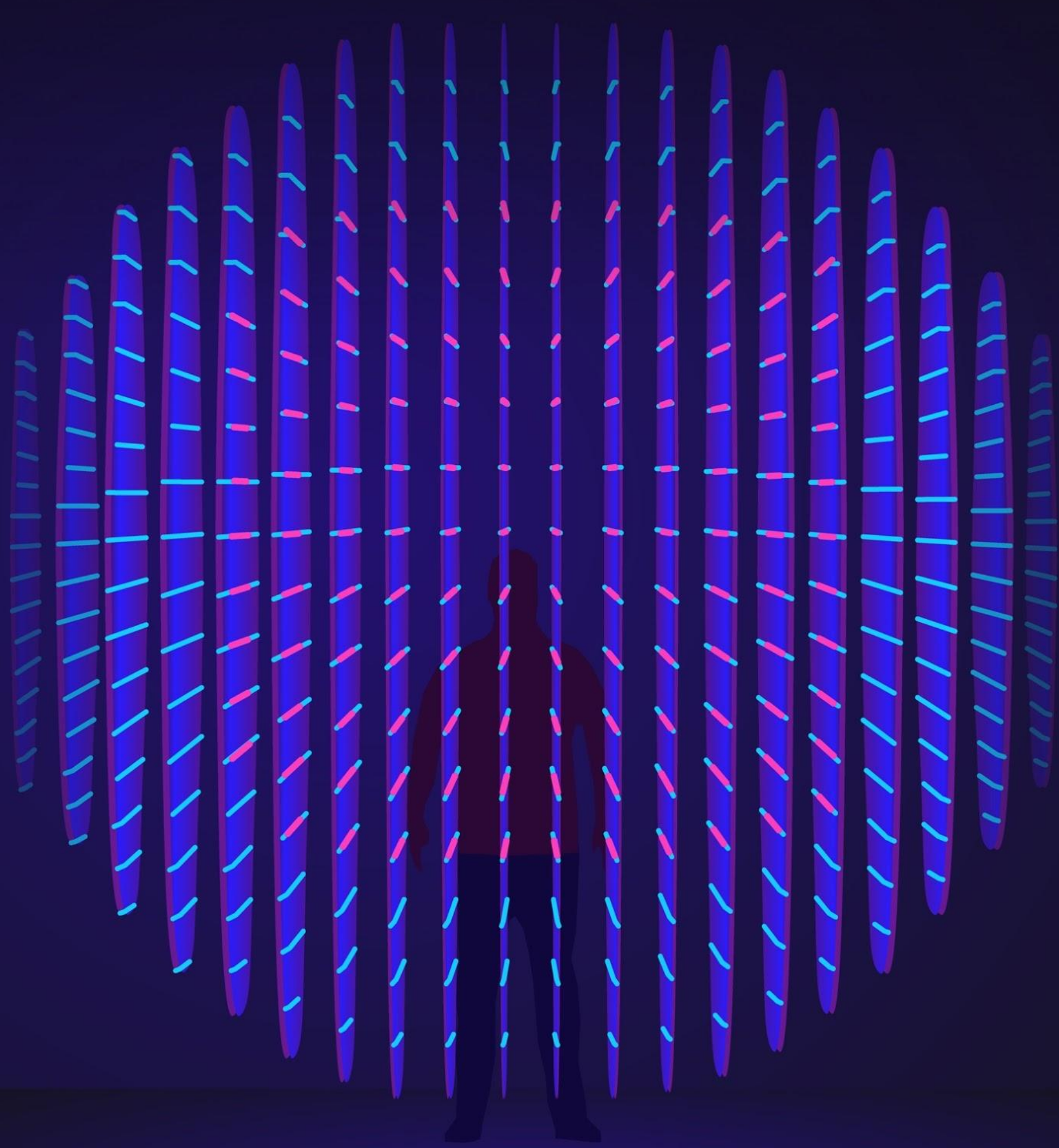
LIGHT STREAMS

Lightstreams White Paper



By Michael Smolenski

25 Jan 2019

LIGHT STREAMS

Lightstreams White Paper

CONTENTS

1 Introduction

This white paper specifies the Lightstreams Network[1], a decentralised application [2] ecosystem that revolutionises the manner in which information flows. Lightstreams empowers individuals and businesses to better track, control and monetise their personal content and intellectual property. Lightstreams does this by using blockchain and the distributed web so that content (movies, music, documents, blogs, posts, and other digital assets) is only hosted and synchronised on devices that are approved by the content owner.

Applications built on Lightstreams will differ from today's applications where social media and other internet companies host, manage and distributes data on behalf of content owners. Instead, data is separated from the applications that use it creating a paradigm shift in data custodianship and opening up the way for an internet where people can consume the same content with different applications at the same time.

Not only does Lightstreams give greater control to content owners but also enables content to become readily available to many more apps, giving greater reach and new and improved revenue streams to individuals and businesses.

Blockchain technology has been hailed to revolutionise many industries, however, blockchain alone is not the entire solution. The cost to store any useful amount of data and the controlled access of data are major barriers to blockchain adoption. The award-winning technology [3] already developed by Lightstreams addresses these issues by utilising a permissioned decentralised storage system integrated into a blockchain network. This provides uncapped storage capacity, zero storage costs for content, vastly improved speeds for transaction processing, and most importantly, the management of data privacy and confidentiality.

To give some concrete examples of the current blockchain problems:

Storing a 1MB file on the Ethereum blockchain at the time of writing would cost 18.75 ETH or $3,750 USD. [4]

The contents of the file would be viewable and any associated activity monitored by anyone.
If the above were still acceptable, it would take 78 blocks (18 minutes) to store one of these files.

Lightstreams is made possible through the combination of blockchain and distributed web technologies. Blockchain is used to manage file permissions, guarantee identity, maintain historical record and the secure transfer of value. While “off-chain” distributed storage is used for efficient data storage and transmission of files without not relying on any one entity for hosting content.

Through integration with the Lightstreams Network application developers can build on and utilize a blockchain platform that centers around speed, efficiency and privacy for distributing content.

2 The DApp Revolution

Decentralised Applications (DApps) are a new breed of applications that run on peer-to-peer (P2P) networks in contrast to traditional applications that run on centralised servers. They are made possible as a direct consequence of blockchain and Ethereum smart contract technology. Through a shift toward decentralised business models, DApps will impact almost every industry, unbundling business models that have been dominated by the few and open the way for new and more efficient models.

The primary disruptive features of DApps are:

- The ability to coordinate transactions (via a smart contract) between two or more participants of a system without requiring an intermediary. For example, a user could sell power to a neighbour in order to charge their car without requiring a power company to act as a go-between.
- The ability to incentivise network nodes through a token that can represent a store of value. Users can then be incentivised to individually and collectively perform tasks that would otherwise have been the responsibility of an intermediary.

Ethereum’s smart contract capabilities have shown huge promise in revolutionising digital agreements, but the network itself is hindered by an inability to provide adequate privacy for the content being shared in smart contracts. This rules out all use-cases where parties are dealing with confidential data (intellectual property, sensitive messages, etc.).

To truly unlock the potential of smart contracts, a network like Lightstreams is required that provides privacy controls for shared content. The protocol runs on a modified Ethereum stack while remaining compatible and version synchronised, and makes use of a permissioned IPFS [6] version to to control access to shared protected content.

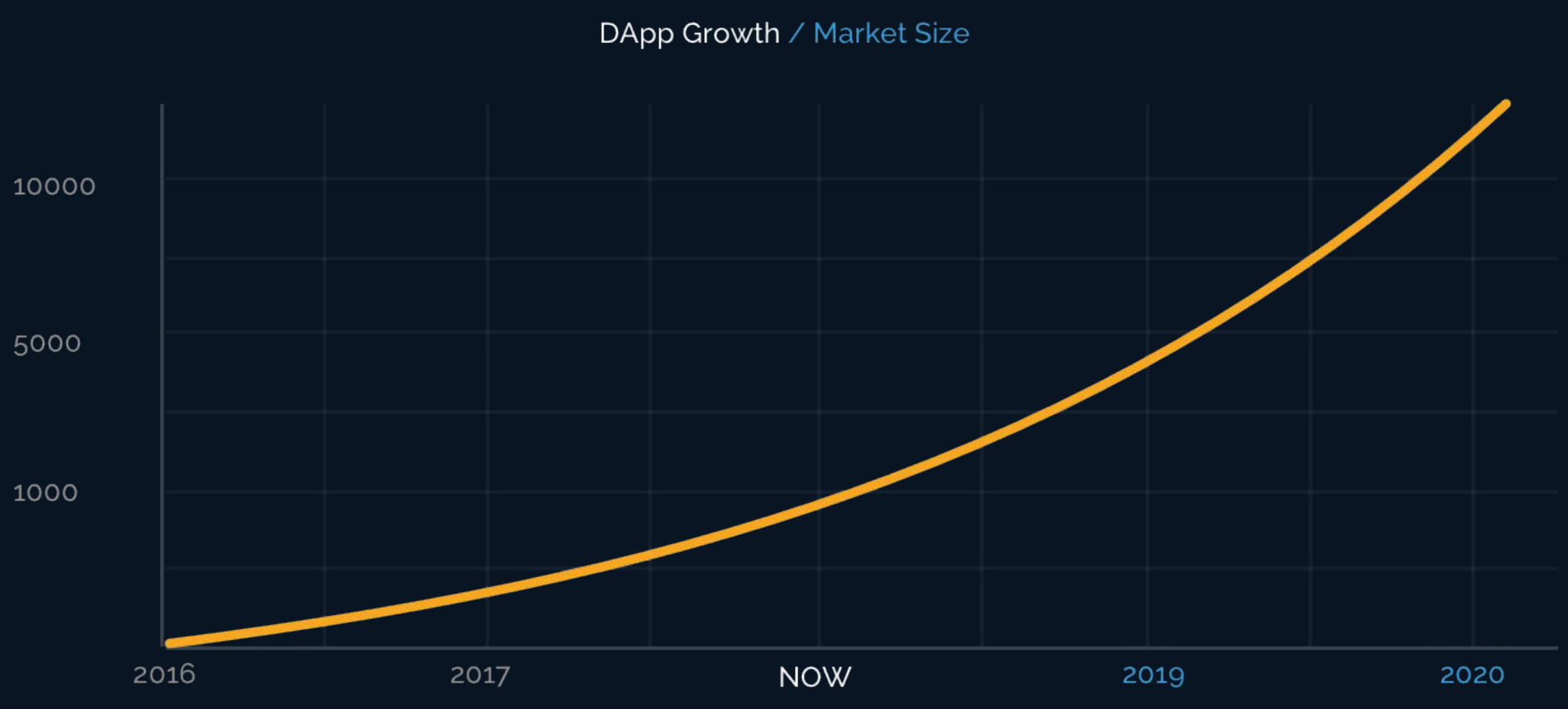
We expect to see Lightstreams play an integral role in DApps development through Lightstreams’ combination of on-chain and decentralised off-chain technology to pave the way for future blockchain applications. By leveraging the smart contract functionality of the Ethereum network and the secure content distribution, Lightstreams brings an unprecedented solution for blockchain privacy and confidentiality.

