



# White Paper | Crypto-Compliance

August 15, 2018  
Prepared by Alex JELIC and Thang DAO



This page is intentionally left blank.

---

## Table of Contents

<b>Documents History</b>	<b>3</b>
<b>1 Introduction</b>	<b>4</b>
<b>2 Abstract</b>	<b>4</b>
2.1 What Do We Do - Flow & Group mode	4
2.2 Data Access - KYC mode	5
<b>3 System Architecture</b>	<b>6</b>
3.1 First Component: Customer Facing Interface, a.k.a. Front-End	6
3.2 Second Component: Blockchain, a.k.a. Back-End	6
3.3 Third Component: Finance-AML Analysis Software	6
<b>4 Cryptocurrency</b>	<b>8</b>
4.1 Complete Cryptocurrency Intelligence	8
4.1.1 Notifications of Specific Activities	8
4.1.2 Alert Monitoring & Fraud Detection	9
4.1.3 Origin of Funds, Flow & Grouping Correlations	10
4.1.3.1 Risk Index	10
4.1.3.2 Flow Mode	11
4.1.3.3 Group Mode	13
4.1.4 Prototype of Crypto Compliance Service	14
4.1.5 Automate your transactions and addresses checks	14
4.1.6 Blockchain News Analysis	15
4.2 Integrated Forensics Capabilities	15
4.2.1 Intuitive Analysis - Interactive data visualization	16
4.2.2 Learn from your customers behaviors	17
4.3 AML Algorithms	18
4.3.1 Machine Learning Algorithms	18
4.3.2 Stochastic Algorithms	19
4.3.2 Econophysics Algorithms	19
4.4 Intelligence & Collaboration With State Agencies	20
4.5 Team of Advisors & Cooperation With Academia	20
4.6 Use Our Service	21
<b>5 Conclusion</b>	<b>22</b>
<b>6 Appendix - Fiat Compliance</b>	<b>23</b>



## Documents History

Name	Date	Reason For Changes	Version
Alex Jelic	23.10.2018	White Paper AML - Crypto Compliance (this is document) <a href="https://docs.google.com/document/d/1HptUw7s6_yk_7T8DGrEVDLHrulWe0pXr91DN6UKIHXg">https://docs.google.com/document/d/1HptUw7s6_yk_7T8DGrEVDLHrulWe0pXr91DN6UKIHXg</a>	0.0.1
Alex Jelic	29.10.2018	Finished crypto part and given to check for sentence construction & grammar.  --5 Conclusion [didn't finish]	0.0.2
Thang DAO <sup>12</sup>	31.10.2018	Review	0.0.3
Sven Roering	25.12.2018	Fix of grammar	0.0.4
Alex Jelic	9.1.2019	Finished:  --5 Conclusion Included Svens fixes, removed Draft Given to Thang before going public to check.	0.0.5
Thang DAO	12.01.2019	Review	1.0.0

---

<sup>1</sup> For the time being, infrastructure is reduced to the minimum, using WhatsApp groups and Google Drive

<sup>2</sup> Website is built according to the framework <https://welles.fr>

# 1 Introduction

We are a company that specializes in creating efficient, scalable and innovative solutions to combat Money Laundering in financial industries.

At WELLES, we recognize that hard work brings results while hard work done with expertise brings perfection. It is an idea we have been following since the beginning and that made us build the most efficient and easy to use solutions.

Our company consists of people with experience in mathematics, IT development and AML. The company also offers legal and fiscal advice on data and system protection, privacy and cyber security.

**WELLES is looking for financial and strategic partners.**

## 2 Abstract

### 2.1 What Do We Do – Flow & Group mode

Private banks worldwide are being approached by wealthy individuals who have generated wealth via cryptocurrencies. These individuals want their cryptocurrency assets to be managed, and naturally go to private banks for this purpose.

These banks, wealth managers & related financial services providers would welcome a tool that can give them a confidence in the level of "cleanliness" of funds transferred to their custody. Our tools will also let customers cherry pick the assets they want to manage. In a nutshell, our tools are designed to analyze the transaction history of each asset in each wallet/portfolio and compare it against all known Money Laundering schemes & threats, and subsequently issue a report on the risks of handling each specific resource i.e. Flow Mode

Group Mode displays the Submitted Addresses, and all other address that are in correlation with these Submitted Addresses. This connects NOT Submitted Addresses to the Entity that owns the Submitted Addresses, enabling you to evaluate the Entity (the would-be Customer), drill down further into investigating the overall compliance.

The development of our tools are done in two phases, with different technologies for different asset classes:

- I. **FIRST PHASE** covers an application for cryptocurrencies, mainly to support BITCOIN and ETHEREUM assets, after which we will expand to the ten largest cryptocurrencies in the market.
- II. **SECOND PHASE** we'll start developing this phase once we have successfully executed on phase one. In this phase, we plan to use our methods developed and expand to other cryptocurrencies.

