IDENTITY
CYCLE

IAN GRIGG

Table of Contents

Cover by André Bonello, production by Rhian Lewis

3

Introduction

> "Το θαύμα της ιατρικής είναι η παράταση της ποιοτικής επιβίωσης των ηλικιωμένων πολλοί από τους οποίους είναι μανάδες και πατεράδες μας, γιαγιάδες και παππούδες. Τιμούμε όλους και σεβόμαστε όλους αλλά κατεξοχήν αυτούς. Δεν μπορούμε να υπάρχουμε ή να έχουμε ταυτότητα χωρίς αυτούς.
> (*Σωτήρης Τσιόδρας*)
>
> The miracle of medicine is the prolonged quality of life of the elderly, many of whom are our mothers and fathers, grandmothers and grandparents. We honor everyone and respect everyone but them above all. We cannot exist nor have identity without them.
> *(Sotiris Tsiodras, Greek Health Lead, 21 March 2020)*

In the beginning, we were a tribe. It would be fair to say that the tribe, or the community as we'd call it these days, is humanity's first institution, first everlasting societal construct. But it would be wrong to claim credit, as tribes and packs predate us mere humanity: many animals work together in groups.

From this humble gift as thoughtful humans in tiny tribes, we yearned to better ourselves. Within the protective and encouraging cocoon of our tribes, we added much more - language, agriculture, writing, technology, trade, rules, money, wars, art, corruption and more.

Each of these changes our lives, for good and bad. Humans respond to change, and in doing so we reveal more about ourselves.

Fast forward through the ages to the middle of the 19th century, in a time of big states, big business, big wars, a new phenomenon emerged to explain and regulate society - Identity by means of numbers and documents issued by the state. But this new tradition, only a century old, met its match at the end of the 20th Century: the Internet! Oddly, unlike most other innovations, the efforts to build flexible large scale identity systems into the digital domain have more or less flopped. More, in that they did not seem to protect and serve people, and less in that they have done something, even as their original promises were discarded.

Why is that? Critics like myself have been able to point out why something failed but have not pointed to something better, which makes it easy for not only the majority to ignore us, but also for new aspirants to repeat the mistakes of the past.

Corruption

Until now. Among those many human inventions, one provided the key to open this book: Corruption, it turns out, triggers a response that tells us a huge amount about ourselves. In 2011-2013 I spent time in Kenya, a developing country that was better known as the birthplace of mPesa, an independent non-banking mobile money system. But more important to me was the dramatically increased levels of corruption; I was fortunate enough to be told, to observe and to appreciate what corruption does to people, and how they respond. This experience brought to life two tremendously important outcomes.

The first outcome was in finance: As we know, a high level of corruption in society causes a general failure of institutions - banking, government, military, etc. But life still goes on. In a society impacted by high levels of corruption, and in which people still retain some choice, the people fight for a better life. A key barrier to a better life is simple finance - people face the burden that savings in a corrupt society are unsustainable, as they are stolen, seized, diverted.

One innovation designed to create a future in a place that defies financial stability is found around the world - the social savings group. In Kenya, they call it a *chama* which is simply the Swahili word for 'group'. This small group of typically women comes together on a regular basis to save. As the corruption they face is strong, the group relies heavily on local trust, tradition, and privacy to achieve their aims.

It works. The fact is, and the numbers show it, that Kenyan chamas deliver stable finances in the face of heavy corruption, and they are the very foundation of the nation's economy in the most positive sense. Chamas are an open secret, they are out there in the open, but the context is obscure, the western bias is heavy, and if you do not look, you do not see.

The second tremendously important outcome is the topic of this book - Identity. Because of the strength needed for a small group of women to create their own savings, the chama is also a bastion of trust and identity. The savings group, which is a widespread phenomena across the developing world, forms a basis on which to build a new digital approach to identity that can be usefully deployed in service of its members.

This book is my attempt to lay out why Identity with chamas works. It should be obvious, but it is not. To figure out why it wasn't obvious, I had to add another several years of thinking to the 2 decades I'd already done in the field, by constructing tentative links from our western notions of identity to the social savings group and back again, over and over, until I'd built a bridge.

Identity is an outcome of Community

The chama (which is how I will term it from now on, although there are many other names around the world) is a small community based on existing local trust and a strong need to save. A typical chama is a group of women running a market place; at the end of the day they come together to sort out their day's takings, pay off their loans, pool the results, and make new loans for tomorrow's working capital.

Of course all their takings could be stolen by an endless list of attackers, corruption coming in many and diverse forms. By placing their takings into their chama it is now defended by the group as a whole. No longer is one member on her own; a theft from one is a theft from them all, and the thief must now deal with a tribe of angry women.

Likewise, insider attacks are dealt with by the process of careful selection of members and consistent meetings. Every member has skin in the game; for every member the success of the chama is not only an aspiration, it's their very life savings.

It is out of this process that we find that not only are these women in charge of their savings, their destiny and their economy, there is unstated power in their belongership. As they trust each other in savings, they trust each other in life. And when you trust your peers in life, you share your identity with them, because they are trusted to protect you.

In reverse, the fact that a person is a member of a certain chama can be a very strong statement of identity. It is stronger than say an identity card or a bank account or an employment contract, because those statements are of compliance not trust. Potentially, it can be even stronger than a family connection, an educational degree, or a professional resume or curriculum vitae.

In contrast, on the Internet, gurus often talk about "solutions" to the problem of Identity. PKI certificates, which failed to roll out; scans of ID cards, which are easy to spoof or buy; smart cards which require everyone to have a reader; mobile phones which require trust in the vendors; and finally reputation, which is numerology - a futile attempt to turn some person's entire life into a single number. For much of China, the social credit score is being utilised for reasons good and bad, but it's still just a number. The USA inspired credit score is much the same - what can we say about someone who is 200 versus another who is 220? Has humanity really strived for 10,000 years of recorded history to reduce each of us to a number?

This notion of belongership brings a powerful alternative to a numbers-obsessed world: *"I am a member of my chama"* is a much more powerful statement because it brings in all the richness of the chama, to which we know the member belongs because it makes her life better. My fellow members and I have skin in a joint game; they guard me, as I guard them. We are bound in a common enterprise, a consensual goal for an aspirational and financially beneficial future.

You can't put that into a number - but you can put that into a simple statement, *"I am from the Dragon chapter of the Bitcoin Association."* My identity is established as being someone from a group with some tangibly real reputation.

And it turns out that not only is this a good thing, it is more closely aligned to the notion of useful identity than other known systems. As we conclude in Part I, your digitally useful identity is what people say of you, and what more powerful statement is there than your group saying you are one of us?

Identity is an outcome of community - which leaves us a much more refined goal in the search.

It may be that you are inspired by this message or equally that you are repelled; but likely the common ground is that for both of you, this proposal is not self-evident. To explain it we must walk a very long, tortured and controversial path. Firstly through Identity, in its depths and meanings, being Part I. Then on to Trust and how it is constructed and used to safely share your identity, Part II. As Trust derives from somewhere, we investigate the origins of Trust in Groups in Part III. Finally, in Part IV we discover the real world example - Chamas as financially enabled groups, and how they draw from Trust, Identity and Community.

(And, if Part V is ever written, we might describe how we construct a system that supports identity, within the limitations of human rights, liabilities and obligations, so that the individual can take her rightful and trustworthy place within her community.)

1

My Identity

Part I - My Identity - You, Me, Us, Them - Who Am I?

> Suddenly realising that he did not know who he was, Mulla Nasrudin rushed into the street, looking for someone who might recognise him. The crowds were thick, but he was in a strange town and he found no familiar face.
>
> Suddenly he found himself in a carpenter's shop.
>
> 'What can I do for you?' asked the craftsman, stepping forward. Nasrudin said nothing.
>
> 'Perhaps you would like something made from wood?
>
> 'First things first,' said the Mulla. 'Now, did you see me come into your shop?'
>
> 'Yes I did.'
>
> 'Good. Now, have you ever seen me in your life before?'
>
> 'Never in my life!'
>
> 'Then how do you know it is **me**?'
>
> *(Idries Shah, The Pleasantries of the Incredible Mulla Nasrudin)*

It is a truism of the Internet industry that in order to build a system of trusted trade, we need an identity component - one that tells us and everyone who you are. With that identity system, we can then construct a trust system, and then we can trade - online and at distance.

We Internet engineers have been following this dream for more decades than we dare to say - the first concept of digital identity surfaced in the mid 1980s plan by phone companies to put certificates in every household phone. Originally, identity on the Internet was assumed honestly until PGP raised the stakes. Soon followed by PKI, and a host of others.

None of the brave projects of Internet Identity worked.

I.1 Schools of Thought

In the face of decades of failure, I suggest that we need to radically depart from the engineering perspective. Instead of asking HOW to build this, I propose that we look into the abyss of identity, and ask first WHAT and and then WHY (Joe Andrieu, "A Primer on Functional Identity").

What is Identity? Let's start by surveying the various and many schools of thought (Ian Grigg, "Identity" 2015), and from that base, maybe we can construct a useful theory to meet the goal: Who am I? Who are you? Why does it matter? In later sections we do the WHY, and finally end up with the HOW.

Who are we? Let's start with the State.

Type 1: The State has Your Number

> Article 7 (Registration, name, nationality, care): All children have the right to a legally registered name, officially recognised by the government. Children have the right to a nationality (to belong to a country). Children also have the right to know and, as far as possible, to be cared for by their parents.
>
> Article 8 (Preservation of identity): Children have the right to an identity – an official record of who they are. Governments should respect children's right to a name, a nationality and family ties.
>
> (*UN Convention on the Rights of the Child*)

The state-led school of thought, as suggested in the UN's Convention above, says that you are the collection of your officially issued identity documents (hereafter, IDs), identity numbers, registered names and perhaps other numerical paraphernalia such as bank accounts, student IDs, etc.

This view - you are who the state says you are - will be an uncomfortable thought to many. But we have to accept this abyss and stare into it, if only because so much of modern western life pyramids off of it. The State is faced with an optimisation problem, and it would seem to the State that Identity would be far better off if it were Aristotelian:

> Aristotle also defined a set of basic axioms from which he derived the rest of his logical system:
>
> - An object is what it is (Law of Identity)
> - No statement can be both true and false (Law of Non-contradiction)
> - Every statement is either true or false (Law of the Excluded Middle)
>
> These axioms weren't meant to describe how people actually think (that would be the realm of psychology), but how an idealized, perfectly rational person ought to think. (*Chris Dixon, "How Aristotle Created the Computer"*)

The more organisations, the more bureaucrats, the more computers, the more supra-nationals that work in concert (conspiracy?) at planetary scale, the more the tendency is towards you having *The One True Identity*. In the State's view, you are one and only one object, you have one and only one number, one gender, and one dress with one colour. Any deviation from simple singular truth sets you up for a world of pain.

Read superficially, the UN's view of the child, above, seems a good thing. Read in depth, nothing could read more Orwellian. What the miscalled Rights of the Child establishes is the Right of the State to own and control each and every child by means of an official record of their existence, a name, a nationality and a graph of family.

The Lives of Others

> [Wiesler enters the elevator at his apartment building. A young boy with a ball joins him]
>
> Junge mit Ball (young boy with ball):
> Are you really with the Stasi?
> Hauptmann (Captain) Gerd Wiesler:
> Do you even know what the Stasi is?
> Junge mit Ball:
> Yes. They're bad men who put people in prison, says my dad.
> Hauptmann Gerd Wiesler:
> I see. What is the name of your...
> [pauses]
> Junge mit Ball:
> My what?
> Hauptmann Gerd Wiesler:
> [thinks for a few more seconds]
> Ball. What's the name of your ball?
> Junge mit Ball:
> You're funny. Balls don't have names.

(Figure 1 - Florian Henckel von Donnersmarck, The Lives of Others)

Imagine the nightmare that 'identity' generates in every refugee camp -- it gives every government the right to declare the *un-existence* of every un-identified person in the camp, thus giving them the "out" on refugee process. If you haven't got an "identity" from a state they recognise, which is by definition routine in many or most refugee situations, you don't exist. If you do have an "identity" they like, they can take it from you and you now exist at their pleasure. Either way, they take away your ability to travel, to work, to study while they "process your case." Which might take a year, a decade, a generation.

Refugees are an extreme, and we can be comfortable that it only happens to them, and not to us, the rich westerners, right?

The risk increases dramatically for those who identify in some fashion with more than one nation, or who get into trouble while travelling. An extreme example: the USA cancelled the passport of Edward Snowden, thus removing his personhood rights and stranding him at Moscow airport. Russia exerted its UN-endorsed rights to un-person Snowden by declining his right to travel for lack of passport, but eventually granted him residence as a political exile. Not quite as tortured a story as that of Mehran Karimi Nasseri (The Terminal), who was incarcerated in Charles de Gaulle airport terminal by France from 1988 to 2006. For the crime of ... travelling without documents issued by a country recognised by France, he suffered what was in effect a life sentence. In an airport terminal.

Every year, thousands of Americans attempt to hand in their US citizenship, and are subject to a process that can only be described as deliberate harassment - for their attempt to pursue life, liberty and freedom in a new state. Many governments around the world attack

dual citizenship; for no good reason, and a range of bad ones ranging from xenophobia to outright jealousy.

> "I understand that by voluntarily applying for a British passport, it may result in losing citizenship of another country."
> *(Declaration on application for British Passport)*

> "How do I lose German citizenship? - by voluntarily acquiring a foreign citizenship"
> *(FAQ on German Citizenship)*

Many nations also treat single citizenship as optional, not a right. President Erdogan of Turkey tried to send captured ISIS alleged terrorists back to their home countries:

> The reaction of a number of European countries, including Britain, has been to strip suspected terrorists of their citizenship, leaving them as stateless and thus unable to be repatriated to their country of origin.
> *(Zerohedge.com "These Gates Will Open")*

Note that the stripping of citizenship was apparently without a trial, a hearing, or due process.

So, yeah. It happens to us, but probably less dramatically than, say, half the population of Syria, or not as recently as WWII (Pamela Druckerham), being the last war in which the west had mass migration. Or, the developing world poor that are being slowly impressed into the UN-approved identity plan on the hope that they'll behave and *be formal*. It happens to rich western immigrants who want bank accounts, it happens to every millenial victim of the current secular depression that is camping in mom's basement and can't prove an address, to every phishing victim who's told their account is empty, to every student loans victim, to everyone who types the wrong memo into a bank transfer or has the wrong friends on social media, to everyone whose social security number is shared, to every one of the people named Lisa S Davis, or everyone who has a non-Aristotelian gender.

But, it doesn't happen to us. Identity abuse - the abuse of those with non-behaving identities - hasn't gone mainstream.

Yet. Give it time, watch China. Turkey. Russia. Or, India's living dead or those declared to have false Aadhaars (ID cards), or the two million Indians denied citizenship. Or the United Kingdom's one to three million unbanked (depending on who you ask). Or Constantin Reliu, who's told to his face in court that he's dead. Or how the war on cash is being waged in your country. As Brett Scott writes:

> So, good luck to you if you find yourself with only sporadic appearances in the official books of state, if you are a rural migrant without a recorded birthdate, identifiable parents, or an ID number. Sorry if you lack markers of stability, if you are a rogue

> traveller without permanent address, phone number or email. Apologies if you have no symbols of status, if you're an informal economy hustler with no assets and low, inconsistent income. Condolences if you have no official stamps of approval from gatekeeper bodies, like university certificates or records of employment at a formal company. Goodbye if you have a poor record of engagements with recognised institutions, like a criminal record or a record of missed payments.
> *(Brett Scott, The War on Cash)*

In sum - the state-led school is not about giving you an identity, it is entirely designed to expropriate your right to your self. This is not the article to rail about the State, but to make this one anti-hypothesis:

```
The State's view of Identity cannot by definition
contribute to a system designed to serve human beings.
```

To claw something of our selves back, we have to start at the beginning.
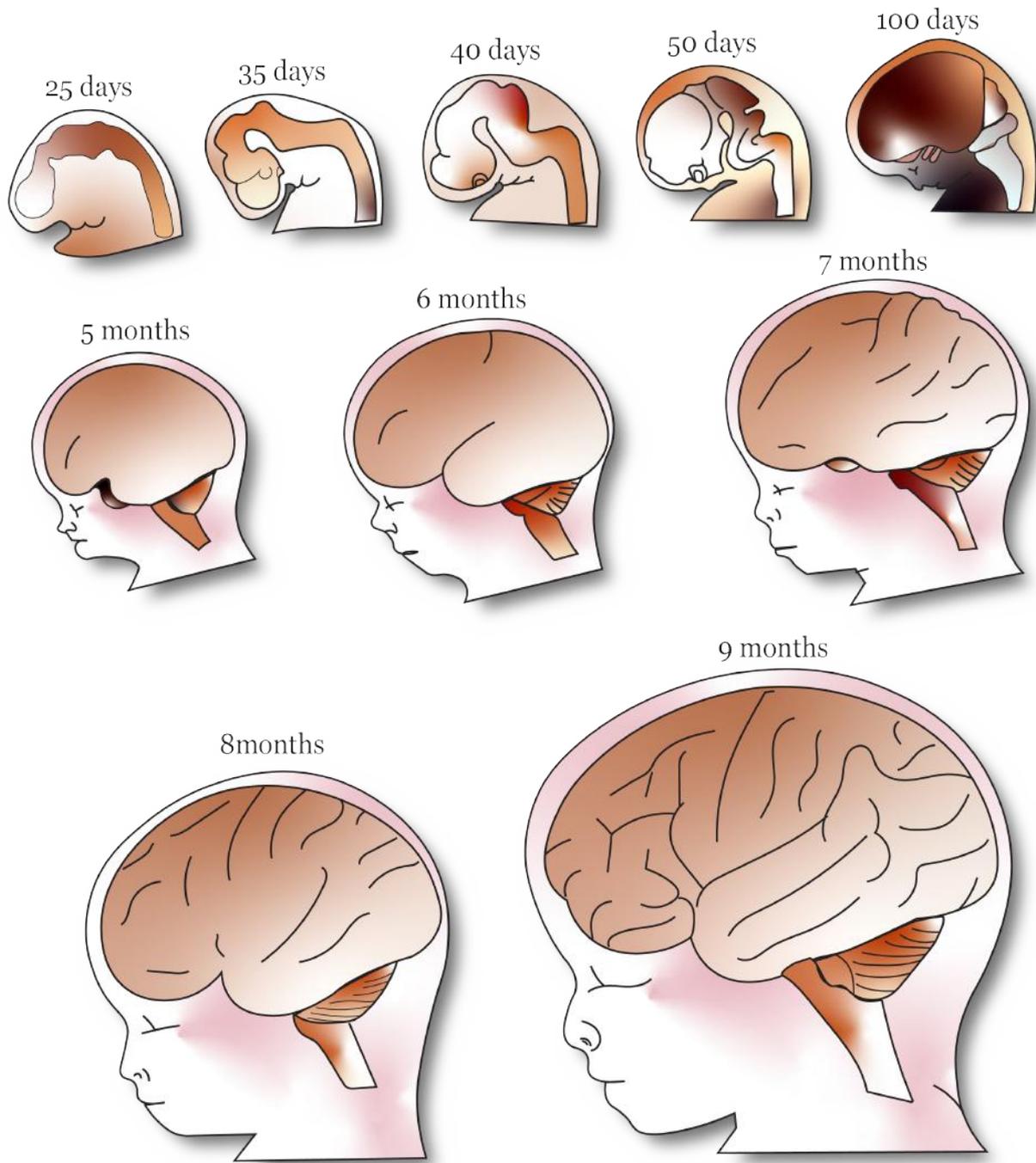
Figure 2 - Development of the embryonic brain

Type 2: Your Self *is* Yourself

> *"Who are you?"*
>
>   "No one of consequence."
>
> *"I must know."*
>
>   "Get used to disappointment."
> *(William Goldman, The Princess Bride)*

Psychologists have a completely different view of your identity. Their theory typically starts with birth, and let's assume for this discussion at least that the newborn baby does not have an identity at that moment.

> According to Ubuntu philosophy, which has its origins in ancient Africa, a newborn baby is not a person. People are born without 'ena', or selfhood, and instead must acquire it through interactions and experiences over time. So the 'self'/'other' distinction that's axiomatic in Western philosophy is much blurrier in Ubuntu thought.
> *(Abeba Birhane, "Descartes was wrong")*

The first thing that baby discovers is Mother. In a sort of pre-formative sense, Mother is self, because Mother is all that exists. If Mother is the only thing, then Mother is everything, nothing else is required, and no concepts of Identity are needed. Baby is Mother is self is happy.

Fairly soon on, assuming a prototypical family, baby discovers Father. While not as clearly useful as Mother, Father has the distinct impact of *not being Mother*. Being mysterious, but present, all the same. The simple singularity of self-as-Mother is broken, and Baby must find a new concept. In time, this process of triangulation leads baby to discover a new worldview, Mother-as-identity, distinct from Father-as-other-identity, finally leading to baby-as-self.

Who am I? I am me, because I'm not mommy *and* I'm not daddy.

As time goes on, baby integrates more complexity in the search for self: name, gender, hurts, words, age, calisthenics, tears, siblings, bruises, neighbours, locality, food, rituals, photos, birthdays, 🙂, 1st smartphone, 1st video, etc. Baby disappears and Alice, our child, appears, a vessel of blooming personality. All of these complexities are processed into the psychological concept of *self*, of her identity.

What stands out? No child, no Alice remembers any of this, and hates to be reminded of it by mother, or any cheek-pinching aunt. But, other than that, what really stands out is that, this concept of identity is totally disjoint with the state view of identity. As Christopher Allen

suggests, we cannot say Identity without saying I (Christopher Allen, The Path to Self-Sovereign Identity). We delve deeper into Alice's Upbringing in Part III.

I Own My Data

> Nasrudin walks into a bank and the teller says 'can you identify yourself?'
> He pulls out a pocket mirror and says yes, that's me.
> *(David Mercer, quoting an old Sufi joke about Nasrudin)*

Perhaps in response to the dichotomy outlined above in two dipoles of state-as-your-identifier and self-as-your-personality, another school of thought derives perhaps from the Western tradition of individualism. It goes like this.

I am sovereign, I own myself. It therefore stands to reason that data about myself is also of myself and is owned by myself. I lay claim to it, and further claim the right to control it.

To some extent this property rights view is reflected in privacy law such as the EU Data Protection Directive (DPD) which gives the individual the right to demand an accounting of data from a firm. To which the *right to be forgotten* has been added within the new version, the General Data Protection Regulation (GDPR).

Yet the tradition of copyright, art, and compilation do not clearly have it so - while you may assert that you own data about you, the law generally backs the compiler or creator of the data. A photograph of you is the property of the photographer - while you may have a right to not have a snap taken, once it is taken, you might not have any rights at all.

Much the same happens with company data. Once my company has collected some facts about you, you are pretty much powerless to do anything about it. The GDPR is said to be a better privacy law, but privacy laws assume that corporates are too stupid to hack it into the shape needed - for the corporate. It could be said that strong privacy laws such as the EU's GDPR are more facade than anything - they give the appearance of control, but they don't do much to stop egregious use.

This strong claim reveals a strong futility - *data just wants to be free* - that has led to frequent claims by governments and startups promising that you will have control over your data. While each might claim success on their websites, their aggregate record suggests abject failure. You may wish to be self-sovereign but what territory you've conquered seems limited to your own mind, which isn't much of an achievement as sovereigns go.

Type 3: In Your Corporated Identity

> Head-bone connects to the headphones
> Headphones connect to the iPhone
> IPhone connected to the internet
> Connected to the Google
> Connected to the government
> *(M.I.A., "The Message")*

A further school of identity is the modern corporate services experience, as experienced over the Internet. As states bungle at limited information, and we ourselves bungle at Huxleyan information overload and declare defeat to the corporation, an opportunity emerges: The Internet can fill that gap and provide us with the Self that we really deserve. Our mobile phone, or for us older folk, our computer can provide us access to social networks, services, shopping, friends, work, and assets; it can let us finally rule our busy lives, as well as our data.

Yet, there is a downside: our *mobo* or *compu* may gain such prominence over our access that it rules our lives, not the other way around.

In some sense, everything known about me is on the computer, on the network: all my secrets, my photos, my life. When I go out into the net, I am totally exposed to the benevolence of the corporations to protect that identity. If I lose my device, I'm screwed; if the corporations that control these platforms lock me out, I'm screwed. Alternatively, if they leak my secrets to a bunch of bot-wielding extortionists from a strange country, I'm screwed. If they hand them over to an overzealous prosecutor with a zest for political advancement, I'm screwed.

Identity Theft

> Are we crazy? / Living our lives through a lens
> Trapped in our white picket fence / Like ornaments
> So comfortable, we're living in a bubble, bubble
> So comfortable, we cannot see the trouble, trouble
> *(Katy Perry, "Chained to the Rhythm")*

Leading to that modern oxymoron, *identity theft*. When the corporations are hacked, their copy of the *me* collection, which they call my identity, is shared with crooks. To the corporations, it is convenient to claim that *my* identity has been stolen, rather than *their* data.