.

3 Market Size

We are only at the beginning of DApp development and already have seen the emergence of popular DApps like Augur [7], Golem [8], and Aragon [9] which have demonstrated the possibilities. With Lightstreams solving key limitations of blockchain storage and content distribution, we believe this will open the possibility for more advanced and disruptive DApps to come.

As more industries become impacted by decentralisation we expect to see an exponential growth in DApp adoption. With features to support advanced DApps, and the team's extensive experience with the limitations of the current generation of Dapps, Lightstreams will be at the forefront of providing the network to accelerate this adoption.

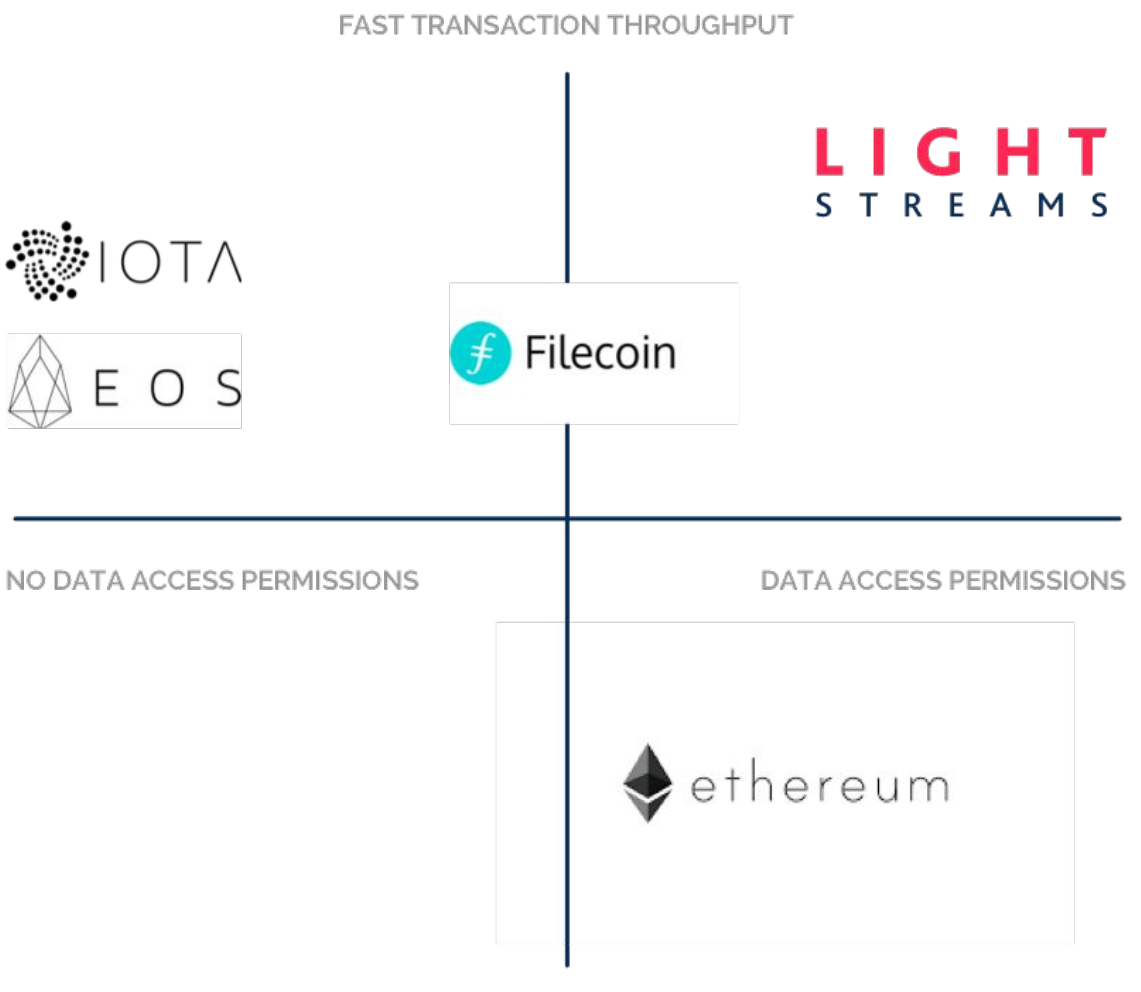


4 Differentiation

The Lightstreams software stack is built using a combination of leading blockchain and distributed web technologies; Ethereum, IPFS and Tendermint. Modifications have been made to each in order to create the award winning Permissioned Blocks [10]. This design improves storage capacity, removes costs, improves speed and most importantly access control management. All these elements are key to any DApp being viable in comparison to traditional applications and to facilitate real-world usage and widespread adoption of DApps.

4.1 How we compare to Ethereum, EOS, FileCoin, IOTA, and other chains?

ETHEREUM - Ethereum only permits a limited amount of data to be stored on the public ledger and charges high fees in order to restrict the use of this storage. Another Ethereum project, Swarm [11] attempts to solve this by allowing the storage of larger files on a very similar system to IPFS, however, there is a cost to storage and no privacy. ZK-Snarks [12] promise a level of smart contract privacy but currently do not scale requiring 40 secs to generate a proof [13]. In terms of speed, Ethereum has a block time of approximately 14 seconds and plans to scale using sharding (Plasma [14]) and Proof-of-Stake (Casper [15]) solutions, but these are very complex solutions and have still yet to be proven.



Lightstreams Differentiation - Comparison of Blockchain Speed / Privacy

EOS [16] - EOS launched with no solution for storing files of any substantial size and recently made an announcement [17] for plans to integrate IPFS to overcome this issue. They are yet to design a privacy solution for distributing content. It's consensus system, called Delegated-Proof-of-Stake, or dPoS, is a consortium blockchain that is validated by a fixed set of 21 master nodes known as ranked delegates with a long block time of 3-40 seconds which is not suitable for many DApps that require responsiveness.

FILECOIN [19] - Based on the same IPFS protocol as Lightstreams but without the capability for permissioning access to protected content. Storage is not free, similar to Storj [20], Siacoin [21], and MaidSafe [22]. Although it plans to add smart contract capabilities in the future there is no indication that this will be Ethereum-based, thus losing the benefit of access to the largest community of developers and tools for smart contracts.

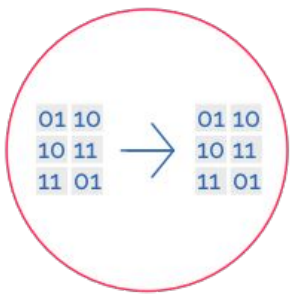
IOTA [23] - Storage is limited and not free. No privacy design for data storage nor smart contract capabilities.

LIGHTSTREAMS - Uses the proven technology of IPFS for uncapped, free data storage, Ethereum for smart contracts and Tendermint for blockchain consensus. Private and large sized files are stored decentrally using the IPFS protocol with an additional security layer for protecting access to content. Tendermint provides a fast block time of 1-3 seconds with instant finality and is Byzantine Fault Tolerant.

5 Use Cases

Lightstreams provides the key capabilities required to manage private and confidential content between participants and fast blockchain transaction throughput with near instant settlement finality for responsiveness. These capabilities are essential to almost any DApp use case. As such, Lightstreams opens the possibility for new and innovative use cases.

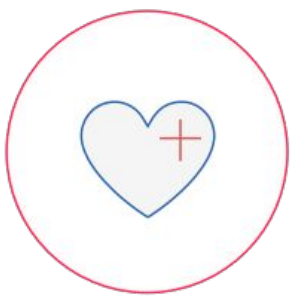
Use Cases - Various DApp Use Cases that can be developed on Lightstreams



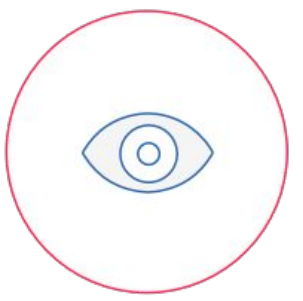
Data Exchanges

Decentralised Elections

Legal Contracts



Personal Health Records



Universal Identity Service

Content Publishing
(Music/Video/Books)

Messaging

Social Media

Title Management

Data Exchanges - Supporting decentralised data exchange markets where users and businesses can purchase and sell various data metrics.

Decentralised Elections - An automated authorisation mechanism to reveal votes after the casting time has expired.

Legal Contracts - Attachment of readable documents to smart contracts. For example, a legal document that is versioned controlled and tracked by a smart contract.

Personal Health Records - a patient can retain and manage their health record on their own devices. Access can be granted to medical physicians and third parties where needed.

Universal Identity Service - a decentralised authentication service providing identity and profile management services.

Content Publishing - Peer-to-peer sales of digital content (music, videos, eBooks) where artists, producers and authors publish and sell content directly to fans.

Messaging -A decentralised WhatsApp or Telegram style messaging services where users share content directly with each other.

Social Media - Users share content within authorised groups without the need to store information on a centralised intermediary that may resell personal information and activity to third parties.

Title Management - Digital certificates and titles can be issued as attachments to smart contracts. An owner of a physical item (real estate, vehicles, art) can prove ownership by granting access to the digital certificate. Also cryptocurrency payments can be exchange for ownership rights of the underlying asset.

6 Team

The Lightstreams' Team has both the breadth and depth of blockchain/crypto-related experience to which few teams can compare, having worked on a number of high-profile, working, blockchain implementations. In addition, the focus is very much of a technical nature which means that we can make strong and verifiable claims to being experts in turning good ideas into reality.

Michael Smolenski - CEO

Ex-Goldman Sachs Software Engineer. Solutions Architect of Westpac Bank's online payment systems which was part of a $1.3Bn transformation. Blockchain engineer at MotionWerk and author of OMOS whitepaper. Founded several start-ups and won various blockchain awards including Consensus Blockchain Hackathon 2017 applying Lightstreams technology to micro-insurance, Santander Bank Global Distributed Ledger 2016 for a Real Estate blockchain concept called Midasium and Citibank Mobile Challenge 2015. Is a certified Advanced Agile Coach and has an honours Degree in Electrical and Electronics Engineer from New Zealand.

Andrew Zappella - Executive Director

Co-founder and previously Head of Product Development at Base7Booking, a Property Management System for hotels that was acquired by Trivago in 2016. He is also co-founder of a successful Marketing and Advertising agency Suisseo that was chosen by Google as a partner company in Switzerland, Germany, and Austria. Andrew has deep knowledge and experience in the end-to-end value chain of hospitality industry. Andrew is passionate about the transformative potential of blockchain technology. In his new role, Andrew will direct his attention toward capitalizing on this technology's incredible capabilities to create new products and services that have a similar impact as in his earlier endeavours.

John Bettiol - Executive Director

Previously, head of Organizational Solutions at Trivago, a leading travel tech company. Pragmatic and direct tech delivery and team management expert. Specialises working on large-scale software projects, team/office/culture building, recruitment and startups mentoring. Previous experience includes CTO/Founder of BuzzPoints, a banking rewards program and Technical Lead at Vodafone, CTO of TranslationBooth a P2P real time distributed translation and localisation platform, Quadriga Worldwide, Virgin Australia, and WorldLingo.

