CONTRACTNET

THE GLOBAL EXCHANGE FOR IOT DATA

contractnet.com

CONTENTS

ABSTRACT

CONTRACTNET IS SET TO BE THE TRENDSETTER FOR IOT AND BLOCKCHAIN. THIS DOCUMENT INTRODUCES ITS KEY FEATURES AND INVITES YOU TO JOIN THE TEAM TO BRING THE PROJECT TO FRUITION

CONTRACTNET AS THE TRENDSETTER FOR BLOCKCHAIN AND IOT

CONTRACTNET – THE GLOBAL EXCHANGE FOR IOT DATA

Frank Capra, the famous American film director, once said: “Don’t follow trends, start trends.”

That quote can be applied to ContractNet today.

While there has been much talk about the intersection of blockchain, smart contracts and IoT, there is not much real application of these technologies together. This is because all of these technologies are still in their infancy, and combining them requires brand new thinking. Developers around the world are talking about potential use cases and are wanting to develop decentralized applications (Dapps) to achieve them. But there are a number of fundamental problems to overcome.

At its inception, ContractNet knew that the business opportunity was in the IoT world, and they developed a new blockchain, a fork from Ubiq and Ethereum, as the base for its platform. Over the past weeks, clear strategies have been developed to use this blockchain to overcome the problems that have been holding others back.

It is now necessary to put together the correct team – those with business skills, technical skills, development skills, marketing acumen, networking reach – to bring this project to fruition.

This document aims to introduce you to ContractNet and to provide you with the reasons to consider becoming part of the team.

1/ INTRODUCING CONTRACTNET

ContractNet is set to become *the global exchange for IoT data*. Its blockchain is purpose-built for the *storage and sharing of IoT data*. It will combine a number of decentralized and centralized technologies, and provide specialised tools for developers who want to operate in this arena. It will put together a ContractNet Partner Network to collaborate and develop smart contracts and oracles.

2/ WHY IS IOT THE RIGHT FIELD TO BE IN?

2.1 MARKET SIZE AND GROWTH

The Internet of Things is a giant network of everyday devices connecting with other devices, servers or platforms on the Internet. IoT has evolved from machine-to-machine communication (M2M), which is about networked devices exchanging information and performing actions without 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 a Forbes 2017 roundup of IoT forecasts, this is a huge global growth market:

- » Statista predicts a compound annual growth rate (CAGR) of 19,92% between 2014 and 2020 – and a market size of $8.9T by 2020. They also predict that the key adopters will be manufacturing, transportation and logistics, and utilities, averaging $40 billion each per year
- » GrowthEnabler predicts a CAGR of 28.5% between 2016 and 2020, with dominance by Smart Cities, Industrial IoT and Connected Health
- » Bain predicts B2B IoT segments will generate more than $300B pa by 2020 – led by enterprise and industrial segments. More than $80 billion has already been invested by vendors into mergers and acquisitions and $30 billion has come in venture capital.
- » KPMG predicts a CAGR of 23% between 2014 and 2019, with focus on agriculture, automotive and infrastructure.
- » PwC predicts that $6T will be spent on IoT solutions between 2015 and 2020.
- » Verizon found that manufacturing dominated the market, growing 84% between 2016 and 2017.
- » Boston Consulting Group (BCG) predicts that IOT will have the most transformative effect on industries that are not yet technology-based. They agree with Statista that the industry will be driven by manufacturing, transportation and logistics and utilities
- » McKinsey Global Institute predicts an economic impact of $11.1T by 2025.

Within these predictions, it is clear that much of this spend will be for IoT *applications and solutions*. The IDC predicts that, by 2021, spending on IoT will have moved away from hardware, and that 55% of spending will be on software and services. This prediction is supported by research undertaken by Forrester, which shows that customer focus is shifting from hardware and radios to software and analytics. *This is the market where ContractNet is positioned.*

The IDC forecast also provides better insight into the use cases for early adopters. These are the *same areas that ContractNet has targeted* for the start of its development of oracles (see **White Paper** for more detail):

MANUFACTURING

Manufacturing operations and production asset management

TRANSPORTATION

Freight monitoring (two thirds of IoT spending) followed by fleet management

UTILITIES

Smart grids for electricity, gas, and water

OTHER

Cross industry use cases, common to all industries, such as connected vehicles and smart buildings

> THERE IS NO QUESTION THAT IOT IS ONE OF THE FASTEST GROWING MARKETS IN THE WORLD. AND CONTRACTNET IS WELL POSITIONED TO BECOME A SIGNIFICANT PLAYER IN THIS MARKET.

