Blockchain Based System for Data Delivery and Certifications

Authpaper Coin

WhitePaper

Table of Content

Abstract

1. Abstract

Delivery of confidential and commercial documents have been relied on physical mailing in the previous decades. Physical mailing allows documents to be delivered confidentially with concrete evidence on delivering / not delivering and current digital delivery solutions failed to do so. Authpaper Delivery uses blockchain to provide a peer-to-peer platform to deliver confidential data with unforgeable delivery records and recipients authentications. Authpaper Delivery is also a platform for users to issue document with unforgeable certifications and this protection works even on the physical document copies. Besides, this platform allows users to deliver huge digital copyright information securely, like movies, software and even system images. In this whitepaper, this solution, its impact to society, and ICO related to this project will be discussed.

Executive Summary

2. Executive Summary

In the era of information technology, technology advancements have changed human lives by a lot. However, document delivery, especially commercial and important ones, are still following years old methods, physical mailing. Physical mailing takes a lot of time and spends a lot of resources.

There are ways to deliver data via digital channels like emails, BitTorrent, instant messaging and centralized servers. However, only physical mailing allows the document to be confidential, provides trustworthy mailing record, and easy to use. Hence, it is still dominant even in this highly digitalized world.

Besides, it is well-known that all printed documents/ credentials are potentially subject to forgery. Every year, billions USD has lost directly due to document fraud.

With a vision of “building trust across real and digital world”, Authpaper limited has been providing document anti-forgery software solutions for years and obtained patent, academic publications, supports and international awards.

In this project, we would like to combine blockchain and other current technologies to build a peer-to-peer digital data delivery platform. All data delivered is confidential except the specified recipients. Data is verified to be unchanged down to every single bit. Operations on the data are properly done and recorded among the peers so that the delivery histories are public verifiable yet unforgeable. Peers are rewarded by delivering the digital data and helping to run the platform with good will.

This platform also works as a decentralized document certification and circulation system. It allows users to issue documents under their email / name and send to other like certificates. Authorized people can “sign” a data (e.g. contract) from others and cannot deny it afterwards. The protection can be readily extended to even the physical copies, with our award-winning document authentication technology.

Authpaper coins (AUPC) (ERC-20 based) is released in this ICO to raise fund for development and testing of the platform. When the platform is ready, investors can exchange the AUPC to the stamps in Authpaper delivery platform and enjoy the service. The contribution details on our ICO can be found in Section 6.

Background

3. Background – The problem we see

We are living in a highly interconnected world. However, trust and reality cannot be delivered more effectively, if not even harder. The advancement in technology has made document forgery even easier. Technologies and operations like digital signature, HTTPS, CA have been implemented to support trusted communications between trusted parties. However, such technologies cannot be printed and cannot connect to many real businesses. Physical mailing is still the dominant way to deliver documents.

On the other hand, whenever there is a need to deliver a huge amount of digital data between two or multiple parties, like a game, operating system, or movie, data integrity in the transfer process often cannot be guaranteed. Also, it requires a very stable connection for a long time between senders and receivers or between a huge server and receivers. It highly increases the difficulty to deliver digital data across network. Hence in many cases, people will simply copy the data into a storage medium like DVD, USB Drive, or a hard disk, and mail it to the recipient.

In this section, the background and pain points in these two markets will be discussed so that readers will understand the need of Authpaper Delivery platform.

3.1 Document Forgery and Certifications

Since the existence of document and certificate, there is a need to verify issuer of the document. The most common way is signing the document at the end or on every page of the document. Signature is also a legal requirement on accepting a document on court. To disprove a document, or prove a document is fraud, the most common method is to perform a signature analysis to prove the signature is not from the claimed person. However, it is often hard to tell if a signature is really from a person, especially for simple and sloppy signature. Asking the issuer to verify a document may not be useful as the issuer may have incentive to deny signing a document (like contract) or is not available (like last will).

Background

The biggest problem is, it is hard for third party to judge if a person has signed a document which he would like to deny.

To provide an additional layer of protection, stamping is often added on official and legal documents. Stamping plus signature is a common measure for lawyers to certify a document copy. Wax seal is often used for cross border legal documents.

The problem is that with current technology, it is very easy to forge a stamp or wax seal to stamp documents. The document recipients often do not know the correct stamp, meaning they cannot distinguish the real and false documents.

Another problem is that both signature and stamp are not bind to a document, meaning a bad person can simply copy the signature and stamp of a person to arbitrary documents and create a perfect false document.

Fingerprint is needed when signing a government related document in countries like China. However, like stamping, it is easy to forge and copy to other documents.
Some documents are printed on materials with anti-forgery protections, like passport and identity card to prevent forging. This greatly increase the cost of forging, but it is not cost-effective and only a few parties when special knowledge can judge if a document is real or forged.

As signature and stamp are too easy to forge, in many places important documents like last will and real estate purchase agreements will require one or more witnesses signature. When there is any doubt, the witnesses will be called to testify the authenticity of a document. This often requires a lengthy trial process.

Background

When judging a document is true or not, supporting evidences usually provide a great help. For example, one can summit mailing record from post offices and courier company as evidence to prove a document is really delivered to a party in Hong Kong according to the Evidence Ordinance. In China, a photo is required whenever signing a document in government agencies, banks and hotels for record and proving the identity of the signer.

The common practice is that a document is accepted unless there is a disproof. Companies and organizations have to bare the risk of accepting a false document to run their businesses. Every year, billions USD are lost due to forge documents.

As all common protections or certifications on documents work only on physical documents, important documents, especially commercial and legal documents, are often delivered via physical mailing or courier delivery.

The mailing business is huge. For example, Hong Kong Post delivers over 3.28M commercial documents every day inside Hong Kong in 2017. The delivery fee is around 2 to 32 Hong Kong dollars (HKD) per mail, it means in Hong Kong alone the market size is at least HKD 6.56 million per day. SF Express (顺丰), one of the largest delivery service providers in great China region, worth around 190 billion Renminbi (RMB). UPS, an international delivery service provider, worth around 110 billion US dollars (USD).

Companies nowadays deliver documents via electronic medium, like email. However, in electronic world all well established protection methods are lost. People argue that document electronic copies can be modified and cannot prove the source of document. There are technologies making sure a document is not modified and is from the expected party, like S/MIME and digital signature. However, the adoption is still very low. Hence even email and instant messengers becomes dominant in communications, only physically mailed documents are considered as official.

Companies like Google, Apple and Amazon have given up mailing documents physical to their customers / business partners. All documents are delivered via emails or stored inside their own database. To prove this kind of documents valid on court, they need to provide the email delivery record from the email provider or well prove that the record in database is not modified intentionally. In most cases a third-party witness (usually the email service provider) is required and the documents are considered as supporting evidence of the witness only.

Companies like DocuSign and Adobe provide document electronic signing solutions. When someone wants to send out a document for signature, they need to upload the file to the platform and let the platform contact the recipient for signature, and then send back the signed copy to the sender. The solution provider works as a third-party witness to the document signing and the document flow, from uploading the document, to signing by the recipient, is properly recorded as a supporting evidence that a party has signed a document. Forrester has estimated in 2017 the market of electronic document signing is

Background

over 0.5 billion US dollars in USA alone and DocuSign has obtained 75% of it.

A major drawback of this solution is that all documents involved are kept in the database of the platform provider in plaintext forever. It is necessary to keep a copy as the platform is a witness. But any loopholes in the system will put all client documents at risk. Documents that need to be confidential cannot use this platform.

3.2 Huge Digital Data Delivery

Delivering a huge amount of data from one party to another is an underrated problem. Common communication channels like WhatsApp, email, skype have size limit on attachments mainly for security purpose and reduce server loading. For example, in outlook each attachment in an email is limited by 10MB. Skype cannot send file larger than 300MB.

When there is a need to send big files like 4K movie and photo album from studio, and game from a game company. People often setup a server or NAS or cloud storage like Dropbox, upload the file to the server and let the recipient download it from there. If the recipient decides to download it via web interface, it will be almost fail for sure as it is very hard to keep a stable connection long enough (hours) to download the whole data from the server. Any short disruption (minute) on the connection will fail the whole download process (over an hour). The speed of downloading speed is limited by uncontrollable factors like server bandwidth, network congestion, and storage medium. So, it normally only works for files less than 4GB.

To address this problem, there are programs like FlashGet which can split downloaded files into sections and supports resuming download after connection disruption. Cloud storages like Dropbox, Google Drive and OneDrive also have desktop client to synchronize data from the server. The download speed is greatly increased, but it is still limited by the storage server.

When it comes to huge data, like system image from software vendor, database backup from hosting company, and hard disk image from a PC for forensic investigations, the centralized solution simply cannot work. It is because the data is too huge for the server storage and the overall transmission time is too long (from local to cloud server, cloud server complete processing and ready for share and from server to destination).

If the data is confidential, the centralized solution also does not work as the server will have a copy of the data.

In these situation, peer-to-peer connection is needed. If two machines are under same intranet, the sender machine can create a network drive for destination machine access and copy the data. FileZilla allows people to setup a temporary FTP server on the sender machine and let the destination machine to connect to it and download the data. In this case both machine must be online at the same time throughout the transmission process and no pausing is allowed. The limitations make these methods not feasible in many

Background

cases.

Another problem is on the file integrity checking. For huge files it is likely that some of the bits inside the file is changed during the transmission. There are error corrections like CRC on the communication level, but it may not be sufficient to fix all errors, especially when the error comes from connection disruptions. An extra file integrity check must be done on both sender and recipient side after sending the file to make sure not a single bit of the file is changed.

Surprisingly, the most common way to send a huge and confidential file between two parties is by physical mailing. Sender copies the file and its integrity checking information to an external storage, like DVD, USB Drive, or a hard disk. The storage medium will then mail to the destination. The destination can verify the integrity using the integrity information. This make sure the data is delivered confidentially, both sides do not need to online at the same time for transmission, and data integrity is conserved. However, it takes a long delivery time and sounds foolish to us under this digital age.

Filecoin, one of the largest ICO projects in 2017, provide a decentralized data storage solution. It allows users to share data with confidentiality and integrity. However, it is still under development and does not keep a record of data delivery.

