A Proof of Concept Pilot for A Decentralized Autonomous Authority (DAA) For KYC Compliant Decentralized Identity And Authentication Services

Dr. John Henry Clippinger
MIT Media Lab/ID3[1]

Abstract

This paper describes a collaborative development between the non - profits ID3 and Fluxtream.org and startup companies Cambridge Blocchain and Intrinsic Inc. to develop an open API platform for forming and hosting decentralized autonomous authorities and organizations for KYC identity and authentication services. This platform was designed to comply with the Windhover Principles to give individuals control over their personal data and identities. The platform provides APIs to enable people to create their own data containers, to share data on a permitted basis and form organizations with identity and credential verification on the blockchain. The project demonstrated the feasibility of this approach and the need for further research and development on the use of smart contracts for regulating and enforcing permissions and autonomous governance.

Introduction:

One of the most burdensome regulations for global financial services is the KYC (Know Your Customer) and AML (Anti-Money Laundering) requirement. Not only are compliance costs extremely high, the requirements are especially difficult to enforce in developing countries lacking the requisite documentation and infrastructure.

In the case of some developing countries, such as Somalia, which depends upon remittances for roughly 50% of its economy, and which has a weak Central Bank and commercial banking sector, the failure to comply with KYC/AML regulations has been devastating. It has resulted in a redirection of remittances into informal

[1] Special credit and thanks to Candide Kemmler of Fluxtream and Intrinsic who helped architect and implemented the open platform and Alex Oberhauser and Matt Commons of Cambridge Blockchain for the KYC use case and integration.

money exchange network, which in some instances are run by terrorist organizations. Hence, not only are KYC/AML regulations onerous and costly to first world banks and economies, they are also an impediment to the growth and welfare of developing economies.

Current methods for achieving KYC and AML compliance are still dependent upon dated documentation and oversight procedures that are unreliable, costly, and vulnerable to fraud. Current practices are also vulnerable to privacy and civil liberties abuses by governments and private actors. This need not be the case. Over the last five years, there have been enormous strides in the ubiquity of inexpensive smart phones, encryption, machine learning, virtualization and cloud computing. Such innovations now make it feasible to institute a new generation of identity and authentication services that are paradoxically more privacy preserving and more effective in achieving KYC and AML compliance. The adoption of this new approach to identity, data and trusted authorities (See Windhover Principles) requires a change in the mindset and practices of financial services operators and regulators, as it relies upon leveraging the data collection powers of the mobile devices and new forms of decentralized "autonomous services" using blockchain and "zero knowledge" cryptographic techniques.

This paper describes a proof of concept open source pilot that was initiated at the non-profit corporation, ID3 (idcubed.org) in collaboration with another non-profit, Fluxtream.org, and two startup companies, Intrinsic and Cambridge Blockchain. One of the goals of this collaboration was to develop a successor infrastructure to the ID3 Open Mustard Seed Project that was compliant with the Windhover Principles and took advantage of the advances in blockchain, virtualization, and "smart contracts" technologies.

Over this last year the financial services sector has been highly active in developing and testing applications of blockchain technologies to identity, authentication, insurance, and payments. The banking industry consortium, R3, for instance, has

over 40 banks involved in trials and testing of blockchain technologies. Banks such as Well Fargo, Barclays, Commonwealth Bank of Australia, Santander, Deutsch Bank, Citibank, JP Morgan Chase and others have set up their own innovation groups and accelerators. The UK government and the EU are pursing new forms of digital identity authentication that can be federated, trusted and inoperable with the public and private sectors. (see EU Trust Service and eId) Industry groups have been formed such as Open Ledger for open source blockchain and smart contract development for both Ethereum and Bitcoin based services. Nearly one billion dollars has been invested by venture capitalists in blockchain and crypto-currency companies.

The UN, International Telecommunications Union (ITU), U. S. Treasury, World Economic Forum, and NGOs such as the Omidyar and Gates Foundations are exploring different ways to provide KYC/AML identity and authentication for the unbanked on the mobile phone. Another company collaborating with ID3, Consent, is a South African startup that won the South African Barclays competition for serving the unbanked in Africa. Along with several major banks such as UBS, Barclays and Commonwealth Bank of Australia have expressed their support of the WIndhover Principles and Open Mustard Seed in addressing the needs of the unbanked.

