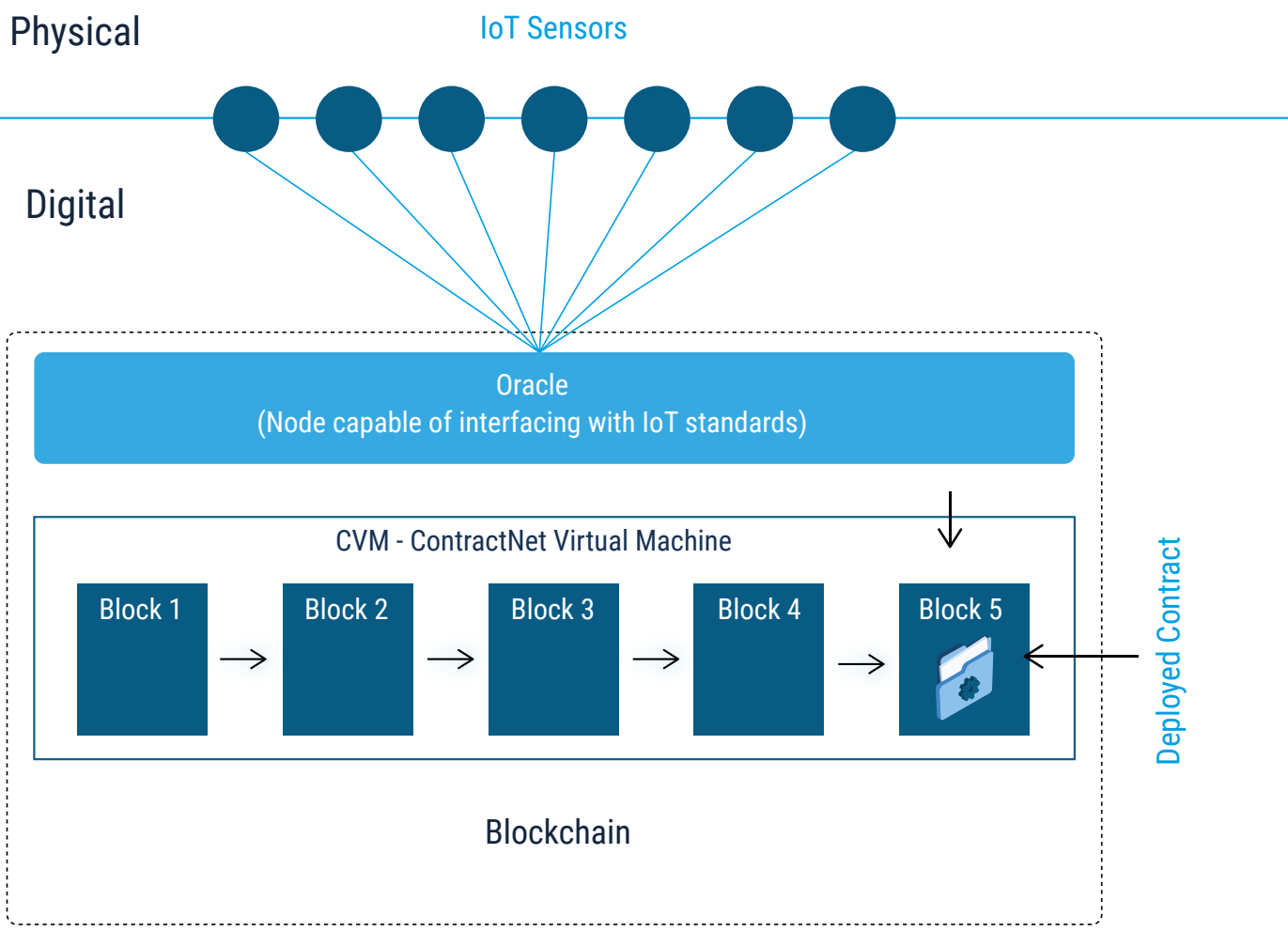
More specifically the IoT oracles will function as illustrated below:

There are a number of excellent resources that will assist in the creation of Oracles for the ContractNet Oracle Hub:

**https://github.com/axic/tinyoracle** - a starting point project to develop an oracle that interacts with a full node

**http://truffleframework.com** - this framework does a lot of the "heavy lifting" when creating Dapps or Oracles for Ethereum, Ubiq or ContractNet. It includes many useful packages and abstracts the low-level RPC calls.

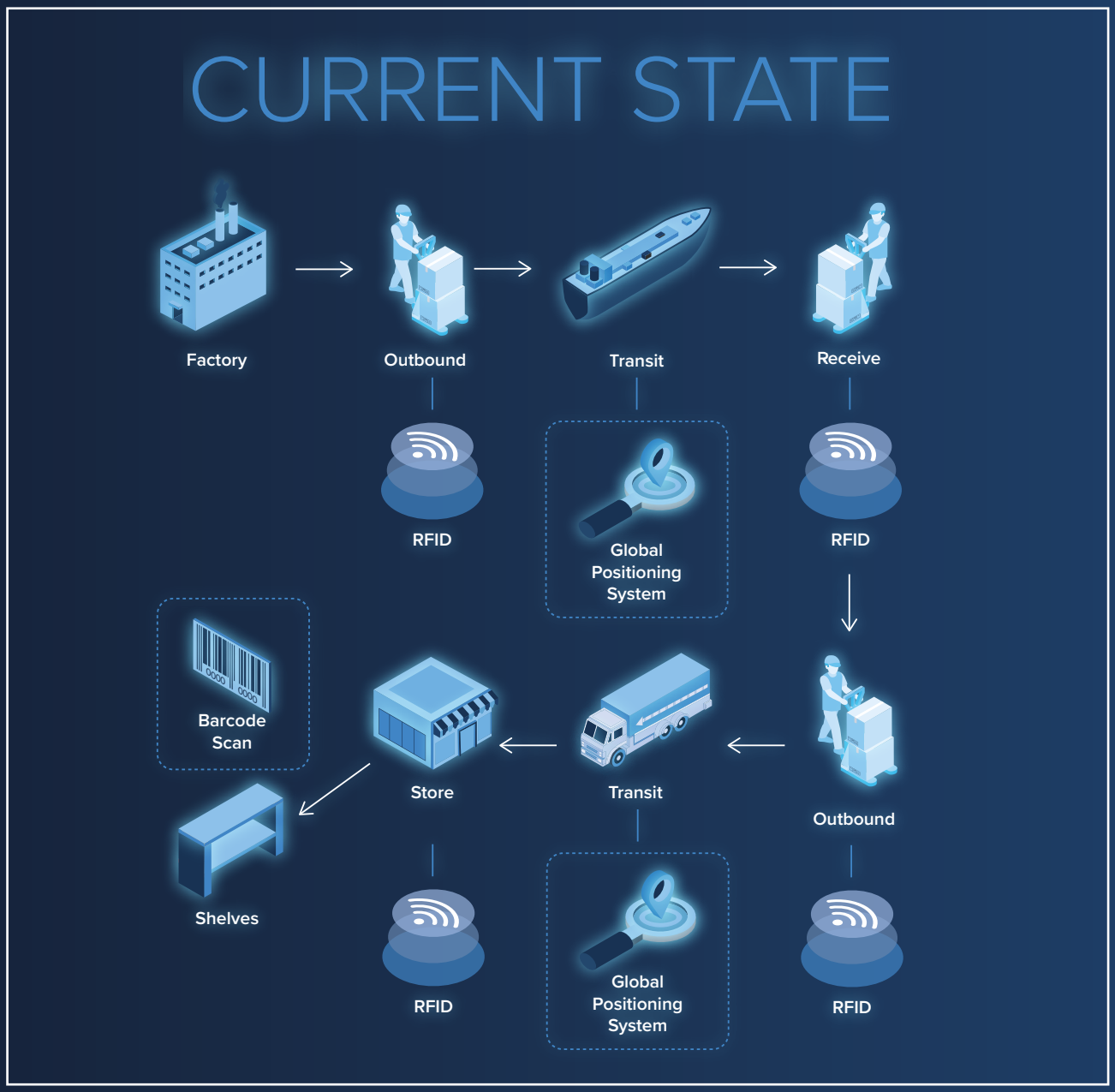
**https://github.com/ethereum/web3.js/** - this is a Javascript API, developed by the Ethereum team. This collection of libraries allows you to connect to a local or remote node via HTTP. As web technologies are everywhere, this library allows you to connect to the ContractNet network from any web-based app.