During the lifetime of this project we'll publish 3 kinds of material:

- **Patent documentation:** This is a way to secure the company's intellectual property and needs to be done on all components of cardinal importance for the system. It is mandatory.
- **Scientific publication:** It is a way to confirm our expertise in the scientific community. This kind of publications may be based on patented components or not.
- **Educational publication:** books, courses, working with academy and simple courses for udeamia should be published on a regular intervals. It is a well-known method to be known.

Our areas of expertise: econophysics, machine learning, stochastic mathematics, blockchain and AML.

## 2.2 Data Access – KYC mode

Our marketing approach is to participate to as many bank and AML, ACAMS conferences as possible, as to spread information about our company and to build relationships with financial institutions.

We will use these opportunities to present our model of information gathering which would give total anonymity to account holder (user of our systems). For each account we'll use cryptographic functions approved by the NSA\*<sup>3</sup> and assign it one number, so only the bank, which has complete details about the user, can see all the history. While this sounds very little information, yet it is enough data on which we can do detailed analysis.

The data that banks share with us about their transactions should not violate any privacy agreements they maintain with their customers or any legislation. Data may be shared through consent from customers, or as a regulatory requirement to prevent money laundering. The ultimate goal is to let banks know that an individual has accounts in multiple places, and issue flags where suspicious activity is found. When implementing a multi-signature algorithm, banks will need to ask other banks from the list for access rights to that user's information.

1. If other banks comply, only the part of information in question will be added and will be seen as transaction data; and only part that is owned by the bank. (if the request is granted by all banks then the whole database will be viewable by the bank which asked for access)
2. If access is not granted, they will simply know that the user has account in a certain number of banks the name of which can be seen, and may use this information.

It's important to notice that without willingness by banks to share transaction data there is no possibility to connect the data with the user.

KYC for Know Your Customer Mode is a premium service with specific information the acces of which is bound to privileges you own or define. Compliance of an asset can be shared, with the right level of access privileges.

---

<sup>3</sup> NSA – National Security Agency

## 3 System Architecture

Modern Software Systems consist of components that are highly scalable, i.e. they can grow in size or/and functionality to serve millions of users.

### 3.1 First Component: Customer Facing Interface, a.k.a. Front-End

This component is what users can see and which handles users interaction:

- Website with mobile and tablet support.

The website has all the necessary information to guide users on the functionality of our system, the benefits as well as pricing.

### 3.2 Second Component: Blockchain, a.k.a. Back-End

We use blockchain technologies as a means of payment on our system, specifically in relation to our cryptocurrency solutions. This is convenient for our customers as they are already familiar with this payment method, and adds competitive advantages as well as exclusivity to our solutions. This also provides a mechanism for potentially financing the company and providing seed funding through an STO issuance.

The blockchain system hosts payments and also defines our currency, which will be emitted in a limited amount. This has the consequence that payment is always calculated in FIAT currency as there is a need to factor in inflation and more importantly deflation of our token. Payments are processed using our coin and all services are to be charged in FIAT currency as we will emit a limited number of coins, and we can only guarantee a bottom price for our service usage. We will convert our tokens to FIAT currency at the actual current rate and this is done for every payment.

We have created two private blockchains. We use the Bitcoin blockchain with battle-tested functionalities.

The reason for this decision is our business focus on working with banks. We offer the most stable and battle tested platform.

### 3.3 Third Component: Finance-AML Analysis Software

This component is the heart of our system and is confidential. Only company employees have access to the back-end algorithms and software, which are also patented.

Because authors can produce algorithms by themselves, we will start creating a system and make that system evolve. Authors will concentrate their efforts into splitting algorithm into basic wholes and then organising research under their supervision.

The supervision and work with academics is of cardinal importance because academic workers have their own view of work and the world. They need to work with those who understand them, so the development can go smoothly and effectively. When core development is drawn to the end, we patent the algorithms.

Our algorithms enable Real Time access through an API, they incrementally calculate risk rates. One of the cornerstones is to use transaction data and standard behaviour, then use econophysics and stochastic models to relate accounts to a user.

Data protection is done in accordance with best industry standards. Statistics are constantly updated. If somebody pulls all data from our systems without us knowing, this individual will instantaneously have outdated information.



## 4 Cryptocurrency

### 4.1 Complete Cryptocurrency Intelligence

We are pioneers in cryptocurrency intelligence and AML policy implementation.

At this moment in time, blockchain and the information revolution have reached its mature phase and enable us to do what was previously only dreamed about., We must use this opportunity to set the standards for others to follow.

Financial institutions must implement AML measures, yet they see it as a massive expenditure and a waste of time and resources. It is thus an opportunity on which we need to capitalize, offering services to their compliance department to alleviate the hard work of uncovering suspicious trails on assets.

We use standard equilibrium statistics as a starting point as it is used in classical economic theory. Why? It was the only econophysics model which predicted the 2008 financial crisis.

Our system uses the following combination:

- Non-equilibrium models which are applied in econophysics.
- Stochastic models.
- Machine learning in combination with the first two approaches.