Background:

Two years ago a group of international regulators, academics, legal scholars entrepreneurs, non-profit researchers, and activists gathered in Northern New Hampshire to articulate a set of principles that gave individuals control over their personal data and also created a framework for regulatory oversight by KYC/AML regulators. These principles were developed in collaboration with 25 digital currency and financial services companies as well as major international regulatory bodies. It was named one of the best ideas in banking for 2015 by American Banker. Its importance to this pilot is that it represents a growing consensus among new

digital financial services companies, banks, and regulators that individuals should be "self-sovereign" in their control over their identities and personal data. This has significant implications for the architecture of future decentralized financial services and the enforcement of new data privacy policies by the EU., US, and UK authorities around privacy and trusted services. It also calls for open collaboration around developing an open infrastructure for identity and authentication services. The pilot described here follows these principles.

The Windhover Principles for Digital Identity, Trust, and Data

1. Self-Sovereignty of Digital Identity and Personal Data: ***Individuals and groups should have control of their digital personal identities and personal data.***

Today we communicate, share and transact digitally over the Internet. Individuals who make use of the Internet for these purposes should have control over their digital identities, ensuring individual autonomy, trust in their communications and counter parties, as well as in the integrity of the data they share and transact with. Individuals, not social networks, governments, or corporations, should control their identity credentials and personal data. Control of one's identity and personal data means that a person should have unfettered access to their personal data, the ability to verify attributes of their personal identity profile, and the ability to prevent unauthorized public and private access.

We support the collaborative open source development of systems that embody these principles and recognize the need to address the requirements of legacy regulatory mechanisms, including by evolving innovative digital technologies to improve privacy, governance, and enforcement.

2.Proportionate Enforcement and Risk-Based Regulation ***Enhancing / improving personal privacy while promoting effective governance and accommodating legitimate auditing and enforcement needs.***

We encourage innovation in identity, trust, security, and data technologies and policies, to provide effective methods to address governance and enforcement concerns.

Governance includes the concepts of transparency and accountability necessary to protect digital transactions from abuse. We believe these technologies can address public policy interests by enabling appropriate access and verification of identity data. Entities and individuals, acting on the basis of verifiable approvals, including due process and appropriate warrants, should be able to access such data through specific and auditable means. New and evolving digital technologies make it possible to protect an individual's privacy while providing authorized government access to customer identification, due diligence, and transaction monitoring information for legally authorized needs.

3. Ensuring Innovation in Trust and Privacy:

An effective, autonomous identity system reiteratively furthers trust, security, governance, accountability and privacy Protecting privacy and fostering trust and governance are foundational Windhover Principles that support a fully functional identity system designed to collect and analyze data in a network in which identities are continuously and independently authenticated. These core principles are intended to foster development of more trustworthy, effective, and resilient products and services to minimize the risks and costs of fraud, money laundering, terrorist financing, and other criminal activity.

4**. Open Source Collaboration and Continuous Innovation:** ***An inclusive, open source methodology to build systems that embody these Principles.***

Supporters of the Windhover Principles agree to cooperate to build systems that deliver these requirements and to participate in Living Labs to develop strong and innovative technical product solutions that interoperate to meet these challenges.

Approach:

The requirement that banks undertake KYC and AML tests of their clients has been one way government authorities, especially U.S. law enforcement and U.S. Treasury have been able to crack down on money laundering and terrorist activities. It was based upon credentials, rules, and methods that were essentially paper based and

developed prior to the Internet and mobile banking. Banks are "deputized" as the primary trusted third party to track, identify and report suspicious financial activity. With the advent of mobile banking, cryptography, crypto-currencies, and the blockchain the manner in which funds can and will be transferred around the world has dramatically changed. Not only has it become easier to transfer funds around the world without the need for costly banking intermediaries, it can also can be done with better and more current digital credentials and data analytics.