To me, identity theft makes no sense, indeed it is nonsense. Nobody can steal my identity - a fraudster can impersonate me, but they cannot steal the very me that is me. But in some sense that is not legally well defined, labelling the fraud that results from the corporate failure as identity theft shifts the burden from them to me. Identity theft is then yet another case of liability dumping - corporate gain, individualised losses.

Voluntary Selfyism

> Personality uploaded
> Transcript process continued
> Welcome to your new life
> *(Nero, "New Life")*

It's all voluntary, corporations will say! I can romantically hide myself on a desert island with no net, but I'd really rather be myself on a resort island with my iPad. I'd really rather connect to the free wifi and share selfies with my friends - selfies of me, the pool, the martini, the bikini. At some stage the voluntary deal that was once offered becomes a public service, with all the complications that brings in. At least in my mind, if not at law.

A modern social network is a collection of corporate data that interlinks me to everyone else and to everything I've done and everything I'm going to do; the notion that I enter voluntarily to get that connectivity fails if it is *my identity*. In the true sense of my Self, I'm at one with my network. If the corporation can provide me with my network, I'm theirs. If you like what I'm sharing with you here, click on my *Like* button. Please!?

> Your Smartphone Can Tell If You're Bored
>
> A group of researchers looked at how people used their
> phones to figure out when they were bored, then
> suggested they go read a BuzzFeed article.
> *(Rachel Metz, "Your smartphone can tell if you're bored")*

One thing we know from history about such services to the public is that they won't be negotiated with our best interests at heart. If you're not the customer, you're the product. Further, it is emerging that the law is more or less a powerless tool to protect us, and contracts or end-user licence agreements are no help because we can't negotiate them and we can't understand them (Adrienne LaFrance, "Not Even the People Who Write Algorithms Really Know How They Work").

We can therefore state with a fair degree of confidence that no In Corporated system is suitable as a basis for you, because you aren't in control of *their* you. The self-interested corporation that started out as a partner has no particularly good strategy nor track record nor incentive to remain your digital angel.

Type 4: My Self is in Your Head

> The best way to find yourself is to lose yourself in the service of others.
> *(Mahatma Gandhi)*

At some stage it must become apparent that the above stories about identity are as compelling as they are contradictory. All that data on Facebook, all those behaviours that your parent(s) taught, the way your significant other acts with you, the way the state belittles you with the simplest denial, there are clearly many faces to identity.

We could do without all that, right? But what can't we do without? We can't do without a sense of self, and we can't do without our friends.

> What would you think if I sang out of tune
> Would you stand up and walk out on me
> Lend me your ears and I'll sing you a song
> And I'll try not to sing out of key
> *(The Beatles, "With a little help from my friends")*

Of your identity, there are more clearly two of you: within you, and without you.

The yin and yang of identity might be thus expressed: there is my self within me, and there is that me outside, that me that all of you perceive of me, as we relate laterally, bilaterally or multilaterally. You, all of my you, might be a small number such as my family, my peers, my neighbours and work partners, a group captured by Dunbar's number of around 150 (R.I.M. Dunbar, "Neocortex size as a constraint on group size in primates").

Or, because I've expressed my identity more into your care and perception, you might be a large number. Conceivably but rarely, a very large number such as the sub-continent of India as led to independence by the Mahatma Gandhi; the churches of the Prophet Muhammad or of Jesus Christ; the fandom of Elvis Presley or the Beatles.

These bipoles of identity have surprising effects. For example, if unconfident, I might be led to be driven by *me-without*, if I am confident or self-actualised as Maslow would have it, my *self-within* drives. Or, depending on my personality it might be the reverse; failure in confidence leads to overdrive from within, complete confidence leads to happy surrender to without.

This is the topsy-turvy world where I am part of your identity, and you are part of mine.

> Ubuntu ungamntu ngabanye abantu
> (People are people through other people)
> *(Xhosa proverb - Michael Kimani)*

Then, if my identity is incomplete, there might be two distinct causes for this. My self-within needs growth as much as my me-without needs gardening. Indeed, any approach to identity needs to take this seriously - both components. We have a more varied task ahead of us than hitherto thought.

As the Kenyan-born philosopher John Mbiti put it in African Religions and Philosophy (1975): 'I am because we are, and since we are, therefore I am.' (Birhane, op cit)

Self-within wishes to be in control, to reach self-actualisation, to be that wholly comfortable person we admire in others. It is this aspect that fights against the loss of control from too much me-without. It is inside-me that is upset about invasion through self-without: of privacy loss, inability to control my life, being pushed around by others. It is self-within that wants control over the me-without in your heads, it is self-without that allows that control to be usurped by state, by institution, corporation and by the social network.

The Social Network

```
                    EDUARDO
            What'd you write?

    MARK goes back to the profile page. There's a new area to be
    filled in...

                    MARK
            "Relationship Status", "Interested In".
                (beat)
            This is what drives life at college. Are
            you having sex or aren't you. It's why
            people take certain classes, and sit
            where they sit, and do what they do, and
            at its, um, center, you know, that's what
            theFacebook is gonna be about. People are
            gonna log on because after all the cake
            and watermelon there's a chance they're
            actually gonna--

                    EDUARDO
            --get laid.

                    MARK
                (over)
            --meet a girl. Yes.
```

(Figure 3 - Aaron Sorkin, The Social Network *)*

Humankind, as Movie-Zuck suggests, is a social animal. Self-within is not enough. Equally we need to be me-without, we need the relationships, the sharings, the likes, attention, the reflected echoes of self that speak to our pride. It is not only the work, the boss, the purchase of today's food - it is the need for interaction, jests and jokes, smiles and admonitions. I am because I am part of something; you think and respond, therefore I am.

My brain lives not in a box, rather, I inhabit a body with 5 senses, which originally were evolved for survival but today are more and more used for interaction with you. With you, all of you, tuned to you all just as your senses are tuned to me and every one of the me's you can sense.

This is the domain of sociological dramaturgy - I am an actor on the stage and you are my audience, as you are the actor to us. Indeed, our early adult selves were only discovered when we finally hard-forked from our parents in our mid teens and took to the road performing to our enthusiastic fan club, the one we had chosen for our identity. My mature self demands to be joined with you many, altogether in our ongoing theatrical drama playing to you, to me.

After all the cake and watermelon, there's a chance you'll validate my sense of self and I'll return the favour, in our mutual, reflective and interactive play known as *Mi Gente* (Spanish, loosely "my people").

Self-Actualisation

Maslow's famous hierarchy of needs places the basics at the bottom (Abraham Maslow, "A Theory of Human Motivation"). Then, we turn to needs of community - Love, Belonging, Esteem - which we see now as the learning of one, then of three, then of many, of community.
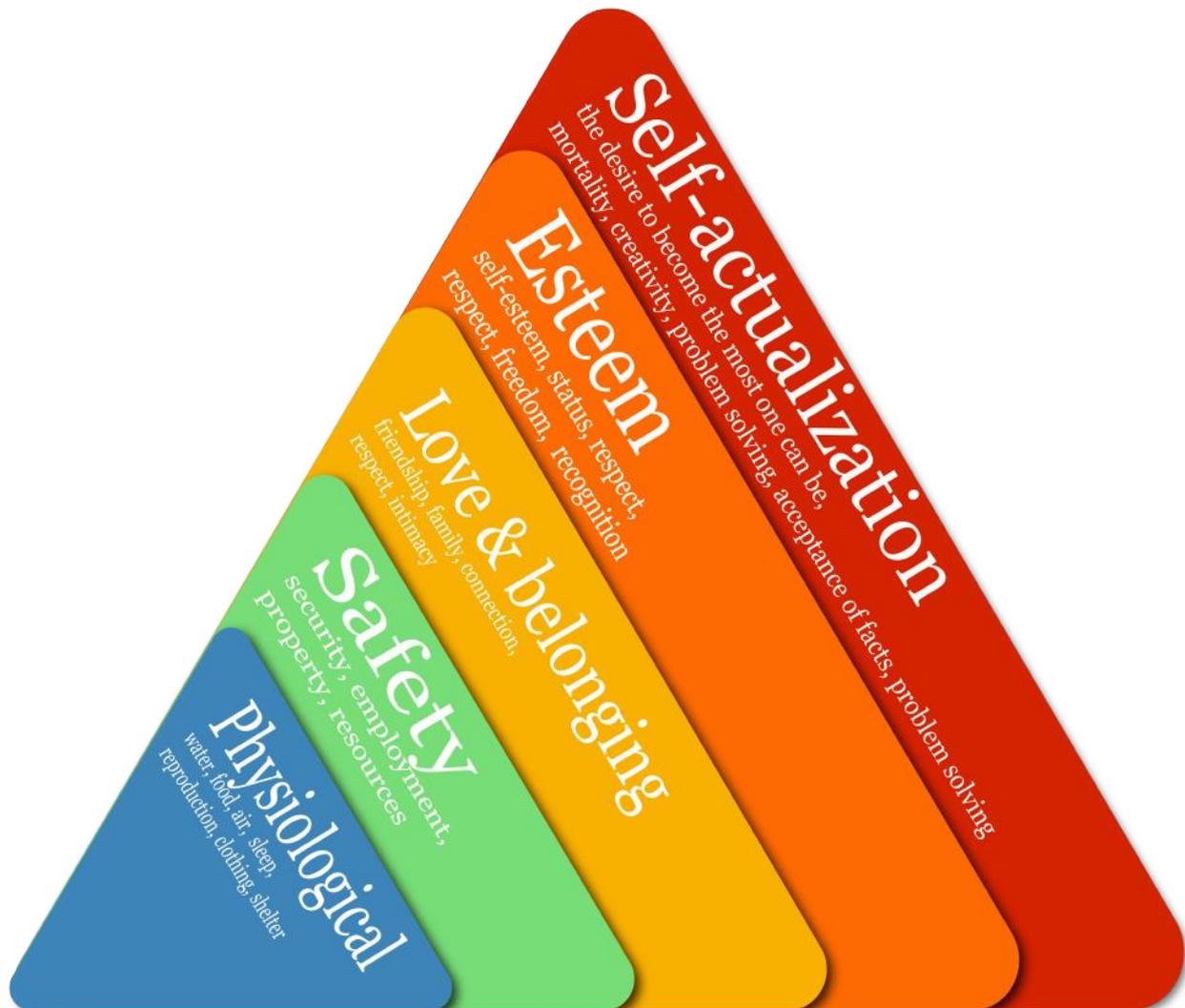
Figure 4 - Maslow's Hierarchy of Needs

Finally, when we are ourselves in our community, we can move upwards to that mysterious apogee of Maslowian enlightenment - self-actualisation.

We can therefore suggest that any approach to Identity must seriously integrate community. Not only must it integrate those that bring esteem, love and belonging to you, but also, it has to protect you from those that would reduce your self: the State which appropriates the right to strip you of your identity, and the corporation which productises you in exchange for the pretence at gratification. Facebook had it right, albeit in the beginning, before it joined the ranks of the corporations - relationship is what drives life.

I.2 A useful theory of Identity

The models, in a box

> All models are wrong, but some are useful.
>
> *(George Box)*

Let's summarise the theories, or models, and see what we can determine.

Source or School	Approach	Intent	Flaws	Reliable?
1. State	Numbers, Birth	Control	Medusa - too many to look at without turning to stone	✗
2. Psychology	Your Self	You modelling the world	Takes many decades to form. Can go off the rails, cf BPD.	?
2b. Property	I own my data	Controlling Privacy	Cannot control egregious behaviour, relies on handwavy application of uncertain theory of rights; Control of multiplicity of data is not scalable within the mind.	✗
3. Corporate	Provision of service	Selling you stuff	Oriented to selling to you, not to your service.	✗
4. Peers	You tell me	Love, Belonging, Esteem	I can't live with you, I can't live without you	?

Table 1 - 4 theories of Identity

What do we have then? Identity is of the self. You are who you think you are, hopefully. And you are who your local network thinks you are, in some dispersed sense. Let's look at the Manhattan story of the two women known as Lisa S Davis, born on the same day.

> She showed me all her driver's licenses, from New York and from down south, and her benefits cards and IDs.
>
> "Why do you keep all those?" I asked her.
>
> "It helps me kind of stay focused," she said, "to see where I came from. I don't have history. My mother died, there are no pictures of me when I was a baby. So there are little things I want to hold on to that I can show, like, I exist, I'm here, I'm here." She spoke in rapid-fire sentences, only pausing to laugh.
>
> I'd spent so many years thinking that she was some kind of identity thief. The more I

> listened to her story, the more I realized that, all this time, Lisa wasn't trying to steal my identity. She was trying to find her own.
> *(Lisa S Davis, "For 18 years, I thought she was stealing my identity. Until I found her")*

You might carry around some State IDs, but although you give greater or lesser credence to the State's view, you don't typically consider your Self to be in the ID. That ID is just an identifier, it's not even a poor proxy for your identity. It might work for the State, but progressively less so for others. You don't send your passport on a date, you go yourself. You might share a photo over facebook, but that's only because some of you can't be there. You might shop on Amazon, but you do not consider yourself a part of their Identity, even after you've accidentally signed up for Prime therapy.

If you are confused about identity at this point, then you're not alone.

The State's approach is all negative - you fear their sanction, and they know where you are. The corporation's approach is about selling you stuff - they'll happily amplify your happiness to sell you what you already had, and they'll as happily amplify your depression to sell you anti-depressants. Where Internet social networks have connected you with your peers, they've also boxed you into their model.

"I Hate You, Don't Leave Me"

> I spit out like a sewer hole
> Yet still receive your kiss
> How can I measure up to anyone now
> After such a love as this?
> *(The Who, "Who are you?")*

None of this is good for your identity, your inner Self. Many people face crises over identity; by some measures such as the DSM, disorders that center on identity such as Borderline Personality Disorder (BPD or commonly 'borderline') are the most common psychological trauma in high stress societies such as the USA (American Psychiatric Association, "Diagnostic and Statistical Manual of Mental Disorders"). Young adults complain "I don't know who I am" which is a rather difficult question, as their peers are struggling at some level with that same question, and their elders are divided amongst those who don't understand the question, those who never answered it, and those who don't know how they answered it.

Today, we can't answer who you are, not least from a paper or a book, although many websites will offer personality tests which prey on the unsure, the vulnerable.

But, with a nod to my original, probably forgotten goal of building a framework for trusted trade, we can ask:

```
is your identity a suitable foundation for that construction?
```

Evidently not. In the earlier 'theories', we can't even coherently describe what Identity is, having covered so many variants that only a politician could use them all in the same speech. And we haven't even looked at heroic identity of sports and pop stars, national identity in time of war or olympics, mathematical identity nor identity in language.

It is then no wonder that people - users, states, corporations and techies alike - tie themselves in knots when trying to build that abomination of modern IT: the identity system. Their starting position is akin to being on top of a loose iceberg, floating in the general direction of the warmer part of the globe. It feels good, it's getting warmer every day, but it's getting smaller, wetter and more slippery with each passing day.

Figure 5 - Who Am I?

Identity in Collision

What we can say is that there is a major gulf or collision between on the one hand, the state and corporate views of identity, and on the other hand, the individual and community sense of identity. These are not the same thing, they're very different! But, even being different, they are not independent, there is a very strong relationship between them. How can we reconcile these dependencies between schools even while recognising the collision?

Today, in most societies and philosophies, we place people above all other things. If there is a debate that needs resolving, we ask, what is best for the people? This simple question results in principles: The state serves the people, not the other way around. The corporation too is in theory subservient to the people, and there are many rules against capture, and occasional fines. To get technical, we can extend this observation to the nature of an identity system:

```
A system of identity must place the human before the system
```

A corollary to this is that a system that does not align with human individuality and community needs will be rejected - by the individuals and by the community. A further observation is that the state and the corporation aren't aligned to this ordering.

The state and corporation view of identity are against the human not for them.

The state and corporation models of identity therefore eliminate themselves from any list of human-centric systems: The state's model is expressly designed to identify unique persons and limit their services; the corporation's model is designed to box the person into a services or sales context, and to exploit their wealth and good nature. Either way, these systems place the interests of the system owner above the human.

Which leave the schools of self, and of our peer group. From the above, we described these two essential and useful but tentative poles of your identity, within yourself and also between you and the people you choose to share it with.

It's easy to narrow this down further: no matter how hard we try, your inner self is a bad basis for a technical system as (a) science fiction aside, we are not as yet capable of designing a system to interact with your true inner self, and (b) no self wants a machine or another person too close, else it endangers the very notion of self.

The psychological self is not a suitable base for a technological system.

Which leaves the outer self, the one you exist within your community.

The only remaining base for a technological system of identity is that which explores the relationships between yourself and your close peers. Your community.

This may seem odd at first. But actually it is what Identity engineers have been drifting towards in their championing of attributes and verifiable claims: we can't trust the grand designs, but we can trust what Alice says of Bob.

The WHAT of identity is many schools of thought. Now expressed, we can narrow them down to one. This one remaining possibility achieves the WHY - because peer identity is the last Identity left standing.

Others have catalogued different forms of identity for example Joe Andrieu et al ("Five Mental Models of Identity") and Kaliya Young (*The Domains of Identity*). However these efforts have tended towards the inclusive, with an assumption that all forms have some benefit or place in the world. Here, I have been exclusive. I want to ask what form is the future foundation of systems of identity? And I want to draw a clear line with the failures of the past, which necessitates cutting away the deadwood and the bad wood; the others all have fatal flaws and therefore exclude themselves.

Can I trust you?

> You're so vain, you probably think this song is about you
> You're so vain, I'll bet you think this song is about you
> Don't you? Don't You?
> *(Carly Simon, "You're so Vain")*

Which then leaves us with many uncertainties, chief of which is this: who do you wish to share your real personality with? Friendly, unguarded, safe, open?

This uncertainty then forms the essence of the inquiry to follow - who do you wish to share yourself with? How do you wish to share? Under what conditions, what limitations, what enticements? What scares you away?

The answer to that is pat and simple: you share your identity with those you trust. Indeed, as if to prove this point, we share more of our self with those we trust more, and less with those we distrust.

(It is also said, "the currency of intimacy is disclosure" - we build intimate relationships via selective sharing of facts, stories, opinions, and experiences with our intimate friends. These are details we withhold from others. When we don't want the relationship we don't disclose. We may disclose something and regret doing so. How do we decide how much to share and with whom?)

Which is seemingly backwards - at the beginning of this essay, we wanted to build a trust system on top of our identity system, and it turns out that we can only build an identity system if we first have a trust system.

No matter, at least we've discovered something. As far as an Identity System is concerned, trust comes first. It is to that we now turn, in our quest of WHY.

2

Trust

Part II - On Trust

In Part I - My Identity, we came to the conclusion that your identity is usefully split between yourself and your community. Which leads us to ask, who is your community? To some extent, that can be answered by saying, *your community is who you trust to hold your identity* - almost a circular definition but with that important link, trust.

To understand Identity, then, we must first understand trust. This section looks at *trust* - what it is, how it comes about, and more importantly how can we tame it for the purposes of assisting Alice with her life? We come back to *community* in the next part.

II.1 Micro-trust - Alice trusts Bob

> What's in a name? that which we call a rose
> By any other name would smell as sweet.
> *(William Shakespeare, Romeo and Juliet)*

The Essence of Relationship

Let's assume that trust is something that humans do with each other[1]. Let's start with a basic scenario of two people, Alice and Bob[2], who are approximately equal as human beings. There is something that draws them together:

```
Alice trusts Bob...
```

Although nice, such statements use romance to avoid a lack of precision. When a person trusts another, she makes a decision over a particular question of some current interest. When we say the above, we mean something like

```
Alice trusts Bob to make dinner.
```

being that Alice makes that decision over that action, and not over another. There is some risk involved, and these two can be both true

```
Alice doesn't trust Bob to mind her kids.
```

Or not, or either/or. Context is important! And therefore, trust isn't some universal thing, it's a set of situation-result pairs. Indeed, because we know that there are so many situations - *does Alice trust Bob to go shopping?* - we can also suggest that there must be some element of purposeful decision by Alice.

Go to the movies with Bob? Introduce Bob to her parents? Ask Bob to recommend an app or a dress or a garden gnome - Alice knows the answer in most cases pretty instantly.

Which tells us something else:

```
Alice knows something about Bob.
```

Alice has a base of experience with Bob that supports her decision.

Then: *trust* is from one person to another, concerning a particular question, in which the decision to trust is made quickly based on experience and information already known about the person(s) and the situation.

So far so good. Yet there is more to say: Let's ask

```
what does Alice think about Bob's gender?
```

This is a particularly interesting question because in classical thinking, gender is both unchangeable and knowable. Although in modern times we challenge the stereotype, and gender is a delicious plot element in comedies, the basic claim is remarkably reliable:

```
Alice trusts Bob is male.
```

For Bob's sake, we're glad that is sorted out!

Figure 6 - Alice's Ladder of Trust

On Knowing

> *Alice: Would you tell me, please, which way I ought to go from here?*
> The Cheshire Cat: That depends a good deal on where you want to get to.
> *Alice: I don't much care where.*
> The Cheshire Cat: Then it doesn't much matter which way you go.
> *Alice: ...So long as I get somewhere.*
> The Cheshire Cat: Oh, you're sure to do that, if only you walk long enough.
> *(Lewis Carroll,* Alice's Adventures in Wonderland*)*

But actually, that's not quite right! If we ask Alice what she thinks of this question, she will not disagree but would prefer to say:

```
Alice knows that Bob is male.
```

Leaving aside how Alice knows this, what is interesting here is that knowledge is a stronger thing than trust. Alice *trusts* Bob to go shopping, but he might forget - and may incur Alice's wrath. On the other hand, Alice *knows* Bob is male, and there is no question about this; he will not return from the shopping mall with a sudden shift in gender.

Which speaks to certainty - if we have complete certainty, then knowledge is used, but if we have a doubt, then a trust decision is called for.

The boundary between trust and knowledge is a fascinating place. A child for example knows the gender of parents - but this was not always the case. A baby of 0 days old knows no such thing, indeed, knows nothing, not even what a male or female is, nor what a person is. As the child grows, first there is mother, then there is father, who perversely is primarily useful only for providing evidence for mother, and later on there is a metamorphosis into the general classes of males and females.

And so it is with all things: Our state of mind over some vague question transitions from nothing to a formative idea or suspicion to a theory to trust to certainty. Read the following table from the bottom to the top:

Name or Level	Description	Process	Source
Knowledge		Belief, Truth, Facts - we are beyond process	Life experience, authority, religion, family, dress
Trust	Analyse by cues at a distance, confirm as more information arrives	Observation of cues	Many prior sources that they have generally proven reliable
Theory	Gender can be guessed from clothing, shape, voice, etc	Tresting, listening	Child tests and asks each new person what gender are you?
Suspicion	Observations mostly point in a direction, some point widly elsewhere	Observation, curiosity, questioning	Senses something different and discordant between choices
Confusion	Sense of ambiguous and contradictory information	Angst, discordance	Sees differences but cannot isolate
Nothing	Absence of any thought on the subject	Ignorance	Light, mystery, amusement, love

Table 2: From Nothing to Knowledge

From trust to certainty, what happens? We no longer make conscious decisions, *we just know,* or in the lingo of the psychologist, we internalise the knowledge. Which is to say, in the transition from trust to knowledge, we forget how we got here because it isn't worth the mental energy anymore.

> "To believe is to know you believe, and to know you believe is not to believe."
> *(Jean-Paul Sartre)*

What happens between a theory and trust? A theory is for fun experimentation - we try things out and watch what happens. Gambling is maybe a theory with rewards and losses; Bob did a mean steak in the past, let's try him out on a pizza?

The differentiator is doubt. When there is substantial doubt, we must use other strategies, but when there is substantially less doubt, we can trust in our decision making and run with the consequences.

Then, Alice trusts in Bob when she has enough information to take a risk - with the reliability of knowing her losses are both acceptable and less than her wins.

So trust is inherent with risk - the loss from a wrong decision is balanced by the reward of a good decision. If there is zero risk, it would be knowledge or irrelevant. If there isn't enough probability of net wins for Alice to go with the risk, then it is not trust, but hope, gambling, experimenting, investment in future knowledge, and present knowledge that she has to deal directly, immediately with failure.

Trust is therefore that space in human observation where the probability of success is high enough to take a risk, and accept the consequences, but not high enough to internalise as knowledge.

Skin in the Game

> "Trusted" means "Someone who can screw you over by acting in bad faith."
> *(Ray "Bear" Dillinger, Cryptography list)*

In this game, on making a *decision*, Alice takes on *risk*. Bob's delivery of his obligations to Alice include some non-trivial uncertainty. E.g., If Alice does risk leaving her kids with Bob, he could drop a pot of boiling water on them, lose them in the park, generally fail to feed them or lose them playing on the freeway.

He probably won't, but he might.

Alice accepts the risk in exchange for some reward. That reward might be intangible and incalculable, but it is generally present in some sense or other - and therefore Alice has to have *skin in the game*! It doesn't make a lot of sense to expose herself to some risk without a commensurate benefit, even if the payoff is small, perceived, manipulated.

Having received the payoff, Alice can analyse the consequences of her decision. Once the deal is done, her analysis is not constrained in time or event - it can happen immediately, slowly, or even wait for a future proposition.

