BCDiploma

by Blockchain Certified Data

WhitePaper v2.1

January 15th, 2018

GENERAL WARNING

This document does not constitute an offer or an invitation to sell shares, securities or rights belonging to BCD or any related or associated company.

None of the information or analyses described in this document is intended to provide a basis for an investment decision, and no specific recommendation is made. This document does not constitute investment advice or an invitation to invest in any security or financial instrument of any nature whatsoever.

This document does not constitute or form part of, and should not be construed as, an offer for a sale or subscription, or an invitation to buy or subscribe securities or financial instruments.

BCD expressly disclaims any liability for any direct or indirect loss or damage of any kind arising directly or indirectly from:

(i) Any reliance on the information contained in this document;
(ii) Any error, omission or inaccuracy in said information;
or
(iii) Any resulting action that may be brought.

We also invite you to read carefully the Terms and Conditions of BCD ITS.

CONTENT

THE BCDIPLOMA PROJECT

The ultimate goal of BCDiploma is to certify diplomas in the simplest, most secure, and sustainable way possible, by associating Ethereum technology with a high level of cryptography. As EdTech experts and higher education specialists, we know the expectations of schools in this domain. Facing the falsification of their diplomas and an increased competition, they are ready to offer their graduates an innovative digital service to protect their image.

BCDiploma develops a DApp for institutions of higher education to enable them to issue their degrees on Ethereum. BCDiploma allows the graduate, throughout his life, to prove the authenticity of his diploma by providing a simple URL. It is a competitive solution, durable, unfalsifiable, compatible with social networks, simple to use, perfectly adapted to the uses of higher education. Schools have not yet adapted a certification standard? We offer it to them. Once put in production for schools, what future for BCDiploma, solution developed by Blockchain Certified Data (BCD)?

BCD will have an inexpensive, fast-running open source ecosystem created, in order to deploy on-chain registries while respecting the right of personal data on Ethereum.

These on-chain registers are usable by all on a daily basis: they read a smart-contract certified data. It's a general application of Ethereum: each and everyone of us can prove in a single click that he is well qualified, doctor, holder of a driving license...
The fields of application are numerous: professional competences or certifications, registers of regulated professions, internal business registers, administrative registers...

Ethereum, by its scalability, is technically ready to store registers on a large scale: we want to develop the framework of it and make the use of DApps a daily action for everyone. To accompany us in this project is to make a step towards a world in which we will all trust in the data issued by the institutions.

STATE OF PLAY

Number of degrees issued worldwide

More than 4 million students graduate every year from higher education throughout the European Union[1].

Almost 4 million college students (Colleges and Universities) graduate in the United States each year[2].

Nearly 7 million university degrees were awarded in China in 2012[3].

The OECD calculated that its member countries, as well as those of the G20, will bring in total nearly **204 million** graduates aged 25 to 34 in tertiary education in 2020, compared with 129 million in 2010[4]:

- China: 29% (about 60 million graduates);
- India: 12% (about 25 million graduates);
- United States: 11%;
- Russian Federation: 7%.

The LinkedIn social network exceeded the **500 million** registered in 2017: a very large majority of them have several diplomas on their profiles.

The fake diploma market

Have you ever searched “fake diploma” on Google? Just give it a try before you read the following paragraph!

It’s a well-established matter of fact, constantly relayed by the media: the fraudulent use of fake diploma, or made-up qualifications on resumes and social media is a hard fact impacting schools, graduates and employers. This problem has been addressed in the news many times.

Yahoo!'s former CEO[5] Scott Thomson, or Melania Trump[6] in the US: scandals are constantly emerging.

> *"In France, 33% of applicants use fake diploma. This number is similar in the United Kingdom. According to the official organism in charge of diploma authentication, (...) 30% of the applicants lie about their qualifications."* [7]

Two markets, the first one being on the edge of the law, the second one being clearly illegal, are taking advantage of this trend:

- Diploma mills / degree mills selling real diploma from schools that don't exist, or having a more than thin physical reality[8];
- Professional websites selling high quality replica diploma.

In order to counter the phenomenon, societies have popped up to "verify" degrees afterwards and check their authenticity: Verifdiploma or RiskAdvisory are some examples of this.

Job boards

Two main trends can be identified in the education and recruiting market nowadays:

- The job market's needs and recent amendments show that the tendency yields towards more flexibility. As a result, short-term contracts are increasing, volatility in the workforce is rising and the recruiting process needs to adapt. Companies need to recruit more, faster and in a decentralized and automated way;
- New actors are emerging from this tendency: job boards (LinkedIn, Monster, Indeed) are platforms operating on a global market, which strive to answer the need of speed, automation and specialization.

A major risk is also emerging from these tendencies: the falsification of data sent by applicants. This is a major issue for companies who rely on the veracity of data provided by their employees. This is a major issue for the actors of the educational and training system, which have to defend their integrity. BCD is here to offer them the perfect solution.

Degree certification: the current offering

Despite a very active EdTech sector these last years, no standard was ever adopted at a large scale to answer to the question of diploma certification.

Historical competitors

The historical competitors, like CertainSafe, relying on digital safes, have been proven inefficient in curbing the prevalence of forged degrees. They have failed to conquer the market of degree certification. Their weaknesses are structural: they are too centralized and proprietary, easy to hack and their code is closed-source. Their sustainability depends on the survival of the competitors themselves. In addition to that, their fee schedule is complex and it is challenging to calculate how much storage will cost over the years.

Blockchain competitors

Some promising blockchain experimentations emerged: a first one of the Holberton School, and a second initiative by the ESILV in France. Blockchain competitors have also tackled this issue: Ledgys, Keeex or Attores for example.

Their approach is identical: store an imprint of the documents on the blockchain. If the method can guarantee the authenticity of the document initially "hashed", it doesn't answer several problems:

- The identity of the sender is not proven, and the authenticity of data is not certified: how to be sure that the hashed diploma is the original one, and that it was really issued by the school?
- The regulation on the right to be forgotten might also be violated. Indeed, if the document is shared, the hash is indelible, and the document stays forever recognizable.

Sony recently revealed its will to commercialize a blockchain application to secure and share school's credentials. They chose a private blockchain (partnering with IBM) and proprietary software, which is the opposite of the BCD's vision.

We want an open source system based on a transparent public blockchain, but a secured one so search engines will not be able to find or use any data.

How does BCDiploma meet the school's expectations?

First of all, BCDiploma brings a solution to a concrete and relevant problem that schools' IT departments struggle with. The number of higher education institutions keeps increasing and competition is fierce amongst them. Each one of these schools is yearning for a stronger reputation and for better quality services for their students. The diploma's certification issue is in every Director of IT System's mind.

An easy implementation

Within schools, IT and administrative services in charge of issuing diplomas are looking for easy and practical solutions to use.

BCDiploma offers a "turnkey" DApp, which will allow schools to issue diplomas by a simple data upload. By doing so, schools:

- Avoid a complex document management, which is necessary today to implement the current blockchain solutions (issuance of a digital "original" document, storage, hash);
- Don't have to handle digital safes and their access anymore. With BCDiploma, the only element the graduate needs to access his diploma is a matching URL.

Safety, reliability and trust

Schools have to deal with the issue of their data's safety, especially with long-term storage.

- BCDiploma's encryption algorithm, associated with data storage on Ethereum, ensures a level of reliability and safety that doesn't exist on the current market;
- The Blockchain technology creates trust between the various players: protocols are clearly defined and the existing rules are always respected and checked.

Sustainability

Choosing a long-term, reliable service without depending on a provider is a major challenge for schools.

- While using BCDiploma, schools cannot lose their diplomas' data any longer, as they are stored on Ethereum;
- BCDiploma uses open source systems called DApps: data's access and DApps' use are guaranteed to the schools without any time limit.

No recurring costs

Long-term cost management is paramount for schools.

- Compared to the other market players, BCDiploma is highly competitive. There is no monthly plan or maintenance cost but only one payment per diploma;
- If deemed more convenient by the schools, BCDiploma offers an “all-included” service, called SaaS, billed after the fact in USD or EUR.

Economies of scale

Alumni or employees constantly solicit schools regarding copies’ issuance or diplomas’ certificates.

Thanks to BCDiploma these issuances can be automated and externalized. Schools will save so much time and energy.

Personal data’s protection

Schools must respect the regulations on privacy and personal data.

BCDiploma complies with the essential principles set by the General Data Protection Regulation (GDPR) and was created so:

- It won’t be possible for the BCDiploma Solution operators to use or collect data;
- The right to be forgotten regulation could be implemented.

Digital innovation

To be attractive and competitive, schools are looking for digital innovations to serve their graduates in a practical way and improve their reputation.

- Thanks to BCDiploma, alumni can use their diploma’s URL on LinkedIn and other social media, without any time limit;
- BCDiploma gives schools a “technological pioneer” dimension.

BCDIPLOMA CONCEPT

BCDiploma's solution has an innovative approach: in our opinion, the diploma's value is based on the data's authenticity rather than on the document itself. This is why BCDiploma will store the specific **data directly on the Ethereum** blockchain.

EvidenZ ecosystem

The EvidenZ Framework

To implement BCDiploma, BCD is going to develop and operate an open source framework[9] called EvidenZ.

EvidenZ allows deploying on-chain registers for diplomas in the first place, as well as for any kind of data. It has been conceived to respect the regulation on data privacy (GDPR[10], as well as the right to be forgotten). **The Legal Opinion written by *Alain Bensoussan Avocats - Lexing* law firm (*BCDiploma-Legal Opinion* - September 19th, 2017 - Ms Nathalie Plouviet) underlines how BCDiploma's tools and methods constitue an approach which is respectful of the GDPR.** Evidenz has been conceived to store small, important and/or permanent data, such as a diploma, a civil status certificate or a nomination to the National Medical Council, etc.

EvidenZ certifies data using an innovative approach:

- The data's issuer is systematically identified and verifiable;
- The data itself is stored on Ethereum and thus cannot be modified any longer;
- Sharing the data is the responsibility of the graduate, employee or citizen it belongs to;
- The data can be made indecipherable by deleting the associated persistence key.