On the down side, however, encrypted phones and messaging can make it all the more difficult for law enforcement to distinguish bad actors from those who simply want to maintain the confidentiality and privacy of their communications and transactions. The approach taken here is intended to overcome some of these problems and to fully leverage the capabilities - current and future - of smart phones, smart contracts, blockchains and cryptography to authenticate and secure all transactions without revealing potentially personal identifying information. The goal of this design was not to develop an "app" per se, but an Applications Interface (API) framework and platform whereby different kinds of identity and authenticated services could be implemented, tested and evolved to meet the needs of different constituents and evolving technologies. This approach has only become feasible within the last few years due to the rapid adoption and innovation in "virtualization" and "containerization" technologies. Personal data accounts and bundles of applications services can now be "containerized" and automatically provisioned and administered in public and private clouds around the world. These developments enable the rapid and secure provisioning of person banking accounts at a scale to support potentially billions of bank account holders.

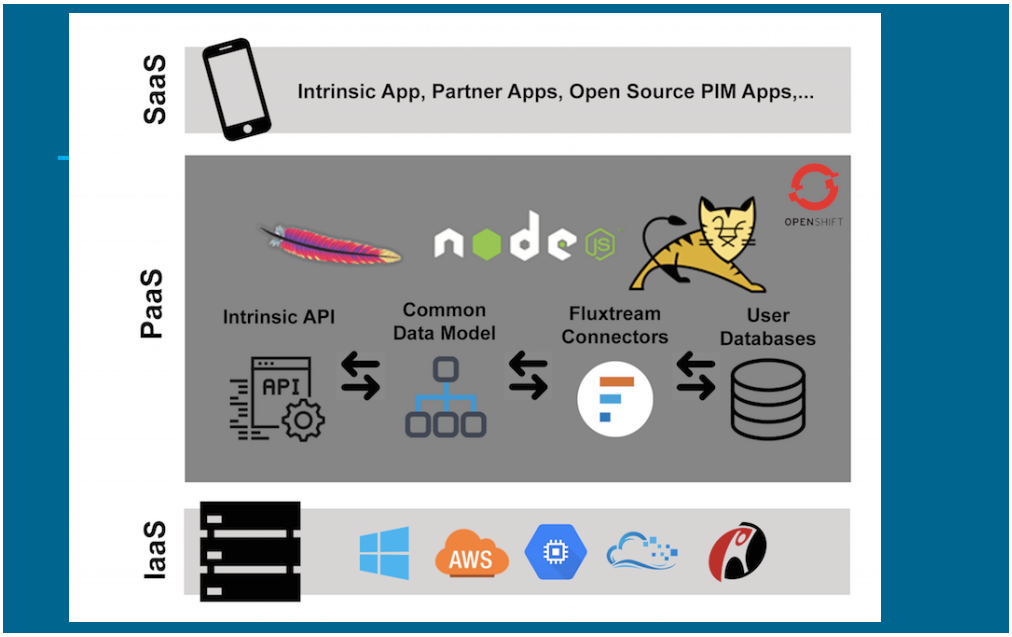
Another key design point is that we want to make all the authentication and credentialing services self-contained within the smart phone. A new bank account applicant need not have a physical face to face meeting with a government or banking authority. Rather individuals should be able to generate and authenticate identity, KYC, and other credentials off of their phone following internationally

agreed to standards and protocols. Through its camera, micro-phone, GPSs Bluetooth, and accelerometer capabilities, a $50 smart phone can be used to generate and verify multi-factor biometrics to satisfy even the most stringent of KYC/AML requirements. For example, some current KYC regulations require a utility bill to prove residence. In developing countries there may not be utility bills or street addresses. Even when utility bills and street addresses are used, they can be easily spoofed, and as people move, they become untraceable. By having an active credential that increases or decreases in value over time based upon GPS activity, regulators would have a more trustworthy credential than a utility bills and also provide law enforcement with a more accurate means of locating criminals.

.

One of the challenges of building a general framework and platform for deploying decentralized autonomous organizations and authorities is being able to "abstract" out" all key components. The design goal is to provide open APIs platform that can evolve with the technology and offer a wide choice in what types of micro-services it can support. The Red Hat OpenShift/Origin framework makes it possible to have a Platform as a Service (PaaS) that is agnostic as to different programing languages, frameworks and applications and is able to deploy and administer different packages of services and applications autonomously in the cloud. (see diagram below).

For example there are many kinds of biometrics (voice, gesture, motion, video) as well as behavior metrics (history of movement and interaction patterns) that can be used to create a multi-factor biometric and behavior-metric for asserting and authenticating core identity. Likewise, there are many ways of setting up personal data accounts and managing those accounts in the cloud. For that reason this task should be done through open APIs by different vendors of such services. Another important use case, is provide open APIs around different measures of credit risk, reputation, and risk scoring. This already is an area of rapid innovation and has evolved far from the traditional FICA scores used in U.S.



