DID:UNCONF AFRICA
Bridging the Digital Identity Gap in Africa
FEBRUARY 24 - 26, 2026

BOOK OF PROCEEDINGS

February 24 - 26, 2026
STIAS / Stellenbosch Institute for Advanced Study
Stellenbosch, South Africa
www.didunconf.africa

Thank You Documentation Center/Book of Proceedings Sponsor: GLEIF

Contents

DID:UNCONF AFRICA
Bridging the Digital Identity Gap in Africa

About DID:UNCONF AFRICA

The intention of the event is to foster innovation and collaboration between emerging digital identity companies and projects across Africa.

About

The inception of DID:UNCONF AFRICA arose from the recognition that the SADC region holds immense potential yet faces unique challenges in digital identity. Our inaugural event emphasizes the vast disparities in the digital identity ecosystem and offers a stage for groundbreaking solutions tailored to the African context. DID:UNCONF AFRICA brings together thinkers, leaders, and innovators who are transforming the digital identity landscape, both locally and internationally.
Inspired by the collaborative and dynamic format of the Internet Identity Workshop (IIW),

DID:UNCONF AFRICA takes a more explorative approach, allowing participants to chart the course of discussions. The Open Space unConference format breaks the mould of traditional events, creating a space where every voice can be heard, from startups to industry giants. The event not only explores the intricacies of digital identity but also works toward weaving a cohesive network of innovators in the SADC region and beyond.

Event Background

DID: UNCONF AFRICA is inspired by the Internet Identity Workshop (IIW) that has been held twice a year, since 2005 in California for the global community working on Internet Identity. The longtime co-producer and Open Space facilitator of IIW Heidi Nobantu Saul collaborated with a local partner DIDx to plan and host the inaugural event. The second and third days of the event will be hosted with the same Open Space UnConference format that the Internet Identity Workshop has used for the past 20 years.

Thank You to our Sponsors!

What an unforgettable three days! To everyone who joined us—whether you flew in from across the continent or just down the road—thank you for showing up with such energy, openness, and curiosity.

Together, we explored what it really means to build digital identity for Africa, in Africa. From deep-dive sessions to spontaneous hallway debates, from big-picture policy to practical tech demos—**DID:UNCONF AFRICA 2026** was a space shaped by all of you.

To our incredible sponsors and partners: your support made this possible. To every speaker, facilitator, builder, and attendee—thank you for being part of the movement. This isn't just a conference. It's a community.

We can't wait to continue the journey with you in 2027!

3 Day Schedule

Day 1 Kick-off: African-Focused Digital Identity Program

Tuesday February 24th / Doors Open at 12:30PM

Wallenberg Center at STIAS ~ Enter STIAS via Marais Road

ACTIVATING DIGITAL IDENTITY IN SOUTHERN AFRICA: FROM FOUNDATIONS to IMPLEMENTATION

Arrival and Registration	12:30 -13:00	Networking Break	15:10 -15:45
Welcome & Framing the Day	13:00 – 13:15	Keynote / SSI in Action (Self Sovereign Identity)	15:45 – 16:20
Keynote / The Need for Proof of Organizational Identity	13:15 – 13:50	Keynote / RICA4U: The Catalyst for Digital Identity Adoption?	16:20 – 16:55
Panel / Making Digital Identity Work: Standards, Regulation, and Scale	13:50 – 14:35	Panel / The Convergence of Identity and Payments	16:55 – 17:40
Keynote / Identity in Content Provenance	14:35 – 15:10	Closing Remarks & What's Next?	17:40 - 18:00

18:00 ~ Welcome Reception in a relaxed and engaging environment directly following the end of the day

Sponsored by PwC!

Open Space unConference Day 1

Wednesday February 25th / Doors Open at 8:30

Coffee/Tea & Breakfast Snacks

Welcome & Introductions	9:30 – 9:45	Session 3	13:30 – 14:30
Opening Circle / Agenda Creation	9:45 – 10:30	Session 4	14:300 – 15:30
Session 1	10:30 – 11:30	Session 5	15:30 – 16:30
Session 2	11:30 - 12:30	Closing Circle	16:30 – 17:30
Lunch	12:30 – 13:30	Conference Dinner	18:00 – 22:30

Join us for a memorable Conference Dinner at the historic Middelvlei Wine Estate.

Sponsored by Mastercard & Smile ID!

Open Space unConference Day 2 Thursday February 26th / Doors Open at 8:30 Coffee/Tea & Breakfast Snacks				
Women's Breakfast **Sponsored by Umazi**	8:30 – 9:25		Lunch	13:00 – 14:00
Opening Circle / Agenda Creation	9:30 – 10:00		Session 9	14:00 – 15:00
Session 6	10:00 – 11:00		Session 10	15:00 – 16:00
Session 7	11:00 – 12:00		Closing Circle	16:00 – 17:00
Session 8	12:00 – 13:00			
No Host Post Event Gathering / Suggested Location to be Announced				

DID:UNCONF AFRICA
Bridging the Digital Identity Gap in Africa
FEBRUARY 24 - 26, 2026

Day 1 Kick-off: African-Focused Digital Identity Program

Theme of the Day:
Activating Digital Identity in Southern Africa: From Foundations to Implementation

This day examines how digital identity is being activated across Southern Africa today – moving from core trust infrastructure and public-sector frameworks to private-sector use cases, emerging agentic identity models, and the convergence of identity and payments. The focus is on what is live, what is constrained, and what is required to scale interoperable identity systems across Africa.

12:30 – 13:00 / Arrival & Registration

13:00 – 13:15 / Welcome & Framing the Day
Gideon Lombard - DIDx

13:15 – 13:50 Keynote / The Need for Proof of Organisational Identity
Karla McKenna - GLEIF

14:50 – 14:35 Panel / Making Digital Identity Work: Standards, Regulation, and Scale

Speakers:
- Dalene Deale - Business Growth Hacking
- Gabi Adontevi - MOSIP
- Karla McKenna - GLEIF

Moderator: Elmo Hildebrand - PwC

14:35 – 15:10 Keynote / Identity in Content Provenance
Eric Scouten - Adobe

15:10 – 15:45 / Networking Break

15:45 – 16:20 Keynote / SSI in Action
Mahir Şentürk - Hashgraph Association

16:20 – 16:55 Keynote / RICA4U: The Catalyst for Digital Identity Adoption?
Shaun Strydom - Contactable

16:55 – 17:40 Panel / The Convergence of Identity and Payments

Speakers:
- Lohan Spies - DIDx
- Ian Thompson - Q LINK
- Shabir Ahmed - Mastercard

Moderator: Martin Grunewald - DIDx

17:40 – 18:00 Closing Remarks & Call to Action: What's Next?
Gideon Lombard & Heidi Nobantu Saul

18:00 – Welcome Reception

A relaxed and engaging environment with complimentary wine and canapes directly following the end of the day.

THANK YOU PwC for sponsoring the Welcome Reception!

Day 1 Summary / Introduction

24 February 2026

Theme: Activating Digital Identity in Southern Africa: From Foundations to Implementation

Day 1 of DID:UNCONF AFRICA 2026 opened with a clear sense of momentum. Hosted at STIAS in Stellenbosch, the day served as the formal conference-style opening to the broader unconference, bringing together regulators, public-sector representatives, academics, enterprise leaders, fintech practitioners, digital identity specialists, and ecosystem builders from South Africa, the continent, and abroad. What emerged across the day was not simply a collection of presentations on digital identity, but a practical and increasingly urgent conversation about trust infrastructure: how it is built, who it serves, how it scales, and what it enables when implemented well.

In his opening remarks, **Gideon Lombard of DIDx** situated DID:UNCONF AFRICA within the lineage of the Internet Identity Workshop (IIW), noting that the gathering is Africa's officially recognised IIW-inspired regional event. He reflected on how IIW historically provided the environment in which major identity ideas and standards could move from whiteboard discussion into internet infrastructure, using OpenID as a powerful example of that journey. He also emphasised that the success of the inaugural 2025 edition had confirmed something important: that Africa does not lack innovation, urgency, or talent in digital identity. What is needed are the right spaces, the right people, and the right conversations. That framing proved prophetic for the day that followed.

Lombard also highlighted the visible broadening of the ecosystem in attendance this year. Public sector participation had grown, with representation from institutions such as SARS, National Treasury and the Presidency. Universities including Stellenbosch University, the University of Cape Town, the University of the Western Cape and the University of Johannesburg were present. Consulting firms, sponsors, startups, large enterprises, technology builders, regulators and implementers were all in the room together. This diversity mattered. It reinforced one of the day's central themes: digital identity cannot be built meaningfully in silos. It is inherently cross-sectoral, and many of the trust layers that matter most become stronger when developed collectively rather than competitively.

Attendance itself was a signal of growing ecosystem traction. After a first year that drew roughly 50–60 delegates, the 2026 event had reached 117 delegates and was close to being sold out. That growth was not treated merely as a logistical success, but as evidence that digital identity is becoming a live and shared concern across a widening set of actors in Southern Africa.

Lombard also used the welcome to make an important distinction about the event format. Day 1 would begin in a familiar conference mode, with keynotes, panels and structured dialogue. Days 2 and 3 would move fully into unconference mode: participant-led, discussion-driven, and shaped by the people in the room. That framing mattered, because it underscored that DID:UNCONF AFRICA is not simply a stage for presentations; it is a

convening designed to generate collaboration, deepen questions, and create the kind of open exchange from which enduring identity infrastructure often emerges.

Download Full Summary Here

Day 1 Summary / Concluding Reflection

Day 1 of DID:UNCONF AFRICA 2026 did more than open a conference. It made visible a field that is maturing in real time.

The day began by placing Africa's digital identity conversation within a lineage of open collaboration and ecosystem-building. It then moved through organisational identity, standards and scale, content provenance, self-sovereign device identity, telecom-led adoption pathways, and the convergence of identity with payments. What emerged was not a single model, nor a simplistic answer, but a far more useful conclusion: digital identity is becoming a foundational layer across multiple sectors, and its success will depend on whether trust can be made usable, portable, interoperable and relevant to everyday life.

For those in attendance, Day 1 offered both conceptual clarity and practical provocation. For those reading these proceedings, the core takeaway is this: Southern Africa's digital identity journey is entering a more serious phase. The question is no longer whether digital identity matters. The question is how to build it in ways that are trusted, inclusive, implementable, and valuable enough to become part of the region's real infrastructure.

Day 2 & 3 Open Space unConference days

A two-day OpenSpace unConference
An immersive two-day exploration, inspired by the Internet Identity Workshop™ diving deep into the world of digital identity. We dispense with traditional keynotes, and engage in authentic collaborations through a co-created agenda. Examine the intricate facets of identity: people, organisations, and even the journey of products. Connect, track, support, and cross boundaries. Investments in standards, protocols, and systems find tangible applications here. Discover, Learn, Collaborate.

This is a participatory two days and it's all about exploring the agenda topics with professional peers from a range of identity areas. Like the Internet Identity Workshop, we will co-create the agenda together live each morning. The Open Space UnConference process will be professionally facilitated by Heidi Nobantu Saul the long-time co-producer and Facilitator of IIW.

Once agenda creation is complete there will be a full Agenda Wall of sessions posted, each with the time and place it will occur. Session topics are not voted on and all sessions put forth by participants at the start of each day will take place. Sessions are run as breakouts and attended by those who want to attend. There will be 5 session time slots a day, each with multiple concurrently running sessions.

Through multiple of sessions, lunches, a welcome dinner and a pre-event networking reception, provided by our generous sponsors (all included in the ticket), participants have plenty of opportunities to exchange ideas and make new professional connections. The Open Space unConference format is perfect for a rapidly moving field where the organizing team cannot predetermine what needs to be discussed, creating a space where every voice can be heard, from startups to industry giants.

Agenda Creation = Sessions Called and Hosted by Attendees

27 distinct sessions were called by participants and held over 2 Days.

We received notes, slide decks, links to presentations and photos of whiteboard work for 22 of these sessions.

Day 2 / Sessions 1 – 5

SESSION 1
1B/ NO SESSION
1C/ NO SESSION
1D/ Identity and Impact / Camila & Alwyn
1E/ Identity in the Card Payment System / What - How - Why - When / Varsha G

SESSION 2
2B/ NO SESSION
2C/ At the start: GLEIF and LEI and how we got to the vLEI/Organizational Identity / Karla McKenna
2D/ Digital Identity for Townships and Rural SME & Implementation & Strategies / Nazire
2E/ Ecosystem SetUp: PID Issuance - Roles? - Certification? / Matt A.

