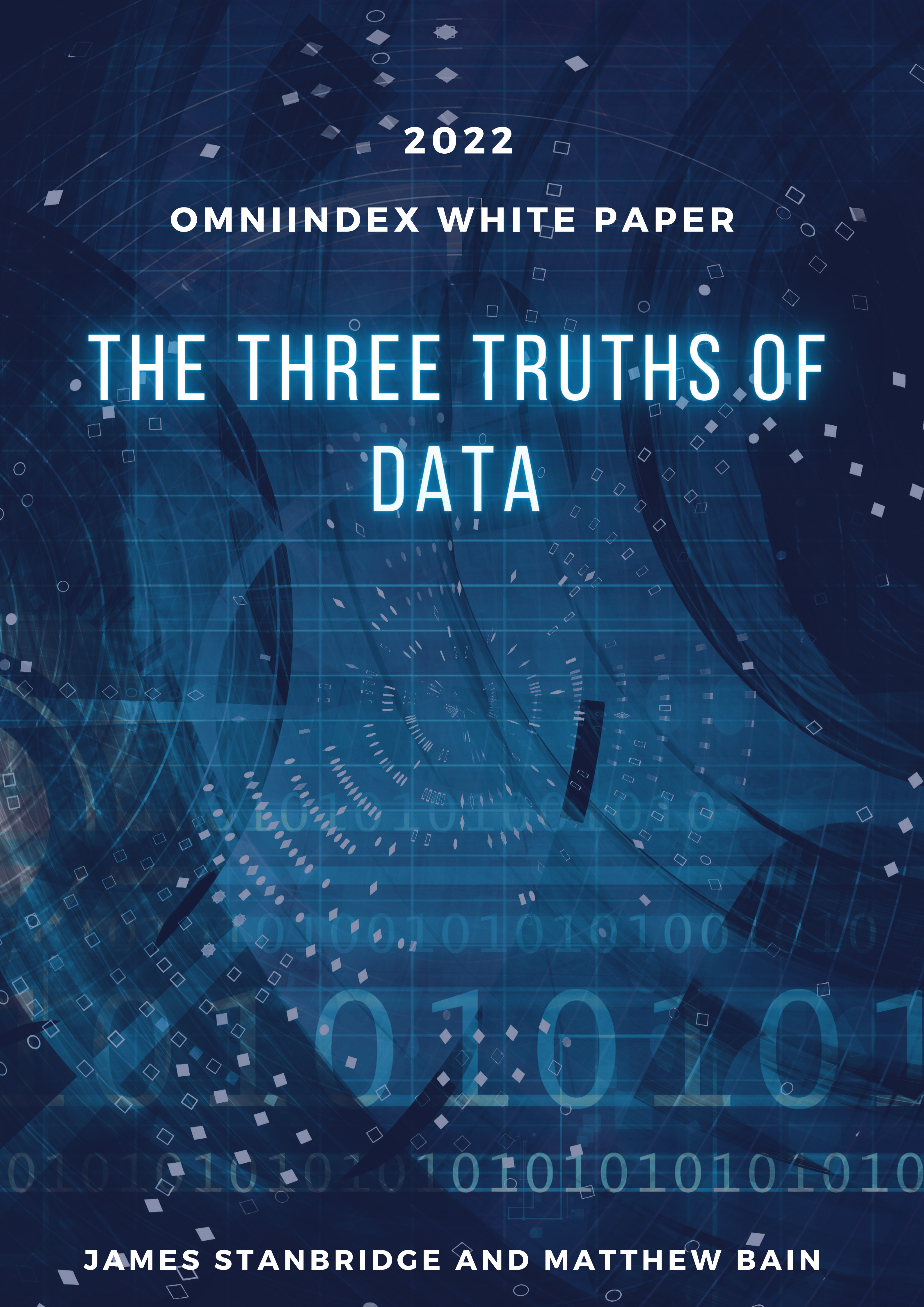


2022

OMNIINDEX WHITE PAPER

THE THREE TRUTHS OF DATA

JAMES STANBRIDGE AND MATTHEW BAIN

Making Sure Privacy Works For Us, Not Against Us.