Machine learning gives us a deeper view on systems using heuristics models. They don't give analytical answers to our questions but they are useful to assess the probability that some suspicious activities/schemes are taking place and to point to similar cases when similar activities occurred. An information not to be underestimated.

We built our app in accordance with the USA AML code under the Bank Secrecy Act (BSA). The software is designed to ensure compliance with all applicable BSA regulations and FINRA and FinCEN rules.

#### **Bulk Analysis & AML API**

For bulk analysis, we offer real-time interfaces to our software, which could trigger deeper analyses. We would raise recommendations when to issue Suspicious Transaction Reports (STRs) and Suspicious Activity Reports (SARs) to abide to obligations to FinCEN and other regulatory bodies.

Some functionalities that our software supports.

#### 4.1.1 Notifications of Specific Activities

Our customers will have the option to choose a set of criteria for which they want notification, for whichever criterion they deem important.

This has a significant value when the ownership of the crypto-assets has not been transferred to the bank.

#### 4.1.2 Alert Monitoring & Fraud Detection

The service, does real time monitoring of suspicious activities. Fast and quick actions are needed and customers will be informed the very moment the activity is taking place.

Our database consists of many types of suspicious activities and schemes, known to have happened before on blockchains, known cases of schemes and frauds published by FinCEN. We combine this data with alert tagging flags, to signal possible money laundering activities.

Our transactions database is continuously analyzed by our patented algorithms. We then report all suspicious activities, showing the probability with which some type of criminal activities is taking place. This will be complemented with data showing past cases with similar activity/schemes of abuse.

In all due essence, this in combination with 4.1.1 will enable our customers to create alerts for specific criteria or schemes, which we will supplement with our own historical data on the localisation and the probability of the suspicious activity.

### 4.1.3 Origin of Funds, Flow & Grouping Correlations

The answers to these questions form the core functionalities of our software. We separate most of our work and effort in this area, and decided to start with well established cryptocurrencies, and expand from that point.

Algorithms that we developed enable us to track coins from multiple different sources; to detect behaviour of owners; and to analyse the cryptocurrency system on a whole new level.

We are able to detect schemes as they occur, to track coins from different funds, and to assign a risk rate for every cryptocurrency currently in use. We also show its evolution over time, the probable owner and how he handled it. .

#### 4.1.3.1 Risk Index

For the time being, we have opted for seven types of cryptocurrency owner groups, and a coloring scheme to foster an intuitive reading of our reports.

The information about which owner belongs to which type is gathered by our algorithms as well as in cooperation with state and private agencies who will provide us trustable data of criminal addresses. For some of these types, we can formally declare that they are illegal.

- Miners (Mining Pools)
- Exchange
- Services
- Gambling
- Mixer
- Scammer
- Dark net
- [In due time we may add more categories... ]

Type	Miner	Exchange	Services	Gambling	Mixing	Scammers	Dark Web
Population	40	150	112	84	5	42	38
RGB	R: 50 G: 144 B: 58	R: 94 G: 205 B: 91	R: 83 G: 239 B: 93	R: 252 G: 195 B: 56	R: 238 G: 163 B: 56	R: 231 G: 91 B: 9	R: 234 G: 48 B: 42
HTML code	#398D3F	#56CE6A	#53EF5D	#FCC338	#EEA338	#E75B5D	#EA302A

### 4.1.3.2 Flow Mode

The blockchain is a public ledger, we have thus the possibility to run through its history, and see how and when each transaction has taken place. This gives us the origins of the coins and our algorithms shows if these coins were stolen or were used in an illegal trade.

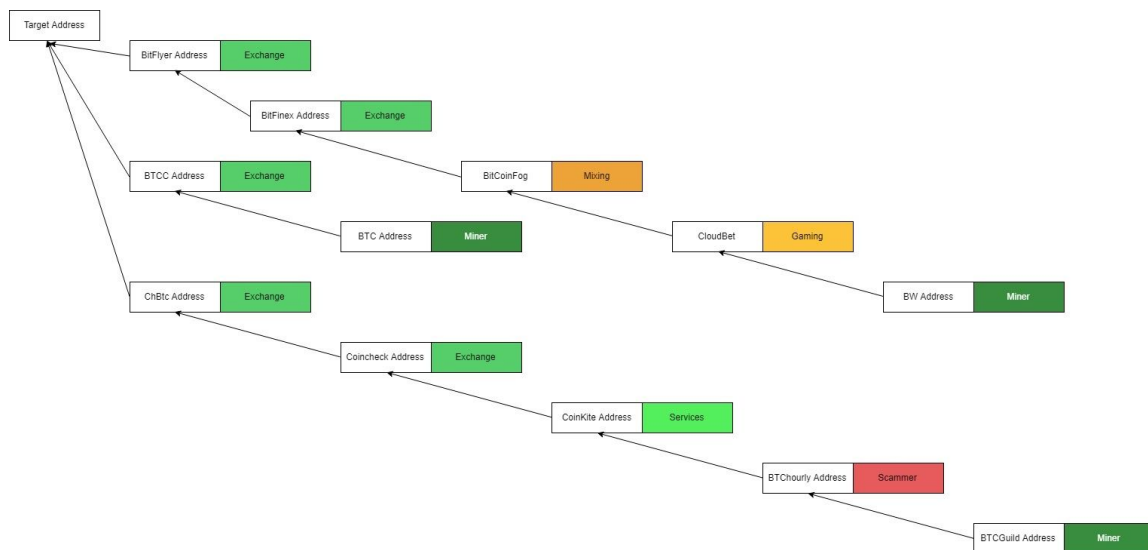
The number crunching activity is quite intensive. However, there is clear regularity in behaviour and there are laws governing this system behaviour. By following this regularities, we can track what matters.