SESSION 3
3A/ Frameworks & Protocols - Building Trust at Internet Scale, Human and Non-Human Identity - List, What's Missing, what's utilised / Cindy
3B/ SCALE - Are we truly focused on the right stuff? / Dalene Deale
3C/ NO SESSION

SESSION 4
4A/ Go To Market / Gajo
4B/ Define the Scope of a PoC for Digital Identity at Stellenbosch University / Hans
4C/ NO SESSION
4E/ Connect the Dots… How do content creators here wish to be Identified? & Identity for Content Royalties / Eric and Gids

SESSION 5
5A/ “Pay With Your Face” sounds scary! Is it? & The evolution of consent in the age of wallets. / Eric Scouton and Carrie Peter
5B/ NO SESSION
5C/ NO SESSION
5D/ Building Community - Decentralized Trust Eco-systems (silent session) :-) / Sam

Day 3 / Sessions 6 - 10

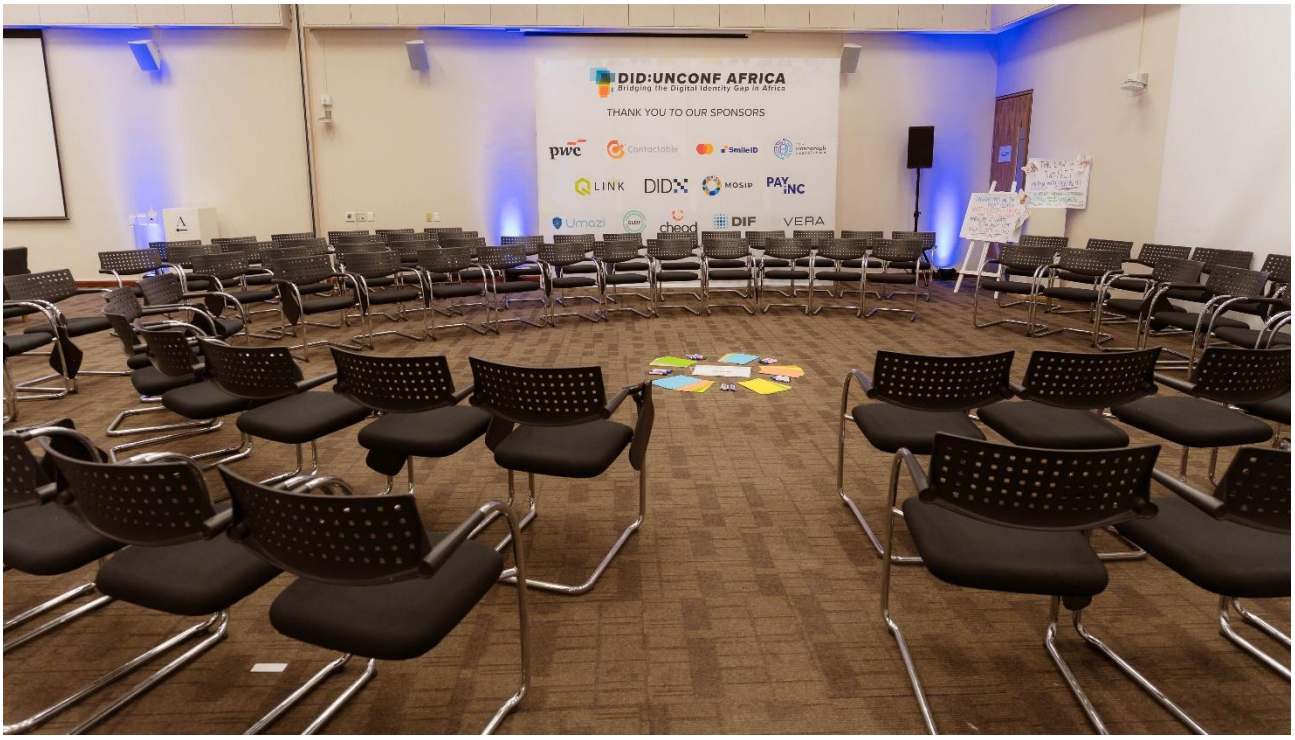
SESSION 6
6A/ ID-Aware ALIAS / Lohan
6B/ What would an interoperable “Trust Layer” look like that allows a fintech in Nigeria to instantly trust the credential of a merchant in Kenya? / Maya
6C/ NO SESSION
6D/ NO SESSION
6E/ SSI (Self Sovereign Identity) for “Dummies” (101) / Jannie + Jason + Eugene
6F/ Youth + DIG ID + IMPACT / Camila

SESSION 7
7A/ Do you have the credential that you need? Let’s discuss levels of assurance, privacy, safety, security, usefulness and usability / Karla McKenna
7B/ NO SESSION
7C/ NO SESSION
7D/ SOLUTION ENGINEERING for Self-Sovereign Identity - from and idea to MVP / Mahir & Shaveen
7E/ Unpacking jargon & who is the target Audience / Annemie Krause
7F/ NO SESSION

SESSION 8
8C/ NO SESSION
8D/ NO SESSION
8E/ Digital Identity Ecosystems in South Africa - how best to collaborate? & Future of Organizational Identity? / Max
8F/ What Digital Identity Verification Technologies can Support & Improve Social Impact? / Alwyn

SESSION 9
9A/ NO SESSION
9B/ Real world Asset (RWA) Tokenization (NFT) and Identity: Where is the meeting point? / Timi
9C/ How to start an ecosystem which uses a Digital Wallet? / OMAR
9D/ NO SESSION
9E then F/ What’s SSI incubator going to be like in 2026 in Africa? / Maya - Moved to Breakout Room F

SESSION 10
10A/ NO SESSION
10B/ Impact of AI…? & Agentic Payments & Digital Identity / Tina V
10C/ How do we include places with those that are not Tech-inclined / aligned? / Maxwell
10D/ NO SESSION
10E/NO SESSION


DID:UNCONF AFRICA
Bridging the Digital Identity Gap in Africa
THANK YOU TO OUR SPONSORS
pwc
Contactable
SmileID
LINK
DIDx
MOSIP
PAYINC
Umazi
chead
DIF
VERA


DID:UNCONF AFRICA
Bridging the Digital Identity Gap in Africa
THANK YOU TO OUR SPONSORS
pwc
Contactable
SmileID
LINK
DIDx
MOSIP
PAYINC

Session Notes / Wednesday February 19/ Sessions 1 - 5

SESSION #1

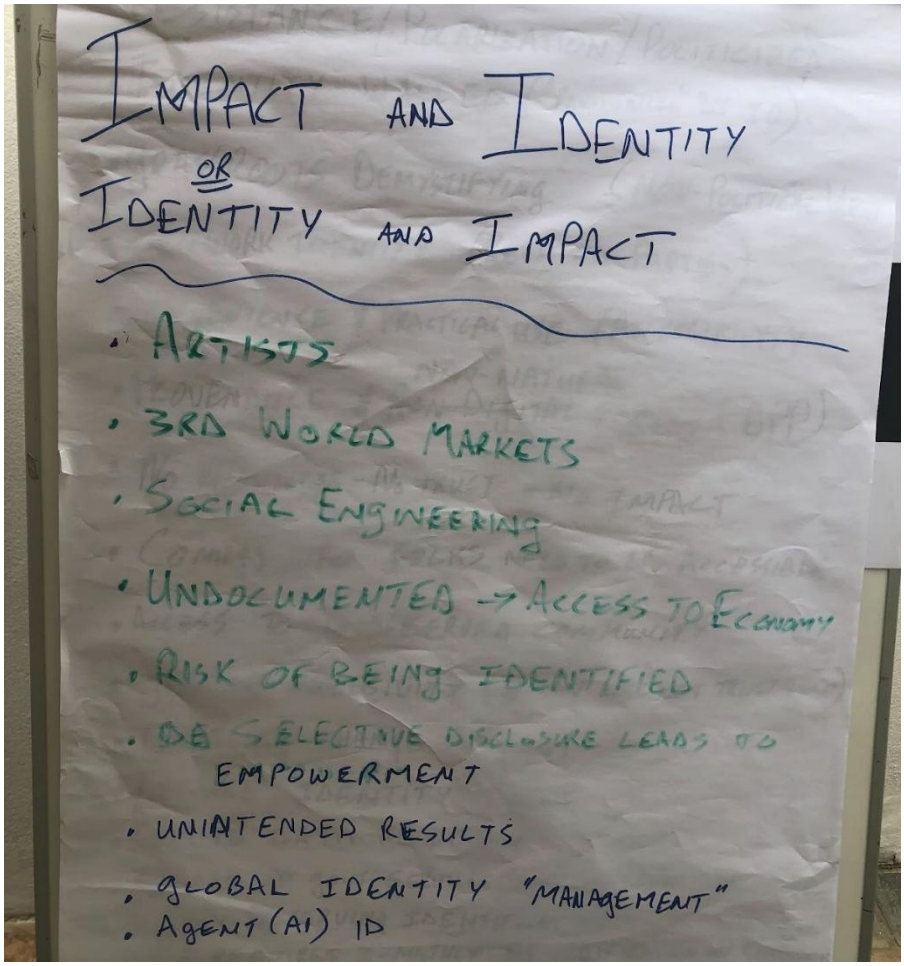
Identity and Impact

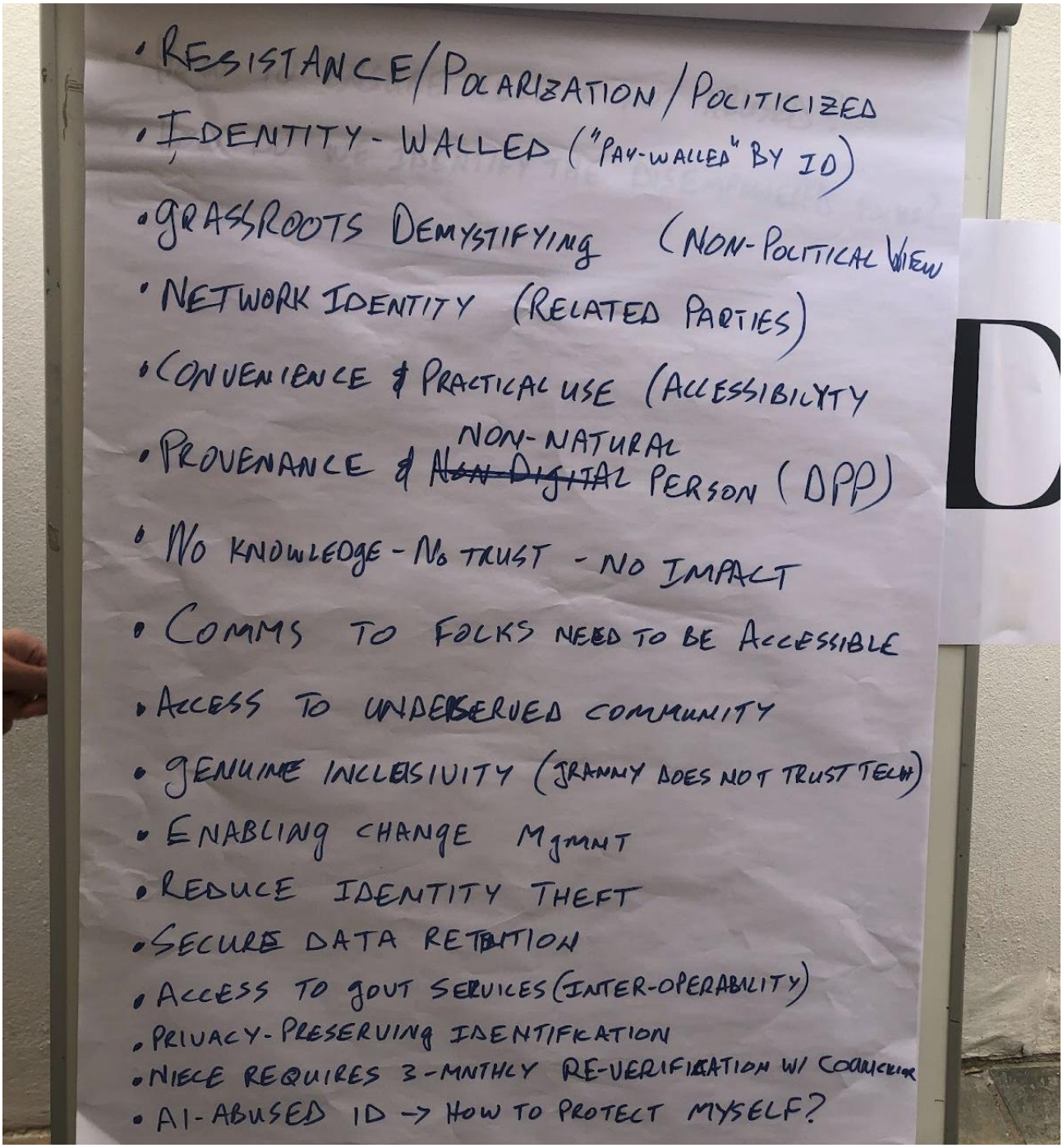
Session Convener: Camila Haux & Alwyn van Wyk
Session Notes Taker: Alwyn van Wyk
(optional) List of Session Attendees: ±25

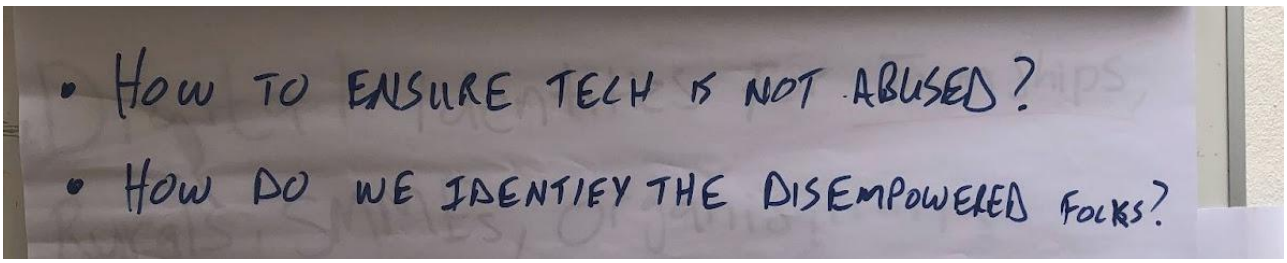
Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

The session was convened to focus on the question of how social impact initiatives can benefit from self-sovereign identity. Attendees each had an opportunity to describe a bullet-point of view about the topic "Identity and Impact". Interesting points of view emerged; in some cases beyond social impact and more focused on "me, as an individual" or "we, the organisation".