These propositions come along in a continuous series, and are subject to continuous analysis - unconsciously or consciously - until she finds a proposal that offers her a profit. Or not. Therefore we can say, in the sense of game theory, that

```
trust cannot exist in a one round game.
```

The only way that trust can exist - build up - is within a repeated round game which is unbounded.

If you are unfamiliar with this notion of game theory, and how it impacts trust, spend 30 mins or so going through *The Evolution of Trust*. It's a fun interactive demo of game theory.

The Cycle of Trust - RADR

> "If there's one big takeaway from all of game theory, it is this:
> What the game is, defines what the players do. Our problem today isn't just that people are losing trust, it's that our environment acts against the evolution of trust.
> That may seem cynical or naive - that we're "merely" products of our environment - but as game theory reminds us, we are each others' environment. In the short run, the game defines the players. But in the long run, it's us players who define the game."
> *(Nicky Case,* The Evolution of Trust*)*

Against any proposition she receives, Alice's analysis needs to promise her that the expected reward will be in excess of her costs. When she finds that, she decides, again!

But her analysis can only be well informed by previous experiences. Therefore, Alice's trust machine is a loop (or spiral), one per each person that she knows. Starting at any point, it continues with each person, going around and around. It has to be a loop because the analysis of any new proposition can only be based on facts which relate to the proposition - and the best proposition is one that looks like the old facts, in which a decision was taken, a risk held against a reward delivered, allowing analysis for a future round.
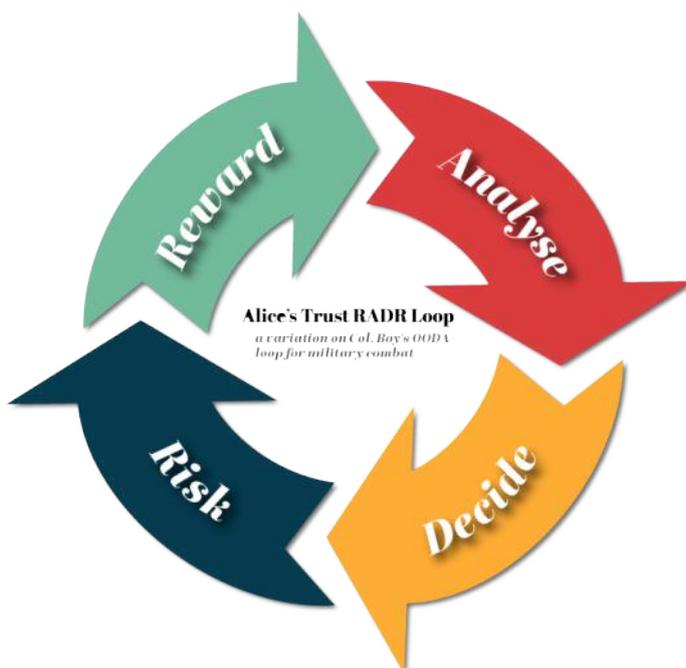
Figure 7 - Alice's Trust RADR (Reward-Analyse-Decide-Risk) Loop

Trust is by definition circular - once a trust cycle has been run a few times, Alice can develop an expectation of future returns.

This expectation of the future allows for favours - Alice can ask for a favour, which in some intangible sense she is expected to return at a later date, or she can deliver favours, and store them in the 'trust bank' for a future call. In such a way, a decision can be built from many such decisions, allowing for amortization of the costs of each decision over collective events - trust builds over time. (If you've spent some fun time on *The Evolution of Trust* you will perhaps notice now how Alice's trust machine is so much more capable than say Copycat or Copykitten, which have almost no memory, or very limited memory.)

Alice's trust of Bob always involves a decision based on some base of information. Hopefully, that information is a collection of past interactions. Even better is if these interactions include a dose of prior trust decisions, in which case her trust increases with each succeeding successful event.

If not, in the absence of previous experience, her decision can rest on proxies such as recommendations, personality, metrics, likeness, tests, environment, safety, customs, etc, but in that case, her risk goes up so Alice would typically reduce the value at risk. Alice might start with something very small - something she can afford to lose.

Limiting Trust

> Don't speak
> I know just what you're saying
> So please stop explaining
> Don't tell me cause it hurts
> *(No Doubt, "Don't Speak,")*

Around the general idea of trust, we can place a number of limits to keep Alice safe.

Identity for Alice to run her *reward-analyse-decide-risk* process over Bob, she needs to know that the Bob in spin 1 is the same as the Bob in spin 2, 3 through 100. In short, she needs an *identifier* to the person she's trusting and a little internal database collecting all the RADR traces from that person. Trust by its very nature is a many-round game, and no trust builds up over a person if he's different every round.

Then, if we were trying to pigeonhole trust, we could say that *to Alice*, Bob's *Identity* is the sum of all the interactions she has done over *identifier* Bob. And, her *Trust* of him is the summed results of all of her RADR experiences. But this is a crude simplification, we know that people are more complicated than pigeons.

Precision. Alice might trust Bob in one question, but that will not relate to another question. For example, Alice might trust Bob with a loan of $10 but she might not trust him to look after her children. Or vice versa, there is no necessary relationship between the questions, only that they exist, and each has to be analysed independently.

Expectation. Alice only proceeds if her expected profit is in the positive. That is, the Cost over *Results + Analysis + Decision + Risk* needs to be less than the Reward deriving from the *the Results*.

Choice. She only *trusts* Bob when she *chooses* to do so. If Alice has no choice, all bets are off, she's in *compliance-mode* not trust-mode. If for example she asks the state registry for a Driving Licence, she is not choosing the state over some other supplier. The state registry is the only authority delivering the document, and so there is no choice.

Authority. Alice has rights. If she exercises these rights, and takes no risk, then there is no trust expended. Likewise if she makes no risky decision, then no new information comes back. E.g., when she gets her Driving Licence, Alice doesn't find herself trusting the state registry more; she has a right to drive, and that right will persist. In contrast, when she drives past a police car, she worries that she'll be stopped. She has no right to speed, her choices in driving then have a lot to do with her taking risks, and her trust of the police to enforce or not is a continual issue.

A Definition of Trust

> The word 'risk' derives from the early Italian risicare, which means 'to dare'. In this sense, risk a choice rather than a fate. The actions we dare to take, which depend on how free we are to make choices, are what the story of risk is all about. And that story helps define what it means to be a human being.
> *(Peter Bernstein,* Against the Gods: The Remarkable Story of Risk*)*

Let's summarise these limits:

- A decision is made
- to take a risk
- over a known person
- in substantial uncertainty
- over some limited question or context
- in exchange for some benefit.
- Voluntary choice is essential
- Based on the history or experience of the maker of the decision over that person.

Enough blahbla, can we come up with a definition? Let's try:

```
When Alice trusts Bob, she chooses to take a risk on Bob's actions in a
limited context, based on her prior experiences, in order to gain some
expected benefit.
```

Like Alice, I take a risk on that definition - if I get it wrong, you will write at length how my definitions are untrustworthy; on the other hand, you may have to take a risk on that definition too, in order to try it - to find your own base of experience, to find out if it works. Trust me?

II.2 Dynamics of Trust

> How did you know, 'Cause I never told / You found out, I got a crush on you
> No more charades / My heart's been displayed
> You found out, I got a crush on you.
> *(The Jets, "Crush on You")*

The foregoing was a closed system - Alice trusted Bob, once, in isolation. Then, Alice moved on to trusting Bob again and again. Adding Alice's Trust RADR, we see there is a distinction between a trust decision (discrete) and a body of trust (continuous).

Let's go further. What Alice does in trusting Bob is non-deterministic, non-modellable, non-normative. It's also dynamic. In the larger sense or continual context, we might say

```
Alice trusts Bob (always) to go shopping
```

to mean that we expect Alice will take a risk with Bob in some future shared understanding. We can then see two different uses of the word trust, being over a particular question and instant, or, over a set of questions of related context, spread over time. I suggest that understanding the one depends on understanding the other; above we concentrated on the singular or discrete context, and now it is time to concentrate on the continuous.

How to Break Alice's Trust

> Perhaps your definition of your self-system lacks authentic boundaries. You've erected a precarious structure of personality on unconscious factors over which you have no control. That's why you feel threatened by me.
> *(Philip K. Dick,* Ubik*)*

Above, we assumed that Bob and Alice were approximately equal in some sense. Let's now consider a multi-decision game where Bob breaks Alice's trust model.

Because of the supercharged benefit that Bob can extract from Alice if he can correctly predict Alice's decision, he tries. And occasionally at least, he succeeds, and Alice loses out.

Which means that Bob is now no longer an uninteresting and uninterested part of the model - Bob's actions on Alice's trust are part of Alice's decision making. There is no algebra of trust, but there might be a calculus of trust.

In each succeeding round, Alice is forced to defend her model from prediction. She is forced to bury her thought processes and decision making behind any tool she has: vaguery, politeness, ditzyness, lies, ivory tower logic, belief, excuses, stonewalling… in order to stop Bob abusing her model. Alice's model becomes very subtle, indeed, in time, Alice becomes too subtle for even Alice to know.

Then, **if we model how Alice trusts, we break it** - Alice is forced by extraction of benefit to both stop trusting in the beneficiary, and *to change her model*. Until she reaches a point where she is defended in her model.

Trust then is Heisenbergian - we can know that trust is there, but we cannot know what that mechanism is. We may be able to measure the trust, but in the act of revealing it we break it. Finally, a use case for quantum computing!

Trust and the Machine

> 🤔 But if we can't trust technology....and I put technology in my head...how could I ever trust myself again?

(Figure 8 - @brian_trollz)

This observation above, that if we model trust we break it, leads us to some tantalising hypotheses.

Machines cannot do trust. If they could, they would have broken Alice's model, and would then become Alice's vulnerability - forcing her to change her model, or hard-fork the machine. She might not realise it at first, it might take a while, but the longer it takes, the angrier she'll be.

Trust can't be interposed. Imagine a perfect machine that captured Alice's trust within and analysed the activity to assist Alice. As the machine gets better, it would become more valuable. Bob would attack the machine - or someone else would.

We can see this spectre of interposed trust in today's social networks and shopping sites - first they gain Alice's trust - or repetitive custom - then they bombard her with adverts, then they sell her data to every other site who tracks her around and feeds her back her private buying habits. Eventually, Alice is forced to realise she cannot trust the system that is providing her the channels - and Alice buries her trust another metre deeper into her psyche.

Humans do not trust machines. As it happens, this is quite reasonable. Humans *rely* on good machines, because they are reliable. They deliver at the level of knowledge, or they are disposed of. When Alice asks the machine, it will always tell her the same thing: assuming the humans have done the right thing, the machine will do the right thing.

Machines can do data collection and prediction and all sorts of other things, but there emerges a natural line that machines should not cross, else the line in the sand is shifted. By Alice, to put the machine back in the box - of unfit machines.

Machines can't be Human. It follows that machines can't trust other machines. Machines can do protocols, run algorithms over data, run errands to other machines, high frequency trading, play Copycat against CopyKitten. Machines can lose all your money, but they cannot enter into contracts, themselves, nor take responsibility for a risky decision, nor fall in love.

A trust system isn't. Therefore, the so-called "trust systems" or "reputation systems" can only record metrics - hard data - that feed into a trust decision by a human. Systems cannot "trust" nor can they replace trust nor "be trusted" in the same way that humans are. The

systems can move some of the calculations and collection that Alice used to do into her more convenient iPad, but what is left for her to do is still called trust, what she put into the machine she calls algorithms and data (Ian Grigg, "Identity is an Edge Protocol").

We could of course explore the edges of these claims. Could Alice trust the weather to deliver rain? Could an AI be built that would be as vaguely hopeful as Bob? (Konstantinos Sgantzos and Ian Grigg, "Simulating the human brain") Does Bob trust his dog, does Alice's cat trust Alice? For the sake of this essay at least, we leave those aside.

Alice's machine calculates, Alice trusts.

Automata in games can show us how to break trust, but they do not show us how to build trust. If you spent some time playing *The Evolution of Trust* you will realise that CopyCat and her friends break their opponent and win quite regularly within certain bounds. These are coded strategies to break the game of others and when they win against others, trust cannot grow. In effect, they are strategies that either break trust or reach steady state with like players, rather than ones to build trust.

But above we say that Alice rebuilds her trust model after each loss, and hides it deeper each time to protect herself. The simple game theory algorithms are small, simple programs called finite state automata and they are not capable of holding the memory that is needed for Alice's trust game.

Economics of Trust

> But, what, you ask, do I do when someone defrauds me? The neat thing about using financial cryptography on public networks is that you can use the much cheaper early-industrial trust models that went away because you couldn't shove a paper bearer bond down a telegraph wire. In short, reputation becomes everything. Like J. Pierpont Morgan said 90 years ago, '...Character. I wouldn't buy anything from a man with no character if he offered me all the bonds in Christendom.' In a geodesic market, if someone commits fraud, everyone knows it. Instantly. And, something much worse than incarceration happens to that person. That person's reputation 'capital' disappears. They cease to exist financially. Financial cryptographers jokingly call it reputation capital punishment. :-). The miscreant has to start all over with a new digital signature, and have to pay through the nose until that signature's reputation's established. A very long and expensive process, as anyone who's gone bankrupt will testify to.
> *(Robert Hettinga, "A Geodesic Society?")*

Another observation that emerges is that trust is expensive - damned expensive. It behoves to consider trust through an economics lens - how is it expensive, and how can we deal with the costs? Because at a minimum, Alice is impelled to seek economies in her trust.

Trust is expensive! To keep doing trade with Bob, she has to be able to extract sufficient benefit from Bob that their relative benefits are in profit, even as they both attack each other's trust models.

Therefore, *Alice searches for economies*.

Trust requires continual testing -- improvement of information and refreshing of the experience is needed. If Alice doesn't invest in the maintenance of trust, by refreshed information, it might not be there when she needs it. If Alice 'trusts' on too few data points, it is too easily gamed.

Alice has to construct a model of Bob's trustworthy behaviour, then test it at her own risk, and then keep testing and trusting.

Society. Worse, as we discover in the following section, Alice needs to work with, that is, achieve net benefit with, many people. So, she is compelled to build a trust relationship with many people.

Not only with Bob, Alice must duplicate this process with all her counterparties = ∑Xpensive.

Alice's model is not transitive. As a consequence of Alice's mindful analysis of Bob and his circumstances, and her need to hide the model deeply, any decision to trust Bob is not trivially shareable with another.

Facts might be transitive - the fact that Alice trusts Bob might be used by Carol to trust Bob, but only within limitations - does Carol know Alice's mind, did she share Alice's experiences, can she duplicate Alice's trust thoughts, can she incorporate the fact into her own trust model? No, she cannot.

If Alice trusts Bob to behave, this bounty does not necessarily pass on to Bob's friends. Now Alice has to look into Bob's mind and into the minds of Bob's friends. Assessing Bob's friends is a distinct trust decision to whether she trusts Bob himself.

What someone understands as a fact is, when transferred, just an opinion shared. Unless that transfer is backed up by an appropriate foundation, it lacks the ability to impress: Bob may claim his friends are cool and safe, but Alice might decide that Bob is unreliable on this point, and in order to permit his friends in the house, Alice may require Bob to up the ante - Bob must back up Alice's decision to trust Bob with some additional offer. Bob might underwrite the risk, cover the direct costs, or place other assets on the line - either way, if Bob wants Alice to accept a risk to her from Bob's erstwhile trustworthy mates, he might have to put something on the table to even the imbalance.

In the language of J. Pierpont Morgan, Alice might accept Bob's character and Bob's bond on a transitive risk such as Bob's mates, but neither alone. This does not mean that trust is now transferrable, or even sellable; more, it means that Bob and Alice can construct an exotic derivative that appears profitable. Bob gives Alice an option on remedy for any shortfalls by Bob's mates. Indeed, relationships might be better off expressed in the language of finance, if only we could recognise the shared risk of Alice and Bob as opposed to the winner take all profit-seeking of the legal entities in finance.

Prisoner's Dilemma. Alice is beset by others looking for personal gain. The easiest personal gain is to steal from each other, but this is a net loss game - Alice loses more than the thief gains, so society loses value over time.

We can create more together, and live in a net-profit game, yet we remain subject to temptation of short term theft. This is the Prisoner's Dilemma, and game theory says that the solution that places us working together for shared gain is always another round, in which the greater part of the reward is always in the future.

Therefore, if trust is the accounting for our solution to the Prisoner's Dilemma - we come together, aim for the future, we build a future together, accepting shared risks made of shared downsides and upsides.

Trust prefers an equilibrium. In order to trust Bob she must interact with him, take risks on him, and balance the books. Unilateral trust is possible - think of rock stars, messiahs, presidential candidates and the new generation of Satoshii at the helm of each blockchain. But the more natural state of affairs for trust is an approximate equilibrium in which both

invest in each other. A lot or a little, as its human nature to game each other's model a little or a lot, and both learn enough of each other to make the micro- or single-round trust decisions needed to proceed to the next round.

Trust is the potlatch of relationships: we both of us have to destroy good time and effort in order to win. Bilateral or mutual trust is therefore the first, easy economy - while I learn about you, you are learning about me.

Trust has economies of scale. Notwithstanding that the model cannot be easily shared, the expense of the process pushes us for a continual search for easier ways. Sharing of something is one way:

- *Database sharing.* Alice can share her information with Carol. She can relate anecdotes and experiences, or share her contacts list.
- *Derivative trust.* Alice can share her decisions - she can tell Carol that she trusts Bob. At its minimum, this is just more information for Carol's information base; at the maximum, it is a proxy decision for Carol - I trust Bob because Alice trusts Bob.
- *Mutual Trust.* Alice and Bob can work the trust game together - each cycle can be a cycle for both.

No matter the simplifications achieved here by Carol, to her economic benefit, she has still chosen where to place the dial - listen to Alice, copy the data or adopt a decision by proxy. Unfortunately, we have no way to be more precise where the dial is set, because we are faced with a recursive problem - Alice can only trust that Carol accepts what Alice says as said, as both of them hide their true trust model too deep.

Trust has diseconomies of scale. And then, it's almost an obviosity at this stage, that if Alice has to invest substantial amounts of time to keep Bob and Carol's trust, she'll quickly run out of capacity. True trust is limited to a very select group - that group you've invested substantial time into, and been invested by, for natural reasons outside the strict goal of acquiring trust.

Islands of Trust. If Alice can invest in Bob, and in Carol, can she invest in Bob and Carol at the same time? Larger groups of trust should emerge - if the components of trust can be shared economically, then the mechanisms of that sharing should encourage groups to form.

Alice wants to share - whether your theory of humanity is based on evolution of the defensibility of groups, specialisation or Maslow's pyramid of needs, humans want to belong and want to contribute. But it goes beyond that - Alice needs to share her identity with those she trusts because that's the only way that her life can move forward. The groups she trusts, those that she feels comfortable sharing her identity with, are then the next essential step in our journey.

Before we turn in the next section to what a group means to Alice, we should review the 'systems' that have to date presented a solution to her. If you are familiar with the 'trust business' or social networks or similar, you might like to skip to the Conclusion, or straight to Part III.

II.3 Critiques of So-called 'Trust' Systems

> It is nice to trust, but it's better not to.
>
> *(Old Italian proverb, recorded by Steve Wilson, "Abandoning identity in favor of attributes")*

It should then be apparent that there is no such thing as a 'trust system' as, if it were, it would be broken by definition. Before we dive into what can exist, let's review what these systems refer to when they say they are in the trust business. Let's find the best trust that money can buy.

The Antithesis of Trust

> Scientists are easier to fool than children.
> *(James Randi)*

The best anti-Trust that money can buy is a certificate from a Certification Authority ("CA"). It breaches most all the above: There is no choice available to the user other than the intractable choice of not using the system; likewise, the decision to take a risk on a website is not made by Alice, as HTTPS is seamless and 2 decades of user experience and testing shows that users do not notice any switch to or from cleartext HTTP. Although the user takes a risk, few will recognise that she is indeed taking a risk, and none will know what that risk is; most insiders in the industry don't know what it is either. The context could be narrow or broad - nobody knows because although the certificate might be tight, the browser is not. Finally, her only foundation for taking that risk - the null decision of doing what she was told to by her bank or browser - is that nothing went wrong before now. Surely, if that is a foundation, it's the same foundation of risk that makes turkeys think that Christmas never comes.

About the only thing that is certain about the use of the term 'trust' in the CA business is that it isn't 'trust' and whatever it is, it has screwed with people's understandings of what trust is and means.

Reliance - a Trivial Cousin of Trust

> There is an unconditional and unchangeable relation between input and output. The trivial machine is extremely reliable. Its internal states constantly stay the same. It is independent of the past, and can be synthetically and analytically determined. We can find out what its transfer function is, should be by change forget it for some reason, by doing simple input and output experiments. The analytical experiment is trivial. And that is why it is so popular. In my opinion, our Western culture has fallen head over heels with this type of machine. It is the epitome of our yearning for certainty and security. When we buy a car, we demand a trivialization guarantee. We want the car to conduct itself in a constantly predictable manner, at least for the length of the warranty. And if this is not the case, we bring it back to a trivialise, who retrivializes the car.
> *(Heinz von Foerster,* Understanding Systems, Conversations on Epistemology and Ethics*)*

There is a close cousin in the PKI ("public key infrastructure") world called *reliance*. In the CA/PKI concept, we can build up a structure of contracts, claims, and verifications such that the user *may rely on* the claims made. For example, the certificate includes the name of the holder, and thus the user may rely that this is the name of the certificate holder; it is said that the user then becomes the relying party.

Because each step is reliable, the hope is that the result is more deterministic than, say, trust. Reliance in this context is the same relationship we have with a machine. Our car will carry us on a journey to work this morning because that is everything about what it does, in a statement: its job is to carry us to work and everything is tuned to that objective.

Reliance aims at belief or knowledge. In contrast trust is a higher order human decision about taking a risk on some decision *where we cannot rely*. In this sense the evolution of an automated system is typically about creating more reliance; a re-interpretation of the CA's marketing might be that you do not need to trust because you can rely. You can believe, there is no risk.

Trustlessness

> If you (or your child) is 16 years old, Bitcoin has been around for more than half your life --- which is "good enough" for trust.
> *(Spencer Bogart)*

In additional analogue, the same could be said of Bitcoin - it has built a system of reliance, in which, you do not need to trust people to keep it running. Hence, *trustless,* a term used by Bitcoiners, is actually a fairly good approximation of some parts of the technical system such as the incentive system promoting a probabilistic finality on consensus over a block. Yet, as with Alice and Bob, the algorithm might be trustless, but the algorithm's friends might not be.

As we saw in the hard fork stories for Ethereum and Bitcoin, *trustlessness* is not reliable, neither in cryptography nor in life. While the mathematics might be unchallengeable, you can still lose your money to a host of enemies. And now, with forks, you can double your tokens, which might sound good for those hoping to win double the money, but it's death to business which earns double the liabilities through forked smart contracts (Ian Grigg, "Cabaret").

As systems, Bitcoin and Ethereum have pushed themselves back down from reliable knowledge down to risky trust. Indeed, the blockchain mechanics don't even reach the challenge of the old Russian proverb - trust, but verify! - as you yourself cannot verify the mathematics nor the system.

Try as you might, you cannot escape the essential law of life: that which we can automate safely, we do, for everything else there is governance. The experiences of the blockchains just cast into stark relief what happens when one single innovation simplifies the governance requirements - does a wild-eyed mystical technocrati class believe they've solved everything? Or can we recast the governance to serve the members, utilising the benefit of the new invention? (Ian Grigg, "The Governed Blockchain").

This is less to criticise Bitcoin than to criticise the weaknesses of the system. Its implementation of consensus over shared facts, or, *"I know that what you see is what I see"* is a thing of great worth, but reliance on the blockchain simply moves the questions of trust to a higher level: Alice and Bob do not need to trust the system for their tokens, but they do need to trust each other, in community, that the tokens are worth something. Whether Alice can trust Bob beyond a shared consensus on value has not been addressed.

Blockchain engineers do not wear the iron ring (Wikipedia). Alice cannot rely on the engineers because she has little or no choice or sway over their actions, they act much like any state registry issuing a licence.

Figure 9 - Blockchain Engineers do not wear the Iron Ring

The Failure of PKI Reliance

Back to PKI. Why then could not the PKI / CA be called a trustless system when Bitcoin could lay claim to the new title? It is because the reliance in web's form of PKI is over nothing, and is therefore not reliable. A relying party in PKI relies on a claim with zero value, because nothing backs it up when it goes wrong (Ian Grigg, "An Open Audit of an Open Certification Authority"). In Bitcoin, we all rely on the coin being acceptable - a Bitcoin is worth 1BTC is worth that Bitcoin to all who agree it is worth a BTC. That works, because we all back it, and the blockchain keeps the numbers solid. If we didn't enter into that compact, it would be worthless, like PKI. But we did, so it's not.

In part this is because Bitcoin has a tight feedback loop that is re-proven many times; you rely that your payment will stick, and as an essential act of commerce, if it fails, you are screwed. You run the payment again, you seek other recourse, you get your money back, or you exit the system. With feeling.

In the CA system you might want the name to be correct, or the connection or whatever, but whether it is or not, is not related directly, haptically, financially to an essential act of commerce. The name is so filtered, the connection so wrapped in other systems, the errors so hidden, that the real act is disconnected. If you're screwed, who do you blame?