Lukas Lukac - Blockchain Engineer

Technical Lead and experienced software developer specialising in development of distributed and decentralised applications. Experience includes leading technical development of products at Trivago where 100s of millions transactions across more than 55 markets are processed daily and full stack developer at TiltBook the largest poker social network with more than 20,000 members. Lukas is passionate about blockchain technology revolutionising our daily lives.

Gabriel Garrido Calvo - Blockchain Engineer

Ex-Amazon software engineer with wide academical background and expert in high performance algorithms and distributed databases. Skilled developer with deep experience in scalable and high performance solutions having worked for major blue chip companies including Trivago and Telefonica.

Aleix Suau - Frontend Engineer

Frontend developer specialising in mobile and desktop software development. An advanced AngularJS trainer where he coaches and mentors other software developers with extensive experience at HotelBeds, a tech giant in the travel industry. Aleix is also an experience Graphics Designer bringing valuable User Experience (UX) design thinking to his work. Has founded several startups and is an active AngularJS community. Has a Technology Entrepreneurship from Standford University and describes himself as a UX carer and a believer in details.

Steve Keane - Digital Design Lead

Graduated from Central Saint Martins with an MA in Communication Design. Steve has 20 years experience in digital design and UX. An award-winning, driven and diversely experienced Design Lead guided by a belief that technology drives innovation and user centred design makes it successful. He is a focused design leader, inspiring, challenging, he sets high standards for his work. Formerly Creative UX Design Lead at Thomson Reuters, now an adept start-up collaborator, he continues to produce highly original design solutions.

Sandra Newhook - In-house Legal Counsel

Sandra has two law degrees in both German and European Law. After gaining experience at German courts, law firms and Lufthansa Technik AG, Sandra worked ten years as in-house lawyer for PricewaterhouseCoopers in Düsseldorf and Frankfurt. Sandra specialised in legal compliance in the areas of investment law, bank and capital market law, supporting well known EU and Swiss investment companies and investment funds.

Lisann Ve Scalhorn - PR and Marketing

Deep knowledge in Public Relations and a M.A. International Events Management Lisann manages Lightstreams in all matters of this field. As an experienced Public Relations Manager at Silk Relations she consulted Lifestyle Brands such as Levi's, Nike and various tech companies.

Juan Wen - Business Relations (China)

Juan is part of the organizational team and focusing on business development in Asia to all new business fields Lightstreams is aiming to. Working in recruitment management and as a consultant with deep experience in this field in Japan, at NOVA Corporation, and in China, at JAC Recruitment and Rundo Cronova. Nowadays she supports businesses in development as a highly specialized key-contact for Asia.

Advisors

Happy Walters - Immortal Records / Catalyst Sports

Through his record label, Immortal Records, Happy was instrumental in launching and developing the careers of artists Korn, Incubus and Thirty Seconds to Mars. He has also worked in conjunction with Sony's Epic Records and artists like Cypress Hill, Wu-Tang Clan, Fleetwood Mac, Rage Against the Machine, Method Man and Velvet Revolver. Happy is now founder and CEO at Catalyst Sports.

George Samman - KPMG

A blockchain and cryptocurrency consultant/advisor to global financial institutions, start-ups and law firms. He has co-founded and worked for various startups in the bitcoin and blockchain space since 2013. He is also a contributing writer for various blockchain publications, including a KPMG report on Blockchain Architecture and a CoinDesk report on Advances in Blockchain Privacy. He was a Senior Portfolio Manager and Market Strategist with a Wall Street firm, and a Technical Analyst. He holds the designation Chartered Market Technician (CMT). He has been entrepreneur in residence at Startupbootcamp and Tyro FinTech Hub. He also writes a blog on blockchain technology and use cases at SAMMANTICS.

Dimitri De Jonghe - BigchainDB / Ocean Protocol

Co-Founder and Head of Research at Ocean Protocol, a leading decentralised data exchange protocol for AI. Dimitri has vast experience in the blockchain industry including Blockchain Application Director at BigChainDB, Co-Chair of the Interledger community, and Senior Developer at Ascribe. A PhD in Robust Modeling of Analog and Mixed-Signal Circuits and a Masters in Engineer. Dimitri is passionate about bleeding edge tech, self sovereignty and public utility networks.

Antony Lewis - Credit Suisse / Crypto Author

One of the foremost fintech influencers in Singapore, heavily involved in the fintech / blockchain space for a number of years, Project Manager in Foreign Exchange at Credit Suisse and Director at the Bitcoin start-up, itBit (now Paxos). He is passionate about evangelising distributed ledger technology, and has recently published his book, The Basics of Bitcoin and Blockchains and long time blockchain blog Bits On Blocks.

7 The Photon Token

The Lightstreams Network consists of an independent Ethereum compliant blockchain. Instead of Ether as the native currency, Lightstreams will operate via its own native token called a Photon (PHT). DApps building on top of the Lightstreams Network may wish to issue their own tokens using ERC20 [23] contracts or similar.

The utility of the PHT token is for:

- Network transaction fees
- Purchasing content
- Network governance

Lightstreams' core blockchain differentiates itself to the current Ethereum blockchain by addressing the following consensus model issues that are further discussed in section 10.

Scalability

Ethereum has reached its limit in transaction throughput.

Transaction Fees

High fees charged by Ethereum validators (miners) for processing transactions is limiting the viability of many micro-transactional use cases.

Transaction Fees

Settlement Finality — Has only probabilistic settlement finality. Settlement finality is the period of time needed to ensure that a transaction has been accepted. Near instant finality with 100% certainty is required for many use cases to be practically feasible.

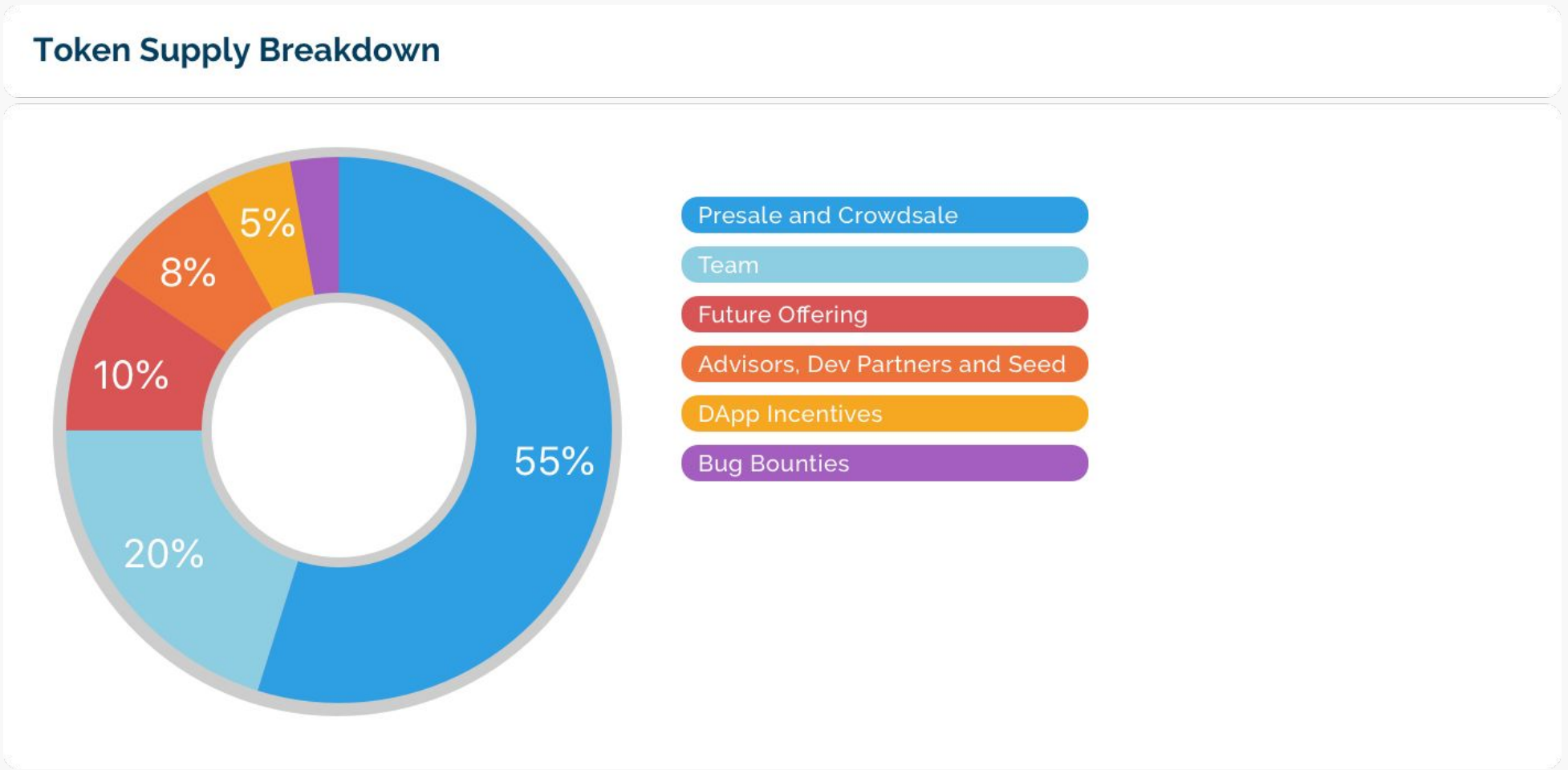
Note: Lightstreams may develop integrations to the Ethereum mainnet or other compatible blockchains in the future.

7.1 Token Sale

Lightstreams' intention is to allow a broad base of community members to participate in a Token Sale where pre-registration and qualification will be required to participate. Lightstreams cannot guarantee that all prospective purchasers will be able to acquire their desired allocations during the Token Sale where the maximum cap will be approximately $20 million (m). The amount of tokens sold during the Token Sale will be from a total sale pool of 165,000,000 Photons (PHT). For all intents and purposes, the total supply of PHT tokens during the formative stages of the network will be limited to 300,000,000 PHT. Post the formative stages, the total supply of tokens will increase as tokens become minted as block rewards by validator nodes. Block rewards mechanics are yet to be determined.

7.1.1 Total Supply Allocation

For a successful token sale reaching the hard cap the intended token distribution will be as follows. 60m PHT will be allocated to an employee bonus scheme. 24m PHT to advisors, seed investors and development partnerships. 30m PHT will be reserved for a future offering. 15m PHT will be allocated as early adopter incentives to teams developing DApps for the Lightstreams Network. 6m PHT will be reserved for bug bounties.



7.1.2 Token Sale Finances Breakdown

The majority of funds will be to continue development of the protocol, automated governance and key value-add services. The remaining portion will be used to raise awareness about the Lightstreams Network to developers, businesses and governments in order to promote DApp development.