In both huge data delivery and commercial document delivery, physical mailing is still a common practice and seems to be the best. Authpaper would like to provide the same advantages of physical mailing without the disadvantage of long mailing time.

In summary, Authpaper Delivery platform is an electronic delivery platform for clients to send confidential data to others with the following properties:

1) *The delivered data is confidential that only the expected party can read.*
2) *The platform will keep all delivery record which is enough as a supporting witness to prove a data is (or is not) delivered to the expected party.*
3) *The delivery record should be public accessible so that all third parties can view and verify it without the confidential data. If a party has access to the confidential data, they can easily verify the delivery record is connected to the confidential data they own and the data is not changed since delivery.*
4) *Unless the data necessary, like time of delivery, identifier of the data, recipient email address, no privacy data should be kept on the platform unless it is for public.*
5) *The platform is completely decentralized so that no single party can control how the data is treated and edit any record on the platform.*
6) *There are economical reasons for the nodes on the platform to keep and deliver the data to the recipient, and after delivery remove the data.*
7) *Client can send a data to the platform for certification. The certified document will be available to the public with supporting evidence of the source and upload time of the document.*
8) *Client can also send a data to the platform for recipients' signature. In addition to the delivery record, document signature record is also kept on the platform.*

Background

9) *There should not be hard limit on the size and type of the data delivered (except the hardware limit like hard disk size), and even nodes with insufficient storage can also contribute the platform / data delivery of data and get reward.*

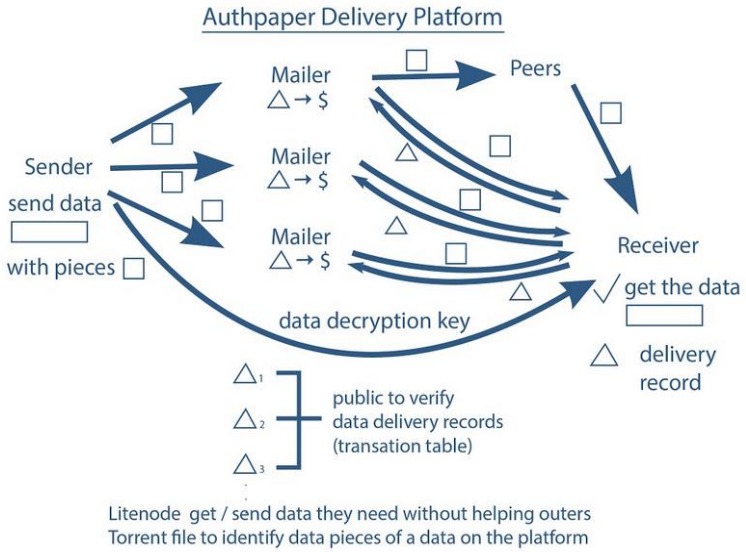
Authpaper Delivery Solution

4. Authpaper Delivery Solution

Authpaper delivery platform provides a decentralized system allowing users to send data between one another confidentially. To make sure only the recipient can read the data, it is encrypted by two encryption keys before sending out. Two encryption keys will be delivered via a trusted channel other than email to make sure only the recipient can decrypt the data. The data delivery is done via BT protocol (with Mainline DHT and magnet link support) so that users can send a large amount of data (>10TB) effectively without incurring the dramatic costs for bandwidth inherent. Senders do not need to keep online when recipients are getting the data.

In addition, peers get rewards (stamps) by helping to deliver the data to the recipient. They do not need to keep a full data copy to contribute the delivery and get reward. This reward mechanism economically encourages users to join the platform and seed the data they cannot access, hence further increase data delivery speed. This is implemented based on a custom built blockchain to make sure it is completely decentralized, and no one can control the platform.

In this section, the details and advantages of the system will be discussed with typical workflows. The discussion will be started from some background knowledge.



Authpaper Delivery Solution

4.1 Background Information

Symmetric and Asymmetric Encryption

Confidentiality serves the purpose that information is not revealed to unauthorized entities. Confidentiality is accomplished by transforming the information to a state that is no different from random garbage data except by authorized entities. This transformation mechanism is called encryption. To read back the data, entities use some private information (keys) to convert random garbage data (encrypted data) back to its original state. This is called decryption.

There are mainly two kinds of algorithms providing encryption, symmetric and asymmetric algorithms. Symmetric-key algorithms also referred as secret-key algorithms which use a single cryptographic key for encryption and decryption purposes. They convert data in a way that is problematic for an opponent to decrypt the data without the key. Symmetric keys are securely generated and distributed to the sender and receiver and are unknown to any other entity. But if a symmetric-key algorithm is being used by more than one receiver then the key must be shared with all entities. If the key is compromised from one entity, communication of all the entities will be compromised.

Asymmetric-key algorithms are commonly referred to as “public-key algorithms” because there are two mathematically associated keys knows as public and private keys involved. The combination of a public and private key is called a key pair. The private key is always kept secret by the owner. The public key is distributed to the public and everyone can access it. The private key cannot be deduced from the public key. The public key is used to encrypt the data in a way that only the party with private key can decrypt it. When a party would like to send a data to another party, he gets the public key from the recipient and encrypt the data. As private key is known by the recipient only, so only recipient can read the data. Unlike symmetric key algorithms, asymmetric-key algorithms allow multiple parties to send encrypted data to the same recipient using the same key pair. Compromising any entity does not compromise the communications of other entities. However, symmetric algorithms are still often used in data encryption as they are much faster. Asymmetric-key algorithms are often used in key exchange and digital signature.

There are a lot of symmetric and asymmetric algorithms. Public and US National Institute of Standards and Technology (NIST) have undergone rigorous security testing and cryptanalysis prior to their approval on an algorithm, to assure that the algorithm provides satisfactory security. In Authpaper Delivery platform, we will use Advanced Encryption Standard with 256-bit keys for symmetric encryption (AES 256) and Elliptic-curve cryptography with 521-bit keys for digital signature and key exchange (ECDSA and ECDH). Both algorithms are recommended by NIST for use beyond 2030, even quantum computing is present.

Authpaper Delivery Solution

Digital Signature

Digital signature is a process that guarantees that the contents of a message have not been altered in transit. A valid digital signature gives a recipient reason to believe that the message was created by a known sender (authentication), that the sender cannot deny having sent the message (non-repudiation), and that the message was not altered in transit (integrity). Digital signatures employ asymmetric cryptography and hash functions. In many cases, a digital signature is a legally accepted alternative to a handwritten signature or official seal certifying the authenticity of the signature, but digital signatures are much more difficult to forge than the handwritten type.

A digital signature scheme typically consists of 3 algorithms, key generation, signing algorithm and signature verifying algorithm. To bind public keys with respective identities of entities (like people and organizations), an arrangement called public key infrastructure (PKI) is established. Under the PKI design, the identity binding is established through a process of registration and issuance of certificates at and by a certificate authority (CA).

In Authpaper Delivery platform, we will use ECDSA and SHA-2 to implement the digital signature. Users can apply a certificate from CA under the current PKI arrangement for the key they use and post it on the platform. But it is not necessary.

BitTorrent, DHT and Magnet Links

BitTorrent is a protocol for distributing data and electronic files between peers. Its advantage over plain HTTP is that when multiple downloads of the same file happen concurrently, the downloaders upload to each other, making it possible for the file source to support very large numbers of downloaders with only a modest increase in its load. BitTorrent is one of the most common protocols for transferring large files, such as digital video files containing TV shows or video clips or digital audio files containing songs. According to Palo Alto Networks, BitTorrent was responsible for 3.35% of all worldwide bandwidth, more than half of the 6% of total bandwidth dedicated to file sharing as of February 2013.

The protocol is designed and released in 2001. As of 2013, BitTorrent has 15–27 million concurrent users at any time.

The BitTorrent protocol can be used to reduce the server and network impact of distributing large files. Rather than downloading a file from a single source server, the BitTorrent protocol allows users to join a "swarm" of hosts to upload to/download from each other simultaneously. The protocol is an alternative to the older single source,

Authpaper Delivery Solution

multiple mirror sources technique for distributing data, and can work effectively over networks with lower bandwidth. A user who wants to upload a file first creates a small torrent descriptor file that they distribute by conventional means (web, email, etc.). They then make the file itself available through a BitTorrent node acting as a seed. Those with the torrent descriptor file can give it to their own BitTorrent nodes, or peers, to download it by connecting to the seed and/or other peers. The file being distributed is divided into segments called pieces. As each peer receives a new piece of the file, it becomes a source (of that piece) for other peers, relieving the original seed from having to send that piece to every computer or user wishing a copy. With BitTorrent, the task of distributing the file is shared by those who want it; it is entirely possible for the seed to send only a single copy of the file itself and eventually distribute to an unlimited number of peers. Each piece is protected by a cryptographic hash contained in the torrent descriptor. This ensures that any modification of the piece can be reliably detected, and thus prevents both accidental and malicious modifications of any of the pieces received at other nodes. If a node starts with an authentic copy of the torrent descriptor, it can verify the authenticity of the entire file it receives. Distributed downloading protocols in general provide redundancy against system problems, reduce dependence on the original distributor.

In the original design of BitTorrent, every torrent file must include a tracker server information so that new coming nodes can get current peer list from the tracker server. Tracker servers also help coordinating efficient transmission and reassembly of the copied file. However, if the tracker server is down, the torrent will soon die. Since the creation of the distributed hash table (DHT) method for "Trackerless" torrents, BitTorrent trackers have largely become redundant. However, they are still often included with torrents to improve the speed of peer discovery.

DHT, or distributed hash table, is a class of a decentralized distributed system that provides a lookup service similar to a hash table: (key, value) pairs are stored in a DHT, and any participating node can efficiently retrieve the value associated with a given key. Responsibility for maintaining the mapping from keys to values is distributed among the nodes, in such a way that a change in the set of participants causes a minimal amount of disruption. This allows a DHT to scale to extremely large numbers of nodes and to handle continual node arrivals, departures, and failures.

Using “Trackerless” torrents, new coming peers connect to a list of DHT nodes. After it's got one node, new peers can use the DHT Network to find other nodes (until it updates/seeds its routing table). From the DHT network, new coming peers can retrieve the peer list of the “Trackerless” torrent file, using the info-hash values of the torrents for queries. As opposed to this, in the conventional tracker approach, new peers need to communicate with the tracker to learn about each additional peer added.

