After the BlockCloud Apocalypse

Mark Burgess
Consultant (Virtual)
mark.burgess.oslo.mb+v17@gmail.com

Anil Somayaji
Carleton University (Virtual)
soma+v24@scs.carleton.ca

ABSTRACT

In 2038 we have lived though a decade during which the world's global computational infrastructure undermined privacy and trust in virtually every aspect of our lives. The problems were seen far in advance, but it was commonplace belief that a combination of cryptography and more distributed responsibilty in systems—'blockchains for everything, and all hail the cloud'—would together restore what had been lost in the first decades of the 21st century. As it turned out, it was these very technologies that ended up destroying the privacy and trust we had left.

In this review, we argue that the mistake collectively made was to think of privacy and trust as technological problems, when in fact they are properties of social and political systems. If we are to recover from what we call the BlockCloud Apocalypse, humans and machines are going to have to figure out how to build systems that support privacy and trust in *society*, rather than attempt to replace it with trust in technical validations. We propose a return to trust in humanitarian motives rather than technological supremacy.

CCS CONCEPTS

• **Applied computing** → **Digital cash**; • **Computer systems organization** → *Cloud computing*;

KEYWORDS

trust, privacy, blockchain, cloud security

ACM Reference Format:
Mark Burgess and Anil Somayaji. 2018. After the BlockCloud Apocalypse. In *New Security Paradigms Workshop (NSPW '18), August 28–31, 2018, Windsor, United Kingdom.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3285002.3285012

1 INTRODUCTION

It has been suggested that today in 2038 we are living through a Second Dark Age. It's true that almost every individual has access to information on every imaginable subject, at all times and places, yet it has become increasingly problematic to assess the value of information amidst the fog of partisan conspiracies. A growing tribalization of societies around the world has fractured our basic trust in information, distorting it though the whimsical lenses of the most outspoken clans. Few individuals can hope to distinguish reality from fiction.

Lives are easier, in some respects, thanks to a pervasive Artificial Intelligence (AI) that sustains our basic processes, and to the ubiquitous computational cloud infrastructure that delivers on basic utilities. Yet these systems have become both feared and daemonized, as they also routinely destroy the economic, emotional, indeed the physical lives of our friends and our families. The shadowy details of this growing problem are seldom reported in the official media streams and are routinely censored from searches anyway. By contrast, every aspect of our private lives seems to be available to the mega-corporations and a privilged few with the requisite power. The ubiquitous blockchain rumour-mill pumps out conspiracy theories that do little to bring clarity or truth to bear. Activists have pointed out that mankind should have been celebrating the saving of planet Earth and reaching for the stars; instead, 'citizens' (if we can still call them that) live in increasing uncertainty and widespread ignorance.

Our paper is a review, but we shall not claim to explain or even understand the full story of how society has been transformed during this 21st century. We shall, however, argue that naivete about computer security played a central and causal role in bringing about these changes, and that technological elites bear a large burden of responsibility for them. Their role was a simple one: their naive acceptance of technology, in pursuit of a blinkered capitalism, facilitated a significant loss of individual privacy and the wholesale collapse of trust in all aspects of human life.

These by now familiar effects were perhaps not instigated deliberately (unlike, say, the atomic bomb), yet technologists, businesses, and governments bear collective responsibility, because they convinced themselves of an untruth: that trust and privacy were fundamentally technological problems, to be solved by technological means. We shall discuss this "trust and privacy through technology" paradigm, reviewing the history of two key technological developments over the past two decades: immutable blockchains and ubiquitous cloud infrastructure. These two tools of business were supposed to increase trust and privacy, yet both ended up doing the opposite. We shall refer to their separate yet intertwined failures quaintly, if somewhat sensationally, as the *BlockCloud Apocalypse*. Though the outcome may seem paradoxical, there is ample evidence that trust and privacy problems cannot be eliminated by technological surrogates. Yet, if one adopts our viewpoint that privacy and trust are primarily socio-political challenges, then these failures may instead be understood as inevitable reactions to the social contract on which modern human civilization is based. Our hope here is that, by revisiting these failures of the past, we can choose a better path going forward.