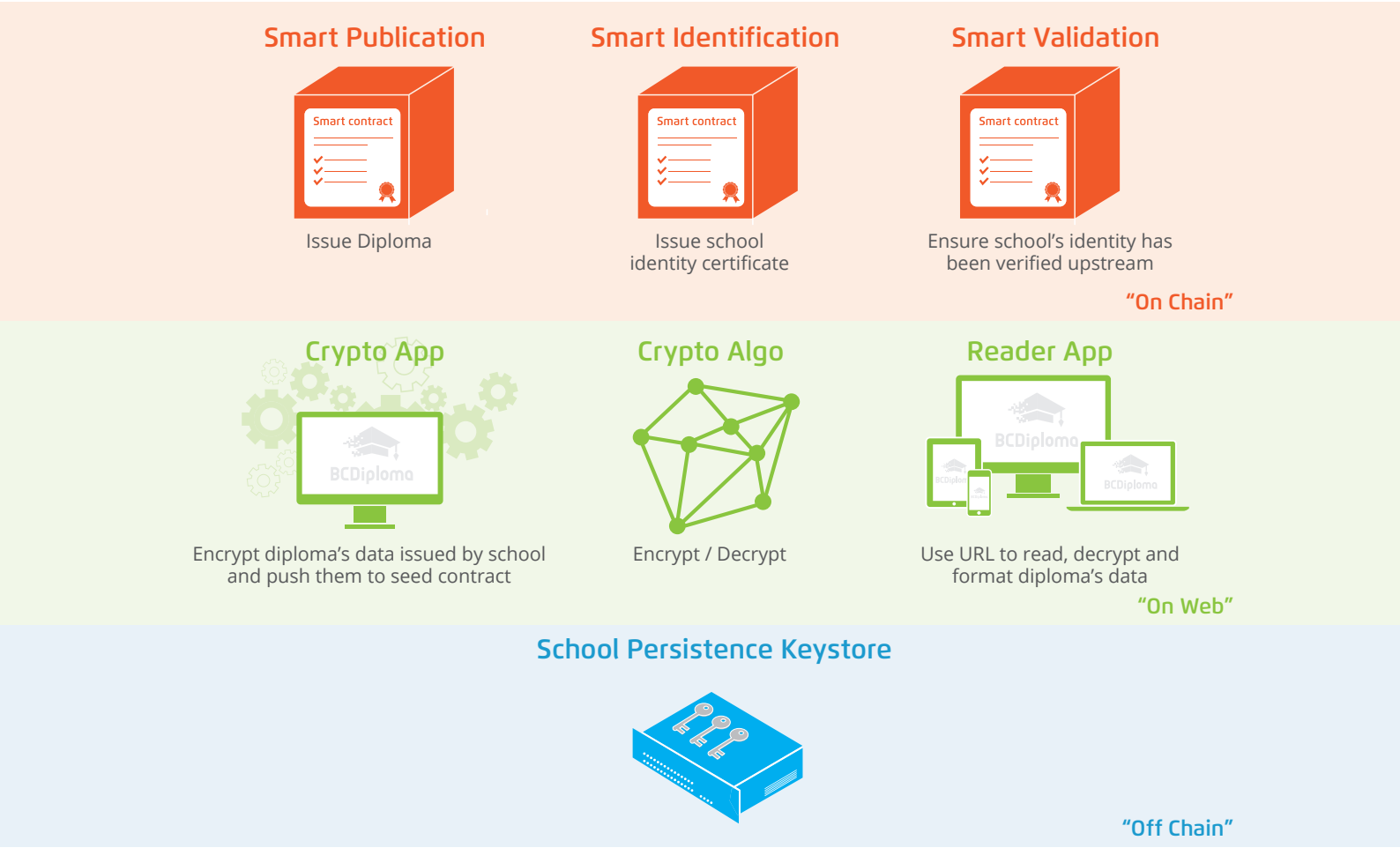
To run EvidenZ, the Ethereum blockchain is the obvious choice. It allows:

- An optimal safety level due to its large deployment and its irreversibility.
- The transparency of a public blockchain, necessary for users to trust it, particularly with the open source smart contracts.
- A vast ecosystem and many improvements to come, particularly regarding scalability.

Architecture

EvidenZ blocks have three levels of classification:

- *On-Chain:* smart contracts - SmartValidation, SmartIdentification, SmartPublication;
- *On Web:* DApps - Crypto App and Reader App, with secured web access;
- *Off-Chain:* keystore[11].



The DApps interact with the Ethereum blockchain and are working exclusively with the smart contracts to guarantee a verified data. DApps are open source systems, so that the clients of the solution can deploy it themselves. The persistence keys are stored in the keystore, which belongs to organizations sharing data with EvidenZ. This keystore guarantees the implementation of the right to be forgotten regulation, which, according to the GDPR, is mandatory, worldwide.

Decentralized deployment or SaaS

Our goal is to develop an open ecosystem, which will technically be independent from BCD. This will allow to:

- Encourage big institutions to adopt it and thus create the on-chain register standard;
- Guarantee a permanent access to the encrypted data stored on Ethereum even if BCD no longer exists.

The EvidenZ framework has been designed for a decentralized deployment. Schools which choose to run it themselves, will operate independently and will benefit from DApps' support and improvements.
If this is the institution's preference, BCD will offer an "all-inclusive" service, called SaaS. Our firm will manage their keystore, by proxy, within a totally secured environment. By doing so, BCD takes up a major challenge: making schools use the Ethereum blockchain, by allowing them to buy a service in commercial conditions which fit their standards.

Focus on the data's size

The data's size sent by BCDiploma is a key factor. The cost of the Ethereum transaction when diplomas are sent varies mostly because of that. Indeed, sending data via an Ethereum's transaction burns off gas[12] and the miners' wage has to be considered. The amount of gas spent to execute the transaction is proportional to the volume of data sent. **Choosing data storage directly on Ethereum over a regular approach (on-chain hash[13] / off-chain document storage) is BCD's DNA.** This type of storage guarantees unchangeable data that can't be hacked and is not limited in time. We believe this is the least you can ask of a secured register.

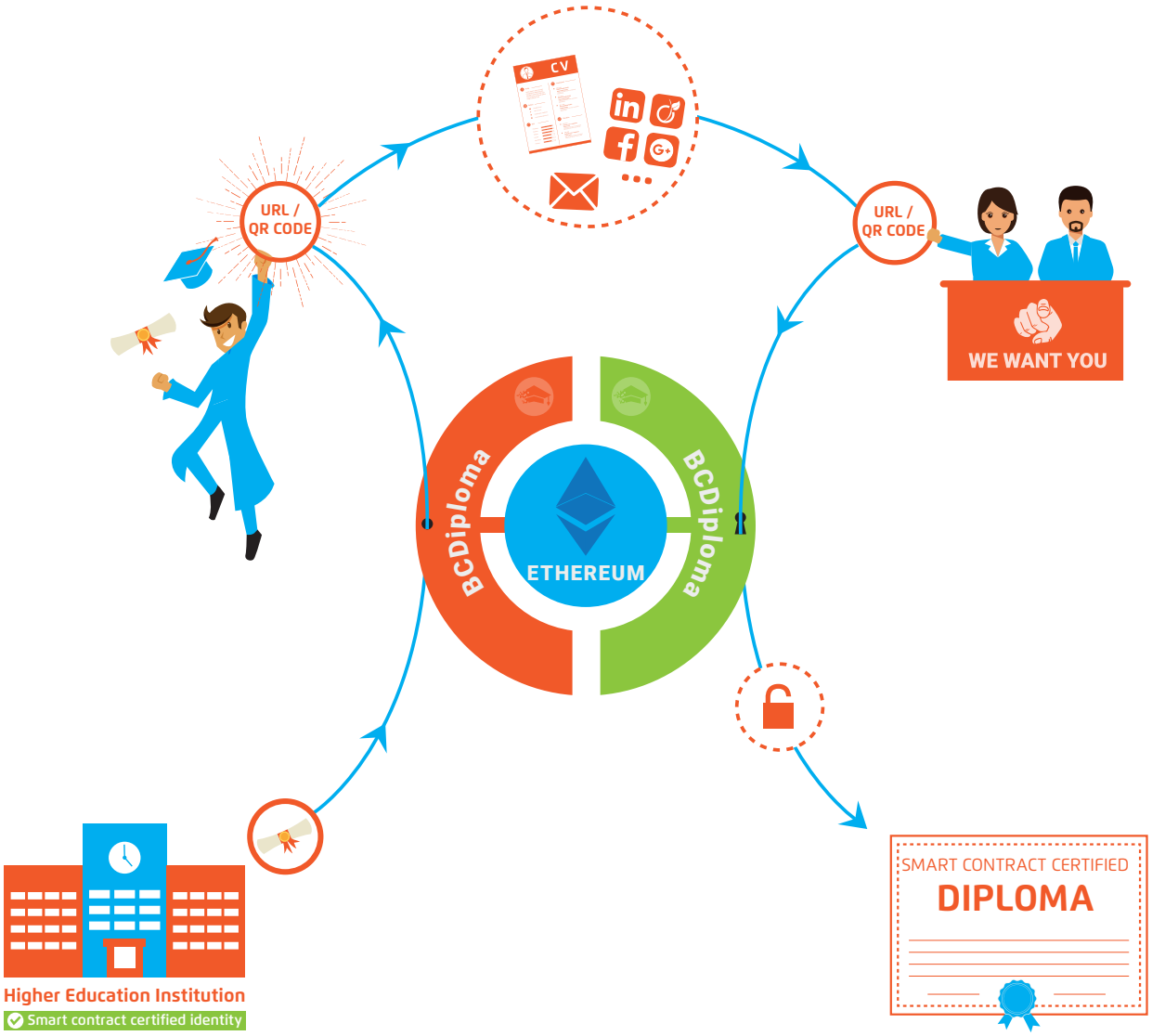
The EvidenZ's architecture was conceived to take advantage of this particularity. The amount of significant text data on a diploma is limited and often redundant from one diploma to another. Using optimized algorithms to reduce the amount of data per transaction, Evidenz pools, structures and zips data. Thanks to the excellent ETHgasAPI, this architecture is combined with an efficient use of gas price, to maintain a low cost when diplomas are sent from Crypto App. In a near future, we believe in Ethereum upscaling capacities: Metropolis[14], PoS[15], sharding[16]. EvidenZ will take advantage of all of them and costs will be constantly optimized.

Diploma Size	Text Data Size (bytes)	Encrypted/ Encoded size (bytes)	Safelow Tx Price (ETH) gas price 4 gwei	Safelow Tx Price (USD) gas price 4 gwei	Fast Tx Price (ETH) gas price 21 gwei	Fast Tx Price (USD) gas price 21 gwei
Normal	111	194	0.000165932	0.05	0.000556143	0.17
Large	327	519	0.000314752	0.09	0.001337448	0.40

Timeline

The development of the EvidenZ framework will begin three months after the end of the ITS. In 2018, in the context of the Incentive programme, we will implement the solution in the partner schools.

Operational specifications



1. The school has to create an ID on Ethereum

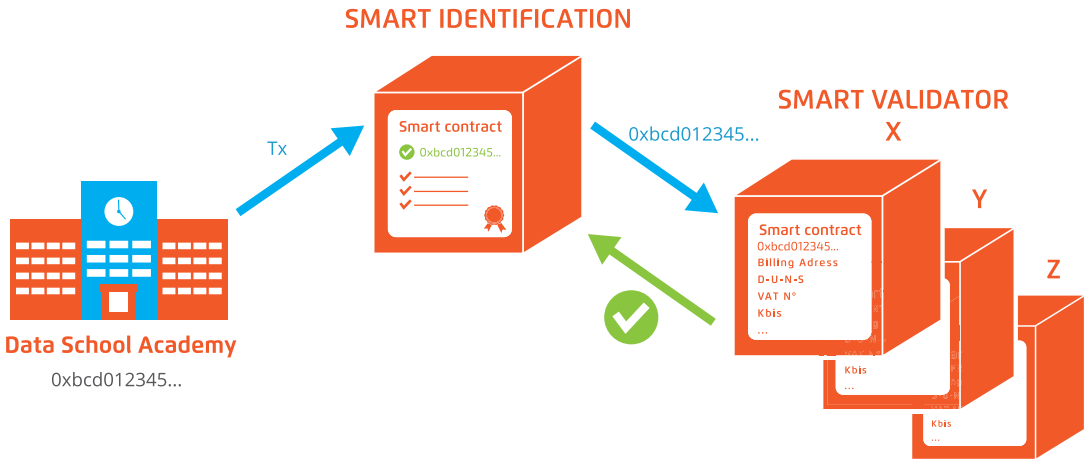
1.1 A validator guarantees the school's identity

Upon the school's request, a third party, which we call "validator", vouches for their identity on Ethereum, so there can't be no doubt about the Ethereum address used to share the diplomas. The validator is an Ethereum actor deploying the smart contract SmartValidation.