2.2 OVERCOMING THE DIFFICULTIES ASSOCIATED WITH IOT

When we look at current discussions about why it is difficult to actually implement IoT projects, it is uncanny to see how many of them are being addressed by the ContractNet technical solution and monetization options.

Some of the difficulties were highlighted in a Forrester presentation of their research findings. In summary, these are that:

- IoT technology is incredibly diverse and segmented by use case. (The sheer numbers of devices could be intimidating. 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 vendor ecosystem is just as complex and fragmented
- Security is vital, but technologies and strategies are still emerging to deal with it
- IoT standards and interoperability will take a long time to solidify
- IoT enlarges the cyber-attack surface, making platforms vulnerable to hacking, spying, and invasion of privacy
- Tech vendors often offer complicated integrated solutions, where customers sometimes want answers to specific problems

Of real interest was the following slide of the issues to be considered in embarking on an IoT journey:

ISSUES TO BE CONSIDERED

Issue	I&O consideration
Input validation	Management and maintenance of devices requires flawless authentication.
System tampering	Detected tampering must drive immediate reaction; tampering detection is critical.
Output integrity	Systems can be misled, causing operational inefficiencies and loss.
Privacy	Storage of and access to large data repositories will be a challenge.
Scale of failure	Failed technology updates will impact millions of devices and lives.
Liability	System interactions and dependencies are difficult to map and understand.
Fail-safe	Failure scenarios or conflicting outcomes must be identified prior to deployment.
Government and legislation	Tracking data ownership and managing access to physical data among interested parties.

Presentation by Robert E Stroud, Principal Analyst, Forrester Research: *IoT Opportunities, Trends and Momentum*, 2017

THESE ARE EXACTLY THE ISSUES THAT CONTRACTNET HAS ADDRESSED IN ITS TECHNICAL SOLUTION.

ISSUES ADDRESSED BY CONTRACTNET

Authentication of devices
Prevention of tampering
Data integrity
Storage of and access to large data repositories
System interactions, interoperability and standards. This will include developing oracles for the most-used sensors and other devices in these industries
Fail-safe mechanisms – the nature of IoT is that systems cannot be allowed to fail
Tracking of data ownership and managing access to physical data among interested parties.
ContractNet also plans to reduce the inherent complexity of the market by starting in clearly defined areas, and developing solutions for the most often-used devices per sector.

2.3 CHOICE OF PLATFORM

At the end of the day, organizations and IoT technology providers are faced with the problem of *choosing the platform* to use as the base for their IoT resources. They want a platform that will integrate with their existing environment, will be secure, and that will evolve over time. They can build their own platforms, partner with existing platforms or develop an application with common tools from a service provider.

What seems to be clear is that in order to drive adoption and build scale, *partnerships* will be essential. This can be between manufacturers of industrial devices and equipment, developers of applications, analytics leaders and storage providers. Proofs of concept should lead to adding more connected devices or expanding the solution to other business units. The more the platform can be opened to third parties, suppliers, and system integrators the more the value of the solution increases.

According to Bain, platforms will be required to

» Connect and authenticate devices and sensors

» Ensure security from the start and across the entire system

» Aggregate data and run analytics

» Provide access to internal and external developers

» Provide monetization options – eg though converting use cases into commercial results or from capturing licencing fees from leveraging the platform beyond the current customer base

BENEFITS OF THE CONTRACTNET PLATFORM

ContractNet will provide a platform that is specifically optimised for IoT, meeting the requirements for connection, authentication and security.
It will provide a hub of authenticated plugins, which will include industry standards for IoT
It will provide access to developers and provide them with tools to develop their own applications.
It will establish a ContractNet Partner Network, made up of strategic industry and developer consortiums, to collaborate and develop applications and technology.