Let's take some time to analyze a simple case:

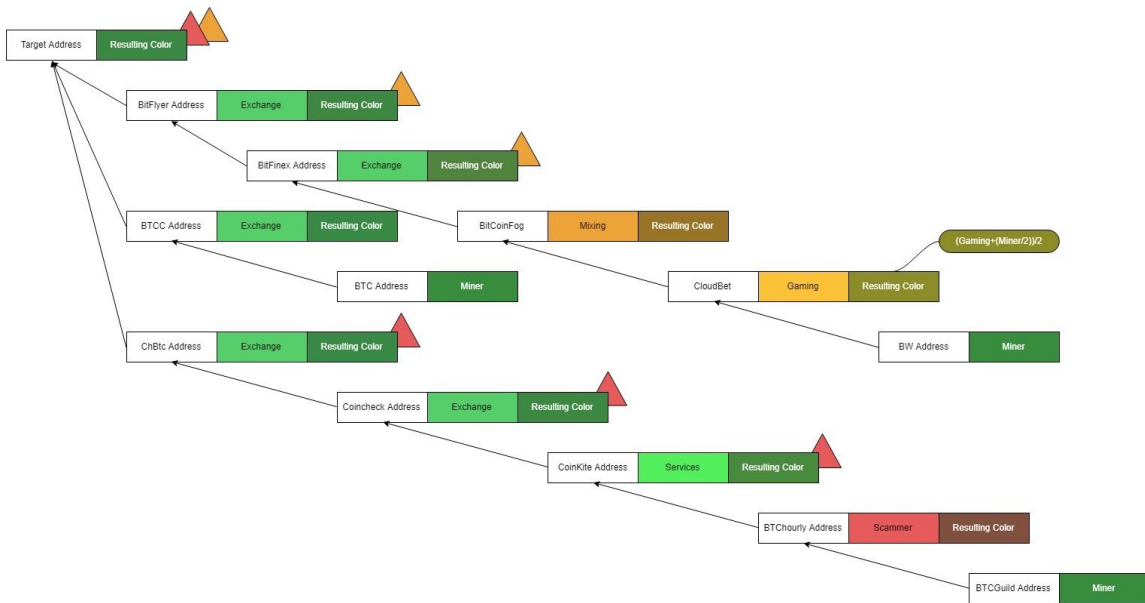
There are transactions happening all the time, so for a given account we can look at the traces of transactions back in time.

- One trace in our example is crystal clear of purity as we can see that it is a miner who submitted it through a well known exchange.
- But in two other traces of transactions, in their history we see that some of the bitcoins are tainted.

Our report will show all the data and the risks of accepting this asset. The customer makes the final choice.



As mentioned in our example, we'll assign the risk probability and color to target address (we'll give a color and risk rate to each of intervening address.)