The matter of legal entities' proof of identification on Ethereum is a subject that will encourage the emergence of benchmark players. In order to build a trustworthy open ecosystem, we need these players to act as validators. When BCDiploma is launched, BCD will be the first validator of the ecosystem and will do the necessary verifications to ensure the reliability of everyone involved and the actual existence of the school: banking information and physical address, e-reputation, trade and company register number (RCS), DUNS number, intra-community VAT number, and authorization to issue diplomas. Come 2018, we plan on introducing more Ehereum's players to act as "validators".

To get an "ID Certificate" the school must proceed with the implementation of a smart contract *SmartIdentification*. The latter allows to:

- Check via a smart contract *SmartValidation* that the validator has checked the school ID;
- Publish the school's "ID Certificate" in the transaction data without encryption.



1.2 The school's ID certificate is proof of the diplomas' authenticity

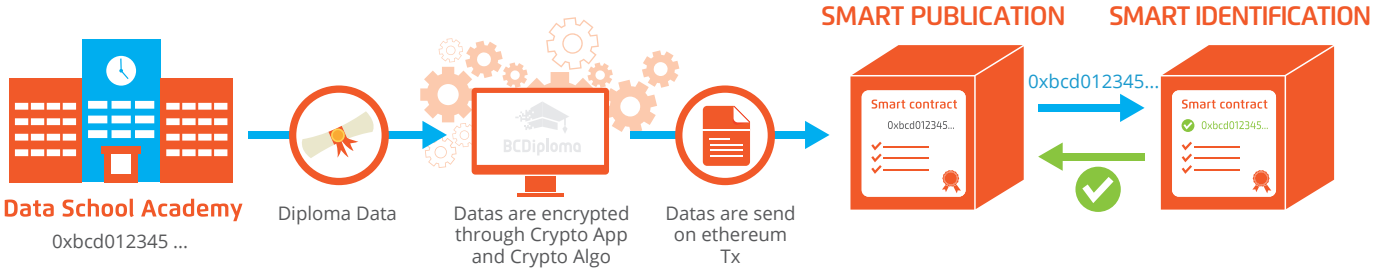
The ID certificate includes the following information: the school's name, the characteristic features of the diplomas that are issued, the URL of the corporate website page on which the Ethereum address will be published and the URL of the web server hosting Reader App.

This certificate serves two purposes:

- A diploma will be shared if and only if the certificate is valid. School will be able to use an expiration date if necessary, using a smart contract SmartIdentification option;
- When a diploma is being checked, the certificate will prove in "clear text" (i.e., directly readable via etherscan[17]) the school's ID, a proof that can be cross-checked by the publication on the school's corporate website of its Ethereum address.

2. The school will put the encrypted diplomas on Ethereum via Crypto App

The steps the schools have to follow are simple: send the diplomas' data via Crypto App (uploading the file or the API[18]) and confirm the encryption and sending request on Ethereum. These two actions are performed by Cypto App, first, and then by the smart contract *SmartPublication*.



For each diploma issued, the smart contract *SmartPublication* will:

- Check the school's ID certificate validity;
- Publish the encrypted diploma in the transaction's data.

At the end of the process, Crypto App will:

- Generate and store the persistence keys in a safe location: the school is the owner of these keys;
- Send, in a secured way, the URL to read the issued diplomas;
- Send a completion report to the school;
- Erase the entirety of the processed data (process *in memory*).

3. The graduate receives the URL to access the diploma

Each graduate will receive, in a secured way, the URL to access his or her diploma. This URL cannot be retraced from the Ethereum's transaction. However, you cannot access the diploma without it.

The graduate is the only custodian of the URL and sharing it is his responsibility. He decides if he wants to share it on social media or send it to a third party upon request. If the graduate wants to assert his right to be forgotten, the school will have to destroy the persistence key after verification of the graduate's ID. Reader App, or any other BCD' app, won't be able to decrypt the diploma any longer.

4. A third party can access the diploma via Reader App

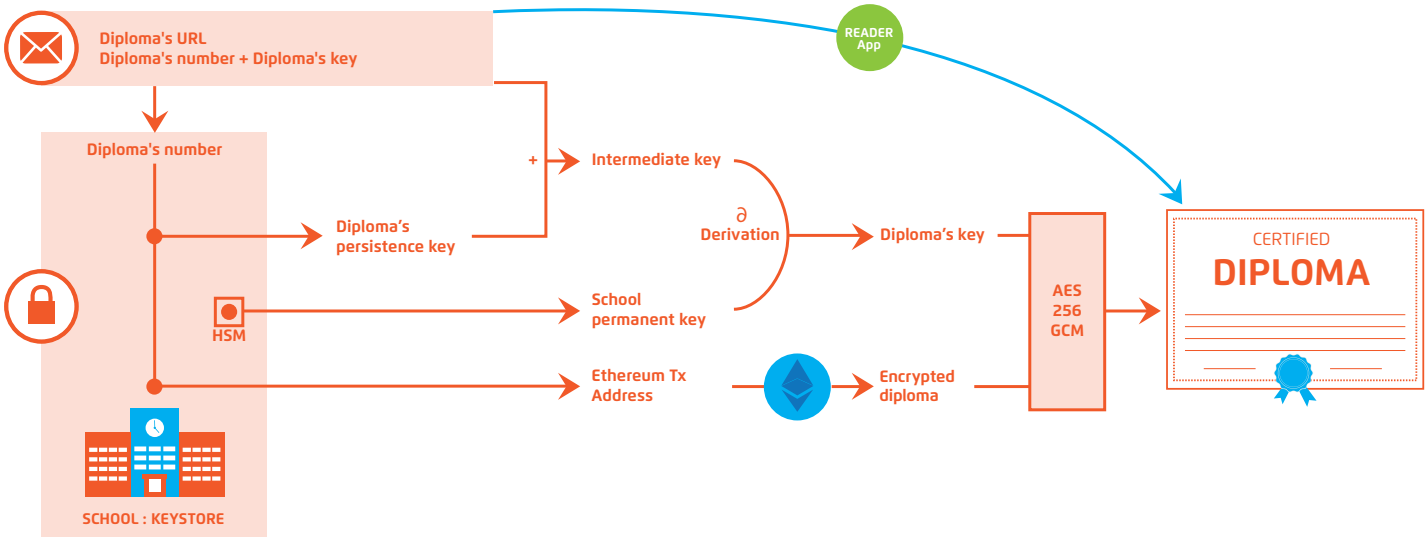
The graduate gives his diploma's URL to a company or university recruiting manager... This URL, redirecting the user towards the Reader App's server, allows him to:

- See the diploma, which will have been designed based on a pattern set on the ID certificate and decrypted by Reader App;
- Access the ID certificate (directly via etherscan for example) in order to check the sender's and web server's authenticity, more specifically the matching Ethereum's address of the school and the exact URL of the web server hosting the diploma he is seeing.

The ID certificate will also be searchable on the corporate website of the validator.

Crypto Algo

Centerpiece of the product, the cryptographic protocol has been conceived by BCD and meets the highest standards required. Thanks to a tailor-made architecture, it executes the project's core principles: **compliance to the right to be forgotten, control of the data access, and the guarantee that the data won't be stolen.** You can check the technical specificities of the Crypto Algo protocol in the White Paper's appendix.



- Even if you have access to the "persistence keys" table, you cannot decrypt the data without the HSM's access, which holds the MasterKey. And even if you have access to these two keys, you still need the "diploma's key", which is in the diploma's URL;
- The only persistent AES key is the MasterKey, however it isn't enough to decrypt the data. When necessary, the AES keys of every diploma can be generated by derivation (during the encryption or when the diploma is seen) and deleted immediately after usage;
- The URL to read the diploma doesn't allow to find the matching Ethereum's transaction or to build an oracle to obtain information. In order to do so, if a wrong URL is used, the server will send back an error to the client without revealing any information. Locally, a detailed log will be generated on the server for analysis purposes;
- The deletion of a diploma's persistence key in the "persistence keys" table will permanently prevent the decryption of the data associated with that key, without impacting any other data.

THE FOUNDERS

Luc JARRY-LACOMBE
CEO

He is the Product Owner at an Ed Tech editor for the higher education system. He is an expert of the education system. Associate professor of Mathematics, director at a "preparatory school" (classes préparatoires aux grandes écoles), and IT consultant at the pan-European business school, ESCP Europe.

> *"My goal is to give BCDiploma an UX/UI dimension so the company can be up to the challenging task of conquering the higher education market. We know its actors and standards perfectly well."*

Vincent LANGARD
CTO

He is the Technical Director at an ERP editor for the higher education system. Software architect and backend developer for open source technologies, he has been developing and integrating Ed Tech solutions in higher education schools' information systems for more than 10 years.

> *"Security, reliability and performance will be my priorities as BCD's lead developer, in order to make BCDiploma the baseline solution of educational institutions".*

Full team, partners and advisors available at www.bcdiploma.com

BUSINESS MODEL

BCDiploma's solution will be deployed in an ecosystem composed of three types of players: the diplomas' issuers (universities, business schools, engineering schools, etc., professional training companies), the international jobboards (LinkedIn, Indeed, Monster & Co) and their users (graduates from around the world and employers).

The business model

Our first clients will be the diplomas' issuers: universities, schools, professional education institutions, and institutions delivering attestations such as TOEIC, SAT or graduating MOOCs. Our main partners will be the jobboards and the players of the recruiting field.