Let's characterise this as Alice layering her trust over components of reliance. The machine provides reliance at the lower level, and that which the machine does not provide is kicked up to the higher, trust or governance layer. Trust is the exclusive domain of humans. As described above, experience is collected and processed, decisions are made, risks are taken; all acts taken by humans. Without these acts, repeated and repetitive, no trust is possible.

In the end, certificates are not *reliable*, but the system is *trustable* - the user trusts the browser every time she goes to a merchant site. With this comes an inherent risk of failure. Phishing opens up the weaknesses in the system and easily slices the browser's security model apart from the certificate model. As the weakness is in the browser, the result is that Alice and her browser manufacturer are in a trust relationship. The only shortfall of this model is recognition - that Alice is ignorant of who she is trusting, and the browser manufacturers deny that their brand as über-CA is what Alice is trusting.

From this point of view, the secure browsing mechanism is a trust relationship and this is a bad thing - we should have been able to build a system that delivered reliance for websites by now.

A System of Real Trust?

> bIlujlaHbe' chugh vaj bIQaplaHbe'
> If you cannot lose, you cannot win
> *(Klingon proverb)*

A system that evolves for the benefit of the user might be said to be one that identifies slices of the user's trust process, automates those subsets, and pushes them into her reliance layer. Each evolutionary step pushes a little more down into the machine, leaving the bulk of thinking still to be done by humans. And, even if the new system is a radical improvement in Alice's lot, it seems that she and her friends find new ways in which to use and abuse the system. Perhaps there is an inner need to gamble, a cognitive limit or a learning block such as Dunbar's Number (discussed in Part III), a limit on her trust on the inner machine, that humans just need a certain balance of trust and untrust in order to function?

Can we conclude that a system of real trust should seek the above happy medium, to find some identifiable mechanism, to capture some subset of the activity, to deliver it safely and reliably wrapped in metrics? Once so captured, Alice our user can discover and decide for herself how to proceed, internalise, and work with the new information.

To do this, Alice needs to have available to her events - memories - of the past actions of Bob, and preferably ones close to or analogous to her current pending decision. Alice needs to live her prior life before she admits any new information. To do otherwise is a denial, a collapse, a fleeing of all that she knows; then all new trust must build on what she knows.

With this in hand, let's continue our review of what people call 'trust systems'. If you are impatient with technical blabla, skip to the Conclusion, or straight to Part III.

There are approximately two popular ways to look at so-called trust systems (sometimes called reputation systems): bottom-up grassroots or top-down hierarchical systems. The former is generally characterised as web-of-trust (WoT), the latter by the Identity Document (ID). In between these two poles are both corporate variants and local variants.

The Identity Document (ID) - top-down

> If you work at Goldman Sachs in New York City and you want to tie up a woman and then have sex with her, there's a good chance you'll first have to speak to Rita. She'll insist on calling your office, speaking to the switchboard operator, and being patched through to your desk. Then she will want to check out your profile on the company website and LinkedIn. She'll demand you send her message from your work email, and require a scan of either your passport or driver's license. And you will comply.
> *(Allison Schrager, "Trust and Crime")*

The popular view of trust starts from a top-down government-issued identity document ("ID") or its close sibling the Identity Number. In this concept, people can look at Alice's ID, and decide whether that's good enough to trust her.

The foundation of this one view on *trust in documents* is a little bit difficult tease out, but history can be found in the Napoleonic code countries in which citizens are required to register with their city office. If a name is known, then the person can be found, as the registry has their address, by law. Lawsuits filed in court can then be delivered reliably by the postal service, and in some sense, history can follow a person from city to city. In European tradition, it is considered bad (illegal?) to engage with others under a different name or use a different address.

Curiously, IDs are considered as worthy of trust in non-Napoleonic code countries, yet they do not feature the above assists. In the anglo-world, it is substantially more difficult and risky to *serve summons* from a court. And, trading under any name or at any address is considered more acceptable, as long as fraud is not entertained. You do not need permission or registration to move to a city, you do not need permission to marry in another country, records do not follow you. People are more free, for good and bad - large countries and free countries tend to hide more scammers.

One confusion with the state-issued ID is that the state itself has a substantial advantage in relying upon it, whereas the ID is less usually created and issued with the purpose of any other entity (other than another state) relying upon it; this weakness can be seen in the use of the social security numbers (SSNs) by American issuers of credit. Even though such was an explicitly unintended use by Congress, and SSNs are not reliable in any technical sense, many rely.

Both systems are weak when borders are involved. Indeed it could be that reliance on IDs by the public is actually reliance on the fabric of law and society within borders - in this sense, by custom we all operate to the standards of the society, the country, the city or *el barrio*. Recording ID could then simply be a ceremony to remind ourselves of this fabric.

Web of Trust (WoT) - bottom-up

The web of trust was first popularised by PGP in the early 1990s, so let's describe that system. A public / private key pair is created by a user, and she distributes her key[3] by some means or other. When Alice meets someone at an event, she conducts some brief and due diligence over Bob, and then decides to sign his key, and return the signed key to him. Hopefully this is mutual.

In this way, Alice collects signatures on her key, as does everyone. When Carol comes across Alice's key, she'll feel a bit more comfortable that it is indeed Alice's key because it has some signing traffic. Better, if she can find one of the signatories who she has also signed, this means someone she knows and already checked out has verified Alice in like fashion. In this way a *web of trust* is constructed across many people.

Alice can also put on a rating on her friend's key of *do not / maybe do / usually do / always do* trust the key to verify the keys of others. In this way, if Bob has signed Carol's key, and Bob is rated as "*usually do trust*" then Bob's signature over Carol's key can be accepted by Alice, at least to that level of *usually*. Whatever that means.

So how does this compare with our version above of trust? The first thing that strikes out is, we're unclear on the meaning: what does "trust" mean in the PGP context? And this is unclear. While it is clear that Alice "trusts" Bob by her rating, what does she trust him for? It's not stated, and if we've learnt anything by now, it is that overly broad expectations must fail.

Typically we would expect a statement of what the signature means, but there is none in PGP doctrine, and this is both formal and deliberate. As a result, we get considerably distinct schools emerging with different meanings within the same web of trust. Some people treat it as an identity check and carefully make sure that the identity encoded into the key is matched by say a passport. Yet other people refuse to look at documents, and insist that it is the meeting that is attested to, not the name. In this way, people in the second group have keys signed as "Mickey Mouse" much to the annoyance of the first group.

Without at least some indication, PGP's web of trust fails to deliver any reliable information and therefore cannot scale as a vector of trust.

Certificates signed by CAs (PKI)

The alternate school of thought was popularised by a startup called Verisign, which to cut a complex story off at the knees convinced the first browser manufacturer Netscape to let it sign the keys of users of SSL, a protocol for securing the web.

Thus, emerged the first widely scaled *public key infrastructure* or PKI. Originally, PKI was developed by telecommunications companies who were looking to deliver email to customers over the one-family-one-landline scenario of the late 20th century. Customers would dial up, download mail, then disconnect from the telco. They could then read *and verify* their emails at leisure.

This model never came to pass for a multitude of reasons, not least because telcos were presumed secure, but the technology lived on through the 1980s and into the 1990s for any opportunity that presented itself. And so it was that SSL dawned as a pilot to secure ecommerce in the uncertain, halcyon and financially charged times of 1994.

Fast forword to now. The business model for SSL certification authorities (CAs) is complicated, tedious and deceptive. But in short it reduces to: the CA checks the first user's identity through standard techniques (ID) and then signs a claim of identity over the key. When (other) users are browsing, their software lets the signed certificates go through and badly signed ones are blocked. The user now knows she is communicating with who she expects to.

Unlike PGP's 'trust model', about which there is almost no writing and therefore no consistency, there is no shortage of literature on the CA PKI model. Unfortunately practically none of it is accessible and/or useful. However, some criticisms standout:

The statement over which the signature is made is fairly consistent across the industry. It is in this sense better than no statement such as PGP, but only just. Unfortunately, the statement is over the ID, which as we suggest above, is more of a proxy of hopeful behaviour rather than anything reliably strong, so the baseline value of the statement is surprisingly weak.

Secondly, because the browsers refuse to differentiate the certificates, they are all the same, resulting in a race to the bottom, which leads to certificate manufacturing (Ian Grigg, "PKI considered harmful"). Hence the structure of the PKI model fairly universally eliminates the ability to rely upon it. These and other problems pretty completely eliminate any potential for the browsing PKI to ever deliver something on which Alice can trust, but for different reasons to those perverting PGP's efforts.

Western Tradition of Trust - Courts

CAs will point out that you are free to take your grievance to the courts and indeed this is the trust system that underpins much of rich, western civilisation. Indeed - you can walk the streets after dark, you can rely on a contract, you can avoid being shot, raped, mugged or extorted in much of the OECD world because of the courts, the police and the integrity of the system.

To learn just how powerful these systems are, you need to leave. In the third world, none of the above are necessarily true. In Nairobi, where we spent a few years, walking after night was not safe, and we heard stories all the time. I walked at night, but I also wore a huge knife on my belt - both obvious and illegal, but the police there would simply steal it not charge me. Corruption is the purpose of a job in government.

In the middle east, honour killings are still commonplace. In much of the world, women are not allowed property rights. In Mexico, the real law is the drugs cartels, the police and the military having been long since corrupted by the USA's war on drugs. In impoverished countries sitting on rich resources, no courts seem to trouble the steady flow of left-leaning revolutionaries or right-leaning western corporations. In the countries I am familiar with, the baton of corruption is fueled by the steady stream of powers delivered by the OECD under the guise of anti-money laundering. What the rich countries don't realise is that power to police is power to corrupt.

Western courts also have two other burdens that make them difficult choices for reliance even for us in the rich white world - they are both too expensive where we find them, and they do not work well across borders. Much of Internet life is across borders, making resort to the courts an expensive hypothetical - until the UN opens a global court of petty sessions, we have no reliable recourse for the vast mass of worldwide interaction.

As a sort of tiny footnote to the history of trust in the Internet, this inability makes the PKI offering of the CAs a joke. But the far more important takeaway is that without the reliable courts system that we assume, *no system, no business, no community has an easy to use 'trust' foundation available to it*.

CAcert

Perhaps in rebellion against the untrustworthiness of the PKI industry, a community known as CAcert formed around a sort of do-it-yourself version called assurance. Members check each other's ID against names, but they also check a few other things: that the person is indeed a member, and has agreed to the user agreement[4]. In the user agreement, there is a clause for Arbitration which all agree to, and CAcert runs its own forum of arbitrators to resolve disputes. Notably, the Arbitrator has wide powers including the ability to fine or eject, and thus there is a recourse available to relying parties which is not practically available to browsing users over commercial CAs[5].

Once members have collected enough assurance, they can then get their keys signed by CAcert's CA as above. CAcert also signs OpenPGP keys. Assurers have to be assured, and they have to pass a test. In this sense, CAcert's community is hierarchical with two layers, assurers and non-assurers. Within the assurer layer, it looks more like a web of trust. Outside, it looks more like a PKI, but there is no strong barrier to becoming an assurer.

CAcert is a notable exception to the WoT and PKI limited systems. It resolves in principle many of the weaknesses of the above models. The certificates are slightly clearer, and they can be relied upon at least in documentation. For structural reasons, the delivery falls down: as a CA, it is not itself trusted by the browser suppliers, for reasons outside scope of this paper.

What is more significant for our present purposes is that, even though the certificates within CAcert have failed to deliver much if any trust neither internally nor externally, the people within CAcert have been remarkably trustworthy and trusting. We within the community put this down to arbitration - if something goes wrong, there is a system to deal with the failure. It is not without its controversies, yet CAcert delivers trust - hundreds of resolved cases suggest that *recourse* or *dispute resolution* is both necessary and useful to maintaining trust.

Facebook

No description of trust would be complete without reference to Facebook. Their system is built on a combination of things, primarily the network of 'friends' by interlinking of users by the friending, commentary and photos, the combination of which is sometimes called *the social graph*. As the graph is combined of many weak links, it is relatively powerful in a Granovetter sense, at least strong enough for many companies to rely on it for low value transactions (Mark S. Granovetter, "The Strength of Weak Ties").

This social graph of weak links allows Facebook to avoid making much of a claim over links or the combination. A user finds out for herself who the other person is, using the many links or out of band confirmation. When Bob connects to Alice, he sees her photo and knows he is connected to Alice.

Facebook creates a pretty good social graph that was originally optimised towards the needs of the US campus females. As the film *The Social Network* lays out albeit opaquely behind a brilliantly deceptive script, the expression of the male-female relationship is captured in such a way as to give the female the substantial protection of distance and transparency - *"Facebook me!"* - reversing the imbalance previously trialled in the earlier experiment of Facemash (Aaron Sorkin, *op cit*). It so happens that males are not unduly disadvantaged by this system, and thus there is a stable equilibrium that fits the needs of both sides of the gender divide. Although narrowly constructed within the narrow domain of WEIRD (western, educated, industrialised, rich, developed) campus undergrads, the system also worked for wider, greater parts of society, and the rest is history.

Facebook is by far the most successful of these systems, both from a metrics and an identity point of view. It is notable that Facebook distinguishes itself from other systems by (a) collecting many weak links, (b) not making much or any claim about them, and (c) helping those that are linked to talk. In this way, it helps Alice with her life by making itself her memory, but it stopped short of directly helping her make trust decisions (at least, seemingly, not until the Trump administration, the 2020 USA election and the COVID19 epidemic). Such a thing sits in marked contrast to competitors which try and fail to provide 'trust' information such as "see who your connections are connected to…" and "add a capability…"

Summary of 'Trust' Systems

> Now let's say you're invited to be on Oprah And you don't have a problem But you want to go on the show, so you need a problem So you invent a problem But if you're not an expert in problems You're probably not going to invent a very plausible problem
> *(Laurie Anderson, "Only an expert")*

Looking at the above, we can do all sorts of 2x2 graphs and views and venn diagrams and polemics. But let's just look at one thing: identity. The state model delivers an ID which hints at some limited view over identity. But at their core, ID relies on and is perhaps a proxy for local custom, so it does little good across borders and even less good online. Worse, applying these models to the developing world is just rubbing more salt in the wound - KYC/AML systems that demand ID are corrupted as channels to know your victim, extort him and money launder the profits. And even if it worked, the people can't afford it.

The CA likewise delivers a certificate claiming some check over ID. Bank systems follow a compliance model delivered to them by far off bureaucrats without a clear meaning and without clear delivery of their stated mission, but like any religion, it is not necessary to understand and prove the model, belief is sufficient. The commercial companies selling trust similarly provide some basic tools then try and convince you that it will all work, as long as you trust them all.

None of these speak to identity.

CAcert created a system of identity pillared on protocols of assurance backed up by dispute resolution. Your Facebook Identity is the combination of weak links or data presented to another (name, photo but also friends in common and commentary on shared context). These speak to identity, but like the thesis suggested above, they are the weakest evolutions of reliance, the minimalist improvements on the machine. If our fate is to wait for these small improvements, then our fate is to be patient in the extreme.

II.4 Where are we on the 'trust' thing?

> I am not particularly crazy about the search for a definition, because doing this always means creating a conceptual limit. You could ask me, "What is a table?" And I'd answer, "A table has four legs and a flat top that kids can jump on." Now we have to clarify what the difference is between a table, a pony, and a horse. And by the time we are done, we will have to clarify the difference between animate beings and inanimate entities. That's what we get. The way I see it, every definition has a fundamental weakness: It excludes and limits.
> *(Heinz von Foerster, Understanding Systems)*

It is somewhat clear that this whole 'trust thing' is far more complicated than any venture capitalist would have the patience for. Let's summarise.

- Alice trusts Bob:
    - Each trust decision is particularly focussed on circumstances,
    - that builds from past information, and adds for the future,
    - to create a model in Alice's mind.
    - Trust then is both a momentary decision as well as repeated game.
- To define trust is risky, and indeed
    - Alice's model of trust is deeply hidden and personal,
    - we cannot model it nor interpose it.
    - If we could model it, we could break it. If we could break it, we will break it.
    - Trust is Heisenbergian - We can know it is there, but not what it is.
- Only people trust;
    - machines deliver reliance.
    - Machines are to deliver reliance over something worthy of relying upon.
- Alice's trust is economic:
    - Trust requires continual investment of a costly type,
    - which means the protocol has to deliver benefits back to Alice,
    - and thus Alice and Bob are naturally led to an equilibrium of trust.
    - It fails to be easily transitive - We can share data, or opinions, but not trust.
    - Which leads to two economies of scale - sharing and mutual reward.
- Most systems labelled as trust aren't up to the job:
    - State IDs deliver reliance to the state - state ID is not intended for you.
    - Courts deliver for local (western) communities, but are broken for developing world & Internet.
    - CAs failed because they said nothing of value over documents that weren't meant for you.

- - Web of Trust failed because it didn't say anything.
- Some notable successes:
  - CAcert delivered trust internally through
    - Assurance over own members, and
    - arbitration - its own courts.
  - Facebook facilitated trust between people through
    - many weak links - much memory;
    - less judgement - the machine that judges or sells is not worth our trust.

That all said, what can we say positively? The big 'trust' thing is that trust is in Alice's mind, and it is an integral part of her Identity. But it is also expensive, and economising means Alice wants to share the cost by sharing her identity, while maintaining the faith of Alice's defensive trust model.

Alice's personal network of trust is then a group. In order to understand Alice's Group, we turn to Part III.

Upbringing

3

Part III - On The Proper Upbringing of a Young Lady Named Alice

> Hiya Barbie
> Hi Ken!
> Do you want to go for a ride?
> Sure Ken
> Jump in
> *(Aqua, "Barbie Girl")*

What becomes somewhat clear from the earlier sections (Part I - My Identity and Part II - on Trust) is that Identity is not a single, simple thing - it is not a thing we can isolate and barricade, then study it to our academic heart's content, as we can with animals in zoos, aboriginals in remote villages or an archeology dig. Nor is identity something we can nail a number to and hope that trust, reputation, and knowingness in the sense of *know your customer* springs into life.

Rather, your Identity is spread primarily between your own mind and the minds of your immediate community - your group. Not a new observation, even in technical circles:

> Human beings have an innate drive to compete for social status; it's wired in by our evolutionary history. For the 90% of hominid history that ran before the invention of agriculture, our ancestors lived in small nomadic hunter-gatherer bands. High-status individuals (those most effective at informing coalitions and persuading others to cooperate with them) got the healthiest mates and access to the best food. This drive for status expresses itself in different ways, depending largely on the degree of scarcity of survival goods.
> *(Eric Raymond, "Hacking the noosphere")*

Anthropologists may shake their heads with amazement, but technologists are slow to learn. While we haven't nailed this down as yet, and may never do so, let us at least propose a working hypothesis, numbered 'x' for now because it's unlikely to survive:

```
Hx. Alice's identity craves to be shared with others.
```

In this section, we leave aside the parts of Identity numbered, appropriated and traded for commercial advantage. Our Identity is strictly that abstract thing within our self, combined with that mirrored thing willingly and hopefully shared with our friends of trust.

Trust! Which we've also established in Part II is a mechanism of some complexity.

We might then ask which comes first, Identity or Trust? An inkling might be emerging that they are very closely connected, and indeed, they might be opposing sides to the same coin.

But for the moment, we are on a journey to establish what happens when these forces laid out come together over Alice, our prototypical Identity. We want to answer the question - who will Alice trust to share her Identity with?

To answer that, we have to tease these forces apart. What follows is a pseudo-scientific explanation that I'm sure will have anthropologists and psychologists cringing alike - but hopefully the conclusion is sound enough for the humble technologist. Onwards!
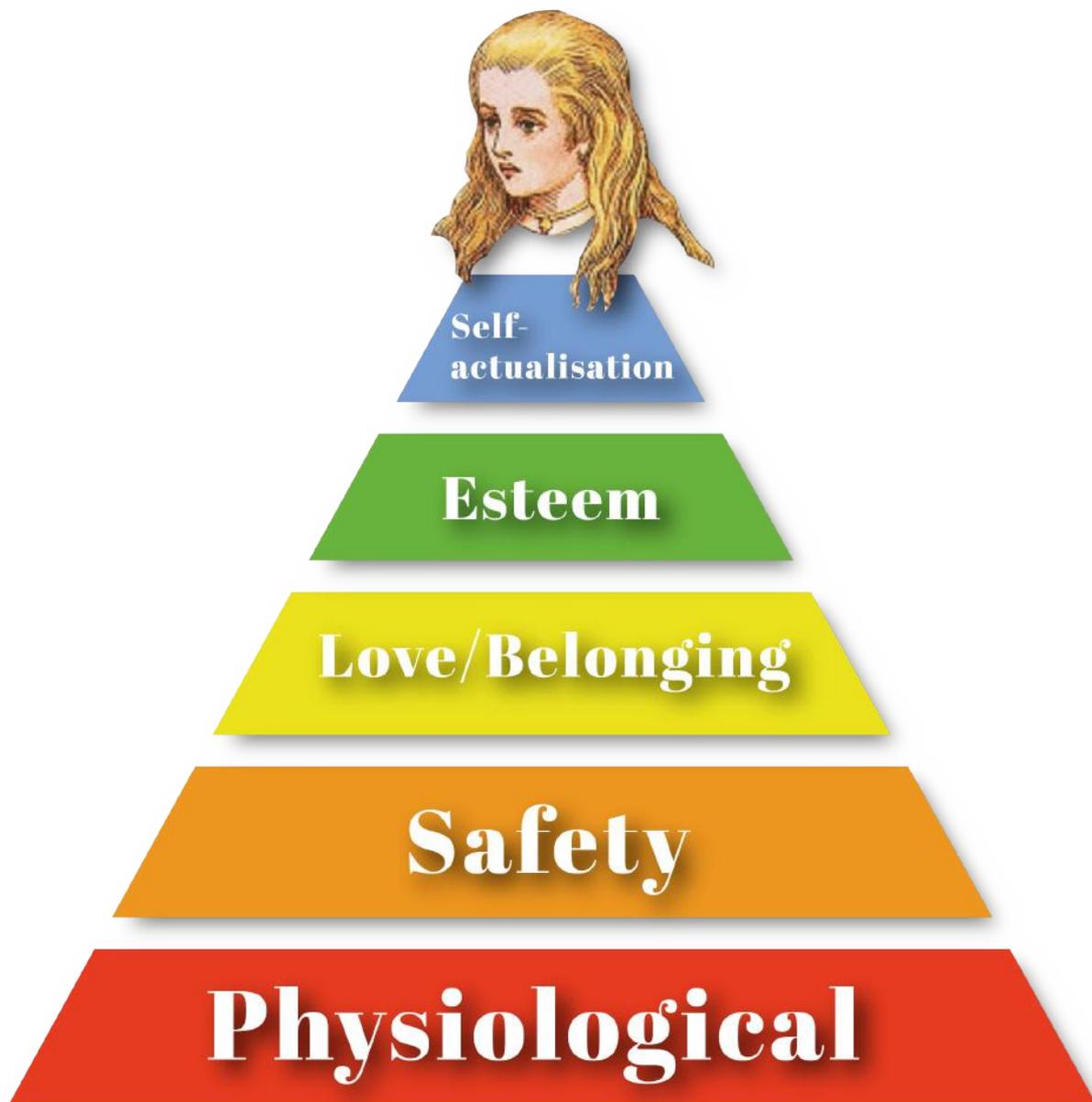
Figure 10 - Maslow's Hierarchy of Needs, revisited with Alice

III-1 Early Civilisation

The Sharing Thing

> I want to play cricket on the green / Ride my bike across the street
> Cut myself and see my blood / I want to come home all covered in mud
> I'm a boy, I'm a boy / But my ma won't admit it
> *(The Who, "I'm a boy")*

Your Identity by its nature has a need to share your self with your peers, and as much as is your need, they have a like need to share their selves with you.

Maslow's pyramid of needs suggests a complicated system of needs built into our psyche. We are not talking about Identity in a vacuum, there are forces at work: Safety and food come first, and these things are related to the wider quest for belonging and esteem, ultimately to self-actualisation.

Time plays a big part, and while it seems that identity speaks louder towards the top of the pyramid, it is not clear that we can say it is absent from the lower layers - safety and physiological. Is Maslow suggesting your Identity is a life & death issue? For now, let's agree that your identity cannot be seen in isolation from your very environmental circumstances. Let's ask - what those are?

A Very Primitive Economics

> Humans first lived in small groups on the African savanna. An artifact of this life is the fact that most people can't have serious emotional relationships with more than about 12 people, depending on how you define serious. :-). Think of it as the carrying capacity of the human 'switch', and things get interesting. These small groups communicated geodesically. When you wanted to talk to someone, you went up and talked to them. Then we developed agriculture...
>
> *(Robert Hettinga, "A Geodesic Society?")*

From economics and life, we know that we trade good for good, and that specialisation of labour is possibly the first law of economics that separates humans from the others: if I specialise in the making of shoes, I can make 100 good shoes in a day; if you do not, you might make a poor pair in a day that wears out the next - which effort will take you away from your specialisation of, say, growing chickens.