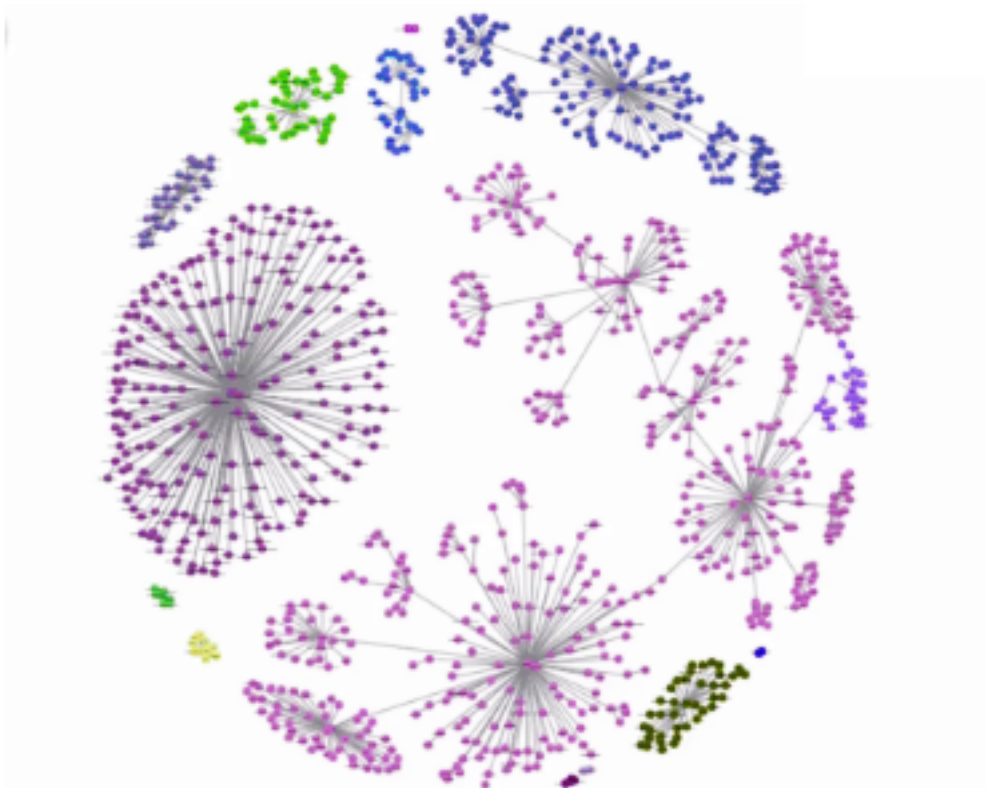
Here we'll use multiple sources of info and we'll categorize our results in three cases:

- **First case** for which we give red flag and guarantee that it's illegal coins with 100%
- **Second case** we'll assign probability of that it's illegal coins from 1% to 99%
- **Third case** is coins for which we can guarantee that are totally legal, i.e. the risk rate is 0% for the customer to handle this asset.

### 4.1.3.3 Group Mode

We can assign addresses to actual cryptocurrency owners and build their portfolio. We follow certain categories of owners and wallet behaviours which allows us to group accounts and connect them to owners.

**Objective:** Identify origin of and group owner addresses.



#### **Addresses with Users Grouping**

To sum up, the grouping algorithm will enable customers:

- To know with a certain probability who is owner of certain category of addresses; and to check that the owner may have hidden addresses.

This information is of high importance for customers as they will know when certain owner comes and says that he owns certain addresses. Customers will know that coins coming from that address are clean; and customers will know all the addresses that owner owns (with probability describing ownership 0-100%).

This is sufficient information for banks to see whom they work with; if the owner gives only a few clean addresses.

Let's look at a simple example as below:

When John Smith goes to a bank and says that he owns 100 BTC on address #12345. The bank official is supposed to know:

- Where the coins come from to address #12345; the legality of them as well as the total money flow history through which coins went from moment of mining or ICO issuance.

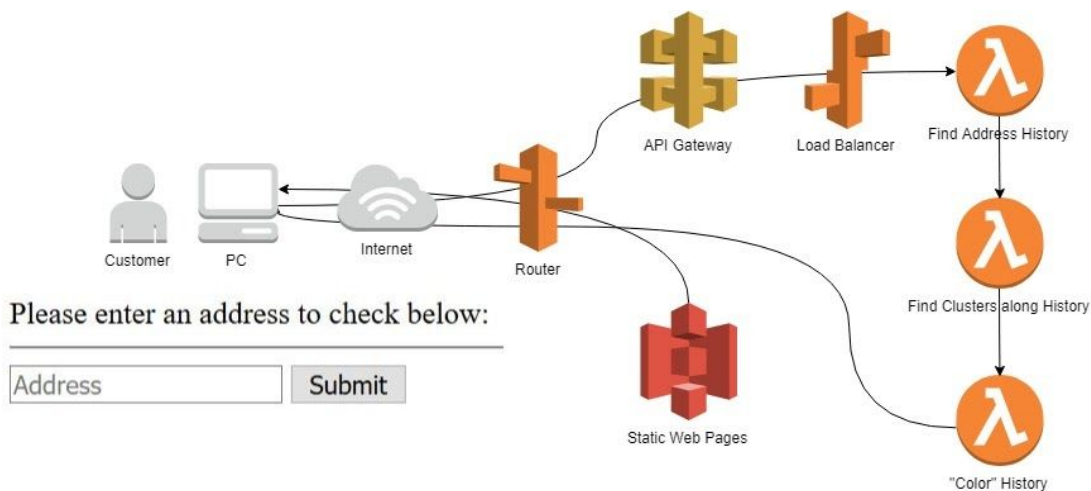
- The bank official will also know all the other addresses that John Smith owns (with probability), their balances as well as the legality of the assets of these addresses.