Some of the key proceed uses include:

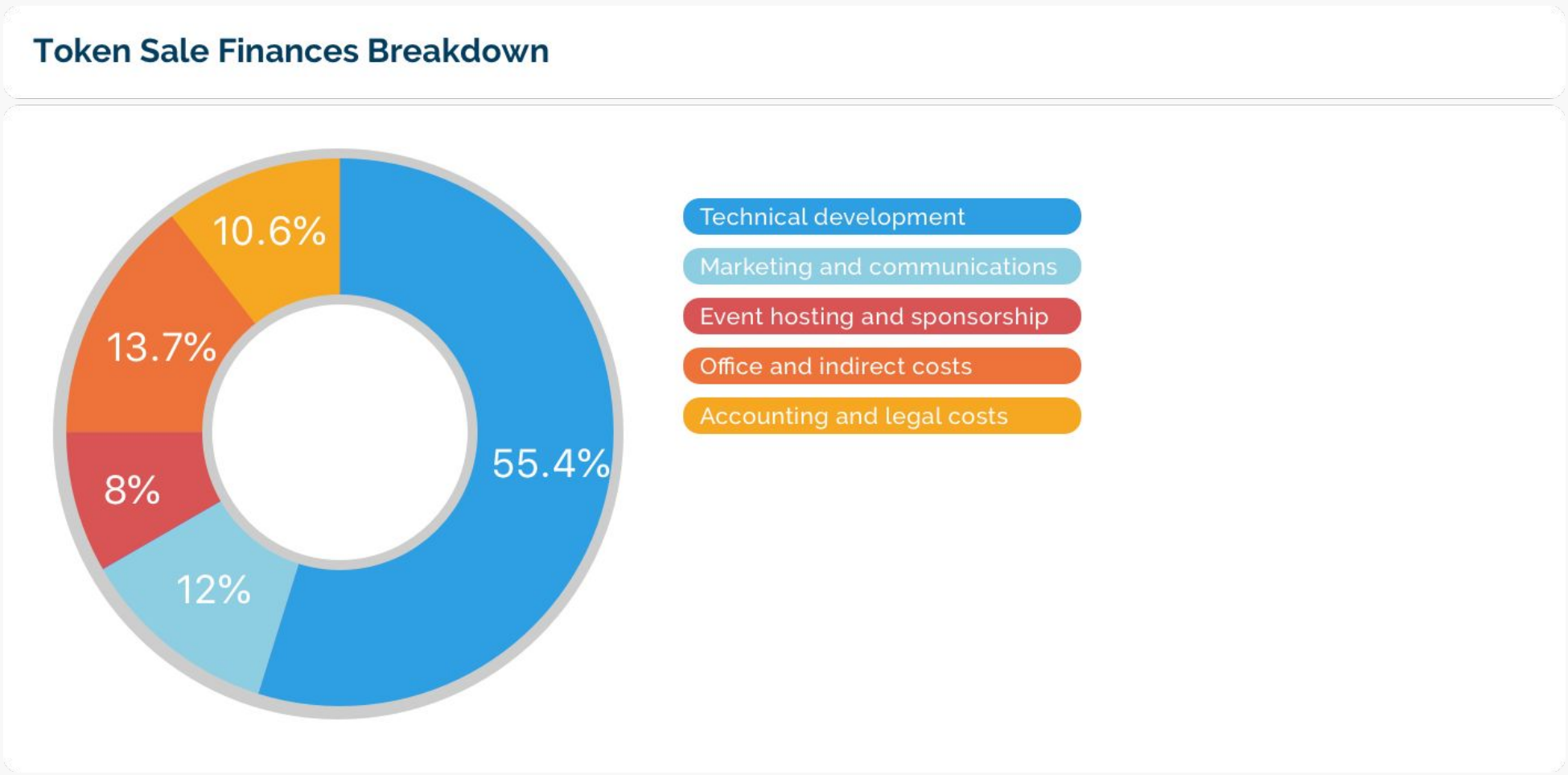
Technical development costs - associated with all three parts of the Lightstreams stack: the protocol, the services layer, and potential application layers . These costs will mainly be allocated to employee salaries and contractor costs for developing and securing the software.

Marketing and communication costs - Marketing to, consulting with, and assisting developers, businesses and government agencies to build DApps on top of the protocol. This will include hackathons, promotions, and workshops with key business partners.

Event hosting and sponsorship - to spread awareness about Lightstreams through attending or sponsoring various events.

Office and indirect costs - for office space primarily in Estonia, Barcelona and London, as well as other employment related costs.

Accounting and Legal costs - for work associated with auditing and compliance within the jurisdictions the Lightstreams team operate in.



8 The Privacy Problem

At the core of any DApp is a smart contract that describes the business rules for processing transactions. A smart contract allows for peer-to-peer transactions between participants where an intermediary would normally be required to facilitate traditional models.

However, a major issue that has limited the usefulness of smart contracts is the lack of privacy and confidentiality when sharing content, including personal information or intellectual property, between participants. Companies and individuals are currently publishing vast amounts of information on blockchain networks that can read by anyone, anywhere. This provides the opportunity to unknown parties to observe the blockchain, including governments and competitors.

Confidentiality of client information is non-negotiable in many industry sectors. The finance and health sectors are prime examples where confidentiality is essential when dealing with privileged client and patient information respectively. To date, servers and centralised protected databases have been the preferred solution [25] to this problem and many blockchain projects are still opting for this approach in their designs.

A key consideration when designing blockchain applications with centralised servers and databases is the requirement for an intermediary entity to be a custodian of data. As a consequence participants must:

1. Rely on the intermediary to administer and manage the servers and databases in order to provide continuous access for the participant.
2. Trust the intermediary to securely store private data on behalf of the participant.

There is also an issue that over time participants may become locked into using the intermediary and find difficulty in migrating to alternative systems. This clearly creates a position of power where the intermediary can:

- Charge higher fees.
- Update terms and conditions where participants have little choice but to agree to such terms including having information and activity sold to third parties.

An alternative choice to avoid the pitfalls of centralisation is decentralised content distribution with an authorisation mechanism for managing access to information. Lightstreams is such a network, allowing files of any size to be attached to a smart contract with the relevant permissions for managing access.

9 Permissioned Blocks

Lightstreams has developed an authorisation protocol called Permissioned Blocks [10] to manage access to protected content in decentralised networks. The protocol integrates two network layers that provide peer-to-peer file sharing and blockchain capabilities. These layers are:

- A Distributed Secure Storage Network (DSSN) layer, based on IPFS for peer-to-peer sharing of protected content, where IPFS blocks of data are only exchanged with authorised nodes.
- An Ethereum layer for cryptocurrency and smart contract capabilities. Smart contracts are used in this layer to manage the programmable file permissions for the DSSN.

The Ethereum blockchain has the capability to store limited data that is not practical for storing large files.

1. The impractical costs for storing large files directly on the blockchain.
2. Files would be duplicated to every node in the network as part of the global distributed ledger. This would be an impractical storage requirement for the network nodes.

The intention of an Ethereum smart contract storage is limited to recording state information required for global consensus. For example, calculating the global view of cryptocurrency account balances. To limit unnecessary data being stored on the Ethereum distributed ledger, transaction fees are charged for using blockchain storage.

Non-global state information including content distributed between authorised participants is not needed for blockchain consensus. Therefore, a complete view of this information is not required to be part of the global ledger. Instead, a reference address can be recorded on the blockchain and the remaining and potentially protected data can be stored off-chain on the DSSN.
By storing non-global state information off-chain and recording a reference address on-chain allows for a smart contract to programmatically manage versioning, registry of ownership and access to this information, while at the same time avoiding the on-chain costs for storing such data.

9.1 Distributed Secure Storage

The DSSN is a version of IPFS that has been extended with a security layer to control access to protected content. The DSSN also provides an alternative to storing data on the blockchain and a significant cost saving to network participants.

IPFS is a peer-to-peer hypermedia protocol [26] with a content addressing scheme for resolving data and has an internal protocol called BitSwap [27] for data distribution. Content-addressing [28] means that each file stored in the DSSN has a unique id in order for the routing mechanism to locate parts of the file on the network. This is similar to how the HTTP protocol [29] employs unique URL addresses to find web pages. The difference is that the unique id is constructed in such a way that the address represents the total content of the file. If any data byte in the file were to change, then the address would also change.

Peer-to-peer file sharing protocols such as IPFS or BitTorrent [30] are protocols that share packets of data between nodes in a network. When a node requests data from the network, an address is given to resolve the data, which determines a routing path to nodes that have a copy of all or part of the file. These are open networks without any security mechanisms for preventing data access.

In order to create a security layer for controlling access to protected data, the DSSN integrates with a File Permissions Registry (FPR). The FPR is implemented as smart contracts deployed on the Lightstreams blockchain and contains a record of authorised accounts that can access the protected content.

The protocol uses a token authentication scheme similar to a JSON Web Token (JWT) [31] to present claims when accessing protected data. The authentication token is signed by the blockchain account requesting the content and upon receiving and verifying the claims against the FPR, the requestor is then permitted access to the content.

9.2 Programmable File Permissions

Smart contracts are tamper-proof computer programs that can record data directly on the global distributed ledger. To deploy a smart contract, a transaction need is sent by an blockchain account, and upon successful validation the smart contract program code is included in the next block.