3/ WHAT MAKES CONTRACTNET UNIQUE?

Most of the narrative from researchers and enterprises quoted above relies on relatively traditional and centralized solutions. ContractNet adds some very different dimensions for a unique solution.

3.1 ContractNet brings blockchain and smart contracts to the table

Blockchain and smart contracts fundamentally change the dynamics of IoT.

Blockchain allows for an immutable record of all sensors and devices, the ownership of data, and all transactions in the saving and sharing of data. Smart contracts automate actions and processes.

However, ContractNet has also recognised the limitations and problems associated with these technologies, and has taken an innovative and pragmatic approach to dealing with them.

» It has designed a hybrid system that combines the trust and immutability of blockchain with the practicality of an off-chain storage layer, managed through a "virtualchain" and specifically designed oracles. This solution is 2,000 – 8,000 times cheaper, and significantly more efficient, than trying to store data on the blockchain itself. It also allows for scalability, which is the current flaw in blockchain technology.

» It has introduced technology to avoid the pitfalls of coding errors in smart contracts and to protect them from malicious attacks as well as problems with confidentiality and integrity of data.

» Consortiums of manufacturers, developers and users bring with them trust already inherent in their off-line relationships. However, all sharing of IP and data will be strictly controlled through access control permissions committed to the blockchain.

3.2 ContractNet brings monetization options to the table

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.

Use of the CNET as the medium of exchange on the platform also allows for monetization options for participants:

- Miners will earn CNET in return for their computational power in the Proof-of-Work consensus mechanism underpinning the blockchain
- In addition, miners can earn additional CNET for providing storage capacity on their computers
- IoT device owners can sell their streams of data to developers or other users
- Developers have access to an open source, fully optimized platform on which to develop and monetize their own Dapps. These Dapps provide physical input into the Blockchain
- Developers can create new Oracles and sell these on the Oracle Hub.
- ContractNet will earn an income from every transaction on the blockchain

3.3 THE CONTRACTNET BUSINESS MODEL

ContractNet aims to be the global exchange for IoT data and the platform for decentralized applications (Dapps) that will drive the growth of the IoT market.

3.3.1 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:

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.

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. These oracles will be available to enterprises and manufacturers in our consortiums. Payments for the use of these oracles will be in CNET. The hub will also provide an opportunity for 3rd party developers to create and share their oracles on the hub.

ADDITIONAL BUSINESS APPLICATIONS. The ContractNet platform 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

3.3.2 THE CNET COIN

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 access to stored data, and for the computation, execution and validation of smart contracts on the network. All transactions on the platform will be paid for in CNET.

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.

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. As new coins are minted by miners, 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.

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. 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 has put in place mechanisms to ensure liquidity:

PRICE APPRECIATION. Initially, this will be from immediate trading of coins at the time of launch of the ICO. However, real price appreciation will come from usage of the coin and from the adoption of the underlying blockchain.

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.

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, 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.

4/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 IoT.

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.

5/ APPENDIX I: CONTRACTNET TECHNICAL SUMMARY

5.1 HOW IS CONTRACTNET THE BEST IN IOT BLOCKCHAIN SOLUTION

In order to clearly explain why ContractNet is the best IoT blockchain solution, we must first review competing offerings in this space. We will evaluate each offering based on the following criteria which we have detailed as key differentiators in the ContractNet Whitepaper:

1. Storage
2. Smart Contracts
3. Access Control
4. Connectivity to External Data Sources
5. Consensus Mechanisms

In addition we will explain precisely why ContractNet is the better option for IoT related data.