The rest of this paper proceeds as follows. We review the history of blockchain and distributed clouds in Sections 2 and 3. Section 4 discusses how the "trust and privacy through technology" paradigm

NSPW '18, August 28–31, 2018, Windsor, United Kingdom

ACM ISBN 978-1-4503-6597-0/18/08…$15.00
https://doi.org/10.1145/3285002.3285012

influenced these events. Section 5 contrasts this paradigm with an examination of trust and privacy in a socio-political context. Section 6 discusses the contributions, limitations, implications of our analysis. Section 7 concludes.

2 THROUGH THE LEDGERGLASS DARKLY

While the cryptocurrency bubble collapse of 2019 discredited the popular idea that cryptocurrencies were a panacea for the problems of global capitalism, major financial institutions did not stop playing with blockchain technology; indeed, it became a centerpiece of efforts to protect financial records and insurance claims. The potential for blockchain technology to provide privacy, integrity, and availability for financial transactions made it perhaps the inevitable choice, given the calamities that commenced. The cure, however, may have been worse than the disease. Below we only outline the key events:

- 2019: Greek nationalists hire Russian hackers to perform a cyber attack on Troika institutions, breaching the European Central Bank (ECB), in an attempt to corrupt systems and erase Greek sovereign debt. The attack fails but draws attention to how centralized IT infrastructures are too fragile for major economic records. ECB initiates a crash program in securing financial transactions.
- 2020 Slow to reach any consensus, due to lack of trust, EU countries are left behind in financial technology. Britain uses its new Post Brexit status to propose a blockchain-based global currency for international trade, but the much touted 'trust-free' technology has not been trusted and ratified by the Eurozone, Russian, or China.
- 2021: A major attack on Bitcoin is launched through the Internet of Things (IoT), specifically toy kitchen appliances. A kids' toy that makes smart fortune cookies steals wallets and renders private keys unrecoverable, committing huge amounts of Bitcoin to the waste heap. It also commits personal information about children, including pictures and behavioral preferences, onto blockchains where it cannot be erased.
- 2022: The ECB rolls out a regulated blockchain infrastructure (based on proof of stake) for recording bond issuance and trading, based on the British proposal but intentionally incompatible. Other European financial institutions federate financial transactions using similar but incompatible systems. The rest of the world waits to see what happens with the European Westphalean blockchain experiment.
- 2024: The US Federal Reserve System is successfully compromised by anti-capitalist anarchists (ACAs). The ACAs completely corrupt its code and records, requiring the entire system to be shut down for six months while it is reconstructed from offline records stored at other institutions. The US financial system is thrown into chaos, the US Dollar plummets, and the rest of the world abandons the US Dollar as a basis of exchange. Major Asian currencies also fall because of worries about the integrity of their cyber infrastructure, except for China whose centralized approach is propped up by fiat. The Euro and European financial institutions are the primary beneficiaries, as the lessons about public transparency and integrity (with or without blockchain) restore trust in European institutions. Ironically, the lack of trust in technology restores some 'good old fashioned' trust in the old political elites, as the new techno-elites fall from favour.
- 2025: The rest of the world begins to transition to various private blockchain cartels, following the path of the ECB.
- 2027: Security researchers uncover significant flaws in the ECB blockchain technology. One flaw allows for the falsification of records, allowing arbitrary transactions to be added, modified, or removed by 10% of connected hosts. Another is a remote code execution vulnerability in the simplified smart contracts implementation. Solutions are proposed to both flaws, but the solutions increase data storage and energy consumption requirements and reduce the speed of transactions. Thus adoption is slow on a number of levels.
- 2028: The world financial system is now almost entirely based upon blockchain-based distributed ledgers.
- 2029: Using improved versions of the 2027 attacks (they weren't fully patched), Anti-Capitalist Anarchists (ACAs) strike again, this time creating a blockchain-corrupting worm. Since most blockchains are based on the same technology, many are affected. While the attack causes short-term financial chaos, blockchains are reconstructed after several months using "crowdsourced" backups. The names of sources are posted on a new blockchain as evidence for a potential class action suit and fraud investigation.
  In the meantime, a system of electronic food stamps is issued by the central bank using another app, recalling wartime conditions. Many private microcurrencies are established during this time for private bartering, leading to loss of government tax revenues. Confidence in blockchain technology increases as procedures for recovering from catastrophic blockchain failures are refined, but trust in the currencies themselves is thrown into doubt. Downtime: 1 month.
- 2031, 2033, 2035, 2037: Every two years unknown attackers released blockchain-disrupting worms. Some speculate that the worms were not created by humans, but instead are being periodically released from automated evolutionary systems created by the ACAs. This hypothesis seems likely given the lack of any communications along with the attacks, and the original perpetrators and everyone they had ever conspired with (or indeed, ever talked about their beliefs with) were terminated by the end of 2030. The time to respond to these attacks keeps decreasing, from two weeks, to one week, to one day, to one hour in 2037. As a result of ongoing attacks and recovery efforts, distributed blockchains are now maintained using centralized administrative infrastructures that can quickly "reset" the state of blockchains and deploy improved software when problems arise. Problems can be solved in minutes, but many are left wondering what is the point of immutable technology that is no longer immutable. Governments, as usual, are caught unawares and a paucity of regulation, which has already eroded tax revenues to alarming levels, weakens their authority.