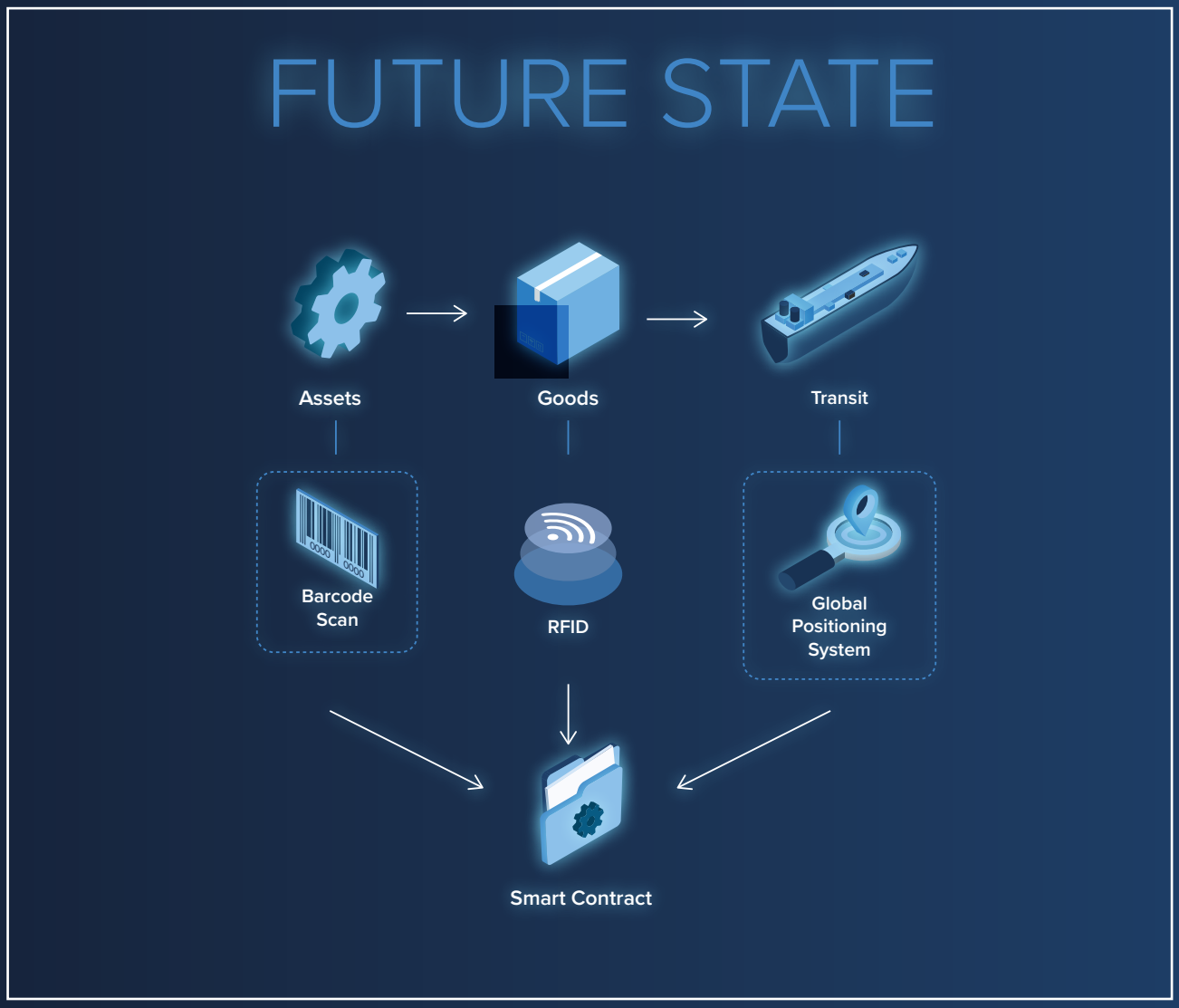


# 5/ THE INTERSECTION OF BLOCKCHAIN, SMART CONTRACTS & IOT

## 5.1 AN EXAMPLE

A supply chain is one of the most obvious and practical examples of the intersection of blockchain, smart contracts and IoT.






The traditional supply chain is dependent on updates from multiple parties along the "journey" of the item from factory to store shelf. This inevitably leads to multiple databases and the difficulty of trying to synchronize them. Even when there are sensors, radio-frequency ID's (RFIDs) and GPS tracking, there is seldom a single end-to-end system. Recording all of the movements and the data from all of the devices onto a blockchain provides a single global database, updates that are verified and an auditable trail of information. The movement of a container is tracked as a virtual transfer of ownership from one point to the next.

