BCDiploma

by bcd
Blockchain Certified Data

WhitePaper v1.0

October 8th, 2017

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.

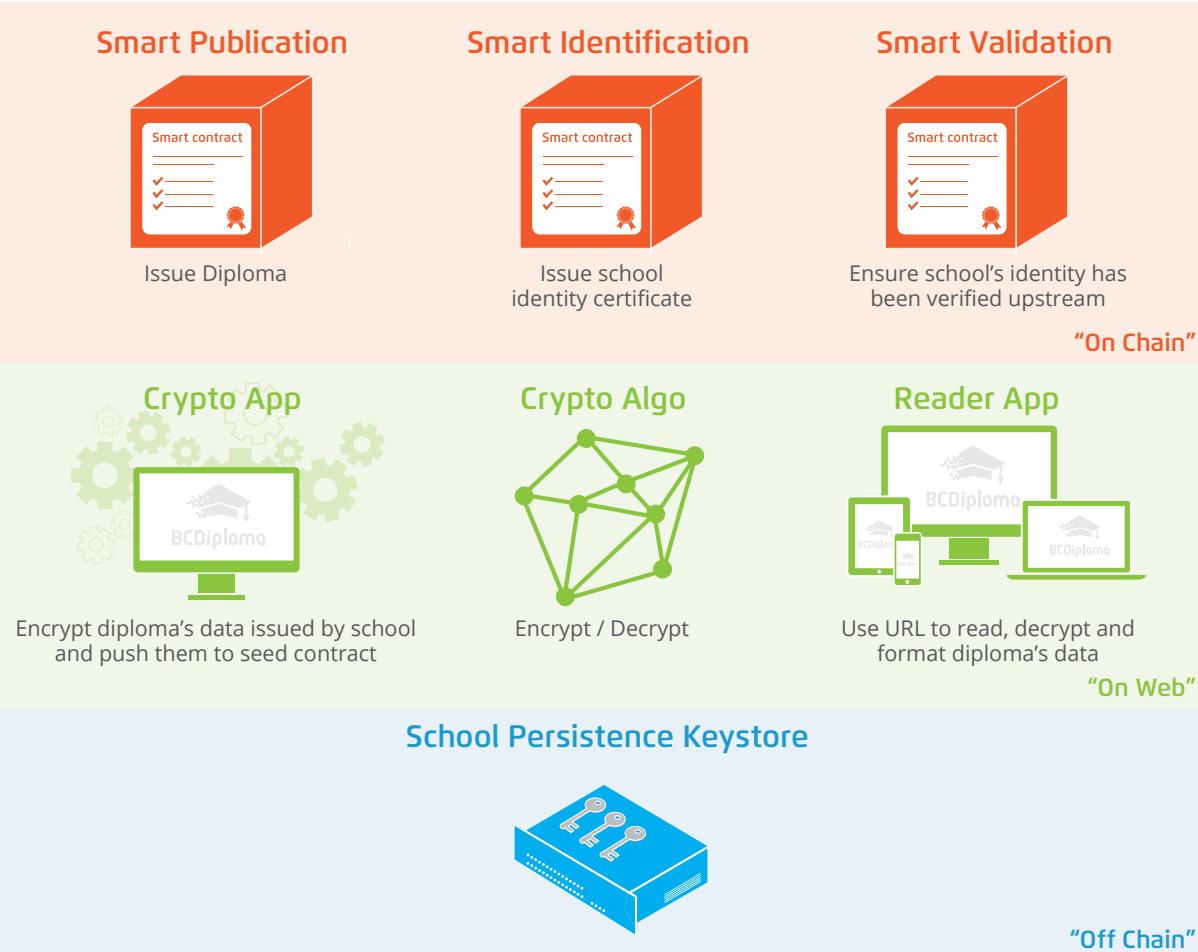
To run EvidenZ, the Ethereum blockchain is the obvious choice. It allows:

- 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.