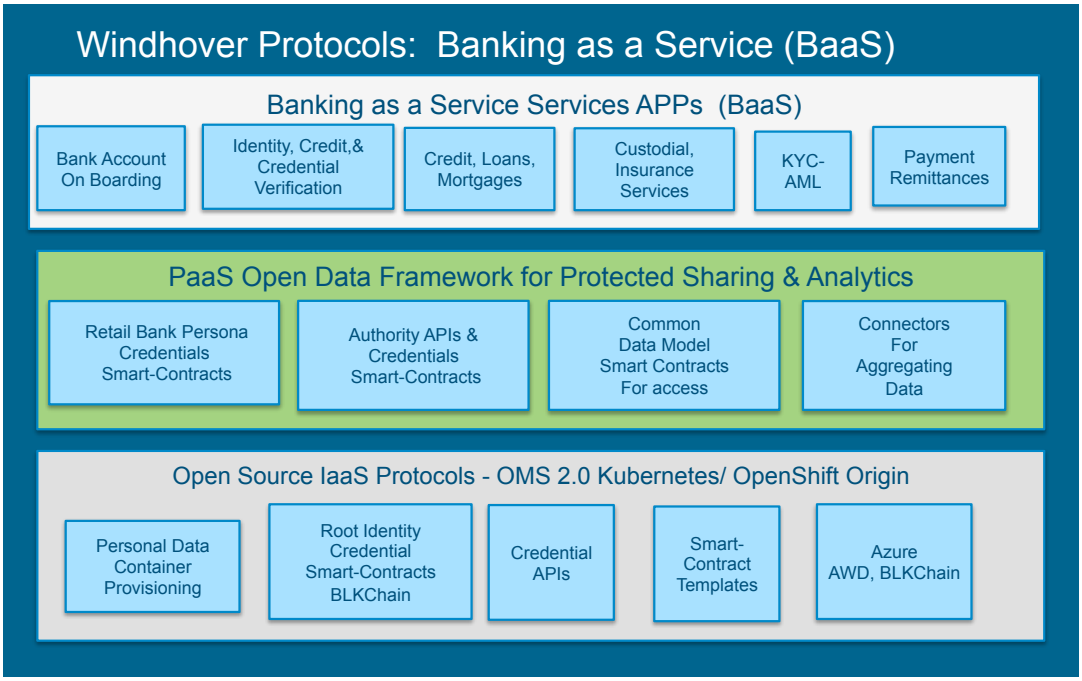
Redhat OpenShift Framework for Platform as a Service

Key Architectural Considerations: Decentralization and Governance

One of the arguments for fully decentralized services with autonomous authorities is that it can be "trustless" in that no human third party is required and one can trust the code of the algorithms in the smart contracts and the blockchain. For the time being we believe that this is not a practical solution as even Bitcoin mining is dominated by roughly 8 "foundaries" primarily in China. Moreover, the informal governance of the Bitcoin protocol is concentrated among a small group of unelected core developers without any independent oversight These developers are themselves divided on how to proceed further with new releases of the Bitcoin software despite the efforts and funding of the MIT Digital Currency Initiative.

This dysfunction within the Bitcoin community, however, does not mean that the decentralized services and the decentralization, encryption and anonymization of data storage and access are not feasible nor important. They are important but they are not perfect and will need to evolve with the technology. Hence, in the meantime

it is important to have open governance mechanisms with credentialed people in the loop providing oversight and accountability. It is our view that through credentialing, auditing and randomization of oversight accountability and trust can be achieved in the near term with decentralized services.