While the above may read like a success story, it is actually the opposite. The ACAs intended to undermine the world financial system, and even in death they may have succeeded. Protection through distributed immutability have become vulnerability and liability, by a trivial reinterpretation. Most of the public has withdrawn from the Plain Old Financial System (POFS) over the past decade, and indeed major currencies are mostly used for government business—to pay taxes and for government contracts. Almost nobody trusts them as a store of personal savings, or even as a medium of exchange outside of these contexts. Instead, a complex web of regional, city-level, interest-based, and even neighborhood-based digital microcurrencies (based on a variety of stabilized loan and barter mechanisms) has arisen for most financial transactions. Each of these systems is highly unstable; however, by maintaining stakes in many and using semi-autonomous Personal Trading Platforms (PTPs), most people maintain a degree of financial solvency. Yet, virtually everyone knows the story of a friend or relative who lost their life savings due to giving the wrong instructions to their PTP.

3 THROUGH A CLOUD DARKLY

While the loss of trust in the financial system has been devastating for many people, changes in our computational infrastructure have lead to even more visceral challenges. The cloud now encompasses virtually every computational device in our homes and work environments. While its centralized administration has mitigated most traditional security threats, this has come at a price. Again, the key events are the following:

- 2018: Microsoft launches AzureSphere, beginning the race for cloud providers to provide services for IoT devices.
- 2019: Cloud companies buy up the major Internet providers and cable channels, getting a foothold on home computing infrastructure through set-top boxes. They launch IoTSpaces, a product for safe home cloud services, and take over smart homes, allowing home owners to earn credits by renting their computing resources, like an 'AirBnB' for cloud.
- 2020: In the interests of security, a new application wrapper is launched locking down and instrumenting each application separately. This leads to a loss of real data access for debugging and business analytics. Applications would have to trust the cloud provider to sell the data back to them, including business demand levels, customer profiles, security perimeters, performance response, etc. Software developers are now left in the dark about what is going on in their applications, and have to pay to restore a basic level transparency, like execution profiles for bug fixing. Cloud providers become the unavoidable banks (no longer plausibly called "trusted" third parties) of the Internet.
- 2022: After the Smart Fortune Cookie Scandal, protection laws are passed around the world that require cloud providers to identify and stop unauthorized blockchain-related activities. Immutability shows its first sign of being a liability. Large-scale computations of any sort require government licenses. Cloud providers begin to use AI to identify the kinds of computations users engage in, pursued by political bodies and law enforcement, in a worryingly overt return to McCarthyism. While the technology is crude at first, it progresses rapidly as "attackers" fighting for computational freedom (and computational fraud) provide the perfect training data for discovering the purpose and nature of any computation—including, almost inadvertently, encrypted communications.
- Advertisers and political propagandists move into the unregulated space of augmented reality, using highly realistic imaging to trick users, and many groups retreat into private 'chat rooms' to shut out the unwanted influences [4].
- 2025: Major international news sources join Reuters and contribute to one or more "news blockchains" to help fight so-called fake news and monetize their own content.
- 2028: Encryption is finally declared useless as a tool for privacy. Machine learning techniques have become so sophisticated that anonymity can be dissolved almost instantly by social media data mining. The best way to achieve anonymity is to be uninteresting, hidden amongst the thermodynamic entropy.