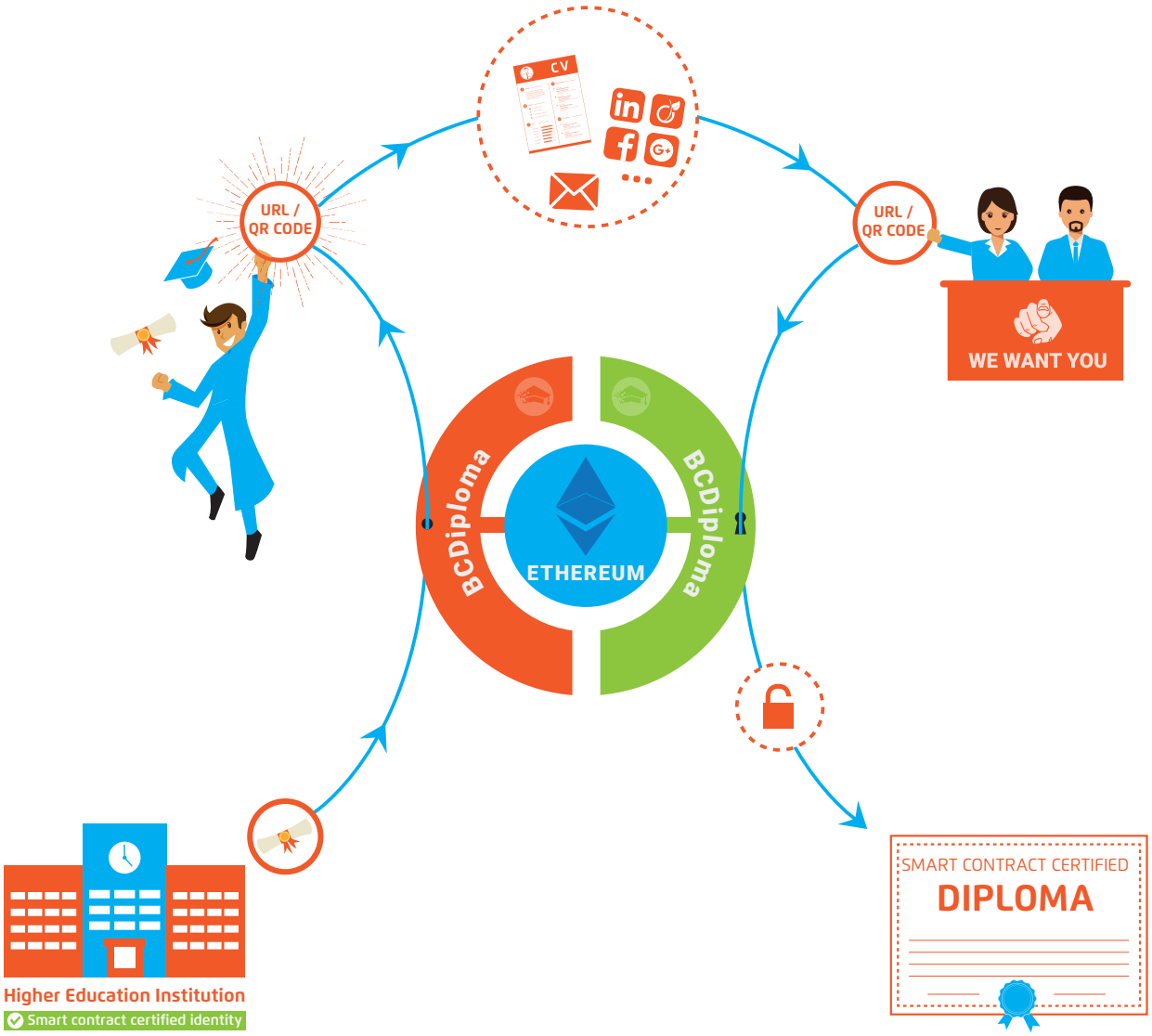
The EvidenZ's architecture was conceived to take advantage of this particularity. The amount of significant text data on a diploma is limited and often redundant from one diploma to another. Using optimized algorithms to reduce the amount of data per transaction, Evidenz pools, structures and zips data. 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