OmniIndex's real-world applications of Homomorphic Encryption

This is an OmniIndex White Paper by James Stanbridge and Matthew Bain. It asks and answers one of the key questions in data today:

How can private information be kept securely private and be available at the same time?

Introduction

This paper proposes three essential truths of data or information. The purpose of these truths is to both protect us, and to aid us if and when the need arises. These truths are:

First Truth

My information and information about me is mine and can only be used solely for the purposes declared in the rights granted to others.

Second Truth

If such a need arises, my relevant information and the relevant information about me should be available and usable immediately.

Third Truth

The truths expressed in 1 and 2 should never be in conflict or caused to be contrary to each other.

These truths are inspired by established Western philosophies wherein notions of ownership are conferred on private citizens to respect both their privacy and the security of private or personal data/information. Societies that refuse or are unwilling to protect individuals' information are regarded as less free or in other ways regressive. Where society suspects that individual rights are being eroded, there is turmoil and dissent and so directives such as the European Union's GDPR are accepted legal protections for citizens across large populations of the World.

However, how can private information be kept securely private and be available at the same time? Indeed, this is a problem that frequently enables hackers to exploit situations by using 'social engineering'. For example by presenting themselves as needing immediate access to private data in order to trick you into authorising access to information that is private and should remain secure. This happens because when we are in a scary situation where our data could and should help us, we are more likely to lower or remove our protections to allow others to access this information. Similarly, it is a problem that means areas such as healthcare are having to limit what can be done with their data to ensure it remains private and secure. This means that potential insights and pools of knowledge are not being generated and utilised causing both patients and providers alike to miss out.

This paper outlines how OmniIndex’s innovative work with homomorphic encryption enables this seemingly impossible third essential truth to actually work in a practical setting. OmniIndex are one of only three entities in the world to receive patents in this space and are the only one to have developed commercial products that combine privacy, security and common availability.

Our intent with this paper is to show that these three truths of data are not just an idealistic future, but something that can be actioned today. The first section introduces our work with homomorphic encryption before then moving to look at its application in a blockchain in the second section. It will go into the technical details and offer use cases that are available today using our platforms and technology previews.

1: OmniIndex and Homomorphic Encryption

To begin, it is important to outline what the difference is between the encryption being used today, and homomorphic encryption.

Encryption is the process of encoding information. This process converts the original representation of the information, known as plaintext, into an alternative form known as ciphertext. Ideally, only authorized parties can decipher a ciphertext back to plaintext and access the original information. This is the industry standard method of protecting data and it ensures that the data can only be understood by someone authorised to do so. While this is the established practice and it has its merits, it is flawed if you want to share or apply modern analytic techniques such as artificial intelligence or machine learning.

Homomorphic encryption, meanwhile, is a form of encryption that permits users to perform computations on their encrypted data without first decrypting it.

From a customer or end user point of view, this is the critical difference and the big issue in encryption today: the ability to use the encrypted data.

Owing to their patented applications of homomorphic encryption, OmniIndex can guarantee the preservation of an individual's privacy with their data and information left in an encrypted form throughout use. Just as importantly, the result set, the output from OmniIndex, is an identical output to that which could be produced had the operations been performed on the unencrypted data without ever breaking the original encryption.

In short, OmniIndex enables all the advantages of powerful data analytics while maintaining the security and privacy of the encrypted data at all times.

As a popular example, almost everyone will know that WhatsApp now uses 'End to End Encryption' in its messaging services. This means that only the sender and receiver of the message can understand what was said. Therefore, if you try to hack a WhatsApp message stream, you will not be able to understand any of the participant’s private conversation.

While this privacy is crucial, the way it works means that it is impossible to run potentially useful analytics on those messages. This is because to do so you would need to remove the encryption and thus remove the privacy and integrity of those sent messages. With homomorphic encryption, OmniIndex makes this possible.