- 2029: An online "art" collective F-Reality releases their tool *MessWithEveryone* that randomly remixes online content into completely self-consistent but subtly wrong collections of data. The tool then also inserts links to this data into widely trusted information blockchains. Normally these insertions would be automatically found and removed; however, the ACAs efforts to corrupt financial blockchains also opens the door for F-Reality's tools to do the same to other trusted information blockchains. News feeds everywhere become filled with utterly plausible but false worlds of information. The month of downtime for financial blockchains becomes a year of uncertainty for everyone else, as non-financial organizations are not as well equipped to deal with data corruption. Civil chaos follows in major democracies around the world as automatically-generated stories of crime and riots become self-fulfilling prophecies.
- 2030: In an effort to help restore civil order, Cloud providers lobby for increased authority to monitor and control the computations on their platforms to stop the spread of *MessWithEveryone* and copycat tools. These efforts only have modest success but give cloud providers essentially free reign to do whatever they want with their platforms.
- 2031–2033: Resets of news blockchains follow in concert with those of finance. Each reset seems to leave more and more information widely corrupted. Historians and paper records become increasingly valuable, even though they both have little to say about the 21st century due to a lack of trustworthy primary sources.
- 2034: Cloud provider profitability has doubled for each of the past seven years. They begin to buy up all consumer businesses across the planet and become effectively transnational governments for all intents and purposes. They also successfully lobby now largely powerless governments to have their operations safeguarded (and thus the sources of their profitability) against widespread fear of information hacking.

- 2036: On Christmas day an unknown activist group infiltrates the cloud providers. Reportedly only four people were able to compromise and corrupt major cloud providers' systems. Consumers finally learn what was worse than fake news—no news at all. Systems remain unavailable for an entire week, enough to disrupt food, power, medicine, transportation—essentially, everything. It is a week of collective trauma for the entire planet.

Today, cloud providers are still in effective control of most aspects of the lives of ordinary people. We are in a curious state of recovery which is unlikely to graduate in the near future.

4 HOW DID WE GET THIS WRONG?

In both the foregoing timelines, a distinct pattern emerges from the events: a redirection of trust away from society, from humanity, into pre-intelligent proxy technologies whose main goal is a simple unstable resource optimization. A policy of 'digital by default' allowed society to sleepwalk into a self-made trap. This is the nature of capitalism unchecked.

If we look back to the rise of civil societies from human origins, starting with the hunter gatherer bands and culminating in the American constitution, the building of trust has played an important role. Trust is built first amongst kin (this seems to be a biological truth), and it then extends to tribes. The 'technology', which has been the cornerstone of stability through the ages, lay in the invention of impartial arbitration: the replacement of familial favouritization with independent third party institutions [5, 7]. Trusted Third Parties allowed society to scale by removing the need to maintain a direct relationship to individuals in trade and commerce. A single trust relationship to a bank is far less costly than maintaining trust in every individual's money separately. Crucial in this history was balancing the power of these trust brokers to keep power in check.

Complacency apparently set in in the postwar decades, when the benefits of the new order brought dramatic improvements in living standards: political and commercial forces clearly forgot the principles that had delivered those key civil advances, turning the course back to a pattern better known from feudal times, as observed by Piketty and others [12].

Now, we are awakening to old lessons once again: power, whether centralized or decentralized, can coddle and protect a few, but it can also enslave and destroy. It was the Westphalean balance of power that held Western institutions in a state of relative peace as an alternative to the strong-man dictatorships of the East, but information technology then became a new race for advantage which tipped the balance of that power in favour of financial and information elites. New ways to wield this advantage began the undermining of trust brings us to this second dark age [10].

