

# Distributed crypto identity as a mechanism for legal empowerment of the poor and stimulating local economic development

*Gavin Chait*  
*[gchait@whythawk.com](mailto:gchait@whythawk.com)*  
*<http://www.whythawk.com/>*

*18 January 2015*

## *Abstract*

Billions of people are excluded from the rule of law. Many have no legal way of proving their own identity. Instead they rely on geographically-bound informal networks of trust to work and invest. Should they move in search of new opportunities, or as a result of conflict, they lose not only their homes and social support structures, but also their identities.

This paper proposes a mechanism by which a distributed information technology network, based on cryptographic proof instead of a single trusted intermediary, can generate secure digital identities without relying on the existence or benevolence of a functioning state.

Importantly, since there is no single point of failure and the identity is vouchsafed by an irreversible and distributed record, that identity can never be taken away from the individual. Government or organisation failure, conflict, or migration will not render a person without identity.

The means to generate secure digital identities already exist, are mature and low-cost. Biometric identity systems are in use in India. Cryptographic transaction mechanisms are in use online.

Nor is illiteracy or poverty a barrier to technology acceptance. Across the world's poorest regions, individuals are more likely to have a mobile phone than a formal legal identity. They are also far more likely to use their phones as a means of financial exchange than to have bank accounts. The obvious advantages of virtual currency transactions and phone-based identity have spurred adoption.

Digital legal identities are now viable and offer even greater opportunities for the world's poorest.

## 1 The impact of legal exclusion on the poor

"Goodbye Thando, your mom loves you so much. I am going to rest with my father, where I will not be asked for my ID."<sup>1</sup>

On 26 May 2007, Bongekile Lucia Mkhize committed suicide. After two years, and three applications to the South African Department of Home Affairs, she gave up waiting for her identity documents. Without them she was unable to register to study nursing or even secure temporary employment.

She was 24 years old.

Mkhize was not alone in having legal exclusion deny her access to opportunity. In "Making the Law Work for Everyone"<sup>2</sup>, the Commission on the Legal Empowerment of the Poor estimates "that around four billion people, the majority of the world's population, are excluded from the rule of law."

Article 6 of the Universal Declaration of Human Rights, which is binding on all UN member-states, declares: "Everyone has the right to recognition everywhere as a person before the law."<sup>3</sup>

A lack of legal identity denies individuals access to a range of rights, grouped by the Commission as the "Four Pillars of Legal Empowerment"<sup>2</sup>:

1. *Access to justice and the rule of law*: a lack of legal identity may be used to exclude individuals from the justice system, denying them recourse or even prevent access to representation in court;
2. *Property rights*: secure title assigned to a specific owner permits persistence of tenure, which supports the development of the economic potential of those assets and the ability to pass those assets on to descendants;
3. *Labour rights*: laws, and contracts of employment with specified individuals, should protect workers from exploitation without reducing their opportunities for formal employment;
4. *Business rights*: informal businesses lack the ability to enforce contracts which leaves them open to exploitation through bribery or violence; ensuring their rights to vend from a persistent and recognised workspace would support economic growth;

A lack of legal identity has "a direct effect on possibilities and opportunities for full participation in social, political, and economic life"<sup>4</sup>. Poverty is, in and of itself, a sufficiently challenging condition without also having legal impediments that act to prevent individual action to escape that poverty.<sup>5</sup>

Post-conflict societies present even greater challenges, especially where refugees have migrated far from home, and where individuals lack any prospect of return or mitigation of the harm they have suffered.

While the study and recognition of the need for legal empowerment of the poor has generated consensus on the costs of their absence, and benefits of extending legal rights to all, there is also recognition that recommendations for implementation are scant<sup>6, 7</sup>.

**This paper proposes a mechanism by which a distributed information technology network, based on cryptographic proof instead of a single trusted intermediary, can generate secure digital identities without relying on the existence or benevolence of a functioning state.**

**Importantly, there should be no single point of failure since the identity is vouchsafed as an irreversible record by a distributed network. Government or organisation failure, conflict, or migration should not render a person without identity.**

In order for this approach to be implemented, three conditions must be met:

1. The technology must exist, and be sufficiently mature and cost-effective, to offer digital identities;
2. It must be possible to offer secure identities independently of a trusted intermediary, such as a government or corporation, so as to avoid political or economic interference, and to ensure that there is no single point of failure;
3. Poverty and illiteracy should not be barriers to the adoption of technology solutions and the advantages to having a digital identity must be sufficiently compelling so as to overcome resistance.