There's an obvious economy here. *"Most ways humans have of organizing are adaptations to scarcity and want."(Raymond, op cit)* In some sense, in a manner that we handwave over here, we should trade the fruits of our specialisations. We should combine our efforts, we should trade your chickens for my shoes.

```
Hx. Alice needs to combine her talents and labours into a
pool with others in order to survive.
```

So, how does Alice trade unlike for unlike?

Figure 11 - Presentation of a Rai Stone of Yap for the inauguration of the Federation of Micronesia

Civilisation, or 'Life in Cities'

> ...Then we developed agriculture and its resulting food surpluses, people tended to congregate at the crossroads of trade routes, and that's where the first cities began. Civilization means, literally, 'life in cities', remember? Once we had large groups of people in a single place, we had lots of information to pass around, but we also had expensive humans 'switching' that information who were only able to trust about 12 people at any time...
>
> *(Robert Hettinga, "A Geodesic Society?")*

The problem with this rosy picture is one of accounting - how do we account for the relative efforts of our labours, and in particular the relative prices between the goods, such that some socially beneficial measure is optimised? How do we surface the special from the mundane, so we can best focus our efforts?

```
Hx. The combination of talents & labours is fraught with
accounting difficulties - noise, error, laziness & fraud.
```

There are approximately four answers to this, and note that I invent words so as to focus your attention on the economic notions, yet avoid the politics and baggage that so often afflicts the economics debate:

Barterism - we trade unlike for unlike, so I might offer a pair of shoes for 10 of your chickens.

Tokenism - there is a neutral object that we all swap into and out of. Your chickens currently price at 10 seashells, and my shoes are 60 to the pair.

Ledgerism - we record my shoes into a giant book, and also your chickens, and we adjust at the end of the season.

Communalism - we all produce what we can, and our elders tell us what is needed, what to do, and that's that.

The problem with all of these is that they all suffer from some inordinate weaknesses. Barterism is very expensive, the 'spread' tends to be huge, and the goods available for trade today result in wastage tomorrow. Tokenism requires either the token to emerge naturally (gold? Seashells? the stones of Yap?) or someone to erect a money which already speaks to an organised society with *inter alia* a monarch, a military, a tradition, a repression. Ledgerism requires the invention of counting, then accounting and even writing. Pacioli's Double Entry Accounting required a high order of civil society in respecting 'the book,' and still, we required a unit of account in order to compare good for good.

Communalism does not scale - such a thing breaks down as soon as too many people are involved, and the censure of the group no longer keeps abuse in check. But it is in communalism that we see that Trust and Identity most resonate, and it is also the most historical.

The Village

> Identity comes from the intersection of belongings
> *(Michel Serres)*

If we imagine early society in tiny villages remote from external influences, or hunter-gatherer societies even further back, it is clear that the only workable arrangement is if everyone works together. Indeed, it is from the human ability to use our brain and work together that we first lifted ourselves above the others.

In such an environment, trust is essential because without earning the trust of the village as an economic unit, it isn't worth the village's efforts to carry the cost.

Without trust, the individual is outcast. Will starve.

And, that trust makes demands of all - including the elders that use their experience of the past to direct the activities of the youth to come.

```
Hx. Alice uses trust to choose who to share with and who to
listen to.

Hx. Alice uses relationships to tell her who to trust.

Hx. Alice needs to invest in deep relationships in order to
develop trust in order to choose.
```

This is really the topic of an anthropology study, but let's move quickly on. What's the cost of that investment that Alice has to make?
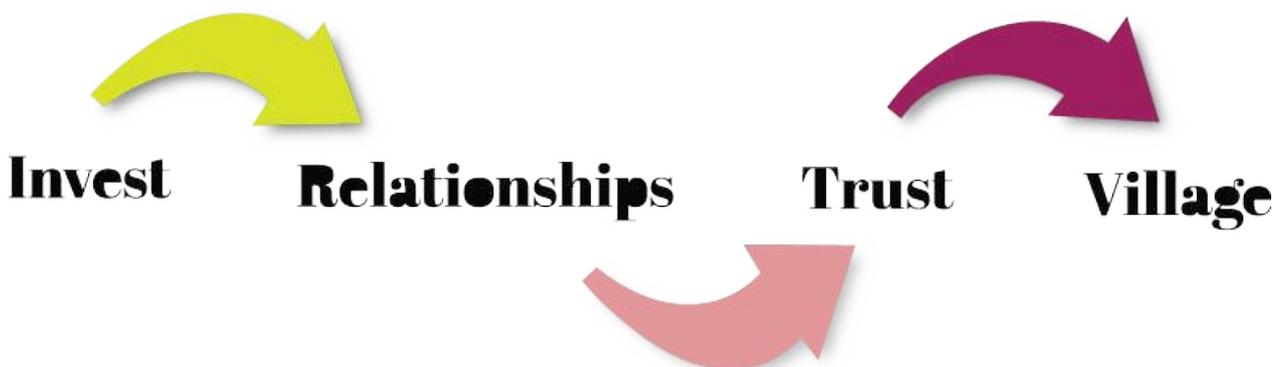

Figure 12 - Alice invests in Relationships to find Trust

Dunbar's Number

> The group size predicted for modern humans by equation (1) would require as much as 42% of the total time budget to be devoted to social grooming.
>
> ....
>
> My suggestion, then, is that language evolved as a "cheap" form of social grooming, so enabling the ancestral humans to maintain the cohesion of the unusually large groups demanded by the particular conditions they faced at the time.
>
> *(R.I.M. Dunbar, "Co-Evolution Of Neocortex Size, Group Size And Language In Humans")*

It is this image of the tiny indigenous society that makes Robin Dunbar's work so tantalising (Dunbar ibid). Robin Dunbar investigated the correlation between (neocortex) brain size and the size of groups in primates; by analysis, he suggests that

> ...there is a cognitive limit to the number of individuals with whom any one person can maintain stable relationships, that this limit is a direct function of relative neocortex size, and that this in turn limits group size... the limit imposed by neocortical processing capacity is simply on the number of individuals with whom a stable inter-personal relationship can be maintained.
>
> *(Dunbar, ibid)*

Therefore, he concludes, the human brain is sized for a around 150 deep relationships, which then suggests more tentatively that the natural group size for communities in pre-history times was around that number.

Dunbar himself suggests that the number is soft, putting the 95% confidence interval from 100 to 230, a very wide range indeed (Dunbar, ibid). Different calculations result in numbers within that range, so we take 150 not as gospel but as a sort of indicator - there is a number, and it's somewhere around there, and it's important.

This can be contrasted with modern research into work groups within civilised society. Above in quotes, Robert Hettinga suggests 12, and Christopher Allen investigates numbers as low as 4 (Christopher Allen, "Community by the Numbers, Part One: Group Thresholds"). Meridith Belbin said that 8 roles was the minimum, but team members could double up on roles, and so the minimum was suggested at 4 (Anthony Jay, "Nobody's Perfect - but a team can be").

But, modern team research is based on the assumption that everyone is safe, everyone has a job, all basic needs are cared for. Which world while arguably more relevant today is not as relevant when safety needs dominate. Which world are we investigating? The cozy world of the safe office, corruption free? Or the primeval village or hunting tribe? Or both?

No matter the scientific stretch that such an analysis predicts, including over assumptions of origin, the existence of a number rings true. Here, we take 150 as the canonical Dunbar hypothesis, but always remembering that Alice has a limit, and science does not tell us precisely where that limit is, for her or for her companions.

```
Hx. Dunbar's hypothesis says that Alice can cope with approximately 150
deep relationships, as determined by a natural limit on human brain size.
```

How many close relationships do you have? Or, more on point, how many *can you have*?
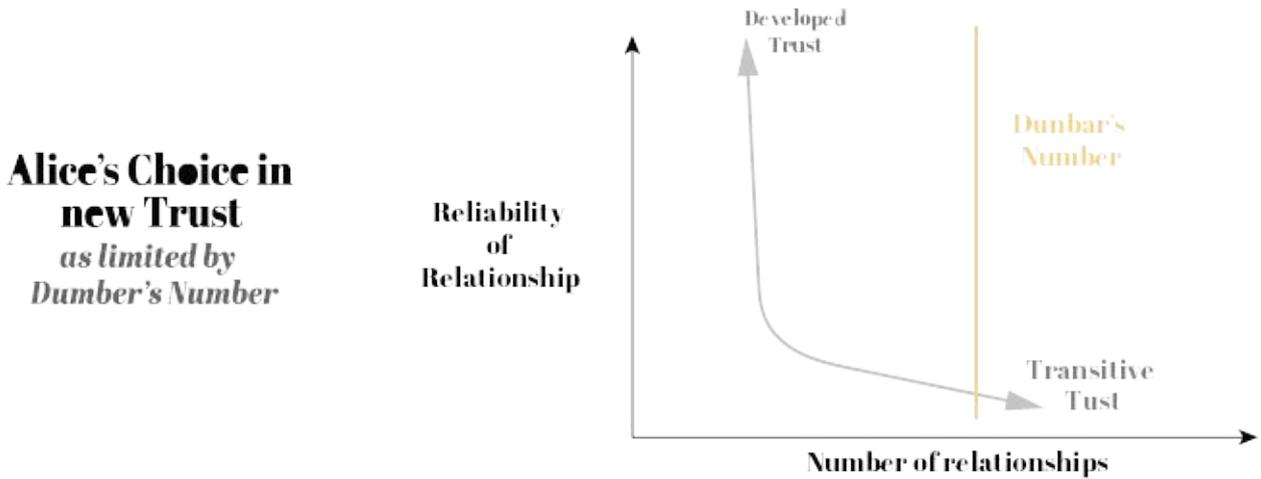
Figure 13 - Alice's Choice in new Trust, as limited by Dunbar's number

Scarcity

> So, we had to develop hierarchical 'networks', social organizations in other words, to move that information around. Notice we finesse the whole trust problem by using the entire hierarchy as one entity in everyone's trusted-person list. That's why people die for king and country, for instance, instead of just their family hunter-gatherer clan.
> *(Robert Hettinga, "A Geodesic Society?")*

It is by now pretty clear that we as humans have limited bandwidth to cope with too many deep, trusting relationships, and although we might debate any particular number, as a concept, Dunbar's number nails a very firm stake in the ground. No matter what we think or debate about the number 150 that Dunbar staked into the ground, the important point is that there is a limit.

```
Hx. Relationships are a scarce resource, and are therefore expensive.

Hx. Developing trust with people - which results in and from
new relationships - is expensive.
```

In pre-history, villages of (say) 100 to 250 people had a capability of surviving, absent aggressive neighbours. Towns that grew larger became more violent and therefore more organised, requiring governance mechanisms: authorities, enforcement, courts to resolve disputes (Gómez *et al*, "The phylogenetic roots of human lethal violence"). In contrast, smaller villages could deal with trouble by simply referring to elders.

Early history seemed to have worked as far as it could. As Dunbar's number was evolutionarily slow to change, the next step in evolution had to be: *economise!*

Alice Grows Up

Risk Mutualised

> I've been standing at the back of your life
> Back row centre just above the ice
> Please don't ask me how I've been getting off
> No please don't ask me how I've been getting off
> *(Divinyls, "Pleasure and Pain")*

Another factor that impacts Alice's life is the game theory of risk. In sharing her Identity, she takes on a lot of risk, indeed vulnerability. As we found in earlier sections, if she can organise to balance that risk to herself with a commensurate benefit or power over her friend, then perhaps there is a balance to be reached - her vulnerability mitigated by his vulnerability.

```
Hx. Alice risks her Identity with Bob if he likewise risks his Identity.
```

This is the prisoner's dilemma, on steroids. If Alice and Bob mutualise their risk in each other, they can reach for that small element of trust that is based on knowing that the other cannot abuse, without also opening up to a one-sided exploitation to vulnerability.

Figure 14 - Trust and Identity are Yin and Yang

Yin & Yang

> that we are each other's
> harvest:
> we are each other's
> business:
> we are each other's magnitude and bond.
> *(Gwendolyn Brooks, "Paul Robeson")*

And, as we saw in Part II, the development of trust is not a one-off thing. Rather, it's a cycle of events, of which the cornerstone is a pact of mutually vulnerability. Each stone, each cycle, develops more trust, as each exposes more identity. Trust from the previous round is intent to share identity in the next. As it is with the village and its resources, your identity then becomes the result of your experiences over the years of your life within the game of trust - your identity is the sum effect of your exposures of identity, and your trust in others is your sum result over your yearned attempts to acquire their trust in yourself.

Yoda would say: deep, it is. Recursive, circular.

There can be no trust built without shared vulnerability to identity.

There can be no sharing of identity without expensive, shared, vulnerable trust.

That which isn't vulnerable cannot support trust. That which isn't trusted should not impact identity, leaving aside abuse:

There can be no self without vulnerability to others.

Other terms might apply - dependency, loyalty, ownership, patriotism, but there is something special about vulnerability and the trust and identity that are derived from that vulnerability that promotes it as mutual and shared.

There can be no identity without trust, there can be no trust without identity.

The mystery of identity, relationship, vulnerability and trust is then solved by considering them all together and related! However, this does not tell us how we unravel it, and perhaps the solved mystery is even more mysterious!

Let's delve deeper. Let's go back to the beginning - where is the start of Alice's Identity, her trust, her everything? In the beginning is Alice's parents.

The Family

> So now I'm praying for the end of time to hurry up and arrive
> 'Cause if I gotta spend another minute with you I don't think that I can really survive
> I'll never break my promise or forget my vow
> But God only knows what I can do right now
> *(Meatloaf, "Paradise by the dashboard light")*

At one extreme, marriage is the ultimate expression of trust. When we marry, we mutualise ourselves in the other, to such an extent that we combine the power of two in mutual trust to have children and bring up those new members to full contribution to society.

Or, so we are taught as children. And, sadly, that strength of mutual trust, and the identity shared within, is proven in the breach - divorce shows us what we lose, giving new irony to the term - the Prisoner's Dilemma.

But, assuming happy tidings for the moment, and leaving aside the investment of the parents, let us consider the newborn child that comes out of this happy union.
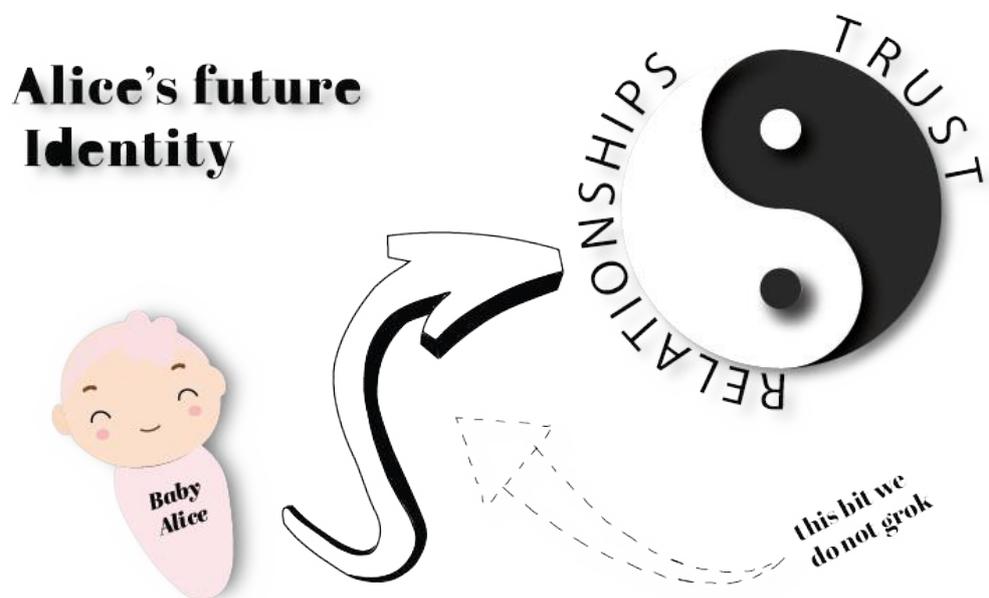

Figure 15 - The Mysterious Growth of Identity to Trust and Relationships

Baby Alice

> And when a child is born
> Into this world
> It has no concept
> Of the tone the skin is living in
> *(Youssou N'Dour and Neneh Cherry, "7 seconds")*

Baby Alice starts with no identity. The challenge of Alice's future Identity is how the empty vessel of her mind is filled to the point that she can trust, she can relate, and she can produce.

The secret is that she is given a full-trust substitute called love. The child learns her first relationship drowning in love and Mother. Closely followed by relatives: Father, siblings, grandparents and whoever is to hand in Mother's trusted circles. The initial interaction of trust and identity is within a close-knit training unit called the family, in which love is assumed, trust is not in doubt, relationships are granted and therefore identity can grow apace. Alice's identity is shared with all of the family, as theirs is with her.

```
Hx. The family is a training unit for Alice's Identity,
giving her free relationships to experiment with
and build upon as she creates her trust model.
```

That investment in costly love contributes directly to the new baby becoming a child, then a teenager and finally an adult with her own model of trust, her own identity, and her own self within and shared with the family. At an age of productivity, our now-adult is fully trusted, fully trusting, and is ready to return on investment.

```
Hx. Growth within the family results in shared mutual vulnerability,
trust, at the adult level.

Hx. As a residual outcome to the training, the family retains Alice's
trust as a natural economic unit within which it can exploit economies of scale.
```

And, or as a reflection of which, is also of the age to marry, and so the cycle begins again. Is it a coincidence that the moment Alice's identity is ready to explore the world, bursting the bounds of close-knit family trust to try out her personal trust model on the nearest other, the family turns to the task to marrying her off?

Probably not, and no less of a coincidence as the relationship of brain size to love - the larger the brain in Dunbar terms, and the emptier it is on birth, the longer the time needed for Alice's Identity to build. And therefore the more investment needed by her mother to create

that journey, firstly with love, then the learnings of language which Dunbar suggests as *"a 'cheap' form of social grooming."* Finally we have proven the old saying - that love does really make Alice's world go around.

The Extended Family

> Desmond has his barrow in the market place
> Molly is the singer in a band
> Desmond says to Molly "Girl, I like your face"
> And Molly says this as she takes him by the hand
> *(The Beatles, "Ob-la-di Ob-La-Da")*

Beyond the simple family, there is the extended family. Having been brought up, an individual is within and trusted by parents and siblings, but also by grandparents, uncles & aunts, and cousins. An extended family, in those cultures that celebrate this model, can grow to 30 or more.

> It takes a village to raise a child
> *(Igbo / Yoruba proverb)*

Why does this work? Let's speculate that the answer lies in the economics. If the foregoing discussion of the simple family has merit, then we should look to the transitivity of relationships, the building of trust and the economics of investment.

That trust which a mother has with her daughter also passes to the granddaughter - for free. It may seem strange to call it out, but there is clearly a transitivity from one member of the extended family to the next - the new born child automatically receives the trust of every member of the extended family.

Further, the granddaughter can be a shared investment of the mother *and* the grandmother, creating economies of scope and increased specialisation.

The return on grandma's investment in fast-tracking solid relationships into Alice's Dunbar slots accrues to the family. Which suggests that the larger the family, the more efficient is the economic unit. In this sense, the investment might be higher in gross for the extended family but is also spread across more people, returns more productive people-units, enjoys more economies of production.

Other things being equal, the extended family should be a better economic unit, and should dominate. Other things are not equal, and Dunbar writes:

> Among primates, the cohesion of groups is maintained by social grooming; the time devoted to social grooming is linearly related to group size among the Old World monkeys and apes. To maintain the stability of the large groups characteristic of humans by grooming alone would place intolerable demands on time budgets.
> *(Robin Dunbar, Co-Evolution Of Neocortex Size, Group Size And Language In Humans)*

suggesting that the larger family is simply inefficient, for too much grooming, love, attention.

Neither space nor knowledge permits us here to say much more, but it is rather fascinating to ask why the extended family survives in the east, but not in the west - is this because of relative wealths making returns on multi-generational investment unnecessary? Or is it the result of strong propertarian legal traditions, undermining some implied contract of birth? Or, in a complex and fast-changing society, are there more returns to be had by *not* following the dictates of the old, and opening the Dunbar bounty for new, interesting and exciting others?

Childhood Forever

> We are what we're supposed to be
> Illusions of your fantasy
> All dots and lines that speak and say
> What we do is what you wish to do
> *(Aqua, "Cartoon Heroes")*

In the pursuit of curiosity, we can also ask: why is the upbringing phase of humans so long?

The answer might be that in order to develop the trust and identity that make advanced economic accounting possible - trading shoes for chickens and benefitting from the specialisation of roles - humans need *both* a powerful brain *and* a large brain.

Power: The depth of processing needed for each of those relationships remains mysterious to us, and following earlier comments on the trust model, the relationship may be impenetrable by definition, which speaks to a very powerful brain.

Quantity: The size of the neocortex indicates 150 slots for relationships, being a pretty large number for primates.

Multiply the breadth of the Dunbar slots with the power of the relationship - language, memory, accounting, trust and identity - and this alone suggests why children take so long to mature. Dunbar's hypothesis suggests that our children's heads are very big, and take a long time to fill.

But after that is done, and Alice bursts out onto the dating scene, her identity is free and under her own control, right? Apparently not.

Figure 16 - Maslow's Mesa

Alice enters Society

Alice the non-savage

> Don't want no paper gangsta
> Won't sign away my life to
> Someone whose got the flavor
> But don't have no follow through
> *(Lady Gaga, "Paper Gangsta")*

Because Alice needs to specialise, she needs trusted relationships to trade. To develop trust, Alice needs identity, to share and grow in a never-ending cycle to build the yin and yang. To bootstrap her identity, Alice's family smother her with love and belonging, until her identity can take root.

As a consequence of Alice's upbringing, Alice has 20-odd years practice in sharing her identity and building her own capability to do the trust RADR loop by herself. If it took her parents and others in the village those 20 years of investment in selfless identity sharing to bring Alice to this point, then this level of investment has consequences:

```
Hx. Alice has to belong.
```

By Darwinian induction, Alice herself is imbued with a need to selflessly share herself with others and find new and deeper trust relationships. Without that viral pay-it-forward, the species wouldn't exist. Maslow's pyramid would be a mesa, Alice a savage and our topic would be about how to kill more wild animals, not how to win her trust.

Further, by training, Alice is imbued with a desire to share with something like her family.

```
Hx. Alice looks for her family.
```

It's true that marriage is on the horizon, much talked about but actually not what she has been trained in. For other and mysterious reasons, she'll have to pick up some new spousal skills fairly soon, but these aren't particularly helpful in our investigation into identity.

What we really want to know is *how she belongs*.

Economising on Trust

> The amount of social capital you have is pretty fixed. It involves time investment. If you garner connections with more people, you end up distributing your fixed amount of social capital more thinly so the average capital per person is lower.
> *(Maria Konnikova interviewing Robin Dunbar, "The Limits of Friendship")*

Notwithstanding the questions and the polemic of simple versus extended families, we can suggest that the (extended) family extracts economic power from the automatic adoption of the child into the family, which fast-tracks her mutualised trust and identity over time with a wider group of people. The ability for Alice to trust Carol, her mother, and have that automatically extend in great measure to her aunt Eve is a valuable thing.

It might also be the case that the transitivity of this trust - mother's trust of her sister passed on to her daughter - is the benefit, rather than the cause of other economies. That is, Alice acquires from her upbringing a capability to exploit Carol's trust in Carol's sister Eve for Alice's own decisions, which yields the profits which make the family more viable. If Alice trusts Bob and Bob trusts Dave, then Alice can use Bob's trust to augment her own risk analysis over Dave.

At a further level, Alice's trust of Aunt Eve through Carol brings Alice to a new skill - how to learn to trust. Alice has no choice but to trust mother Carol, but Alice's trust of Eve is mediated by her Mother - cuddle by cuddle, nod by nod, word by word, mother transits trust to child.

It should come as no surprise, and it is indeed essential to the development of Alice's core identity that life is a progression of people, with each of whom she has to do a risk analysis over the signals she is presented. First mother, then father, then siblings, grandparents, aunts, uncles, and various cousins and additional players. As well, people not related - some with transitive familial trust, some with none - the procession of players in the village is Alice's training ground to learn how to trust, whom to share her identity with, with whom she feels a sense of belonging.

It's expensive, but it's a reality, and if Alice wants to get off of Maslow's mesa, she has to learn to open up. Alice has to learn how to be vulnerable.

How Alice Opens Up

> "Did it occur to you Circle people, ever, that we can only contain so much? Look at us. We're tiny. Our heads are tiny, the size of melons. You want these heads of ours to contain everything the world has ever seen? It will not work."
> *(Dave Eggers,* The Circle *)*

There are many challenges to this as a general model. Clearly, there are two poles of trust: in the extended family, the assessment is golden, but two people passing on the street might have zero expectation of a good assessment. How then does Alice achieve an assessment as valuable as her extended family's trust across a broader range of people?

There appear to be three or four answers.

1. Develop. The baseline answer, as suggested above, is that Alice invests in a new relationship, as she's been taught in her upbringing. This is expensive, perhaps so expensive it can be seen as a rarity. Alice can use her family-taught RADR loop, she can share vulnerability to develop this trust, but it requires hours or weeks or even years of effort. Not only that, she might be hitting up against her Dunbar limit.

Of course this happens. People meet strangers, and 10 years later they are no longer strangers but friends for life, colleagues in business, married or otherwise joined in mutualised sharing of risk and identity.