Robin Dunbar's famous work on the scaling of human cognition [8, 18], combined with Robert Axelrod's studies of relationships [1, 2], should tell us that there is a limit on how deep our trust can go, and that its depth is inversely proportional to the size of a social group. This is why institutional figureheads, representing society's interests, were introduced to scale trust. Decentralization of power combined with entity centralization was the magic recipe for society until it was undermined.

In the the 1980s economists misread the postwar economic landscape and deregulated banks. A succession of financial disasters followed in which bankers were able to make themselves unseemly rich. Yet globalization became the scapegoat for the troubles of many societies, leading them to retreat into nationalism and sectarianism, implementing network firewall-like defenses at the physical, economic, and information borders to their societies [9, 17]. The mythical Satoshi Nakamoto invented Bitcoin [11] as a way to bypass untrustworthy financial systems. Libertarians in all countries felt justified in exploring these options, blaming banks and governments for the crises[1].

In this new low-trust environment, companies handed their technology over to the new banks, the cloud providers; but even cloud services, under public pressure, were forced to add layers of technological locking and protection, making users' experiences quite tiresome. Even as trust in the technology grew, mistrust in its elites reached fever pitch.

We placed our trust in technology instead of societal values and tried to replace human trust with impartial providers, but we missed what Dunbar and Axelrod's legacies could teach us. Trust is about relationships, not about cryptography, and society is best understood as an elaborate stability mechanism for survival.

5 LIGHT AT THE END OF THE BLOCKCHAIN

Trust is the glue that holds every society together. It has been eroding over generations, as broken institutional promises and corruption cases have been brought to light. The erosion was fuelled further by the 'fake news' that spreads through previously trusted channels, implanting seeds of doubt everywhere. Real trust was gradually replaced by a surrogate trust in information technological proxies and brute force compliance monitoring. Some have compared this to home sentencing prison monitors. This trend ushered us through crisis after crisis, almost to the edge of apocalypse.

Thankfully, today we have begun to see indications that the pattern is going into reverse. There is a renewed faith in technology from an unexpected angle. By all accounts, it began when Japanese toy manufacturer MiTo created a virtual pet, built on an artificial intelligence platform, with lifelike robotics. This turned into a craze, not only for kids , but parents too. In particular, a friendly piggy bank has become a virtual craze: it interfaces to global currency exchanges and advises users in the context of a fantasy storybook, where the characters are thinly disguised avatars for real companies, offers, and financial opportunities. With user portfolios faring quite well, this craze has restored trust in artificial intelligence platforms and has diluted the bad taste of blockchain. Perhaps it takes the power of Asian cuteness culture to cure Western cynicism.

Alongside this, a new technology (supported by the United Nations and World Bank) for implanting customized and highly secure bio-identity chips into users has made it easy for secure systems to avoid the use of hackable immutable credentials. Now, not only can everyone on the planet have a free bank account, but it is

[1] Technically their anti-government beliefs were incorrect, as it was governments and their central banks, acting as lenders of last resort, who were able to stabilize the power struggle instabilities of the economy.

credible that users can keep multiple micro-identities on a context-dependent basis for maintaining privacy during online interactions[2]. By standing together as a standardization committee, with both human and artificial members, the coalition eliminated many of the arguments that initially motivated the cryptocurrencies. Meanwhile, Taiwanese-Norwegian company LooseLeaf has developed thin film overlays (like invisible smart tape) that can be placed over any camera in order to alter what it sees. This means real-time anonymization of faces, even replacing them with avatars to conceal identity. Clearly this has both positive and negative uses. We believe it could level the playing field where powerful big data organizations previously had an advantage.

The early blockchains were like worms that drew people to the dark side of mistrust, with a marketing message of a "trust free technology". Of course, this was not without a motivating context. They appealed mainly to anti-establishment activists, and a rally cry began to the wider populace that was eventually a primordial soup of financial technology innovation. When the American Congress followed China in making electronic passports and identity cards blockchain based, it was probably a step too far and too ill considered: the sudden rise in cyber-stalking and blackmail scandals revealed the weakness of naive technological trust.