## **2 How the poor create trust for identity and economic transactions**

Not all the Zimbabweans queuing at the long-haul taxi rank in Johannesburg in 2007, at the height of Zimbabwe's hyperinflationary crisis, were going home. Many were there to bargain with the drivers to send money across the border.

They rely on networks of trust, from driver to their distant families in the rural areas, to ferry a bundle of notes thousands of kilometres. With Zimbabwe's finance minister capturing legal transfers this was the only way for many to support their wives and children. Despite the seeming impossibility, the system works, although it exacts tremendous transaction costs of up to 60% of the initial amount.<sup>8</sup>

Throughout the world – and in the absence of formal credit systems or legal identity – groups of people come together to save and borrow money. In South Africa they're *stokvels*, in West Africa they're *susūs*, in Cambodia they're *tontines*, *arisan* in Indonesia, *likelembas* in the Democratic Republic of the Congo, *xitique* in Mozambique and *djanggis* in Cameroon.<sup>9</sup>

These Rotating or Accumulating Savings and Credit Associations are universal and produce trillions of dollars in savings and investments worldwide.<sup>10, 11</sup>

The mechanism by which these transactions are vouchsafed is for a group of individuals to get together and agree to pool their resources. Each month they pay over a part of their incomes into the group. Any of the members can request to borrow from that pool.

The interest on borrowing is extremely high, giving the lender a good return on their investment. At the end of a fixed period, all the money is repaid into the group and distributed to all members according to the level of their investment.<sup>12</sup>

Dr Samuel Johnson, a British author of the 1700s, wrote of credit associations, “that it takes 240 poor men’s pence to make one capitalist’s sovereign. But once the sovereign is so put together, it is a totally different sovereign from that taken out of the rich man’s purse. It has behind it 240 wills, 240 pairs of watchful eyes, 240 thinking brains. It has, so to speak, become an animate sovereign, with prudence, energy, vigilance, diffused throughout all its parts. Every spring, every wire of the composite machine takes a personal interest in the collective doings, watching the other parts, guarding against loss and waste, correcting the slightest irregularity.”

There are an extremely wide range of mechanisms by which such associations exist. Nor, as the long-haul cash transfer system reveals, is cooperation limited to credit transactions. Wire crafter-makers in South Africa often form labour cooperatives, and work on risk collectively, in order to secure or support large manufacturing contracts.<sup>13</sup>

Microfinance institutions, like the Grameen Bank in Bangladesh, have used this capacity for peer monitoring to reduce the cost of lending to the poor.<sup>14</sup> The risk of default is transferred from the bank to the credit association. The group itself ensures repayment from its members in order to secure future loans.

Lending to groups is a kludge, though, that occurs because of a lack of proof of individual credibility. Lack of legally enforceable individual identity is what prevents banks from lending to individuals in the first place, and prevents individuals from securing their prosperity directly.

**What both defines and limits these associations is the ability of individual members to recognise and remember the credibility of each of the other members and their individual transactions. Individuals gain both proof of their identity and their transaction history from their network.**

There is a limit to how large a group is sustainable under peer monitoring. Research into both social networks and neocortex size implies that the maximum network size is about 150 individuals.<sup>15</sup> Overly large groups give rise to corruption or mismanagement of the funds.

This imposes constraints on individuals. Not only are their maximum lending opportunities limited by the size of their network, but they are also limited by geography.

**When impoverished individuals move in search of new opportunities, or as a result of conflict or climate disruption, they lose not only their homes and social support structures, but also their identity.**

### 3 Trust in internet-based identity and peer-to-peer transactions

Another world fraught with a lack of centralised governance and mechanisms for authenticating legal identities is the virtual world of the internet. Every moment, millions of people interact; debating, buying and selling, and making promises.

It is a world where a lack of definitive identity, and the ability to secure both individual and financial integrity, has expensive consequences.

#### 3.1 Securing digital identities

You may have invested a great deal into a Facebook profile but it will not permit you to open a bank account or cross a border. Neither do you own it.

A digital identity is the data that uniquely describes a person, or a thing, and contains information about that subject's relationships.<sup>16</sup>

That there is, as yet, no universal mechanism for managing digital identity is obvious to anyone who has to sign in to multiple web services and juggle multiple passwords and accounts. People also find that their identities do not belong to them but to the platforms they use. All the data associated with that identity are entirely outside of that individual's control.