In the original design, a torrent file is necessary in order to join the swarm and start

Authpaper Delivery Solution

connecting to the peers for a file. Magnet links take a step further, containing only the info-hash value already calculated for a specific torrent file. With the magnet link, new coming peers can query the DHT network to get the peer list for a torrent file, download the torrent file from one of them, and start the BT process.

In Authpaper delivery platform, all data is delivered using BT protocol. Recipients and helping peers only need a magnet link to download the data. As all data is encrypted before sending out, seeds and peers cannot read the data, hence do not want to contribute to the data delivery process. An economic incentive is needed to make them contribute the data delivery process. Hence a custom cryptocurrency is needed to provide rewards to them.

Blockchain and Cryptocurrency

Cryptocurrency is a digital token that uses encryption (cryptography) to generate money and to verify transactions. As of 2017, cryptocurrency has been used as a decentralized alternative to traditional fiat currencies (which are usually backed by some central government) such as the US dollar (USD). Modern digital currency starts in 2008 when Satoshi Nakamoto released their paper detailing what would become Bitcoin. Bitcoin became the first decentralized digital coin when it was created in 2008. It then went public in 2009.

In decentralized digital coins, a method is needed for peers to reach consensus on a growing list of transaction records, also known as blocks, without any help of centralized authority. Satoshi Nakamoto invented blockchain to serve as the public transaction ledger of Bitcoin. The invention of the blockchain for bitcoin made it the first digital currency which solves the double-spending problem without the need of a trusted authority or central server. The most beautiful part of Bitcoin is that no one in the network has control on the currency (unless under 51% attack) and all transactions recorded on Blockchain are public verifiable and cannot be modified by any single party. Many applications have been developed based on Blockchain and Bitcoin since then.

After the invention of Bitcoin, many alternative cryptocurrencies, or altcoins, have been developed. As of January 2015, there were over 500 different types of cryptocurrencies – or altcoins – for trade in online markets. However, only 10 of them had market capitalizations over $10 million. As of September 2017, there were over 1,100 cryptocurrencies and the total market capitalization of all cryptocurrencies reached an all-time high surpassing $60 billion! Then, by December 2017, the total market cap reached $600 billion (a multiple of 10 in only two months).

In Authpaper delivery platform, a new cryptocurrency will be created so that peers can

Authpaper Delivery Solution

get rewards from contributing to the network. Blockchain and BT protocol will also be integrated into a unified decentralized network.

Authpaper Delivery Solution

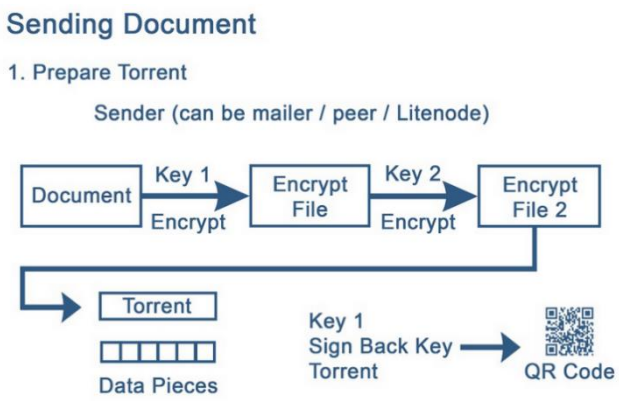
4.2 System Overview

Authpaper delivery platform is a BT-based decentralized data delivery platform using Blockchain based cryptocurrency (stamps) to pay the delivery and provide rewards to the nodes. In this platform, each peer serves as both peer in the DHT network (for BT) and node in the Blockchain network. There is no server in the platform. When a new peer joins the network, it creates a new public key pair (crypto-wallet) and connects to a list of known peers to join the DHT network. Each peer needs to submit their network IP, wallet address (public key of the crypto-wallet), and an email address to the DHT network. The peer's client software also need to access the peer's email account (reading and sending). Then it is ready to use the service. There are mainly two kinds of flow inside the platform, encrypted files and stamps. All operations on encrypted files were done through the DHT and BT protocols, while those on stamps are done via blockchain. Data delivery will involve an interaction between these two networks. A typical workflow is discussed in the following as illustrations.

Data Delivery Workflow

To send out a data from a peer A (Alice) to another peer B (Bob), multiple steps are needed to be done by Alice, Bob and client software of other nodes. Unless specified, all operations are done inside the client software of the peer and do not need human interactions and all communications are encrypted.

Before sending out anything, Alice first encrypts the data she would like to send using symmetric encryptions two times with two different encryption keys (key 1 and key 2 respectively). Key 1 will be sent to Bob so that only he can read the data. Key 2 will be held by other peers so that Bob must provide enough evidence to the peers to redeem stamps before decrypting the file. After that Alice creates a torrent file and a magnet link on the encrypted data and divides the data into pieces. Torrent file allows the peers to share the encrypted file and allows Bob to check the integrity of the data delivered. Key 1, magnet link and a sign back key are packaged in QR code. Sign back key is a newly generated key pair for ECDSA operations.

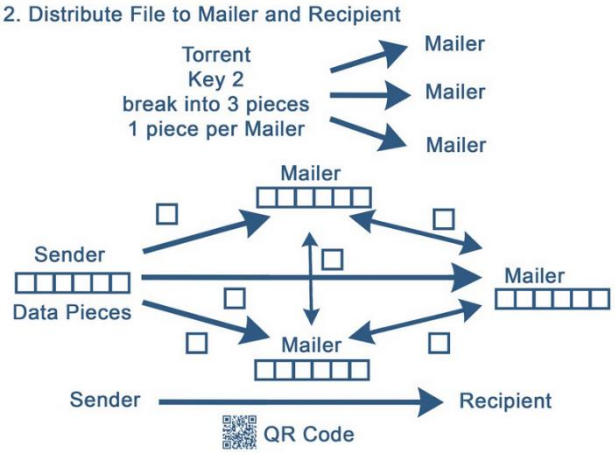


Authpaper Delivery Solution

After that, Alice broadcasts a request for Mailer to the peers. Some peers respond, and Alice randomly selects some of them (3 by default, at least 2) as mailers and signs a smart contract with them. Smart contract indicates when a data is delivered using a torrent file, and a delivery record signed by the sign back private key on that data is available on Blockchain, Alice will pay a certain number of stamps to each mailer. The torrent file and magnet link are attached with the smart contract. There is an expire time on the smart contract, 50% of the deposit will be paid to mailers and 50% will be returned to Alice when contract is expired. Every node other than Alice and Lite nodes can apply for mailer.

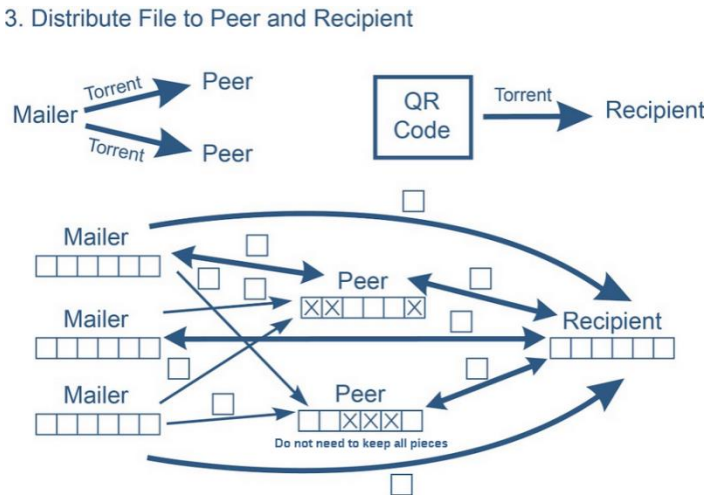
Alice then breaks the key 2 into pieces using Shamir's Secret Sharing algorithm with k=2, meaning getting any 2 pieces can recover the key 2. Each mailer will receive a different piece of key 2 and the torrent file.

Alice seeds the encrypted file with initial seeding mode until all mailers become a seed. During that time Alice sends the QR code to Bob manually via a way the legitimate Bob can receive. With the magnet link in the QR code, Bob can manually join the swarm and download the file. When all mailers become a seed, Alice can disconnect the swarm or stay as a normal seed.



Mailers distribute the magnet links to other peers and invite them to join the swarm to increase the file sharing speed. Joining peers can decide how much percentage they would like to download to save their own disk space, the default is 100%.

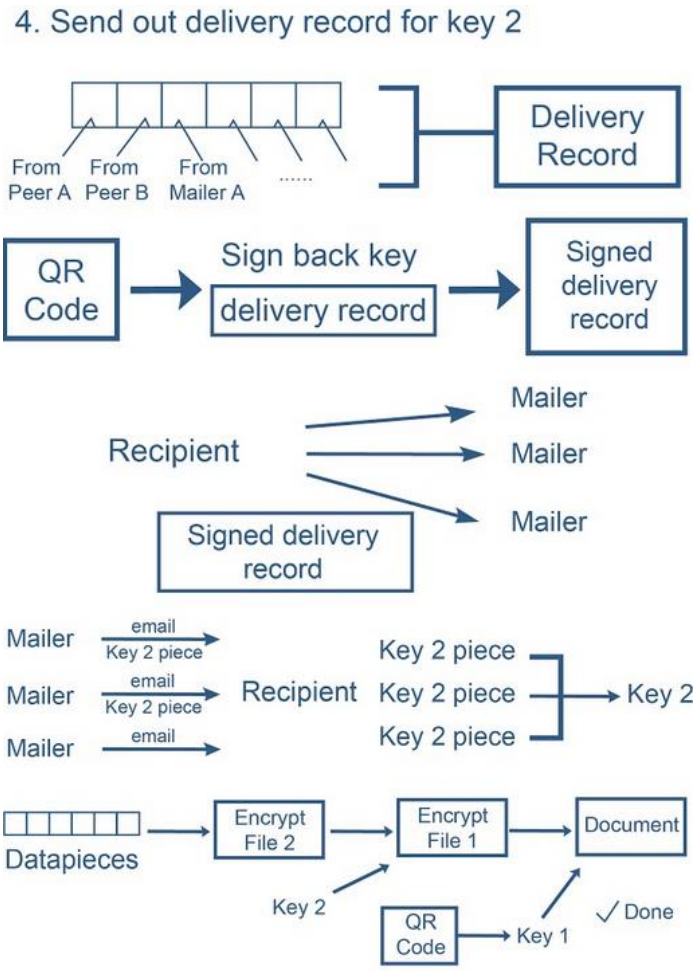
Authpaper Delivery Solution



Bob keeps track of the source of each piece, which forms a delivery record. When Bob finishes downloading the file, he signs the delivery record by the sign back key from the QR code and send the record to all seeds (including the mailers).

