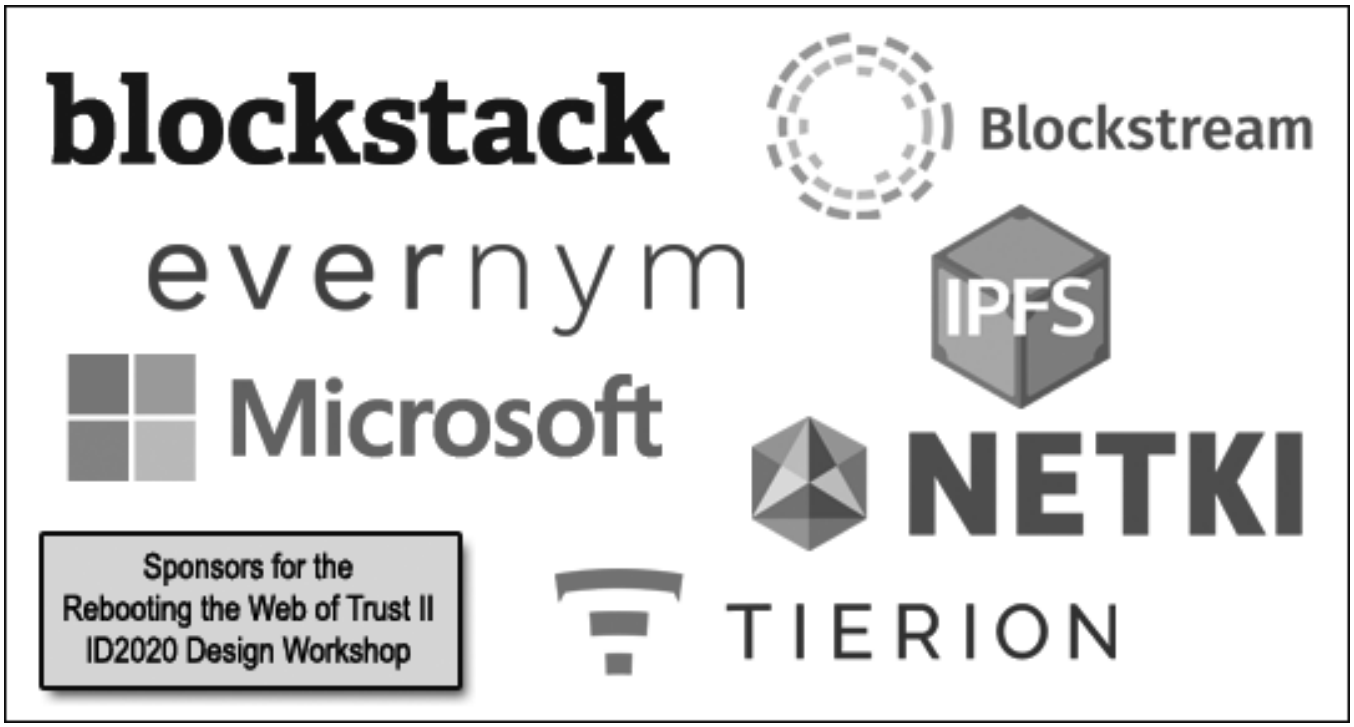
Protecting Digital Identities in Developing Countries (v1.3)

A Use Case from Rebooting the Web of Trust II: ID2020 Design Workshop

by Wayne Hennessy-Barrett

ABSTRACT

People in many parts of the developing world have little or no infrastructure for well-regulated government and commercial processes. This creates a pressing need for a safe place to store important personal data needed to access financial, insurance, education and healthcare services. A universal digital identity system would underpin information assurance through verifiable and reliable data that can be presented when required. This paper presents a strong use case for a self-sovereign identity system with verifiable information and user-controllable release.



1. CONTEXT

Large parts of Sub-Saharan Africa and other frontier markets are characterized by immature or dysfunctional national governance. Physical infrastructure is crumbling and public services are substandard or non-existent. In many places predatory and corrupt public officials abuse their authority and augment their salaries by extracting payments from the public.

Political power and discourse are frequently apportioned on ethnic and tribal lines, rather than by ideology. This perpetuates divisive identity-driven grievance politics, clan-based thinking and short-termist behaviour to fund patronage networks.

"Despite this, mobile phone ownership and coverage is widespread. Well-developed telecom and internet penetration sits alongside erratic public services and transport networks.

1.1 Persona

The informal economy, where self-employed workers operate outside regular salaried employment, greatly outstrips the formal sector, comprising over 65% of employment in many African countries. These informal workers by definition are 'off the grid'. In the absence of a functioning social contract they lack incentives to register their businesses or to pay taxes.

Women are often the primary breadwinners despite conservative and patriarchal social structures. Individuals are aspirational, hard working and resilient; they want a better future for themselves and their families.

While citizens receive a national identity number in many places, this does not equate to representation or to access to public services, as these functions often do not exist.

1.2 Threats

Threats to the individual can be categorized into three broad themes:

- **Thieves** seek to enrich themselves by the appropriation of monies and properties from their victims. Corrupt officials and service providers such as bankers or retailers fall into this category. Identity theft is an increasing vector for scammers, criminal gangs and individuals.

- **Murderers** seek to harm or physically remove or displace their victims. They can be motivated by ethnic rivalry, terrorist ideology or the political desire to acquire power or retain control of it.