IoT devices can communicate with each other and provide real time visibility for the movement of product from factory to store shelf. Devices could also, for example, be tracking the condition of the trucking fleet or monitoring the temperatures of refrigeration containers.

However, a smart contract adds some automation to the processes. So, for example, as devices recognise each other or note positions or proximity, they can automatically send a notice of this as a transaction to the blockchain, without any human input. Rather than just monitoring the trucks, a sensor may be triggered to adjust the temperatures in the refrigeration containers. Other actions may be triggered – eg obligatory rest periods for drivers, maintenance checks, tire replacement, license renewals. Conditions may be set for automated invoicing or payments.

A smart contract adds verification to visibility, facilitates buying and selling of commodities, provides clarity of agreement terms and self-executes them. It provides tamper-proof data storage and becomes the "single source of truth". It clearly identifies all players, whether they are suppliers, distributors or the sensors attached to trucks, and cuts across traditional silos in business processes.

Moving into the future, smart contracts on top of blockchain technology can be the solution to the integration of IoT and Artificial Intelligence (AI). At the moment, smart contract codes trigger rule-based reasoning when certain conditions are met. As AI techniques become more advanced, nodes may move beyond pre-defined rules and conditions and reason in a more intelligent manner. This will develop both local and collective intelligence and will allow the traditional blockchain to become a cognitive blockchain that can learn from past cases and adapt over time.

## 5.2 THE PLACE FOR CONTRACTNET

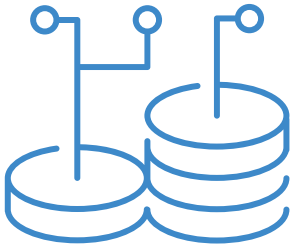
ContractNet is positioned at the intersection of blockchain, IoT and Smart Contracts:

- When blockchain is combined with IoT, we have resilient, truly distributed peer-to-peer systems and the ability to interact in a trustless, auditable manner.
- Smart contracts allow us to automate complex multi-step processes.
- The devices in the IoT ecosystem are the points of contact with the physical world.
- Our solution takes the massive amounts of data that IoT devices produce, and stores them in a unique, cost-effective and decentralized manner

Combining them allows us to automate time-consuming workflows in new and unique ways; all activities are cryptographically verifiable; significant cost and time savings can be achieved.

We believe that this technology will lead to the transformation of several industries and the rethinking of business models, systems and processes.

# 6/THE MARKET



## 6.1 TOTAL AVAILABLE MARKET (TAM)

The rapid advance of blockchain technology and the Internet of Things (IoT) are starting to be felt in our daily lives and are set to disrupt processes across multiple industries.

A Gartner study estimates blockchain will add $3.1 trillion in business value by 2030, and in another analysis the global IoT market is expected to grow from $157 billion in 2016 to $457 billion by 2020.

We have provided some detail in this section on the use cases for blockchain and IoT, because this is the market within which ContractNet will be functioning. Dapps for any one of these uses can be hosted on the ContractNet blockchain:

**Wearables**: This is driven mainly for the health and fitness information they provide. This industry is expected to grow from 46 million units in 2014 to 285 million in 2018.

**Nearables**: iBeacon (Apple) and Eddystone (Android) implementations of Bluetooth Low Energy proximity devices.

**Healthcare**: Pacemakers that will broadcast data to the cardiologist and perform ECGs, razors that will scan your chin for signs of acne, glasses that will monitor your eyesight and advise on correction, toothbrushes that will advise you of bad breath! It includes the management of chronic diseases, delivery of health information for health professionals and health consumers, the management of health resources, collaboration among institutions, tracking of legitimate drugs and cracking down on counterfeits, etc

**Smart living environments** at home, at work, in public spaces.

**Smart buildings** and architecture, especially in enabling the green economy and in improving the comfort of occupants.

**Supply chain**: This is one of the most obvious and practical uses for blockchain and IoT. (See our practical example in Section 5.1)

**Auto insurance**: Smart contracts can record the details of auto insurance policies, together with driver and vehicle details and history, then link with IoT devices in cars to record driver reports, driving records, etc and automate claims processing in the event of an accident. This ensures "one source of verified truth", eliminates disputes and duplicated reporting and saves time and costs.

**Energy sector**: A blockchain network which includes a cryptocurrency provides a convenient billing layer and also facilitates the sharing of services and property in general. So, for example, a popular use of smart contracts is in the energy sector, where machines can buy and sell solar power to each other. Solar panels record their excess output on the blockchain and sell it to neighbouring parties via smart contracts.

**Emerging technologies**

- **Edge computing**: Edge pushes applications, data and computing power away from centralized points to the edges of the network, closest to the sources of the data. There is potential for IoT devices to be configured to share their computing power and to form peer-to-peer content distribution networks (P2P CDNs), without involving cloud computing resources. (See Section 6.3 for how this can be monetized.)
- **Communication technologies**: Various communication models, that will co-exist in heterogeneous environments. These models range from:
  - device to device
  - device to cloud
  - device to gateway
- **Tactile IoT**: Internet of Mobile Things (IoMT), the Internet of Autonomous Things (IoAT) and the Internet of Robotic Things (IoRT)

## 6.2 TARGET MARKET FOR CONTRACTNET

According a Forbes Internet of Things forecast, the biggest market adopters of IoT in 2020 will be as follows:

| Sector | Investment |
|---|---|
| **Discrete Manufacturing** | $40 billion |
| **Transportation and Logistics** | $40 billion |
| **Utilities** | $40 billion |
| **Other** | $30 billion |
| **B2C (Business to Consumer)** | $25 billion |
| **Healthcare** | $15 billion |
| **Process** | $15 billion |
| **Energy and Natural Resources** | $12 billion |
| **Retail** | $12 billion |
| **Government** | $12 billion |
| **Insurance** | $5 billion |

This table gives us some insight as to the industries, software developers and IoT standards ContractNet needs to target. As far as IoT device manufacturers in the top 4 rows, these are a few of the companies we have identified:

| | | | |
|---|---|---|---|
| Cisco | Epson | Fanuc | Gartner |
| General Motors | IBM | Intel | KUKA Systems |
| Lockheed Martin | Microsoft | Honeywell | Ericsson |
| Black & Decker | Zebra Technologies | Infineon Technologies | ARM Holdings PLC |

This list of vendors is by no means exhaustive as there are thousands of manufacturers across a range of different technological standards. However this list would be a good place to start as most of these companies have SDKs which we could develop Blockchain Oracles around to interface directly with their devices.