Receiving the signed record, mailers send the piece of key 2 they keep to Bob via email. Sending key 2 pieces via email is a kind of multi-factor authentications, making sure only legitimate Bob can decrypt the data (have key 1 directly from Alice, have key 2 via the specified email). With at least two pieces of key 2, Bob generates back the key 2, and decrypt the downloaded data by key 1 and key 2. Hence the original file is obtained. The data is delivered.

Authpaper Delivery Solution

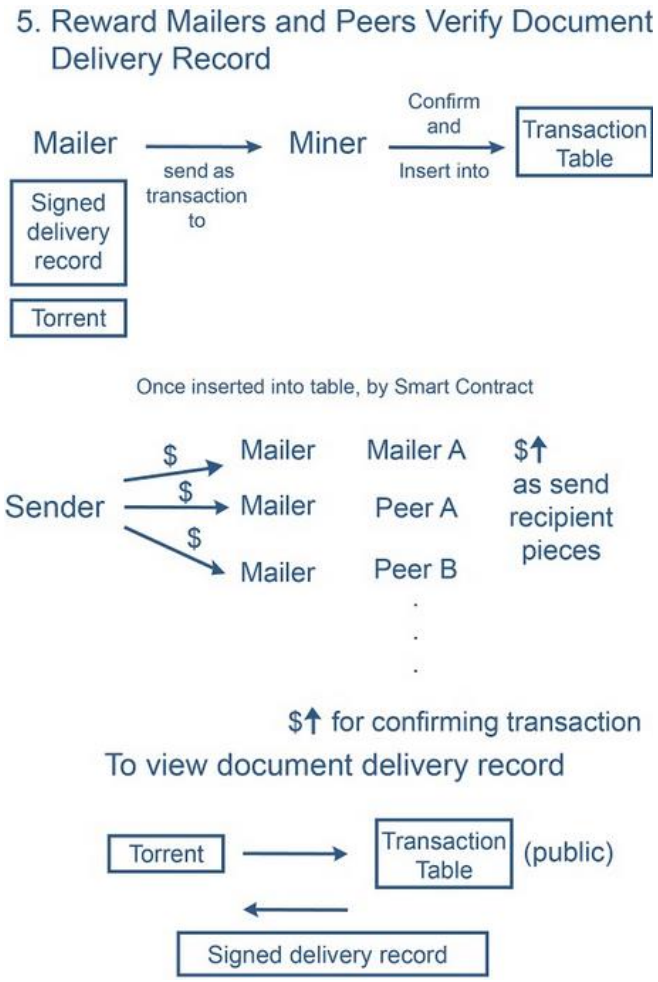


On the other hand, mailers receive the signed delivery record and send them out with the torrent file and magnet link to Blockchain. Miners confirm the delivery record is signed by the sign back key and execute the smart contract, i.e. giving stamps to the mailers. According to the number of data pieces a peer has given to Bob, new stamps are created to reward the peer. Miner will also receive the transaction gas (in stamps). If a contract is expired, only mailers will receive 50% fee from Alice and no new stamps will be created to reward peers.

After delivery, mailers and peers will leave the swarm and delete the encrypted data.

During or after delivery, when someone would like to check the delivery record, they can query it from blockchain using the corresponding torrent file / magnet link. Failed delivery will also be kept on blockchain. The blockchain stores the delivery smart contract, contract result and signed delivery record for each torrent. This provides an evidence that a data is sent / attempted to sent from a party to another and whether the data is received by the recipient.

Authpaper Delivery Solution



Peers, Lite Nodes, Miners and Mailers

In Authpaper Delivery, all joining nodes have access to both DHT network and blockchain. We call such basic node to be a peer. Sometimes a party does not want to join the network for a long time, they only want to download a specific file and leave the network. In this case they can join as a Lite Node. A lite node does not have a crypto-wallet account. It joins the DHT network only and download the torrent and hence data using a magnet link. Once download is completed, it will send messages to mailers for key 2, waiting for their emails, and decrypt the data. Once the data delivery is completed, the lite node will stop its work. Downloading another data will need to start as another lite node.

Miners, on the other hand, only joins the blockchain. They do not care about anything inside the DHT network and data transferring between peers. They are equivalent to a miner in blockchain network. However, mining in Authpaper delivery platform is different

Authpaper Delivery Solution

from the mining in Ethereum or any smart contract supporting cryptocurrency. In Authpaper delivery platform, each smart contract has more than program codes, it also has attachments (torrent file / magnet link) and peers involved in the contract can add attachments to it (mailer adding delivery record). Whenever new attachment is added to a smart contract, the smart contract will be evaluated again and see if it should be executed. The consensus process is PoW at the first stage. Migration to PoS is under study.

Mailers, the most important peers in the data delivery process, is no more than a peer which signed contract with data sender and able to send email to the data recipient. Different files may have different mailers. Mailers can gain stamps from two sources, sender according to the contract and network according to number of data sent to recipient. On the other hand, it must be always online during most of the delivery process and send out key 2 piece whenever receiving a signed delivery record, otherwise the data cannot be delivered.

As data recipient himself may be selected as one of the mailers, the key 2 is divided into pieces so that each mailer cannot have the whole key 2. To avoid individual misbehaving mailers, multiple mailers are needed and key 2 can be recovered whenever 2 of the mailers succeed to send recipient the key 2 piece.

Reasons to Work Legitimately and Stamp Supply

In the design of Authpaper Delivery platform, rewards are provided so that peers are always better to act legitimately from the economical perspective. This is also the main new supply of the stamp of the system.

In the delivery process, data sender will pay stamp to enjoy the service. Even the delivery failed, half of the fee will also be paid to make sure mailers are guaranteed to get paid. They will be always online to upload data pieces to the recipient for extra rewards and wait for the delivery record for full mailing fee from sender. Peers are willing to join the swarm as they can get rewards by uploading data to the recipient. The recipient is not known until the signed delivery record is sent out. Peers and mailers will share their data pieces to others as much as possible to increase the chance of getting rewards. This increases the download rate and data availability of the recipient, shorten the delivery time.

Rewards of uploading data to the recipient is the only source of the new stamp supply. Hence the inflation of the stamp supply is directly proportional to the data transferred inside Authpaper delivery platform. It is better than setting a hard value because supply of a coin is adjusted automatically according to the coin usage.

Authpaper Delivery Solution

Mining receive transaction gases as reward and there is no block reward. The block time is 10 seconds using ethash algorithm. The block gas limit follows the Ethereum voting mechanism, starting from 0.08 stamp.

Authpaper Delivery Solution

Other Workflows
This platform works more than only data delivery. With small changes on the smart contract, this platform allows other data, especially document related, workflows. This platform also allows senders to set their own workflow with the smart contract. In this section, some other default workflows are discussed.

Data Certifications
When a user, say Alice, would like to create a certificate or provide a public proof on the ownership of a digital data. She can provide a certification on the data on this platform. She does not need to encrypt the data by key 1 but still encrypt the data by key 2. And there is still sign back key. The smart contract between Alice and mailers will involve a payment to the mailers and a validation period. The payment will be sent out after the validation period. Mailers do their job as before. Whenever someone (Bob) would like to get a copy of the data, he can get a QR code containing the magnet link and sign back key from Alice, download the data from the platform, and send out the signed delivery record for key 2. Every time a signed delivery record is uploaded, the peers and mailers uploading the data will still get reward like before.

When someone with the data, say Charlie, would like to check if it is certified by Alice. He first gets the QR code from Alice, download the torrent file from the platform, and send out a special signed record which no one can get upload data reward. Once he gets the key 2, he encrypt the data with key 2 and compare the result with the hashes stored in torrent file. This can prove if the data is same as the data indicated in the torrent file. The blockchain contains the delivery and certification history and smart contract of the torrent file, giving a valid timestamp of Alice certifying this data and the data ownership. In addition, only the parties with QR code can read the data.

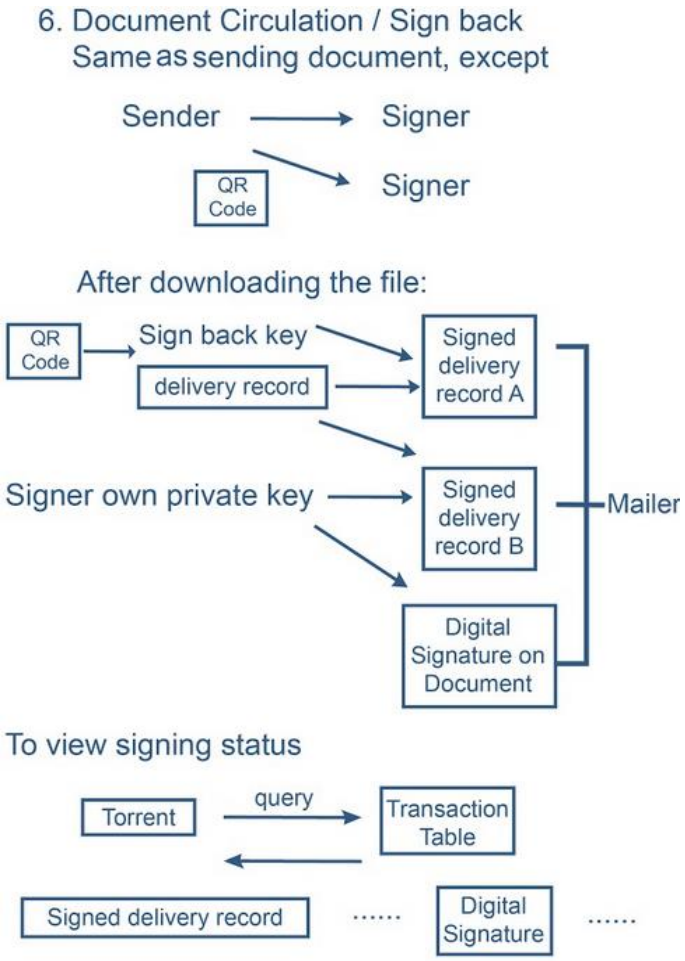
Any time before the validation period is over, Alice can decide whether to pay more to extend the validation period or ends the validation. No matter which she chooses, Alice provides a random string to mailers to create another BT torrent with the random string attended before the data and without any DHT or peer information. If a mailer fails to do it, or the result is different from others (Alice and other mailers), the payment to that mailer will be canceled. If the validation is over without modifications, the payment will be made without further action.