	HYPERLEDGER	RIPPLE	IOTA	ETHEREUM	CONTRACTNET
Storage	Performs well as a Blockchain but would not be suitable to store petabytes of IoT data streams	More focused on Financial Markets and not on large scale storage	Storage is managed in the Tangle. Uses a proprietary technology without blocks and proof of work. Initial implementation, so hasn't been tried and tested.	Ethereum has Swarm for file storage which is still in development.	ContractNet will use an implementation of IPFS which is a decentralized off-chain storage method. Similar to Ethereum's Swarm but seems to be more mature.
Smart Contracts	Yes	Not capable of running smart contracts.	Not capable of running smart contracts.	Yes	Yes, with the added FSolidM implementation to protect smart contract developers from making the most common coding mistakes.
Access Control	Yes. Hyperledger is a permissioned blockchain.	N/A	Yes.	N/A	Yes, enhancements will allow storage of permission data to the blockchain.
External Connectivity	Natively possible but without security	N/A	N/A	Possible by way of Oracles but security and validation are still challenges.	Possible by way of Oracles. ContractNet maintains an Oracle Hub of trusted and tested oracles for the community. In addition, oracle development guidelines are provided to develop redundancy and accuracy into the Oracle layer.
Consensus Mechanism	Various are possible to use. Byzantine Fault Tolerance is a common selection. Lower cost but due to the permissioned nature of Hyperledger, fine for this use case but wouldn't be sufficient for a public blockchain	Proprietary Majority Approval System	Proprietary	Proof of Work with intent to move to Proof of Stake	Proof of Work. This is still the most robust consensus mechanism and ContractNet will only consider changing once Proof of Stake has been proven as a successful implementation on other blockchains.

ContractNet has been technically designed with IoT in mind. While other offerings may be generally good at solving a broad range of problems, *we have chosen to focus on the exchange of IoT data*. We have chosen to keep the monetary and payment portion of the system as pure, public, permissionless blockchain. In addition, access control permissions and file identifiers will be committed to the chain as an auditable, public record.

We have proposed a “hybrid” solution for the storage of IoT streams, the reason being the massive cost involved in trying to store large amounts of data on a blockchain. This has been estimated at 2,000-8,000 times more expensive than regular cloud storage. Instead, we have opted to fork and modify the IPFS (Inter-Planetary File System) project and repurpose it for IoT data streams. It is believed by many in the community that this type of decentralized file storage could eventually offer cheaper per GB rates than centralized cloud storage. In addition, a virtualchain will be developed to coordinate access, key management and revocation between the blockchain and this storage layer.

As for the development of Oracles, a lot of effort has been placed into how to make Solidity smart contracts secure. It was estimated that, as of the beginning of February 2018, $500 million worth of cryptocurrency had been “lost” as a result of bad code. A fair share of this number can be attributed to poor smart contract design. This has left funds open to being siphoned out of contract accounts, or these funds have been “frozen” without the possibility of getting them back. ContractNet plans to implement FSolidM (*Anastasia Mavridou & Aron Laszka*) which aims to provide a safer smart contract template to prevent introducing common vulnerabilities into code.

In addition, ContractNet aims to deliver real world relevance of smart contracts by introducing the Oracle Hub. One of the biggest obstacles preventing smart contracts from mainstream adoption has been that they operate in a *walled garden*, theoretically able to solve a multitude of problems, but without a secure connection to real life events. ContractNet’s oracle layer aims to solve this by introducing the following steps to secure data feeds to the blockchain:

1. *Rating and Review* of Oracles on the Hub and the developers that authored them

2. Patterns for reducing the influence of malicious sensors or nodes through *redundancy and aggregation*

5.2 WHY USE CONTRACTNET

At ContractNet we believe that our offering to developers is unparalleled in the industry. IoT, Blockchain and Smart Contracts are some of the most exciting and well paid in the industry. At ContractNet, we have an extremely aggressive development roadmap over the next 12-18 months which will require the best engineers in the business. Once the platform has been developed, you will have been part of the global standard in the sharing of IoT data.

One of the most exciting opportunities that ContractNet provides is that anyone can submit an Oracle for approval on our Oracle Hub. An Oracle is an agent that submits real-world information (in our case by way of IoT sensors) to smart contracts on the blockchain. Should the Oracle pass review, it will be available to a global network of Software Engineers as a plugin to use in their smart contracts. You can choose to offer this plugin for free, or you can charge a fee, much like you would on the Apple App Store or Google Play Store.

