The Secure ESG Reporting Network

Technical Whitepaper
&
Architectural Overview

Team Zabel

30th August 2021
Version 2_8

Contents

1. Introduction

Many organisations possess legacy ESG reports in formats such as PDF which have proven difficult to digitalise.

Additionally, it has been challenging to compare information for various industries and sectors across different geographic locations and economies.

The purpose of the Secure ESG Reporting Network is to create a trusted integrated financial and non-financial reporting network, powered by a DLT(Blockchain) network (Distributed Ledger Technology) and taking advantage of all the benefits that this technology provides.

We also transform both digital and non-digital information into fully digitalised structured taxonomies which are manageable, comparable, and readable by both people and machines alike.

2. Our Approach

2.1. Our product addresses the issues identified above by:

1) Accepting ESG and/or financial reports in various formats and standardising them to a structured data format. The base of our information uses XBRL (eXtensible Business Reporting Language). (https://www.xbrl.org/) . However, we have extended the technology by incorporating:
    a. Object based JSON XBRL to enable the efficient exchange of data objects over webservices type APIs
    b. Use of XHTML for ease of management of reporting dashboards, allowing users to drilldown and 'slice & dice' through information in customised ways according to their needs
    c. The implementation of an object-relational database (PostgreSQL) over IBM Cloud servers, which optimises the storage of information across a decentralised ledger network architecture (https://www.postgresql.org/)
        - ➢PostgreSQL is fully supported by IBM Cloud Services
    d. The use of this architecture facilitates the data to interoperate the transaction and reporting formats simultaneously:
        - ➢As information/reports are exchanged and updated among participants in real-time
        - ➢Users can simultaneously apply AI and BI (Business Intelligence) tools on the information to create complex analytics including multidimensional hyper-cube technology etc.
2) We have created a best-of-breed hybrid structured data taxonomy based on XBRL which encompasses the key indicators from several different financial and non-financial reporting standards including, IFRS, GAAP, GRI, SASB, UNSDG etc
3) We have developed a unique architecture which combines the use of:
    a. Latest 3rd Generation DLT technology – Hedera Hashgraph (https://hedera.com/). Hedera Hashgraph is the fastest and most energy efficient DLT networks in existence and boasts very low microtransaction fees to operate
    b. IBM Cloud services to run the decentralised application (Dapps)
        - ➢Note that IBM are one of the Hedera Governing CouncilMembers and run their own Hedera Hashgraph Proof-of-Stake Node on the IBM Cloud Services, and thus provides direct two-way benefits to run our product
        - ➢https://hedera.com/council

4) The Secure ESG Reporting Network Dapps are successfully deployed and running on the IBM Cloud Account provided by the G20 TechSprint 2021

5) The Secure ESG Reporting Network is prepared to include value-add participants. These include financial and ESG assurance and auditing firms that review reports. The audit/assurance firms can have their own Certification NFT (Non-Fungible Token) which is added to the original Report NFT. In this way report viewers such as banks can see the exact level of assurance that has taken place for each report they review

3. Our Choice of Strategic Partnerships

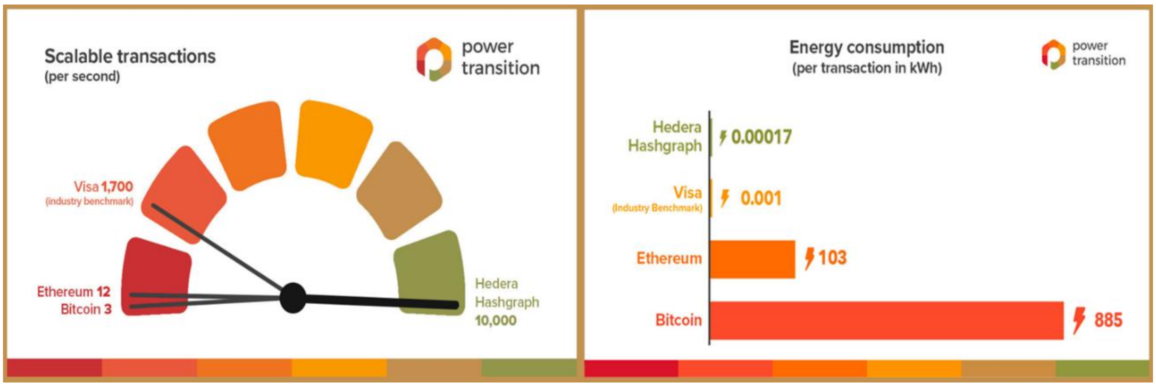
The Choice of Hedera Hashgraph DLT(Blockchain)