Below are pictures of the complete list of bullet points.




• RESISTANCE/POLARIZATION/POLITICIZED
• IDENTITY-WALLED ("PAY-WALLED" BY ID)
• GRASSROOTS DEMYSTIFYING (NON-POLITICAL VIEW
• NETWORK IDENTITY (RELATED PARTIES)
• CONVENIENCE & PRACTICAL USE (ACCESSIBILITY
• PROVENANCE & NON-NATURAL PERSON (DPP)
• NO KNOWLEDGE - NO TRUST - NO IMPACT
• COMMS TO FOLKS NEED TO BE ACCESSIBLE
• ACCESS TO UNDERSERVED COMMUNITY
• GENUINE INCLUSIVITY (GRANNY DOES NOT TRUST TECH)
• ENABLING CHANGE MGMNT
• REDUCE IDENTITY THEFT
• SECURE DATA RETENTION
• ACCESS TO GOVT SERVICES (INTER-OPERABILITY)
• PRIVACY-PRESERVING IDENTIFICATION
• NIECE REQUIRES 3-MNTHLY RE-VERIFICATION W/ COUNCILOR
• AI-ABUSED ID → HOW TO PROTECT MYSELF?


• HOW TO ENSURE TECH IS NOT ABUSED?
• HOW DO WE IDENTIFY THE DISEMPOWERED FOLKS?

Identity in the Card Payment System / What - How - Why - When

Session Convener: Varsha Gokool
Session Notes Taker: Varsha Gokool

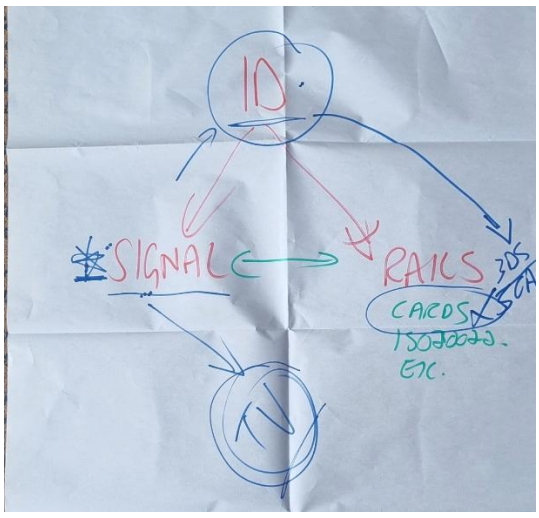
Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

The session was called to gain a better understanding of the role of Identity in the Payments Ecosystem.

- What role does identity play, if any?
- How can Identity be used in the Card ecosystem?
- Why do we need Identity in the Card ecosystem?
- When do Card industry players need to worry about adding this to their roadmap?

Notes:

- There is a need to make identity in payments transactional.
- SCA/3DS can already be used to inject/use identity as part of authentication
- SCA only solves for Card not Present transactions
- 3DS caters for confirming the identity of the payer, but not who they are paying
- Clarity is needed around:
    - What information sits in the digital identity construct?
    - What information does each entity in the payments flow need from the identity?
- Authentication credentials may be used, but how would these work across the various payment rails?
- Should a new standard be established that is rail agnostic?
- Tokenisation may be used - send a tokenised proxy to the scheme and only release the PAN after authentication
- For card present transactions, we need to be aware of the processing turnaround times if friction is introduced into the payment process (till minutes)
- Enhanced signalling and Trust scores updated in real time may provide a solution for card present and card not present transactions



SESSION #2

At the start: GLEIF and the LEI and how we got to the vLEI and Organizational Identity

Session Convener: Karla McKenna
Session Notes Taker: Karla McKenna

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

I called the session as an opportunity for attendees not familiar with the GLEIF, the LEI or vLEI or had basic/background questions about these.

Topics covered were the history of and the reason for the LEI to be developed, how the policies and requirements for the LEI and how GLEIF was required to operate, the reference data set, how LEIS are issued, what types of organizations are eligible for registering for LEIs, the cost recovery model for LEI issuance, governance of the LEI system and the vLEI Ecosystem Governance Framework.

There also was an extensive discussion on how the LEI could be useful and beneficial for South Africa. A particular focus was how SMEs could have access to LEIs as in South Africa most SMEs are not legal entities but are a significant part of the economy. Both SMes which could participate in sales or trade outside their jurisdiction and SMEs who offer services more locally or only locally. Also discussed was how public sector organizations could fund the registration of LEIs for their markets.

The role of regulators, supervisors, infrastructures, the traditional and decentralized finance industries also were considered during the discussions.

Digital Identities for Townships, Rural areas, SMMEs, and organisations & Implementation Stragies

Session Convener: Nazire Mathe
Session Notes Taker: Masibonge Shabalala

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Today we discussed Digital Identities for Townships, Rural areas, SMMEs, and organisations. We also touched on implementation and strategies, but we didn't really finish everything because we had some unexpected discussions that took up time.

Main points:

Here we were trying to understand what digital identities actually are and how they apply to different people and communities.

Digital Identities

We discussed that a digital identity is basically an online version of who you are. It can be used to prove who you are when using digital platforms or services.

- **Personal identity** – This is your normal identity as a person (name, ID number, etc.), just in a digital form.
- **DHA approved identity** – We spoke about identities that are officially recognised by the Department of Home Affairs, meaning they are legally valid.
- **Digital representation of a person** – This is how a person is shown or verified online through systems or platforms.

We also spoke about:

- **World ID** – An example of a global digital identity system and how it could work.
- **Digital IDs used in utility** – How digital IDs could help with things like electricity or other services.
- **Banking / earning** – How digital identity makes it easier to open bank accounts or receive money.
- **Access to services** – Digital IDs can help people in rural areas and townships access government or private services.

Other important things mentioned:

- **Custodial wallets** – Wallets where a third party helps manage your digital identity or assets.
- **Biometric verification** – Using fingerprints, face scans, etc. to confirm someone's identity.

We didn't fully conclude everything because the discussion became more problem-led and we started debating practical challenges and different opinions, so we ran out of time before finalising all the points.

Ecosystem SetUp: PID Issuance - Roles? - Certification?

Session Convener: Matt Aberdein
Session Notes Taker: Granola AI (with permission)

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

European Digital Identity Framework Overview

- Architecture Reference Framework (ARF) defines 600+ requirements
    - 250 requirements specifically for wallet providers
    - Clear role definitions: issuers, verifiers, intermediaries, wallets
    - Very clearly stipulated requirements but process questions remain
- Large-scale pilots underway with real transactions (ferry tickets in Greece)
- New pilot streams focus on organizational identity, payments, blockchain integration
    - Corporate vs retail payment streams
    - Stablecoin payment experiments using identity verification
- Implementation timeline: next 2 years for compliance requirements
- Standards dictate protocols and formats across all implementations
- Current state: mostly experimental learning with established blueprint
- Company experience: built crypto libraries in Rust, provides tech stack to customers experimenting in space

South African Digital Identity Landscape

- Personal Identity Document (PID) as foundational layer
    - DHA likely to be primary issuer but role scope unclear
    - Will include biometric data (facial image from existing records, not real-time capture)
    - Metadata: name, surname, address, national ID number
    - Address inclusion problematic - many citizens lack formal addresses
- Multiple issuer model emerging
    - DHA issues foundational PID only
    - SARB issues financial credentials
    - Telcos issue mobile customer credentials (RICA verification creates financial identity pathway)
    - Driver's license requires PID but adds driving credential
- Tension: DHA may see itself as custodian of all digital identity vs limited role
- Open question: Can financial/other credentials be issued without PID foundation?
    - FICA law currently requires national identity substantiation
    - Debate whether this introduces necessary risk controls or excludes legitimate users (e.g., Zimbabwean workers)

Trust Framework Architecture

- National governing body needed (currently undefined - major gap)
- Scheme-based approach proposed
    - Financial services scheme (SARB ownership)
    - Healthcare scheme (Medical Aid Council)
    - Each scheme defines trust rules for participants
- Qualified Trust Service Providers (QTSP) model
    - Annual certification requirements
    - ISO standards compliance
    - Technical and security standards enforcement
- Trust levels vary by context
    - RICA verification acceptable for some use cases
    - "Golden source" DHA verification required for others
    - Lower trust from intermediary vouching vs authoritative source
- Risk of fragmentation if departments proceed independently
    - SARB could build DFID in isolation
    - Home Affairs might later impose different standards
    - Need upfront agreement on national standard

Privacy and Data Protection Concerns

- Major concern: lack of privacy rights representation in discussions
- Risk of over-collection by institutions
    - Risk/compliance officers tend toward maximum requirements when uncertain
    - Example: "selling bunny rabbit requires blood sample" mentality
- Need for contextual data sharing
    - Binary verification (yes/no) vs full data disclosure
    - Minimum necessary information principle
    - Technology enables selective disclosure but governance must enforce it
- Current system worse - no control over ID document scans and storage
- Comparison to caller ID: convenience vs privacy trade-off without informed consent
- Legislation needed to prevent banks requesting excessive data
- Concern about "nanny state" scenario where digital ID becomes mandatory for basic functions
- Technology can protect privacy if implemented with proper guardrails

Implementation Challenges

- Standards vs regulation debate
    - Standards more flexible and adaptable (easier to issue and modify)
    - Regulation takes 5-7 years, often outdated on arrival
    - Parliamentary approval process too slow for technology evolution
    - Innovation should drive regulation, not vice versa
- Regulatory sandbox exists for financial services but not other industries
- Fragmentation risk if departments proceed independently
- Political coordination required across multiple government entities

- Certification and compliance infrastructure needed
- Regulators typically reactive, not proactive (ICASA example from telco sector)
- Question: Do we need regulation or just standards and frameworks?

Technical Considerations and Fraud Prevention

- MDOC standard adoption (US driver's license model) - DHA reportedly considering
- Continuous verification vs point-in-time KYC
    - Current KYC "valid 10 minutes ago but still accepted" problem
    - Need for perpetual KYC/continuous due diligence
- Biometric interception for fraud prevention
    - Facial image in PID enables real-time biometric verification
    - Prevents mule account fraud (legitimate account holder paid to allow misuse)
    - "Prove life to biometric reference" concept
- AI-driven fraud detection with dynamic learning models
- Community-based validation through digital traces
    - Aggregated presence across use cases (RICA, transactions, etc.)
    - Credit score-like construct for digital identity trust
- Wallet security and interoperability requirements
- Cryptographic verification capabilities
- Iris scanning accuracy: 350 trillion scans with zero false positives (Iris Guard example)

Alternative Models and Global Perspectives

- Worldcoin/World ID discussion
    - Sam Altman's OpenAI project using iris scanning "orbs"
    - Decentralized identity system independent of national registries
    - Pays users to onboard (banned in Kenya and other countries)
    - Potential global pillar of trust vs national government control
    - Concerns about single entity controlling global identity
- Trust infrastructure debate
    - Preference for digitizing existing systems (ID cards, passports) vs new global systems
    - "One system to rule them all" concerns
    - Decentralized implementation vs centralized control tension

Current Government Initiatives

- Interdepartmental Working Group (IDWG)
    - National Treasury, DHA, Reserve Bank collaboration
    - Not regulatory body - coordination effort
- SARB Digital Financial ID (DFID) project
    - Originally banks' IAMZA project hit political obstacles
    - SARB coined "DFID" term - potentially world's first
    - Discovered financial identity inseparable from national identity
- Multiple government entities with dedicated budgets and teams
    - Reserve Bank, Presidency, SARS, Competition Commission involvement

- Regulatory sandbox available for financial services innovation
- Need for cross-departmental standards alignment
- Informal exploration of standards across government entities
- Communication happening but formal framework still needed

SESSION #3

Frameworks & Protocols - Building Trust at Internet Scale, Human and Non-Human Identity - List, What's Missing, what's utilised / Cindy

Session Convener: Cindy Vn
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

NO NOTES SUBMITTED

SCALE - Are we truly focused on the right stuff?