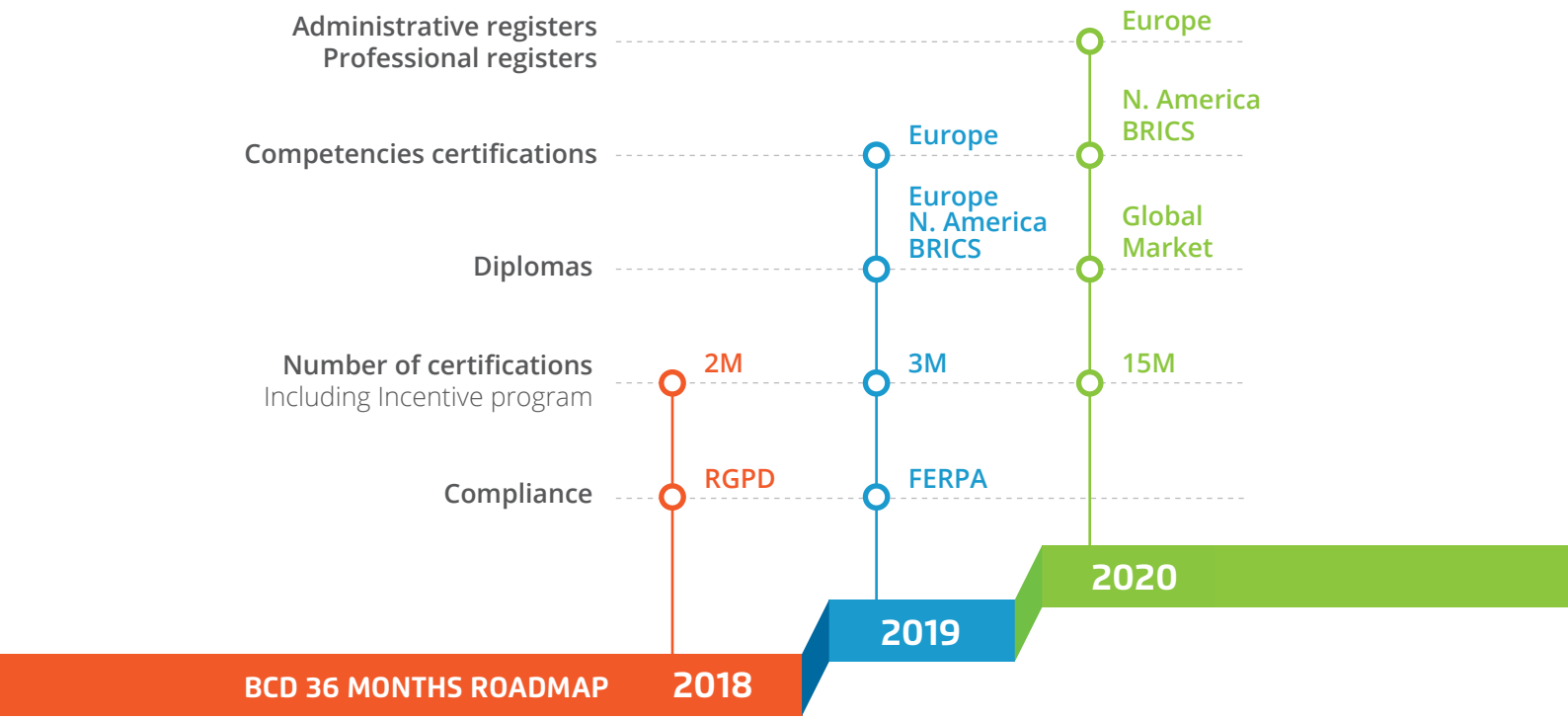
- Seeing the diploma will be free for all;
- **Our service will be free for the graduate,** the employee or the citizen, without any time-limit;
- For our clients, the unit cost for issuing a degree will be competitive compared to the actual players, who use "digital safes";
- **The payment for issuing diplomas will be in tokens BCDT** at a constant FIAT price (USD) through the Smart contract SmartIdentification. BCDiploma develops an "all-included" SaaS service, allowing the clients to be directly billed in USD or EUR: then, BCD handles the acquisition of the tokens on behalf of its client;
- There will be no recurring cost, nor subscribing or conservation costs. In the long run, the total cost (issuing and conservation) of a degree will be significantly less than that of the actual players using "digital safes".

Strategy

In 2018, we will launch our application and offer it to the education and recruiting market's leaders, primarily in Europe. Our goal for the first year is to gain a **worldwide legitimacy** publishing the diplomas' history of the top schools on every continent. An incentive budget that meets all the above-mentioned issues will support this goal (15% of the tokens' sale amount).

2019 will see the launch of a **massive marketing campaign** to conquer the diplomas' certification market in Europe, in North America and in the BRICS members. In the meantime, in Europe, we will take hold of the skills certification, professional certification and professional registers' market.

In 2020, being a global market player, we will have reached the necessary scale to enter the **massive market** of administrative registers.



THE INITIAL TOKEN SALE

An Initial Token Sale (ITS) is an event in which a project related to cryptocurrency sells a part of its tokens to early adopters and enthusiasts in exchange of financial supports. This process of crowdfunding is now an acknowledged and standardized mean to obtain funds destined to the large-scale development of a product or a service, be it an existing service or a in construction service. The necessary funds to launch our BCDiploma application will be raised through a Ethereum-based crowdfunding.

The ecosystem of BCDT's token

BCDiploma's goal is to become the point of reference for diplomas' certification. Our challenge today is to gain schools' confidence and patronage worldwide, and to expand our services and offer them to companies and administrations in the near future. These institutions, public or private, might not have "blockchain" knowledge. In the first place, to convince them, we have to offer a product fitting their needs perfectly. We also have to be ready to offer a billing system, which is easy to use and understand and meets their standards. The right way to encourage schools to use Ethereum on a daily basis is to bill them in USD.

What added value do we propose? The value created by BCD will be measured proportionally to the volume of on-chain data issued by the institutions.

The key-words of the BCDT tokens ecosystem are: trustless and automation.

The unit cost of issuing a diploma will be measured in BCDT tokens at constant FIAT (USD) prices. The BCDT / ETH / USD rate will be updated at regular intervals on the smart contract Smart Identification by a decentralized exchange bot to guarantee the issuer this fixed unit price in Fiat (USD). To protect the issuer from the variability of the BCDT token, the issuer will "buy", if he wants to, a "Number of diplomas to be issued", thus limiting transactions in BCDT tokens for users of the eco-system. More precisely:

- For each ID Certificate, the smart contract Smart Identification stores a variable “Number of diplomas to be issued”;
- At the creation of the certificate by Smart Identification smart contract, this variable is initialized to 20 (i.e. “20 offered diplomas”), in order to facilitate the adoption of the product;
- Subsequently, the issuer values the “Number of certificates to be issued” variable of his ID Certificate by sending BCDT tokens to the smart contract Smart Identification. At the time of this transaction, the issuer knows the unit price in BCDT tokens of a diploma yet to be issued;
- In the same operation, the smart contract Smart Identification burns the equivalent of 5% of BCDT tokens paid for “diplomas to issue”, as a manufacturing fee.
  This rate is increased during the first three years of activity to support the token price:
  - 25% as long as the set of tokens burnt does not exceed 10% of tokens minted;
  - Then 20% as long as the set of tokens burnt does not exceed 20% of tokens minted;
  - Then 15% as long as the set of burned tokens does not exceed 50% of tokens minted.

  BCD reserves the right to change this rate at a later date if more than 66.6% of tokens minted have been burned;
- When issuing a diploma via the smart contract Smart Publication, the “Number of diplomas to be issued” variable is decreased by one.

The BCDT token is therefore an application token to “reload” the “Number of diplomas to be issued” of a school. As such, it has every chance of being placed on a large number of exchanges and not being constrained by the securities legislation.

The Initial Token Sale

During this ITS, the token we offer will be called “BCDT token”. It is compliant with the ERC-20 standard.

Presale will start December 2017. Detailled timing will be available on www.bcdiploma.com.

During the ITS, the Ethereum (ETH) will be the only accepted currency to buy BCDT tokens.

The contribution’s address will be unveiled on www.bcdiploma.com.

BCDT tokens will be available in the investors’ wallet immediately and will be transferable 12 days after the end of the ITS. The tokens’ distribution will happen exclusively through BCDT token’s smart contract. Its source will be provided.

If the total amount raised during BCD’s ITS is below the softcap, the investors will get the totality of their contribution back. These rules will be fully followed by BCDT’s token smart contract.

Tokens' sale: settings

The hardcap (maximum funding goal) is equal to the softcap (minimum funding goal), either 1800 ETH. Unsold tokens will be burned.

- **Time of the ITS:** Presale will start December 2017;
- **Number of tokens for sale:** 28,080,000 BCDT tokens;
- **ITS' maximum sale revenues (hardcap):** 1,800 ETH;
- **ITS' minimum sale revenues (softcap):** 1,800 ETH;
- **ETH / BCDT's exchange rate:** 1 ETH = 13,000 BCDT tokens.

If the total amount raised during BCD's ITS is below the softcap, the investors will get the totality of their contribution back. These rules will be fully followed by BCDT's token smart contract.

Incentive Program: depending on the ITS stage, bonus BCDT tokens will be offered:

- Presale: 20% bonus. **The softcap rule includes presale;**
- First round: 10% bonus.
- Second round: no bonus.

Presale and all rounds managed by smartcontract, contributors have to be whitelisted through a KYC. More information on www.bcdiploma.com.

ITS's completion

The ITS will end when all the tokens are sold, and, failing that, after the second round is over.

If, at the end of the ITS, the minimum sale revenues isn't achieved, the totality of the funds raised will be refunded to the BCDT's buyers.

If, at the end of the ITS, the minimum sale revenues is reached, then the smart contract of the BCDT token will proceed to the issuing of the saved tokens. Those tokens will be allocated to the community and to the BCD team, according to the proportions described below.

The tokens allocated to the BCD founders will be blocked during one year.

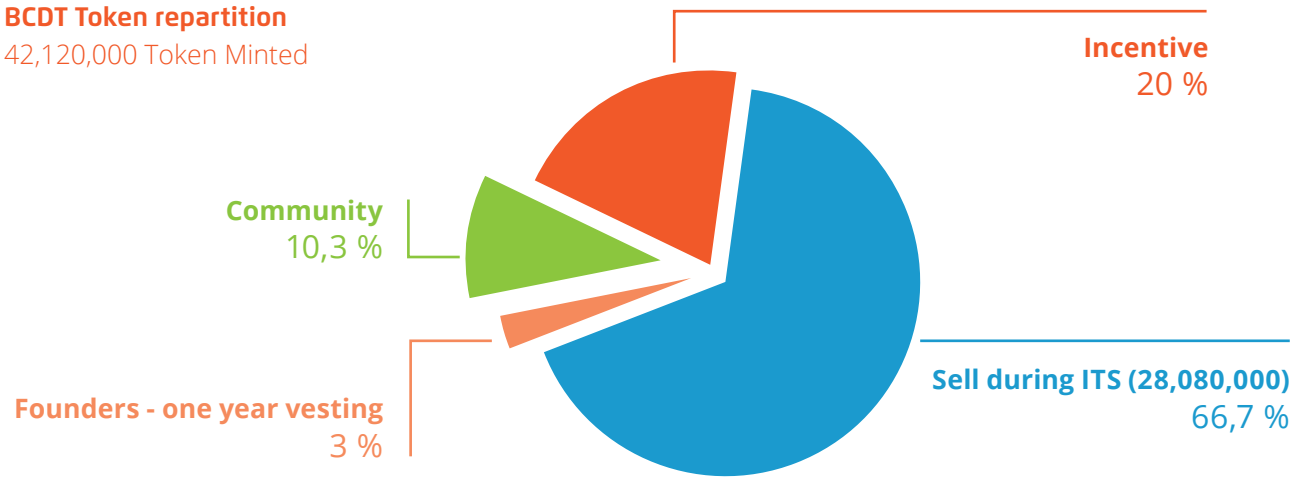
BCD will not create any new BCDT tokens after the BCDT Initial Token Sale.

Tokens distribution

Our goal is to guarantee a BCDT token distribution as wide and as fair as possible.

Based on a token sale of 1,800 ETH:

- **Initial BCDT tokens' sale offering:** 28,080,000 BCDT;
- **BCDT Tokens set aside:** 20% of tokens minted;
- **BCDT tokens allocated to community members promoting BCD, including team, excluding founders:** 10,3% of tokens minted. The allowance will be at BCD's sole discretion;
- **BCDT tokens allocated to BCD's founders:** 3% of tokens minted.