In addition, our inner technical team will have a number of challenges to solve as detailed in our roadmap. We at ContractNet have taken the approach that we wish to have a working platform in production as soon as possible, by repurposing what exists in the market already, rather than to try and invent something new. Therefore, we have opted to fork and modify a number of existing projects and assemble them in a unique way, rather than trying to develop everything from scratch. We believe that this approach will allow us to bring the ContractNet to market within a year.

To further bolster support amongst the development, user and IoT device manufacturing communities, ContractNet will create a partner network. This network will create industry specific consortiums where technical teams will work together with the ContractNet core technical team to develop smart contracts and oracles for that industry.

For example, a consortium may be setup for the automotive industry. Partners could be Toyota, BMW, Bosch (Components) and KUKA (Robotics). KUKA manufactures robotic arms for automotive assembly lines. An oracle could be developed to pass telemetry information from a welding robot, to a smart contract to confirm that all the welds have been completed and that there were no diagnostics issues at the time of the event. Committing this kind of information to ContractNet could be useful when trying to determine if there was a factory fault on a vehicle.

These consortiums will be vital in creating a thriving developer community, and for creating the first oracle offerings on the Oracle Hub.

5.3 WHAT ARE THE CONTRACTNET DEVELOPMENT MILESTONES

Over the next few months ContractNet will be embarking on a number of exciting development challenges. The development team will need to have a diverse range of skills to deliver the entire offering. The details of these milestones, the specialization and programming languages used are shown in the table below:

MILESTONE	SPECIALIZATION	LANGUAGES	CURRENT STATE	OBJECTIVES
Complete Blockchain	Blockchain	Go	Forked from Ubiq	Incorporate the technical aspirations of the whitepaper into code. These include writing the permission schema for sharing IoT streams to the blockchain
Develop the Storage Layer	Decentralized File Systems, Peer-Peer Networks	Go, Javascript	Yet to Start	IPFS (Inter-Planetary File System) needs to be forked and optimized for IoT data streams.
Develop the Virtual Chain	Blockchain, Cryptography	Go	Yet to Start	The virtual chain will be an intermediary between the blockchain and the storage layer. It will be responsible for ensuring requests are permissible and is required to encrypt, decrypt and chunk streams.
Develop the Storage Miner	Blockchain, File Systems, Peer-Peer Networks	Go	Yet to Start	Storage Miner Nodes will allow the ContractNet community to share any additional disk space that they have with the network by getting paid CNet in return. It will be similar to an IPFS node, just optimized for the ContractNet network.
Develop the Desktop Wallet	Blockchain, Smart Contracts	Go, Solidity	Yet to Start	This project will most likely start with a fork from the Ubiq or Ethereum Wallet. The wallet will allow an IoT device owner to register an account, and to append devices to that account. In addition, a full Solidity parser and compiler will be released with FSolidM plugins included. In addition, a plugin framework for Oracles will need to be developed where developers can browse for Oracles on the Oracle Hub and plug them in to their smart contracts.

MILESTONE	SPECIALIZATION	LANGUAGES	CURRENT STATE	OBJECTIVES
Develop Oracles	Blockchain, Embedded devices, Smart Contracts	Go, Solidity, Assembly (nice to have)	Yet to Start	Prior to the launch of the Oracle Hub, early adopter oracles will be developed to encourage adoption. These oracles will most likely target a device/sensor that is popular in the market.
Develop the Oracle Hub	Javascript Frameworks, Blockchain	Go, Aurelia, Angular, CSS, Typescript	Yet to Start	The Oracle hub will be an online marketplace where developers can share Oracles. A ContractNet Payment Gateway will need to be developed to remunerate developers and a full review and rating platform will need to be created.
Develop the Mobile Wallet	Mobile App Development	Swift, Java	Yet to Start	The mobile platforms that we will be targeting will be iOS and Android to start with. The mobile wallet will be a lightweight version of the desktop version.
Creation of Development Tools	Plugin and Extension Development	.Net, Java, Go, Python, Objective-C	Yet to Start	In order to increase developer support, we will be creating Development Kits for popular IDEs (Integrated Development Environments).

contractnet.com