A practical application of this can be found in healthcare. This is because it is a space where people's private data can be crucial in a number of scenarios while needing to remain protected and private. For example, a Doctor or Surgeon can use OmniIndex to perform analysis of patient information or review it with peers or colleagues without ever breaking patient confidentiality. This is because OmniIndex ensures the private data remains encrypted and cannot be accessed while still gaining all the advantages of 21st century Artificial Intelligence, Machine Learning and Data Analytics.

This means that by using OmniIndex, owners and operators of medical facilities can now safely use patient data to improve outcomes for their patients, boost the efficiency of service provision and serve their patients better - all while maintaining complete patient confidentiality.

It sounds so simple!

However, without homomorphic encryption theory and OmniIndex's patented technology, this has been impossible until now.

Furthermore, OmniIndex's homomorphic encryption is used for privacy-preserving outsourced storage and computation. This extends the capabilities described above and allows data to be encrypted and out-sourced to commercial cloud environments for processing while remaining encrypted.

This has a number of important real-world benefits for sensitive data, including healthcare information. These include:

Enabling new services by removing the privacy barriers inhibiting data sharing by retaining the integrity of the data's security and privacy. For example the secure use of Predictive analytics service providers. These have been hard to apply in healthcare via a third party service provider previously due to medical data privacy concerns. However, with OmniIndex these privacy concerns are diminished because providers can operate on encrypted data instead.

Increasing the security of existing services. This security comes from the fact that even if a service provider's system is compromised, the data would remain secure as it is always encrypted regardless of the processes running on it.

Searchable Encryption

Is at the heart of all OmniIndex products

This technology is called Searchable symmetric encryption (SSE) and it allows a customer to share the storage of its private, firewalled data to a third party outside the firewall in a private manner. While just sharing the data would be useless, OmniIndex's products are unique as they maintain the ability to selectively search the encrypted information.

The privacy model is:

1: Users encrypt their files locally.

2: OmniIndex is given access to them encrypted.

3: OmniIndex (homomorphic, searchable symmetric encryption) exposes selective data objects.

4: Whenever users wish to access their files for whatever purpose including Artificial Intelligence, Machine Learning and Data Analytics, they can search directly over the encrypted data for specific keywords.

Crucially, throughout steps 1 - 4 OmniIndex does not have access to the encryption key and cannot learn anything about the private users' data.

Private Customer Data

OmniIndex treats all data as private and confidential. This means that from our first contact with your data we promise it will not be exposed.

Highest Grade Encryption

Our patented technology uses homomorphic encryption to index data sources without ever needing to decrypt or expose them.