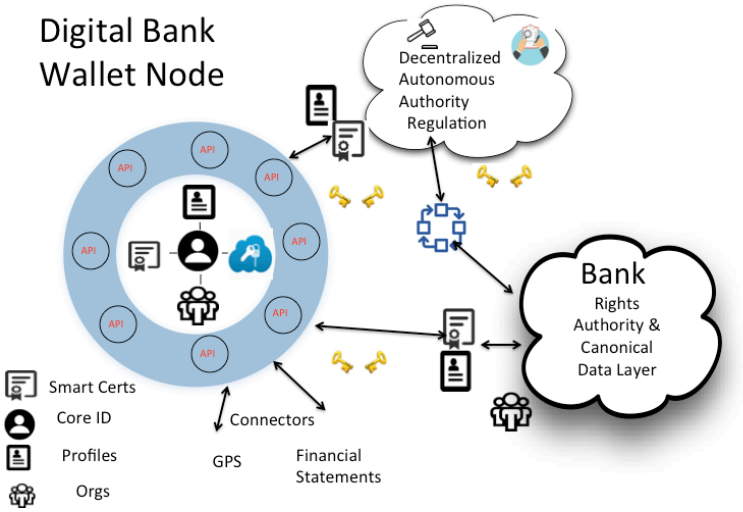


Overview of Banking As a Service Platform Stack

Key Components for a Open API Framework and Platform for Forming and Participating in Decentralized Organizations and Authorities

1. ***Provisioning Personal Data Accounts and Collection of Personal Data in Private or Public Clouds With Individual Control***: A foundational principle that cannot be overemphasized is that the individual at the edge of the network is in control over their data and identities. They are the natural aggregation point for all personal data. Through U.S. and EU law individuals are entitled to have copies of all their personal data. These can be accessed through connectors (APIs) that take that data off the different sites and store them in the personal data container. By having a canonical data schema the

individual becomes the natural aggregation point for data and the catalyst for network effects/preferential attachment whereby all parties come to rely upon personal data containers for access to personal data. In short, personal data containers become "silo busters" and the natural aggregator of data. It should be pointed out that the individual is the "logical" aggregation point, but in "physical" implementation, the data may be highly distributed and encrypted. Through such connectors individuals can automatically acquire their data off other sites and services such as Google, Facebook, Amazon, banks, health services, schools, DMVs, and retailers.



Another key principle is that personal data containers can be hosted and administered in any cloud services that abides by the Service Level Agreements (SLA) of the individual. At any point an individual can take all their data off one service and transfer it to another without cost or convenience penalty. This requirement has also been adopted by a number of international banks as well and is consistent with U.S. and EU regulations about "portability" of personal data.

2. ***Asserting and Authenticating Core Identities:*** As was noted previously, every individual has a biometric and behavior metric "signature" that can uniquely identify them. Since this "signature" is an expression of the uniqueness of the individual and derived from whom they are and how they act, it is self-sovereign and not an artifact of a state or organizational authority. Moreover, a valid core identity is absolutely essential to protect the integrity and authenticity of any subsequent credentials issued by a state or other authorities. Without such a core credential it would be possible for an individual to acquire multiple personas and fraudulently assert that they are different. Sybil Attacks are an example of such an exploit as are any instance where someone has an identity credential revoked and is able to get a new one. How that core identity signature is derived and verified is beyond the scope of this project, but suffice it to say that there are many techniques being explored. Hence, core identity is treated here a micro-service that is accessible through an API.

3. ***Creating Organizations, Personas, Smart-Certificates:*** Once the prior two steps are completed, the next step is to create an appropriate "org" or organizational entity. The reason for this is that according to our approach all "personas" - profiles or "roles" are defined in terms of an organizational form. This can range enormously from something that is informal such as a, family, or transitory such as a soccer club, or as permanent and formal as a bank, a government agency, a LLC, or a Delaware Workers Cooperative. Yet in every case the organization decides what the key attributes are for a specific persona and what privileges that persona has visa vie other personas and members of the organization. In more formal organizations, there may be by-laws and intricate rules of voting, participation, resource allocation, succession, dispute resolution, etc. Though we have explored different digital forms of organizational governance in earlier research ((www.lawlab.org) that is not within the scope of research here. There is

ongoing research and development on smart contracts for organizations being undertaken by Ethereum , Open Ledger, academia and startups.