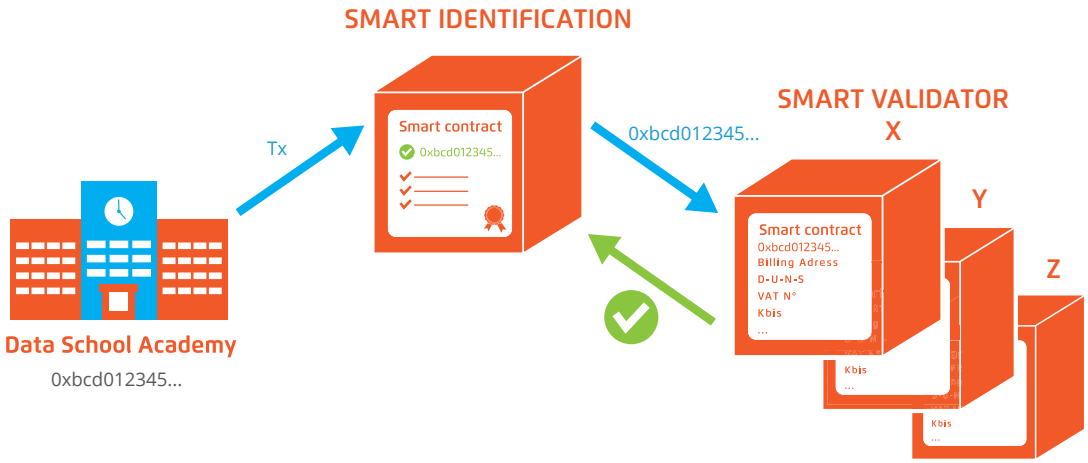
1.1 A validator guarantees the school's identity

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

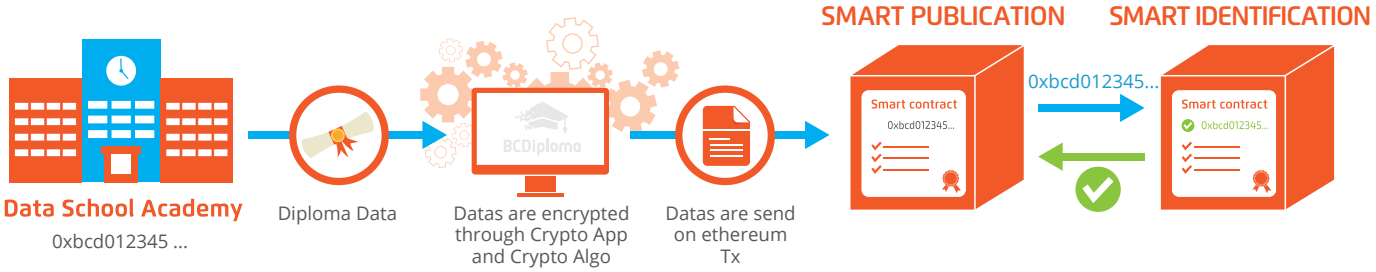
The ID certificate includes the following information: the school's name, the characteristic features of the diplomas that are issued, the URL of the corporate website page on which the Ethereum address will be published and the URL of the web server hosting Reader App.

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

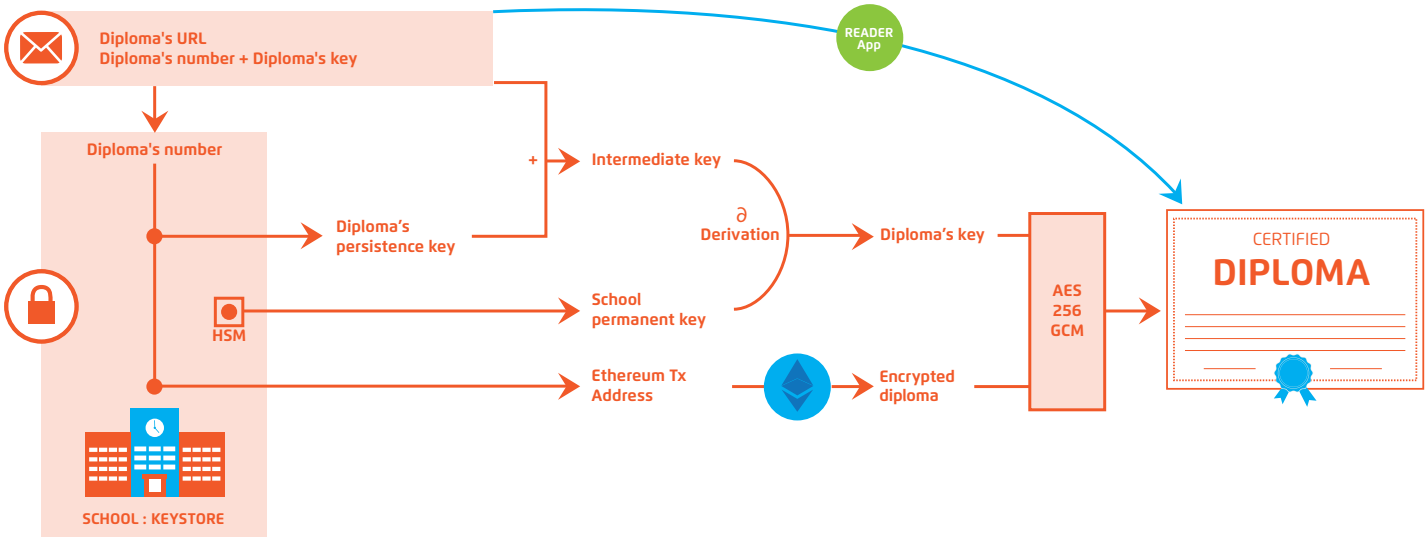
The graduate gives his diploma's URL to a company or university recruiting manager... This URL, redirecting the user towards the Reader App's server, allows him to:

- 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 guaranty 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.

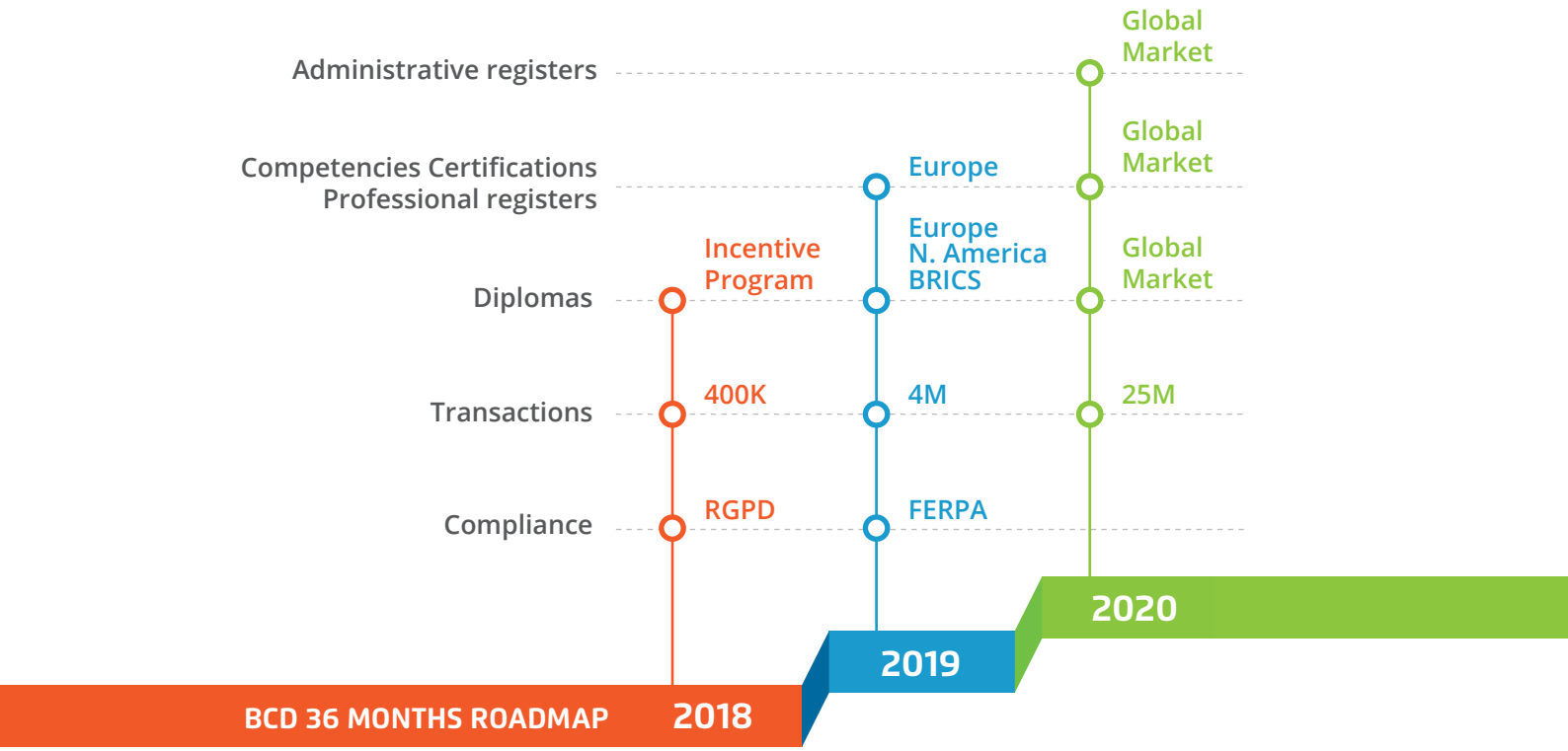
- Seeing the diploma will be free for all;
- **Our service will be free for the graduate,** the employee or the citizen, without any time-limit;
- For our clients, the unit cost for issuing a degree will be competitive compared to the actual players, who use "digital safes";
- **The payment for issuing 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;
- 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.