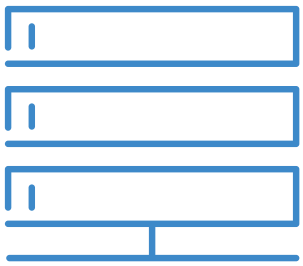
## 6.3 ATTRACTING IOT DEVICE OWNERS, DEVELOPERS, MINERS AND ADOPTERS

ContractNet's philosophy and reason for existence is to be the global interchange of IoT data, and the platform for some of the most exciting applications on the decentralized web. This unlocked batholith of data will create some of the most useful forecasts, visualizations and decisions that will better humanity and drive innovation forward.

In addition, the global community can benefit from the platform in the following ways:

- As a miner, providing computational resources, "gas" can be earned.
- As a storage miner, providing storage capacity, "gas" can be earned.
- As an IoT device owner, data can be monetized through a global sharing platform while retaining ownership.
- As a developer, Oracles and Dapps can be shared with the community, either on the Oracle Hub for a fee, or by providing distributed services to the market.
- As an early adopter, you can invest in the development of this exciting network through our token sale and own a stake in the asset.

# 7 / TECHNICAL FEATURES



## 7.1 CORE FEATURES

ContractNet has been developed as a Blockchain which combines several industry features, resulting in a unique approach.

ContractNet is a public, permissionless, turing-complete blockchain, much like Ethereum. One of the main differences between the platforms is, where Ethereum aims to create blocks as quickly as possible to avoid latency (resulting in a 90-second block time average as of writing this), ContractNet has targeted a block time of approximately 17 seconds. The reason for this is two-fold:

- Improved security by reducing the instances of “stale” blocks (see 2013 paper by Decker and Wattenhofer regarding block time)
- IoT devices are often either event-driven or schedule-driven, and tend to be low latency (i.e. information is generally transmitted in n minutes, rather than n seconds).

In addition, Ubiq’s Flux Difficulty Algorithm has been implemented for more consistent block times during volatile/variable hash rates.

ContractNet uses an implementation of Dagger Hashimoto proof-of-work, chosen for its ASIC resistance and light client verification allowance. ContractNet manages its block size by means of a Gas Limit of 0x8000000 (134,217,728). Ethereum has a gas limit of 1,500,000 which is sufficient for a shorter block time hence the need to boost this in ContractNet. An average transaction (non-smart contract) will use 21000 Gas, hence the network has the capacity to process over 6,000 transactions per block (3 times as much as Bitcoin).

Verifiable and autonomous smart contracts will be stored and executed on the ContractNet’s blockchain and virtual machine (CVM – ContractNet Virtual Machine). ContractNet has also implemented Swarm for unlimited distributed storage and Whisper for communications. Smart-Contracts can be created using Solidity contract-oriented programming language, and can be committed to the network using ContractNet’s geth equivalent, gContractNet (a golang client). A fully-fledged CNET wallet is on our roadmap, and we will provide a graphical user interface with intellisense for authoring smart contracts.

## 7.2 STORAGE OF IOT DATA STREAMS

Blockchains are inherently good at storing narrow rows of immutable data. IoT data streams are all time-series (value + timestamp) based and can run into multiple Gigabytes rather rapidly if the frequency of the sensor data being transmitted is high. Therefore, storing these streams on chain is not feasible. What we propose is to take a number of different decentralized technologies, combine them into a hybrid solution that ticks all of the following objectives:

1. Decentralized, resilient and auditable access control management of data streams
2. Stream Ownership and Cryptographically Secure Sharing
3. Secure Data Storage
    a. Confidentiality
    b. Authenticity
    c. Integrity
4. IoT compatibility
    a. Single Writer
    b. Several Readers

The aforementioned strategy borrows from the paper *"Towards Blockchain-based Auditable Storage and Sharing of IoT Data"* by *Shafagh, Hithnawi, Burkhalter & Duquennoy* (https://arxiv.org/pdf/1705.08230.pdf).

Therein, the solution is to separate the storage from the blockchain, and implement a "virtual-chain" as an intermediary between it and the storage layer.

The platform will be broken up into 3 main parts:

1. **Blockchain** - for transactions, execution of smart contracts and storage of access control data. The IoT data in the system will be structured into streams to accommodate for IoT specific needs (One sensor = One stream). Furthermore, ownership and sharing permissions will be defined on a per-stream basis. Transactions on the platform will contain metadata describing stream ownership and access control permissions thereof. These access control transactions, just like the underlying currency, will be written to the publicly auditable blockchain. Should privacy of access permissions be required, stealth addresses could be implemented (see *Courtois, N. T., and Mercer, R. Stealth Address and Key Management Techniques in Blockchain Systems. In ICISSP (2017)*)

2. **Virtualchain** - initially a stream owner will register a stream on the blockchain by issuing a transaction with the stream identifier. To share a stream with another user or service, a transaction will be issued that includes a stream identifier and the public key address of the user/service. This could further be developed to only grant a limited time range on the stream. For any request to retrieve data, the storage node will first check the blockchain for the required access. To allow owners to revoke access to data, all streams will be encrypted and the key management approach will frequently update keys and re-encrypt streams. These key changes will be shared with all users/services that have the required access permissions at the current point in time.

3. **Data Plane** - for the storage of IoT streams, we propose to optimise IPFS (Inter Planetary File System - *see* https://ipfs.io/). The IoT stream will be encrypted (and periodically re-encrypted) using the key generated from the virtualchain, and will be stored using the same stream identifier committed to the blockchain. Compared with storing data on the blockchain, this will at present time work out to be 2,000-8,000 times cheaper and could eventually be cheaper than cloud storage. In addition, just like the “gas” that is used to pay miners for computational power, the same incentive can be provided to miners for providing storage to the network. The benefits of using such a storage solution are:

    a. Deduplication
    b. Self-Distribution
    c. Peer-to-Peer Transfer
    d. Archiving
    e. Directory Browsing

4. **FSolidM** - Smart contracts will be further secured by implementing *FSolidM*. FSolidM is a proposal from *Anastasia Mavridou & Aron Laszka* (https://arxiv.org/pdf/1711.09327). In short, the proposal aims to address common vulnerabilities in the Solidity language (and the greater EVM ecosystem) by designing contracts as Finite State Machines (FSM). A finite state machine is a mathematical model of computation. This abstract model can be in exactly one of a finite number of states at any given time. (see https://en.wikipedia.org/wiki/Finite-state_machine).