Session Convener: Dalene Deale
Session Notes Taker:
(optional) List of Session Attendees:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

NO NOTES SUBMITTED

SESSION #4

Go To Market

Session Convener: Gajo Maksimovic
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

NO NOTES SUBMITTED

Define the Scope for a PoC to showcase digital identity at Stellenbosch University

Session Convener: Hans Scheffler
Session Notes Taker: Hans Scheffler

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

To seed and promote the implementation of digital identity at Stellenbosch University, decision makers need to understand the value which it can unlock. Seeing is believing and thus this collaborative workshop session to explore potential use cases to be used for a proof of concept.

Idea summary:

- Exam verification / class attendance (prove the the correct person is in the room)
- Student cards (unfortunately the existing card readers at SU do not support NFC)
    - proof of student enrolment when claiming student discounts
    - ticketing for events
- Proof of successful completion of field / practical work outside of the University
- Badges
- Transcripts & degree / diploma certificates
- Onboarding / offboarding / student life cycle
    - major benefit for short (non-degree) courses
- Password self-help
- Alumni
- Focus on use cases that offer commercial value

Several vendors offered to assist. Thank you!

Next steps: Stellenbosch University to consider and refine the available options internally.

Content Provenance and the Identity Problem in Media

Session Convener: Gideon Lombvard & Eric Scouten
Session Notes Taker: Gideon Lombard

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

This session focuses on a practical problem in the South African media environment: royalties cannot be addressed properly without addressing identity.

In many cases, the issue is not only whether payment is made, but whether the correct person can be identified and linked to the relevant work, role, or rights entitlement. In the public sector, royalties may be payable, but institutions often struggle to pay the right people because beneficiary identification is weak, contributor records are incomplete, and ownership or representation may be unclear. In the private sector, payment is often inconsistent, opaque, or absent altogether. Across both, attribution breaks down easily as content moves through production, editing, publication, distribution, and reuse.

The discussion therefore places identity at the centre of the problem. Royalties are not only a rights issue or a payment issue. They are also an identity issue.

The session explores how content provenance technologies and identity-linked assertions may help address this. The relevance of C2PA and related CAWG work is not treated as abstract standards theory, but as a possible way of solving practical problems in media ecosystems where attribution is fragile, modification is constant, and payment depends on being able to identify who did what, and in what capacity.

A number of practical questions sit underneath the discussion:

- Who created the content?
- Who performed in it?
- Who edited, translated, remixed, or republished it?
- Who owns which rights?
- What happens when the content is changed?
- How should derivative use be treated?
- How do we deal with synthetic media and deepfakes?
- How do we preserve attribution across circulation?
- Who should be paid, and on what basis?

A useful distinction in the conversation is between content provenance and accountable identity. Provenance can help record what happened to a file, what tools were involved, whether AI was used, and what source material or ingredients were incorporated. But provenance on its own is not enough. The more difficult question is who is prepared to stand behind the content, the claim, the edit, or the publication. That is where identity becomes material.

The discussion returns repeatedly to the fact that authorship and ownership are no longer simple one-to-one relationships. A single media object may involve multiple valid participants and claims: creator, performer, editor, producer, publisher, translator, rights holder, distributor, platform, archive, or custodian. The group therefore leans toward a role-based understanding of media contribution rather than a simplistic single-author model.

This has direct relevance for royalties. If systems cannot represent multiple contributors and their different forms of participation, then they cannot support fair allocation. If contributor data cannot travel with content, then attribution degrades and downstream payment becomes harder to administer. If identity is weak, then rights become harder to enforce and legitimate claimants become harder to distinguish from false or incomplete claims.

The conversation also deals directly with modification. Editing, clipping, subtitling, translation, remastering, and re-publication are normal parts of how media circulates. The problem is not that content changes. The problem is that changes often become detached from attribution, permissions, and responsibility. This is where provenance infrastructure becomes useful: not because it prevents editing, but because it may preserve a visible chain of transformation and help show what changed, by whom, and under what authority.

That question becomes especially important in relation to synthetic media and deepfakes. The session does not treat deepfakes only as a detection problem. The more practical issue is how to establish credible origin, responsible editing, and inspectable provenance for media that should be trusted. A repeated point is that authenticity is not the same as truth. A file may have provenance and still be misleading. A signed or attributable piece of media may still be manipulated. Provenance does not replace editorial judgement, fact-checking, or governance, but it can strengthen accountability and make claims easier to interrogate.

Piracy is discussed in similar terms. It is not only a question of unauthorised copying. It is also a question of broken attribution, lost permissions, and severed economic linkage between a work and its contributors. Once content moves through informal or uncredited channels, visibility drops and the basis for payment weakens. The conversation therefore treats piracy not only as a legal issue, but also as a traceability problem.

The ethical side of ownership is another clear thread in the session. The group raises questions around contested rights, derivative works, synthetic alteration, and whether provenance systems might either protect creators or unintentionally privilege large institutions over individuals. That tension is important in the South African and wider African context, where records are often fragmented, contributors may not be formally documented, and many creators operate across informal and formal systems at the same time. Any future model would need to improve trust and fairness without creating new barriers for participation.

There is also discussion around permissions for reuse, remixing, and AI-related uses of content. As media increasingly enters automated pipelines, the ability to attach machine-readable information about identity, provenance, and permissions becomes more important. This is relevant not only for authorship and attribution, but also for questions of consent, training, transformation, and downstream use.

What the session surfaces clearly is that content provenance, identity, and rights information need to be treated together. In the South African media context, this has direct relevance to royalty allocation, creator recognition, contributor tracking, authenticity of content, deepfake response, piracy, derivative works, and fairer value distribution across the media chain.

The strongest practical takeaway is that the media problem being discussed is not only about proving where content comes from. It is also about identifying who is connected to it, who can make claims over it, who has modified it, and who should be paid.

Key points discussed

- Royalties in media are also an identity problem
- Public-sector payment processes often struggle to identify the correct recipients
- Private-sector payment practices are often inconsistent or absent
- Attribution degrades as content moves across people, platforms, and contexts
- Provenance is useful, but provenance without accountable identity is incomplete
- A single media object may involve multiple valid contributors and rights-bearing roles
- Modification is normal; hidden or misleading modification is the problem
- Deepfakes raise questions of both authenticity and accountability
- Piracy is also a traceability and attribution problem
- Permissions for reuse, remixing, and synthetic transformation are increasingly important
- Any technical model has to work in conditions of fragmented records and uneven institutional capacity

Possible next steps

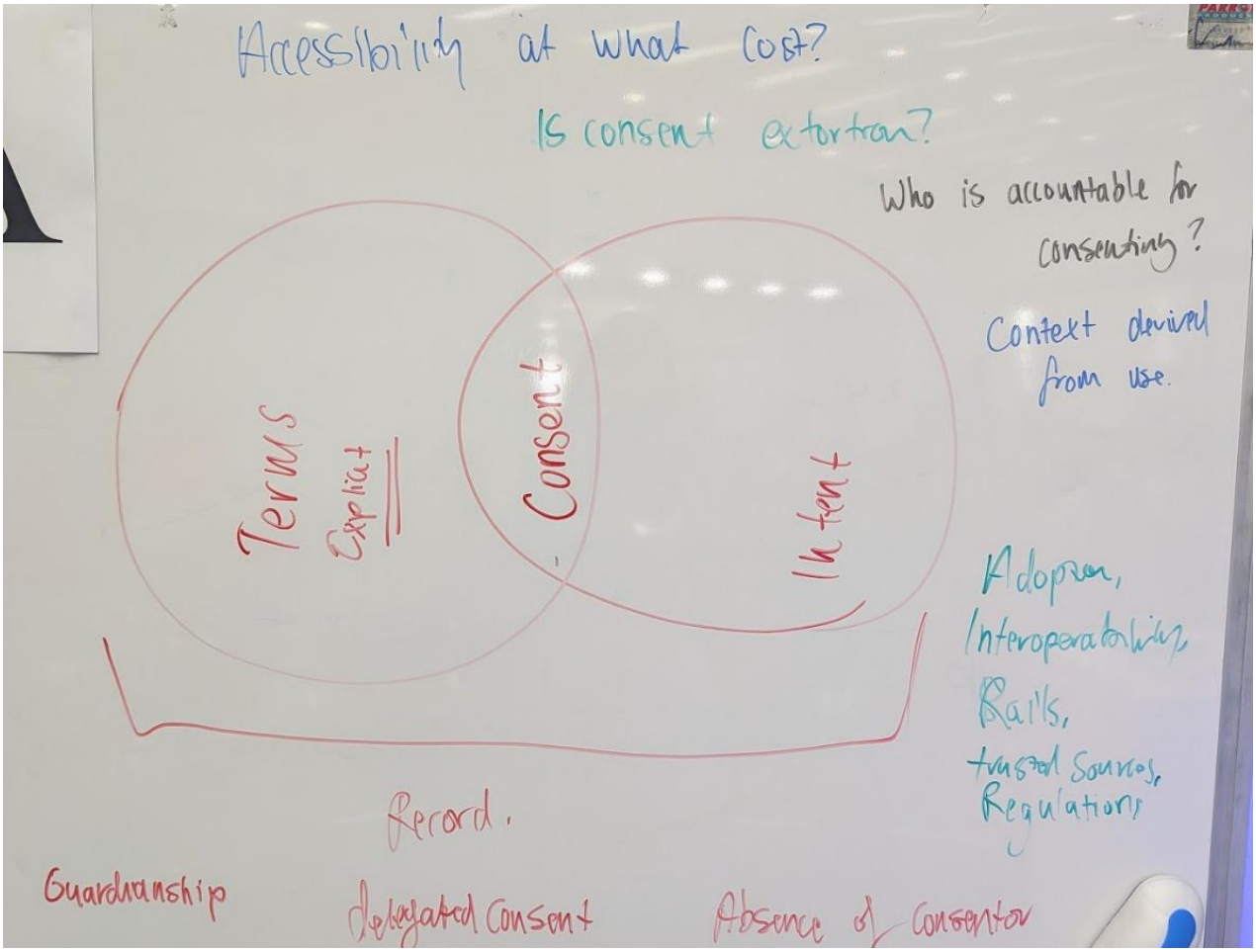
- Develop the South African film and media royalties use case further as a concrete identity problem
- Map contributor roles more clearly across the media lifecycle
- Explore how provenance and identity-linked assertions could support contributor recognition and payment
- Examine the legal and operational implications of derivative works, modification, and contested ownership
- Consider a follow-up session focused specifically on media provenance, creator identity, and royalty administration in the South African context

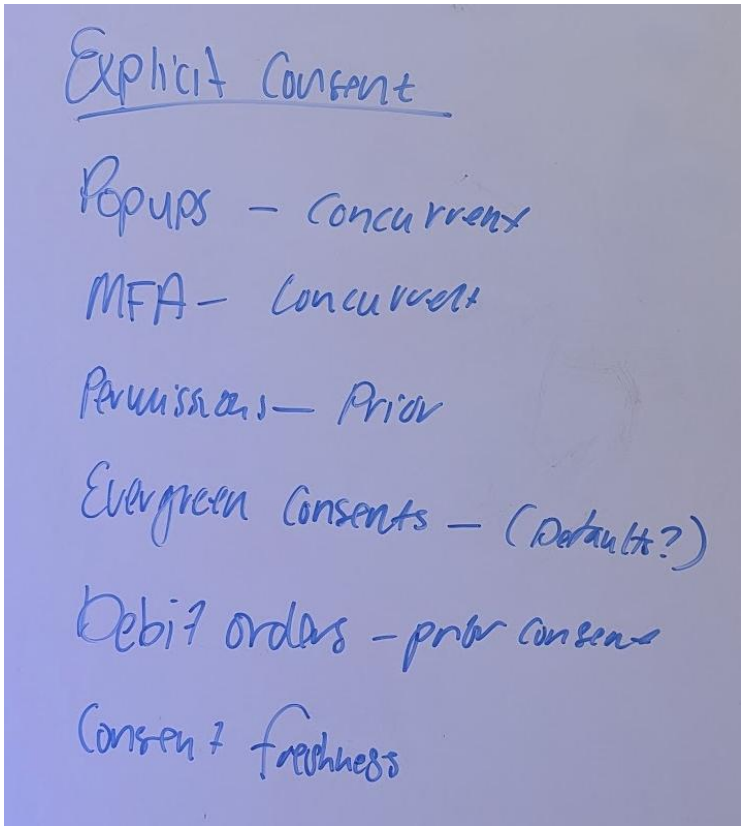
SESSION #5

"Pay With Your Face" sounds scary! Is it? & Evolution of consent in the age of wallets

Session Convener: Eric Scouton and Carrie Peter
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?





Building Community - Decentralized Trust Eco-systems (silent session) :-)

Session Convener: Sam
Session Notes Taker:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

We spoke of how to use decentralised identity beyond the single use case most were thinking of: SA gov adoption.

How can we rebuild trust into communities using this tech.