### 4.1.4 Prototype of Crypto Compliance Service

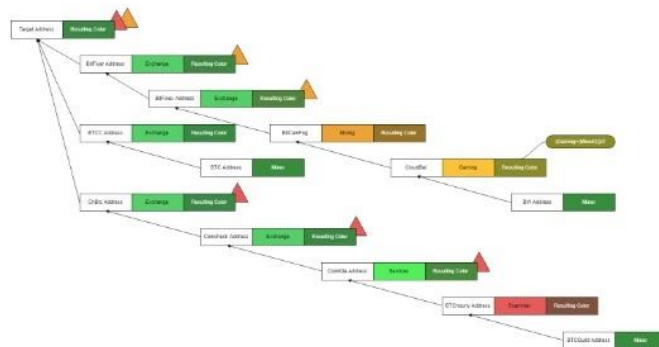
Below is a simple schematics of our prototype.

Our objectives here are to enable customers to have all basic functionalities. While we are improving our software, the community can grow and we get recognized as a trustworthy and reliable partner.

Minimal set is for user to access a static web page which will ask him to supply an address / public key to check.



### AML Prototype Schema



The address is submitted to the first service listed in the history whilst the transaction stains through history connected to the address. This generates a list of addresses and transactions that have led to the target address being supplied with the bitcoin amount.

Once this history is established, it wakes another service up, which will build a good estimate of all the clusters that the history has traversed.

### 4.1.5 Automate your transactions and addresses checks

Because addresses are free, one person may have many addresses. We deem necessary to offer automatization and checking of both transactions connected to:

- one address (transaction address went through during history)
- group addresses (or group of wallets)

These are two building blocks from which all can be reconstructed as wallets are just set of addresses.

#### 4.1.6 Blockchain News Analysis

We run a news collecting service and issue reports once every month to pinpoint the major events on blockchain scenes from the eyes of experts. Hence, our customer would learn about current behaviours in blockchain technologies, markets, as well as in legislation with new laws and regulations.

Analysis of this kind should be short and consistent with expressed advantages, risks. It should be written without bias and understandable to the banking community.

The author of report must remind himself about basic characteristics of report.

- Our readers are bankers and financial experts, good-standing citizens.
- The purpose of the report is to give the expected way that blockchain systems will be developed in future and shine light on scams. This is deeply needed in this time because of huge amount of hype and hard access to meaningful data in this new area.
- Important information that must be included in the report are new developments on blockchain and progress of current blockchain including estimation, new chains which are simply forks or some other deeper meaning, and any new development in AML policy relating to cryptocurrencies.



This report needs to be acknowledged by the banking community and seen as a reliable source of information.

## 4.2 Integrated Forensics Capabilities

The nature of the blockchain makes tracing transactions possible. It is known that blockchain ledger contains every detail of every Bitcoin transaction ever made, but this data alone has little value and need to be analyzed in the context of additional data and real-world domain expertise. System of such complexity needs to be analysed with special care and by qualified people to be of any use.



We are offering services as we stated above with pattern recognition, an advanced API, interactive visualization. We also use a lot of data by gathering through state and private references, geolocation data, and decoy deception data, police data and from our relationships with regulators, law enforcement, and exchanges.

As we stated above, our approach combines 3 components and has the best industry most capable analysing hybrid algorithms because we supply it with data from trusted sources.

**CRYPTO-COMPLIANCE data sources:**

- Proprietary Welles discovery algorithms and analysts
- Public sources
- Honeypots and other active capture sources
- Trusted communities, including law enforcement and regulators
- Welles Crypto Recovery Network
- APWG eCrime Exchange (eCX)

## 4.2.1 Intuitive Analysis – Interactive data visualization

We'll offer our customers a set of tools that they can use for detailed analysis, tracing transactions and accounts with an easy-to-use graphical interface. User interface will be intuitive in such a way that any bank worker without too much effort could use. It will also offer to remind bankworker of AML laws and terminology. There is no programming or technical jargon that is not from the banking industry. This means that software user interface is indeed intuitive.

1) **Manage Transactions with graphs of history**

We support bulk analysis of transactions and addresses that can speed up complex investigations and audits.

2) **Access entire history of Bitcoin addresses or entities**

With this kind of access, customers will be able to detect and track any entity behaviour, as well as its client. Even if just one address is given, that is enough for customers to know whom they work with: is he a simple user, or a part of a bigger entity.

3) **Interactive data visualization**

Our graphs are interactive; for purpose of intuitiveness they show as much data as possible on the smallest amount of space.

We show a summary to our customer as well as we make available a detailed report. interactive design makes it possible to move quickly from summary to details in just a few clicks.

4) **Track Bitcoin and ETH related cyber threats**

A user simply types or pastes a cryptocurrency address or Transaction ID into the Search field. Even with only a partial address, intelligence in the search engine fills in the available valid addresses that match what is entered in the search field.

Search engine then displays a valuable set of basic data attribution data. It then very quickly returns the date and amount of the transaction.

Users can then move into the analysis, which starts with a visual representation of the transaction. The users can then step forward and backward in the transaction history of the anchor transaction.

#### 5) **In-Depth Transaction Visualization**

The platform intuitive user interface makes it easy to perform deeper inspection and analysis of suspicious transactions. Once a transaction is identified as high-risk or non-compliant, the user can click to drill down and look for relationships such as groups, or search back through related transactions or multiple parts of a transaction and uncover any useful pattern.