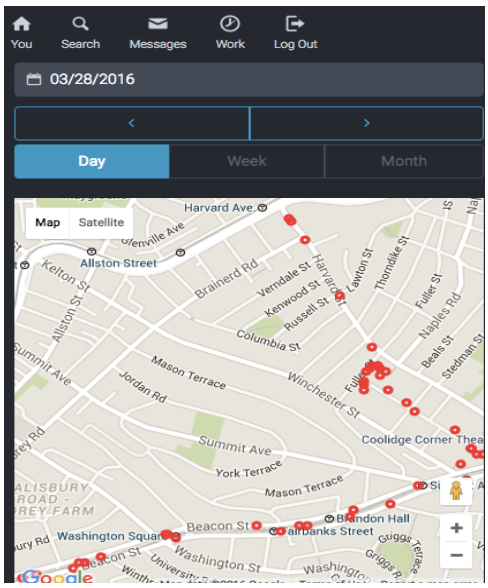
The other critical component of an organization is the smart-certificate that controls how individuals' personal data are accessed and used. For that a member of an organization is granted access tokens governed by the rules of smart contracts/certificates that are specific to certain attributes or the data or modes of interacting with the data. For example, a certificate may only allow certain questions and queries for a limited time or limit access to only meta-data. The point is that there is a wide range of choices available for how to design the permissions and the access tokens - each with different degrees for privacy and security risks. Also the verification of all activities involving access tokens are recorded on a private blockchain (Ethereum) so as to provide accountability, auditability and transparency.

4. **Providing Independent Governance and Compliance:** There is another form of governance that is not limited to making sure that the rules of an organization are being followed and enforced. That is in the area of applying and enforcing data privacy and security measures that are compliant with different private agreements and different national policies - such as the U.S. White House Consumer Privacy Data Bill of Rights and the E.U. Data Privacy Directorate. Especially concerning to many privacy advocates is the use of personal GPS data to infer living, working, association, and purchasing patterns. Such data are highly identifying and subject to abuse and hence, are highly regulated in some jurisdiction. Through the implementation of and enforcement of internationally agreed to data privacy provisions on the blockchain and through the use of smart certificates we believe that "data commons" can be implemented and enforced that serve the needs of different stakeholders. The oversight of these regulations and agreements can be implemented and enforced to a large degree through smart contracts

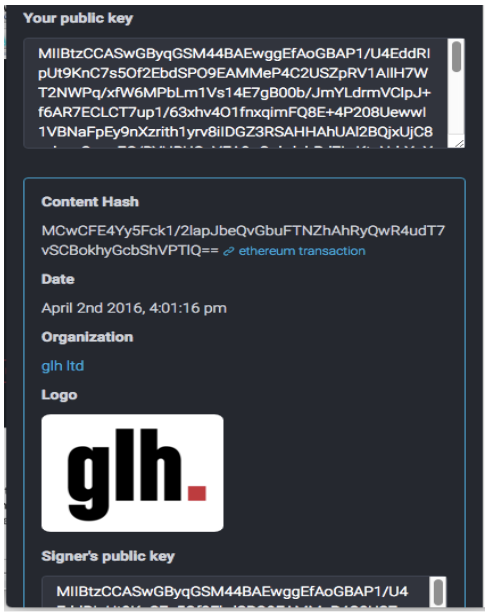
with the proviso for the near future that there be some independent human oversight body.

Trial Testing of Platform:

The proof of concept pilot platform was trial tested for a sample of users for three different use cases: banking; work and a data commons. The Platform as a service was implemented using Red Hat Open Shift/Origin enabling an individual to set up a core identity, join an organization and assert and acquire a credential from a third party. The onboarding process also enabled an individual to set up their own personal data container in a cloud service and use Fluxtream connectors to collect GPS data from a user's mobile phone and store, visualize and control it in the Personal data container. (see screen shot 1) By placing it within the container the individual is able to make it available for sharing with a third party with a smart control control and verification. The individual is also able to asset a credential such as a particular work competence or affiliation and have it verified and signed on the block chain by a trusted third party. In the screen shoot example, below the individual's public key and that of the signing party (GLH) is shown.



Screen Shot 1



Screen Shot 2

Proof of Concept KYC and AML Compliance Using Blockchain for Rigorous Use Case: Catastrophe Bonds

The following is a highly sophisticated use case of a KYC/AML process for the purchase of a catastrophe bond by a highly qualified buyer. The requirements for this process are much more involved, (five different checks in all) stringent than for most banking services, but it illustrates how this process can be undertaken digitally and secured using the blockchain. This KYC process was developed by Cambridge Blockchain and made part of the Intrinsic/OMS open platform through API integration. This same process can be applied to compliance for less onerous KYC checks for unbanked and for determining compliance with U.S. and EU data privacy provisions.