Session Notes / Thursday February 26 / Sessions 6 - 10

SESSION #6

ID Aware Alias (using Proxies)

Session Convener: Lohan Spies
Session Notes Taker: Sharon Oelofse

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Background with PayShap as context of an alias (proxy).
The Proxy or alias can be used to identify a specific entity (personal or juristic), to take this alias and use it to discovery or resolve information about you.
For eg in PayShap, you use the Proxy/alias to resolve to a bank account. For PayShap the proxy is a MobileNumber@Domain(bank) or just 'MobileNumber' in the case where a user only have 1 proxy with its primary banking entity. PAYINC is the holder of the database for these proxies. And from this lookup, it is able to reroute those to the correct domain (bank) to resolve to a bank account.

Limitations/Issues with PayShap:
- this does not resolve directly to an individual identity
- PayShap currently only supports bank account resolution, implying you must own a bank account to get a Payshap proxy.
- this is a 1 to 1 link. 1 proxy to 1 bank account, and 1 bank will only allow 1 proxy per person.

What we need to work towards is;
- to use a proxy, from any provider, not necessarily from a bank,
- allow multiple proxies.
This allows multiple Store of Values stored in my wallet, this allows me to have multiple proxies, which ultimately allows multiple bank accounts, each linking to a specific credential. Now if this proxy is linked to not only bank account, also other non financial transaction functions, then I have more flexibility on what I can store, and what I can use it for.

This is achievable by allowing multiple Proxy SPs, which can route to other Proxy SP(say at banks) which will be able to resolve different information about me. and this proxy SP does not need to be a bank.

Our end wish state is allow any S of V (not necessarily a bank account) to pay another SoV (not necessarily a bank account). to use this fort more than just payment.

To allow a proxy to be used in more than just payment, we can add an attribute of 'CAPABILITY' to a Proxy. This defines what functions this Proxy can do, and it will not always be

payment. Think of a retailer (we used PNP in this example), who has a proxy. As a user i can use this proxy to access digital functionality, such as perhaps applying for a SmartShopper account. The proxy becomes more than payment, we can now do onboarding to an entity we can trust and verify.

So now we have a proxy that has the following functionality:

- Discovery
- Resolution
- Verification
- *NEW* Capability (which can route you to a different functional flow. i.e: onboarding, issue loyalty card, KYC, payment, etc)
- finally routing to Payment (optional)

As a Juristic Proxy, i would need to have ability to push notifications to the wallet holder to notify them of the specific function or update I want them to make (update your credential or renew ...) To do this i need to look at options such as DIDComm, to ensure secure end to end comms both for push to wallet and send/recieve from/to wallet, and to check for revoke certificates.

Still need to resolve:

- This must protect from data harvesting, if there is a centralised database of proxies, this opens up risk. Since we see multiple Proxy SP's this is multiple databases open for risk
- must be able to solve for the Governance issue. A way around this would be to also offer 'point in time' proxy, created just for this instance, then destroyed after, which is useful for scenarios when you wish to pay/action something, but no need to keep the relationship or the beneficiary after this. (think once off payments, although this extends of course to more than just payment)
- solve for QR issue, that you need to be present to scan or show
- in the case of the PayShap rails, we need to solve for pre-authorisation of an individual (ie like a banking app is pre authenticated the person since they need to login to their application)
- must be self healing, must auto update the system when credentials change
- can this solve for the Hooder being offline, but still be able to share to a 'nominated once off agent' (who is online) to transact on your behalf. This permission could be temporary, or permanent?

What would an interoperable "Trust Layer" look like that allows a fintech in Nigeria to instantly trust the credential of a merchant in Kenya?

Session Convener: Maya Kanerhara
Session Notes Taker: Maya Kanerhara

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Connect all dots below:

- African Export Import Bank
- LEI - KYB in registry
- ISO 20022
- Identify geography (protocol)

POS is separate

Youth + DIG ID + IMPACT

Session Convener: Camilla
Session Notes Taker:
(optional) List of Session Attendees:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

NO NOTES SUBMITTED

SESSION #7

Do you have the credential that you need? Let's discuss levels of assurance, privacy, safety, security, usefulness and usability . . .

Session Convener: Karla McKenna
Session Notes Taker: Karla McKenna

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

We started the session by asking should choice of credentials be offered within a particular context or usage? We concentrated on two aspects - different levels of assurance (focusing particularly in Identity Assurance in the issuance of credentials) and ease of access.

The group came to the conclusion that curated choice was the answer. Each choice should have a clear definition noted and publicly available indicating the level of assurance that was used in the issuance of the credential. Then a user group, group of stakeholders, regulator, etc. could list the types of credentials which would be acceptable for use in a particular context or usage.

To support this and achieve clarity, there may be a need for a standard vocabulary to define levels of assurance.

Something like this already has been published by ETSI for 5 levels of digital certificates (details in TS119461).

It was noted that choice could result in friction. If a potential credential holder would not want to go through the process of securing a credential type from the approved list, this could result in restricted usability and capability, limitations on access and approval to use services and processes.

Verifiers and industries could define, promote and force best practices for credentials choices that are best suited for their purposes.

SOLUTION ENGINEERING for Self-Sovereign Identity - from and idea to MVP

Session Convener: Mahir Senturk
Session Notes Taker: Shaveen Bageloo
(optional) List of Session Attendees: Many

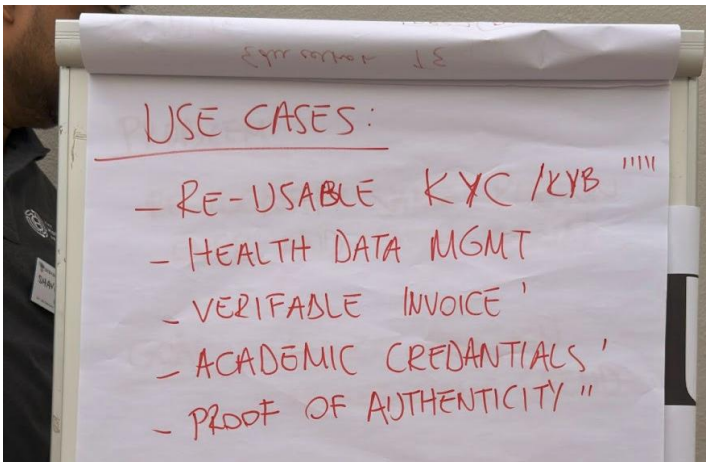
Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

The audience was asked to vote on a problem pain point that we could solve for them using SSI Principles.

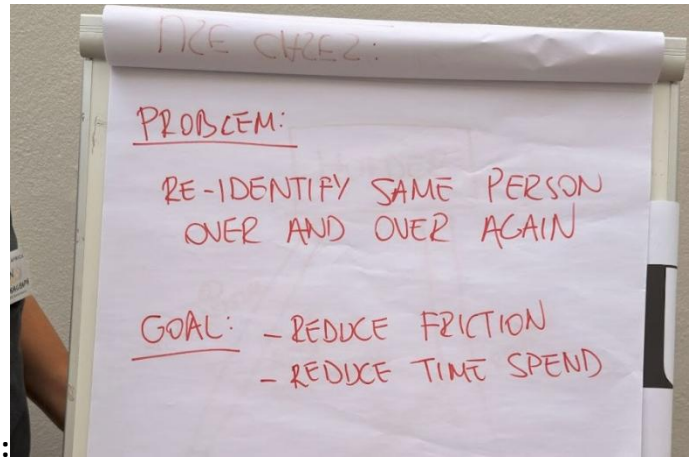
There were a few problem areas / use case that attendees shouted out (picture 1):

- Government invoicing
- Buying and Selling of Property and the tedious KYC process & reprocessing
- Medical records
- etc..

Ultimately the majority voted on the reusable KYC process.

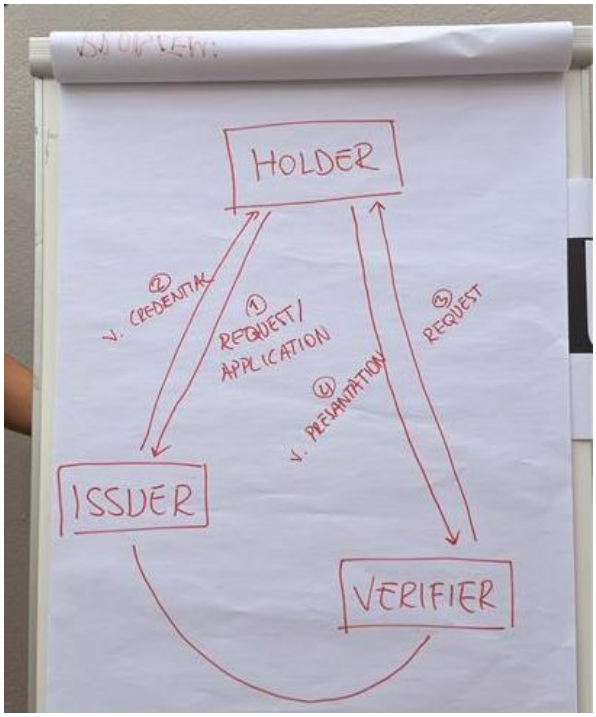
Picture 1: 

We began by mapping out the problem and what the goal would be for this solution (Picture 2). Whilst there were many more goals to achieve we listed the most painful points from the attendees.

Picture 2: 

And so we being solutioning and explaining each step of the process with numbers:

1. An individual—referred to as the Applicant, User, or Holder—initiates the process by completing an application form to request a KYC credential from a trusted institution, such as a bank.
2. Once the Applicant's information has been thoroughly reviewed and verified by the institution (the Issuer), a verified digital credential is generated and issued to the individual (now the Holder). The Holder then accepts and securely stores this credential within a digital wallet on their mobile device.
3. At a later stage, when the Holder wishes to present proof of their verified KYC status, a requesting organization, branch, or institution (the Verifier) will present a QR code for the Holder to scan. This QR code specifies the particular credential attributes being requested, such as KYC verification status.
4. The Holder unlocks their digital wallet and scans the QR code, authorizing the transmission of the verified credential to the Verifier. The Verifier then validates the credential against a Trust Registry, thereby completing the verification loop in alignment with the Self-Sovereign Identity (SSI) principles.

Picture 3: 

SSI-based Verified Credentials (VCs) for KYC eliminate repetitive verification and streamline property transactions by enabling secure reuse of once-vetted identity data across parties.

Current Friction in Property Deals

Traditional KYC demands buyers and sellers resubmit documents (e.g., passports, income proofs) to banks, notaries, and registries for each transaction, causing delays of weeks, high costs from manual reviews, and fraud risks from data silos.

Reuse Benefits of SSI VC KYC

Holders store a single KYC VC in their digital wallet after initial issuance by a trusted entity; verifiers scan a QR to request and cryptographically validate specific attributes (e.g., identity, funds source) against a trust registry—without re-verification or data sharing.

Reduced Friction Outcomes

This cuts transaction times from months to days, slashes operational costs by minimizing redundant checks, boosts security via blockchain immutability, and enhances privacy as users control selective disclosure.

END.

Unpacking the Jargon: Demystifying Digital Identity - who needs to know what, and when?

Session Convener: Annemie Krause
Session Notes Taker: Annemie

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Successful adoption of digital identity among South African citizens rely on the right communication - via traditional media, social media and through our own interpersonal interactions.
We have a collective duty - as crafters of digital identity infrastructure - to promote DID as a means to **solve real world challenges**. It is not a mere tech solution, but an **ENABLER**.

Communication should centre around WHAT'S IN IT FOR ME - but remaining cognizant of the very specific needs of different target audiences across all levels of society.

Comms should focus on sharing case studies - borrowing from global success stories, but also learning from WHAT NOT TO DO.

The question is: who is taking ownership of the communication? Is this happening on an individual organisational level, i.e. through thought leadership articles, blog posts, LinkedIn posts, etc.? Or is there perhaps a way in which we can amplify and streamline the communication efforts in a phased and targeted manner?

How open would the SARB / Reserve Bank be to share their content knowledge as a member of a 'DID Industry Collective / task team'? Which other industry partners would be willing to share their knowledge, or wish to contribute to the conversation around DID, its potential impact and benefits to society as a whole?

What are the outcomes of a successful DID communication strategy?

- Citizens will understand what DID is (and what it's not)
- They will see the practical benefits
- They trust that their data is protected
- Adoption grows organically

Questions remain as to who owns the conversation…. Looks like KPMG is already playing in this space!

https://www.itweb.co.za/article/digital-trust-is-critical-infrastructure-for-africas-digital-future/j5alrMQApNeMpYQk
DANKIE!

SESSION #8

The Future of Organizational Identity (South Africa Lens, Global Context)

Session Convener: **Max Coleman**
Session Notes Taker: Max Coleman

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

1) Why this conversation matters

Core framing: South Africa has multiple digital identity initiatives emerging (PID, DFID, and others). The open question is how these **fragmented systems** converge into a coherent ecosystem where **organisational identity becomes practically usable** for businesses.

Global comparison raised:

- Europe has moved toward more standardisation (eIDAS and the move toward a European Business Identity Wallet).
- South Africa is seeing multiple parallel efforts, but lacks a single, clearly adopted organisational identity framework.