Support on Document Physical Copies
If the data going to be certified is a document, and the document is supposed to be printed, sender can decide to print the document with the QR code attached at the end of the document. Anyone would like to certify the document physical copy just scans the QR code, download the document, and compare the digital copy (certified copy) with the physical copy. An even better way is to just send out the QR code without the document.

Authpaper Delivery Solution

Data Circulations

In business world, a digital data often needs approval from multiple parties before further process, especially reports and official announcements. This is called circulations. When a sender, say Alice again, would like to circulate a data, she first encrypts the data with key 1 and key 2, and sign a smart contract with mailers. The smart contract contains public keys of the peers Alice wish to get approval from. After the normal delivery process, when a signing peer, say Bob, would like to sign a data, he sends out the delivery record again which is signed by his wallet private key instead of the sign back key. Mailers publish the signed delivery record and get paid from smart contract as usual, but the data uploaders cannot get rewards again as doing so will be a double payment. Public, especially Alice, can check the data delivery and circulation status by querying the blockchain with the torrent file.



Hugh Data Delivery

By default, the file is divided into 4KB pieces in BT. When the data is very high, like above 4GB, the torrent file will become very high. In this platform, the senders are advised to

Authpaper Delivery Solution

increase the size of the data pieces to keep the number of pieces to be smaller than 131,072 (1024*128) to reduce the processing time. For example, when the data is 1TB, the data piece size will be 8MB. To further utilizes the network benefit of this platform, sender can also divide a very large file (likely over 1TB) into multiple parts, each part to be sent out like individual files. And then sends the combination of the torrent files to the recipient via the platform. When Bob receives the set of torrents, he will automatically start downloading data from each of the file and combine them together afterwards. The delivery record of the torrents and each data part will form a delivery record to the large data.

Delivering Data for Multiple Times and Recipients

When a data is supposed to deliver across multiple parties, the whole operation is the same, only the smart contract is set to deliver the data multiple times and the QR code is sent to multiple people by the sender. The delivery fee from Alice is proportional to the number of delivery and is paid when the last delivery is done, or the smart contract is expired. The data upload reward is provided every time a signed delivery record is sent out.

Advantages of Authpaper Delivery Platform

This platform is the only platform which allows users to deliver a digital data with confidentiality, integrity checking (using torrent file), availability, unchangeable yet public verifiable delivery record, and non-deniable when signing a data. Current solutions require the data to be known by the delivery or mailed physically.

Besides, this platform also allows users to prove he or she owns a data at a certain time and deliver digital copyright content with trace to find out the source, when it is leaked. Next section will discuss these applications further.

A Better System for the World

5. A Better System for the World

5.1 Potential Applications

This platform provides a lot of impacts across multiple industries. In this section, some of the business impacts are highlighted.

5.1.1 Commercial

There are a lot of documents delivered and circulated every day in the commercial world. In 2017, there are over 3 million business mails delivered every day in Hong Kong. With this platform, all physical printing and mailing of documents are saved. Companies also do not need to find spaces to keep the documents they receive or send, as they are not printed in the first place. No matter a document is circulated internally or externally, it can be circulated inside this platform instead of printing out and mailing around for confirmations.

For software companies and education institutes, they do not need to host their software or certificates for others to download and verify because they can host their files on this platform. Many resources are saved.

5.1.2 Trading

In international trading, a lot of documents are shipped between different parties in every step of the merchant process. Whenever there is a document to mail, people may need to wait up to weeks for the document before moving on the next step, like manufacturing or applying loans from bank. With this platform, the time for mailing is saved because the documents are sent instantly over the Internet and it is confidential with public verifiable record on mailing and document source.

5.1.3 Copyright Data Delivery

Copyright data leaking is a huge problem across the world. The biggest problem is that it cannot trace the source of the leakage, especially the videos and movies. Companies have proposed solution to solve this problem by embedding some special random noises to the video frames for each customer. Hence when a video is leaked, video owners can trace back the source of the video. The biggest problem to this solution is that video owners do not have enough computing resources to compute the video on the fly. If they do not do it on the fly, they do not have enough storage to keep a copy of the modified video for each customer.

With this platform, video owners can create videos with random noise one by one first and send to the platform. Video owners only need to keep the original copy of the video, and the torrent file for each modified copy. When a customer buys a video, video owners

A Better System for the World

just send a torrent file for him / her to download and keep a record. The customer will download a protected video copy so that whenever there is a video leak, video owner can trace it back. On the other hand, video owners do not need to keep multiple copies for each video and do not need huge computational resources to make video when customers request it. A major difference between this solution and a cloud storage / content delivery network is that the content is kept encrypted online and all delivery records are kept on blockchain, acting as a solid evidence about where the data is sent to.

5.1.4 Legal and Compliance

In legal and compliance, there are often needs to send out documents. Unlike other industries, the delivery must keep a signature of the recipient to prove the document is delivered. Even the delivery is not successful, the record of delivery attempts is also needed. It makes normal delivery services and electronic delivery not feasible to solve their needs. With this platform, document sender can send a data with full delivery record, including how the document is delivered, by when and who the data is picked. If the delivery is failed, a record of attempting delivery is recorded on blockchain as smart contract. Hence it fits in the legal and compliance need.

5.1.5 System Maintenance and Investigations

The biggest problem on system maintenance and investigation is that administrations need to create a copy of a system and send to others confidentially. The data size of often too large to be sent over network. It is because current network cannot keep a stable yet high speed connection between two parties for a very long time (hours). Currently companies, especially cloud service providers, create a snapshot on the system, copy the snapshot to an external drive and ship it to customer. With this platform, companies can send the snapshot confidentially online. All data has integrity checking and encrypted. The data is sent via BT protocol, data transfer can be readily continued after connection lost. On the download side, the data is transferred from multiple peers, increasing the data delivery rate.

5.1.6 Law Related to Document Certifications and Delivery

In many legal systems, a document can be certified by a signature, or digital signature with detail evidence showing the digital signature belongs to a party. A document delivery record is accepted if it is signed by a third party with evidence showing how the delivery is done.

In Authpaper delivery platform, when a data is certified, the certification record is kept on blockchain with digital signature on the data owner. The certification record cannot be changed by a single party, providing a solid proof that the document is certified by the data owner. This proof cannot be denied by even the data owner. All data delivered, or

A Better System for the World

failed to deliver, on this platform are recorded on blockchain with details. Hence it provides a solid evidence about a data is delivered or attempted delivery but failed.

Token Utilities and Sales

6. Token Utilities and Sales

To make this platform happens, external resources like funding, test users and marketing partners are necessary. To reward the contributions of others and fund raising, we will create an ERC-20 based coin, Authpaper Coin (AUPC) and distribute to the investors and partners. As Authpaper Delivery platform requires a customized blockchain, the coin cannot be used directly on it. Once the platform is ready, we will provide an offer to exchange the coins with Authpaper stamp, the currency in the platform, at a certain rate. Coin holders can also trade the coins on public exchanges or use it to redeem other services from us. Here is a simple comparison between the coin and the stamp.

	Authpaper Coins (AUPC)	Authpaper Stamp
When it is created	ICO of this project	With the Authpaper delivery platform
Base	Ethereum (ERC-20)	Custom build
How to gain	Contribute to the project Join the Token Sale Buy from public exchanges	Mining / Staking inside the platform Working as Mailers Exchange AUPC to stamps with us
Consensus Algorithm	PoW (ERC-20)	PoW / PoS (Custom built)
Maximum Supply	400 million, all will be mined already during ICO	Unlimited
End of Token	Exchanged to Stamp, consumed by us or our partner companies for services	Always there with Authpaper delivery platform

In this section, the details of Authpaper Coin and Token Sale will be discussed.

Token Utilities and Sales

6.1 Token Utilities

Holding Authpaper coins will be benefitted in different ways.

6.1.1 Services in Authpaper Delivery platform

When the Authpaper Delivery platform is ready, coin owners can exchange the coins to stamps, the currency of the platform. With stamps, one can send a confidential data to others, certify a data, circulate a data among people for approval, and even backing up their own system to other machines via the platform. Authpaper Coin serves as the major source of stamps in the first one to two years of the platform. Holders are early birds to the platform.

If there is a big need on the platform, holders can also sell their coins to parties who find this platform useful and need more stamps.

6.1.2 Services from Authpaper Limited

Authpaper Coin can also be used to redeem services from Authpaper Limited. Authpaper Limited provides customized solutions for companies to issue public verifiable certificates and coupons. Currently the products are integrated inside the clients' systems and not available to the public. But we will release a public version of certificate issuing system and coupon solution during the development of the Authpaper Delivery platform for coin redemptions.

We and our partner companies also provide computer and mobile forensic investigations, security risk assessments, and consultant services, mainly in Hong Kong. Authpaper coins can also be used to redeem discounts for these services. The list of company accepting Authpaper Coin for discount, services they provide, and contact will be listed on the ICO website.