Cambridge Blockchain

Counterparty Diligence Report

— Generated 12 February 2016, 12:06:03 GMT —

— Pre-Trade Buyer Diligence —

APPROVED

11 Feb 2016, 12:53:00 GMT

— Security Trade Status —

SALE CONFIRMED

11 Feb 2016, 12:57:22 GMT

Security Summary

Issuer	Azzurro Re I Limited
Sponsor	UnipolSai Assicurazioni S.p.A.
Calculation Agent	AIR Worldwide
Covered Risk	European earthquake
Issue Size	EUR 200,000,000
Coupon	2.15 %
Trigger Type	Parametric
Issue Date	16 Jun 2015
Maturity Date	16 Jan 2019
CUSIP	055065AA4

Transaction Summary

Account	1907 Pine River Fund Ltd
Account LEI	549300B9OGLHNK048630
Submission Time	11 Feb 2016, 12:56:03 GMT
Block Verification Time	11 Feb 2016, 12:57:22 GMT
Platform	CatBlock Express
Notional	EUR 10,000,000
Clean Price	101.50
Dirty Proceeds	EUR 10,364,795
Proceed Form	CatBlock Cash Tokens

Counterparty Pre-Trade Diligence of Buyer

1. KYC/AML/ATF Check		☑
1.1 Identity Provider	→ Whitelisted EU Bank	☑
1.2 Most recent validation	→ < 1 year	☑
1.3 Primary validation criteria	→ EU Directive 2005/60/EC	☑
2. Banking Secrecy Act Check	→ Counterparty-Only	☑
3. Securities Act Check	→ 144A, Non-US QIB	☑
4. Commodities Exchange Act Check	→ Safe harbor security exemption	☑
5. Investor Suitability Check	→ LEI segment yields non-whitelisted country	⚑

>>> Advanced Diligence Checks REQUEST >>>

5. R1 LEI Country	→ Italy	☑
5. R2 Identity Provider	→ Whitelisted Italian Bank	☑
5. R3 Applicable Rule	→ Italy Decree 58 Art 100	☑
5. R4 Exemption Provided	→ Consob regulation 11971 Art 33 (insurance license exemption)	☑

<<< Advanced Diligence Checks ACCEPTED <<<

Counterparty **APPROVED**

Detailed Blockchain-Backed Proof

Smart contract call by seller to buyer with contract address 0x5070088c14bba7299b991efd9d08fe80973c8575 > .
Sensitive information in plaintext are send via off-chain secure channel.

1. KYC/AML/ATF Check (Block #34567)

→ SmartContract#**requestProperty**(*idp*)
← (blockchain return) **0x8d7d8948f67c531298aef20f7a436b7add0fb6bad4459948655ae5dd9cbb443c**
← (off-chain return) **Whitelisted EU Bank**
sha256('Whitelisted EU Bank') == 0x8d7d8948f67c531298aef20f7a436b7add0fb6bad4459948655ae5dd9cbb443c

→ SmartContract#**requestProperty**(*lastValidation*)
← (blockchain return) **0xa4c0cb3c925393ccfdcd0259150806f09179642f75366d4ff8c5629de32a5d4d**
← (off-chain return) **1 Jan 2016, 8:57:22 GMT**
sha256('1 Jan 2016, 8:57:22 GMT') == 0xa4c0cb3c925393ccfdcd0259150806f09179642f75366d4ff8c5629de32a5d4d

→ SmartContract#**requestProperty**(*primaryValidationCriteria*)
← (blockchain return) **0x01b6dddeb4873ee2ce1adc60d263429eb18b90c5b6b620f788e05f7d780b5774**
← (off-chain return) **EU Directive 2005/60/EC**
sha256('EU Directive 2005/60/EC') == 0x01b6dddeb4873ee2ce1adc60d263429eb18b90c5b6b620f788e05f7d780b5774

2. Banking Secrecy Act Check (Block #34567)

→ SmartContract#**requestProperty**(*bankingSecrecyAct*)
← (blockchain return) **0x3fa05b0737ec961704759230151de3e2e6a2749daf99b9414907e0446faed945**
← (off-chain return) **Counterparty-Only**
sha256('Counterparty-Only') == 0x3fa05b0737ec961704759230151de3e2e6a2749daf99b9414907e0446faed945