Our data can be integrated into SIEM or analytics platforms such as Maltego, IBM or Palantir for further analysis and record retention. Data can also be exported in CSV and XML formats.

#### 6) **Transaction Risk Scoring**

Risk scores for transactions are based on whether the funds have traveled through suspicious paths and are associated with known bad actors. This transaction risk scoring of giving percent and color simplifies compliance efforts by helping to identify and highlight suspicious transactions for further scrutiny or action.

### 4.2.2 Learn from your customers behaviors

We are trying to give enough informations as well as lists of places and services that the owner has been visiting while doing transactions on the net. So banks will have a general overview with which kind of client they work with.

This will give enough information to recreate an owner habits and to start a KYC analysis. This can give a lot of informations to bank as the whole user transaction history is viewable in an intuitive way.

#### 1) **Improve your compliance management**

Our application will have plugins to adapt it to laws for big financial hubs. With this we are able to change statistics to certain part of the world where laws might differ.

We will need support of local banks and lawmakers. At first our application by default is supporting only US and Switzerland laws.

#### 2) **Manage due diligence and risk procedures**

We need to be careful in what we do; and all localization of this kind will help and consult local partners. By agreement, we will either give them special conditions, or share a part of profit earned thanks to their effort and consultation they invested into cooperating.

This will allow us to have view in local due diligence and risk procedures of the country in question or even to tailor it for needs of certain banks.



## 4.3 AML Algorithms

We take the opportunity to shed some light on which models we are using in analysing data:

### 4.3.1 Machine Learning Algorithms

Machine learning is the science of making computers learn like humans do and to also improve their capabilities to learn to act without being explicitly programmed, a.k.a. Artificial Intelligence. It is used as a general term for computational data analysis: using data to make inferences and predictions. Interpreted broadly it includes computational statistics, data analytics, data mining and a good portion of data science.

Machine learning algorithms are often categorized as:

- 1) **Supervised machine learning** algorithms can apply what has been learned in the past to new data using labeled examples to predict future events. Starting from the analysis of a known training dataset, the learning algorithm produces an inferred function to make predictions about the output values. The system is able to provide targets for any new input after sufficient training. The learning algorithm can also compare its output with the correct, intended output and find errors in order to modify the model accordingly. In contrast, unsupervised machine learning algorithms are used when the information used to train is neither classified nor labeled. Unsupervised learning studies how systems can infer a function to describe a hidden structure from unlabeled data. The system doesn't figure out the right output, but it explores the data and can draw inferences from datasets to describe hidden structures from unlabeled data.
- 2) **Semi-supervised machine learning** algorithms fall somewhere in between supervised and unsupervised learning, since they use both labeled and unlabeled data for training – typically a small amount of labeled data and a large amount of unlabeled data. The systems that use this method are able to considerably improve learning accuracy. Usually, semi-supervised learning is chosen when the acquired labeled data requires skilled and relevant resources in order to train it / learn from it. Otherwise, acquiring unlabeled data generally doesn't require additional resources.
- 3) **Reinforcement machine learning** algorithm is a learning method that interacts with its environment by producing actions and discovers errors or rewards. Trial and error search and delayed reward are the most relevant characteristics of reinforcement learning. This method allows machines and software agents to automatically determine the ideal behavior within a specific context in order to maximize its performance. Simple reward feedback is required for the agent to learn which action is best; this is known as the reinforcement signal.

### 4.3.2 Stochastic Algorithms

Stochastic optimization (SO) methods are optimization methods that generate and use random variables. For stochastic problems, the random variables appear in the formulation of the optimization problem itself, which involve random objective functions or random constraints. Stochastic optimization methods also include methods with random iterations. Some stochastic optimization methods use random iterations to solve stochastic problems, combining both meanings of stochastic optimization.<sup>[1]</sup> Stochastic optimization methods generalize deterministic methods for deterministic problems.

### 4.3.2 Econophysics Algorithms

Econophysics is an interdisciplinary research field, applying theories and methods originally developed by physicists in order to solve problems in economics, usually those including uncertainty or stochastic processes and nonlinear dynamics. Some of its application to the study of financial markets has also been termed statistical finance referring to its roots in statistical physics.

## 4.4 Intelligence & Collaboration With State Agencies

We are using our connection inside governments and institutions in a number of countries. With their help, we are supplementing our database with the best reliable data.

This is an important part for us and we believe that without this support and information gathering, it would be much harder to develop and keep track of bad actors.

## 4.5 Team of Advisors & Cooperation With Academia

We take special care of our team. We express our gratitude because at this moment in time we cooperate with:

- Belgrade University
- Heidelberg University
- Nis University
- Skoltech University
- Universita di Trieste

Our advisors expertise is spread from theoretical physicists, mathematicians, IT experts to finance and law experts.