3.1. Lately the Blockchain sector has been criticised for:

- Its enormous consumption of electrical energy to operate. For instance, the Bitcoin network consumes as much electricity per day as 5 large households in the USA (>800 Kilowatt-hours)
- The slowness to complete transactions. Bitcoin network is only capable of completing only about 6 transactions per second
- High cost of transaction fees is another problem facing legacy Blockchain networks. Bitcoin costs over US$23 per transaction
- The governance model of legacy Blockchain networks has also been brought into question. Blockchain networks like Bitcoin and Ethereum are governed by the votes of the 'mining' community. Past performance has shown that the'mining community' prioritises its own financial gains above the overall efficiency and the benefit to users

3.2. Hedera Hashgraph:

- Uses a tiny fraction of the amount energy compared with other Blockchain networks (< 1 watt-hour) and
- Operates at over 10,000 transactions per second
- Only charges US$0.0017 per transaction. See figure below.
- Unlike other Blockchain networks, Governance of the Hedera Hashgraph is managed by a 39 strong Governing Council who determine its technical and financial roadmap. The Hedera Governing Council Members, which includes IBM, are all Fortune100 companies and world-leading academic institutions from around the world

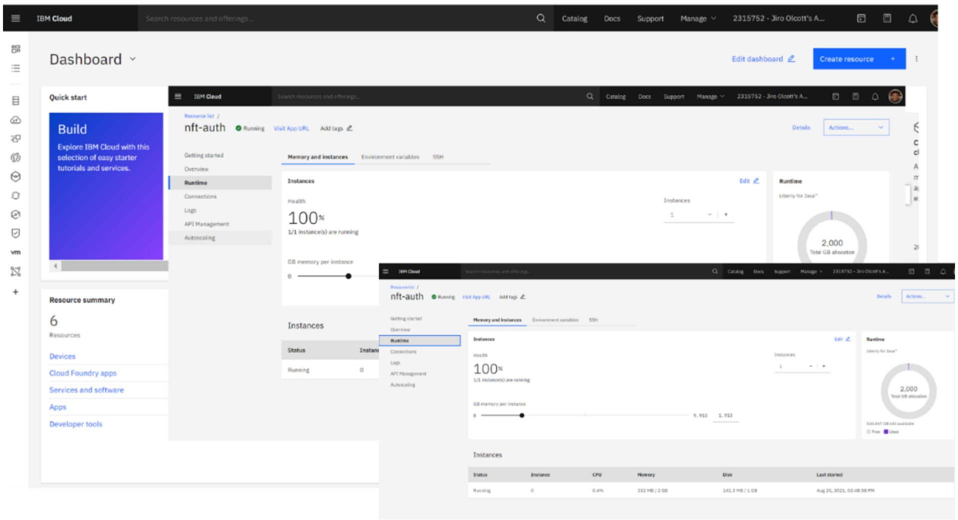


https://ptvolts.com/sites/default/files/documents/sustainable-blockchain-power-transition.pdf

3.3. Why Hedera: Conclusion

We can conclude that unlike legacy Blockchain networks, Hedera Hashgraph is ideally suited for high-volume commercial business models

3.4. Why IBM Cloud Server



Our Dapps run on the cloud servers using the credit account provided through the G20 TechSprint. Our systems can run on Google-GCP or IBM-Cloud. We see the relationship with IBM particularly strategic since many financial institutions are accustomed to running their IT infrastructures on IBM systems, and the fact that IBM are a Hedera Governing Council Member and already running a Hedera Hashgraph Proof-of-Stake Node on the IBM Cloud Services.