3. Securities Act Check (Block #34567)

→ SmartContract#**requestProperty**(*bankingSecrecyAct*)
← (blockchain return) **0xb186de1b4ad32b0e4b6a48b5f412d37c1a1be2ff2bf8c43feaa8e225eb0e1a54**
← (off-chain return) **144A, Non-US QIB**
sha256('144A, Non-US QIB') == 0xb186de1b4ad32b0e4b6a48b5f412d37c1a1be2ff2bf8c43feaa8e225eb0e1a54

4. Commodities Exchange Act Check (Block #34567)

→ SmartContract#**requestProperty**(*commoditiesExchangeAct*)
← (blockchain return) **0xc5cdb319111c2942884a2138b99f19c472e640542721adeb25a18ead9f023fd8**
← (off-chain return) **Safe harbor security exemption**
sha256('Safe harbor security exemption') == 0xc5cdb319111c2942884a2138b99f19c472e640542721adeb25a18ead9f023fd8

5. Investor Suitability Check (Block #34571)

→ SmartContract#**requestProperty**(*loiCountry*)
← (blockchain return) **0x5a9cf672c8be6b5ab9546a2fb49b06dd81a4e364c86ed023898c49d9bb0605dc**
← (off-chain return) **Italy**
sha256('Italy') == 0x5a9cf672c8be6b5ab9546a2fb49b06dd81a4e364c86ed023898c49d9bb0605dc

Conclusion:

This project demonstrated the technical feasibility of developing an open APIs platform for implementing the Windhover Principles to form decentralized autonomous organizations for KYC/AML versification on a mobile platform. Part of the challenge going forward is to develop autonomous smart contracts for organizational design and governance for regulatory compliance. The blockchain and smart contract technology is in its early phases and questions remain about production level performance at massive scale. Nonetheless, decentralized banking services using digital credentials and secure decentralized ledgers on mobile platforms offer great promise for secure, affordable and privacy persevering banking services for both the banked and the unbanked.

Sources & Bibliography

American Banker, 10 Big Ideas to Improve Your Bank, December 31, 2015; http://www.americanbanker.com/gallery/10-big-ideas-to-improve-your-bank-in-2015-1071923-1.html

Clippinger, John, Bollier, David eds. From Bitcoin to Burning Man and Beyond: The Pursuit of Identity and Autonomy in the Digital Society, 2015, Amazon Kindle.

Clippinger, John Henry, The Crowd of One; The Future of Individual Identity, Perseus, Public Affairs, 2009

Ethereum.org

European Union
Trust Services and eID
https://ec.europa.eu/digital-single-market/en/trust-services-and-eid

Financial Action Task Force:

GUIDANCE
Anti-Money Laundering and
Terrorist Financing Measures and
Financial Inclusion Feb. 2013
GUIDANCE FOR A RISK-BASED APPROACH
PREPAID CARDS,
MOBILE PAYMENTS AND
INTERNET-BASED PAYMENT
SERVICES 2013

INTERNATIONAL STANDARDS
ON COMBATING MONEY LAUNDERING
AND THE FINANCING OF
TERRORISM & PROLIFERATION

The FATF Recommendations 2012
FATF (2012), International Standards on Combating Money Laundering and the Financing of Terrorism
& Proliferation, updated October 2015, FATF, Paris, France,
www.fatf-gafi.org/recommendations.html
DOI: 10.17265/1934-7332

Hardjorno, Thomas, Clippinger, John, Degan,Patrick,
On the Design of Trustworthy Compute Frameworks for Self-Organizing Digital Institutions from 16th International Conference on Human-Computer Interaction, June 22-27,2014.

Hochstein, Marc, Rethink Identity so Personal Data Can Stay Personal, American Banker, December 21, 2015

OpenLedger Project
https://www.hyperledger.org

White House Consumer Data Privacy in a Networked Work: A Framework for Protecting Privacy and Promoting Innovation in The Global Digital Economy :
https://www.whitehouse.gov/sites/default/files/privacy-final.pdf

World Economic Forum
Disruptive Innovation in Financial Services
Impact Project Applications
Working Group Consultations
September 2015