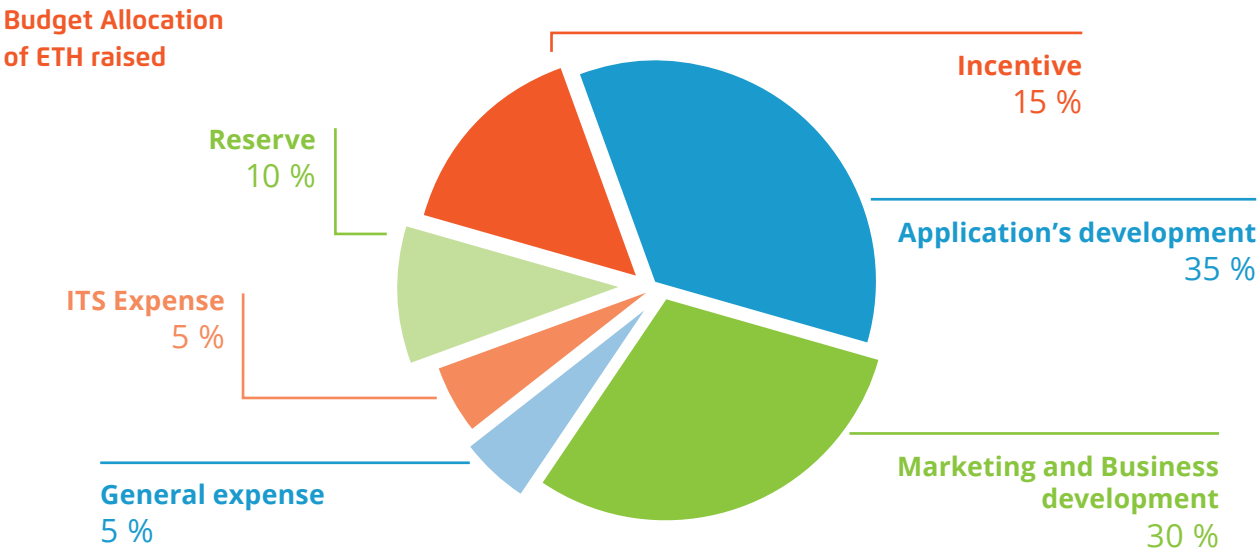
How are we going to use the funds ?

To implement BCD's strategy during the first 36 months (see the "strategy" section), we plan to use the ITS' tokens sale revenues as follow:

- **Application's development:** 35% of the revenues generated by the tokens' sale ;
- **Marketing and Business development:** 30% of the revenues generated by the tokens' sale ;
- **Incentive campaign:** 15% of the revenues generated by the token's sale.

  In 2018, BCD's goal is to publish, on every continent, the diplomas of the most important schools, offering them an incentive program up to the task. This program will be the object of a massive marketing campaign toward:

  - The education field players;
  - Graduates;
  - Recruiting field players (LinkedIn, head-hunters, job search tools);
- **Reserve:** 10% of the revenues generated by the tokens' sale will be kept as long-term savings;
- **ITS expense:** 5% of the revenues generated by the tokens' sale will be reserved for ITS advisors bounties, workers bounties, legal and IT charges refund;
- **General expense:** 5% of the revenues generated by the tokens' sale. **BCD is a lean, cost-effective start-up and will continue to be so in the future.**



CRYPTO ALGO APPENDIX

Technical features

The encryption algorithm we use, **AES – 256 – GCM,** is standardized:

- AES-256: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf
- GCM mode: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf

The AES-GCM is often used and is referenced for many security protocols:

- IPSEC: RFC 4106
- IKEv2: RFC 5282
- TLS: RFC 5288
- CMS: RFC 5084
- SSH: RFC 5647
- SRTP: RFC 7714

The AES is recommended for usage exceeding 2030 with a 128-bit key. For a 256-bit key, it is among the safest standardized cryptography algorithms.

A standardized derivation **algorithm KBKDF** (Key-Based Key Derivation Functions) will be used;

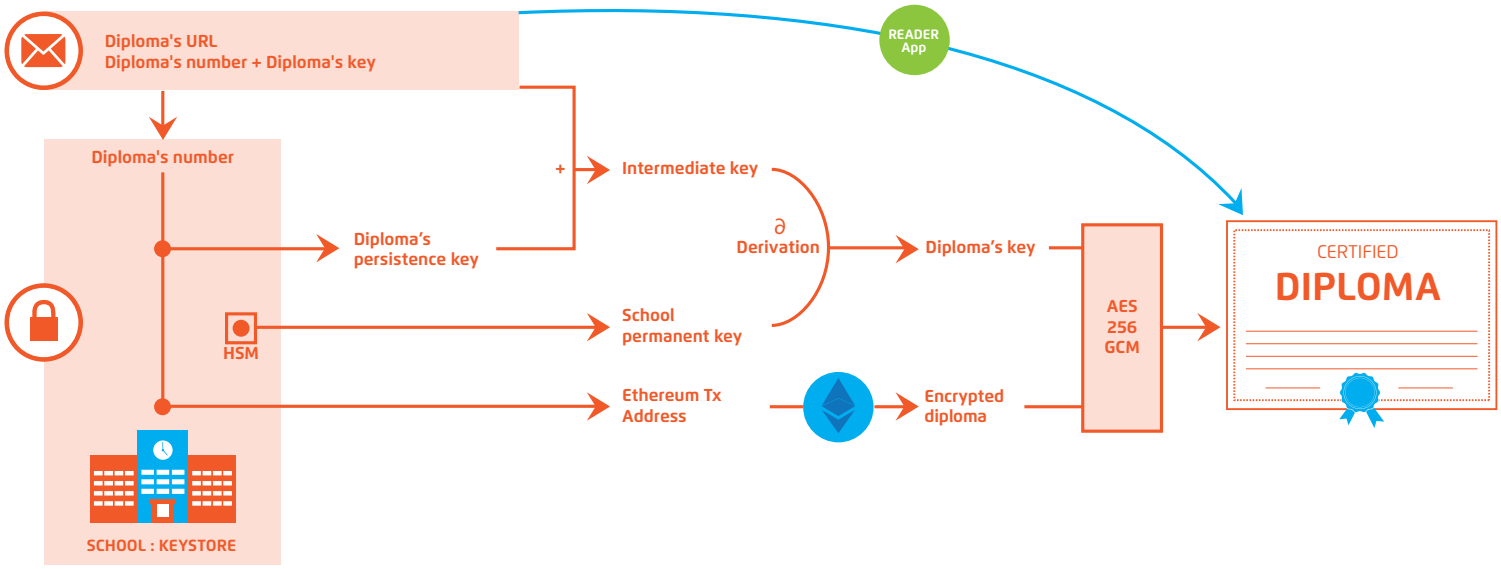
Key sizes:

- MasterKey and KAES: 256-bit AES keys;
- Nonce: random value of 96-bit;
- RND: 96 alphanumerical octets base64 encryption of a 576-bit random value.

For a school, we will create a secured environment (Key store):

- An AES MasterKey, in a **HSM** (Hardware Security Module): it will be used to derive the RND intermediate keys;
- A MasterNonce random value;
- A CtrDerivation derivation meter: updated every issuance;
- A “persistence keys” table: [IdData, RND1, Nonce, idETH].

Architecture



Glossary for the algorithm description:

- Diploma's number = idData
- Graduate's key = RND2
- Diploma's persistence key = RND1
- School's permanent key = MasterKey
- Intermediate key = RND
- Diploma's key = KAES
- Encrypted diploma = EncData
- Diploma = PlainData

Double pipe || symbolizes concatenation.

Encryption (via Crypto App)

The manager files the diplomas Data_1, Data_2, ..., Data_n.
For each data:

1. A random value IdData is generated
2. A random value RND1 is generated and saved in the "persistence keys" table (IdData entry)
3. A random value RND2 is generated
4. A KAES encryption key is generated, by-product of the MasterKey key and random RND1 et RND2 values: KAES = KBKDF(MasterKey, RND1 | | RND2)
5. Nonce calculation = MasterNonce + CtrDerivation
6. Safeguarding data (encryption, authentication); EncData = AES_256_GCM_Enrypt (KAES, Nonce, Data)
7. KAES deletion
8. Incrementation and registration of CtrDerivation: CtrDerivation = CtrDerivation +1
9. Diploma's URL is generated: https://serveur_READER_APP/IdData || RND2
10. RND2 deletion
11. Nonce registration in the "persistence keys" table (IdData entry)
12. EncData data writing in the Ehtereum's transcription
13. As a result, retrieval of the matching transaction ID idETH = writeETH(EncData)
14. idETH writing in the IdData's table

All the random values are generated using the HSM's random number generator, which offers a better quality than a software version. The MasterKey won't be used above 1.000.000 of keys' derivation. A new MasterKey will be generated each time this number is reached.

Reading (via Reader App)

Someone who wants to read the data goes to the HTTPS website:
https://serveur_READER_APP/ IdData||RND2
The Reader App Application goes then through the following steps:

1. IdData value retrieval
2. idETH value reading in the “persistence keys” table (IdData entry)
3. Retrieval of the idETH’s referenced transaction on Ethereum and EncData’s value retrieval
4. RND1 value reading in the “persistence keys” table (IdData entry)
5. Reader App application retrieves the RND2 value
6. Encryption key calculation KAES = KBKDF(MasterKey, RND1 || RND2)
7. Memory deletion of idETH, RND1 et RND2
8. Nonce value reading in the “persistence keys” table (entry IdData)
9. Data decryption PlainData = AES_256_GCM_Decrypt(KAES, Nonce, EncData)
10. Memory deletion of KAES, EncData, Nonce
11. Showing of the PlainData data to the claimant
12. Memory deletion of the PlainData

TERMS AND CONDITIONS

These Terms and Conditions (hereinafter **"the Terms"**) are entered into between the Company Blockchain Certified Data SAS, with registered office at 84 avenue Albert 1er, 92500 Rueil Malmaison, France, registered in Nanterre Trade and Companies Register under number 833 138 951 represented by Luc Jarry-Lacombe, duly authorized for the purposes herein, (hereinafter **"BCD"** or **"the Company"**), and the natural or legal person using the Company's services, (hereinafter the **"Purchaser"**).

Article 1 – General Provisions

These Terms apply fully and automatically to all the tokens offered for sale by BCD as part of BCDiploma Initial Token Sale (hereinafter the **"Commercial Operation"** or **"ITS"**) towards its Purchasers.

BY CLICKING ON "I HEREBY CERTIFY THAT I HAVE READ, UNDERSTOOD AND EXPRESSLY ACCEPT BCD WHITE PAPER AND TERMS AND CONDITIONS", THE PURCHASER ACCEPTS AND ACKNOWLEDGES THAT HE IS ENTERING INTO A BINDING CONTRACT WITH BCD AND AGREES TO ABIDE BY ALL THE PROVISIONS.

IF THE PURCHASER DOES NOT UNDERSTAND THE WHITE PAPER AND/OR DOES NOT AGREE WITH ALL THE TERMS AND CONDITIONS, HE SHOULD NOT PARTICIPATED IN THIS ITS, USE BCD PLATFORM NOR ITS SERVICES.

BCD RESERVES THE RIGHT TO CHANGE, MODIFY, ADD OR REMOVE ANY CONTENT OF THE TERMS AT ANY TIME, FOR ANY REASON. THE PURCHASERS SHALL REVIEW THE TERMS PERIODICALLY AS THE PURCHASERS WILL BE DEEMED TO HAVE ACCEPTED THESE MODIFICATIONS AS SOON AS THEY VISIT AND USE THE WEBSITE(S) FOLLOWING PUBLICATION OF SAID MODIFICATIONS.

All the details on the Commercial Operation are available on the following official website: https://www.bcdiploma.com.

These Terms prevail over all other documents issued either by the Purchaser or by BCD and, as from their date of entry into force, shall apply to all purchases, and are deemed to be unconditionally accepted by the Purchaser. Any derogation from the Terms herewith will require the express agreement of both parties. Any other document (e.g. sales prospectus, quotation, presentation, etc.) is therefore given for information only and shall not constitute a contractual document that commits BCD, which may therefore withdraw or modify such documents, without entitling the Purchaser to any compensation. This clause is a key requirement for BCD's consent.