4. Cybersecurty

Worldclass cybersecurity is one of the great benefits that DLT(Blockchain) technology brings to business. Hedera Hashgraph is the preeminent leader in cybersecuity. The following table illustrated by Harvey-Balls shows how Hedera addresses cybercecurty compareed to peers:

Cybercrime Scorecard

High-level view of cybercrime categories comparison:

Cybercrime Category	Description	Cybercrime Scorecard			
		Bitcoin	Ethereum	Hashgraph	VISA
DDoS	Rendering systems inoperative	◕	◕	●	◑
Surveillance Hacking	Illegal gleaning of private information	●	●	●	◔
Sybil and Bot Attacks	Creating false identities/users	◕	◕	●	◔
Network Infiltration	Poisoning network functionality	●	●	●	◑
Overall Score:		350	350	400	150

Cybercrime Scorecard Index		Score
Highest levels of Cybercrime Prevention have been implemented with solid ongoing security program	●	100
Cybercrime prevention is good, but more attention required as criminals evolve	◕	75
Cybercrime issue addressed but poorly designed and implemented	◑	50
Cybercrime has been identified, but inadequate effort made to prevent it	◔	25
Cybercrime issue has not been identified or addressed	○	0

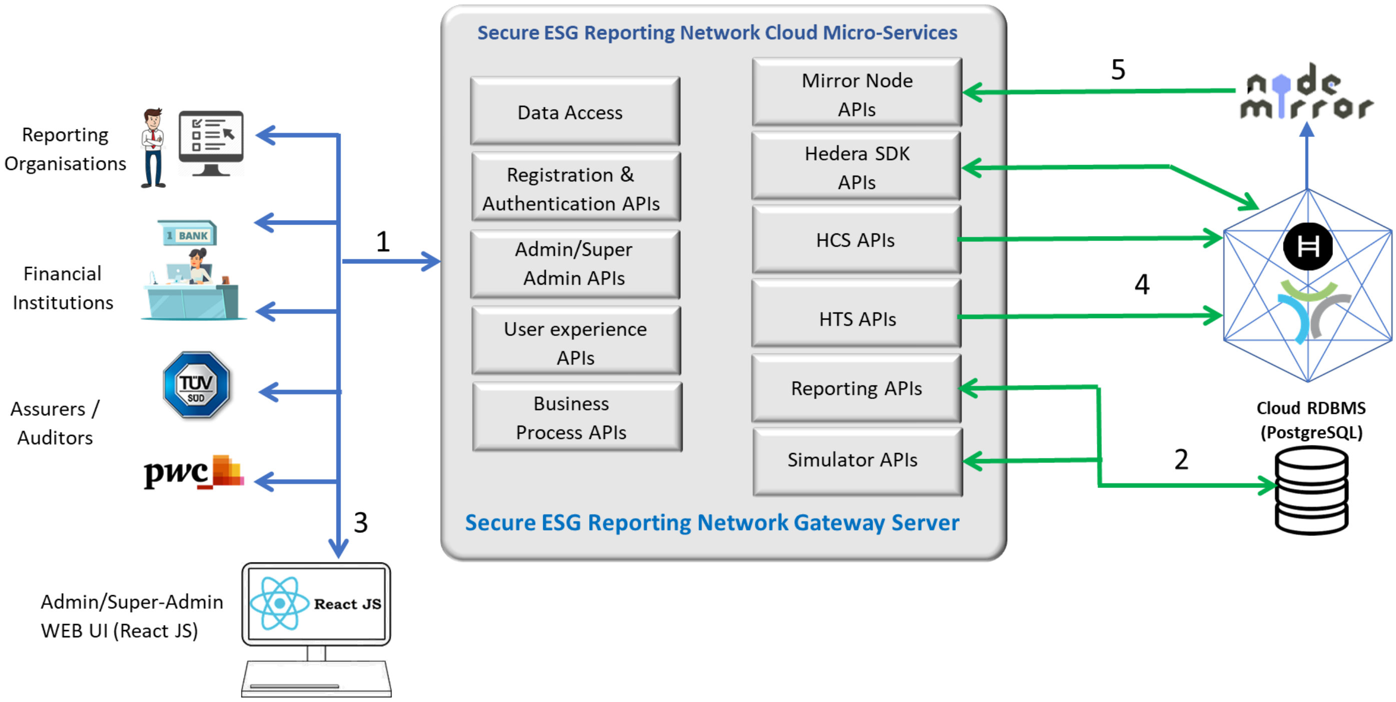
4.1. Cybersecurity References:

https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018
https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/overviewoffraudandcomputermisusestatisticsforenglandandwales/2018-01-25
https://www.hedera.com/hh-whitepaper-v1.4-181017.pdf
https://www.cointelligence.com/content/hashgraph-vs-blockchain-secure-fast-transaction-processing-system/

5. Microservices Architecture

Our microservices architecture is the ideal approach to customise, deploy and scale our Secure ESG Reporting Network Dapps. The system can be quickly customised and adapted to various markets and user demands at the microservice level.

The following diagram shows how the Secure ESG Reporting Network Cloud uses Cloud based Micro-Services to manage application architectures and the information flowing among participants and business functionality:



1. Each request/response uses a Secure JWT Token over HTTPS - SSL/TLS for all requests. Secure ESG Reporting Network Gateway Server is Firewall protected

2. REST APIs communicate with IBM Cloud database providing persistent records of Hedera Transactions and operations data for reporting purposes

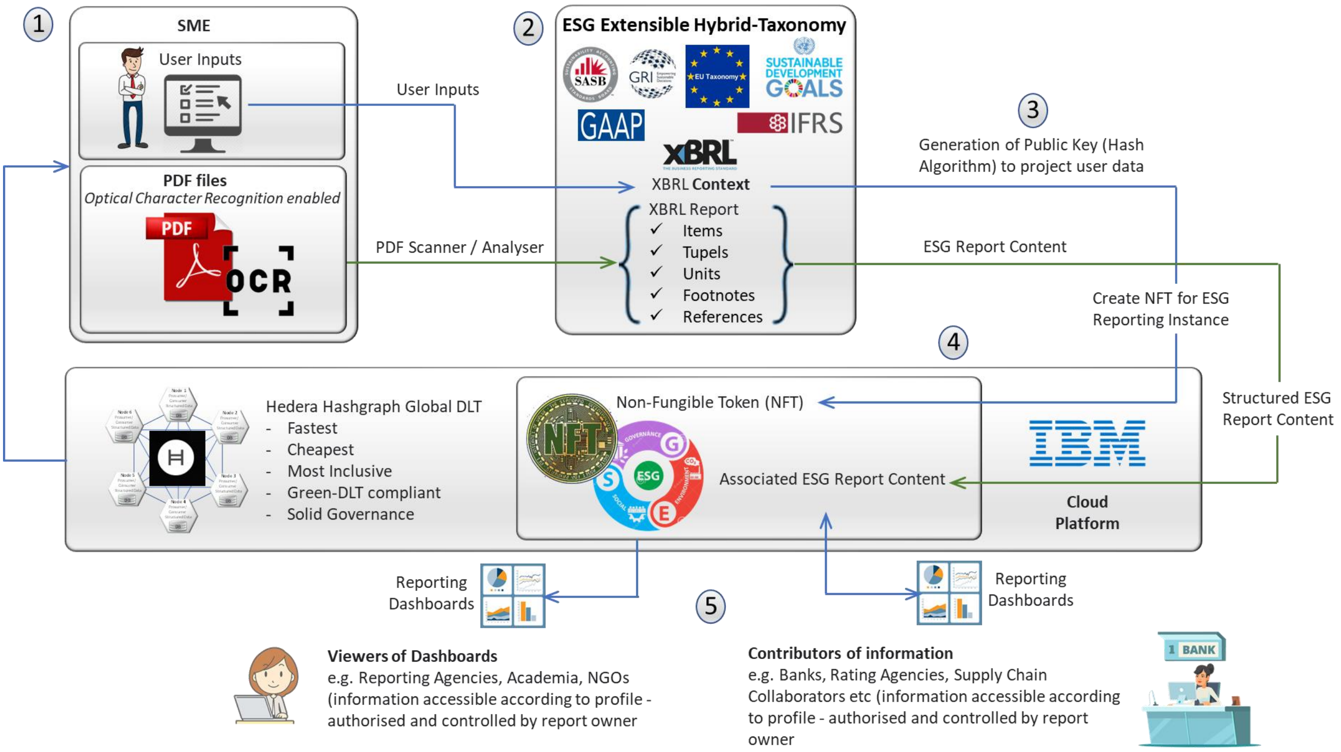
3. Admin/Super-Admin APIs are used for central NFT and fungible-token banking and administration as well as user provisioning and security