Some efforts have been made to create a more reliable identity authentication system. The OpenID 2.0 platform for user-centric identity management, the most popular approach, is a light-weight authentication protocol which others can adopt.<sup>17</sup>

This collection of protocols and approaches is known as Identity 2.0 and has not yet solved many of the concerns related to digital identity, especially the ownership of identity-based information by the individual herself. It is also not linked to any legal identity.

The framework for the next version of digital identity, Identity 3.0, is starting to be agreed.

“Key to the trust in this whole identity ecosystem is being able to immutably (enduringly and changelessly) link an entity to a digital Core Identifier, so that we can place full trust in knowing that only the person (or other type of entity) holding that Core Identifier can be the person (or other type of entity) it was created from, and no-one or thing can impersonate it. This immutable binding must be created in a form that guarantees the binding and include the interfaces necessary to connect with the digital world. It should also be easy and cost-effective for all to use,” say Jim Hietala and Ian Dobson of the Open Group.<sup>18</sup>

**Many of the challenges for authentication may be solved by an authoritative third-party able to authenticate all users. However, individuals on the internet do not come from one country and so a single impartial and globally trusted intermediary is improbable. Nor is it desirable as it presents a single point of failure.**

### 3.2 Securing transaction integrity in the absence of trusted third-parties

Third-party intermediaries can verify the bona fides of the participants but at the expense of confidentiality of the transaction, and additional fees.

Trusted intermediaries' credentials also, unfortunately, are not beyond reproach. Their financial and credit card systems are routinely compromised and have cost consumers and companies billions of dollars both directly and indirectly.<sup>19</sup> During 2014, the US experienced credit and debit card breaches at Home Depot, Target, Sally Beauty, PF Chang's and a host of other major retailers and exposing millions of people to account fraud and identity theft.<sup>20</sup>

“What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers.” wrote an individual or group known as Satoshi Nakamoto, in October 2008.<sup>21</sup>

Nakamoto developed the bitcoin cryptocurrency software to implement his theory. By September 2014, \$24.5 billion of transactions had been traded in bitcoin.<sup>22</sup>

The ‘impractical computations’ used to demonstrate proof are derived from hashing, a complex mathematical process which generates a digital fingerprint from arbitrary data. Cryptographic hashes are considered practically impossible to reverse<sup>23</sup> and production of a hash can be used as proof-of-work that a specific hashing function has been used.

A block is a list of signed transactions between different identities. Once the integrity of the block is agreed by all in the network then the block is approved and added onto the end of the chain of previously approved blocks, forming a blockchain of publicly-accessible transactions.<sup>24</sup>

As described by Nakamoto, “The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work.”

Individual identities remain anonymous via public-key cryptography, although the public-keys involved in each transaction are public permitting a high degree of transparency and inspection of the information stored in each transaction.<sup>25</sup>

**The irreversible and public nature of the blockchain provides persistent and irrefutable proof of the occurrence and details of individual transactions occurring between one or more entities.**

While Bitcoin itself has proven controversial, largely as a result of its anonymous use in illegal transactions<sup>26</sup>, the underlying blockchain technology removes the requirement for a trusted third-party.

Contributors to the blockchain must expend computing power, at real financial cost, in order to prove that they have authenticated transactions. Anyone attempting to impose

fraudulent transactions on the network needs to provide computational power that exceeds the rest of the network combined. This is extremely expensive and, therefore, highly unlikely.

To put this in perspective, in November 2013 the total computing power available for bitcoin proof-of-work was 64 exaFLOPS (floating-point calculations per second) while the total available combined power from the world's top 500 supercomputers was only 0.25 exaFLOPS. A year later, the processing power of the network had grown twenty-fold.<sup>27</sup>

In late 2013, Vitalik Buterin, one of the founders of Bitcoin Magazine, released a paper about an extended approach to the blockchain called Ethereum.

“The intent of Ethereum is to ... allow developers to create arbitrary consensus-based applications... Ethereum does this by building what is essentially the ultimate abstract foundational layer: a blockchain with a built-in Turing-complete programming language, allowing anyone to write smart contracts and decentralized applications where they can create their own arbitrary rules for ownership, transaction formats and state transition functions.”<sup>28</sup>

The blockchain has matured far beyond being a record of financial exchanges.