ITS will start December 1st, 2017. Detailled timing 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 a few hours before the ITS’ beginning. A guideline explaining how you can contribute will be also given.

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 following figures might vary based on the USD / ETH exchange rates. They were our best estimations on October 6th, 2017.
The ITS goal is to raise a maximum amount of $12M (approximately 40,000 ETH).

- **Time of the ITS:** ITS will start December 1st, 2017. Detailled timing available on www.bcdiploma.com;
- **Number of tokens for sale:** 100,000,000 BCDT tokens;
- **ITS' maximum sale revenues:** $12M (approximately 40,000 ETH);
- **ITS' minimum sale revenues:** $3M (approximately 10,000 ETH);
- **ETH / BCDT's indicative exchange rate :** 1 ETH = 2,500 BCDT tokens.

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

- First round: 20% bonus, 100 ETH is minimum contribution, contributors have to be whitelisted (contactus@blockchaincertifieddata.com). $6M limit;
- Second round: 10% bonus on 25% remaining tokens;
- Third round: no bonus.

ITS's completion

The ITS will end when all the tokens are sold, and, failing that, on January 15th, 2018.

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 six months.

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

Security Program

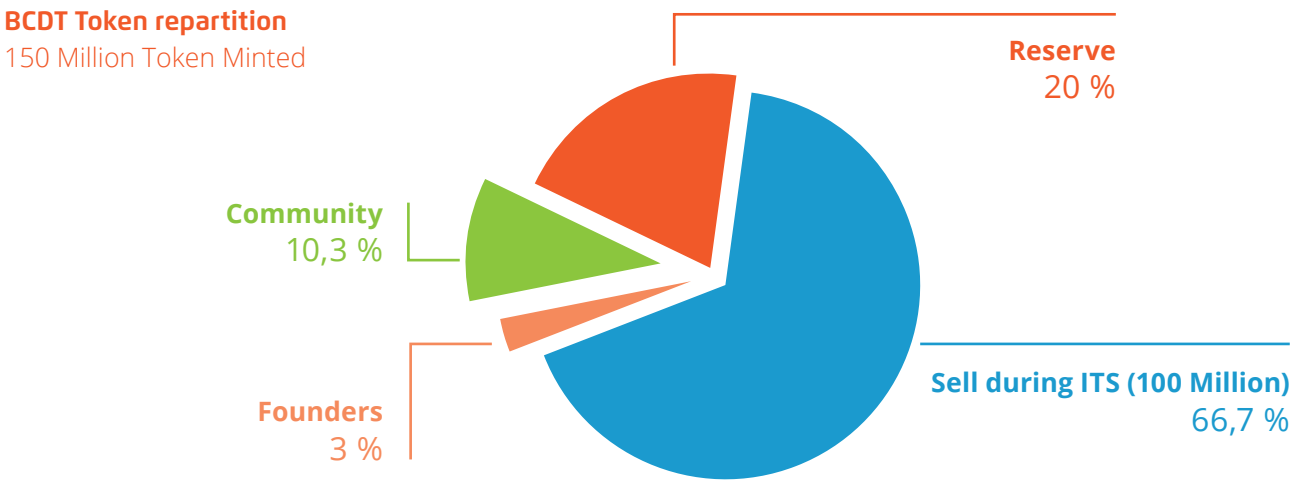
A 3-signatures ledger multisig will lock the access to BCD's address during the ITS. These signatures will be those of the 2 founders and a trustworthy third party.