4. HCS and HTS (+ SDK) APIs manage and administer all interactions with the Hedera Mainnet

5. MirrorNode APIs enable stakeholder to subscribe to all information that that has been published onto the Hedera Mainnet by HCS/HTS

6. Secure ESG Reporting Network – sequence of reporting operations:

1. After the Reporting Organisation has created a network account the reporting manager uploads PDF reports into the application along with some report details
2. The application takes the report file and turns it into XBRL format using our hybrid-structured data taxonomy
3. The system then generates a unique NFT and attaches it to the new report
4. The Report NFT is then circulated around the global Hedera DLT network and made available to all other Secure ESG Reporting Network
5. Participant request to view a report and the reporting organisation then grant access to view. Feedback can then be sent back to the reporting organisation. Note that the level of private information disclosed in the reports depends on the profile of the requesting organisation i.e., either a bank, who is doing business with the company or another organisation e.g. an ESG NGO who is simply interested in the statistics



1
SME
User Inputs
PDF files
Optical Character Recognition enabled
PDF
OCR
User Inputs
PDF Scanner / Analyser
2
ESG Extensible Hybrid-Taxonomy
SASB
GRI
EU Taxonomy
SUSTAINABLE DEVELOPMENT GOALS
GAAP
IFRS
XBRL
XBRL Context
XBRL Report
✓ Items
✓ Tupels
✓ Units
✓ Footnotes
✓ References
3
Generation of Public Key (Hash Algorithm) to project user data
ESG Report Content
Create NFT for ESG Reporting Instance
4
Structured ESG Report Content
Hedera Hashgraph Global DLT
- Fastest
- Cheapest
- Most Inclusive
- Green-DLT compliant
- Solid Governance
Non-Fungible Token (NFT)
NFT
GOVERNANCE
G
ESG
S
E
Associated ESG Report Content
IBM
Cloud Platform
Reporting Dashboards
5
Reporting Dashboards
Viewers of Dashboards
e.g. Reporting Agencies, Academia, NGOs (information accessible according to profile - authorised and controlled by report owner
Contributors of information
e.g. Banks, Rating Agencies, Supply Chain Collaborators etc (information accessible according to profile - authorised and controlled by report owner
BANK

Note: for the purposes of the G20 TechSprint 2021 competition certain security features have been disabled for simplicity of use within the community. These include:

- OTP email authentication during the Know Your Customer (KYC) process
- 2FA (2-Factor-Autentication) during login

The PDF to XBRL scanning process for the G20 TechSpring pilot is limited in sophistication. However, our platform comes with an Open Integration Bus (OIB) application programming interface (API) that allows the easy integration of 3rd party AI (artificial intelligence) systems that are able to analyse legacy reports in much more detail.

7. Business Model

Our aim is to create the Secure ESG Reporting Network using a profitable sustainable development business framework. To help enable this, we have created a digital currency gateway to incentivise participants to join in:

7.1. The Payment Gateway:

a. The pilot system has included a payment gateway to demonstrate the overall business model for the network operator

b. The payment gateway is denominated in Digital- € and is a fully fungible token, linked directly with the value of the Euro.

c. There are micropayments made for the creation of the Structured Data Report and its connection to an NFT (Non-Fungible Token). Micropayments are also made to view reports.