**Anyone can place a proof of individual identity inside the blockchain and create an irreversible record of that transaction. Similarly, any transaction – from medical history to an asset register – can be recorded without agreement other than from the parties concerned.**

**The aggregated computing power of the network ensures that such transactions are secure and available as proof anywhere they are needed.**

#### **4 Digital currency and identity use by the poor**

The worlds of high-tech network-based security and the lives of the world's “bottom billion” are not that far apart.

**A range of sophisticated digital services have experienced widespread adoption by the poor despite the abstract nature of virtual currency transactions and phone-based identity.**

M-PESA is a mobile phone-based mechanism for sending and storing money. It is offered by Safaricom, Kenya's largest mobile service provider, and there are versions of this service across Africa, India and Eastern Europe. Since March 2007, 11.6 million Kenyans have signed up for the service and undertaking transactions worth over \$1 billion a month.<sup>29</sup> This is equivalent to about a third of Kenya's GDP of \$37 billion a year being processed via the SMS-based system.

Illiteracy has not been a barrier, nor has the esoteric nature of a virtual private currency. The greatest barrier has often been banking regulations which have kept M-PESA out of specific markets. Advantages spurring adoption include the significant reduction in

transaction costs and time for migrants to send money home, as well as for the unbanked to use the system as an informal place to save money.<sup>30</sup>

In 2013, there were over 500 million active SIM connections in Africa (out of a continental population of 1.1 billion), with 6% of Sub-Saharan Africa's GDP derived from mobile phones.<sup>31</sup>

**Across the world's poorest regions, individuals are more likely to have a mobile phone than a formal legal identity. They are also far more likely to use their mobile phone as a means of financial exchange than to have a bank account.**

A similar positive response to biometric identities was revealed as India adopted the ambitious target of offering its 1.2 billion citizens the opportunity to gain a unique legal identity with their Aadhaar Project. The project itself is controversial<sup>32</sup>, but the technology offers a repeatable, low-cost, system for giving a biometric and unique identity to anyone in any part of the world.

India licensed the work of enrolling individuals to more than 35 agents drawn from India's booming technology industry. The agents bid against each other and win more work based on past performance as well as price.<sup>33</sup> As of September 2014, India has registered almost 700 million Aadhaars. The biometric nature of the enrolment process ensures that these are genuine and unique identities rather than accidentally enrolling the same people multiple times.

The budget for the program (from January 2009 to September 2013) was \$570 million, at a cost of about \$1.15 per person per registration.<sup>34</sup>

Amongst the objectives for the Aadhaar are to link identities to bank accounts, as well as to access subsidies for cooking gas and housing support.

For both M-PESA and Aadhaar, technical and financial literacy has not been a barrier to access or prevented adoption.

With the success of these initiatives, the question arises: can programs like Aadhaar be scaled up to work in other countries?<sup>35</sup>

Estonia hasn't waited. Their existing biometric digital identity system – used for healthcare, banking, signing contracts and for public transport – is to be extended to identify non-resident 'satellite' Estonians.

As The Economist describes it, "Only a minimum of private data are kept on the ID card itself. Lost cards can simply be cancelled. And in over a decade, no security breaches have been reported. Also issued are two PIN codes, one for authentication (proving who the holder is) and one for authorisation (signing documents or making payments). Asked to authenticate a user, the service concerned queries a central database to check that the card and relevant code match. It also asks for only the minimum information needed: to check a customer's age, for example, it does not ask, 'How old is this person?' but merely, 'Is this person over 18?'"<sup>36</sup>



The technology exists, but the greatest barrier and potential danger for the poor is that the value in their identities is carved up by private companies and their own governments. Nigeria, for example, has recently formed a relationship with MasterCard to offer citizens a digital biometric identity card.<sup>37</sup>

This imposes long-term costs on individuals since a single company has been granted a monopoly on transactions in their identities. Nor can it be guaranteed that their transactions will remain anonymous. Consider the implications when such identities are used for electronic voting.

## **5 Crypto identity is a viable mechanism for legal empowerment of the poor**

At the beginning of this paper I posed three conditions which must be satisfied in order to offer crypto identities authenticated by a network as an alternative to a single trusted intermediary. Taking each of these in turn:

### **5.1 Technology exists and is both sufficiently mature and cost-effective to offer digital identities**

India has proven that biometric registration can be done at scale with some of the poorest people in the world. Estonia has demonstrated how digital identities can be used in a wide variety of applications. Biometric enrolment ensures the uniqueness of each person and that no-one receives multiple identities accidentally.