BCD reserves the right, with no prior notice, for any reason, to block, limit or restrict access to the website, in whole or in part, temporarily or permanently. BCD may not be held liable for the website being unavailable or difficult to connect to, regardless of the consequences for the Purchasers.

Article 2 – Eligibility and pre-requisites

Participation in the ITS is reserved for natural or legal persons acting within the scope of their professional activities. Any natural person acting on a non-professional basis as a simple consumer within the meaning of EU Directive 2011/83/EU relating to consumer rights is excluded from the ITS.

Participants cannot contribute to the ITS if there are applicable legal restrictions in their country of residence. It is the responsibility of each participant to know these laws regarding their participation in the ITS.

Due to legal restrictions, the ITS is not accessible for any person (including a legal entity) who is considered a "U.S. person", a Canadian, a Singapore or a Chinese citizen.

Documents linked to the issue of BCDTs may not be transmitted or distributed to a "U.S.person", a Canadian, a Singapore or Chinese citizen or to a mail or email address in the United States of America, Canada, Singapore or People's Republic of China. It is prohibited to transmit, distribute or reproduce documents linked to the issue of BCDTs to or for a "U.S. person", Canadian, Singapore or Chinese citizen, or within the territories of the United States of America, Canada, Singapore, and People's Republic of China in whole or in part.

To ensure their eligibility for the purchase of BCDT tokens, **the Purchaser declares that he is not a Canadian, Singapore or Chinese citizen, nor a "U.S. person",** (within the meaning of Regulation S of the Securities Act 1933 in U.S. law), i.e.:

- Any private individual resident in the United States;
- Any partnership or business organized or established under U.S. law;
- Any property of which the executor or administrator is a U.S. citizen;
- Any trust of which a proxy is an American citizen;
- Any agency or branch of a foreign entity located in the United States;
- Any non-discretionary account or similar account (other than a trust or property) held by a trader or other trustee for the benefit of or on behalf of a U.S. citizen;
- Any discretionary account or similar account (other than a trust or trust) held by a trader or other trustee, that is organized, established or (if a private individual) resident in the United States; and
- Any partnership or company if:
  a) It is organized or established under the law of a foreign jurisdiction; and
  b) It is formed by a U.S. citizen primarily for the purpose of investing in securities not listed under the U.S. Securities Act, unless it is organized or established, and owned, by accredited investors who are not private individuals, trusts or properties.

The sale of tokens under this Commercial Operation is reserved for experienced professionals who have an in-depth understanding of the nature of the products and services they are purchasing, a firm grasp of the technologies on which they are based (in particular blockchain), and who are fully aware of all the associated risks as described hereinafter.

The Purchaser is solely liable for determining which legal, accounting, financial and fiscal conditions of any nature it is required to comply with in order to participate in the Commercial Operation, in accordance with the laws and regulations applicable in his country of residence. BCD may not be held liable for the Purchaser's filing obligations in the country in which it is domiciled. The same applies to any tax or charge that would be payable by the Purchaser, in relation to the purchase, ownership, use or passing of his tokens.

Article 3 – Information and knowledge of BCD Project and the Commercial Operation by the Purchaser

By adhering to these Terms, the Purchaser expressly acknowledges having read and understood the White Paper, BCD Project and business model and been comprehensively informed about the Commercial Operation.

The Purchaser is deemed to be fully aware of all the legal norms and technical constraints relating to the purchase, possession, functionality, use, storage, transmission mechanisms and intricacies associated with tokens and cryptocurrencies (like Bitcoin and Ether) based on blockchain technologies, blockchain-based software systems, and to the services offered by BCD Platform.

The Purchaser expressly acknowledges the random nature of this ITS and BCD project as presented in this document and that this project may not come to fruition or may have to be abandoned due to technical, legal or regulatory constraints, without the BCDT tokens being used.

Article 4 – KYC Procedure and contribution process

4.1 The "Know Your Customer" (KYC) procedure is instrumental in the prevention against money laundering and terrorist financing. By obtaining information on the identity and source of the funds of Purchasers, BCD would like to protect itself and protect BCD Platform from being used to conceal illegally-obtained funds.

This is the reason why Purchasers and their Ethereum address **("Contribution address")** will be white-listed through a KYC procedure. This KYC procedure will be performed through the form provided on the website www.bcdiploma.com.

Any contribution in this ITS will be accepted by the ITS Smart Contract if and only the Purchaser's Contribution address has been white- listed.

4.2 For contributions strictly greater than 10 ETH, as part of the KYC procedure (hereinafter "KYC 1"), the following information and documents shall be provided by any Purchaser willing to access to the ITS:

(i) Where the Purchaser is a natural person (acting within the scope of his professional activities): Family name, first name, country and residential address, email address, nationality, ID card/Passport scan, photo "selfie" on which appear simultaneously the face of the contributor and the registered ID card, address from which the funds will be disbursed;

(ii) Where the Purchaser is a legal person: Organization/Company name, headquarters registered address, scan of business licence, tax identification number, address from which the funds will be disbursed and for its legal representative: Family name, first name, ID card/Passport scan, photo «selfie» on which appear simultaneously the face of the contributor and the registered ID card.

Purchaser shall then:

- Declare that he is not a Canadian, Singapore or Chinese citizen, nor a "U.S. person";
- Tick the box "I HEREBY CERTIFY THAT I HAVE READ, UNDERSTOOD AND EXPRESSLY ACCEPT BCD WHITE PAPER AND ITS TERMS AND CONDITIONS";
- Provide his Contribution address;
- Provide the **indicative** amount of his contribution in ETH.

Each step needs to be followed and complied with by the Purchaser.

BCD will then proceed with the KYC 1 verification. Once the Purchaser's identity has been verified, his Contribution address will be added to the ITS White List 1 and BCD will send him a message for the Purchaser to confirm and finalize his contribution in the ITS.

4.3 For contributions lower than or equal to 10 ETH, as part of the KYC procedure (hereinafter "KYC 2"), the following information shall be provided by any Purchaser willing to access to the ITS: Family name, first name, email address, address from which the funds will be disbursed.

Purchaser shall then:

- Declare that he is not a Canadian, Singapore or Chinese citizen, nor a «U.S. person»;
- Tick the box "I HEREBY CERTIFY THAT I HAVE READ, UNDERSTOOD AND EXPRESSLY ACCEPT BCD WHITE PAPER AND ITS TERMS AND CONDITIONS";
- Provide his Contribution address;
- Provide the indicative amount of his contribution in ETH.

Each step needs to be followed and complied with by the Purchaser.

BCD will then proceed with the KYC 2 verification. Once the Purchaser's identity has been verified, his Contribution address will be added to the ITS White List 2 and BCD will send him a message for the Purchaser to confirm and finalize his contribution in the ITS.

4.4 In any case, **BCD will NOT accept "anonymous purchasers" or those using aliases, fictitious names or false identity in general.**

BCD may request from the Purchaser additional information and/or documents to evidence his identity and/or source of funds or to ensure the accuracy of the details they have supplied. If the Purchaser refuses to provide such additional information or documents, BCD may, at its sole discretion, refuse the purchaser's contribution and may not be held liable for such refusal.

BCD may, at its sole discretion, refuse purchasers who are (or may be) suspects of being involved in money laundering, or any sort of criminal activities, related to drug trafficking, terrorism and organized crime. The same applies to potential purchasers holding businesses that due to the nature of the business make it impossible to verify its legitimacy or that of the funds being inconsistent with their financial status.

4.5 ITS address will be made available to the public on www.bcdiploma.com. Only Purchasers that passed the KYC procedure as described hereinabove will be technically allowed to make their contribution.

4.6 Once the Purchaser's Contribution address has been white-listed, the Purchaser shall then provide the final amount of his contribution in ETH according to the threshold indicated during the KYC procedure (i.e lower than or equal to 10 ETH or strictly greater than 10 ETH).

- If the Purchaser is part of the White List 1, he may make as many contributions as he wants.
- If the Purchaser is part of the White List 2, he may make several contributions but in any case, the cumulated amount of his contributions will be capped at 10 ETH.

4.7 Failure for the Purchaser to provide the final amount of his contribution in ETH at the address specified on www.bcdiploma.com, the Purchaser will not be able to receive BCDT tokens.

4.8 Purchaser's contribution in ETH is deemed to be irrevocably binding upon validation of the final contribution by the Smart Contract. As from this date, a contribution may no longer be cancelled or amended. Purchasers will then receive BCDT tokens.

4.9 BCDT tokens will be made available in the Purchaser's wallet immediately after the contribution and will be transferable twelve (12) days after the end of the ITS.

4.10 BCDT period of validity, during which they can be used, is not time-dependent. Tokens cannot be deleted due both to their strictly decentralized nature and to the fact that, once issued, they are no longer under BCDiploma's control. They would, in any case, remain the property of their owner.

4.11 In any event during the KYC procedure and contribution process, the Purchaser shall notify in writing BCD concerning any information likely to impact on its contribution directly or indirectly (contactus@blockchaincertifieddata.com). Failure to do this, BCD may not be held liable in any way in this regard.

Article 5 – BCDT Tokens

The Commercial Operation involves the sale of virtual tokens, referred to as **"BCDT Tokens"** or **"BCDT"**).

5.1 Tokens Role and Attributes

BCDT tokens will provide their owners with access rights to use the BCD Platform (and its service), once it has been designed, developed and deployed and provided that BCD Platform operates on a permanent basis.

The Purchasers' attention is therefore drawn to the fact that purchasing tokens during the Commercial Operation does not confer automatic rights to access to BCD Platform and service in the future. BCDT tokens may not be used before the effective implementation of BCD Platform.

UNLESS OTHERWISE SPECIFIED HEREIN, BCDT TOKENS WILL NOT BE REIMBURSED IN THE EVENT THAT THE BCD PLATFORM IS NOT ULTIMATELY DEVELOPED, OR DOES NOT OPERATE ON A PERMANENT BASIS. BCDT OWNERS ACKNOWLEDGE THAT THIS IS A SIGNIFICANT RISK THAT THEY ACCEPT.

The Purchaser acknowledges that he is fully aware that:

- **a BCDT does not represent an investment or a financial instrument** within the meaning of EU Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 relating to markets in financial instruments: a BCDT token confer no direct or indirect right to BCD's capital or income, nor does it confer any governance right within BCD;
- **a BCDT is not proof of ownership or a right of control:** Control over a BCDT does not grant the individuals any asset or share in BCD, or in the BCD Platform. A BCDT does not grant any right to participate in control over BCD's management or decision-making set-up, or over the BCD Platform;
- **a BCDT is not an electronic currency** within the meaning of EU Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions: BCDT tokens are not accepted (and have no use) outside the BCD Platform and a BCDT does not have a fixed exchange value equal to the amount delivered at the time of its issue;
- **a BCDT is not a payment** service within the meaning of EU Directive (2007/64/EC) of 13 November 2007 relating to payment services in the internal market, nor within the meaning of the (EU) Directive relating to payment services 2 (DSP 2) n° 2015/2366 of the European Parliament and of the Council of 25 November 2015: the ITS does not involve the purchase/sale of cryptocurrencies and BCD's business does not consist in receiving currencies against the delivery of cryptocurrencies;
- **a BCDT is a cryptographic token used by the BCD Platform to issue diplomas.**

5.2 BCDT token issuance and distribution

ITS timeline and instructions are posted on the Commercial Operation website at www.bcdiploma.com.