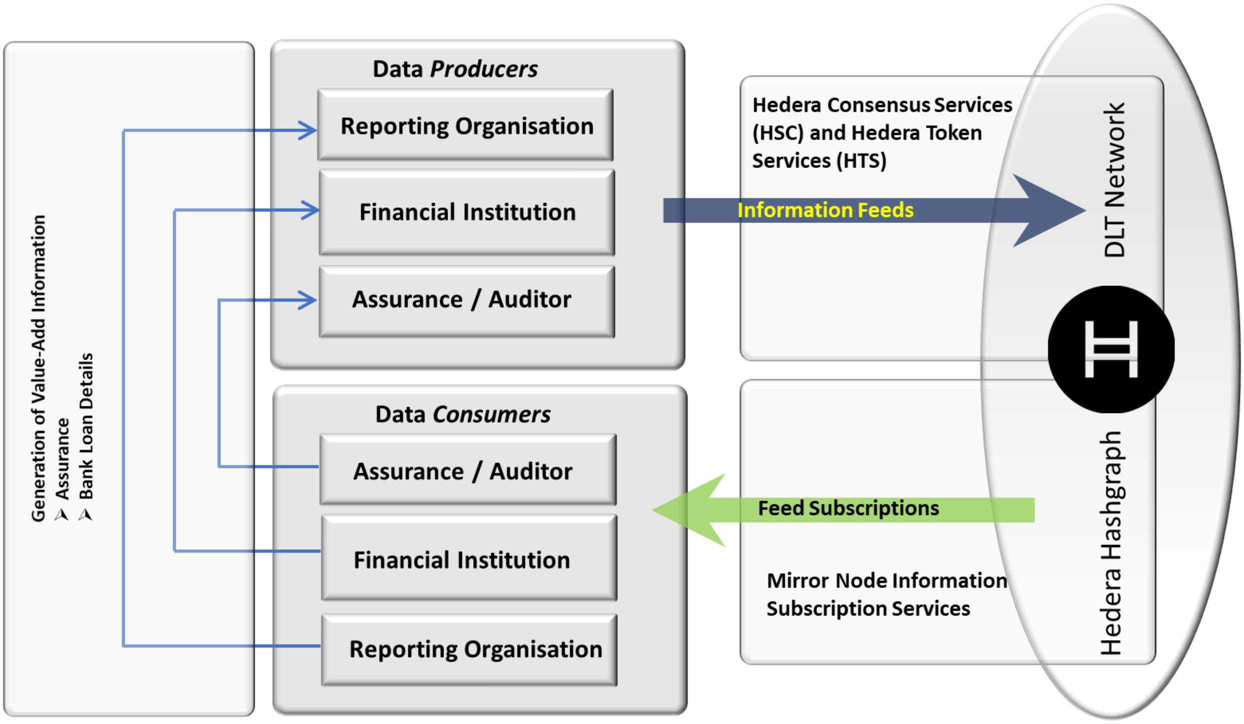
d. This is a pay-as-you-go Software as a Service (SaaS) model and does not require annual subscriptions while allowing the operators to create a sustainable business development model

e. All payments for various functions and flow of funds can be easily modified by the administrator

f. One of the objectives of the payment gateway can be to incentivise producers of reports by offering them payments every time their reports are read