India has been able to issue digital identities to over 500 million people at a cost of \$570 million, with the remaining people to be enrolled during 2014 and early 2015.

Enrolling the 4 billion people without identities can be done and it can be estimated that it would cost about \$4.5 billion.

### **5.2 Authentication by trusted intermediaries can be replaced by a distributed network**

A peer-to-peer network, using a cryptographic blockchain can be used to provide secure and irreversible transaction records which serve to verify digital identities. This means that digital identities can be offered which are not explicitly tied to a company or organisation.

Governments fearing that the network is biased can simply contribute processing power of their own. While this may reduce antagonism from governments whose citizens will benefit, state support is not required for such identities to be successful or useful.

### **5.3 Literacy and poverty are not barriers to adopting virtual currencies and identities**

The poorest people in Africa and India are already using secure digital mechanisms to exchange virtual money and pay for goods. Mobile phone, and SMS-based financial, adoption is in the hundreds of millions of unique users.

Proof of identity enables individuals to scale their existing village-level credit and contract associations to an equivalent global digital transaction registry. That proof will be available anywhere. Clear identities will also permit individuals to access aid services directly. All of these promote adoption and use.

**It can, therefore, be seen that the three conditions have been met. What is needed next is financial support from aid agencies to pay for implementation.**

## **6 Proposing a global biometric identity enrolment program based on distributed cryptographic methods**

The eradication of smallpox happened as a result of the concerted effort of the World Health Organisation. Many of the countries where the disease was endemic were unable to halt the virus on their own or were indifferent to doing so. Individuals signed up because of the immediate benefit of vaccination.

A similar coordinated effort by aid agencies can enrol every vulnerable person into a global biometric digital identity program based on cryptographic methods even in the absence of local government support.

**Funders should work with leading cryptographic experts to develop an open source and open standards biometric registration device and protocol to link the lessons learned from India's Aadhaar project to the Ethereum blockchain (or suitable equivalent).**

**These devices can be used by aid-agencies or private firms to enrol the beneficiaries of development agencies during the course of their work. Such identities can be managed by individuals to access aid from support agencies, as well as for agreeing contracts or in other applications where a unique proof of identity is required. These immediate benefits will also spur enrolment and adoption.**

The means of providing an individual with an identity does not depend on the benevolence or existence of a functioning state, and that identity can immediately be used by the individual to benefit from legal access and opportunity.

## **7 Cryptographic identities promote transparency, open data and research**

While all participants to transactions in a blockchain are anonymous, the transactions themselves are all public.

Aid agencies can, therefore, track the aid they have spent and assess the impact of that aid by studying the transaction record. This will also permit agencies to assess different approaches through meta-analytic studies.

**Digital identities are not limited only to individuals. Aid agencies can similarly create and use crypto identities. If aid agencies then publically acknowledge their**

**public keys their activities can be tracked. In this way they can be held to account and the nature of their activities monitored.**

Having a public transaction record – even where the individuals remain anonymous – permits analysis of the volume, frequency and value of interactions, as well as (where this is specified from known identities) the geographic location of such services.

There are numerous benefits to providing individuals with crypto identities that support any type of digital transaction:

- Individuals can maintain their personal credit record based on their interactions with credit associations and so take their good rating with them should they need to move;
- Bank accounts belong to the individual and can be used to store money outside of the formal banking system, as well as making migration between service providers easier;
- No individual can be deprived of their identity, or the reputation they have earned through various transactions, by any government or organisation;
- Additional services, like medical records and asset registers, can be explicitly (and confidentially) tied to their identities;
- Emergency aid can be distributed directly to individuals so as to ensure they can address their needs specifically instead of relying on the access of aid agencies;
- Refugees can be processed and tracked and reunited with family members much more readily;

By no means is this an exhaustive list and new applications will emerge once such identities are widespread.

Researchers, too, will benefit from having a real-time and public transaction record of aid interventions. Meta-analysis can provide insight into common economic concerns, or mechanisms by which one community overcomes adversity which can then be shared with others.

## **8 Securing individual sovereignty through legal identity**

Legal exclusion of the universal right to identity does not require the deliberate brutality of a nation like North Korea. Inefficiency and neglect are as effective.