   Mavridou & Laska have provided the following which can integrate directly with Solidity (the Smart Contract language of ContractNet, Ubiq, Ethereum, etc.):

   An FSM-based model for creating smart contracts

   A graphical interface for defining states, transitions and guards that outputs a smart contract in Solidity code

   Code design patterns implemented as plugins, that can be added to Solidity contracts to enhance security and functionality. Most notably these plugins seek to secure the contract by:

   - **Locking** - this prevents reentrancy vulnerabilities which were responsible for "The DAO" attack
   - **Transition Counter** - this plugin will prevent "unpredictable state" deadlocks where assets or execution are "frozen".

# 8 / BUSINESS MODEL

## 8.1 CONTRACTNET VISION

ContractNet's philosophy and reason for existence is to be the global interchange of IoT data, and the platform for some of the most exciting applications on the decentralized web. This unlocked batholith of data will create some of the most useful forecasts, visualizations and decisions that will better humanity and drive innovation forward.

ContractNet is a new public, permissionless blockchain which is purpose-built for the storage and sharing of IoT data streams. It provides entrepreneurs with a platform to host their businesses, using our proprietary blockchain, smart contract and IoT technology.

It also has the potential for many other business applications, which will be developed over time.

## 8.2 REVENUE STREAMS

The focus of ContractNet will be on delivering the best IoT solution. Income – and the value of the CNET coin – will be dependent on attracting large numbers of companies/consortiums of companies looking for this solution. In addition, focus will be on attracting Dapp developers, who will bring their own clients to the platform. A considerable amount of the income to be raised during the ICO will therefore be allocated towards marketing and community building.

Once there are users on the platform, revenue will accrue in the following major ways:

### 8.2.1 TRANSACTION FEES

As for other blockchains, there is a fee for each transaction completed. In Ethereum, "gas" is the unit of cost for a particular operation – it can be regarded as the "wage" needed by a miner to cover the cost of mining inputs. This means that even if you are running a Dapp with its own coin or token, there is still a requirement to pay for the gas used if it is necessary to secure your transaction on the Ethereum blockchain. ContractNet will implement a similar process, using CNET as the mode of payment.

### 8.2.2 ORACLE MARKETPLACE

Oracles will be extensions of full nodes that have interfaces to IoT technologies. ContractNet will launch an Oracle Hub of in-house developed *plugins* for the most common IoT devices. The hub will also provide an opportunity for 3rd party developers to create and share their oracles on the hub, for a fee.

### 8.2.3 ADDITIONAL BUSINESS APPLICATIONS

The ContractNet platform also allows for additional business applications. These will, however, be considered only at a much later stage, once the IoT solution has been delivered. Some ideas include:

- Dapp development for client businesses
- A decentralized exchange
- An ICO hosting platform
- A payment merchant

## 8.3 COIN MECHANISMS

### 8.3.1 INTRODUCING CNET

ContractNet will issue its own coin, known as CNET. It is both a store of value and a medium of exchange, required to access services and technology on the ContractNet platform. It is the base payment mechanism for computation, execution and validation of smart contracts on the network. All transactions on the platform will be paid for in CNET.

### 8.3.2 THE CNET REWARD TABLE

The CNET will also be the block reward for proof-of-work. CNETs are divisible by 18 decimal places and are minted through mining at a rate of 8 per block. So CNET is exactly the same as Ethereum in this regard where it has 18 decimal places, the smallest unit being called a wei. The smallest CNET unit will be called IoTFS. It will be optimized for storing time series data of IoT, to make storage and retrieval speeds faster.

The block reward decreases by one every year and trends towards zero, as per the following table:

| Year | Supply | Reward |
|---|---|---|
| **0** | **23,000,000** | |
| **1** | **25,866,909** | 8 |
| **2** | **28,375,454** | 7 |
| **3** | **30,525,636** | 6 |
| **4** | **32,317,454** | 5 |
| **5** | **33,750,909** | 4 |
| **6** | **34,826,600** | 3 |
| **7** | **35,542,727** | 2 |
| **8** | **35,901,091** | 1 |
| **9** | **36,259,455** | 1 |
| **10** | **36,617,819** | 1 |

### 8.3.3 MAXIMUM COIN LEVELS

ContractNet will only ever support a limited supply of 23 million CNETs, creating a scarcity that mimics the value of Bitcoin or gold. This is a deviation from the Ethereum protocol which has an inflationary supply of coins. So, although the table shows an increase in the number of CNET to approximately 36 million coins, ContractNet will burn coins to maintain a maximum level of 23 million. This burn-back will be from coins received as revenue for services, coins held in reserve or coins bought back from the open market.

### 8.3.4 ENSURING LIQUIDITY OF THE CNET COIN

Liquidity is becoming a significant driver for participation in ICO's and for adoption of proprietary coins. Investors expect returns for investment and look for proof of the liquidity of assets.

The technical definition of liquidity is, "The degree to which an asset or security can be quickly bought or sold in the market without affecting the asset's price". The higher the volume of activity in a market, the more an asset can be regarded as liquid.

This is exactly where many crypto startups fail. They do not consider how the value of their coin will sustain and grow its value while they work towards completing their project. Nor do they put in place mechanisms that will manage exchange rates.

If people believe that an asset is liquid, it tends to gain in value. This then drives participation in ICOs and the adoption of new coins.

ContractNet proposes the following mechanisms for increasing the value – and the liquidity – of the CNET coin:

**a. Price appreciation:**

Some price appreciation is anticipated at the time of the ICO launch. Some investors will immediately trade their CNET coins. This will be the first step in creating liquidity of the coin.

Incentivizing miners and IoT content writers through payments in CNET will increase the volume of activity in the market, thereby increasing liquidity.

More sustainable price appreciation comes from *usage of the coin* and from *adoption of the underlying blockchain,* and the goods and services associated with it. This will be achieved because the ContractNet solution is a top-level solution to a growing market need, likely to be taken up by a wide variety of industries. And the CNET is the only mechanism for payment on the ContractNet platform. Anyone wanting to undertake a transaction on the blockchain, will have to buy CNET from the open market in order to do so. This will encourage investors – and miners - to hold onto their CNET coins as they are likely to become more valuable as adoption of the blockchain increases.

It should be noted, in this context, that the Blockchain is already in its beta format, which means that investors are assured of the initial project coming to fruition fairly quickly. Considerable attention will also be given to marketing and deliberate solicitation of business from key market players as described in Section 6 above.