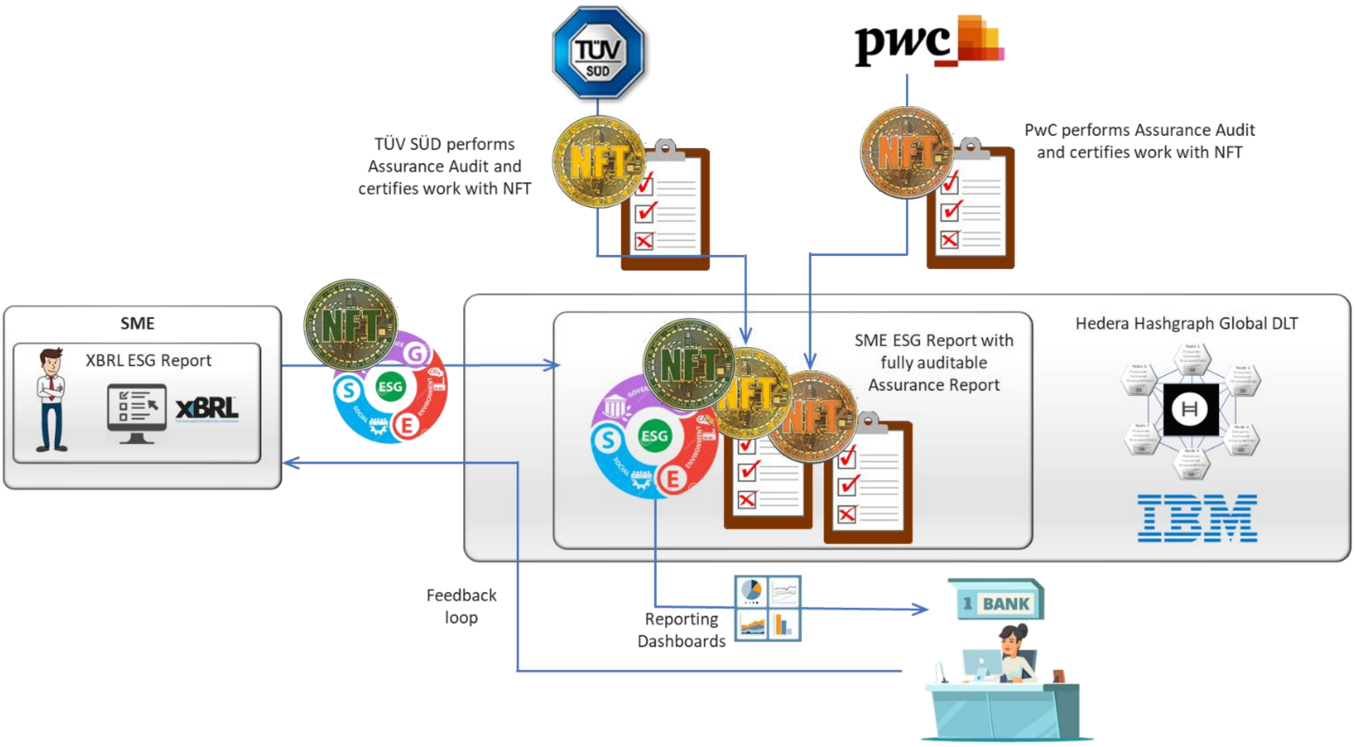
8. Further Value-Add to the Secure ESG Reporting Network

One of the beauties of running Secure ESG Reporting Network is that travels among all participants in decentralised iterative loops where each participant that add value and pass it along in a trusted and secure environment when every action maintains an immutable audit trail.



8.1. Assurance and Banking example

A good example of this iterative value-add loop is the role of the assurance or audit firm who can work with the reports and validate the information. The assurer can then add their own NFT to the original Report NFT in an interlinked chain of NFTs. Then when the banker reviews these reports they will be in not doubt about the authenticity of the reports being reviewed. The following is an illustrative diagram showing the value-add function of the auditor/assurer:


TÜV SÜD
pwc
TÜV SÜD performs Assurance Audit and certifies work with NFT
PwC performs Assurance Audit and certifies work with NFT
NFT
SME
XBRL ESG Report
XBRL
ESG
S
E
G
SME ESG Report with fully auditable Assurance Report
Hedera Hashgraph Global DLT
IBM
Feedback loop
Reporting Dashboards
1 BANK

For any enquiries please contact:

- Jiro Olcott, Director, Guard Global Ltd
- jiro.olcott@guardglobal.org