Tokens distribution

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

Based on a token sale of a maximum amount of $12M or 100 million tokens:

- **Initial BCDT tokens' sale offering:** 100 million – only sold tokens will be created. The total supply of the issued BCDT tokens will amount to 1.5 times the amount of the sold tokens;
- **BCDT Tokens set aside:** 20% of tokens minted;
- **BCDT tokens allocated to community members promoting BCD, including team:** 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.



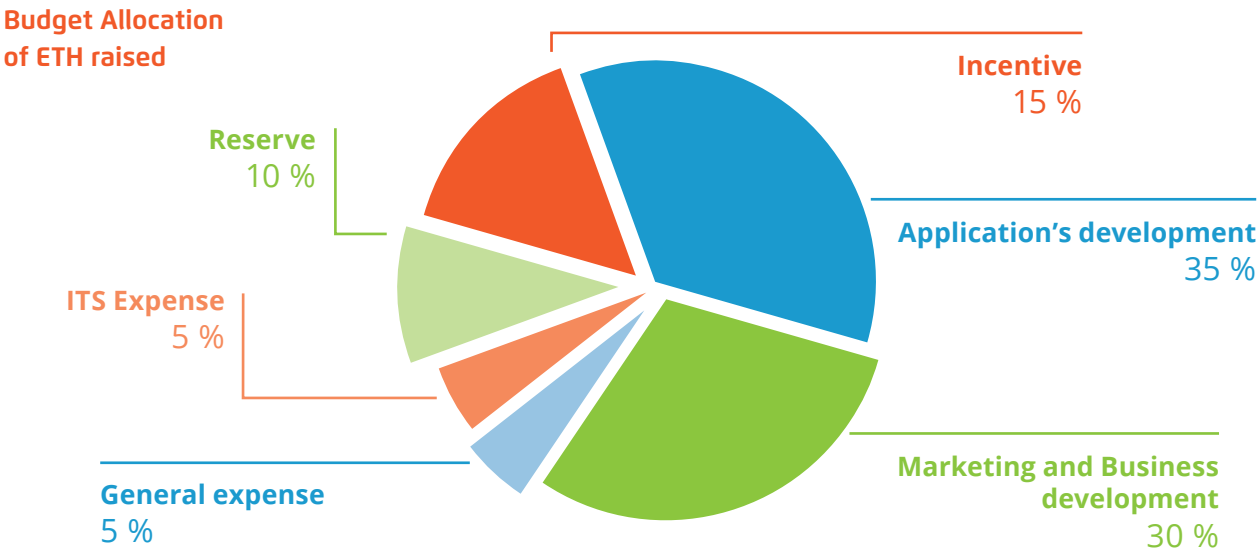
How are we going to use the funds ?

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;

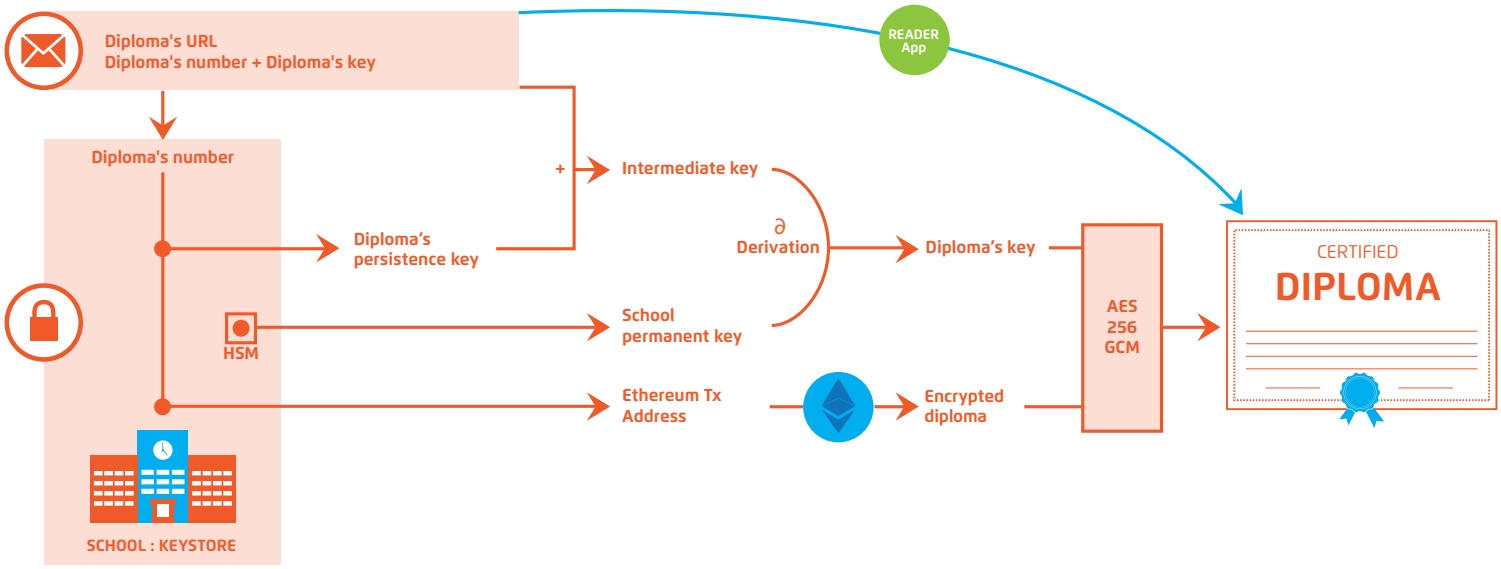
Key sizes:

- 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

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 RDN2 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

DISCLAIMER

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

Clients seeking to buy tokens are deemed to be acting for the purposes of a professional business activity and not as a consumer.

The Client 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 their country of residence.

BCDiploma may not be held liable for the Client's ling obligations in the country in which it is domiciled. The same applies to any tax or charge that would be payable by the Client, in relation to the purchase, ownership, use or passing of its token.

Prior to any Order, the Client acknowledges and accepts that tokens sold by BCDiploma do not, under any circumstance, represent any form of investment or financial investment and agrees not to attempt to divert their function for speculative purposes.

The Client expressly acknowledges the random nature of the BCD auction network development project as presented in this document (see below for risk factors) and that this project, therefore, may not come to fruition or may have to be abandoned due to technical constraints, without the tokens being used. In such a case, the Client expressly acknowledges and accepts that it will not be entitled to sue or bring any direct or indirect legal action before the courts, the arbitration bodies or any alternative dispute settlement body, either in France or abroad, against BCD, its directors, shareholders, employees and subcontractors in the event of the non-performance, non-deployment or non- implementation of the BCD auction network, even in cases where their tokens have lost some or all of their value.

In addition, BCD may not be held liable for any of the following:
(a) use of services that are not compliant with the terms of the contract
(b) non-performance, failure, malfunction or unavailability of the services due to a third party, the Client, a third-party product, or the Client's breach of its obligations
(c) indirect damages such as business loss or disturbance, loss of orders, operating loss, infringement of the trade mark, loss of profits or clients (e.g. improper disclosure of confidential information concerning said clients due to failure or piracy of the system, third-party proceedings against the Client, etc.)
(d) loss, disclosure or unlawful or fraudulent use of user sign-ons by the client or third parties
(e) suspension of access or temporary or permanent suspension of services (in particular, arising from a request issued by an appropriate administrative or judicial authority, or notification received from a third-party
(f) 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 client activities, and data backups in particular;
(g) mismatch between the services and the client's needs (in particular, with regard to the sensitivity of the relevant data),
(h) security incidents relating to use of the Internet, concerning in particular the loss, alteration, destruction, disclosure or unauthorized access to the Client's data or details on or via the Intern
(i) damage to systems, applications and other items installed by the client on the infrastructure

What do BCDT represent?

BCDTs are tokens in a new Blockchain. They are not refundable, nor are they securities or for speculation. There is no promise of future performance. There is no suggestion or promise that BCDT has or will hold a particular value. BCDTs give no rights in the company and do not represent participation in the company. BCDTs are sold as a functional good. Any value received by company may be spent without conditions. BCDTs are meant only for experts in cryptographic tokens and blockchain-based software systems.