An anecdote told to me by the narrator a few years ago: the narrator was queueing to renew her South African passport. Ahead of her was an elderly Xhosa man who was illiterate. He had lost his identity book and needed a replacement otherwise he could not receive his state pension. He was unable to fill in the forms and was being subjected to brutal verbal abuse by the government representative behind the counter.

The narrator left her place and helped him fill in the forms and then returned him to the front. She demanded that he receive attention and ensured his forms were correctly submitted.

The man found the experience humiliating and embarrassing. Such matters are a normal occurrence in the registration office. That narrator had no idea if he ever received his identity documents.

It is shameful that anyone should be so humiliated. It is shameful that a person should be unable to prove their very existence. It is shameful that a person should be denied the opportunity to better themselves because of a lack of documentation.

We have the means to generate secure digital identities and authenticate these via a distributed information technology network, based on cryptographic proof instead of relying on the existence or benevolence of a functioning state or any single point of failure.

We can do this while promoting individual autonomy and the sovereignty that comes with ownership of ones' own identity.

Let there be no more Bongekile Lucia Mkhizes.

Let us give people the means to own proof of their own existence.

## 9 References

- <sup>1</sup> Gerretsen, B. "ID book delay drives woman to suicide", IOL News, 20 June 2007, <http://www.iol.co.za/news/south-africa/id-book-delay-drives-woman-to-suicide-1.358419>
- <sup>2</sup> Commission on the Legal Empowerment of the Poor and United Nations Development Programme. "Making the Law Work for Everyone Volume 1", 2008; [http://www.unrol.org/files/Making\\_the\\_Law\\_Work\\_for\\_Everyone.pdf](http://www.unrol.org/files/Making_the_Law_Work_for_Everyone.pdf)
- <sup>3</sup> Universal Declaration of Human Rights - <http://www.un.org/en/documents/udhr/>
- <sup>4</sup> Harbitz, M and dell Carmen Tamargo, M. "The Significance of Legal Identity in Situations of Poverty and Social Exclusion", Inter-American Development Bank, November 2009, <http://publications.iadb.org/handle/11319/5456>
- <sup>5</sup> Commission on Legal Empowerment of the Poor. "Making the Law Work for Everyone: Working Group Reports. Vol. 2", LEP, 2008.
- <sup>6</sup> Stephens, M. "The Commission on Legal Empowerment of the Poor: An Opportunity Missed", Hague Journal on the Rule of Law, March 2009
- <sup>7</sup> Banik, D. "Legal Empowerment as a Conceptual and Operational Tool in Poverty Eradication", Hague Journal on the Rule of Law, March 2009
- <sup>8</sup> Mashiri, G. and Chait, G. "Zimbabwe Informal Sector under Hyperinflation", 2007
- <sup>9</sup> Wikipedia, "Rotating savings and credit association", accessed 8 September 2014, [http://en.wikipedia.org/wiki/Rotating\\_savings\\_and\\_credit\\_association](http://en.wikipedia.org/wiki/Rotating_savings_and_credit_association)
- <sup>10</sup> Conning, J and Udry, C. "Rural Financial Markets in Developing Countries", Yale University, Economic Growth Centre, June 2005, [http://www.econ.yale.edu/growth\\_pdf/cdp914.pdf](http://www.econ.yale.edu/growth_pdf/cdp914.pdf)
- <sup>11</sup> Huppi, M and Feder, G, "The role of groups and credit cooperatives in rural lending", The World Bank Research Observer, July 1990
- <sup>12</sup> Ramuelo, M. and Chait, G. "Report on the findings of Burial Society's, Stokvels and Informal Trading Businesses", January 2008
- <sup>13</sup> Chait, G. "Making and organising decisions", Cape Craft and Design Institute, August 2009
- <sup>14</sup> Stiglitz, J. "Peer monitoring and credit markets", The World Bank Economic Review, 1990, <http://www.jstor.org/stable/3989881>
- <sup>15</sup> Hill, RA and Dunbar RIM. "Social network size in humans", Human Nature, 2003
- <sup>16</sup> Windley, P. J. "Digital Identity", O'Reilly Media, 2005
- <sup>17</sup> Recordon, D, and Drummond R. "OpenID 2.0: a platform for user-centric identity management." Proceedings of the second ACM workshop on Digital identity management. ACM, 2006.
- <sup>18</sup> Hietala, J and Dobson, I. "Challenges to Building a Global Identity Ecosystem", Open Group, 14 August 2012, accessed 10 September 2014, <http://blog.opengroup.org/2012/08/14/challenges-to-building-a-global-identity-ecosystem/>
- <sup>19</sup> Anderson, R., Barton, C., et al. "Measuring the cost of cybercrime", In The Economics of Information Security and Privacy (pp. 265-300). Springer Berlin Heidelberg., 2013
- <sup>20</sup> Krebs, B. "Data: Nearly All U.S. Home Depot Stores Hit", KrebsOnSecurity, 3 September 2014, accessed 10 September 2014, <http://krebsonsecurity.com/2014/09/data-nearly-all-u-s-home-depot-stores-hit/>
- <sup>21</sup> Nakamoto, S. "Bitcoin: A Peer-to-Peer Electronic Cash System". bitcoin.org. October 2008.
- <sup>22</sup> <https://blockchain.info/wallet>
- <sup>23</sup> Wikipedia, "Cryptographic hash function", accessed 10 September 2014, [http://en.wikipedia.org/wiki/Cryptographic\\_hash\\_function](http://en.wikipedia.org/wiki/Cryptographic_hash_function)
- <sup>24</sup> Grigorik, I. "Minimum Viable Block Chain" 5 May 2014, accessed 8 September 2014 <https://www.igvita.com/2014/05/05/minimum-viable-block-chain/>
- <sup>25</sup> Ron, D., and Adi S. "Quantitative analysis of the full bitcoin transaction graph." Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013.
- <sup>26</sup> Christopher, C.M. "Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Laundering." Lewis & Clark Law Review, 2013
- <sup>27</sup> <https://blockchain.info/charts/hash-rate>
- <sup>28</sup> Buterin, V. "A next generation smart contract and decentralized application platform", Ethereum White Paper, 23 January 2014
- <sup>29</sup> Safaricom Financial Year 2014 Annual Report, 5 November 2013, [http://www.safaricom.co.ke/images/Downloads/Resources\\_Downloads/Half\\_Year\\_2013-2014\\_Results\\_Presentation.pdf](http://www.safaricom.co.ke/images/Downloads/Resources_Downloads/Half_Year_2013-2014_Results_Presentation.pdf)
- <sup>30</sup> Morawczynski, O and Pickens, M. "Poor People Using Mobile Financial Services: Observations on Customer Usage and Impact from M-PESA", CGAP, August 2009.