We needed to set up a team with this wide scope because of the complexity of tasks to solve, and that only smart and highly intelligent people can work on. Our problem is unlike of many other software developments which are focused on a number of lines of code, but it differs essentially from that as our job is to devise new and inventive way to tackle a real world issue, sorting bad from good apples.

## 4.6 Use Our Service

One or two sentences why you should use us:

- 1) **As a crypto broker**, hedge fund and exchange, monitor transactions flow.  
If you own an exchange, you should be also interested in using our service since AML compliance can affect your business; and banks will choose even how they will treat you if you work with tainted coins.
- 2) **As a financial institution**, verify the origin of crypto assets.  
As financial institutions will check legality of coins given to them by individuals or by entities and to know how to charge fee as to compensate for risk or by accepting their funds.
- 3) **As an STO project**, mitigate the risk of your investors.  
STO can be variable because if one part of coins invested into your STO is tainted it means your entire funds can be treated by banks as tainted.
- 4) **Be notified** when specific activity occurs.  
We have options to set up specific events as alerts, and this will automatically be notified to you.
- 5) **Use our API** to automate your transactions and addresses checks.  
You can use our API to automate checking of your resources.
- 6) **Report per user**: Crypto Compliance made easy, All-in-one reports for STOs, AML and crypto cash in/out.
  - a) We support with our software different legislations via plugins. We also try to automatize suggestion by of laws depending on the country, what bank should do.
  - b) All in one reports for STO on how they get money and which percentage is dirty and which percentage is good.
  - c) Following crypto cash in and cash out from one currency to other.
- 7) **Exports as XLS and CSV**.  
All our reports can be exported in XLS or CSV format to enable additional analysis if banks want to do it with their own procedures.

## 5 Conclusion

We presented our improvement and advantages over our competitors i.e. CypherTrace & Scorechain.

We deem this product is a good prospect as no STO or any kind of bigger transfer of Crypto- Currencies can be made without assurance of compliance of the assets as given by our product. ur customers are everywhere.

- Individual user
- Crypto Exchanges.
- Entities that accept crypto assets.
- Investment funds - Crypto
- Crypto Investment management
- Crypto Hedge fund management
- Crypto Custody services
- Users & Organizers of ICO IPO STO platforms
- Small Entrepreneurs - Crypto
- Small Wealth manager - Crypto
- Investment managers - Crypto
- Private banking - Crypto
- Hedge fund management - Crypto
- Custody services - Crypto
- Private equity funds - Crypto
- Every ICO/STO it will be impossible to do when investments are received in cryptocurrencies without using our services or they start with a high credibility risk.
- For standard user we offer QuickCheck service to ensure them of the legality of assets with only two possible answers (GOOD, BAD). If the user wants to know more they can engage into getting the full report.

Extra Functionalities:

- Everyone will be able to store their Whitelist in our block chain and get signature and time stamps so they can prove that at moment of publishing/receiving crypto assets they were legal. (As this can change over time as some owners in a few years can be found to be involved in criminal activities and as such all of their assets will be marked according to court decisions)

**CONCLUSION: We think this product is necessary and will reshape future of compliance done the right way. It will be used extensively yet now it still is one of the pioneers.**

## 6 Appendix – Fiat Compliance

After development on cryptocurrencies, we will tackle more complex problems, like Fiat currencies. There are many standard red flags that are possible signs of money laundering and are part of every AML policy, which we have already implemented as part of our cryptocurrency solutions.



Proving our solutions via cryptocurrency transactions will provide the necessary stepping stone for fiat currency monitoring applications. This could potentially be our largest marketplace as global financial services institutions spend over one trillion USD annually to combat money laundering and terrorist financing. Surveys show that added compliance costs that come into effect every year are the biggest concern for upper management, therefore effective transaction reporting solutions are required to save on costs and flag suspicious transactions and accounts before regulators hand out fines.

FIAT currency systems are more complex and information harder to get we will need some time to adapt to it. Main idea that we want to propagate is a way of anonymous information gathering, and receiving authorization from banks to share transaction data with us. A key element would be having access to transaction data from a large number of banks and customers, aggregated via a single source or database, either from a regulatory agency or a singular transaction database that would be mandatory under Common Reporting Standards (CRS) or Automatic Exchange of Information (AEOI) requirements.

are already positive developments with regards to banks who are willing and able to share customer and transaction data, as well as using third-party service providers (TSPs) to integrate services via open APIs. We require support from regulators to compel and incentivise banks to open API and share transaction data. This is already evident through the United Kingdom Competition and Markets Authority (CMA) which, in 2016, issued a ruling compelling 9 of the biggest UK banks to allow licensed start-ups direct access to transaction data right down to the level of transaction account.

More information about Fiat Compliance you can find on our website or in white paper given by next links:

- [www.welles.fr](http://www.welles.fr)
- [White Paper | Fiat Compliance](#)



**WELLES**  
PARTNERS

WELLES RESEARCH | **PUBLIC** | PROPRIETARY

---



**WELLES**  
PARTNERS