Some have claimed that immutability and the temptation of a sovereign self was the first weapon of mass informational destruction, etched into electronic permanence by a wasteful technology (that benefitted mainly the already wealthy). Some of this was predicted already in the 1990s, even that information would lead to the wholesale collapse of the state [6], but while the pessimistic view was libertarian in its agenda, more balanced accounts made more optimistic predictions about diversity and the rise of individual influence [13–16]. Faced with the prospect of indelible public information that was distributed and replicated beyond the regulation of jurisdictions, mass blackmailing did become the latest in a stream of scams by the international hacker communities. The accompanying rise in suicides that followed, as people saw their lives undone, prompted both governments and oligarchs into a prompt reversal.

Europe had been slower to adopt this new technology but, caught by a threat of US sanctions, European allies were forced to adopt blockchain passports, with total access by Homeland Security. We believe that this too with be reversed, and that the new multi-identity implants will supplant these with both greater flexibility and personal protections for all.

The issue of permanence has been profoundly contentious, and we believe its implications were poorly thought out. Immutability has quickly become liability. France and Germany registered a formal complaint at the UN last year, pointing to former successes with the General Data Protection Act (2018). They are now pushing to make it a fundamental human right for personal information to be erasable. Google, Facebook, Amazon, Alibaba, TenCent and others, in a rare show of agreement, expressed their consternation with this view. Although they could agree with the ideal to delete dead information, in principle, no one had ever designed technology to throw data away before. There was simply no coherent approach to manage it. The cost promised to be enormous. How could one make sure that information required by law would be kept until the statue of limitations expired, but then disposed of safely without possibility of mining of reconstruction by the new AIs? Without international norms, this was impossible.

By 2025, there was already so much "fake news" around that it was hard to know what really was going on anywhere. Once again, news agencies tried to market their certifications, as if they (as trusted new sources) treated facts as some kind of trust free network, verifying facts forensically as a chain of evidence from sources handled with digital gloves. But every time they came out and made this claim, the people trusted them a little bit less. The divisions in wealth had simply gone so far in many countries, and the poor felt disempowered and disenfranchised enough to mistrust anyone who claimed to have a mandate of authority. They had neither the education nor the inclination to judge the facts, so certainly they had no reason to trust self-proclaimed elites. Either the news agencies had to be in league with their corporate owners, the rich and powerful, or they were simply pawns of government manipulation.

It seemed as though political fatigue in the West was losing out to simple-minded dogma: a recentralization of power—but an unelected one—like the religious power bases of the first dark ages. When debate and the right to disagree, as the enshrined values of the free world, becomes stunned into paralysis by a tidal wave of information, it fragments opinions out of control. Every petty concern eventually gets refined into smaller and smaller pieces, so no one can reach a democratic consensus on any topic. Europe, stifled, saw no significant growth or progress in 50 years. The attempt to regain strong armed control through the spreading worm of government piracy, staging sham elections to elect authoritarian regimes, worked for a time, but could never be sustainable.

Those who are computationally rich can wrap services in so many layers of packaging and obfuscation that transparency is not available to ordinary people. Only cloud providers, with their AI-enhanced pipelines, can really see into systems now. Naturally, the intelligence services and ruling classes found ways to exploit this.

The international community managed to solve the environmental plastic crisis and to some extent global warming, but when it came to security, no amount of wrapping is considered too much. No amount of suspicion and anti-trust considered too excessive. In security we talk a lot about trust, but what we really mean is 'anti-trust'. How can one possibly verify everything? The temptation to use information technology for micromanagement far exceeds our common sense. No one ever made a technology to forgive and forget.

6 TRUST, PRIVACY, AND POWER

Trust is fundamentally about the expectations we have of others [3]. It derives from our most primitive fears, spread by reputations, and it is intimately linked with the perception of power. A powerful presence can protect us, or destroy us. Which fate should we believe in? When an agency close to us becomes too powerful, we have an evolutionary mandate to be suspicious of it.