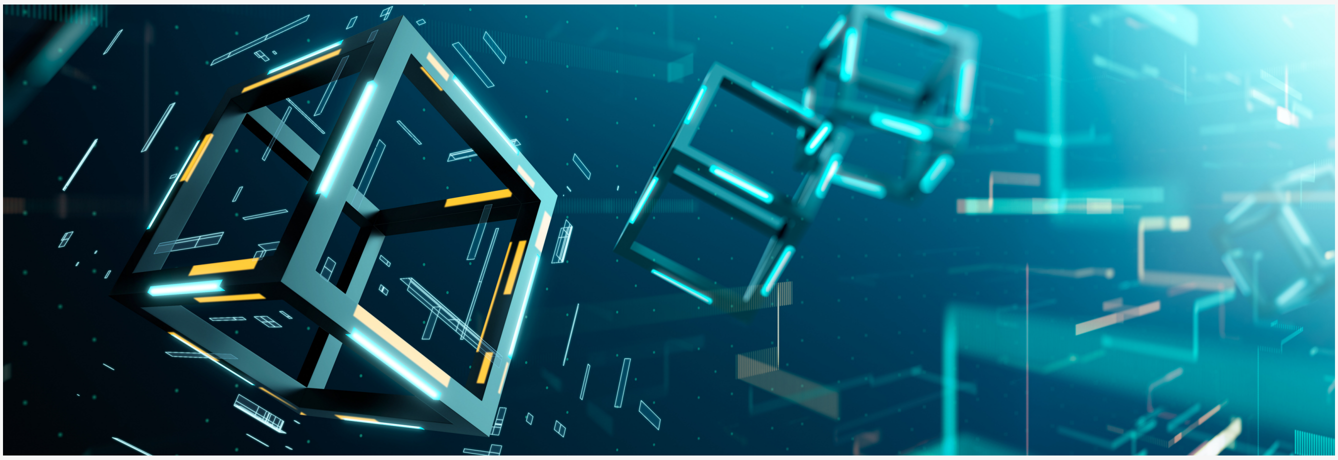
Industry Leading Data Management

Our patented technology enables us to take the needed information from the encrypted data and turn it into raw data objects that can be used to create complex analytics and reports.

OmniIndex Dashboard

Our powerful yet simple to use Dashboard enables users to take this raw data and view the information quickly and easily. You can also easily generate data visualisations and powerful reports.

2: OmniIndex Blockchain



To begin, it is important to introduce the blockchain in its current most used iteration before looking at the OmniIndex blockchain.

Commonly described by technologists as a distributed ledger, a blockchain is blocks of information chained together in a locked, unchangeable (immutable) fashion that forms a 'ledger' or record of account that may be reliably used by anyone both to verify the details of a record and to store the information of that record for use. The record can be of anything you wish. Either as mundane as the record of a lock being opened or closed (when you open your car door for example), or as complicated as a medical procedure or even an image of a scan of your ankle. The value of the blockchain is both its accessibility, it can be stored or retrieved anywhere by anyone, and in its reliability meaning that even though it exists in multiple copies, those copies are always and forever identical - meaning they can never be edited or changed intentionally or by mistake.

Furthermore, the method of distribution is known as 'peer-to-peer' which means there is no central or single server that holds the blocks and the chain, but rather it is shared and stored by anyone. This means that if you wanted to attack, destroy or take ransom any of the data, there is no single store for that attack, and the other holders of the information can reshare until the chain is complete again.

OmniIndex have added to these already impressive characteristics the ability to search within, up, and down the chain of blocks. Furthermore, while maintaining all the advantages of the blockchain, OmniIndex uniquely adds analytic data including **content context** and **content sentiment**. This information is a valuable addition to anyone holding the chain, along with **organization's private information** and **individual's private information**.

These additions mean a number of things are possible with the OmniIndex blockchain that are not possible elsewhere. These include:

1: Organizations are able to baseline and compare their analytics with all other organizations while knowing their anonymity is completely secure.

2: Individuals are able to do exactly the same.

3: Highly sensitive and confidential information can also be stored in the same chain, with access only given to the authorised recipient, where such permission is part of the immutable ledger. It can never be altered, accessed, corrupted or compromised.

HEALTH CARE
• INVENTION • HEALTH • INSPIRATION
• RESEARCH • INNOVATION • TECHNOLOGY
• INVENTORS • CREATIVITY • DISCOVERY
• MEDICAL CARE • SOLUTION • IDEA
• INVENTORS • CREATIVITY • DISCOVERY

Like OmniIndex's homomorphic encryption, these innovations have significant real-world applications. For example, let's imagine we have brought to market a device that measures blood-pressure. The device would be able to capture those readings automatically, with a time-stamp of the reading as it is taken.

The block of information we would want to store would include:

Patient identity [private]
GP identity [private]
Time-stamp of the reading [public]
Blood pressure (systolic) [public]
Blood pressure (diastolic) [public]
Pulse rate [public]

For this example, we decide that patient and GP identity are private and confidential, but so long as they are anonymous the time and readings are publicly available. (We could change our mind about this, but for the purpose of this hypothetical example we made these choices). Using the OmniIndex blockchain (tm) and the OmniIndex homomorphic index (tm), we can store a new block each time our device is used and gain insights into the information we have collected while protecting our customers' and their health-providers' privacy.