But it is so expensive that we count these relationships as treasures - one spouse, 10 lifelong friends, 100 people in our narrow address book.

2. Transitive. Alice asks Carol for an assessment on Dave. This works, but it is weak, as the assessment only transits two hands. Alice trusts Carol's assessment of Bob because she knows Carol very well. But Alice is highly skeptical of Carol's assessment of Bob's assessment of Dave. For some reason, two hands works, and three does not. Notwithstanding that everyone is linked by 6 degrees, all but the first and second are practically worthless for the topic here - Alice's trust - which might explain why some social networks are all bark and no bite. Indeed Granovetter's theory of weak links (*op cit*) stresses the paucity of this - it only provides for a weak basis, it assumes that everyone is trustworthy, and it is only good for low value information transfer. Not trust.

3. Group-wise. If two people mutualise their risks with a third - at a comparable level of trust - then they can economise on the costs of analysis and even their risks. Three people is more efficient than two, and four people can share more than three.

Which leads to the group - if there is an economy in sharing a risk, this creates a natural force to create a group. The economic way to achieve high trust might be within a group where the ground rules are oriented to that task - sharing, trusting, transiting.

In some sense there are economies of scale in groups that allow Alice to push past her personal limit as imposed by Dunbar's number and the cost of deep relationships. We know that depth trades off against quantity, and therefore there is a curve of natural limits; in some sense yet to be fully understood, Alice's group pushes that curve outwards. And we know that Alice was trained in a group called her family, which suggests precedent.

```
Hx. Alice is comfortable with groups.
```

This hypothesis states that the natural attraction for Alice is to mutualise herself in a group because of the economies of trust, which leads to more trust and therefore more trade and as a consequence, deeper identity.

Alice possibly wants a few groups in order to avoid capture, or possibly not, as the group is likely an expensive investment. It's worth stressing that a group is more similar to her family experience, a point we return to later on.
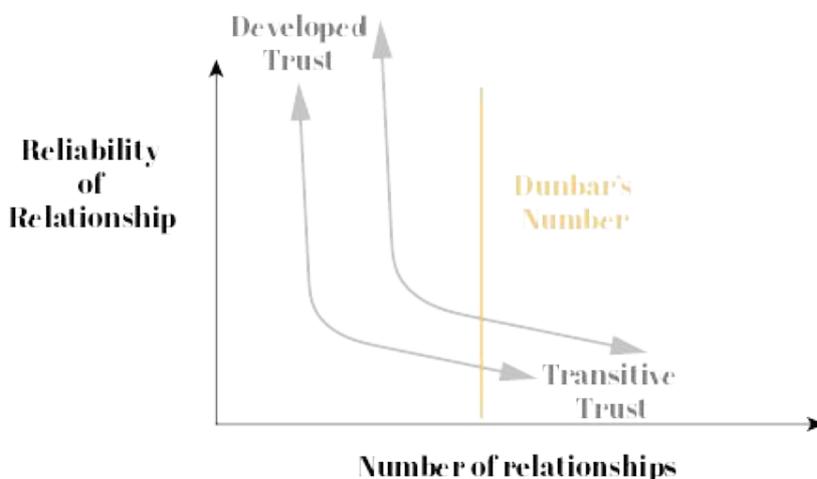
Figure 17 - Alice joins Groups to Mutualise Trust, and thus escapes the tyranny of Dunbar's Number

4. Institutions and Symbols. Some readers will leap at the absence of society and brands and institutions in this discussion.

That absence is deliberate. Although an assist in modern life, it assumes a basic level of cooperative society, which is not always consistently present. E.g., Kibera does not have the level of behaviour expected by say Londoners, and in contrast, modern corporations in the west are often mired in scandal and fines which developing world corporations are unimpacted by. The Internet does not deliver a reliable substrate of reliable behaviour, and institutions and symbols mean less.

Further, the presence of reliable institutions reduces the need for Alice to deploy all of her wiliness in developing trust - while a good thing in general, it hampers our ability to discover how trust really works. For the purposes of this endeavour, we concentrate on places and scenarios where there are few or none institutions of trust.

Alice is her group

> "If you want to go quickly, go alone. If you want to go far, go together."
> *(Old African proverb)*

Alice endeavours to bind herself into groups because it is a more efficient use of her Dunbar capabilities and other limitations, but it still hits up against Dunbar's number.

For example, if personal verification of all her relationships is a requirement, as it is for Alice's view over Bob, then Alice can only know 100 or so people at a useful level of confidence, and Bob can only know a further 100 others.

She can go further if she trust Bob's recommentation. In this transitive process, through her network, there is an upper limit on her trust of 100 * 100 people. In reality the actual number would be much lower, as generally many of the friends of Alice's friends will be her direct friends too.

If on the other hand Alice joins a group, and each of those groups is say 10 people, she gets transitive access to 10 * 100 people, for the price of one relationship - being the relationshop with her group. Alice finds it economical to invest in her group over say one more friend.

Further, if we assume that groups can trust each other, for example, by Alice and her friends joining two groups each, then the groups can act as transitive vectors as well. If each of those groups is say 20 people, then Alice's group connects to 20 other groups. Each of those, now being trusted, can refer transitively to 20 * 100 people, and combined we get four times the size that Alice and Bob could do alone. For the price of 2 relationships, her web of trust has exploded.

In reality, the numbers are much lower than the limits because of overlap. Also, Alice and Bob are busy people and already have families - in effect Alice's Dunbar slots are already filled, and to make room for another hyper-trusted person, she has to eject someone dear and loved. Further each group is likely a bigger investment than a single person.

Still, when it comes to identity, it should be clear that, aside from her own family, Alice's groups are a more attractive investment than a single random person.

Conclusion

What is Alice in Isolation?

To summarise. Humans:

- Specialise in trade to achieve economy,

- which requires deep relationships in order to negotiate trustful deals.

- Deep relationships need a large brain size - thought to be limited by Dunbar's number to around 150 deep relationships.

- Teaching Alice to use these deep relationships themselves is costly.

- Leading to the long term family unit as the basis for society,

- which bootstraps a Maslowian pyramid of needs into Alice.

All of which establishes that there are strong supply constraints on deep, trusted relationships. Which is upsetting to Alice, as she has strong demand for depth. Alice wants to trade, Alice wants to relate! To economise, then:

- Alice is a member of her family.

- More, as an investment of her family, she desires to return the investment.

- Alice needs to establish trusted relationships outside her family to support her self with her Maslowian challenges.

- But every new deep relationship she enters is limited by Dunbar's number and the cost of maintaining that relationship.

- To deliver economies, Alice mutualises her efforts on relationship to work with a third person, and a fourth, and so on,

- and is therefore heavily incentivised to join groups of like-minded people so as to maximise the direct mutualising benefit.

The natural economic sweet-spot for trust then is found in a strong, mutually bound group. And thus, Alice's identity is inherently bound up in the need to share her self with that group, knowing that all in the group are also sharing the risk. Alice is nothing in isolation; Alice is more within her network, and Alice is everything in her group. Alice's identity is the sum of her groups, and each group is the combined identity of her and her companions.

Alice, revealed

> I've been through the desert on a horse with no name
> It felt good to be out of the rain
> In the desert you can remember your name
> 'Cause there ain't no one for to give you no pain
> *(America, "A Horse with no name")*

Why have we taken so long to get to here, to reveal Alice? Because it is impossible to reason about trust and identity without reasoning about the group. Only in the place that trust and relationship and vulnerability are actually used at a high powered level - in Alice's family and her groups - is the context established that allows Alice to share her Identity, and for us to consider what that means.

Nowhere is this clearer than in Alice's proper upbringing within her family. To understand the group factor, we had to walk a long mushy loving romantic path from baby to adult. The evolution of Alice's ability to work a relationship, swapping trust for vulnerability, and building up Identity *within her groups* is something we all know because we're all Alice at some level. But, having internalised it as childhood, science has blinded us from seeing identity as anything but science.

When it comes to childhood, we've forgotten what we've forgotten. Diving back in, we've found that everything works well inside the extended family, but transitivity is heavily limited outside. It is probably fair to say that Alice can trust Bob's assessment of his friend a little, but no further; therefore we are likely to say that high trust levels can only deliver when many people know each other. Where, we feel we can do better than 10 friends. Numbers like 100 resonate not because they seem elegant but because we know that high trust groups such as extended families reach towards that number, but 1000 is clearly beyond expectations.

Which suggests that when high trust is needed, either Alice falls back to her family, or Alice finds a group in which she can develop sufficient mutualised risk-taking to set a level of trust *and* to share her identity. In a sense, the group is Alice's simulated family, and as against her groups, there's nothing that compares.

Alice on her Island

> I'm worse at what I do best / And for this gift, I feel blessed
> Our little group has always been / And always will until the end
> *(Nirvana, "Smells like Teen Spirit")*

The import of this chapter is to lay claim that most of the world's understanding of identity systems have got it wrong.

Either, systems have assumed a stronger person-to-person relationship than has been plausible (they exist but Alice isn't sharing), or, they have assumed Granovetter's theory of weak links, and have agglomerated a massive database of these weak links. Similar but worse, institutions have built their systems on state or corporate data sets, and loaded up more trust over the data than it possibly supports. All of these endeavours are in a state of sin because their assumptions are not validated by Alice's reality.

Alice's group is the key. It was perhaps this insight that inspired Reed's Law - the group forming network was the one that wins (David P. Reed, "That Sneaky Exponential").

Alice's groups are *islands of trust* for her Identity. Having discovered that, we can now ask: How big is your island? What happens on your island?

And, how can we help? What can we do, the humble builders of tools, to help your island prosper? We know that your groups are your castle, your island, your bailiwick. Small in number, small in members, but high in trust, relationship, they are your self.

Our goal is not so much to protect your Identity or gain your Trust because you've already cracked this problem - this view shifts up a step in the scheme of things. Our goal is to help your island with its identities, its members, the interactions and the trust between them. The system is the island, our goal is to provide some tools and driftwood for you and your peers, so you can build your own island.

It is to *the group* we explore next.

4

Finding Alice

Part IV - Finding Alice

> From the moment I could talk, I was ordered to listen
> Now there's a way and I know I have to go away
> I know I have to go
> *(Cat Stevens, "Father and Son")*

Our challenge from Part III is to find a group worthy of Alice's attention. She needs it because in the normal course of modern life, she has left behind her primary group, generally by the normal course of growing up and becoming "too big" to fit comfortably into what has clearly become the group of others.

Like all young adults before her, Alice rebels, leaves the family, and goes off to seek both her fortune and her freedom.

Yet, the essential home of Alice's Identity remains in her groups, as a proxy or augmentation or replacement for her family. Alice needs an environment so trustworthy that her identity can grow within. We'd also like a structure that is widely accessible - Alice wants to travel the world, and to discriminate against her because she's a modern woman is just unreasonable.

Having established that groups are the core expression of Alice's Identity, we can ask many things but key amongst are … which groups? How are they structured? Where do we find them? And these turn out to be surprisingly hard questions.

Up until now, we've used a pseudo-scientific approach to lay out Alice's identity, her trust mechanism and how she discovered the yin and yang of both - through her upbringing in, and as part of, trust, that led to the evolution of her identity.

But at this point, I face a pseudo-scientist's block. Like a writer's block, I cannot proceed on the basis of logic or science or empiricism, because I don't know how I made the next leap, other than to wave at broad and sweeping platitudes such as David Robson's "how east and west think in profoundly different ways". I'm left with blind luck and anecdotes, and therefore the time has come to inflict them on the reader.

Anecdote time!

Figure 18 - "That's quite enough—I hope I shan't grow any more"

IV.1 Anecdote Time!

mPesa or Bust!

> "kitu kidogo"
> *(Swahili request for a bribe - "and a little something for me")*

On the invitation of an old mate, Ken Griffith, I travelled to Kenya for a week in 2012 to check out the scene. Now, as we all know, Kenya was the birthplace for that economic miracle known as mPesa, and it was Ken's thesis that this was our bright shining star guiding us to the next generation of financial cryptography. I'll let others be the judge of whether that happened!

Kenya is an amazing place. I'm not saying that in the sense of "fantastic" or even "good" but in the sense of "completely different" to the westerner and oh so interesting. It has a booming economy, and the main streets are lined with crowded informal vendors selling anything you can think of. It has massive levels of corruption - where you and I might hear the occasional story of a corrupt politician, in Kenya it's the opposite. Kenyans know and Kenyans act as if everyone is corrupt, top to bottom; Kenyans hear the occasional story of an honest politician, or of a road being built. I kid you not - there was a new highway being built just back of our place and the actual construction of it was a local marvel.

Because, it was actually happening, the road was getting better and better. This is a mindshift that westerners don't really get. You have to be there. The whys and wherefores of the highway are for another anecdote, but the axiom is this:

```
Everything is corrupt.
```

Trust me vicariously, and keep the thought in your mind.

For me this was fascinating because pervasive corruption gave so much grist for the mill - how does this work, how does that work, when nobody can be trusted? I got that mothers were fanatical about getting their children to school. I got that husbands, brothers, children, teachers, bureaucrats would simply steal any saved money. I got that the mothers handled the finances and ended up in control of everything. I got that all officials were practiced in the phrase *"kitu kidogo" and a little something for me*… I got that informal was the only formal.

But in that wild-eyed Alice in Wonderland sense, none of it made sense, because from my small Western-economics mindset such an economy should simply collapse. Right?

Now, one evening, I was told some of this by a rare person, Warigia Razia. She was educated, from a wealthy background, but had a deep sense of understanding. And Warigia could explain herself. By some stroke of good fortune, I asked what was bugging me about the whole thing:

```
"OK, but how do you save?"
```

This was the key question as I recall it because although every detail made sense, put together it left a great gaping hole. If the husband drank away the money, how did the school fees get paid? These were due in January (two thirds) and July (one third) and they obviously required planning. What happens when medical emergencies hit? What happens when you need to travel and the kids have stolen the money? What happens when... And on and on went my vicarious confusion at living the life of corruption.
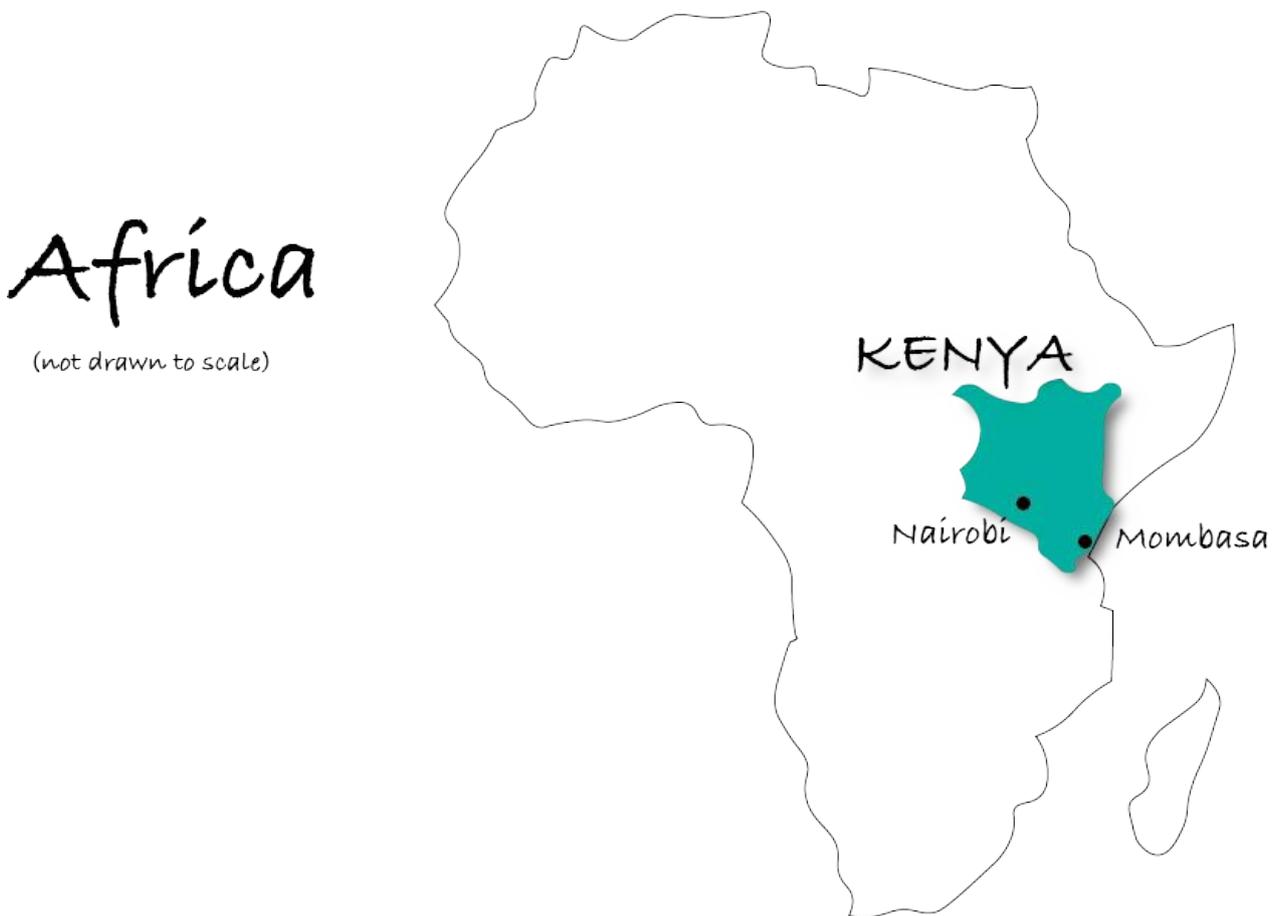

Figure 19 - Kenya!

How Do We Save?

> "Was told a very interesting story by the Central Bank Governor: Turns out that, for one of the mobile phone credit services, up to a third of loans are taken between the hours of 3 a.m. and 5 a.m. Most are repaid within twenty four hours. When the CBK dug deeper into this statistic, here is what they found out: a mama mboga (fruit and veg seller, for the non-Kiswahili speakers among us – typically a woman) will be awake at that hour, and borrow around 5,000 bob.
> She will then send money to her wholesaler at Marikiti. Once she's placed her order, she then sends money to her mkokoteni – handcart – dude, who knows where to drop off the consignment. She then wakes the children up, prepares them for, and dispatches them off to school. She then calls her nduthi – motorbike – guy, who picks her up at home and drops her off at her trading location. She trades all day, and by evening, repays the mobile loan, only to begin the process again a few hours later."
> *(Wallace Kantai, "Why Most M-Shwari Loans Are Taken At 3:00AM In Kenya" 2017)*

People in Western civilisation generally save by using banks.

Banks require a bank account - something that once was just a utility in the service of the public, but now has morphed to a major vector of control over the disadvantaged, whether they be the poor, the unusual, the foreigner or the small employer struggling from the central banks' blunderous handling of the great financial crisis.

We have neither time nor patience to document the fall from grace of banking, but permit me to slide in this one digression, as this cycle is about identity: when I was young, my bank gave me my first *"identity"* in the form of a passbook. To use the words of modern anglo-style banking, and see Part I - My Identity to disambiguate.

Nothing went wrong, no juvenile terrorists were running around pulling wings of flies, nobody was laundering money in my school canteen. The very austere gentleman - my image of him places him at about 20, but my memory casts him as an ancient wizard of finance - wielded a monstrous portable calculating machine that printed actual calculations on my passbook.

He turned my pocket money into lines in my passbook. And back again. He didn't tell me how that worked.

And nobody's permission was asked, which isn't the case in the English-speaking world anymore as bank accounts are now inordinately hard to open. Apparently banking as a service still works in places like Germany and Austria, so the concept of banking as a service to the public isn't totally lost in the Western world, but we can only hope they resist.

The West's Three Answers

SECRETS ARE LIES

SHARING IS CARING
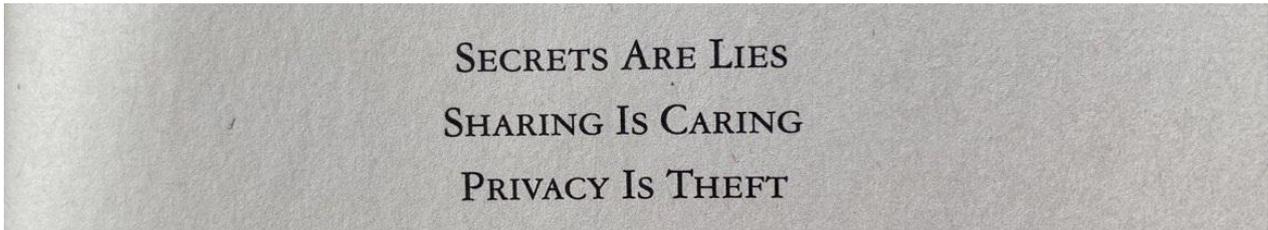
PRIVACY IS THEFT

(Figure 20 - "Privacy is Theft" (Dave Eggers The Circle *))*

Back to the point. The point of this slight digression is to ask: *how we save.* Unfortunately in the West there are two answers. One, the politically acceptable version, is that, at banks, you can save. If you're allowed, permitted, accepted, barriers so usual that you question your own identity.

Permission, as applied to your "identity" in the view of the banks, is paramount. If you're not identified, you're out. If your identity has a spotty record, you're suspect. If you're new to this, and as a consequence, you have no credit history, you're screwed. If you move around, you're not setting down roots, you're not one of us, we can't help. If you talk Bitcoin, you're black-listed. If …. The reasons are many, evolved, hidden, discriminatory and evidence of the worst of humanity.

And another answer, in evolving, developing painful history-now, is a range of methods, *but not at banks*. Greeks don't save at banks; as the bondmeisters moved to de-cash Greece in the aftermath of the GFC, the locals reverted to traditional means. Cypriots don't save at banks. Nor Venezuelans nor many other Latam countries. Russians are wary of their banks, although 1998 is a long time ago. Indians save in gold and in cash, still.

One way to tell if countries save in banks is to walk around the suburbs; if you see houses that have flat roofs, with 'rebar' (the metal bars that reinforce concrete to make it really strong) sticking out at each corner, that's a sign. The owners of the house are saving by building their house; as more money comes in, they build another floor. Somewhere in a corner might be a pile of blocks or other building material, waiting for the next opportunity. If the people are doing it this way, they don't trust the banks.

Germans still remember hyperinflation. Asians likewise recall the Asian financial crisis, and the West cringes at the global financial crisis of 2008, which for the life of all of us has never been resolved. Are we still in it? Or are we in another crisis? Australians and Canadians weren't, they are just now getting around to booking their housing collapse, as their private lending bubble starts to pop.

Actually, in the English-speaking world, the savings rate isn't so good anymore, so we don't save at all, whether at banks or otherwise. What we do is take on debt, private debt, and lots of it. Whether it be student debt, car loans or mortgages. Ask any student in the English-speaking world who's traded a degree for lifelong debts, debts are not a pretty sight.

Africans don't trust their banks - more on this as we go. Indians do trust their banks, but nobody can figure out why, following Modi's demonetisation disaster. This doesn't stop them saving in gold, especially for life events such as marriages. Germans remember the Reichsmark, and don't trust their money, nor their major banks. But they do retain a network of small local cooperative banks that support about a third of the market, and those are trusted (See for example "Community Banking in Bavaria" on youtube).

Which is to say, "how do we save" is becoming not just a question of idle cocktail conversation in a dinner party in Nairobi, it's becoming one of the future issues of the planet. We do not have a good answer, not any more, not since 2008.

But I wasn't thinking about that when I asked her, I was thinking of Kenya, corruption, school bills, dreams and thefts, and banks that could not be trusted, I was thinking, "how do YOU save?"

Chamas

> "kidogo kidogo hujaza kikapu" *(Swahili expression)*
>
> "Φασούλι το φασούλι, γεμίζει το σακούλι." *(Greek expression)*
>
> "Little by little fills the basket" *(Translation of both to English)*

And Warigia told me.

> "We have our chamas."

This single answer opened my eyes to the wonderful new old open secret world of Kenya's informal economy. I can't recall the words of the conversation, but I can lay out the chama thing as best I understand it.

Chama simply means 'group' in the dialect of the region (called *Swahili*) and every other region has its own name - in Uganda, Nigeria and the Caribbean they are called *Susus*, in the Caribbean *hand-outs* or *asu*. In China, Vietnam and Korea, it's a *Hui*. In India they call it a *bishu* or *chit fund*. *"In Ghana, it's popularly known as susu. In Cameroon, tontines or chilembe. And in South Africa, stokfel."* (Ken Banks, "Mobile Finance: Indigenous, Ingenious or Both?")

Chamas - the name I will use from here on in - are formed around a strong affinity that provides the bootstrapping of trust: long term friends, women trading in the same market for years, school alumni, employees of a company (typically excluding the boss), extended family and similar relationships. In essence, chamas import strong trust from prior relationships and context.

Technically, a chama is a group formed along cooperative lines for a single purpose for the benefit of its members, equally. Chamas are typically focussed on one thing - save money together. The money is apportioned to the savings of each member, but each member gets the same vote in the affairs, regardless of their financial contribution.

About three-quarters of members of chamas are women - they are thinking of school fees, emergencies, and the future. They are *biashara*, women in trade, thinking of supply, today's capital loan, their market, their neighbours.