6.1.3 Public Exchanges

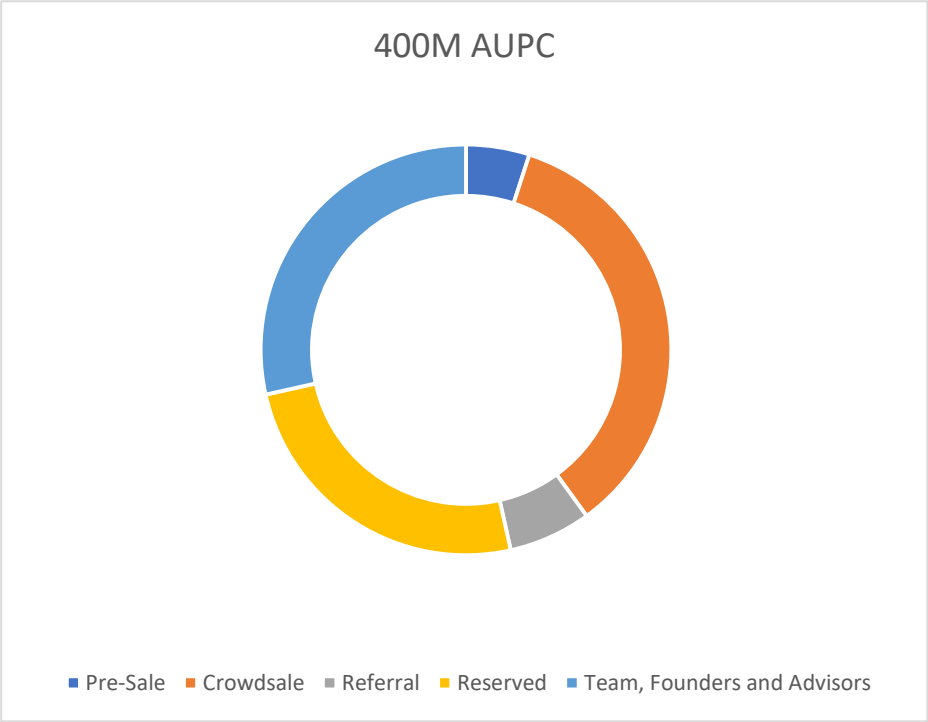
We will discuss with public exchanges to list our coins on their platforms so that our investors can sell the coins when needed. But we would recommend holders to keep the coins and become the first-tier users of the platform.

Token Utilities and Sales

6.2 Token Sale
Authpaper Delivery Platform ICO will be issuing 400 million AUPC, target to raise 41.5M US dollars equivalent of Ethereum, Bitcoin and / or Bitcoin Cash in the first round of sale. Soft cap will be USD 1 million, hard cap will be USD 41.5 million. The price of the coin will be USD 0.1 at first and minimum investment amount will be USD 100 equivalent of cryptocurrency.

Among the 400 million coins,

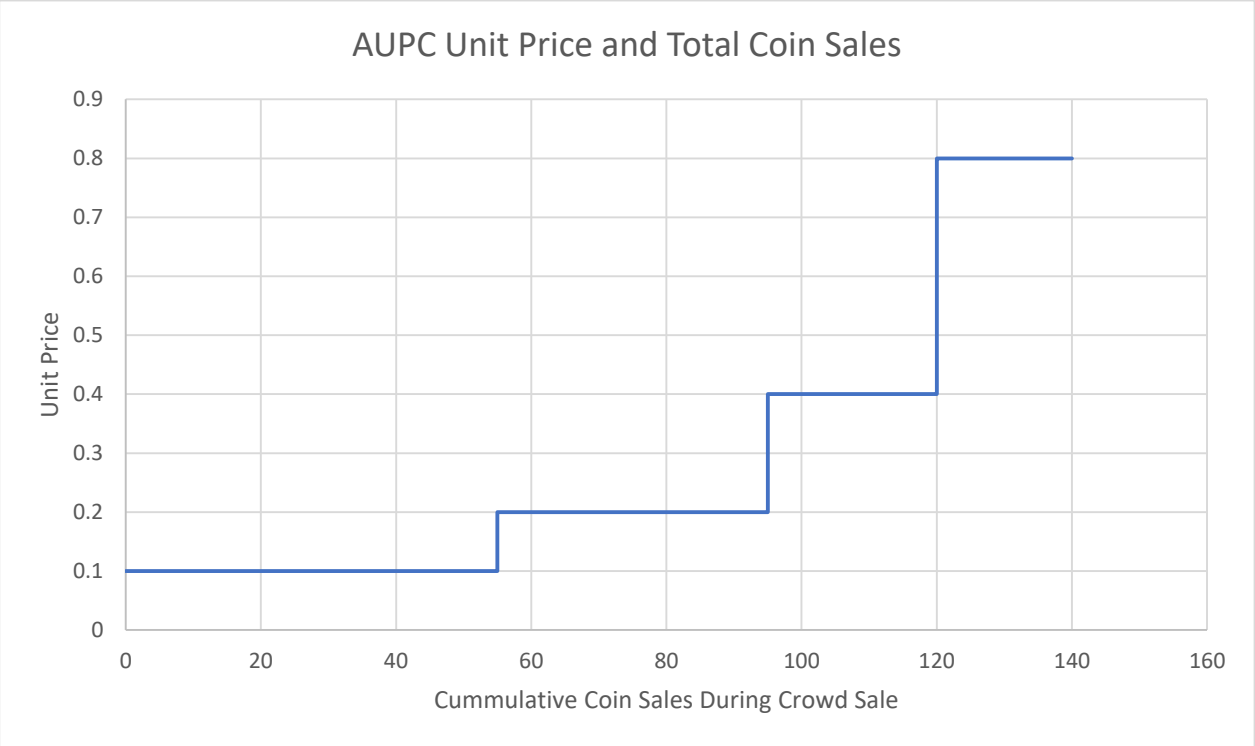
5% will be offered in pre-sales
35% will be offered in crowd sale
25% will be reserved for optional future sale, post-ICO bounty program, marketing and exchange listing fee
6.5% will be reserved for referral
28.5% will be reserved for team, founders, and advisors



Token Utilities and Sales

Coin price
In pre-sales, the coins are sold in 0.05 USD. During the crowd sale, the price will increase according to the coins sold out following a discrete step function. The first 55M AUPC sells in USD 0.1 per coin. Next 40M, USD 0.2. Next 25M, USD 0.4. Next 20M, USD 0.8.

The increasing mechanism reflects the demand of the coin and let more people have a chance to hold AUPC. More holders means more supporters of the platform.



Referral
To provide rewards to those promoting the coins, 6.5% coins are reserved to reward the referrers. When an investor purchases coins, they can provide the address of the referrer. Then the referrer will receive coins 10% of the amount investor has purchased as a referral gift.

Team, Founders, and Advisors
28.5% coins will be provided to team, founders and advisors for their effort to make the project possible. Any potential marketing coin expenses before releasing the platform is also allocated here.

Token Utilities and Sales

Lockup period
To make sure the investors will not be harmed by speculators due to the price fluctuations of AUPC. A lockup period is introduced to everyone holding AUPC (especially the Team and Founders). Only 8*N% of the AUPC an investor bought during the ICO period can be transferred to others before 15th September 2019. N is number of months after 15th September 2018, the ICO launch date. It means for 100 AUPC bought during ICO, only 8% can be traded from 15th September 2018 to 15th October 2018, 16% from 15th October to 15th November, and so on. After 31st September 2019, all AUPC are tradable. AUPC paying for Authpaper services and bought from public exchanges do not have such limitation.

Coins Burning
Within one month after the crowd sale, all coins for pre-sale and crowd sale will be burnt. After the platform is released, all coins in the reserved portion will also be burnt. It is to make sure the team cannot take extra coins.

Difference between Soft Cap and Hard Cap
There is a big difference between Soft Cap and Hard Cap, and it is not usual in an ICO project. The reason behind is that we will use different approaches to implement the platform according to the funding amount we have.

To maximize the data transfer rate, there should be one or two mailers geometrically near the data sender and a lot of peers and at least one mailer near the data recipient. It means that mailers with high speed Internet access and disk I/O speed (multi-TB SSD) are needed around the world. Hence if the funding is allowed (near Hard Cap), we will build or rent small server farms to act as mailers and miners. Two in Asia, two in Europe, one in North America, one in Central or South America, one in Africa and one in Australia.
If the funding raised does not support this, we will rent cloud servers in some regions instead. This saves the cost tremendously, but the platform will need more peers to keep the quality of service. Unlike mailers, peers only need small disk storage to work as they only keep some data pieces to accelerate the data transfer speed.

If the funding is barely above the Soft Cap, we can still implement and release the platform, with only one cloud mailer server and some miners in Hong Kong. Peers and miners from the supporters around the world are needed to make the platform efficient globally. We will use the profit from selling the stamps of the platform to extend the server coverage.

Token Utilities and Sales

6.2 Cost Impact Analysis

Authpaper delivery platform saves a lot of cost across different companies, hence they will find the coin attractive.

Trading and sourcing companies

A lot of documents are exchanged and signed between multiple parties in each sales purchase. Trading and sourcing companies are always flooded by paper documents and keep waiting for document delivery. With Authpaper delivery, days of document mailing and rooms of document archives are saved, especially in the international trades. No matter how far a supplier or merchant is, important documents can be sent, circulated and signed within an hour. There is no need to rent storerooms for keeping the previous signed trading documents as they are electronic from the first place. A lot of papers are also saved.

Education institutes, laboratories, and authorities

Every day, these parties print out many certificates and reports to their clients / students. They also need to answer the enquires from the public to verify the certificate / report they have released before. With Authpaper delivery, they no longer need to answer the calls as people can verify the certificates and reports from them on the delivery platform readily. They also save a lot of paper and mailing cost to deliver the result to their clients or students. Clients and students, on the other hand, do not need to wait for a long time because they can receive the reports electronically and print out themselves. All printed copies can be verified as true copies.

Auditing and legal firms

Paper and mailing usage are intensive in these two industries. It is because for every official and confidential document, it is delivered by a promising method to other parties and there must be a trustworthy record of the delivery, no matter success or not. Authpaper delivery provides a paper-free way to do it and the time of delivery reduces from days to seconds. It also saves a lot of space for paper storage and the firms can package the documents and send together without worry of the mailing fee. The mailing cost of Authpaper delivery will be much lower than courier services.

Software companies

Nowadays software become larger and larger, software developers, especially game developers, start finding even a DVD cannot keep their software and game and send it to customers. Instead of sending multiple copies of DVD or USB drive, software companies can now send the file electronically without the worry of stressing their network. It is because Authpaper delivery platform handles the huge data delivery with confidentiality without stressing the network of any parties.