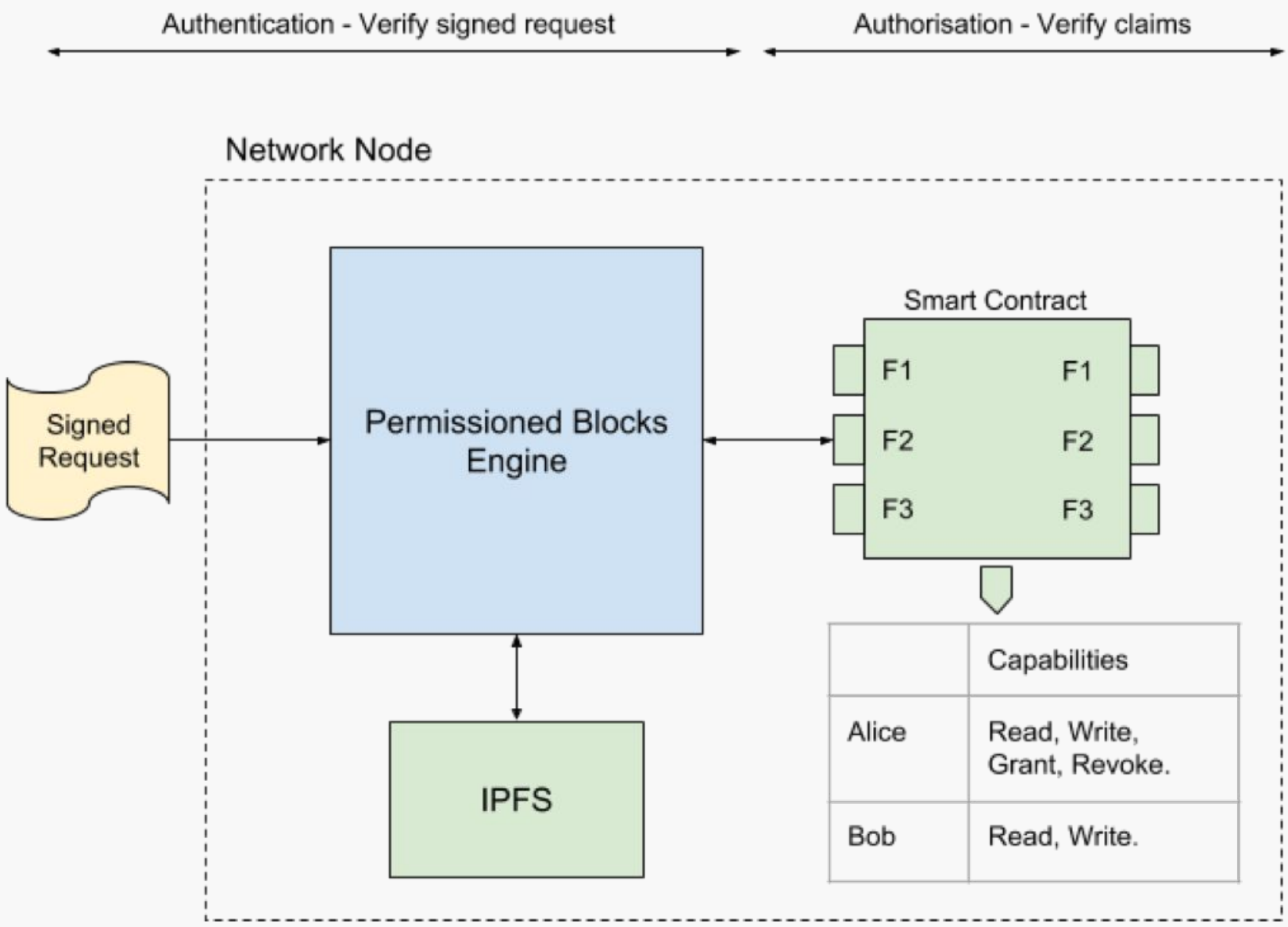
To set up an FPR for a file, a smart contract is programmed such that the deploying account is designated as the administrator account. In this way, a decentralised file manager is achieved where initially one account has access to the file with the capability to grant permissions to other accounts.

The account capabilities are stored in an FPR on a per file basis and specify the permissions granted to individual accounts.

9.3 File Access Control

Accessing data on the DSSN requires both authentication and authorisation. Authentication verifies that a message sent by an account requesting access to a file is authentic, and authorisation verifies that the account is permitted to access the information.

- **Authentication** - is achieved by a requestor sending a digital signature from a blockchain account to prove the authenticity of the message. The digital signature is generated by the requestors private key and validated by using the requestor's public key.
- **Authorisation** - occurs by verifying that the requestor is authorised to access the address of the protected file. A querying is made to the FPR to verify that the requestor has permission to access the file.



Access Control - A digital signature is used to authenticate the requesting account. The requesting account is then verified that it is permitted to access the protected content by checking whether there are associated Read permissions.

9.4 Comparisons of Privacy Solutions

Many people use ‘privacy’ and ‘confidentiality’ interchangeably, yet the two words and ‘anonymity’ mean significantly different things. The differences matter when it comes to data ownership, rights, responsibilities, and protections [32].

- **Anonymity** – is ensuring that an individual described is not known and cannot be identified.
- **Privacy** – is the individual or an entity’s right to keep personal data to themselves and not have their actions recorded or monitored.
- **Confidentiality** – refers to controlling access to protected information that is shared between parties by consent.

We can see using these definitions that it is possible to have anonymity whilst having no privacy when transmitting data, or to have privacy without an ability to authorise and revoke access to data to multiple parties.

Lightstreams authorisation protocol gives both privacy and confidentiality. Anonymity can also be achieved using a Ring Signature [33] scheme to hide payments from specific accounts. Plans to develop a custom Ring Signature implementation for Lightstreams or integration to an existing system is yet to be decided.

Platform	Anonymity	Confidentiality	Notes
Monero	Ring signatures	-	Sending anonymous payments between participants.
Raiden	-	State channels	Transactions are recorded off-chain. Suitable for multiple ongoing transactions between two parties. System of deposits to activate state channel. No seamless access to a transaction audit trail.
Ethereum	-	ZKSnarks	Smart contract functions are obfuscated. Currently does not scale for complex custom functions.
Quorum	-	Constellation	Private data is stored in separate ledger to the global distributed ledger. No public blockchain implementation. Authorised accounts cannot be amended.

9.4.1 Ring Signatures

Ring signatures are a cryptographic method that can be used to achieve anonymity for blockchain transactions. A ring signature allows for a digital certificate to be derived from a group of possible public keys without revealing which particular key was used to generate the certificate. The Monero [34] network uses the CryptoNote [35] protocol with ring signatures to achieve anonymity by obscuring a participant's transactions among accounts with identical balances.

An observer of the blockchain will see that a particular transaction came from an account for a certain amount but cannot say with certainty from which address it was sent.

9.4.2 State Channels

The Raiden network is an Ethereum implementation of state channels [36]. State channels can achieve a level of transaction privacy by recording a set of transactions off-chain. State channels are primarily useful for when two parties are constantly sending payments back and forth between each other. A system of deposits are used on-chain to ensure double spending does not occur.

The weakness with state channels is a reduction in various benefits of blockchain features including transaction auditability and traceability.

9.4.3 ZK-Snarks

Zero Knowledge Succinct Non-Interactive Arguments of Knowledge (ZK-Snarks) [37] is the foundation of the Zcash protocol [38] and recently has been integrated to the Ethereum protocol [39]. This technology provides a method to hide the smart contract fucntions using obfuscation and at the same time preserve the functionality.

ZK-Snarks hold much promise and we plan to add this feature to the Lightstreams software. The current challenge with this technology is that constructing custom ZK-Snarks circuits is difficult and they do not scale well for complex functions. For example, it takes 40 seconds to generate a proof on a standard desktop computer or 5-10 minutes on a smaller device like a smartphone [40].

9.4.4 Constellation

Quorum [41] developed by JPMorgan has developed a privacy protocol using a clone of Ethereum. Privacy is achieved through the Constellation protocol [42], a peer-to-peer encrypted message exchange for directed transfer of private data to network participants.

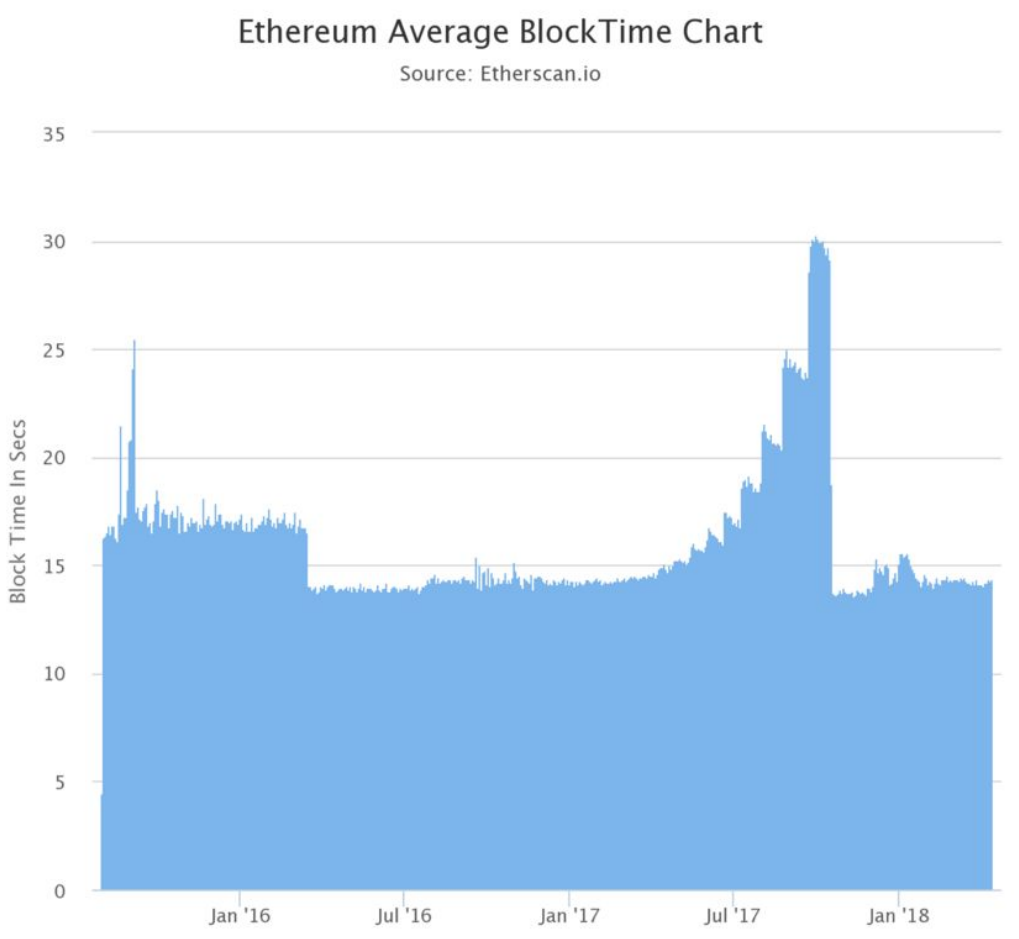
Quorum splits the local data store of the blockchain into having a private component and a public component. Only authorised accounts can access the private data store through the Constellation protocol.

Quorum does not have a public cryptocurrency and is aimed more towards consortium configurations. Private smart contracts are created by specifying the authorised accounts when deploying the smart contract. Unfortunately, once deployed the smart contract list of authorised accounts cannot be programmatically amended.

10 Consensus Model

10.1 Scalability

As of writing, the current mainnet of the Ethereum blockchain is faced with a significant bottleneck issue that limits its scalability in processing transactions. The issue is related to the network's Ethash [43] Proof-of-Work (PoW) [44] consensus algorithm where validator nodes attempt to solve arbitrarily difficult mathematical problems in order to create new blocks. The block time [45] of the Ethereum mainnet is approximately 14 seconds. PoW also has the side effect of needing an immense consumption of energy and is estimated to produce over 10,000 tons of CO2 per day [46].



Source: https://etherscan.io/chart/blocktime 18 April 2018

Already the Ethereum mainnet is reaching its transaction maximum throughput, limiting its expansion and usability. For this reason, Lightstreams will utilise the Tendermint [47] consensus that will give a block time of approximately 1-3 seconds with the ability to shard for scalability.

The Lightstreams software architecture is decoupled in design meaning that components are modularised to be more easily upgraded or replaced . This allows for modules including the consensus component to be easily replaced when innovations become available.

10.2 Settlement Finality

The current Ethereum PoW consensus lacks settlement finality. Settlement finality in PoW consensus is the period of time needed to ensure, within a certain probabilistic level of confidence, that a blockchain transaction has been accepted by the majority of the nodes in the network.