At a meeting, the members bring their cash. They've got their governance sorted out:

- Cash is typically kept in a tin with 3 locks, the keys of which are shared amongst the

members. Or for the more advanced groups, a bank account or mPesa account. Next month, they open up the tin and check that nothing's gone wrong.

- Books are kept to account for all of the savings and other activities.
- Procedures - If a member needs to withdraw, there's a procedure. If a member needs a loan, there's a way. If a member needs help, this is her community. If there is a fight, they've got dispute provisions as well. If someone turns up late, she can be fined.

Meetings are often conducted with food, as the ritual of sharing is important.

Figure 21 - How do you say 'social savings group' in Africa?

IV.2 Alice finds herself in a Chama

> reH tay' ghot tuqDaj je
> (one is always of his tribe)
> *(Old Klingon adage)*

Behind that boring title is a rich culture of Kenyan informal finance, and as of right now the best example of what we are looking for. But, why it is the best example is not because of its structure but as a reflection of African society - when all is corrupt, all is done inside little islands of anti-corruption. The chama is that island of integrity, as people desperate to make things happen come together with their trusted friends and lock themselves into shared arrangements that keep all of them together, honest, cooperating in a shared need and a shared goal.

You might or might not be able to see where I am going with this, so I'll nail it:

```
Alice wants to be part of a chama.
```

Coming together to save money in a corrupt environment calls for a degree of attention to governance and to security that makes it a special place. It is the place where Kenyan women work together towards a common goal, and over the years, they get there. It is the place where they can feel proud that they themselves are in charge. Everything that happens is because they made it happen. Every shilling came from them, every decision too. And every shilling not lost to corruption, waste, thieves was saved because they did it *together*.

```
In a life of corruption, the chama is the one island of integrity.
```

As a consequence of all their work, their savings, their hopes and dreams and successes, Kenyans identify with their chamas. Perhaps, it is the only place where her goals have a chance. Perhaps as a consequence of the failure all around them, the chama is the one positive dream they have?

Whatever the reason, Alice identifies, and her chama friends identify with her. In a nation of individuals all looking out for number one in the struggle for survival, Alice might feel like she is a nobody. But in a chama made up of her friends, Alice is somebody. The chama members are all in the same boat together; and in this boat, Alice's opinion, her vote and her consent have value.

More so than they do with football clubs, more so than Kenya as a nation, more than their tribal affiliation, and sometimes as much as they do with their family. Her relatives may help her raise money if she needs to pay for a hospital visit, but most of the time they are as likely to ask for money for others than to contribute. As we claimed in Part III, Alice's family may be her very upbringing and spirit, but it is also the family she left behind for many reasons. Likewise, her church may want her tithe, but they are not going to help her pay her child's school fees.

Alice identifies with her chama, and is so doing, she shares her identity. The chama, at least in the form I saw it in Kenya, is the ideal place for Alice's identity. She already trusts her chama to a high level, by dint of the fact that they are together saving on their island in a sea of corruption. Alice sees and feels the trust, and she shares the goal, but more than that, or perhaps as a result of all that, Alice wants to belong. She trusts her chama if only because she's no-one else to trust, Alice shares her identity within, if only because she has no other choice and if she does not share she does not grow.

If her identity does not grow, it shrinks; maybe Alice and her friends form Chamas to share and grow their identity. Maybe the Chama exists for themselves, and finance is just the excuse - I do not know the answer to these mysteries, but it is at least clear to this humble observer that the Chama is where Alice hides, secures, grows her self, in a culture and life that has no such other option.

It is incredibly difficult for Westerners to understand this. In part because our lives are so safe and protected, we can share our identity with anyone we like, any time, in slivers or in depth. In further part, safety means we can form broad and quick relationships, and therefore have no clear sense of a shortage.

We haven't the sense of risk, neither psychologically or financially. We westerners all have roofs over our heads, we all have our support groups, we all have our fallbacks. Africa isn't that place. Everyone is struggling for survival, and the people you meet on the street are just as likely to rob you as help you.

Uniquely, the people Alice shares herself within the chama are bound together in not only identity but a common goal - she knows that when she needs a loan the chama is there for her.

And by putting her savings into the chama, Alice can honestly say she doesn't have any cash on hand when one of her relatives ask for money. To us in the West, this is illusory because we don't have the same threats to our finances, our tradition of individualism also extends to money. Why would we do that? Want that? To Alice in Africa, it's probably her only choice.

In a culture where everyone wants a handout and everyone is supposed to share, the chama gives Alice a way to save the fruit of her labor, and yet, not have it. This need is shared, and it locks the chama members together. They all use the chama to accumulate their savings toward their personal goals, and to hide them from the common threats.

Figure 22 - Chamas account for the savings of members

The Club of the West

How would Westerners do this?

The above sounds very much like a club, and in essence that is what it is. The governance feels much the same, the regular meetings, the focus on an agreed purpose, and the way in which some people come in, argue and leave is very similar.

Clubs can be informal, or they can be registered when there are assets to protect. Local sports clubs often register themselves under local association rules so as to buy jerseys, organise transport, hire facilities and the like. In some nanny-states like Australia it is hard to hire a room unless you are a registered body with insurance and so forth. It can also simplify and save tax. Registration is also seen as a signal that you are important, serious.

Many in the West do really get into their sports clubs and in this way they become part of their identity. Indeed the shared identity of the football club is perhaps the strongest identity of them all in the West, in peacetime at least. I remember when Barça played Real Madrid for *Copa del Rey* and the crowds raged outside my window. I and my entire country stayed up all night to watch Australia II take the America's cup. And I remember when USA played Russia for the Olympic gold medal in ice hockey during the first Afghan tussle.

We all have our moments when our identity is joined, aligned, is us, together, as never before.

Chamas are much the same as a small footy club, in that they typically start off informally and only get around to registering much later. Registration is surprisingly easy, perhaps because there are so many of them - you pop into the Chief's office (like the local council), fill in a form, pay a fee. Done. There is only one rule of import, which is that the chama keeps an internal copy of every member's Kenya ID card.

But, a western non-profit club is a different thing in one respect - it is formed for a purpose that is strictly non-commercial. Corporations needn't smile either, as typically, in the Anglo world at least, ordinary corporations are banned from doing financial activity in their incorporation documents. Financial activity requires a special licence, and these are more or less impossible to get.

Cooperatives and Mutual Societies

Chamas don't exist in the West, but cooperatives, mutual societies, and investment clubs do. These are membership organisations where every member has the same vote and they are permitted to take on savings. Coming from a similar history as the chama, cooperatives and mutual societies spring up wherever there is an affinity or Schelling point around a particular commercial or financial mission, and the existing opportunities - commercial for-profit companies or government services - don't work so well.

There are some key differences.

Firstly, the notion of *non-banks* is frowned upon to a greater or lesser degree. At the extreme of the English-speaking world, it is quite hard to start as a financial Cooperative or Mutual Society because the registration and build-up process is onerous. As with most things in an oligopolistic market, once the purpose becomes clear, the regulations are piled on by the big banks, so crossing the barrier to entering that market is generally too hard in the west.

The Anglo world fails the test of open community finance, but Germany still champions a strong diversified finance scene known as the 3 pillars of banking: local community or cooperative banking, *Landesbanken* and *Sparkassen* (state-owned banks and regional savings banks), and the big private banks. It could be said that the 3 pillars saved Germany from the 2007-08 crisis.

Secondly, at least in Africa, it's an easy market to get started in. Start as a chama with a dozen friends, grow for a bit, register as a 'self help group,' grow some more, make an investment or two, grow some more. And only then think about stepping up to the formal cooperative regime, known as a SACCO or a *Savings and Credit Cooperative* in Kenya. This ability to enter easily into the market for savings is a critical feature of Kenya's success at growth and rising wealth, recognised in competition theory as *low barriers to entry* (Michael E. Porter, "How Competitive Forces Shape Strategy").

Thirdly, a cooperative or building society (or S&L in US of A) operates in the banking business, and it is typically prescribed to do that. That is, it takes savings from members *and* lends out loans to them. In the banking business, to hold working assets is to be in a state of sin. Whereas a chama is more of an investment fund - it takes in contributions from members, and makes investments with the value saved. Everyone has a say in those investments, whereas the cooperative society model is that everyone typically has a say only on the annual accounts, not the detailed decisions to invest.

Fourthly, in the West, this concept is simply unnecessary. Westerners have many options to save, and they are basically safe in most or all of them. Westerners are safe in daily life for the most part. They don't need another option for saving, and they don't need to pay the cost of the relationship development to get that option.

The Future is Less Clear

But there are two caveats to that blithe and innocent happiness of the Western citizen - the first of which is that saving *on the net* is not safe. Think here Bitcoin, and its altcoin and DeFi cousins; it's a wild wild west and ordinary western savers dare not enter into the warzone of *crypto*.

Secondly, banking is changing to become less of a right and more of a control. Entire countries such as India and Greece are being modernised to control access to finance; bail-in is now a legal thing in many countries in the post-Cyprus scene; and *decashing* or *demonetisation* programmes continue with gusto if not actual economic or societal success. Programmes such as KYC and AML are proceeding on a 35 year programme to reduce money's function from supporting an open society to enabling mass surveillance and control by means of centrally determined notions of *suspicion*[7]. This control costs money, causing *derisking* or the chopping off of entire countries from the financial system. A decade after the 2008 Global Financial Crisis, there remains no clear resolution nor clear defence against it happening again, and regulators answer every problem with the search for more 'control'.

As society becomes more mobile, as the regularity of workers reduces due to economic and pandemic trauma, as social control programmes gain fruition, and as we explore the net for more aspects of our financial security, we in the West may find ourselves admiring the chama more and more.

The Right to Financial Independence

In effect, the right to start a financial institution is preserved for all Kenyans, and registering it is cheap if needed. At the other extreme, in the Anglo world we are allowed to trust a club with short-term money, but not for the purpose of long term savings for each member. Hence, we English speakers cannot place our identity into a framework where it really matters, one where

```
    Alice has skin in the game.
```

And therefore, Alice is not served in the rich world in quite the same way as she could be. Her identity is unserved when the groups she is involved with don't matter, don't watch, don't have *skin in the game*, or her financial relationship is dominated by faceless and uncaring banks - credit card debt & mortgages. She'd be better off in Kenya, where her financial future is shared with her chama, a group of like minded women who are all in it together. In her chama, she can share her worries of children, useless husbands, nosy neighbours; sharing all this will earn quiet support to save more. We in the west can't share anything with our banks without the fear of being sold another inappropriate high-fees debt product.

Or, Alice's Identity may be better off in any lesser developed country, as this model stretches in different forms all the way across Africa and also the Indian sub-continent as well as into Asia, where the chama is called a "Hui." It's also found in the Caribbean and in Latin America. Although the model exists across the entire developing world, seemingly, it is possible that Kenya has the most advanced form[8].

This Little Chama Goes To Market

> "kidogo kidogo hujaza kibaba"
> *(Swahili expression "Little by little fills the basket")*

Of course, this story has to continue, it has to go somewhere. Once the chama has met in trust and built up a savings war chest, it's time to go out and do something with it. Invest! And that is what happens.

Chamas invest in small businesses, in land, in buildings, and especially in transport - those little jitney buses known as *matatus*, whizzing up and down the road, with a young kid yelling *"bebabeba"* or "git on da bus" hanging out the side, are primarily financed by chamas. These days they invest in Ubers.

In this success, you can see where Alice is excited to be part of it - she saves with all her women friends, towards a wildly ambitious target, "*kidogo kidogo,*" little by little, and it takes the trust of everyone of the chama to make it possible.

Chamas are more of Alice's identity than any football club could be. With a football club, you can watch a winning game. With a chama you can become an owner of a fleet of matatus, be the boss of a business, a landlord.

Chamas are not only wildly successful, they are the base of the economy. By this I mean, they are the capital that powers most of the informal sector. There is a government report that lists Chama-based capital as powering 42% of the Kenyan economy. Most every report that delves into finance and *actually includes the informal sector* shows the chama to be the largest single source of capital.

> Kenya Association of Investment Chamas estimates that there are over 200,000 investment chamas in Kenya, 50% of the groups are based in Nairobi and they control over kshs170 billion [usd $1.7 billion] of investable savings. If well harnessed, these groups have the potential to grow and become financial empires but often lack relevant financial and investments information which can help them make informed decisions, grow, mitigate risks and attain sustainability.
> *(Chamas Expo)*

Now, by the natural law of things, what I have described above cannot possibly sustain such a huge effort, and so it is with Chamas - they grow. And, once they reach a certain size, such as for example hundreds of members, they graduate to the next level. But the next level is a fork in the road. Some chamas incorporate as a limited company. Others choose to upgrade to a credit union. Ultimately that decision depends on whether they want to focus on lending or investing in non-financial assets like real estate and transportation.

Limited companies aside, the next level is formally called a SACCO, or Savings And Credit Cooperative Organisation. It is much the same as a cooperative or mutual society, and unlike with a chama, there are many more rules and governance restrictions on how to run one. Two things push the chamas towards becoming a SACCO, one of which is that it becomes much harder to secure a lot of money with just informal techniques.

And the second is that it represents a very powerful boost to the identity of the chama to convert to a SACCO. Everyone wants their chama to become successful enough to join the adults' club. It's another life goal, it's another combined challenge, and another flowering of the identity of all within.

IV.3 What the Wazungu Did

Now, this all sounds rather idyllic, and it would be so easy to present the concept in glowing words in a report, accompanied by that modern classic of Western charity, the staged photo of a poor black child playing in clean running water. This would be the normal *modus operandi* of the countless NGOs and supra-national organs: write a report, call for more funding, more research and definitely more funding!

The locals name these transient white tourists the *wazungu* or "aimless wanderers" (singular, *mzungu*). It's accurate.

But these wazungu were not to be deterred, and we even started a little chama to find out just how far we could wander. Chamas are, like any club, hotbeds of trouble and intrigue. Our adventures revealed several issues and we put in a little startup to build a product to solve those problems:

1. Bookkeeping
2. Governance
3. Investment

We didn't go into this to make their identity more white or ask them to trust us. I originally spotted that their bookkeeping could be done better as issues of values in good old Ricardian contracts (Ian Grigg, "The Ricardian Contract") and triple entry accounting rather than using ye olde double entry and paper ledgers (Ian Grigg, "Triple Entry Accounting"). Every chama was a triple accounting picture of two Riccys - cash and their investment. That problem, sure, solved.

But once we saw the difficulties under which chama governance laboured, it became clear that they needed better. Corruption was reduced but not eliminated! Even more, we recognised that better governance had to cost zero money, because some of the chamas were working with people who saved $2 each time, and that doesn't leave a lot of spare cash to pay for professionals[9].

Back to governance. If it is going to be free, that means the chama has to do it itself. The people in the organisation have to govern themselves. Luckily, we already had some experience of self-governance with CAcert, the community CA, which provides reliable assertions over people across the planet (Ian Grigg, "An open audit").

Copying CAcert's web of trust into the chamas proved to be not only possible but also popular and easy[10]. The Kenyan chama members were already doing the actions, they just needed our 'systems' view to turn it into actionable intelligence. The essence is a constitution that binds people into a jurisdiction of dispute resolution before our own

arbitrators. As we ourselves in the chamas get to pick our arbitrators, not only are we in control of our destiny, we are building trust in the system. Add in CAcert's concept of *web of trust* in which members make statements over each other, we were not only building Alice's trust in her group, we were laying the lines of that trust across the net.
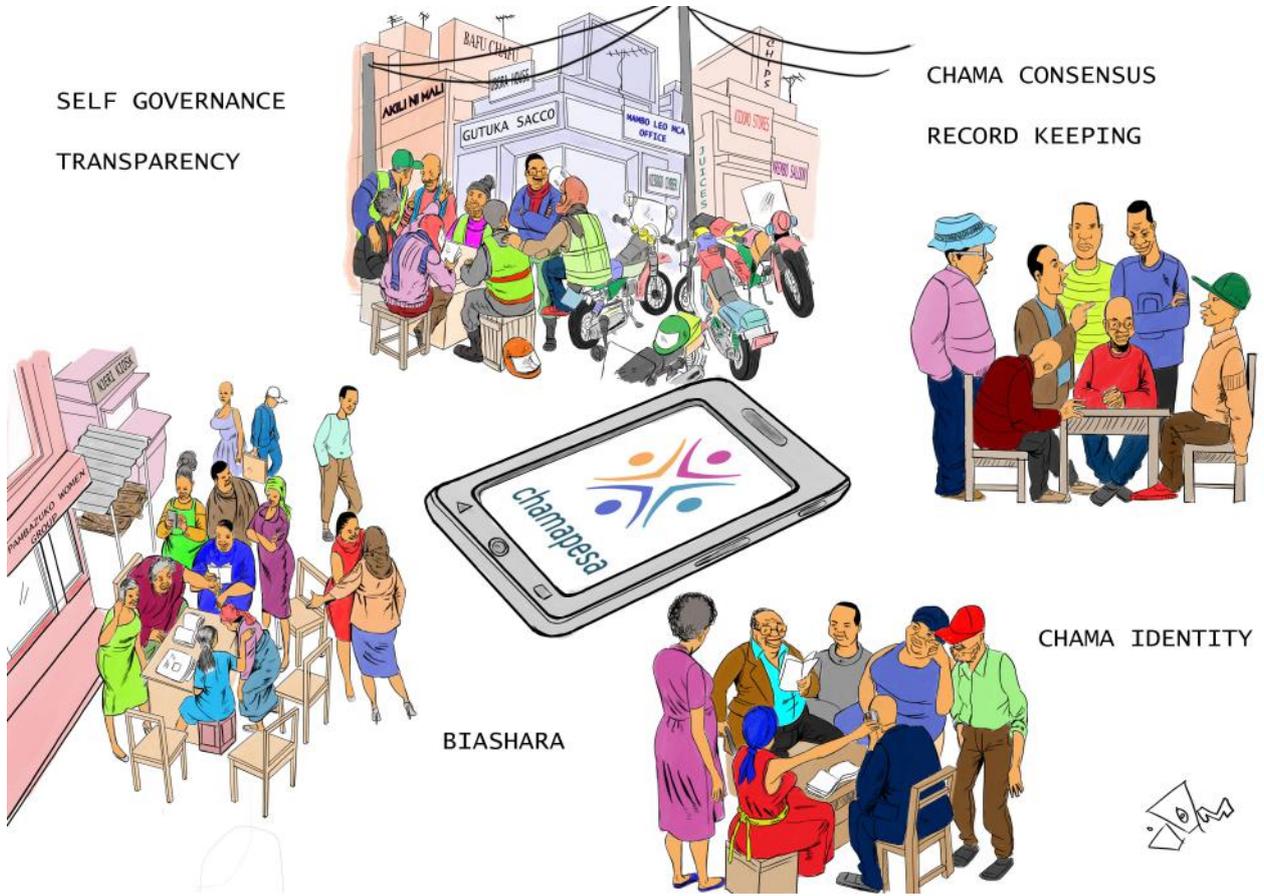

Figure 23 - Chamapesa

Alice Finds Her Identity

> "Un pour tous, tous pour un"
> "One for all, all for one"
> *(Alexander Dumas, The Three Musketeers)*

Outstanding! Finally, it all started to make sense. Finally an Internet Identity framework that worked - not for the technologist, not for the corporation, but for the user. But, to do it we needed all the elements laid out in laborious detail in these 100 pages or so - trust, identity, money, risk, financial cryptography and social groups - to get to the structure, being chamas.

To get Alice to share her information, she had to be inside a group that not only protected her, but was part of her identity and her identity was part of them - to save for her future, they all saved together, took on risk together, made money together. A credible commitment to be united was needed to ensure the stakes are high enough for Alice and everyone else in her group to go all in -- both in order to make that costly investment in trust worthwhile *and* to get the returns on the shared risk, the mutual vulnerability brought about by identifying with common savings goals.

It was pointed out earlier on in the cycle - unless there is skin in the game, there is no game. What we are seeing now is that even skin in the game isn't enough because Alice can fold her cards, go home and chill.

To be a suitable recipient for her identity, Alice has to know that the recipient is all in with her, which, under the principle of mutuality means, Alice is all in with the recipient. We know that one such construct is marriage, but that doesn't scale, so for the mutuality to kick in *and* scale, we need a lot of people, more than Alice's husband, to reach that benefit.

The group we seek then is a group in which Alice and her partners have mutualised, to the extent that they are prepared to share their Identity for the building of mutual trust. This is a tall order; we in the west have no such organisation, so on the face of it, we either adopt something like the chama to our own, we find something new, or we miss out on the possibility of true Internet Identity.

I'd like to go with the first. But I fear we have lost that opportunity, and I also fear that the writing is on the wall for Kenya and the developing world, as well, a point which underscores the unmitigated harms of the Wazungu invention of Anti-Money Laundering (AML).

Alice's Circle

The discovery of how the chama worked closed the loop on Identity. Finally we had a cohesive picture of how to make it work:

- The Dunbar-framed small local group solved the problems of scale that all larger groups exhibited, be it CAcert, a 2000s model social network or *The Circle* of 2010s fiction.

- The purpose and affinity gave meaning to the processes, something that web of trust and PKI failed at, both, dismally, in their own ways.

- And finally they had skin in the game - our savings, our financial future, our jobs, our family at risk - that gave the group their foundation.

The chama model is the one closest to anything yet seen for the purposes of Alice's Identity. It gives protection, purpose, support, and hope. It promotes both Alice's business aspirations, and her family. And it is robust - strong enough to survive in corruption. Even its one weakness, of success leading to growth leading to loss of direct relationship, had an in-built defence mechanism: chamas could split up, there is free entry to start another, and there is a defined path to grow towards a more formalised institution (SACCOs, like mutual societies or coops).

Dinero Encircled

Our designs for Kenya were prototyped as ChamaPesa and run briefly, but our exuberance outstripped our capital, so we had to close down before any large scale validation occurred. For those who might criticize our lack of startup spirit - we were dealing with people's savings, their futures, their very hopes and plans. There was no way I would let their exuberance for our system off the leash unless we had two years runway: to keep the systems going, to prepare for a bigger raise, and to keep their savings safe.

Notwithstanding the glowing brochures of *impact investment*, the average white male capital investor does not know what to invest in, and has an institutionalised or recycled view on what made for an investment. In plainer words, they were looking for past echoes of western myths - clean water, solar, toilets - which made them utterly useless to local circumstances. That was actually a good result - there were some groups that were better informed, and more dangerous. It was somewhat illusory that both of the two celebrated major western technology investments into Kenya were embarrassing to their investors, and would never have been made with fuller understanding or forethought. And local money was even more naive, looking for the quick kill or the carnival investment (Herman Wouk, Don't stop the Carnival).

We also had to decamp the country because of one of the interminable wars within government. We became a direct casualty of the President's war against corruption; as visas became poker chips to save corrupt jobs, *wazungu* were sacrificed. Back in the West, we then spent several years searching for the Western Chama, and came up empty handed. There are no strong, available institutional structures that have the characteristics.

We've found the model. What's the implementation answer? Go back to Kenya? Find the western alternate? If we ever find it, I'll record it in a future Part V, in which world Alice strides forth into an exciting future of mutualised economic safety.

Conclusion

Let me Summarise

In *Part I* we concluded that the useful identity information was that which one person said about another, with an emphasis on this first person being related in some sense to the second.

Other models towards digitising identity (whatever that means) we examined and discarded. Government's view of identity is too shallow to be useful. The business or corporate model is out of our control, so we the people don't want them to have valuable data. Our identity within our minds is powerful, but for that very motive, we wouldn't want anyone else in there.

"Bob says something about Alice" has then emerged as an atomic element in the quest for digital identity. And, indeed, the current state of the art in thinking in identity circles is exactly that - that very statement could be very useful to Carol, which would be encouraging except that big tech is waiting in the wings, salivating at the prospect of monetising Alice's somethings.

Leaving that fear aside, because we come from a user-centric worldview, it behoves to ask where this something comes from? Alice had to have shared something of import with Bob at some point.

Why would Alice do that? Probably because she trusted him at that point in time with that information. This sounds glib, trite, but that's only because everyone assumes that trust is a simple thing.

What if it's not?

Trust is the question of *Part II* - we explore how context specific trust is, even as we tend to perceive it as a general quality. Indeed, it is so specific to the moment and the context that Alice's capability to run a trust judgement is like a machine - she does it so fast and so frequently that she doesn't even recognise the act.

Even more fascinating, the result of today's trust decision creates new data for tomorrow's trust decision. It's a feedback loop! Alice cannot instantly trust someone she doesn't know - she has to find some prior experience first. And that means taking a risk. As well as trust being of the instant, trust is also an outcome from taking a lot of risks over time.

Having modelled trust as a risk feedback loop, it is clear that this is very intelligent behaviour. It's also circular, it exists but that intelligent behaviour was some form of learned response. So where did it come from? We weren't born with the capability to trust.

Or were we? *Part III* looks at the origins of trust and starts with the tabula rasa theory: the baby is a blank slate or empty vessel as far as intelligence is concerned. How does it survive, let alone grow to be the supremely trusting Alice?