This is how it would work:

1: Using their private encryption keys, patients can view their full data sets and view analytics over time etc.

2: Using their access to the public chain, individuals can baseline and compare their results with other cohorts or the general population. This would include reviewing if similar patients were getting better or more effective treatments as well as where.

3: Using their private encryption key, patients can choose who has access to their private records. This makes it easy and secure to switch between providers at will.

4: Using their private encryption keys, Health Practitioners (GPs) can view their patients as a cohort and baseline or compare their results with other practitioners. This enables them to identify the factors that increased or reduced the effectiveness of interventions and remedies.

5: Using their private encryption keys and rights granted by a patient, Health Practitioners (GPs) can review with a patient the details of their results and treatments.

6: Using their access to the public chain, Healthcare Practitioners (GPs) can baseline and compare their results with other cohorts or the general population. This would include reviewing if similar patients were getting better or more effective treatments, including where this is happening at a competitor or across group practices etc.

This example demonstration has only the simplest information in the block. However, imagine adding more dimensions such as age, ethnicity, religion, location and the wealth as well. When we start adding more information to this secure and confidential resource, we can begin to see the real-life applications possible in regards to the benefits for both the patients and the healthcare providers alike. All while protecting the desired confidential information.

OmniIndex Technical Appendix

WHAT THE OMNIINDEX DICOM ANALYTICS BLOCKCHAIN HOLDS:

Standard Data

- Block Position
- Previous Block Hash
- Time Stamp
- Current Block Hash
- Analytic Data
- Sentiment
- Context

DICOM Image Analytics

- Hardware Use
- Procedure Data

Organization Available Data

- Homomorphic Full-Text Content Search
- Patient Data
- Clinic
- Clinician

Patient Available Data

- Homomorphic Full-Text Content Search
- Patient Data
- Clinic
- Clinician

Technical Encryption

1. Blockchain wide 256 AES Encryption Key used for creation of hashes
2. Organization has their own 256 AES encryption key
3. Customer has assigned Username/Password pair that creates 256 AES encryption Key
4. Organization & Customer data is encrypted using a homomorphic encryption algorithm.

Node Allocation

1. Each node is separate to its peers.
2. On inception, a node has to be told of one other node in the chain. It will call this node and download a 'Node Map'. It uses this map to keep sight of other nodes within the peer network.
3. Once it has the map, it will create a copy of the chain from one of these nodes.

Node Update

When a node has a new block added, it will call out to up to 10 randomly selected nodes from the Node Map and inform them of the update. Each of these nodes will update their chain and make a similar call to 10 randomly selected nodes. In doing so the chain will be updated without placing a large bandwidth call on any single node's network.

Node Searching

Searching of a blockchain can be highly problematic, slow and very memory inefficient. OmniIndex has overcome this. Our search enables Analytics output as well as full-text searching of your own private data, without compromising the privacy of that data.

Conclusion

This paper proposed three essential truths of data or information. The purpose of these truths is to both protect us, and to aid us if and when the need arises. These truths are:

1: My information and information about me is mine and can only be used solely for the purposes declared in the rights granted to others.

2: If such a need arises, my relevant information and the relevant information about me should be available and usable immediately.

3: The truths expressed in 1 and 2 should never be in conflict or caused to be contrary to each other.

This white paper has shown that with OmniIndex all three essential truths of data are attainable. This is because OmniIndex utilises homomorphic encryption theory and patented technology to enable all the advantages of powerful data analytics while maintaining the security and privacy of the encrypted data at all times.

Crucially, this white paper focussed on the technical details and use cases that are available today using our platforms and technology previews. As such, the three truths of data are not just an idealistic future, but something that can be actioned today.

If you would like to discuss this paper or OmniIndex's technology further, please contact us with the information below. We can also supply a simpler print friendly version of the white paper if required.

sibain@omniindex.io 1 (650) 268-4699