Ethereum PoW consensus is such that there are different competing versions of the blockchain, where the longest chain is considered the correct version. Technically, this algorithm never allows for a transaction to truly be “finalised”; for any given block, there is always the possibility that there may be a longer chain that does not include that block. In general, the blockchain community has settled on the standard of 6 block confirmations as a practical means for determining when a transaction is sufficiently close to being final.

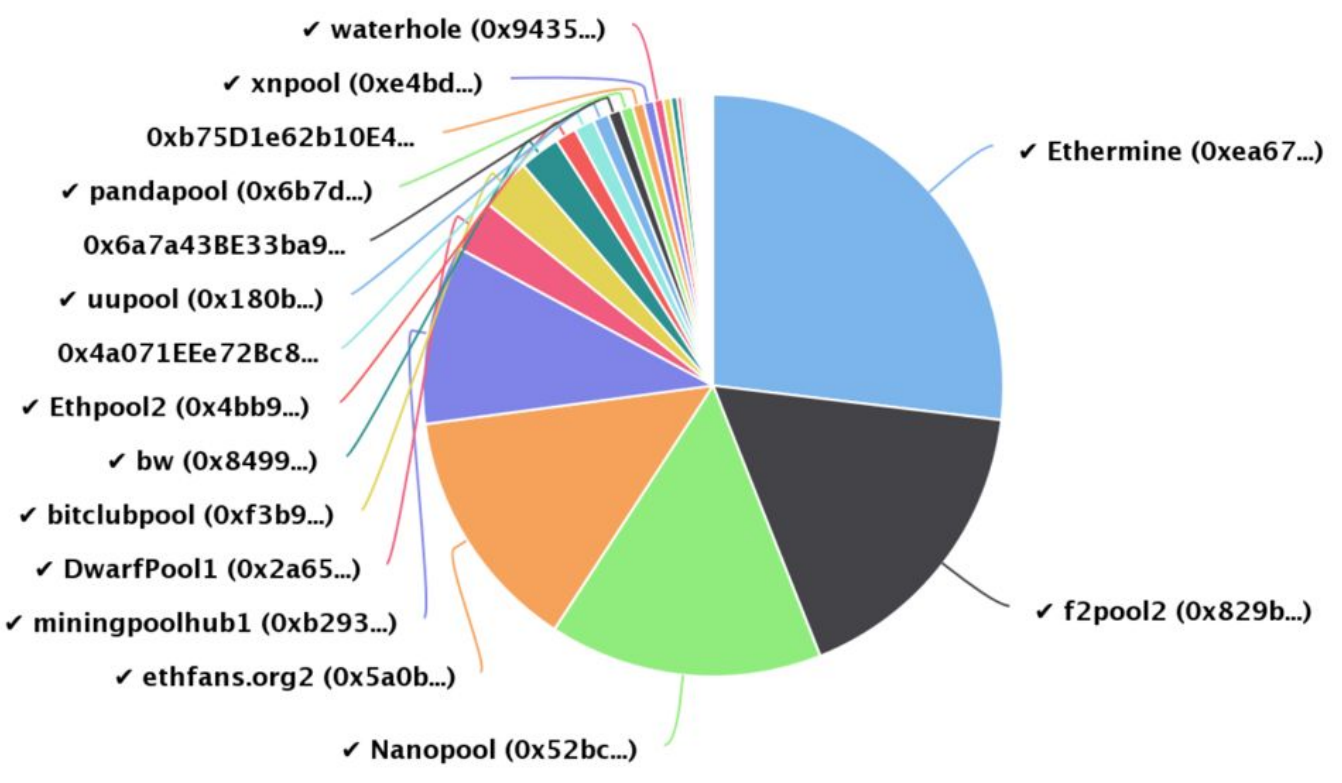
With a current average block production times of 14 secs and 6 blocks to confirm settlement, the safe settlement finality period for Ethereum is approximately 2 mins.

We believe that it is critical for the Lightstreams authorisation protocol to have near instant settlement finality for blockchain transactions. This ensures that there is no ambiguity when permissions have been granted to access protected content.

10.3 Transaction Fees

In the Ethereum network validators (miners) provide the service of processing transactions by validating and adding transactions to new blocks. In return for this service, validators charge a transaction fee and only process transactions that pass their own threshold of a gas price. In this way validators are very much in control of transaction fees..

In Ethereum and other blockchain networks, validation has also been centralised into “mining pools” where validators work together to process transactions and share in the revenue earned through gas prices and block rewards. A block reward is a hard-coded value within the Ethereum client and is currently set to 3 ETH ($2000 USD) for producing a new block. At the time of writing there are five mining pools on the Ethereum network that process over 80% of all transactions [48].



Ethereum mining pools - Top Miners, source https://www.etherchain.org/charts/topMiners

In order to ensure lower gas prices, the Lightstreams protocol will publish a set gas price for validators. Validator nodes will be obliged to charge this fee or risk being removed from the validator set.

10.4 Proof of Authority

Lightstreams will implement a Proof-of-Authority (PoA) consensus mechanism for issuing new blocks and securing the blockchain. The term PoA [49] was coined by Gavin Wood, co-founder of Ethereum and Parity Technologies [50] for a class of consensus models that includes Aura [51] and Tendermint [52]. The Tendermint algorithm was originally developed by the Tendermint project [53] and subsequently developed by Parity. PoA consensus occurs via a set of authority nodes that have been explicitly permitted to create new blocks and secure the blockchain. A round-robin of turns occurs between authority nodes for proposing new blocks. Only when a majority of authorities sign-off a proposed block does it become part of the permanent record.

Kovan [54], one of the Ethereum test networks, is an example of an existing functioning PoA network using the Aura consensus algorithm.

Authority nodes are compensated through:

- Gas fees collected for validating transactions.
- Block rewards for proposing a new block.

Block awards are newly minted tokens created by authority nodes. There will be an enforced cap on block rewards such that the total annual increase in token supply does not exceed an annual threshold set in the Monetary Policy.

Lightstreams has selected Tendermint as the PoA consensus algorithm for transaction validation. The key beneficial features of Tendermint is that it provides Byzantine Fault Tolerance [46] and has a near instant settlement period in comparison to Aura.

On-boarding new authority nodes will be via a majority vote of other token holders. To be eligible, candidates must fulfil three main conditions:

1. Identity must be formally verified.
2. Validators must obtain an accredited license.
3. Validators must have operated as an authority on the testnet for a fixed period.

To continue to operate, authority nodes must maintain a valid license and adhere to the policies and regulations set by Lightstreams governance. Further details of the licensing scheme will be published later. If a node fails to comply with regulations, a voting round via a smart contract will determine whether they remain part of the validator set.

10.4.1 Updating Authority Nodes

A smart contract will keep a record of authority nodes that are part of the PoA validator set. The smart contract will be part of the initial genesis block with a predefined set of validators. New authorities will be added to the smart contract via an election process by token holders. Proposals to remove an authority will be by a similar election process.

Authority nodes will only vote on block proposals that have been submitted by nodes that are part of the validator set.

11 Governance

Current leading blockchain networks do not have well defined governance processes. Instead, reliance is on informal and sometimes controversial governance processes that result in unpredictable outcomes.

Lightstreams will be a self-governing network where token holders collectively curate the constitution and associated by-laws will influence the behaviour of authority nodes in order to maintain a stable functioning network with the primary aim of low transaction fees and low price inflation.

It is intended that a Token Curated Governance (TCG) System using Stake Machines [55] will be developed. In such a system, token holders submit proposals that are voted upon in order to amend the constitution or add new by-laws.

Changes to the protocol will occur incrementally based on the newly approved proposals. Authority nodes, which are the only nodes in the network permitted to create new blocks, will follow out these instructions through coordinated software upgrades.

Software changes will give the authority nodes power to:

- Change the underlying protocol.
- Update defective smart contracts.
- Freeze malicious accounts.
- Amend transaction prices.
- Amend block rewards.

If an authority node fails to implement new regulations by upgrading their software to the latest approved version then an election will take place for that node to be removed from the validator set.

Token holders that are not interested in minor policy changes can delegate their voting power to others.

11.1 Monetary Policy

Authority nodes will follow a Monetary Policy that will be reviewed on a periodic basis. The purpose of the Monetary Policy is to maintain low transaction prices and low price inflation. The aim is to ensure price stability of the Lightstreams ecosystem. Inflationary controls will only come into effect once the network reaches a level of maturity. Much like central banking systems today, the inflationary control mechanism will be via a process of minting new tokens using block rewards.

The inflationary target of the network and other procedures and measures for managing price stability will be set by the Lightstreams Monetary Board elected accounts via the TCG system.

11.2 Constitution

The Lightstreams Network will publish a human readable terms of service document that will be known as the constitution of the network. The constitution will detail the terms of service of the network and the intended protocol behaviour. Amendments to the constitution and the introduction of bylaws will be translated as software protocol changes approved via the TCG system.

Bounties will be given to software developers to implement the protocol modifications. These modifications will be reviewed by peers through a bounty system to ensure the code matches the intent of the constitution and bylaws.

If any part of the protocol for whatsoever reason does not follow the intended written constitution and bylaws then proposals can be submitted through the TCG process to implement the appropriate changes.

11.3 Emergency Protocol Changes

In rare circumstances protocol changes may be accelerated through the approval process and immediately released to authority nodes. This may be in situations where a change is required to fix a software bug or security exploit that may be detrimental to the stability of the network.

12 Conclusion

Lightstreams is a blockchain based network with a unique authorisation protocol for controlling access to private and confidential data including personal information or intellectual property. The technology focuses on the requirements of privacy, confidentiality and scalability for Decentralised Applications that interact in direct, peer-to-peer channels.

Lightstreams is compatible with the existing ecosystem of Ethereum developer tools and libraries. Its governance model is smart-contract based and utilises token incentives to shape policies and actions that are curated by the token holders of the Lightstreams network. In this way, the real users of the network are empowered to shape the day-to-day behaviour of the protocol and its long-term direction, with the ability to build the next iteration of the internet through decentralised applications.

With Lightstreams, we will begin to see a greater shift towards decentralization and accordingly an exponential growth in the use of DApps in our everyday lives.