- **Oppressors** seek to exercise local power by exploiting comparative advantage to the disadvantage of others. Leverage may come through population size, access to resources or control of power such as political, police or military appointments. They ruthlessly suppress opposition to their dominance, often through the means above. Their objective is limited to maintaining hegemony.

All groups seek to identify their victims, assess their economic or symbolic value, confirm their location and access their data, in order to extract the greatest possible value relative to their purpose.

1.3 Problem/Opportunities

Individuals lack the ways and means to safely and reliably store their important personal data. Where government-issued IDs exist, they often bear little relation to the access and provision of adequate products and services. When individuals' data is illegitimately acquired and abused, they become highly vulnerable to fraud, theft and compromised personal or family safety.

Developers and administrators of any system must operate on the assumption that all official systems are inherently vulnerable. Therefore, the digital identity system must complement and augment existing national identity systems, providing additional assurance, rather than undermining or supplanting national government sovereignty. A reliable, trusted identity will enable the provision of key services in the following ways:

- **Human Rights Protection**. The fundamental impact of a digital identity system is to 'give voice to the voiceless' by the positive attestation of an individual's existence. Absence of a formal identity contributes to denial of both the most basic amenities (even where they exist) and a sense of social belonging. This becomes more stark in periods of conflict, civil unrest or natural disaster. Refugee identification is a prevalent issue today; the inability to positively identify individual migrants, let alone validate their qualifications, their medical history or their

sources of wealth is the heart of host nations' concerns regarding immigration risk.

- **Financial Services**. Credit scoring, 'Know Your Customer' and due diligence would all be enhanced by the provision of verifiable, trusted data. The absence of reliable data on individuals is a key driver of financial exclusion. Digital IDs would remove risk from an enormous market for financial services.

- **Insurance**. Verified personal information would permit risk-assessment and pricing of insurance products to a greater resolution than currently possible. Event recording and claims assessment would be similarly enabled by the creation of secure systems where information can be recorded and assured by trusted third parties.

- **Education**. While the Massive Online Open Course model of online education provides access to knowledge, the verification of qualifications and achievements requires a trusted identity to protect any linkage to academic awards. Provision of secure identities would underwrite individual academic qualifications, enhancing access to opportunities and creating confidence in human capital.

- **Medical Services**. Individual identity integrity is a fundamental component for maintaining medical records (such as immunization or prior clinical treatments) and can also assist in assessing insurance premiums or other qualification for treatment.

1.4 Self Sovereignty & Security

The concepts of self-sovereignty and security are fundamental to the utility and adoption of a digital identity system. The private individual must be the owner and steward of their personal data, independent of any issuing or approving authority. They must have right of control over which information is released in exchange for access to services and which information they choose not to disclose. While the individual retains full agency over disclosure, this data must be validated by accredited third parties (such as governments, academic institutions or credit agencies) when it is appropriate and necessary. The highest forms of system authentication, data integrity and confidentiality are required for this paradigm to function.

1.5 Adoption & Scaling

The challenges of adoption and scaling could be met by the deployment of independent identity systems, providing a means of enhancing personal information security. Such systems could deliver value and improve lives when adopted by individuals ahead of official acceptance by public sector institutions. Commercial or freeware models could reduce the risk of the initiative and encourage use by existing national ID systems. As confidence develops, these systems could be used to access government services to the benefit of both individual and the government. This approach was endorsed by US Government representatives at the UN ID2020 summit in May 2016.

Creation of a workable digital identity system will require collaboration between governments, industry, NGOs and customer representation stakeholders.

2. CONCLUSION & CALL TO ACTION

The central thesis, as well as characteristics and possible system architectures, has been described in *other works*. The benefits of a digital identity system extend beyond the theoretical, and have the potential to fundamentally improve basic conditions for *billions* of people. This paper calls for the applied effort of the development community to find ways to deliver an independent digital identity system to the developing world where the need is most pressing.

Additional Credits

Author & Lead Paper Editor: Wayne Hennessy-Barrett

Contributors: Timothy Ruff, Jon Geater, Dave Crocker, Russ Haywood, Kimberly Little, Marta Piekarska, Thessy Mehrain, Fatma Nasujo, Kaliya Young

About Rebooting the Web of Trust

This paper was produced as part of the **Rebooting the Web of Trust II** design workshop. On May 21st and May 22nd, 2016, over 40 tech visionaries came together in Manhattan, New York following the ID2020 Summit at the UN to talk about the future of decentralized trust on the internet with the goal of writing 3-5 white papers and specs. This is one of them.

Workshop Sponsors: Blockstack, Blockstream, Evernym, IPFS, Microsoft, Netki, Tierion, ID2020

Workshop Producer: Christopher Allen

Workshop Facilitators: Christopher Allen and Kaliya Young with graphic facilitation by Sue Shea, additional paper editorial & layout by Shannon Appelcline, and additional support by Kiara Robles.

What's Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments, thoughts, or expansions on this paper, please post them to our GitHub issues page:

https://github.com/WebOfTrustInfo/ID2020DesignWorkshop/issues

The next Rebooting the Web of Trust design workshop is scheduled for October 19th-21st in San Francisco, California. If you'd like to be involved or would like to help sponsor these events, email:

ChristopherA@LifeWithAlacrity.com