Token Utilities and Sales

Online video production house
Video and movie are the most pirated data in the world. Video production houses must bear the risk that the video being illegally copied and posed online. Companies have proposed solution to solve this problem by embedding some special random noises to the video frames for each customer. Hence when a video is leaked, video owners can trace back the leaking source. However, this involves a huge online database. When Authpaper Delivery platform, they can host the encoded video on the platform without an expensive online data storage. Huge costs can be saved.

Society
This solution tremendously reduces the cost and resource on printing and mailing documents. A lot of fuels are saved, and a lot of tree are prevented from cutting, this provides an environmental friendly alternative to the activities which are harmful to the environment and we thought we have no choice. Now people can make a choice to save our planet without damaging the businesses.

Project Timeline

7. Project Timeline

Authpaper Delivery Platform So Far
Authpaper Limited is founded in 2016. Since then we have been working on electronic document stamping solutions. When we were aware about Blockchain, we knew for sure it can help on the electronic document delivery and certifications and started studying integration between Blockchain and other technologies to build a data delivery solution. The architectural design has been completed and we decided to kick start ICO for fund raising to make it come true.

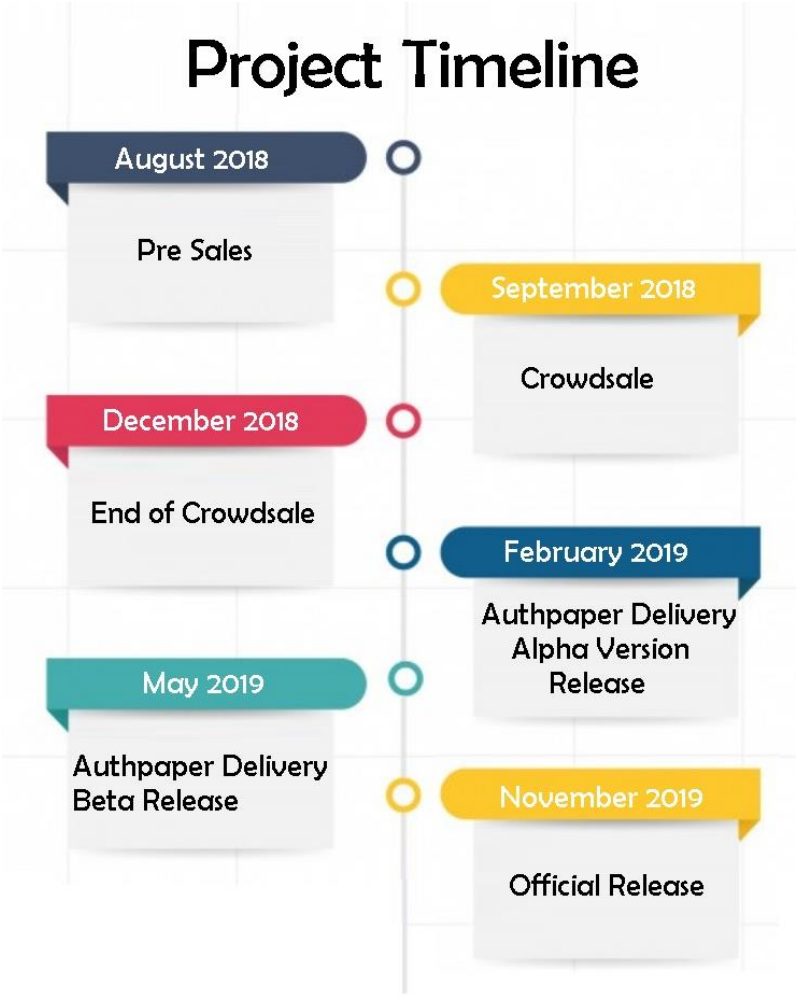
Current Developments
A detailed system analysis and security risk evaluation on the system is running to make sure it is secure and able to provide the promised features. A proof of concept is also under development.

Future Schedule
We target to start the ICO in 15th September 2018 and run for three months. At the same time, a proof of concept and API design will also be developed.

The alpha version of the system for internal testing should be available in February 2019. Supporters and early investors of the project can also join the testing and suggest any additional feature enhancements. The public testing version, or beta version, will be available in May 2019, after three months of intensive bug fixing. The mining and mailer program will also be public at that time. New features maybe added between alpha and beta versions. But the feature list will be fixed during beta and official release.

Official release of the system will be available on November 2019. We will also start the coin to stamp conversion with the official release. We will also keep a test net for new features developments.

Project Timeline



Contingency Plan

In case the ICO is not successful, i.e. cannot raise enough money to develop the project (Soft Cap). We will pay back the coins to the supporters. Authpaper Limited will seek extra funding from other channels like venture capital investments in order to continue the project. Such extra round of fund seeking will provide unknown delay to the project, but the delay should not be longer than one year. Extra capital raising after this ICO may be needed during the development and advertising process. In this case extra round of coin selling may be done in the future.

Legal Terms

8. Legal Terms

8.1 General Information

The Authpaper Coin (AUPC) does not have the legal qualification of a security, since it does not give any rights to dividends or interests. The sale of Authpaper Coin is final and non-refundable. Authpaper Coin are not shares and do not give any right to participate to the general meeting of Authpaper Limited. Authpaper Coin shall not be used or purchased for speculative or investment purposes. The purchaser of Authpaper Coin is aware that Hong Kong securities laws, which ensure that investors are sold investments that include all the proper disclosures and are subject to regulatory scrutiny for the investors' protection, are not applicable.

Anyone purchasing Authpaper Coin expressly acknowledges and represents that she/he has carefully reviewed this whitepaper and fully understands the risks, costs and benefits associated with the purchase of Authpaper Coin.

8.2 General Knowledge

The purchaser of Authpaper Coin undertakes that she/he understands and has significant experience of cryptocurrencies, blockchain systems and services, and that she/he fully understands the risks associated with the crowd sale as well as the mechanism related to the use of cryptocurrencies (incl. storage).

Authpaper Limited shall not be responsible for any loss of Authpaper Coin or situations making it impossible to access Authpaper Coin, which may result from any actions or omissions of the user or any person undertaking to acquire Authpaper Coin, as well as in case of hacker attacks.

8.3 Risks

Acquiring Authpaper Coin and storing them involves various risks, in particular the risk that Authpaper Limited may not be able to launch its operations and develop its blockchain and provide the services promised. Therefore, and prior to acquiring Authpaper Coin, any user should carefully consider the risks, costs and benefits of acquiring Authpaper Coin in the context of the crowd sale and, if necessary, obtain any independent advice in this regard. Any interested person who is not in the position to accept or to understand the risks associated with the activity (incl. the risks related to the non-development of the Authpaper Delivery platform) or anyother risks as indicated in the Terms & Conditions of the crowd sale should not acquire Authpaper Coin.

8.4 Disclaimer

This whitepaper shall not and cannot be considered as an invitation to enter into an investment. It does not constitute or relate in any way nor should be considered as an offering of securities in any jurisdiction. The whitepaper does not include nor contain any information or indication that might be considered as a recommendation or that might be used to base any investment decision. This document does not constitute an offer or an invitation to sell shares, securities or rights belonging to Authpaper Limited or any related

Legal Terms

or associated company. The Authpaper Coin is just a utility token which can be exchanged to operating credits on the Authpaper Delivery platform and is not intended to be used as an investment. The offering of Authpaper Coin on a trading platform is done in order to allow the use of the Authpaper Delivery platform and not for speculative purposes. The offering of Authpaper Coin on a trading platform is not changing the legal qualification of the token, which remains a simple means for joining the Authpaper Delivery platform and is not a security. Authpaper Limited is not to be considered as advisor in any legal, tax or financial matters. Any information in the whitepaper is given for general information purpose only and Authpaper Limited does not provide with any warranty as to the accuracy and completeness of this information. Given the lack of crypto-token qualifications in most countries, each buyer is strongly advised to carry out a legal and tax analysis concerning the purchase and ownership of Authpaper Coin according to their nationality and place of residence. Authpaper Limited today is not a financial intermediary according to Hong Kong Law and is not required to obtain any authorization for Anti-Money Laundering purpose. This qualification may change in case Authpaper Limited will offer services which are to be considered as qualifying a financial intermediation activity. In this case, the use of Authpaper Delivery services may require the positive conclusion of an AML/KYC identification process. Authpaper Coin confer no direct or indirect right to Authpaper Limited's capital or income, nor does it confer any governance right within Authpaper Limited; an Authpaper Coin is not proof of ownership or a right of control over Authpaper Limited and does not grant the controlling individual any asset or share in Authpaper Limited, or in the Authpaper Delivery network. An Authpaper Coin does not grant any right to participate in control over Authpaper Limited's management or decision-making set-up, or over the Authpaper Delivery network and governance to the purchasers. Regulatory authorities are carefully scrutinizing businesses and operations associated with cryptocurrencies in the world. In that respect, regulatory measures, investigations or actions may impact Authpaper Limited's business and even limit or prevent it from developing its operations in the future. Any person undertaking to acquire Authpaper Coin must be aware of the Authpaper Delivery platform business model, the whitepaper or Terms & Conditions may change or need to be modified because of new regulatory and compliance requirements from any applicable laws in any jurisdictions. In such a case, purchasers and anyone undertaking to acquire

Authpaper Coin acknowledge and understand that neither Authpaper Limited nor any of its affiliates shall be held liable for any direct or indirect loss or damage caused by such changes. Authpaper Limited will do its utmost to launch Authpaper Delivery operations and develop the Authpaper Delivery platform. Anyone undertaking to acquire Authpaper Coin acknowledges and understands that Authpaper Limited does not provide any guarantee that it will manage to achieve it. On concluding the Commercial Operation, these tokens will be issued by a technical process referred to as a «Blockchain». This is an open source IT protocol over which the Company has no rights or liability in terms of its development and operation. The token distribution mechanism will involve a Smart Contract; this involves a computer program that can be executed on the Ethereum network or on a blockchain network that is compatible with Smart Contract programming language. They acknowledge and understand therefore that Authpaper Limited (incl. its bodies and employees) assumes no liability or responsibility for any loss or damage that

Legal Terms

would result from or relate to
the incapacity to use Authpaper Coin, except in case of intentional misconduct or gross negligence. Authpaper Coin is based on the Ethereum protocol. Therefore, any malfunction, unplanned function or unexpected operation of the Ethereum protocol may cause the Authpaper Coin or Authpaper Delivery platform to malfunction or operate in a way that is not expected. Ether, the native Ethereum Protocol account unit may itself lose value in a similar way to Authpaper Coin, and also in other ways.