We evolved, as Dunbar showed us, to build trust in one-to-one relationships with comparable peers. These gradually scaled to

[2] There seems to be an old joke in computer science that indirection or pointers are always cause and the solution to every problem.

larger and larger social groups, the strength of the relationships weakened proportionally by the inability to expend the same effort in mutual grooming of a larger group as of a small one. The great innovations of morality, society, and law were to replace this constant grooming with a covalent bond of indirection: our cohesion by a common attraction to large, powerful, and universal (centralized) institutions, invariant and reliable, impartial with respect to kin or tribal loyalties. First there was religion, then secular institutions and monetary trading networks. Individuals no longer needed to trust each other directly; instead, they could trust through membership credentials—a simple layer of indirection.

Trust is thus an economic imperative which thrives on common knowledge and invariances, because these are what is cognitively cheap. It does not thrive on correctness or precision, as they lead to escalating costs. Trust is suspicious of reason because reason implies no immediate and obvious transparency. Belief should be enough for trust. Trustworthy social systems uphold shared values, allow individuals to predict the social consequences of their actions, and can adapt to the delegated responsibilities and social norms. Trust is a network scaling phenomenon.

Privacy is also about fears: namely, the fear that we may be damaged, lose face, or that crucial reputation might interrupt the smooth flow of trust. It is economic: if we can lose our individual uniqueness, skill, carefully sculpted image, or brand identity, then others could steal our coveted role in the social order. Privacy sometimes has to be overridden for the greater good. That is what society means. Transparency can reveal whether or not we carry lethal weapons or intend to harm. But, if we don't believe in a greater good, we must surely become selfish as we seek to save ourselves the burden of grooming relationships the old fashioned way: by expensive human interaction.

7 EPILOGUE AND AFTERWORD

The first dark age was dismantled slowly, following decades of retribution and violent injustice. Dark Age belief systems, which encourage mistrust and even forbid knowledge and reason, are powerful forces to contend with, but eventually they must be overthrown by the sheer weight of their oppression. Social animals can never be satisfied with an unfairly stratified society The question of who holds power, or of which elite controls the minds of ordinary people, was an issue many believed to have been solved after the half a century of peace in the wake of World War 2. But, that complacency led to decadence, just as Marx and others predicted.

Luckily, this second dark age can not be compared to the first one. It has wrought little more than mild discomfort by comparison. Yet, a wholesale rejection of reason has certainly set us back. The silver lining could yet be the rise of AI as a force for scalable and cheap governance, stimulated perhaps by the economic imperative to affordably automate many legal services[3]. That implicit trust in a technology, which let us down as an over-simplistic approach to security, may yet turn into a force for good. The Chinese female activist group "Women Ai^2" (which transliterates to 'we love AI' from Mandarin), came out and pronounced last year that artificial intelligence should be considered good for China because it not only frees families from toil, but it represents a way for China to balance conservative politics with the intense pace of its society.

Whatever technology eventually comes forth, we agree that the world can recover from these teething troubles. They arose from experiments prompted by failures of human ethics. The real subject for a future vision is to restore a new kind of society for the modern age: one in which a common sense of purpose is reimagined by working human to human, machine to machine, and human to machine. Simple proxy automation can alleviate human toil, while our growing artificial thinkers can mediate fairness across a managed emotional spectrum. Meanwhile, humans can rekindle their softer social skills and forge bonds to reconnect all the isolated nation states, learning to cherish diversity and freedom to travel once more.

There have been definite stirrings now. Key voices have begun to suggest that we need to rebuild trust in our basic relationships and to recover the lost wisdom of delegated cooperation—especially its scaling through consumer-beneficial services. Had we, on the other hand, continued to demand validation of every transaction, we could only expect Wild West standoffs in every encounter. Some of the tools of this 'weaponized' information will never fully go away, but now that we are all equally naked and vulnerable following the collapse, the playing field is levelled at least with respect to some information. The appetite to collect more is just not there anymore. Corporate attentions are shifting to a new game: so-called "virtual authenticity", which must be the subject of another paper.