Tension introduced early:

- Global standards like **GLEIF / LEI / vLEI** are powerful, but may be **too expensive** or heavy for the average SME in South Africa.
- So: what does a **South African-friendly** organisational identity stack look like, without losing trust and assurance?

2) A working definition: "Organisation" vs "Organisational Identity"

A major portion of the session centered on clarifying definitions, because the definition determines:

- what can be trusted
- what business models can be built
- what should be solved by "identity" vs "due diligence" vs "governance"

2.1 Organisation (what counts as an organisation?)

Key point: in emerging markets, "business activity" includes many actors who are not formal legal entities.

- **LEI scope (ISO 17442)** covers "garden variety" legal forms (companies, trusts, funds, partnerships where applicable).
- But South Africa has a broader reality:
    - informal businesses
    - individuals acting as businesses

- entities that behave economically like organisations, but are not registered traditional "legal entities"

Implication: Any SA organisational identity approach needs to acknowledge that **the set of "organisations" in practice may be larger than the set of registered companies**.

2.2 Organisational identity (what the identity is meant to prove)

A strong distinction emerged:

- **"Company registry existence" is not the same as organisational identity.**
  - A registry (CIPC / Companies House) tells you a company exists and is not deregistered.
  - It does not guarantee legitimate operations.
  - It does not guarantee correct directors/UBO records.
  - It does not bind real humans to authority in a way that is usable for trust.

A proposed layered idea:

- Organisational identity should include:
  1. the entity exists
  2. who controls it (directors/UBOs/controllers)
  3. who is authorised to act (roles + entitlements)
  4. the ability to prove those authorisations digitally (credentials)
  5. governance controls and ongoing updates (revocation, changes, monitoring)

3) Reality check: registry trust problems and "shelf company" fraud

A central challenge discussed: **company registries can be exploited**.

Example shared:

- A company can have an elderly/grandmother listed as the director for years.
- Criminals operate behind the scenes.
- The director may not even know they are listed.
- The entity remains registered, but the "identity" is effectively meaningless for trust.

Conclusion from this thread:

- If your organisational identity product only proves "registered + not deregistered," you can't safely build high-trust use cases.
- The system must bind **real humans** to **real authority** through verification, not just registry records.

4) Key assertion: "Start person → company (not company → person)"

An important principle surfaced:

Why "person → company" is better:

- One person can be associated with many entities.
- Fraudsters often hop from company to company.

- If you start with the company, you chase messy, often unreliable corporate records.
- If you start with the person, you can build:
    - continuity
    - reputation signals
    - association graphs
    - patterns of behaviour

This is the beginning of a "traceability" model:
Even if you don't fully stop fraud, you can make repeated abuse easier to detect and harder to scale.

5) Binding: the minimum viable trust step

A key convergence point:

To issue meaningful organisational credentials, you must ensure:

- an authorised representative is onboarding the company
- the person is verified (KYC)
- the person is legitimately linked to the entity (director check / proof of authority)

Practical rule suggested:

- Only an actively listed director (or verified authorised role) can initiate onboarding and credential issuance.

This became the "bridge" between:

- registry existence checks
- and real-world authorisation

6) LEI → vLEI parallels and what they teach South Africa

The discussion used LEI/vLEI as a reference model:

LEI (baseline)

- Proves the entity exists (validated against business records)
- Useful globally
- Already has rails in payments standards (e.g., ISO 20022 has fields for LEI)

vLEI (higher assurance)

- Requires strong verification of the people who act for the entity.
- Checks roles like director/secretary, etc.
- Creates a verifiable chain: entity exists → person has role → person can act.

Key insight:
vLEI does not replace business judgement.
It improves the ability to prove *authority and provenance*.

7) Trust is not “good vs bad company”... identity is a reusable onboarding enabler

- Organisational identity shouldn’t imply “this company is good.”
- It should support reusable onboarding and verification.
- Due diligence like tax status, financial health, sanctions screening, etc. changes often and remains necessary.

The “identity layer” vs “trust relationship layer”:

- Identity gives cryptographic proof of “I am this business / I represent this business.”
- Trust and risk still require:
    - business judgement
    - additional credentials (tax, bank ownership, etc.)
    - continuous re-verification and revocation mechanisms

8) Primary use cases where organisational identity shines

The group converged on a simple but powerful point:

There aren’t 500 use cases. There are a few repeating ones:

1. onboarding (repeat due diligence fatigue)
2. sharing verified bank details (avoiding payment diversion)
3. proving tax status / compliance indicators
4. vendor onboarding and procurement enablement
5. role-based signing authority (who can sign what)
6. secure communications tied to verified org identity (reduce impersonation)

UK research reference cited:

- SMEs reproduce due diligence data **multiple times in early months**, wasting time and slowing growth.
- Organisational identity is a “consent-based reuse” mechanism:
    - share once
    - reuse many times
    - revoke when needed

9) PID / DFID as foundational enablers for organisational identity (South Africa)

A key forward-looking section: how PID and DFID could help bind people to companies.

Proposed flow:

1. company registration number check (CIPC)
2. director list check
3. user provides ID number
4. system matches ID number to listed director
5. KYC performed on the actual person
6. PID helps confirm identity + streamline KYC / reduce friction
7. in future, DFID likely applies to any financially active actor (not just individuals)

Critical missing element highlighted:

- Not just "ownership," but **roles and entitlements**:
  - shareholders may not have signing authority
  - someone can own a tiny share but control everything
  - therefore the system must model:
    - roles (director, secretary, authorised rep, etc.)
    - entitlements (can sign, can approve payments, can update bank details, etc.)

10) Corporate governance and "self-declared authority" as a trust upgrade

A strong idea emerged:

- Beyond registry facts and identity checks, there is a **governance layer**.
- Companies can optionally (but powerfully) self-maintain:
  - who can do what
  - role-based authority
  - signing permissions
  - operational entitlements

This was described as:

- "optional but increases level of assurance"
- a governance signal
- a "corporate access control" model

If a company maintains this accurately, relying parties can trust that:

- documents are signed by legitimate authorities
- approvals come from the right roles
- internal controls exist

11) Cost reality: why vLEI is expensive and what "low-cost SA" could look like

Key points on cost:

- vLEI cost is mainly verification rigor, not "a fee for a label."
- High assurance requires:
  - robust checks
  - often video-based proofing
  - anti-deepfake countermeasures
  - strong identity assurance and liveness

Important trade-off agreed:

- Lower cost often increases downstream risk.
- But the ecosystem can support multiple tiers:
  - LEI as globally useful baseline
  - local identity credential as lower-cost stepping stone
  - vLEI as the high-assurance governance/role model

A pragmatic concept surfaced:

- Not one standard to rule them all.
- Different segments will pay for different assurance levels.
- Some verticals bundle wallets + other services with vLEI to justify cost.

12) Levels of Assurance: the emerging framework

A very actionable outcome: define levels of assurance for organisational identity and let relying parties choose what they require.

A rough ladder proposed in discussion:

- **Level 0:** company exists and not deregistered (basic registry check)
- **Level 1:** company + verified directors / KYC of onboarding authorised rep
- **Level 2:** additional authoritative credentials (e.g., LEI attribute, verified bank account ownership, tax status credential)
- **Level 3:** UBO, role/entitlement modelling, governance disclosures, stronger assurance mechanisms
- **Level 4:** vLEI-style organisational authority credentials (high assurance + robust proofing)

Two parallel concepts were introduced:

1. **Levels of assurance** (how verified / how strong)
2. **Credential verification matrix** (what's considered strong evidence vs weak evidence)
    - e.g., address from PDF is weak; address verified via trusted rails is stronger
    - relying party chooses requirements based on risk and use case

Commercial implication:

- Pricing can align to assurance levels.
- Relying parties pay based on what level they require.

13) Ecosystem principle: who should issue credentials?

- The ecosystem should allow:
    - government, banks, registries, regulated entities, or standards bodies to issue
    - Different providers/wallets/applications such as VERA to be the workflow + trust layer that consumes/uses these credentials
- But in early markets, platforms may need to issue initially because the ecosystem isn't ready.

This was framed as:

- "Until the ecosystem exists, you do it yourself."
- But the strategy is to evolve toward a multi-issuer environment.

14) Strong closing insight: organisational identity is "shuffling trust around"

A memorable summary from the discussion:

- The core function is to ensure credentials originated from the right entity.

- The platform takes responsibility for what it issues:
    - if it goes wrong, it carries reputational and operational accountability
- The trust model is practical, not philosophical:
    - prove provenance
    - prove authority
    - reduce repeated onboarding burden
    - enable safer transactions and communication

Practical Takeaways (What this session clarified)

1. **Define organisational identity by what it enables** (reusable onboarding, authority proof, verified payment details), not by whether a company is "good."
2. **Registry existence is not enough** — the human authority layer is essential.
3. The future is **tiered assurance**, not one universal credential.
4. **PID/DFID can reduce friction** and strengthen person→company binding.
5. **Roles + entitlements** are the missing middle layer in South Africa.
6. Governance disclosures are optional but significantly increase assurance.
7. LEI is globally useful baseline; vLEI is high-assurance authority model; SA likely needs an intermediate, lower-cost bridge.

What Digital Identity Verification Technologies can Support & Improve Social Impact?

Session Convener: Alwyn van Wyk
Session Notes Taker: Alwyn & Sam
(optional) List of Session Attendees: ±7

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Assumption going into the session:

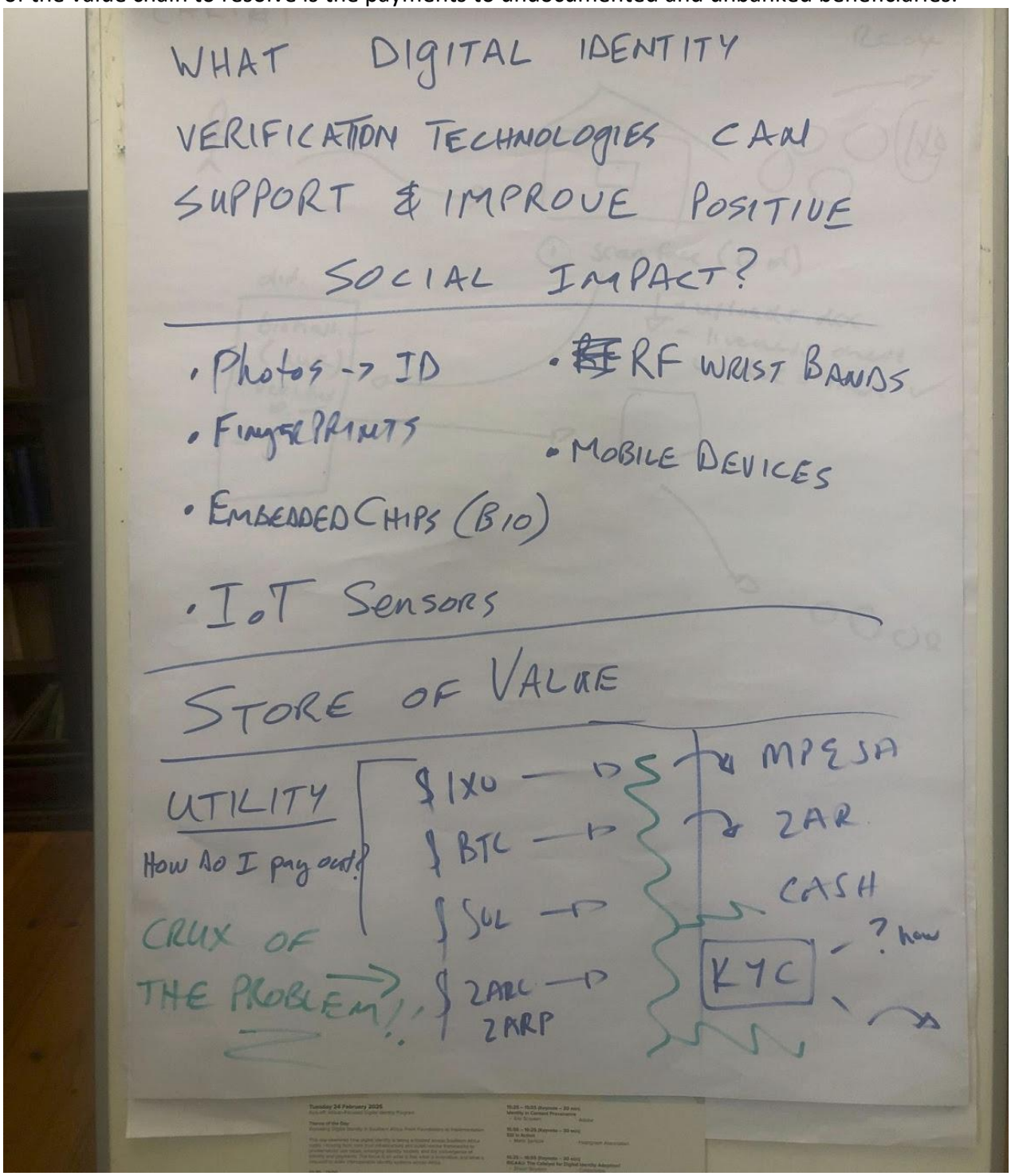
- There are very few technologies available to improve social impact