<sup>31</sup> GSM Mobile for Development, “Sub-Saharan Africa Mobile Economy 2013”, 2013

<sup>32</sup> Dalal, P. “Aadhaar In Its Present Form Has No Welfare Elements Attached To It Whatsoever But Is An E-Surveillance Project”, Privacy Laws In India And Privacy Rules And Regulations In India. 3 August 2014, accessed 9 September 2014. <http://www.electroniccourts.in/privacylawsindia/?p=122>

<sup>33</sup> Chen, G. “India’s Unique ID Could Generate Big Boost in Financial Access”, CGAP, 30 January 2014, accessed 9 September 2014, <http://www.cgap.org/blog/indias-unique-id-could-be-about-generate-big-boost-access>

<sup>34</sup> Unique Identification Authority of India. “Expenditure of UIDAI for the year 2009-2010, 2010-2011, 2011-2012, 2012-2013 and 2013-2014 (Up to September 2013)” [http://uidai.gov.in/images/web\\_exp\\_sep2013.pdf](http://uidai.gov.in/images/web_exp_sep2013.pdf)

<sup>35</sup> Medley, L.C. “How India’s Unique ID System is Changing Lives”, World Bank Blog, 30 April 2013, accessed 8 September 2014, <http://blogs.worldbank.org/voices/how-indias-unique-id-system-changing-lives>

<sup>36</sup> “Estonia takes the plunge”, The Economist, 28 June 2014, <http://www.economist.com/news/international/21605923-national-identity-scheme-goes-global-estonia-takes-plunge>

<sup>37</sup> Guess, M. “MasterCard-backed biometric ID system launched in Nigeria”, Ars Technica, 3 September 2014, accessed 9 September 2014, <http://arstechnica.com/business/2014/09/mastercard-backed-biometric-id-system-launched-in-nigeria/>