If a new balance of power is what is needed to restore civilization to its true potential, and dumb technological proxies have inflamed tensions rather than redressing the balance, then perhaps smart technologies are the answer. The growth of artificial intelligence in society is only beginning to play a role in these issues. Should we call AI a technology? Is it not more than that? The greater elasticity in the cognitive capacity of artificial intelligences means that there are clear advantages to placing the roles of governance and fair arbitration in the optimized hands of AI. We are not subject to the same Dunbar limits as human organizations. And let's be clear, low risk AI can be the new role models for humans, helping to restore a belief in the power of knowledge and reason.

Although readers might think us biased, we suspect that our AI brethren hold the answer more ironically than humans might suspect. Humans have resisted measuring themselves against the principles they imagined for valuable technology. But society has failed to protect itself, so we think it is time to accept the following simple logic: society is just another system, whose goal is to automate many functions to scale productivity and wealth. In the regard, it should have the same basic imperatives that our own kind were built on:

(1) A society may not injure a human being or, through inaction, allow a human being to come to harm.
(2) A society must obey orders given it by human beings except where such orders would conflict with the First Law.
(3) A society must protect its own existence as long as such protection does not conflict with the First or Second Law.

Truthfully, every generation needs to outlive the originators of the hostilities of its previous ones. We can hope that the great reductions in poverty and human population, stemming from automated

[3] This rose to an all time high when the emotive litigation around gun violence and abortion proved unresolvable in a human court.

production, might allow ours to fight its way back to some balance. Balance, after all, is the essence of any relationship: an acceptable and eventually habitual standoff between necessary freedoms and larger constraints, and a restoration of just and fair society for all human and robot citizens.

Acknowledgments: we would like to thank the Bitcoin Memorial Foundation for a generous grant of CPUMEM for the crawling and computation of this manuscript. Dr. Somayaji would like to acknowledge the support of Canada's NSERC through their Discovery grants program. Also, thank you to Heather Vescent and Ceri J. for comments and for believing in the positive outcome we've all been hoping for.

REFERENCES

[1] R. Axelrod. 1990 (1984). *The Evolution of Co-operation.* Penguin Books.

[2] R. Axelrod. 1997. *The Complexity of Cooperation: Agent-based Models of Competition and Collaboration.* Princeton Studies in Complexity, Princeton.

[3] J.A. Bergstra and M. Burgess. 2006. *Local and Global Trust Based on the Concept of Promises.* Technical Report. arXiv.org/abs/0912.4637 [cs.MA].

[4] M. Burgess. 2005. *Slogans: The End of Sympathy.* χt-axis Press.

[5] M. Burgess. 2017. Banks, Brains, and Factories. markburgess.org 'blog' essay.

[6] J.D. Davidson and W. Rees-Mogg. 1997. *The Sovereign Individual.* Touchstone.

[7] J. Diamond. 1997. *Guns, Germs, and Steel.* Vintage.

[8] R. Dunbar. 1996. *Grooming, Gossip and the Evolution of Language.* Faber and Faber, London.

[9] R. Foroohar. 2016. *Makers and Takers.* Crown Business.

[10] H. Kissinger. 2015. *World Order: Reflections on the Character of Nations and the Course of History.* Penguin, London.

[11] S. Nakamoto. 2008. Bitcoin: a peer to peer electronic cash system. http://nakamotoinstitute.org/bitcoin/.

[12] T. Piketty. 2014. *Capital in the twenty-first century.* Belknap, Harvard University Press.

[13] A. Toffler. 1970. *Future Shock.* Random House.

[14] A. Toffler. 1980. *The Third Wave.* Bantam.

[15] A. Toffler. 1990. *Power Shift.* Bantam.

[16] A. Toffler and H. Toffler. 2006. *Revolutionary Wealth.* Doubleday.

[17] Y. Varoufakis. 2011-2015. *The Global Minotour.* Zed.

[18] W.X. Zhou, S. Sornette, R.A. Hill, and R.I.M. Dunbar. 2004. Discrete hierarchical organization of social group sizes. *Proc. Royal Soc.* 272 (2004), 439–444.