As every parent knows, a new born baby has a couple of behaviours - the need to feed, to interact, to recognise, to cry. The newborn also has one major advantage, being the mother, who more or less provides for everything else needed, including love, which means that the baby's inability to trust is not a problem.

At least in the short term. Gradually, mother teaches baby Alice to handle more and more by herself - independence. And much of this teaching involves others within the family. Alice discovers from her mother that those within the family are trusted! First a father figure, literally or a near relation. Then siblings, cousins, aunts, uncles, and grandparents, a group sometimes called the extended family.

Before long, schooling comes along which involves other children and typically a new set of independent adults. New groups, new challenges! Until Alice becomes an adult and leaves her origin group to travel the world, become independent, join new groups or even start her own - a family.

Alice learns how to trust within the context of groups that she was brought up in. Which suggests that when looking for Alice's trust, we should start with her groups. Which is an odd remark for those of us in the rich western world, as other than her direct family, Alice's groups tend to be lighter, more casual, social, almost hobbyist.

Not so in the developing world. Here, *Part IV* examines how groups of peers come together as trusted partners in a serious mission - savings. Which is made all the more serious because corruption makes savings otherwise impossible; the less trust, the more need for trust. The seriousness of the chama's mission to save also makes the chama a powerful protector of identity, a group that is second only to members' families.

And now we're at full cycle - useful identity is that knowledge of our selves found in others (Part I) and especially, in those that we trust with the knowledge (Part II). Figuring out who we trust means how we trust, and that process emerged with birth, from and to Mother, to Family to School and eventually to our own groups (Part III). Then, Part IV provided an example of strong groups based on an existential need to defend from corruption.

The future of useful identity is found in our groups, and for once the developing world has it and the rich world does not.

How to Move Forward

I am a technologist. I build technical systems, and to me, identity must be a technological inquiry. How do we build identity properly?

Yet identity turns out to be something that defies technology both in spirit and history. A grand puzzle to solve, but also a salutary warning - identity is too important to muck up.

To find the answer on which this book is based required leaving behind the techno-centric western world and spending time - a couple of years as it happened - with people in Africa. Kenya is a developing country, very different to my western ways but strangely a decade ahead in several areas, mobile phones and mobile money being one, and societal investment being another. Having observed the chamas as the answer to corruption in finance, we built an app based on what today would be recognised as blockchain technology. It worked, it tracked savings.

But all good times come to an end, and ironically a war against corruption launched by the President sent us foreigners scurrying.

A silver lining on our exile is that we've now had the time to ponder on the strength of the chama. To walk the forests and debate, present experiences, write it into words and eventually this book. To fit all our experiences into a plausible theory that spoke to our identity took about 5 years.

Having dived deep into finance, security, psychology, anthropology and institutions, it's now time to go back to technology and build a platform for groups. To do that we need: principles, an architecture, and a plan.

Objectives or Principles or Hopefully Both

The end goal or far mission of this inquiry is

```
To grow and share trust on the Internet in a scalable and safe fashion - to enable
safe and mutually beneficial trade among peoples who do not know each other.
```

We propose that the way to reach this aspirational goal is by way of a couple of phases: Firstly, to form communities into small groups that are internally strong and trusted.

```
To nurture and share the trust of neighbours and peers, each into a strong but
tiny institution, the chama, such that this community of members can build its
own strength towards their own aspirational future, together.
```

Chamas already exist, but we face two challenges. (1) in order to move them to the digital sphere without losing their specialness, we will need strong accounting, clear ties to underlying assets, to work with their governance processes, and to not break their existing security against attackers of all forms. (2) to export this movement of financial groups from the developing world, where in some cases it is so strong that it is the economy, to the west where institutions do all that, and individualism is championed against family.

Institutions that are losing trust and resiliency by the year, so there is some urgency in this.

Secondly,

```
To introduce the groups together into a wider community of communities, and
thus bind their local trust into a global net of reliable information that can
communicate the strength of their members to each other.
```

This all by means of communication, consensus & standards and resolution of disputes, all good stuff that has been trialled and shown to work at least in some experiments (Grigg, "An Open Audit") (Grigg, "The Governed Blockchain").

To Practical Matters

Such a grand plan is however a thing of delicacy - all the obvious ways of sharing identity have failed in the past, it is far easier to destroy than to create.

The actual way to build this - to deploy the identity structure outlined in this book - starts from one iron law: *Ignore identity.* No technical system that starts from the goal of capturing your identity will ever work, because users won't let it.

That said, the chamas aren't about identity. Chamas form to fight corruption and save. Identity might be an interesting spin off or might not, they really don't care as long as savings are now possible.

Savings. Which brings us to the epiphany I had way back when I was first told of the how and why of chamas: *This is financial cryptography.* More particular, this is Ricardo, a system Gary Howland and I built back in the 90s (Gary Howland, "Development of an Open and Flexible Payment System"), best remembered for one small component called the Ricardian contract. Updated to today's lingo, this is narrowly *blockchain* or more broadly *decentralised ledger technology* (DLT). Which leads to the first observation:

```
We need a DLT or blockchain.
```

Yet, therein immediately we hit a problem. The point of chamas is to be secret - to conduct finances in private. Forget your notions of exotic cryptography and MPC and all that technology. The only secure data is the data that isn't shared, until proven otherwise. To resolve this conundrum:

```
We need a tiny blockchain that is permissioned for only the group.
```

I call this an append log. Because it is permissioned, and because the group is trusted, we don't need consensus as per the blockchain business, we just need ordering.

Next, we need accounting. Accounting can be anything from a ledger to crypto issuance, but because I'm a triple entry sort of guy, I lean closer to the full cryptographic ledger of receipts.

With accounting, we can account for savings. That might sound simplistic but accounting is actually one of humanity's enduring inventions. Indeed, both writing and arithmetic evolved out of accounting, so it's no historical slouch. Building accounting into a platform that the small chama can use, own, dominate and defend is the intermediate target.

Next: Governance. As a group, the members are paramount and the group also is the outcome of the members' centrality. But all groupings fall to self-interest and selfish decision making, which ultimately spells ruin - check any history since the Argonauts. The defence to this is governance, not technology (sorry blockchain purists), and that means using all of the techniques that humanity has developed since forever.

Which means: communication. All governance requires, as an assumption, strong communication. Today, that's a high bar as a storm of social media apps compete for your attention, but hopefully this is enough to set the tone. What minimum social communications can we provide to establish the foregoing? Let's settle for a squall of media.

Institutions. Finally, we need to cast all of the above technical tools within a structure and relationships that protects the individual, the chama and the whole. Against all enemies, domestic and foreign, to abuse a phrase.

Then, and only then, can we create sufficient foundation and strength of pillars for each and every member to join their identity and know that their identity is protected by the group, by the whole, and not be leaked or otherwise abused by the tech.

My Chama

This book was a journey, and no journey happens without the support of many along the way, both historical and direct. "If you want to go far..."

Historically, the CAcert community was the schoolyard that taught me what worked in digital identity, and as importantly why the classical systems of identity did not work, be that the state, the corporation, PGP's web of trust, or PKI. We came, we saw, and maybe we moved the border a little further forward. Actually, a lot further.

In strange resonance, the eternal lessons of the family were thrust into my mind and daily life in the early 2000s, when my then-partner, her little girl and I struggled to make sense of our adventure. I struggled, I researched, I learnt, I did the best I could. I remembered my own childhood, that of others, my own mother and father. I still failed, and that failure rings loud in every word in Part III. To not do as well as one could is the curse of every parent, the forgiveness of every child.

In 2011, one Kenya woman, Warigia Razia, opened my eyes with a few words, "we have our chamas." Unwittingly, our own little chama spoke the truth *en vivo* of the cycle of identity, simply by meeting, saving, glowing and being. Many thanks to Basra, Chris, Jacque, Joan, Matayo, Monica, Richard, Safia, Sue, Symprose, Vincent and others. I felt the light, but it took more years to see.

The Robin Hood Coop workshop in London, 2015, sparked the intellectual beginning to this book. In one 8 minute video, Part I was laid down. The logic in Parts II, III was developed on long walks in the forests of Chapel Hill with Ada. It wouldn't have been possible to build the intellectual bridge from that first London spark back to the burning furnaces of the chamas of Kenya without her whole and uncompromising support.

Finally - this presentation has been made entirely and only possible with the production talents of Rhian Lewis, who went above and beyond to create a book, and the graphical wizardry of André Bonello to present a message.

Many people have critiqued the work: Arthur Doohan, Toni Lane Casserly, Thomas Cox, google Engineering Support, Ken Griffith, Michael Kimani, Ada Lovelace, Tim Pastoor, Ily More, Laurent MT, Christian Lundkvist, Joseph Perling, Konstantinos Sgantzos, Philip Sheldrake, Lee Smith, Eva Stöwe, Tatsu, Christopher Whipple.

Thank you, my people, my chama.

Iang, Planet of Humans, 2021

Appendix - Types of Groups

The types of groups that exist are legion: countries, clubs, sports, fan bases, school classes, support groups, professional verticals, housing and industry cooperatives. Groups form around purpose, and around structure.

It also seems wherever a group of people forms, sub-groupings form naturally within, perhaps best shown in the army: sections, platoons, companies, battalions and that's only within the 1000.

Yet, only some of these groupings are approximately relevant for our present topic. Let's do a fast flyover of some interesting groups and surface some of the differences we are looking for.

Type	Source of cohesion	Positives	Limitations
Nation	Geographical / Historical / legal / force	Unlimited capital	broad base of voting power results in diffuse projectual power
Local Club	Affinity with topic / self-managed rules	Closely aligned around narrow topic	Very low capital base, inability to manage large amounts
International professional association	Need of the professionals to merge and share and learn	Spreading of knowledge and promotion of the science and culture behind the profession	Guilds - too focussed on own survival, own promotion, as if there is no alternate view.
Cooperative or Mutual Savings Society	Affinity for a particular financing need, region, profession.	Aligned to community values	Unable to marshal disparate savings or investments.
Webs of Trust (CAcert)	Affinity over security and privacy	Capturing relationships, wrapping in contract -> activity -> DR	No basis in output
Alumni	Affinity over shared experience of alma mater	Shared incentives in validation and networking	Unfocussed and often captured by funding mania
Social Network	Technological communication medium for affinity	Brings those of affinity closer together	Does not really address the core of the affinity; eventually captured for profit
			rofit motive favours

Corporation	Need for a job, entrepreneurship	Highly defined lines and economic incentives	owners & managers over employees & customers
Church	Affinity in religious belief	Strong in trust and relationship	Fixed viewpoints, unable to move with the times

Let's do a quick risk analysis. If we look at the above groups, it is clear that only a few of these are suitable repositories for Alice's identity.

Type	Size	Trust	Identity
Nation	No - too large	No	No - too heavy
Local Club	good	maybe	maybe
International professional association	No - too large	Yes	No - too formal
Cooperative or Mutual Savings Society	Maybe	Yes	No - focussed on money
Webs of Trust (CAcert)	Large - but local	Yes	No - too light
Alumni	Yes	Yes	Yes
Social Network	Very large	maybe	maybe
Big Corp	Large	No	No
Small Startup	small	If founder?	maybe

Size. Too large and Alice's ability to conduct risk analysis on each member runs into capacity limits - time, Dunbar, and so forth. Too small and Alice can't enjoy the economies of shared trust. By observation rather than science, I peg the number as between 10 and 30.

Trust. Is Alice in the habit of trusting her group? Is it voluntary, or is she forced by societal circumstances to pick, or birth, etc? Does the group feel like trust is what it's about?

Identity. Can Alice place her very self into the group? Is she sad without them? Do they work together to protect Alice's self, as she does for them?

Endnotes

[1] Which is to say, we are for now ignoring other idiomatic uses of the term trust: you trust your car starts, you trust an institution, you place your loyalty and trust in the party, etc.

[2] In this cycle we use the cryptographic convention of Alice & Bob as first and second persons respectively. In English, this also allows us to use third person gender as an efficient signal, but that doesn't work in Spanish.

[3] Public Key. When we say key without describing which key of the public-private pair, we generally mean the public key.

[4] It is worth noting as *disclosure*, the present author spent many years with CAcert auditing, designing and managing some of the mechanisms so described.

[5] It is also worth noting that Identrust, a company that manages corporate PKIs for large companies such as banks, has also solved this problem with a similar solution: their corporate customers and employee/users are bound into a common arbitration framework in order to provide recourse.

[6] "This is an old Klingon adage that years ago was rendered into Federation standard [=English] in the form cited using the word "tribe" for "tuq," an ancestral grouping now usually translated as "house." The literal meaning of the Klingon phrase is "A person and his house are always together." Though cast in terms of family, the expression can apply to friendship as well. The basic idea conveyed is that no matter what happens and no matter where one may go, one remains attached to family and significant friends." Marc Okrand, *The Klingon Way - A Warriors's Guide*, 1996, page 34

[7] KYC or Know Your Customer used to refer to the branch manager having knowledge of your business at a personal level, but now is mostly an AI-informed filtering based on risk according to current understandings of *suspicion* by current regulatory viewpoints. AML stands for Anti-Money Laundering but has no particular relationship to actual control of serious money laundering, mostly being an AI-informed control system to reduce the risk to banks of compliance-based fines. Cf, *suspicion*.

[8] I don't know for sure on this point. And I'm not asking. My job, my purpose is to help not to destroy, nor to enter into *paralysis by analysis* that the supranationals and aid/NGO world is so bent on.

[9] As an aside, this is the first reason why banks are not in the market - they are simply too expensive. A bank account in Kenya costs $5-$10 per month in minimum fees, which is 5-10% of the average Kenyan's income. Banks exclude small chamas as much as they

exclude the informal economy on the basis of costs. The second reason is that the costs are rising all the time for all banks all across the world, thanks to government policies, in effect financial exclusion is baked into the government policy and banking practice. And, that isn't going to change any time soon. The third reason is the axiom above - banks are corrupt and the chama market is leery of them. Note that to some extent this is changing as banks now feed through mPesa, but that's a whole other story.

[10] It took Ada about a month part-time to port the CAcert dispute resolution framework into our Chama, while taking time off from writing a reliable protocol to move big photos over tiny UDP datagrams.

Bibliography

Articles, books, lyrics and proverbs, in order of appearance.

Introduction

- Sotiris Tsiodras, Greek Health Lead, 21 March 2020

Part I

- Idries Shah, *The Pleasantries of the Incredible Mulla Nasrudin*, ISF Publishing, 2015
- Joe Andrieu, "A Primer on Functional Identity" 2018
- UN Convention on the Rights of the Child, United Nations 1989
- Ian Grigg, "Identity," Robin Hood Coop - London Pop-up office Video by Tomer Kantor. Transcript 2015
- Chris Dixon, "How Aristotle Created the Computer," The Atlantic 2017
- Florian Henckel von Donnersmarck, *The Lives of Others* 2006
- The life of Mehran Karimi Nasseri, as told in *The Terminal* 2004
- German Government, "FAQ on German Citizenship," 2016
- Zerohedge.com "These Gates Will Open - Erdogan Declares As Turkey Begins Deporting ISIS Captives To Europe," 11 November 2019
- Pamela Druckerham, 'If I Sleep for an Hour, 30 People Will Die,' The New York Times 2016
- "India's living dead," Wikipedia
- Mira Kamdar, "What Happened in Delhi Was a Pogrom," The Atlantic 2020
- Shaun Walker, "Romanian court tells man he is not alive," The Guardian 2018
- Brett Scott, "The War on Cash," 2016 The Long + Short
- William Goldman, *The Princess Bride* 1987
- Abeba Birhane, "Descartes was wrong: 'a person is a person through other persons'," 7th April 2017, Aeon
- Christopher Allen, "The Path to Self-Sovereign Identity"
- Jane Mercer, "tweet," Twitter 201 possibly quoting "Can you identify yourself?" Nasrudin.org
- Steven Loveridge and Sugu Arulpragasam, "The Message," (M.I.A) 2010
- Sia Furler *et al*, "Chained to the Rhythm" (Katy Perry) 2017
- Daniel Stephens and Joseph Ray, "New Life" (Nero) 2011
- Rachel Metz, "Your smartphone can tell if you're bored," MIT Technology Review, 2016

- Adrienne LaFrance, "Not Even the People Who Write Algorithms Really Know How They Work," The Atlantic 2015
- Lennon/McCartney, "With a little help from my friends" (Ringo Starr / The Beatles) 1967
- R.I.M. Dunbar, "Neocortex size as a constraint on group size in primates," Journal of Human Evolution 1992
- Xhosa proverb - tweet by Michael Kimani
- Aaron Sorkin, *The Social Network* 2010
- Abraham Maslow, "A Theory of Human Motivation," Psychological Review Vol 50 No 4 1943
- Lisa S Davis, "For 18 years, I thought she was stealing my identity. Until I found her," The Guardian 2017
- Pete Townshend, "Who are you?", (The Who) 1978
- American Psychiatric Association, "Diagnostic and Statistical Manual of Mental Disorders"
- Joe Andrieu *et al*, "Five Mental Models of Identity," Rebooting Web of Trust 2018-2020
- Kaliya Young, *The Domains of Identity* Anthem Press 2018
- Carly Simon "You're so Vain," 1972

Part II

- William Shakespeare, Romeo and Juliet, 1597
- Lewis Carroll, *Alice's Adventures in Wonderland*, 1865
- Ray "Bear" Dillinger, Cryptography list, 15 January 2017
- Nicky Case, *The Evolution of Trust* 2017
- Stefani & Stefani, "Don't Speak," (No Doubt) 1995
- Peter Bernstein, *Against the Gods: The Remarkable Story of Risk,* Wiley 1998. Cited by Gunnar Peterson: twitter.
- Jerry Knight and Aaron Zigman, "Crush on You," (The Jets) 1986
- Philip K. Dick, *Ubik*, 1969
- @brian_trollz, tweet Twitter 2017
- Konstantinos Sgantzos and Ian Grigg, "Simulating the human brain. A Neuroscientific conjecture on the hard problem of consciousness," forthcoming
- Ian Grigg, "Identity is an Edge Protocol," R3 2017
- Robert Hettinga, "A Geodesic Society?" 1998
- Old Italian proverb, recorded by Steve Wilson, "Abandoning identity in favor of attributes," 2014
- Heinz von Foerster, *Understanding Systems, Conversations on Epistemology and Ethics*, Springer 2002
- Spencer Bogart, tweet Twitter 2017

References

- Ian Grigg, "Life is a Cabaret... Or how to split and merge a blockchain" Steemit 2017
- Ian Grigg, "The Governed Blockchain" 2017
- "The Iron Ring" Wikipedia
- Ian Grigg, "An Open Audit of an Open Certification Authority," 22nd Large Installation Systems Administration Conference (LISA 2008) 2008
- Marc Okrand, *The Klingon Way - A Warriors's Guide*, Star Trek 1996
- Allison Schrager, "Trust and Crime," Quartz 2016
- Ian Grigg, "PKI considered harmful" -2008
- Mark S. Granovetter, "The Strength of Weak Ties," American Journal of Sociology, Vol. 78, No. 6 1973
- Laurie Anderson, "Only an expert," 2010
- Heinz von Foerster, *op cit*

Part III

- Søren Rasted *et al*, "Barbie Girl," (Aqua) 1997
- Eric Raymond, "Hacking the noosphere" 1998
- Pete Townshend, "I'm a boy," (The Who) 1966
- Robert Hettinga, "A Geodesic Society?," 1998
- Michel Serres, "Science and the Humanities: The Case of Turner," The Journal of the International Institute, 1997
- R.I.M. Dunbar, "Co-Evolution Of Neocortex Size, Group Size And Language In Humans," 1993, quoted in Christopher Allen, "The Dunbar Number as a Limit to Group Sizes" 2004
- Christopher Allen, "Community by the Numbers, Part One: Group Thresholds" 2008
- Anthony Jay, "Nobody's Perfect - but a team can be" 2004
- José María Gómez, Miguel Verdú, Adela González-Megías & Marcos Méndez, "The phylogenetic roots of human lethal violence" Nature 2016, as reported in Ed Yong, "Humans: Unusually Murderous Mammals, Typically Murderous Primates" The Atlantic, 2016.
- Chapman & Knight, "Pleasure and Pain," (Divinyls) 1985
- Gwendolyn Brooks, "Paul Robeson," 1983
- Jim Steinman, "Paradise by the dashboard light," (Meatloaf) 1977
- Neneh Cherry et al, "7 seconds" (Youssou N'Dour) 1994
- Lennon-McCartney, "Ob-la-di Ob-La-Da," (The Beatles) 1968
- Igbo / Yoruba proverb
- Søren Rasted *et al*, "Cartoon Heroes," (Aqua) 1997
- Khayat / Germanotta, "Paper Gangsta," (Lady Gaga) 2008
- R.I.M. Dunbar, in "The Limits of Friendship," interview by Maria Konnikova, The New

Yorker 2014

- Dave Eggers, *The Circle*, 2013
- Dewey Bunnel, "A Horse with no name," (America), 1971
- Cobain/Novoselic/Grohl, "Smells like Teen Spirit," 1991
- David P. Reed, "That Sneaky Exponential—Beyond Metcalfe's Law to the Power of Community Building" 1999

Part IV

- Cat Stevens, "Father and Son," 1970
- David Robson, "How East and West think in profoundly different ways" 2017.
- Wallace Kantai, "Why Most M-Shwari Loans Are Taken At 3:00AM In Kenya" 2017.
- Dave Eggers, *The Circle*, Vintage Books 2013
- Richard Werner, Community Banking in Bavaria BBC 2013
- Ken Banks, "Mobile Finance: Indigenous, Ingenious or Both?" PCWorld 2008
- Marc Okrand, *The Klingon Way - A Warriors's Guide*, Star Trek 1996
- Michael E. Porter, "How Competitive Forces Shape Strategy," Harvard Business Review, May 1979
- 2nd Annual Investments & Chamas Expo 2017 Eventbrite 2017
- Ian Grigg, "The Ricardian Contract" First IEEE International Workshop on Electronic Contracting (WEC) 2004
- Ian Grigg, "Triple Entry Accounting" 2005
- Ian Grigg, "An Open Audit of an Open Certification Authority," 22nd Large Installation Systems Administration Conference (LISA 2008) 2008
- Alexander Dumas, *The Three Musketeers*, 1844
- Herman Wouk, *Don't stop the Carnival*, 1965

Conclusion

- Ian Grigg, "An Open Audit of an Open Certification Authority," 22nd Large Installation Systems Administration Conference (LISA 2008) 2008
- Ian Grigg, "The Governed Blockchain" 2017
- Gary Howland, "Development of an Open and Flexible Payment System" 1996

Images

Book cover and each of four detail preface pages for each Part, by André Bonello, 2021.

Figures and images, in order of appearance.

1. Florian Henckel von Donnersmarck, *The Lives of Others*, 2006
2. André Bonello, "Development of the embryonic brain," 2020
3. Aaron Sorkin, *The Social Network*, 2010 pp 52-53
4. André Bonello, "Maslow's Hierarchy of Needs," 2020
5. André Bonello, "Who Am I?" 2020
6. André Bonello, "Alice's Ladder of Trust," 2021
7. André Bonello, "Alice's Trust RADR (Reward-Analyse-Decide-Risk) Loop," 2020
8. @brian_trollz, "how could I ever trust myself again?" Twitter 2019
9. André Bonello, "Blockchain Engineers do not wear the Iron Ring," 2021 from an original by PCStuff (https://en.wikipedia.org/wiki/Iron_Ring#/media/File:Canadian_Engineer_Iron_Ring.jpg).
10. André Bonello, "Maslow's Hierarchy of Needs - revisited with Alice," 2020
11. (unknown), Presentation of a Rai Stone of Yap for the inauguration of The Federation of Micronesia, photograph part of the archive of Trust Territory of the Pacific Islands Archives Photograph Collection (http://digicoll.manoa.hawaii.edu/), Public Domain, (https://commons.wikimedia.org/w/index.php?curid=12525413), (https://en.wikipedia.org/wiki/Rai_stones#/media/File:Presentation_of_Yapese_stone_money_for_FSM_inauguration.jpg)
12. André Bonello, "Alice invests in Relationships to find Trust," 2021
13. André Bonello, "Alice's Choice in new Trust, as limited by Dunbar's number," 2021
14. André Bonello, "Trust and Identity are Yin and Yang," 2021
15. André Bonello, "The Mysterious Growth of Identity to Trust and Relationships," 2021
16. André Bonello, "Maslow's Mesa," 2021
17. André Bonello, "Alice joins Groups to Mutualise Trust, and thus escapes the tyranny of Dunbar's Number," 2021
18. John Tenniel, "That's quite enough—I hope I shan't grow any more," original woodprint from *Alice in Wonderland*, 1865 Public Domain
19. André Bonello, "Kenya and Africa, not to scale," 2021
20. Dave Eggers, "Privacy is Theft," 2013
21. Funmi Oyatogun, "How do you say *social savings groups* in Africa?" 2012 chamapesa project
22. Tomer Kantor, "Chamas account for the savings of members," 2018 chamapesa project
23. William Abiha, "Chamapesa," 2018 kindly provided by Micheal Kimani

Tables:

1. "4 theories of Identity" 2020
2. "From Nothing to Knowledge," 2020

1. "4 theories of Identity" 2020
2. "From Nothing to Knowledge," 2020