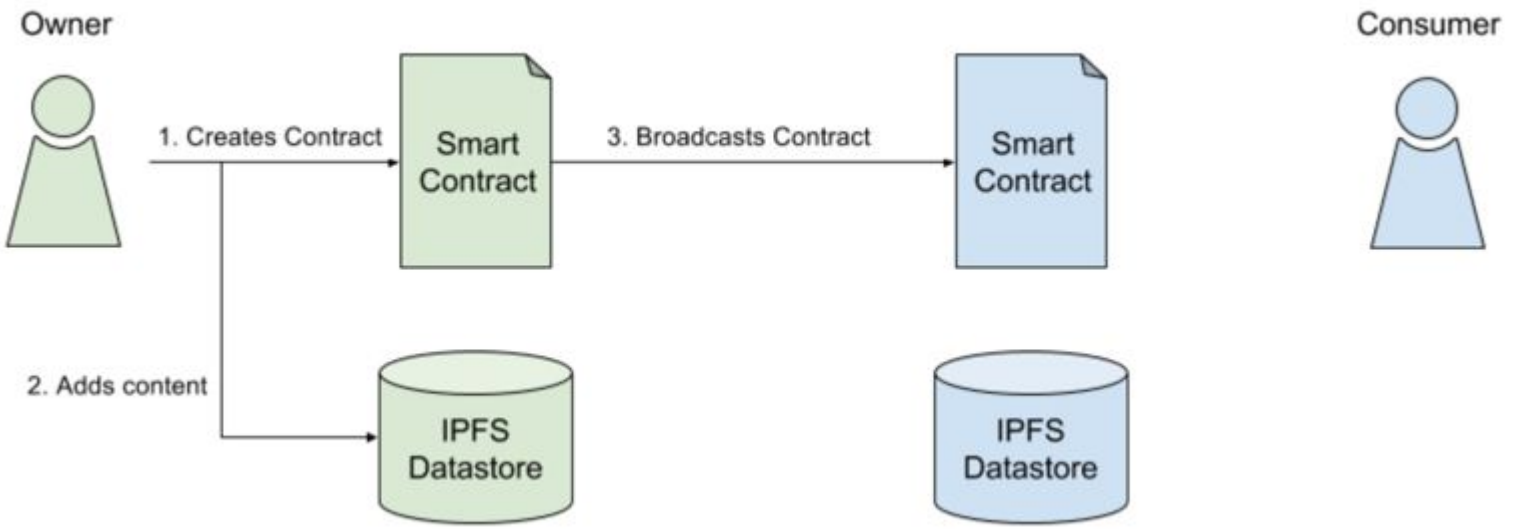
13 Appendix

13.1 Purchasing Content

The following is an example of using Lightstreams for peer-to-peer sales of digital content..

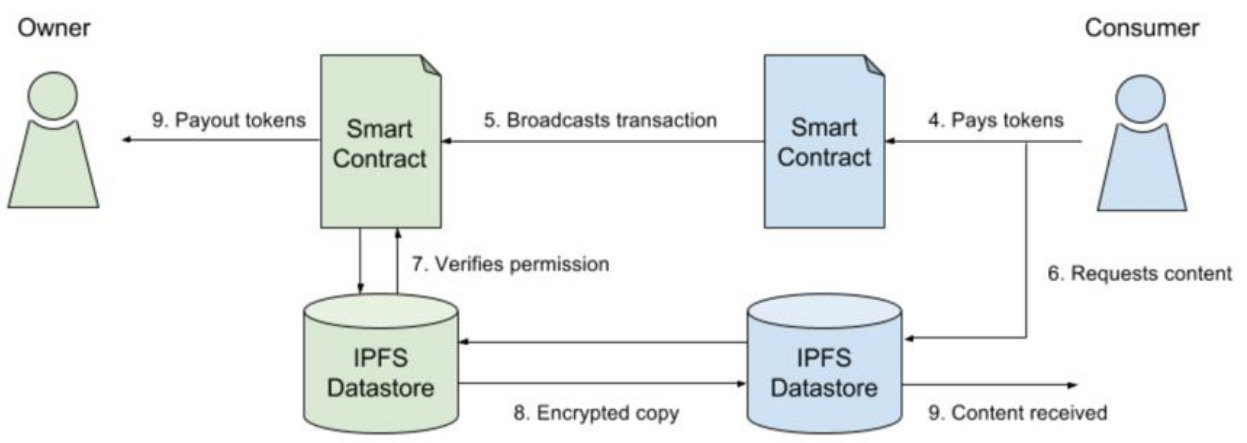
The smart contract behaviour is as follows:

1. The owner creates the smart contract with a set price.
2. The owner uploads a version of the content that is stored in their local IPFS data store and this address is added to the smart contract.
3. The smart contract is published to the Lightstreams network.



4. A consumer purchases a copy of the content by sending PHT tokens to the smart contract at the specified price. The smart contract transfers the tokens to the owner.
5. The transaction for purchasing a copy of the content is broadcast across the Lightstreams network.
6. To retrieve a copy of the content, a request is made via the IPFS bitswap protocol. The IPFS address specified in the smart contract is used for the request.

7. The smart contract on the owner's node (or any node that has the content), verifies that the consumer has purchased the content.
8. An encrypted copy of the content is sent to the user via the IPFS bitswap protocol.
9. The copy of the content is decrypted and is received by the user for reading.



Consuming of Content - Consumer pays the price and retrieves a copy of the content.

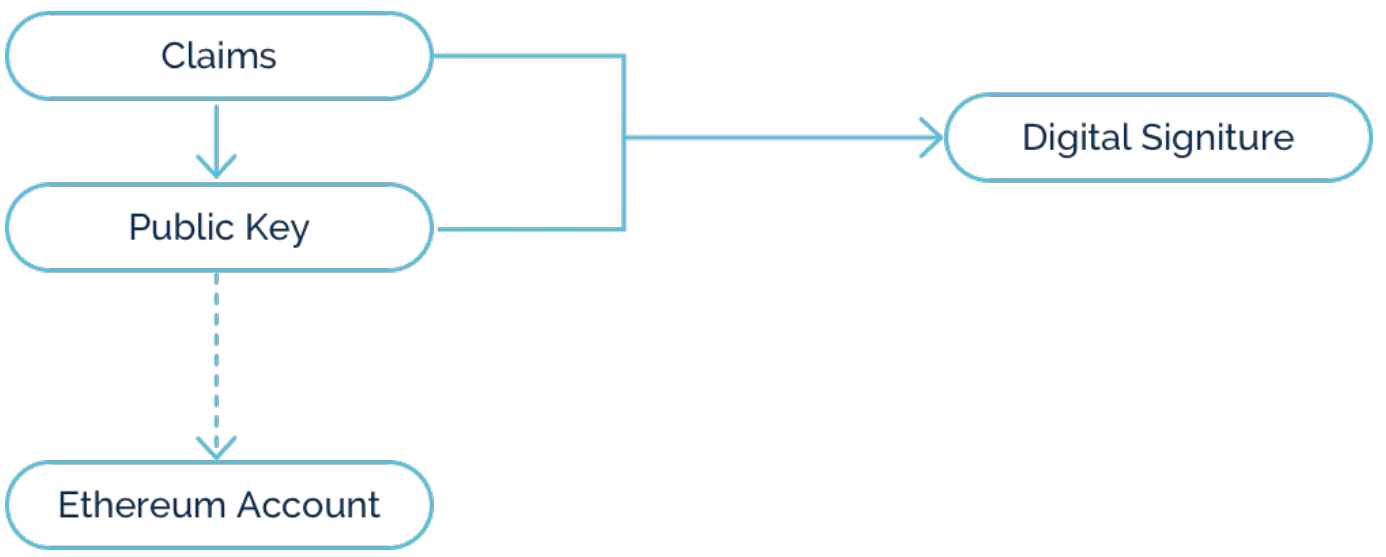
13.2 Authentication Model

Lightstreams utilises a A token authentication scheme to verify the authenticity of message requesting data from the DSSN. The authentication token is similar to a JSON Web Token (JWT). The authentication token is divided into two segments, the first segment contains claims, and the secondary segment contains the digital signature. The token's signature is generated using the blockchain account of the requestor.

```
{
    Content Address: [IPFS Address]
    Blockchain: [Target Blockchain e.g. ETH]
    ChainID: [Main chain, test net]
    Contract: [Smart Contract]
    Account: [Blockchain account]
    Issuer: [Node ID]
    IssuedAt: [BlockNumber.TransactionNumber.TransactionHash]
}
```

Claims - The first section of the token are the claims asserted by the requestor in JSON format and then Base64Url encoded.

In order to produce a reliable timestamp for the IssuedAt claim, the blockchain itself is used as a reference point in time. Usually a time-stamping authority is used in such distributed architectures to establish a unified reference point in time, like in PKI systems. This however would create a dependency on a third party, and the blockchain transaction count is a reliable, trustworthy heartbeat by design. The timestamp is generated by using the latest Block Number and Transaction Number in combination with the associated Transaction Hash.



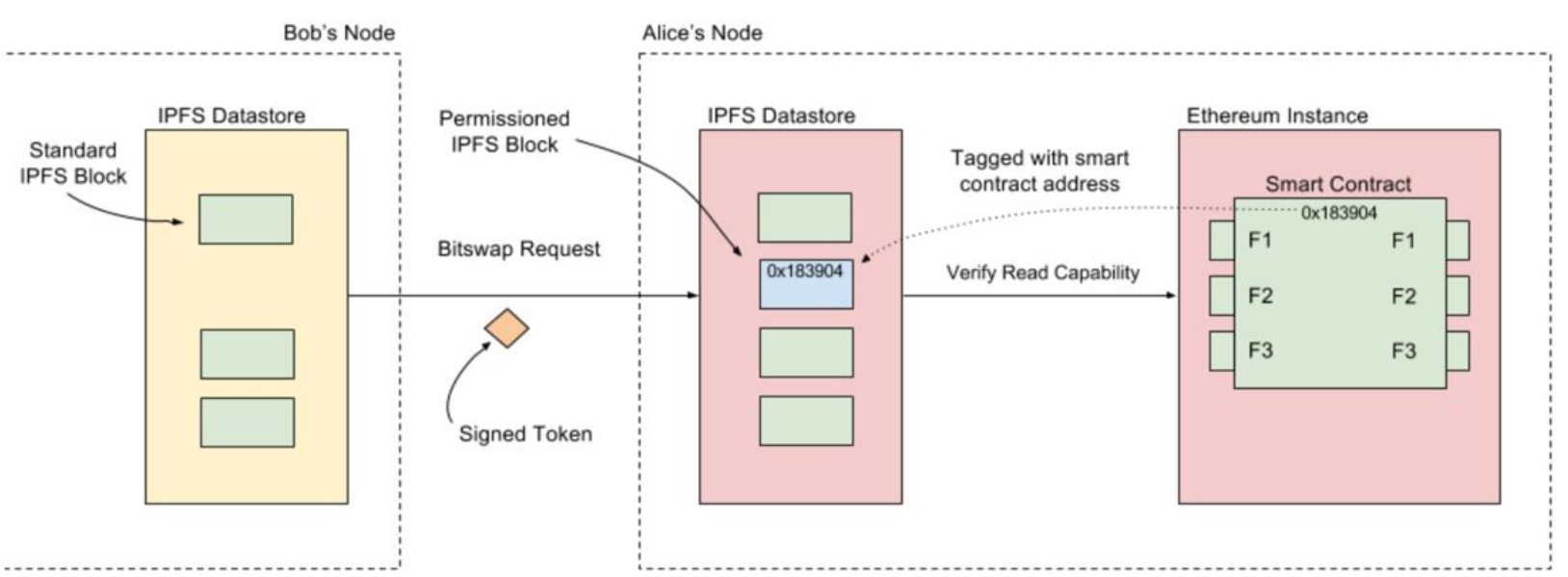
Digital Signing - The second section of the authentication token is the digital signature for the claims. The public key of the requestor is used to generate the digital signature. An Ethereum account is derived by the associated public key.