BCDT tokens will be issued by a technical process referred to as "blockchain". This is an open source IT protocol over which BCD has no proprietary rights or liability in terms of development and operation.

The token distribution mechanism will be controlled by 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. The tokens will meet the 'ERC20' standard (https://theethereum.wiki/w/index.php/ERC20_Token_Standard), and will be subject, inter alia, to the operating conditions of the Internet computer network and the Ethereum blockchain protocol.

BCD has no control, right or liability over the operation of the Internet computer network and the Ethereum network and protocol.

The ITS will end if and when all the BCDT tokens are sold or after the second round is over. If, at the end of the ITS, the minimum sale revenues as indicated in the White Paper has not been reached, the totality of the funds raised will be refunded to the Purchasers (provided that the contributions process has been completed as per the procedure explained hereinafter).

If, at the end of the ITS, the minimum sales revenues has been reached, then the tokens will be issued by the Smart Contract pursuant to Article 4 and distributed according to the proportions described in the White Paper.

BCD may not be held liable in any way for any feature that might affect the token distribution or ownership of the tokens sold, or that might hamper the Purchaser's ability to use the tokens, including display of the tokens in an electronic wallet compatible with the ERC20 token standard, or the assignment of these tokens to a third party.

The acquisition of tokens by transferring tokens or crypto-currencies to the Smart Contract comes under the Purchaser's sole liability and will be subject to the terms and conditions of the protocol and the Ethereum network.

As BCDT tokens are issued under a Smart Contract, BCD is not obliged to reimburse or compensate in any way any Purchaser whose BCDT tokens have not been issued by the Smart Contract for any reason.

Once issued, the tokens may be assigned or transferred to third parties by the Purchaser, in whole or in part, at their sole discretion, in return for payment or free of charge. However, the Purchaser shall be solely and fully liable for the conditions and consequences of such an assignment or transfer of the tokens in their possession. In particular, given that BCD will have no control over such transactions, the Purchaser may not claim against BCD for any loss of their tokens due to any error of any kind that may occur during the transfer.

The BCD cofounders warrant that they will not purchase BCDT in their own ITS or from any third party, or acquire BCDT in any manner, during the period of the ITS.

Article 6 – Limitations of Use

Prior to any contribution, the Purchaser acknowledges and accepts that BCDT tokens do not, under any circumstance, represent any form of investment or financial investment and agrees not to attempt to divert the tokens function for speculative purposes.

The Purchaser acquires BCDT tokens primarily to support the development, testing, deployment and operation of BCD project, being aware of all the risks associated with this project and Commercial operation as set forth hereinafter.

The Purchaser also agrees not to use the Commercial Operation website, BCD Platform, the issued tokens and, more generally, any content or service provided to the Purchaser by BCD that does not comply with the objectives and methods set out in the White Paper and/or in these Terms. Under no circumstances may BCDT token be used for other services than those offered by BCD Platform. BCD is solely responsible for deciding whether to provide the service to token owners, within the technical, legal, economic or other constraints imposed by third parties or by BCD itself on its operations.

In particular, the Purchaser agrees not to modify, interfere with, deactivate or saturate, nor to breach the security of or impair data integrity and confidentiality in relation to any service offered by BCD.

Purchaser shall not obtain or use BCDT for any illegal purposes wherever in the world, in particular for money laundering and/or terrorism.

Article 7 – Cancellation - Refund policy

ALL PURCHASES OF BCDT TOKEN COMPLETED PURSUANT TO ARTICLE 4 OF THESE TERMS ARE FINAL. PURCHASES OF BCDT TOKEN ARE NON-REFUNDABLE. BY PURCHASING BCDT TOKEN, THE PURCHASER ACKNOWLEDGES THAT NEITHER BCD PLATFORM NOR ANY OTHER OF THE BCD TEAM & PARTIES ARE REQUIRED TO PROVIDE A REFUND FOR ANY REASON, AND THAT THE PURCHASER WILL NOT RECEIVE MONEY OR OTHER COMPENSATION FOR ANY BCD THAT IS NOT USED OR REMAINS UNUSED.

Besides, as the tokens offered for sale are deemed intangible property, having no value or functionality other than the BCD Platform service, no guarantee is attached to them following issuance.

No final contribution confirmed on the BCD website may be subsequently canceled or refunded.

The Purchasers acknowledge that they are fully aware that they will not be entitled to claim any full or partial reimbursement under any circumstances whatsoever.

Article 8 – Risks inherent to bcd ITS

The Purchaser understands that BCDT tokens, blockchain technology, Ethereum protocol, Ether and other associated and related technologies are new and untested and outside of BCD's exclusive control and adverse changes in the technology, broadly construed, will excuse BCD's performance under these Terms.

Risks inherent to BCD Project and Commercial Operation may be various. As mentioned

hereinabove, the Purchaser acknowledges that he has been warned of the following risks, that he understands and accepts purchasing BCDT in consideration of these risks (which are not exhaustive).

7.1 Legal risk or risk of adverse regulatory intervention in one or more jurisdictions around the world

Blockchain technologies, cryptocurrencies and projects financing through cryptocurrencies have been the subject of close scrutiny by various regulatory bodies around the world, including within the European Union and France. The Commercial Operation has been structured to comply with EU law applicable at the time of the ITS.

Operation of BCD Platform and BCDT tokens may be impacted by the promulgation of restrictive laws, the publication of restrictive or negative opinions, the issuing of injunctions by national regulators, the initiation of regulatory actions or investigations, including but not limited to restrictions on the use or ownership of digital/cryptographic tokens such as BCDT, which may prevent or limit the development of BCD and its activities. This uncertainty significantly adds up to risks connected with the acquisition and use of BCDTs.

Given the lack of crypto-currency qualifications in most countries, each Purchaser is strongly advised to carry out a legal and tax analysis concerning the purchase and ownership of BCDT tokens according to their nationality and place of residence.

7.2 Risks associated with the ITS documentation

The White Paper is the only documentation that introduces BCD Commercial Operation and exposes BCD project. Such documentation does not comply with any legal requirement as there is no regulation at the time of the ITS. The Purchaser acknowledges and accepts that the White Paper may potentially contain inaccuracies, errors or omissions and express BCD's opinions and forecasts.

The ITS documentation has not been subject to prior approval from any regulatory bodies such as *L'Autorite des Marches Financiers* (AMF) in France.

7.3 Risks associated with the Ethereum protocol

Both BCDT tokens and the BCD Platform are based on the Ethereum protocol. Therefore, any malfunction, unplanned function or unexpected operation of the Ethereum protocol may cause the BCD Platform or BCDT to malfunction or operate in an unexpected or unintended manner.

Besides, the Purchaser understands and accepts that an upgrade or split of the Ethereum protocol may occur in the future (hard-fork) and that BCD has no control over it. The Purchaser may no longer be able to use his BCDT and/or his BCDT may lose their functionality in full. Ether, the native Ethereum Protocol account unit may itself lose value in a similar way to BCDT.

For more information on the Ethereum protocol, please visit the Ethereum website: www.ethereum.org.

7.4 Risk of a lack of interest in the BCD Platform or distributed applications

There is a possibility that the BCD Platform may not be used by a large number of companies, individuals and other organizations, and that there may be limited public interest in the creation and development of distributed applications. Such a lack of interest could have an impact on the development of the BCD Platform and, therefore, on the uses or potential value of BCDT tokens.

7.5 Risk of loss of BCDT due to loss of credentials

The Purchaser can only access the BCD account using the credentials selected by the Purchaser. The Purchaser understands that if his credentials (and in particular his private key) are lost or stolen, BCDT associated with his account will be unrecoverable and permanently lost. It is thus recommended to Purchasers to store their

credentials securely in one or more backup locations that are geographically separated from the work location and not to share his credentials with anybody. There is no recovery mechanism for lost keys, so BCD will not be able to help the Purchaser retrieve or reconstruct a private key and/or provide the Purchaser with access to any lost BCDT.

7.6 Non-release, software and technical risks

Some BCD platform features are currently under development. As a consequence, the Purchaser accepts that the development may not succeed, that BCD Platform may never be released and operational, even though BCD makes reasonable efforts to complete such platform, that the Platform may be subject to software and/or technical risks, or that features may never be installed on the Platform.

7.7 Risk that the BCD Platform, as developed, does not meet Purchaser expectations

The BCD Platform is currently under development and may undergo significant changes prior to its launch (for technical, financial, commercial, marketing, legal or regulatory reasons). As such, Purchaser expectations concerning the BCD Platform or BCDT token may be met on the launch date.

7.8 Risks of theft and hacking

Hackers or criminal groups or organizations may attempt to interfere with the BCD Platform or the availability of BCDT tokens in several ways including, but not limited to, denial of service attacks, smurfing, Sybil attacks, malware attacks or consensus-based attacks.

Besides, the BCD Platform is based on open source software. There is a risk that third parties, may intentionally or unintentionally introduce weaknesses or bugs into the BCD Platform, by interfering with the use of or causing loss of BCDT.

7.9 Risk of capital loss

Capital invested in BCD ITS is not guaranteed. Investing in tokens entails a significant capital risk, which the Purchaser acknowledges and accepts.

7.10 Risk of an uninsured loss

Unlike bank accounts or accounts in other regulated financial institutions, funds held through BCD Platform or Ethereum network are generally uninsured. At present, there are no public or private insurance agents providing Purchasers with coverage against a loss of BCDT or a loss of value.

7.11 Internet transmission risks

The Purchaser acknowledges that there are risks associated with using BCD Platform or BCDT tokens including, but not limited to, the failure of hardware, software, and Internet connections. The Purchaser acknowledges and accepts that BCD shall not be responsible for any communication failures, disruptions, errors, distortions or delays the Purchaser may experience when using the BCD website or ITS website and tokens, howsoever caused.

7.12 Unforeseen risks

Crypto-currencies and cryptographic tokens are a new, untested technology. In addition to the risks stipulated above, there are other risks that the BCD team cannot predict. Risks may also occur as unanticipated combinations or as changes in the risks stipulated herein.

Article 9 – Representations and Warranties

EXCEPT AS EXPRESSLY STATED IN THIS AGREEMENT, BCD PLATFORM, BCDT TOKENS, INCLUDING ALL FUNCTIONS THEREOF, ARE PROVIDED ON AN "AS IS" AND/OR "UNDER DEVELOPMENT" BASIS, WITHOUT REPRESENTATIONS OR WARRANTIES OF ANY KIND WHATSOEVER, EXPRESS OR IMPLIED TO THE EXTENT PERMITTED BY LAW, INCLUDING, BUT NOT LIMITED TO, ACCURACY AND COMPLETENESS OF ANY INFORMATION PROVIDED IN THE WHITE PAPER AND/OR IN THESE TERMS, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, THAT BCDT TOKENS ARE USED AND HOLD AT THE SOLE RISK OF THE PURCHASER, THAT BCD PLATFORM, BCDT TOKENS AND/OR THE UNDERLYING BLOCKCHAIN PROTOCOL WILL BE AVAILABLE

UNINTERRUPTED AND TIMELY, WILL BE FREE FROM DEFECTS, ERRORS AND BUGS, AND/OR WILL BE ENTIRELY SECURE.