**b. Buyback and burning**

A *buyback,* also known as a repurchase, is when a company buys back its own shares – or, for the crypto market, its own coins or tokens. This may be viewed as an exit strategy for investors, but is also a way to maintain liquidity. It reduces the number of coins in the public market, sometimes to avoid hostile takeovers, and sometimes to minimise dilution as more tokens are created.

Burning or destroying coins has the same effect of reducing the total number of coins in existence and therefore increasing scarcity value. The value of each remaining coin increases and investors have a greater percentage share than they originally had.

Both buyback and burning will be required by ContractNet, in order to ensure that the number of coins in existence does not exceed 23 million. Some mechanisms for it include the following:

- From revenue for services: a percentage of CNET received for transactions on the platform will be burned
- From coins held in reserve: if the number of coins being mined increases, coins from the reserve will be burned to maintain the number in existence
- Coins bought back from the open market: To facilitate easy access to the ContractNet platform by potential users, ContractNet will allow them to buy CNETs from its coins held in reserve, rather than insisting that they buy coins on the open market. However, an equal number will then have to be bought back from the open market and replaced into the reserve.


## 8.4 COMPETITION

There are currently multiple versions of blockchains, including the better-known Bitcoin, Ethereum, and Ripple and some newer versions such as Stratis, Blockstack, BlockCypher, Nxt, Credits, Symbiont, Chain, Gem, Stellar, Hyperledger, Blockchain Engine, Coinstack, Ubiq.

Each of these has been developed for a specific purpose. Some key features of a few of them are summarised in the table below.

## a. Blockchain comparisons

| Attribute | Ripple (inter-bank remittances) | Ethereum (distributed applications) | Hyperledger Fabric (generic blockchain fabric) | Ubiq | ContractNet |
|---|---|---|---|---|---|
| Major purpose | Global financial transactions | Smart contracts<br>Decentralised applications (Dapps) | International business transactions, (financial, technological and supply chain). | Ethereum Fork, Smart contracts and Dapps, Flux Algorithm | **Marketplace for IoT streams, platform for smart contracts and Dapps for IoT** |
| Public or private | Private | Public | Private | Public | **Public** |
| Consensus algorithm | (custom-made) Byzantine fault tolerant (BFT) consensus | Proof of work<br>Proof of stake<br>eTash algorithm | Uses PBFT consensus model<br>Allows for interoperability of multiple blockchain ledgers within one consortium. | PoW | **Proof of work, but proof of stake will be considered**<br>**Flux algorithm** |
| Smart contract support (business logic can self-execute) | None (had Codius, but discontinued) | Solidity domain specific language (DSL) (Turing complete) | Go (golang), Java (in progress) + Support for other languages and DSLs envisioned in future | Solidity | **Solidity** |
| Native cryptocurrency for transactions | Yes (XRP) | Yes (ETH) | No | Yes (UBQ) | **Yes (CNET)** |
| Transaction confidentiality (Encryption, key-distribution Cryptographic mechanisms) | No | Smart contract level confidentiality | Smart contract (chaincode) level + fabric-level confidentiality | Smart contract level confidentiality | **Smart contract level confidentiality, permission based storage and encryption** |
| Language | | Golang, C++, Python | Golang, Java | | **Golang, C++, Python** |
| Other | Supports cryptocurrencies, fiat, commodities and other value units, like mobile minutes, frequent flier miles | Decentralized virtual computer called the Ethereum Virtual machine (EVM)<br>Turing-complete script | Open source, supported by Linux Foundation.<br>Can support a broad range of asset types – tangible (real estate and hardware) to intangible (contracts and intellectual property) | Fusion (Desktop) wallet, that combines all functionality into one interface. | **Faster blocktime, virtualchain, data plane, shared file system infrastructure** |

b. Major competitors:

**Ubiq**:

Ubiq is a decentralized platform which allows the creation and implementation of smart contracts and decentralized applications. It is built upon an improved Ethereum codebase, with changes to block times and rewards. It has also designed and applied the Flux difficulty algorithm to maintain an 88 second block time. The Ubiq blockchain acts as a large globally distributed ledger and supercomputer, allowing developers to create decentralized and automated solutions to thousands of tasks which today are carried out by third party intermediaries.

CONTRACTNET IS A FORK FROM UBIQ, SO INCLUDES THE UBIQ FEATURES, AND AIMS TO GO BEYOND THEM.

**ChainLink:**

ChainLink is a decentralized oracle network. It allows smart contracts to connect, to bring in off-blockchain data (eg APIs), push data to external off-blockchain services (eg to make bank payments) and connect with other blockchains.

Their primary contribution is that they have provided a decentralized mechanism to deal with the problem of trustworthiness of oracles. They have done this by creating a consensus mechanism (much like the proof-of-stake mechanism) to test and agree the validity of data, therefore decreasing the likelihood of data being manipulated to unfairly skew the execution of a smart contract.

CONTRACTNET HAS ADDRESSED THE SAME PROBLEM OF TRUSTWORTHINESS OF ORACLES, BUT HAS APPLIED ITS PROPRIETARY HYBRID MODEL TO SOLVE IT.

# 9 / ICO CAMPAIGN


## 9.1 KEY PARAMETERS

An ICO is planned for Q1 (March) of 2018, with a private sale during Q1 (February) of 2018. The proceeds of the private sale will be used to bring the project to MVP level and to market the main ICO sale.

Some key parameters for the full ICO include:

- All payments will be in BTC and ETH only.
- Private sale goal = 250 BTC
- ICO Soft Cap = 250 BTC
- ICO Hard Cap = 1500 BTC

It is anticipated that many of the investors will be developers or people involved in IoT. Marketing will be directed at these groups, together with the broader base of investors into crypto-based projects.