General information

The BCDT token is a utility voucher, which will allow its holder to make use of the BCD Platform. Through the Token Sale, Purchasers acquire the future rights to use the BCD platform at a price that takes into consideration the risk that BCD may not be able to launch its planned business.
The BCDT token does not have the legal qualification of a security. The BCDT token is final and non-refundable. The BCDT token is not a share and does not give any right to participate in the general meetings of BCD S.A.S. The BCDT token cannot have a performance or a particular value outside the BCD Platform. The purchase of BCDT token shall therefore not be done for speculative usage.
Any person purchasing any BCDT token (hereafter referred to as "Purchaser"), expressly acknowledge and represent that he/it have carefully reviewed the Terms and fully understand the risks, costs and benefits associated with the purchase of cryptocurrencies as indicated in the Terms.
Knowledge required
Any person undertaking to purchase BCDT token in relation to the Token crowdsale should ensure that he/it understands and has significant experience of cryptocurrencies, blockchain systems and services, and that he/it fully understands the risks associated with the Token Sale as well as the mechanism related to the use of cryptocurrencies (incl. storage).
BCD shall not be responsible for any loss of BCDT token or situations making it impossible to access to BCDT token, which may result of any actions or omissions of Purchasers or any person undertaking to acquire BCDT token.

Risks

Acquiring BCDT token involves various risks, in particular that BCD may not be able to launch its operations and develop its platform.
Therefore, and prior to acquiring BCDT token, any interesting person should carefully consider the risks, costs, and benefits of acquiring BCDT token within the Token Sale, and, if necessary, obtain any independent advice in this regard. Any interesting person being not in the position to accept nor to understand the risks associated with the Token Sale (incl. the risks related to the non-development of BCD network and operations) or any other risks as indicated in the Terms, should not acquire BCDT token, at this stage or ever later.

Important disclaimer

The Terms shall not and cannot be considered as an invitation to enter into an investment. They do not constitute or relate in any way nor should they be considered as an offering of securities in any jurisdiction. The Terms do not include nor contain any information or indication that might be considered as a recommendation or that might be use to base any investment decision. The BCDT token is just a utility token and is not intended to be used as an investment.

Neither BCD nor any of its affiliates are to be or shall be considered as advisor in any legal, tax or financial matters. Any information in the Terms is given for general information purpose only and BCD does not provide with any warranty as to the accuracy and completeness of this information.

BCD will be an operative entity managing a platform and the BCDT token are only utility token. Therefore, BCD is not a financial intermediary according to Swiss Law and is not required to obtain any authorization for Anti Money Laundering purpose.

Acquiring BCDT token shall not grant any right or influence over BCD's organization and governance to the Purchasers.

Regulatory authorities are carefully scrutinizing businesses and operations associated to cryptocurrencies in the World. In that respect, regulatory measures, investigations or actions may impact BCD's business and even limit or prevent it from developing its operations in the future. Any person undertaking to acquire BCDT token must be aware that BCD business model and the Terms may change or need to be modified because of new regulatory and compliance requirements from any applicable laws in any jurisdictions. In such case, Purchasers and any person undertaking to acquire BCDT token acknowledge and understand that neither BCD nor any of its affiliate shall be held liable for any direct or indirect loss or damages caused by such changes.

BCD will do its best to launch its operations and develop BCD platform. Any person undertaking to acquire BCDT token acknowledge and understand however that BCD does not provide with any guarantee that it will manage to achieve it. They acknowledge and understand therefore that BCD (incl. its bodies and employees) assumes no liability or responsibility for any loss or damage that would result from or relate to the incapacity to use the BCDT token, except in case of intentional misconduct or gross negligence.

Representations and warranties

By participating in the Token Sale, the Purchasers agree to the Terms and in particular, they represent and warrant that they:

- are authorized and have full power to purchase BCD according to the laws that apply in their jurisdiction of domicile;
- are not acting for the purpose of speculative investment;
- will not use the Token Sale for any illegal activity, including but not limited to money laundering and the financing of terrorism;
- are solely responsible for determining whether the acquisition of BCDT is appropriate for them;
- are acquiring BCDT for a future use of the BCD platform;
- understand the risks associated with the Token Sale (incl. the risks related to the non-development of BCD network and operations);
- Understand the use of cryptocurrencies and its associated risks.

Governing law and arbitration

Any dispute, controversy or claim arising out of or in relation with the present White Paper, shall be resolved according to French Law by arbitration in accordance with the French Rules of International Arbitration of the French Chambers of Commerce in force on the date when the Notice of Arbitration is submitted in accordance with these Rules. The arbitration panel shall consist of one arbitrator only. The seat of the arbitration shall be Paris, France. The arbitral proceedings shall be conducted in French.

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.