13.3 Authorisation Model

IPFS has been modified such that certain blocks require authorisation to be resolved.

IPFS divides and stores data in block sizes of 256KB. To identify blocks requiring authorisation from regular blocks, blocks are tagged in the IPFS data store with the smart contract blockchain address. When a request is made to retrieve a block from the data store, if it is tagged then the security process of authentication and authorisation occurs.

Authorisation of the requestor to access a block occurs by verifying that the requester has been granted a 'read' capability. The capabilities are stored in the smart contract and these are queried via an inter-process remote call from the IPFS instance to Ethereum instance using the smart contract address specified by each tagged block. If authorised, the IPFS sends the block to the requestor via the IPFS bitswap protocol.



Permissioned Bitswap Protocol - A request is made from Bob's IPFS instance to Alice's IPFS instance for a Permissioned Block. The request contains a signed token that authenticates Bob's identity. Alice's IPFS instance makes a remote call to her Ethereum instance to verify if Bob is authorised to access the requested block.

When a requestor successfully receives the IPFS block, it is then tagged in their data store with the smart contract's address and the same authorisation will occur if any other node in the network requests this block.

If the requestor is not authorised, then the request is simply ignored. The IPFS Distributed Hash Table (DHT) routing system will route the request to other nodes until a timeout occurs. When the timeout occurs, this will signal to the requestor that the block cannot be resolved either because the block does not exist or they do not have permission.

13.4 Account Capabilities

The account capabilities are stored in an File Permission Registry for each file and specify the permissions granted to each account. An account can have multiple capabilities. The capabilities are defined as follows.

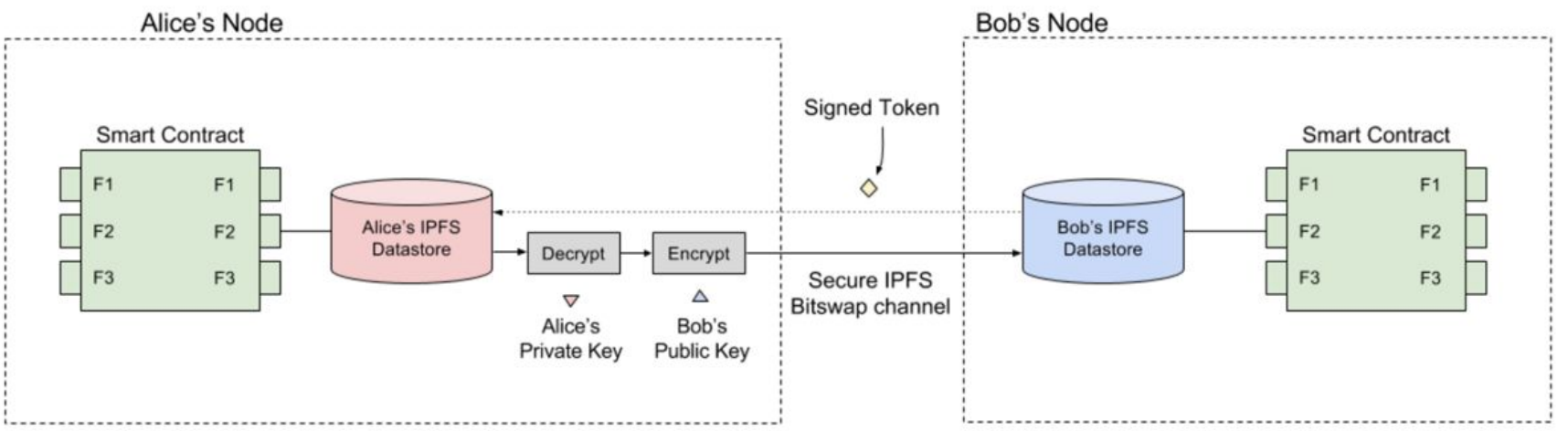
Capability	Description
Read	The account is able to read the contents of the file.
Write	The account is able to change the version of the file.
Grant	The user is able to grant a capability to another account.
Revoke	The user is able to revoke a capability from another account.

Account Capabilities - Account permissions that can be mapped to a file.

13.5 Secure Transmission

The channel for transmission of blocks needs to be secured in order to avoid messages being read by unknown participants while in transit. To secure the channel, all communications are encrypted so that only the receiver can decrypt the information being sent.

Encryption is performed using an asymmetric key. An asymmetric key has a public key element for encryption and a private key for decryption.



Secure communication channel - The IPFS bitswap channel is secured by encryption of the IPFS blocks using the requestor's public key.

Private information is encrypted by the sender using the receiver's public key and decrypted by the receiver using their private key. The public key is stored in the smart contract and the private key is kept secret by the receiver and is never transmitted.

14 Citations

[1] Ethereum Project - https://www.ethereum.org/

[2] Ethereum Homestead - DApps http://ethdocs.org/en/latest/contracts-and-transactions/developer-tools.html

[3] Permissioned Blocks - Hackathon Win! Consensus 2017 - https://mikesmo.github.io/blog/2017/06/09/Consensus-hackathon.html

[4] Calculating Costs in Ethereum Contracts https://hackernoon.com/ether-purchase-power-df40a38c5a2f

[5] EU General Data Protection Regulation - https://www.eugdpr.org

[6] IPFS - A peer-to-peer hypermedia protocol https://ipfs.io/

[7] Augur - http://www.augur.net

[8] Golem https://golem.network

[9] Aragon https://aragon.one

[10] Permissioned Blocks - https://github.com/autocontracts/permissioned-blocks/blob/master/whitepaper.md

[11] Ethereum Swarm http://swarm-guide.readthedocs.io/en/latest/introduction.html

[12] ZK-Snarks in a Nutshell by Christian Reitwiessner - https://blog.ethereum.org/2016/12/05/zksnarks-in-a-nutshell

[13] Zk-SNARKs: Under the Hood - https://medium.com/@VitalikButerin/zk-snarks-under-the-hood-b33151a013f6

[14] Plasma white paper - https://plasma.io

[15] Ethereum Casper - https://github.com/ethereum/casper

[16] EOS - https://eos.io

[17] EOS Storage White Paper - https://steemit.com/eos/@eosio/eos-io-storage-white-paper-now-available

[19] FileCoin - https://filecoin.io

[20] Storj - https://storj.io/

[21] Sia - https://sia.tech/

[22] MaidSafe - https://www.maidsafe.net

[23] IOTA - https://www.iota.org

[24] ERC20 Token Standard https://theethereum.wiki/w/index.php/ERC20_Token_Standard

[25] Advances in Blockchain Privacy and Confidentiality by Nolan Baurle, George Samman and Pete Rizzo https://www.coindesk.com/research/advances-blockchain-privacy-confidentiality/

[26] IPFS - Content Addressed, Versioned, P2P File System by Juan Benet https://arxiv.org/pdf/1407.3561v1.pdf

[27] IPFS Bitswap Specs - https://github.com/ipfs/specs/tree/master/bitswap

[28] Content Adressable Storage https://en.wikipedia.org/wiki/Content-addressable_storage

[29] Hypertext Transfer Protocol -] https://en.wikipedia.org/wiki/Hypertext_Transfer_Protocol

[30] Bit Torrent - https://en.wikipedia.org/wiki/BitTorrent

[31] JSON Web Tokens - Introduction https://jwt.io/introduction

[32] Privacy vs. Confidentiality vs. Anonymity: What you need to know https://breakthroughanalysis.com/2017/04/14/privacy-vs-confidentiality-vs-anonymity-who-knows/

[33] Ring Signature - https://en.wikipedia.org/wiki/Ring_signature

[34] Monero - https://getmonero.org/

[35] CryptoNote - https://cryptonote.org/

[36] Raiden Specification http://raiden-network.readthedocs.io/en/stable/spec.html

[37] Zero-knowledge succinct non-interactive argument of knowledge - https://en.wikipedia.org/wiki/Non-interactive_zero-knowledge_proof

[38] ZCash protocol - https://z.cash/

[39] Integrating ZCash with Ethereum - https://blog.ethereum.org/2017/01/19/update-integrating-zcash-ethereum/

[40] ZK-Snarks in Ethereum - https://etherworld.co/2017/02/28/zk-snarks-in-ethereum/

[41] Quorum - https://www.jpmorgan.com/global/Quorum

[42] Quorum GitHub repository - https://github.com/jpmorganchase/quorum/blob/master/README.md

[43] Ethereum Ethash - https://github.com/ethereum/wiki/wiki/Ethash

[44] Proof-of-work system - https://en.wikipedia.org/wiki/Proof-of-work_system

[45] A gentle introduction to Ethereum - https://bitsonblocks.net/2016/10/02/a-gentle-introduction-to-ethereum

[46] Ethereum PoW Pollution - https://github.com/ethereum/EIPs/issues/861

[47] Tendermint: Byzantine Fault Tolerance in the Age of Blockchains - https://atrium.lib.uoguelph.ca/xmlui/handle/10214/9769

[48] Etherchain - Top Miners https://www.etherchain.org/charts/topMiners

[49] Proof-of-authority - https://en.wikipedia.org/wiki/Proof-of-authority

[50] Parity Technologies - https://www.parity.io

[51] Aura https://wiki.parity.io/Pluggable-Consensus.html#aura

[52] Tendermint https://wiki.parity.io/Pluggable-Consensus.html#tendermint

[53] Tendermint - https://tendermint.com

[54] Kovan Testnet - https://github.com/kovan-testnet/proposal

[55] Token Curated Governance with Stake Machines - https://medium.com/@DimitriDeJonghe/curated-governance-with-stake-machines-8ae290a709b4

General and Utilities Disclaimers

These materials (the “materials”) are not intended to be an offer to sell, or a solicitation of any offer to buy, any security or other financial instrument or to invest in the photon token and are for informational, illustration and discussion purposes only. These materials are as of 22 October, 2018, may not be complete or final, may be estimated, are subject to change and do not contain material information regarding an investment, including specific information relating to an investment’s risks. The offering of the photon token has not been registered, qualified, or approved under any securities, futures, financial instruments, capital markets, or exchange control legislation, regulation, or ordinance of any jurisdiction. In all jurisdictions,the offer to sell and solicitation to buy a photon token is directed solely to qualified institutional investors, qualified professional investors, and those other sophisticated persons to whom offers and solicitation may be made without any licensing, registration, qualification, or approval under applicable law (collectively, “qualified persons”). These materials do not constitute an offer, distribution, solicitation, or marketing to any non-qualified person, and is not an offering to the retail public in any jurisdiction where such offering is unlawful. You should disregard this information sheet if you are a non-qualified person before you decide to purchase in a photon token, you should carefully read photon’s documents and consult with your own advisors. Lightstreams does not make any representation or warranty as to the accuracy or completeness of the information contained in these materials. Lightstreams also has no obligation to update or keep current any information or projections contained in these materials.