By participating in the ITS, the Purchaser represents and warrant that he:

- Is authorised and have full power to purchase BCDT according to the laws applicable in his jurisdiction;
- Is not a Canadian, Singapore or Chinese citizen, nor a «U.S. person»
- Is not acting for the purpose of speculative investment;
- Will not use the ITS for any illegal activity, including but not limited to money laundering and financing of terrorism;
- Is solely responsible for determining whether the acquisition of BCDT is appropriate for him and for seeking any tax, legal, accounting or financial advice in order to participate to the ITS;
- Is acquiring BCDT for a future use of BCD Platform;
- Understand the risks associated with the ITS (including the risks related to the non-development/non-release of BCD Platform and services);
- Understand the use of cryptocurrencies and its associated risks.

Article 10 – Limitations of Liability

IN NO EVENT WILL BCD BE LIABLE TO THE PURCHASER FOR INCIDENTAL, INDIRECT OR CONSEQUENTIAL LOSS OR DAMAGE, INCLUDING ANY LOSS OF REVENUE, CONTRACTS OR OPPORTUNITIES OR FAILURE TO REALIZE EXPECTED PROFITS OR SAVINGS, LOSS OR CORRUPTION OF ANY DATA, DATABASE OR SOFTWARE, DECISIONS OR SANCTIONS FROM A REGULATORY BODY OR A COURT.

BESIDES , BCD SHALL NOT BE HELD LIABLE FOR ANY OF THE FOLLOWING:

a) Use of BCD Platform and services or BCDT tokens that are not compliant with these Terms ;

b) Non-performance, failure, malfunction or unavailability of BCD Platform and services due to a third party, the Purchaser, a third-party product, or the Purchaser's breach of its obligations;

c) Loss, disclosure or unlawful or fraudulent use of user sign-ons by the Purchaser or third parties;

d) Suspension of access or temporary or permanent suspension of BCD Platform and services (in particular, arising from a request issued by an administrative or judicial authority, or notification received from a third-party);

e) Loss, alteration or destruction of all or part of the content (information, data, applications, files or other items) hosted on the infrastructure, insofar as BCD is not responsible for managing the continuity of Purchaser activities, and data backups in particular;

f) Mismatch between BCD Platform and services and the Purchaser's needs;

g) Security incidents relating to use of the Internet, concerning in particular the loss, alteration, destruction, disclosure or unauthorized access to the Purchaser's data or details on or via the Internet;

h) Damage to systems, applications and other items installed by the Purchaser ;

i) Failure of Ethereum or any other blockchain protocol or smart contracts.

Article 11 – Intellectual property

BCD is the licensee or owner of all of BCD intellectual property rights existing prior the date of this ITS.

Ownership of any of BCD Platform or BCDT tokens intellectual property or know-how used, developed, created or any documentation will vest with BCD at all times.

BCD grants to the Purchaser a royalty-free, non-exclusive, non-transferable, worldwide right to use BCD Platform and its services.

The Purchaser acknowledges and accepts that it shall not:

(i) Distribute, export, translate, transmit, merge, transfer, modify, adapt, hypothecate, encumber, create, derivative works of, loan, rent, lease, share, resell any of BCD Platform, in whole or in part;

(ii) Remove or modify any proprietary notices of BCD Platform; or

(iii) Reverse engineer, decompile, disassemble or otherwise attempt to discover the source code, object code or underlying structure, ideas, algorithms of BCD Platform or BCDT tokens or any documentation provided by BCD (except in accordance with the provisions of the applicable law).

The Purchaser shall take all necessary precautions to prevent third parties from using BCD Platform or BCDT tokens or any documentation provided pertaining thereto in any way that would constitute a breach of these Terms or BCD intellectual property rights.

The Purchaser shall not license, sublicense, or otherwise grant any intellectual property rights pertaining to BCD Platform or BCDT tokens.

Article 12 – Security

The Purchaser shall implement reasonable and appropriate measures designed to secure access to (i) any device associated with the email address associated with his account, (ii) private keys required to access any relevant Ethereum address, and (iii) Purchaser username, password and any other login or identifying credentials.

In the event the Purchaser suspects a security breach in any of the abovementioned, he shall inform BCD immediately, so BCD can take all required and possible measures to secure the Purchaser account, the website, BCD Platform and systems as whole.

The Purchaser will assume full responsibility for the consequences of any theft, malfunction or misuse of BCD Platform or BCDT tokens acquired, as a result of a lack of security or any use by any person to whom the Purchaser has provided his credentials.

Article 13 – Protection of personal data

Pursuant to the EU Data Protection Directive (95/46/EC) and the subsequent General Data Protection Regulation (EU) 2016/679 that will apply from 25 May 2018, BCD shall implement appropriate measures to prevent the unauthorised use or disclosure of any personal data made available to and processed by BCD in connection with BCD Platform and the ITS (**"Covered Data"**).

To this end, BCD has implemented and maintained physical and technical measures that reasonably and appropriately protect the confidentiality, integrity, security and availability of the Purchaser Covered Data.

Only the minimum and necessary amount of personal data of the Purchaser is collected by BCD at the time of the KYC procedure to complete the ITS and to comply with the best practices recommended by the regulatory bodies. Besides, only those personnel of BCD that have been duly authorized will access the Covered Data and such access is strictly limited to ensure the operational process of the ITS and/or the security of the Covered Data.

Personal data collected from the Purchaser on the forms available on the website are intended for BCD personnel for administrative and business management purposes. These data are processed (i) to allow Purchasers to access the ITS and use BCD Platform, and (ii) to enable BCD to prospect for new users. Data marked with an asterisk are mandatory. Failure to provide such data may prevent the Purchaser from participating in the ITS and using the service.

By participating in the ITS and using BCD Platform, the Purchaser agrees and authorises BCD to share, if and when necessary the Covered data with any trusted third party (which may be located in a non-EU jurisdiction but providing an equivalent level of protection across the European Union) for the sole purposes of the provision of the service. Besides, the Purchaser acknowledges that BCD may be required to provide the Covered Data to any regulatory bodies or administrative authorities if required by law.

BCD will maintain Purchaser's Covered data only for as long as is it is necessary, or as required by law.

The Purchaser is entitled to object to the processing of his personal data for legitimate reasons, as well as to object to the use of such data for the purposes of prospecting activities.

Pursuant to the General Data Protection Regulation, the Purchaser shall be entitled to request access to, rectification, erasure of his own personal data, or restriction of processing concerning the Purchaser or to object to processing as well as the right to data portability. However, given the nature of the blockchain technology used, the Purchaser may not be able to exercise all of these rights. However, as far as technically possible, BCD will enable the Purchaser to exercise his rights. To do so, the Purchaser shall notify in writing his request to BCD, with a copy of its signed ID document to the following address: contactus@blockchaincertifieddata.com

Article 14 – Legislative and/or Regulatory Developments

The Purchaser acknowledges and accepts that BCD Commercial Operation is taking place within a French legal environment that is still under development. New laws or rules may subsequently frame, modify or clarify the practice of such operations. Where necessary or applicable, should legislative and/or regulatory changes conflict with all or part of these terms and conditions, BCD reserves the right to amend the terms of the Commercial Operation as appropriate, retroactively if necessary, in order to ensure that the operation remains legal and compliant with the various laws and regulations or best practices that may be issued by the French regulatory bodies.

Article 15 – Force majeure

Force majeure is deemed any event beyond the parties' control, which they cannot reasonably foresee or reasonably avoid or overcome, provided that its occurrence makes it impossible for the parties to fulfill their obligations, and adversely affects purchase execution (e.g. earthquake, storm or other element of nature, embargoes, substantial change in the price of resources, electrical telecommunications, hardware, software or other utility failures, armed conflicts, labor disputes or other industrial disturbances, changes in laws or regulations, changes in blockchain technology (broadly construed), changes in the Ethereum protocol or any other blockchain protocols, etc.). The most diligent Party shall promptly notify the other Party by any means, and the Parties will then agree to negotiate in good faith any changes required to ensure the continuity of contract obligations. If, however, such impossibility exceeds three (3) months, the most diligent Party may terminate the contract in writing without incurring its liability and without entitling the other party to claim any right of compensation, with BCD retaining previously collected amounts, which are irrevocably acquired.

Article 16 – Miscellaneous

If any clause of these Terms is deemed to be invalid, illegal, deemed unwritten or unenforceable, all other clauses shall nevertheless remain in full force and effect.

The failure or omission by BCD to enforce any clause of these Terms will not constitute a present or future waiver of such clause nor limit BCD right to enforce such clause at a later time.

Article 17 – Language and Jurisdiction

These Terms are governed exclusively by French law. Translations of the terms and conditions herein, made available to the Purchaser, are purely informative and are not legally binding. The French version of these Terms has sole legal force.

The Parties agree to seek an amicable settlement prior to bringing any legal action. Failing this, any dispute, of any nature whatsoever regarding the Commercial Operation, will be brought expressly before the court with jurisdiction over BCD's registered headquarter.

REFERENCES

[1] Statistics on higher education, Eurostat: http://ec.europa.eu/eurostat/statistics-explained/index.php/Tertiary_education_statistics/fr

[2] « Fast Facts: Back to school statistics »: https://nces.ed.gov/fastfacts/display.asp?id=372

[3] « Chine : la poudrière des diplômés », Yu Yiwei, Courrier International, 11/01/2012: http://www.courrierinternational.com/article/2012/01/12/la-poudriere-des-diplomes

[4] « Indicateurs de l'éducation à la loupe » http://www.oecd.org/edu/skills-beyond-school/PIF%205.pdf

[5] « Le DG de Yahoo! Accusé d'avoir menti sur son CV », Marie-Catherine Beuth, Le Figaro Economie, 04/05/2012 : http://www.lefigaro.fr/societes/2012/05/04/20005-20120504ARTFIG00514-le-dg-de-yahoo-accuse-d-avoir-menti-sur-son-cv.php

[6] The First Lady claimed to have a degree in architecture that she didn't achieve: « Melania Trump Website, Biography Have Disappeared From The Internet », Christina Wilkie, 28/07/2016.

[7] Translated from Loignon, Stéphane. Big Bang Blockchain: La seconde révolution d'internet (French Edition). Tallandier, 2017.

[8] « Un site internet chinois vend de faux diplômes français », Marie-Estelle Pech, Le Figaro, 29/04/2009 : http://www.lefigaro.fr/actualite-france/2009/04/29/01016-20090429ARTFIG00064-un-site-internet-chinois-vend-de-faux-diplomes-francais-.php

[9] A framework is a group of software components organized following an architectural layout.

[10] General Data Protection Regulation: this is the authoritative text about personal data protection in the European Union. The scope of this text is extraterritorial.

[11] A keystore is a secured location where encrypted keys are stored.

[12] Gas is miners' earnings unit when a smart contract is executed. This gas is Ether. It is used in infinitesimally small amount and market price fluctuates.

[13] A hash function is a particular function, which calculates the imprint of a initial data, imprint used to quickly identify the later. These functions are used in cryptography.

[14] Metropolis is the name of Ethereum's new update. It use will be easier and more flexible for the smart contract developers.

[15] Proof-of-Stake: Method by which a cryptocurrency blockchain network aims to achieve distributed consensus.

[16] Sharding: process that divides the blockchain in shards, which will be easier to manage.

[17] "DApp" or "Oracle" application, which allows reading a transaction's data on Ethereum via a secured web access.

[18] Application Programming Interface: interface through which a provider software offers services to other consumer software.