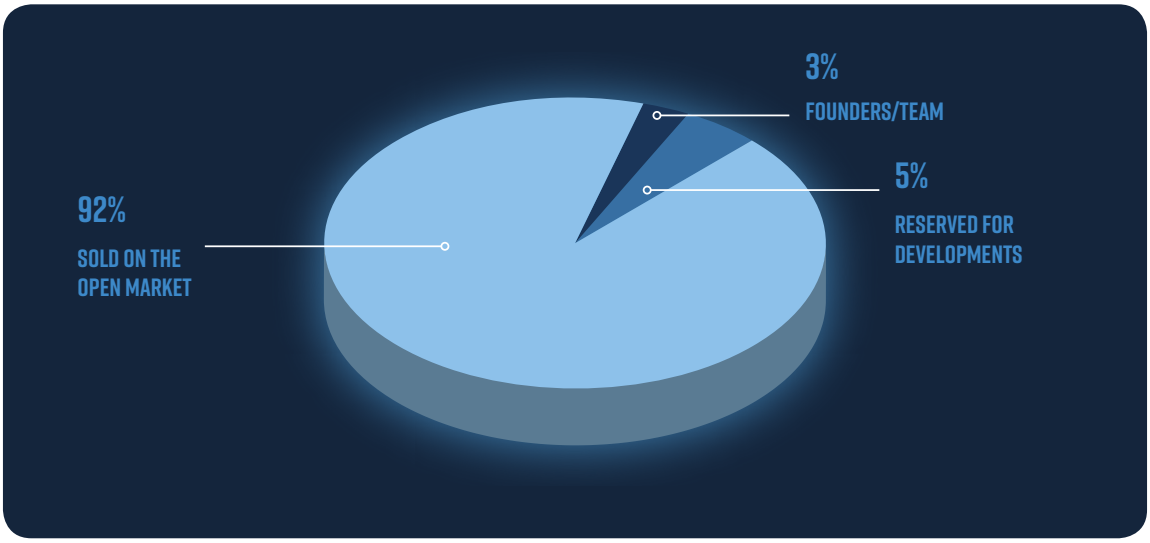
Reaching the soft cap (approx $2.5 million) will allow for the completion of the first 6 steps of the road map, at which point there will be a functional MVP. There will also be funds to start the development of the oracle hub, with focus on interfaces to IoT technologies. We will start with Manufacturing, as outlined in Section 6.2. Every additional 100 BTC raised (approx $1 million) will allow for the extension of the Oracle Hub to cover the IoT devices associated with additional industries.

## 9.2 DISTRIBUTION OF COINS

A maximum of 15 million coins will be distributed after the coin sale.

Three percent of the coins will be allocated to the ContractNet team. A further five percent will be allocated as development funds. This leaves a balance of 21.16 million coins (92%) for the public market.

The image below shows the anticipated distribution of CNET coins:




All unsold coins and unclaimed bonuses will be burned. The final number of coins will be announced after the sale.

There will be minting of additional coins through mining on the proof-of-work protocol, as described in section 7.1 above. However, the total number of coins available will never exceed 23 million, as additional coins will be burned.

One of the reasons behind the up growth of Crypto Currencies is its quick and hassle-free tradability. All new crypto currencies strive to achieve this feat as soon as possible to satisfy the initial customers and to attract more. ContractNet as a new project is doing its work on the same, trying hard to get Cnet Coins into exchanges like Gate, Exx, Huobi, Kucoin, Liqui so on and so forth. Currently the preference has been given to those exchanges which implemented Proof of Solvency (PoS) measures and which have the facility to audit cold reserves.

Having said that, we would like to make known the listing of Cnet coin into any exchange named, or not named, above would purely depend on the response from those respective exchanges. We are genuinely working to get the coins listed in as many exchanges as possible for the benefit of our customers.

## 9.3 AFFILIATE MARKETING PAYMENTS

An affiliate is someone who has registered for the ICO and has made an investment.

Affiliates who actively and directly market the ICO to others will be paid a marketing fee in BTC or ETH for every successful sale, ie if the referral translates into an investment in the ICO. These referrals and payments will be managed by a smart contract.

| Referral payment structure | |
|---|---|
| Level 1 | 11% |
| Level 2 | 2% |
| Level 3 | 3% |
| Level 4 | 4% |
| Level 5 | 5% |

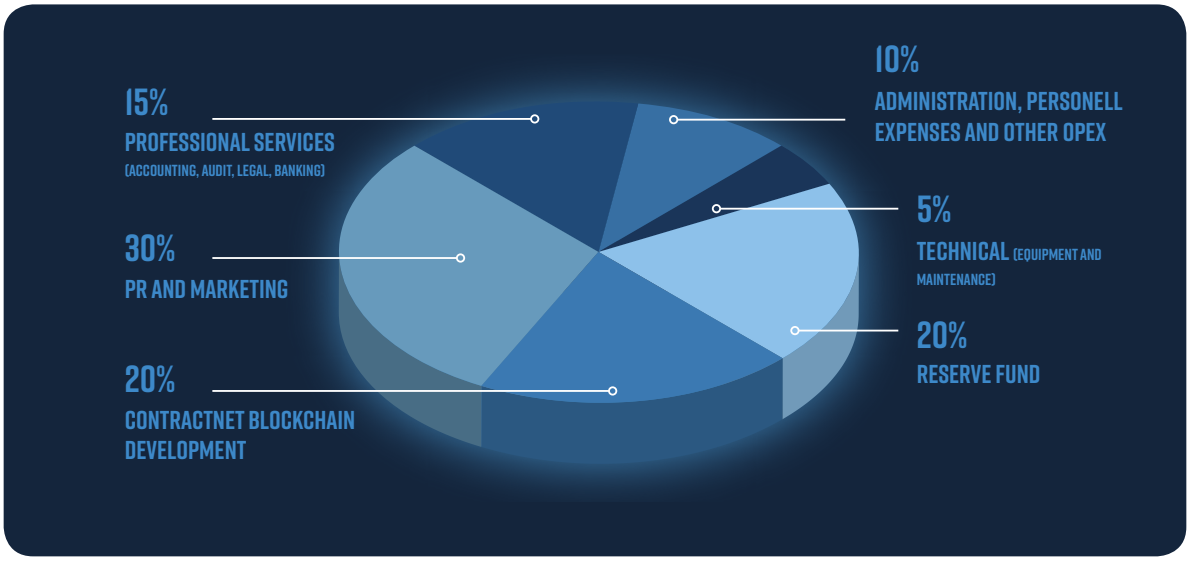
It should be noted that this is a payment for work done, and is an incentive for affiliates to actively market the project. It should not be confused with a multi-level marketing or a bounty programme. All payments are made by ContractNet directly to the affiliate in the form of BTC or ETH taken from the marketing fund.

Where an affiliate is active and markets the project to a number of friends, he/she can earn 11% of each of their investments. From the 2nd level, where a friend recommends his/her friends, the payment structure is inverted compared to the usual MLM structures. Here there can be no suggestion that “you are using your friends”, as the commission payable gets higher for subsequent levels, up to level 5.

Provision has been made in the marketing plan for the maximum referral payments, which would be 11% of all investments that came from referral. Referral commission is paid in BTC or ETH only.