8.5 Representation and warranties
By participating in the crowd sale, the purchaser agrees to the above and in particular, they represent and warrant that they:

- *have read carefully the Terms & Conditions attached to the whitepaper; agree to their full contents and accept to be legally bound by them;*
- *are authorized and have full power to purchase Authpaper Coin according to the laws that apply in their jurisdiction of domicile;*
- *are not a U.S. citizen, resident or entity (a "U.S. Person") nor are they purchasing Authpaper Coin or signing on behalf of a U.S. Person;*
- *are not resident in China or South Korea and nor are they purchasing Authpaper Coin or signing on behalf of a Chinese or South Korean resident;*
- *live in a jurisdiction which allows Authpaper Limited to sell Authpaper Coin through a crowd sale without requiring any local authorization and are in compliance with the local, state, and national laws and regulations when purchasing, selling and/or using Authpaper Coin;*
- *are familiar with all related regulations in the specific jurisdiction in which they are based and that purchasing cryptographic tokens in that jurisdiction is not prohibited, restricted or subject to additional conditions of any kind;*
- *will not use the crowd sale for any illegal activity, including but not limited to money laundering and the financing of terrorism;*
- *have sufficient knowledge about the nature of the cryptographic tokens and have significant experience with, and functional understanding of, the usage and intricacies of dealing with cryptographic tokens and currencies and blockchain-based systems and services;*
- *purchase Authpaper Coin because they wish to have access to the Authpaper Delivery platform;*
- *are not purchasing Authpaper Coin for the purpose of speculative investment or usage.*

Legal Terms

8.6 Governing law – Arbitration

The Client acknowledges and accepts that the Authpaper Limited ICO operation is taking place within a Hong Kong legal environment that is still under development. The Parties agree to seek an amicable settlement prior to bringing any legal action. All disputes arising with the with papers provided, shall be resolved by arbitration under the Electronic Transaction Arbitration Rules of Hong Kong International Arbitration Centre (HKIAC) in force on the date when the Notice of Arbitration is submitted in accordance with these Rules. The place of arbitration shall be in Hong Kong at Hong Kong International Arbitration Centre (HKIAC). There shall be only one arbitrator. The arbitral proceedings shall be conducted in English. Authpaper Coin will not be listed on any regulated stock exchange, such as Stock Exchange of Hong Kong Limited, abb. SEHK, or any regulated future exchange, such as Hong Kong Futures Exchange (HKFE). These Terms have been prepared without regard to the legal standards for prospectuses the listing rules of any other stock or future exchange in Hong Kong.

Neither these Terms nor any other material relating to the Offer, Authpaper Limited or Authpaper Coin will be or have been filed with or approved by any Hong Kong regulatory authority. Specifically, these Terms will not be filed with, and the Offer of Authpaper Coin will not be supervised by, the Hong Kong Monetary Authority (HKMA) and Hong Kong Securities and Futures Commission (SFC). Furthermore, the Offer of Authpaper Coin has not been and will not be authorised under the Securities and Futures Ordinance. Thus, the protection which is given to purchasers of interests or units in collective investment schemes under the Securities and Futures Ordinance does not extend to purchasers of Authpaper Coin.

Authpaper Limited

9. Authpaper Limited

Authpaper limited is found in 2016. With a vision of “building trust across real and digital world”, Authpaper limited has been providing software solutions on e-document anti-forgery based on founder’s research work and testing web and mobile applications against common cyberattacks.

9.1 Management Team

Solon Li,
CEO / Founder

LinkedIn : https://www.linkedin.com/in/solon-li-9502b026/

Solon is the authorized trainer for Oxygen Forensics, a worldwide developer and provider of advanced forensic data examination tools for mobile devices and cloud services, in Hong Kong.

He graduated from the Chinese University of Hong Kong (CUHK), with double degree in Mathematics and Information Engineering in 2011 and Master of Philosophy (M.Phil) in Information Engineering in 2013.

During his research study and work in CUHK, he invented a document anti-forgery technology using customized QR codes. This technology has won the winner award in Asia Pacific ICT Alliance in 2013 in the R&D category, and received over 1.5 million funding support from Hong Kong Government (ITF) and CUHK. He also received outstanding teaching awards for tutoring in courses on cyber security and web programming.

With a strong interest in cyber security, authentication and mobile system, as well as an enthusiasm to bring his research to solve real world problems, he founded Authpaper Limited in 2016. Solon had joined Unissoft Technology Company Limited in 2017, focusing on developing Blockchain applications to certify document signings. He is also a certified examiner (EnCE) to provide computer examinations and forensic services.

Authpaper Limited

Derek Leung
BlockChain Consultant
LinkedIn :
https://www.linkedin.com/in/derek-leung-5853a9172

- MSc in Intl' Banking & Finance & B Com (Marketing & Advertising)
- More than 8 years business planning experience
- Sophisticated in strategic planning
- Combined innovative business planning with technology
- Focused on quantitative analysis into businesses

Alex Chiu
COO
LinkedIn :
www.linkedin.com/in/ckgalex

Jack of all trades. Alex is a Hong Kong entrepreneur who has previously founded successful companies in IT. Twenty years of experience designing and implementing software solutions. His primary expertise is in: B2B Ecommerce, Business Workflow system, Blockchain based systems development, data driven applications and document management applications. Bridging the gap between technical solutions and business. Participated as a technical consultant in many startups. Helped design and build scalable, durable and cost optimized solutions covering mobile, front-end and back-end tracks.

Lawrence Chiu
Business Development Manager

LinkedIn :
https://www.linkedin.com/in/lawrence-chiu-550a07b4/

Authpaper Limited

LC98 Automatic Trend Trade System is designed and coded by myself. The system provides the user with a whole new way on trading securities, index future and options automatically in the capital market.

The system has three main parts. One is Artificial intelligence (AI) or Business Intelligence (BI) which is feed by real time market data. The A.I. makes calculation on the real time data and generates the trading signal.

The modeling used here included a wide range of methods. For example I turned the physic theories into the program code and implemented by the mechanical models to build up the A.I. system. For example Dynamic system, Chaos theory, Fractal Geometry, Thermodynamic system etc also together with the classical analysis method.

In our recent expansion pack study, we are estimating the use of Big Data technology. Just like what the Morgan Stanley did in the past years to use Hadoop (A kind of distributed file system) in their data analysis system. Although I am familiar with SQL Server but now for Big Data Project we should not just using the rational database but also together with the Hadoop. In result to improve the power of the predictive ability on capital market trading activities. One of the examples is the system collect information from Google and Facebook activities and turns it into useful information for decision making. What I did is somehow like the data scientist does.

The other part of the system is an order controlling system. The controlling system is direct connected to the broker system. Actually there are many real time calculations in the system and it was designed in a distributed server base to improve the overall system performance.

Third, the system has a self errors detecting function and connected to the Android App developed by myself. The App will communicate with the server. And the users can get the updated information anywhere from the server just by checking the App or reading the auto alert sent by the App.

9.2 Previous Recognitions

The core technology inside Authpaper Limited is based on a research project Authpaper by Solon during his research study in The Chinese University of Hong Kong (CUHK). The technology has won the winner award in Asia Pacific ICT Alliance in 2013 in the R&D category and received over 1.5 million funding support from Hong Kong Government (ITF) and CUHK. The research was published in multiple international academic conferences like MobiSys 2014, IEEE International Conference on Communications (ICC) 2015, and IEEE International Conference on Image Processing (ICIP) 2016.

Authpaper Limited

Upon founding in 2016, Authpaper Limited has been under the Cyberport Incubation Program until 2018. Cyberport is an innovative digital community with 1000 digital tech companies. It is managed by Hong Kong Cyberport Management Company Limited, which is wholly owned by the Hong Kong SAR Government.

Besides funding, Authpaper Limited has obtained a PCT Hong Kong short term patent HK16113902.2 filed on 06 Dec 2016 with title “A METHOD AND SYSTEM FOR COMPRESSING DATA”. This patent is also filed via PCT system, dated 14 June 2018, publication number WO/2018/103490.

Authpaper Limited has provided software solutions to Hong Kong companies. We have created a certificate stamping solution for a gallery to add anti-forgery solution on their certificates of authenticity. A coupon solution for a solution company so that they can issue coupons which can be verified by public offline and redeemed by partnering companies through mobile. All redemptions are detailed recorded and managed by the backend system.

Authpaper Limited

BLINK GALLERY

CERTIFICATE OF AUTHENTICITY

This document certifies that the following is an original work of

Simon Yung 容子敏

TITLE:	Back Garden 香江後花園
DIMENSIONS:	70 x 138cm
YEAR:	2016
MEDIUM:	Ink and Colour on Paper
No. :	SAA053

ARTIST
Simon Yung 容子敏

Proof of true certificate

CO-FOUNDER of BLINK Gallery
Mr. Albert Chung

www.blinkgalleryhk.com

Authpaper Limited

Authpaper Limited also partner with Unissoft Technology Hong Kong Limited and Yiu & Associates Solicitors to create an e-document blockchain signing solution which allows users to circulate and sign a document, all signatures are certified by solicitors and signing records are stored on blockchain.


Document Signature Result

This document is signed by all parties.

The signing is verified by Yiu & Associates, Solicitors

Yiu & Associates SOLICITORS 姚文鑫律師行

Besides, the hash of the signed document is also recorded on the BlockChain.

SHA-256 Hash (Think it as the fingerprint of the signed document) :
d614b927fd19a5dc9d749f4e6cefbbf9fa20febac5bfbe6653c95611997c167

Txid (indicating the signature record in BlockChain) : 8628637f4a8524673262359 2b54acfe0ca1bf3f212f6481b5d88570cf67fd32c

Time of first signature: 23 November, 2016, 2:44pm (Hong Kong Time)

Time of second signature: 23 November, 2016, 3:15pm (Hong Kong Time)

Time of verifying by Yiu & Associates, Solicitors: 24 November, 2016, 10:00am (Hong Kong Time)

Scan the QR code to check the signature history on BlockChain.

A secured digital postal services Using BlockChain Technology

Authpaper.io

hello@autpaper.io