Conclusion at the end of the session:

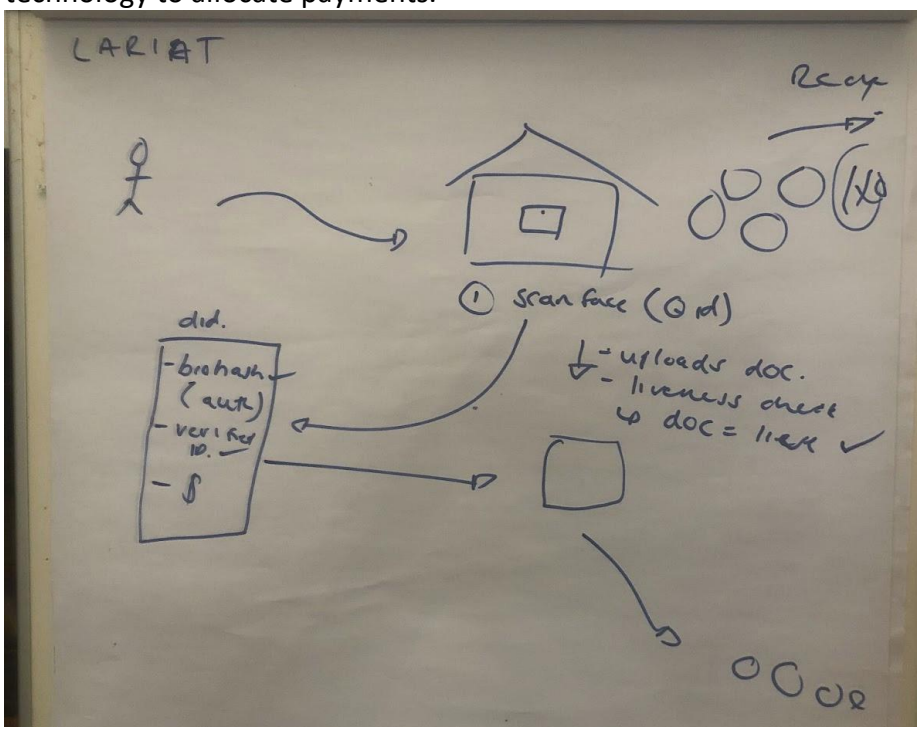
- A viable technology that supports waste collection is available and currently in production use.

Below are flip chart pictures of the notes.

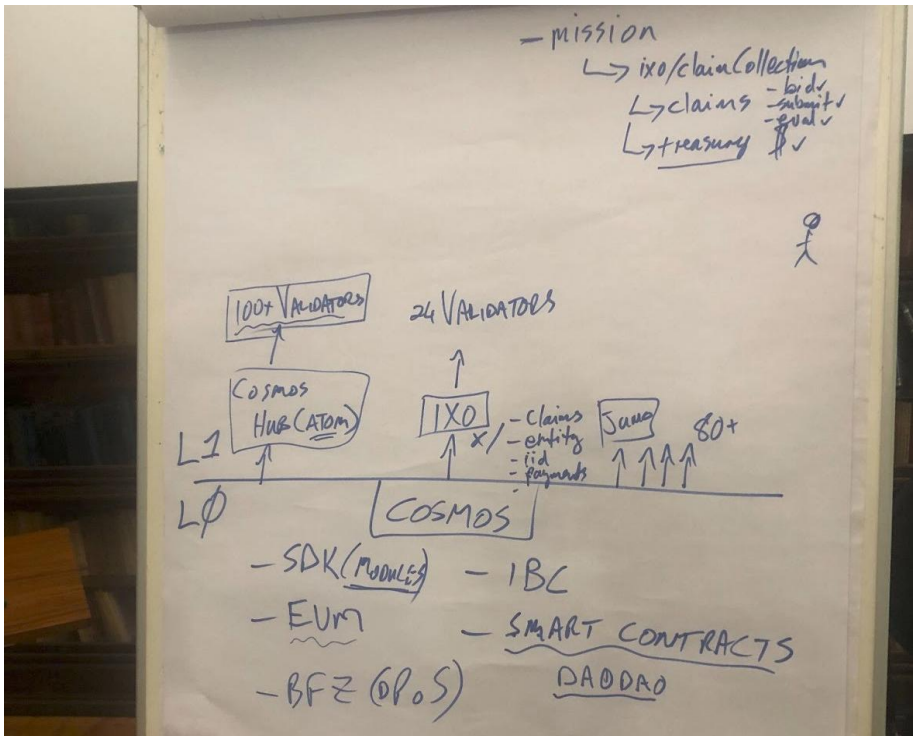
We started by listing an inventory of possible technologies and noting that the most difficult part of the value chain to resolve is the payments to undocumented and unbanked beneficiaries.



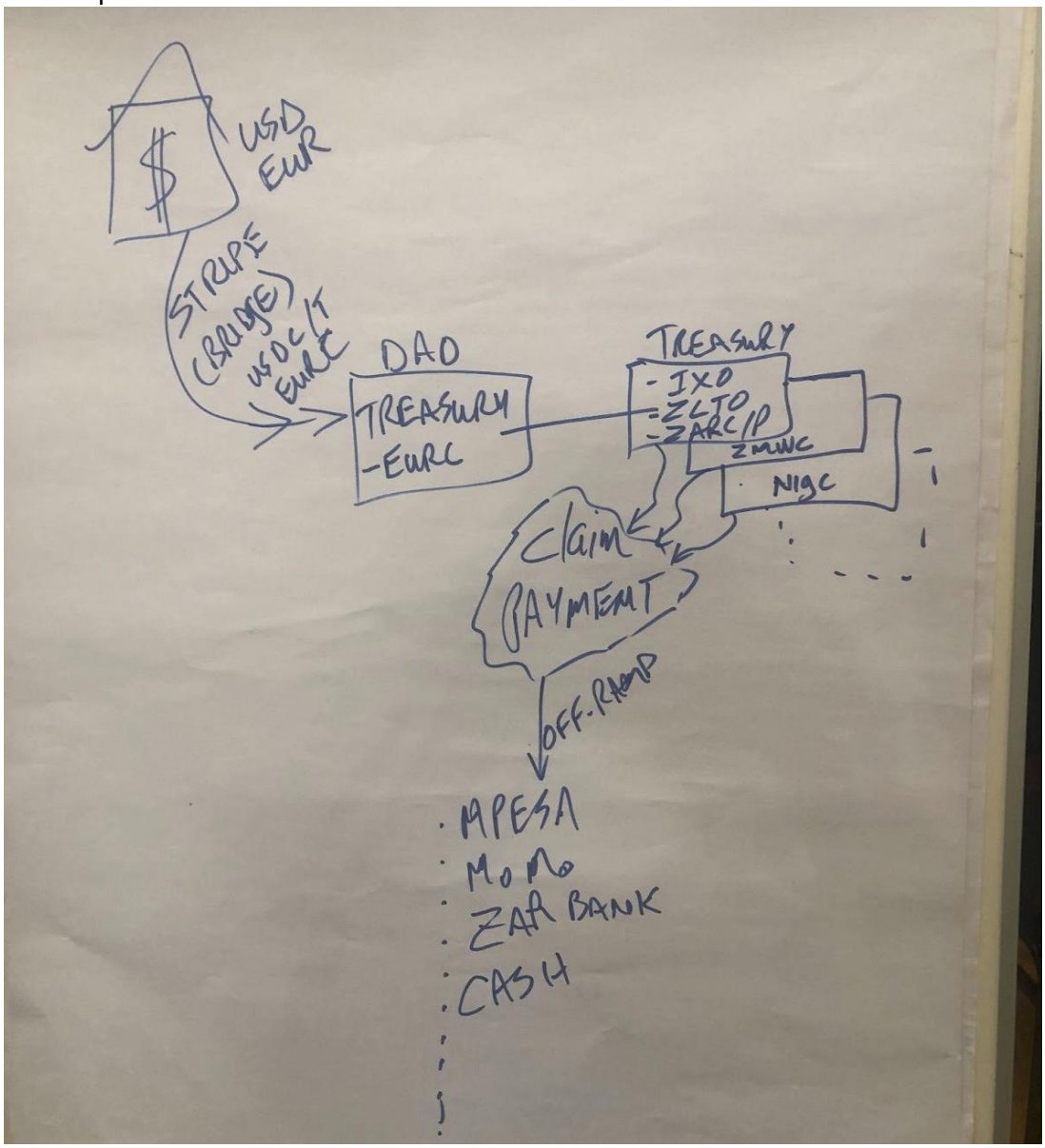
Sam and Wynand described the Lariat solution that uses privacy-preserving facial recognition technology to allocate payments.



We diverged into the Cosmos blockchain network and how it enables the IXO Impact Hub to use Cosmos software building blocks to have a sovereign Layer-1 Delegated Proof-of-Stake blockchain network with 5-second finalisation and decentralisation across 24 independent trustless validator nodes.



Finally, we further discussed how we might be able to solve the payments issue and agreed that off-ramps are the main issue.

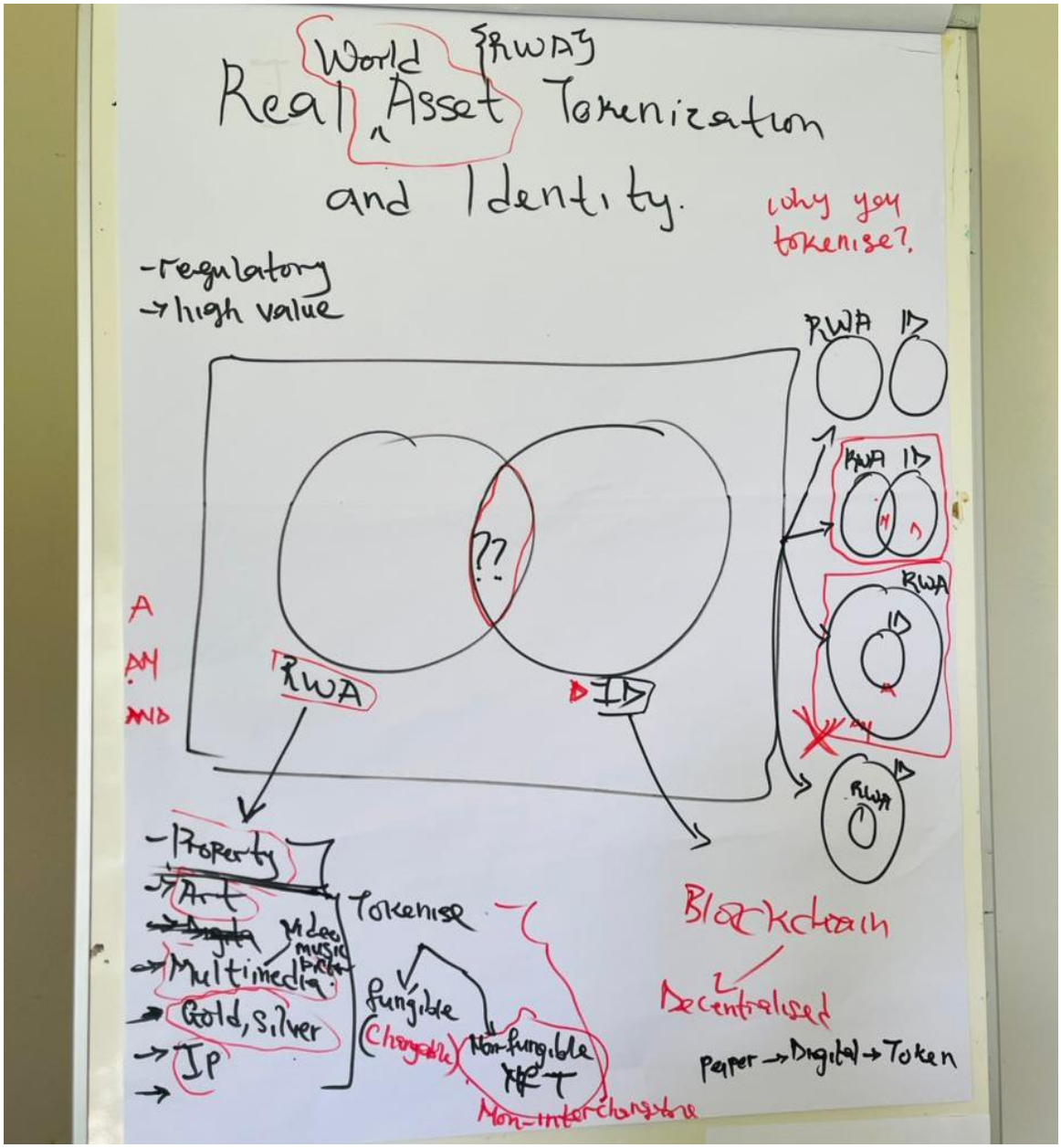


SESSION #9

Real-world Asset (RWA) Tokenization (NFT) and Identity: Where is the meeting point?

Session Convener: Timileyin Abiodun
Session Notes Taker: Timileyin Abiodun

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?



How to start an ecosystem which uses a Digital Wallet?