# 10/ COST STRUCTURE

The diagram below shows the projected costs of the ContractNet Platform development, and therefore the distribution of proceeds from the coin sale.




| Coin Sale Budget Distribution | |
|---|---|
| Reserve fund | 20% |
| ContractNet blockchain development | 20% |
| PR and Marketing | 30% |
| Professional services (accounting, audit, legal, banking) | 15% |
| Administration, personnel expenses and other OPEX | 10% |
| Technical: equipment and maintenance | 5% |
| | 100% |

## 10.3.1 DOWNSIDE PROTECTION

20% of the proceeds from CNET Distribution within the Distribution Period will be reserved for a guaranteed buyback of CNET coins at 80% of the Distribution Rate nominated in BTC. The reserve will be stored in the form of a differentiated portfolio of major cryptocurrencies. Information on the structure of the reserve and its status will be publicly available.

### 10.3.2 BLOCKCHAIN DEVELOPMENT

Development costs are predicated on the following assumptions:

- 3 x Full Stack Engineers
- 1 x Project Manager

The monthly burn of such a dedicated team would be approximately $40,000 (this is negotiable but team size and delivery dates would be affected as a result). Assuming we start the project from 1 Feb 2018 it will take us until the end of Q4 2018 to deliver the entire roadmap, covering up to 4 industries.

### 10.3.3 MARKETING

It is to be noted that the largest percentage (30%) is allocated to marketing. This will be used initially to cover the costs of the Affiliate Marketing program. However, a major part of the success of this project will be in marketing its value to industries and companies in the IoT space. Getting them on board will also guide the direction of the Oracle hub.

# 11/ PROJECT ROADMAP

## 11.1 BLOCKCHAIN (PARTIALLY COMPLETE)

The Blockchain and the foundational technology have been started. The project can be viewed on Github (*https://github.com/ContractNetLabs/go-ContractNet*).

Storage of the Stream Identifier and Access Control Permissions, need to be incorporated into transaction creation lookups.

## 11.2 WEBSITE AND WHITEPAPER LAUNCHED (JAN 2018)

- The findings in this document are currently being incorporated into the existing whitepaper
- The website will also need to be changed to reflect the findings within this document

## 11.3 IPFS (INTER-PLANETARY FILE SYSTEM) GIT REPOSITORY FORK (FEB 2018)

The open source IPFS project will need to be forked and modified to optimize the storage and encryption of IoT time-series data as explained in Section 2. A suggested codename for this project could be “StorageNet”.

## 11.4 VIRTUALCHAIN LAYER LAUNCHED (Q2 2018)

As detailed a virtualchain needs to act as an intermediary between the ContractNet Blockchain and the *StorageNet*. This layer will be the gatekeeper that validates stream requests, and implements time based key management through key regression.

## 11.5 STORAGE MINER SOFTWARE LAUNCHED (Q2 2018)

Storage Miner software that integrates with our data layer (*StorageNet*) needs to be developed. It needs to be clearly communicated that just as regular miners earn “gas” to process computations in smart contracts, an additional revenue stream can be generated by providing hard drive storage to the network.

## 11.6 DESKTOP WALLET SOFTWARE LAUNCHED (Q2 2018)

- Fork of the Ethereum or Ubiq wallet repository
- Network and setting modifications to integrate to ContractNet
- Branding Changes to be complete
- Integrate FSolidM proposed graphical interface into the wallet software to generate *finite state machine* based contracts
- Integrate FSolidM *Locking* & *Transition Counter* plugins into the Solidity IDE. As FSolidM is an ongoing project, review whether additional useful plugins can be incorporated
- Include Bitcoin payment gateway into the wallet to facilitate the token sale, as well as a space to purchase tokens when the Sale is launched

## 11.7 OFFICIAL LAUNCH OF THE CNET WALLET AND TOKEN SALE (Q1 2018)

Users will be able to download Node, Miner, Storage Miner and Desktop Wallet software. In addition, investors will be able to acquire ICO coins.

Creating and maintaining a core, cross-platform, desktop wallet will be the primary focus of the development team. This will allow for an expansion of accessibility to the network, as we create a robust application for interacting with and supporting the ContractNet. Users can use the ContractNet's desktop wallet client as a primary, secure wallet for making transactions on the ContractNet. They will also be able to increase the decentralization and transparency of the network by running a full node and becoming a peer on the network. They will have full access to the blockchain as they interact with it, making for a more robust experience. Two--factor authentication will be implemented for additional security.

## 11.8 ORACLE HUB LAUNCHED (Q3 2018)

Oracles will be extensions of full nodes that have interfaces to IoT technologies. ContractNet will launch an Oracle Hub of in-house developed plugins for the most common IoT devices. The hub will also provide an opportunity for 3rd party developers to create and share their oracles on the hub, either for free, or for a fee.

## 11.9 MOBILE WALLET LAUNCHED (Q4 2018)

A safe secure mobile wallet for iOS and Android will be launched on the App and Google Play stores respectively.

## 11.10 DEVELOPMENT TOOLS AND AUXILIARY APPLICATIONS (Q4 2018)

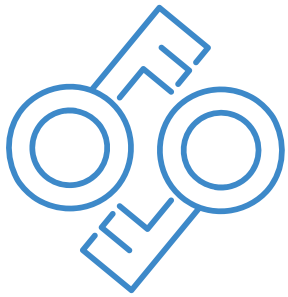
The development team envisions a community of open source and private developers building mutually beneficial smart contracts and Dapps. In our effort to support enterprise applications on the ContractNet, the Contract Net team will build robust tools that aid in the testing, securing and deploying of these smart contracts and Dapps. Some of these will include:

- Plugins to build Dapps and Smart Contracts on popular IDEs:
    - Eclipse
    - JetBrains
    - Visual Studio
- App templates

## 11.11 FUTURE PROSPECTS AND UPGRADES

- Once a viable, robust and thoroughly tested solution to Proof-of-Stake has been created, we would consider replacing Proof-of-Work which is the current consensus mechanism for ContractNet.
- Regular communication via the ContractNet Blog will keep the community up to date with technical, philosophical and personnel decisions within the ContractNet ecosystem.

# 12/ CONCLUSION



The rapid advance of blockchain technology and the Internet of Things is predicted to become a multi-billion dollar industry. It will transform industries, business models, systems and processes.

ContractNet is poised to become an integral part of this new world. It is in the process of developing the technology to overcome current obstacles to the widespread adoption of smart contracts in the IoT environment.

It promises to develop stable and robust platforms, to address issues of security, authentication and standardization, to include ideas from others in the form of Dapps, to integrate these new systems into legacy systems and to demonstrate benefits to investors, developers and industrialists alike.


contractnet.com