Session Convener: OMAR
Session Notes Taker:
(optional) List of Session Attendees:

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

NO NOTES SUBMITTED

What's SSI incubator going to be like in 2026 in Africa?

Session Convener: **Maya Kanehara**
Session Notes Taker: Maya

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

It was an open discussion for anyone who was ready to kick off startups or already has startups. Questions were below:

- How to find investment?
- How to find the right investors?
- How do we actually launch projects out of innovator hubs?
- How does investment work?
- How do I assess product market fit?
- Hoto approach investors?
- How to scale?
- What can founders prepare before talking to investors?
    - Founders who know everything about their subject
    - Team with a variety of skills
    - Invest in yourself first
    - Market sizing
- How to protect ideas
    - NDA
    - Under university rules
    - Hide ideas in unique way

SESSION #10

The Impact of AI?

Session Convener: Tina Valab
Session Notes Taker: Tina Valab

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

The impact of AI with DID
The Promise and Current Misuse of AI

The discussion opens with the observation that AI is an incredibly powerful tool meant to make our lives easier, yet many people currently misuse it for trivial things (like generating caricatures) or fail to prompt it correctly. Because AI models are still in their learning phases, giving them poor instructions leads to poor outputs (or "hallucinations"). The consensus is that AI shouldn't be feared as a world-taking overlord, but rather understood as a tool that requires proper direction.

Biometrics vs. Digital Identity

A major concern raised is the fear of AI stealing a person's face, voice, or fingerprints to commit fraud. The group clarified the difference between raw biometrics and a true Digital Identity:

- **Biometrics (The Risk):** If a company stores your actual face or fingerprint data, it creates a "honeypot" that hackers could target.
- **Digital Identity (The Solution):** A digital identity acts like a verified, encrypted digital passport on your phone. You prove who you are *once* (using your biometrics securely on your own device), and the device issues a verifiable credential. This allows you to prove your identity to other services without actually handing over your physical face or fingerprint data.

AI Agents and Delegation (Agentic Payments)

The group explored the future of "AI Agents"—giving an AI permission to execute tasks or spend money on your behalf.

- **The Challenge:** If you give an AI the "key to your kitchen" to wash dishes, you must ensure it doesn't also use that key to "drive your car."
- **The Fix:** We will need systems that allow for strict delegation. For example, you might authorize an AI agent to buy groceries or find deals automatically if the cost is under R200, but require a manual push-notification approval (a "friction point") for anything more expensive.

Open Banking and the Technical Hurdles

For AI agents to actually manage your money or shop for you, they need secure ways to connect to banks and retailers. The conversation touched on APIs (Application Programming Interfaces) and Open Banking. While the technology exists for AI to securely interact with banking systems without needing your raw login passwords, the banking industry is moving slowly due to regulatory, security, and competitive concerns.

Security, Deepfakes, and "Liveness"

The most pressing fear discussed is the rise of deepfakes and AI voice cloning (e.g., scammers cloning a family member's voice to ask for emergency money).

- **The Defense:** The countermeasure to this is **Liveness Detection**. Modern security systems don't just look at a static photo or listen to audio; they use sophisticated methods (like analyzing blood flow, microscopic movements, or reacting to hidden flashing screen colors) to prove a live human is on the other end of the device.
- **The Reality:** It is a constant arms race. Cybersecurity experts and AI developers are building walls, while "bad actors" are trying to break them down. The ultimate advice from the group is to stay vigilant, maintain a healthy level of paranoia, and rely on verified digital identities to navigate the digital world safely.

How do we include places with those that are not Tech-inclinded / aligned?

Session Convener: Maxwell Tlou
Session Notes Taker: Maxwell Tlou

Please list the key points of your conversation, what you would like to share with your colleagues and are there any next steps?

Key Strategies:
* Navigate safely through tech: Providing a safe path for those unfamiliar with digital tools.
* Use relatable language: "Teach them language they understand" , avoiding jargon to make tech more accessible.
* Leverage local expertise: Establishing a Local Training Unit led by a trusted person within the community.
* Simplify: Reducing complexity in tools and processes.
* Build trust: Using clear communication to establish confidence in new systems.
* Address friction through education: Proactively educating users to solve common frustrations.
* Educational integration: Implementing courses or programs within schools and communities.

Thank you to our Women's Breakfast Sponsor Umazi

A tradition started early on at the Internet Identity Workshop, the Women's Breakfast provides the opportunity for the women attending the event to meet informally and share about their experiences working in a field of mostly men, their career paths, share pointers and generally get to know each other.

This year at the suggestion of Umazi Ltd 's founder Cindy van Niekerk the Women's Breakfast included a 30min facilitated session with business coach Diane Lindemann on the topic of 'Your Identity', but not a digital ID — your identity as a woman and the impact it can have, depending on how you frame it. Do you think of yourself as an assistant or a change maker? How you frame it to yourself will influence how others see you.

Online Posts by Attendees

PayInc
31,670 followers
3w • Edited •

PayInc is proud to sponsor the Barista, a welcoming connection point at this year's DID:UNCONF AFRICA from 24-26 February 2026 at the STIAS: Stellenbosch Institute for Advanced Study. If you're attending, come visit us, and say hello to the team!

We're looking forward to facilitating great conversations to shape the future of secure digital payments.

#MakingGreatConnections #DIDUnconfAfrica2026 #DigitalIdentity

Contactable
2,594 followers
2w •

Self-Sovereign Identity (SSI) might sound niche right now — but it's fast becoming a foundation for how digital identity evolves in a Web3 world. Who controls your data? Who can verify who you are — and on what terms?

At DID:UNCONF AFRICA, our COO Jason Shedden joined Jannie Pretorius (Chief Product Officer at DIDx) to make SSI practical in a breakout session: Self-Sovereign Identity for Dummies. The only rule? If it gets too technical, someone shouts "🍍!"

Less jargon. Better questions. Better progress.

Shoutout to our Eugene Bauling for joining the session (and making a cameo in the pics too)!

#DIDUNCONFAFRICA #SSI #SelfSovereignIdentity

Maxwell Tlou • 2nd
Experenced Data Protection specialist MySql Solution Engineering Digital Iden...
2w •

I had the opportunity to attend DID:UNCONF AFRICA, hosted at STIAS: Stellenbosch Institute for Advanced Study, and it was truly an inspiring experience.

The event brought together innovators, policymakers, technologists, and thought leaders who are actively shaping the future of digital identity and digital trust across Africa. What stood out the most was the Open Space unconference format, where participants collaborate and drive the discussions based on real challenges and opportunities in the digital identity ecosystem.

Throughout the sessions, there were insightful conversations around digital identity frameworks, interoperability, innovation in Africa, and how technology can enable more secure and inclusive digital systems.
Grateful to have been part of such an impactful gathering and to connect with people who are working towards building Africa's digital future.

#DigitalIdentity #DIDUNCONFAfrica #AfricaTech #Innovation #DigitalTrust #TechC

South Africa-Swiss Bilateral Research Chair in Blockchain Technology + Follow
1,238 followers
1w •

The final day of DID:UNCONF AFRICA!

The South Africa-Swiss Bilateral Research Chair in Blockchain Technology (#UJBlockchain) delegates had an incredible time joining conversations with thought leaders and global experts to help shape the future of digital identity. The team spent the final day demystifying concepts around self-sovereign identity (#SSI), engineering solutions from an initial idea to an #MVP, creating and pitching #startups, and more.

A special highlight was one of our delegates, Mr Timileyin Abiodun, moderating a session that explored the intersection of Real-World Asset (#RWA) #tokenisation and digital identity.

Several key takeaways from the event will serve as our action points going forward. Some of which include securely integrating self-sovereign identity frameworks with #IoT and #blockchain infrastructure for verifiable data provenance, and advancing the tokenisation of real-world assets by leveraging decentralised identity to build trust and scale compliance across the continent.

Sarah Mulaji • 1st
PhD Candidate (Information Systems) at the University of Cape Town | Doctor...
2w • Edited •

It has become almost undeniable that Digital Identity (ID) is desperately needed in Africa. DID:UNCONF AFRICA has taught me again just how much researchers, technology experts, policymakers, and innovators are willing to sit in the same room to brainstorm complex issues around digital ID in Africa.

A shared conviction is that digital ID is a high-stakes technology, yet the technology alone does not solve the digital ID problems: the social & organisational side of digital ID is the elephant in the room, i.e. coordination, ID governance, trust framework, inclusion, privacy, communication, etc.

Like many attendees, I come in with questions and worries, e.g. siloed ID projects going on in South Africa, the proliferation of #AI agents and #deepfaking posing threats to the digital ID endevor, ... I left with more confidence that everyone is working behind the scenes to solve, prevent, and mitigate what could go wrong when rolling out the Digital Identity at a national scale.

Confronting research discourse with innovation discourse has been a rewarding experience for me, something I had not planned as part of the 'PhD toolkit', yet it has been critical in demystifying concepts. I am grateful Prof Irwin B. encouraged me to attend these events.

Thank you to DIDx and sponsors for affording us again the opportunity to represent the University of Cape Town (UCT) at the conference.

It was pleasing to reconnect with many people, including UCT alumni and cofounder of one of the cutting-edge Digital ID startups in South Africa, VERA.

VERA
381 followers
1d •

It was an honour for VERA to be a sponsor at the DID:UNCONF AFRICA 2026. What an inspiring gathering.

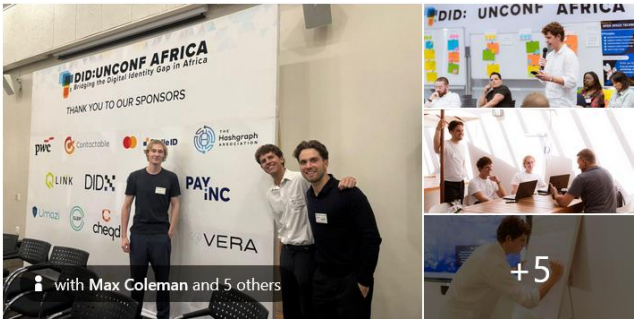
DID:UNCONF AFRICA continues to stand out as a space where builders, policymakers, startups, NGOs, and global experts come together to have open, practical conversations about the future of digital identity in Africa.

One theme that came through strongly this year was the growing convergence between identity and payments. As financial systems become more digital, verifying who is behind a transaction or organisation is becoming critical infrastructure. Discussions explored decentralised identity adoption across payments, security and privacy, inclusive identity for rural communities, real-world asset tokenisation, and the broader impact on healthcare, finance, and employment for African youth.

Our co-founder Max Coleman hosted a session exploring the future of organisational identity in South Africa within a global context. The discussion focused on how organisational identity must go beyond simply proving a company exists in a registry. Instead, it must bind verified individuals to real authority within organisations and enable trusted business interactions such as vendor onboarding, procurement, verified payment details, and secure communication between companies.

A huge thank you to DIDx, and especially Gideon Lombard, as well as Heidi Nobantu Saul from the Internet Identity Workshop, for bringing together such an important community and orchestrating such a thoughtful and impactful event.

We are excited to continue contributing to this ecosystem as Africa shapes its own path for digital identity.



Umazi Ltd
1,190 followers
2w •

What an incredible few days at DID:UNCONF AFRICA 2026!

We were thrilled to attend and proudly sponsor the Women's Breakfast at this year's DID:UNCONF AFRICA conference — a vibrant gathering dedicated to advancing digital identity innovation across Africa.

This event brought together local and international leaders, technologists, policymakers, and innovators to co-create solutions that will shape the digital identity ecosystem on the continent.

From deep conversations on interoperability and trust to collaborative unconference sessions, the energy and insight across STIAS in Stellenbosch were truly inspiring.

We were especially honoured to support the Women's Breakfast — a space for women in tech and identity to connect, share experiences, and champion representation in a rapidly evolving field. This important tradition fosters community and empowerment, and we're proud to have played a part in making it happen.

A huge thank you to the organisers, participants, and fellow sponsors who made this conference such a meaningful and impactful experience. Looking forward to continuing the conversations and collaborations sparked over the past few days!

#DIDUnconfAfrica2026 #DigitalIdentity #Inclusion #Innovation #WomenInTech #C

Event Highlights Photos and Testimonial Videos

You can see the DID:UNCONF AFRICA 2027 Event Summary here: https://didunconf.africa/past-events

DID:UNCONF AFRICA 2027

DID:UNCONF AFRICA returns to STIAS, Stellenbosch, March 16 – 18, 2027. Registration opens in September.

Visit www.didunconf.africa for updates or email info@didunconf.africa for more information about attending and sponsoring. Stay tuned for updates via email, LinkedIn, and our other channels—we'll be sharing news, program highlights, and ways to get involved.

DID:UNCONF AFRICA is an IIW Inspired™ Regional Event co-hosted in South Africa with DIDx

DID:UNCONF AFRICA
Bridging the Digital Identity Gap in Africa

IIW Inspired™ Regionally Focused Open Space unConference

DIDx

Open Space unConference Facilitation: Heidi Nobantu Saul
Notes Collection & Compilation: Heidi N. Saul