Richard Gendal Brown

Thoughts on the future of finance

POSTED BY

GENDAL
POSTED ON

AUGUST 24, 2016
POSTED UNDER

BLOCKCHAIN, CORDA, R3, UNCATEGORIZED, WHITEPAPER
COMMENTS

2 COMMENTS

Corda: An Introduction

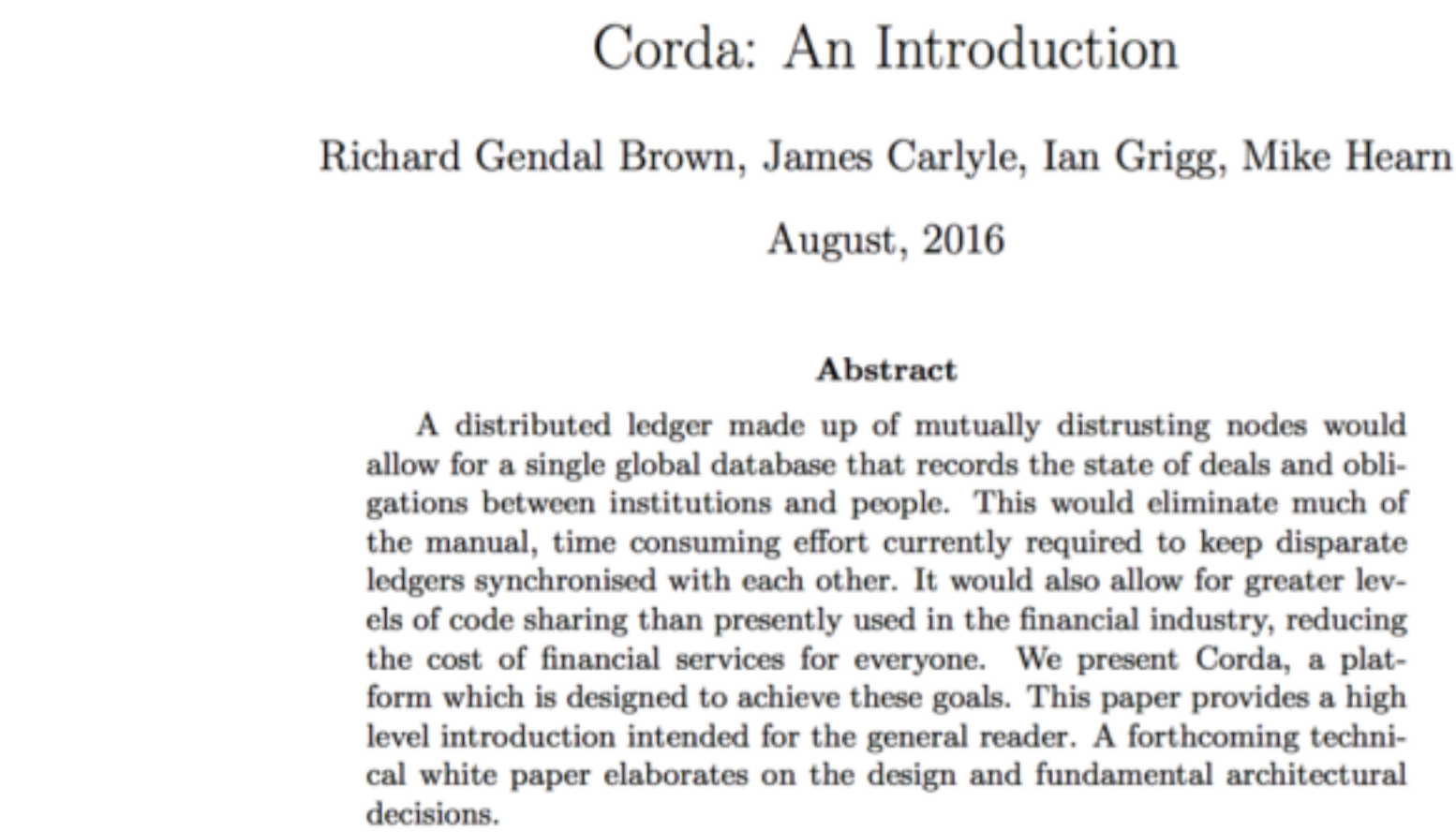
Announcing the Corda Introductory Whitepaper

The Wall Street Journal had a couple of (http://blogs.wsj.com/moneybeat/2016/08/24/a-closer-look-at-r3s-concord/?mod=ST1) good pieces (http://www.wsj.com/articles/bitcoin-tech-firm-thinks-this-name-can-unify-wall-street-behind-blockchain-1472044968?mod=ST1) this morning that describe some of the work we're doing at R3 and our vision for the future of financial services.

Project Concord is our codename for the overall vision, with Corda as our underlying distributed ledger software.

I first wrote about Corda (https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/) back in April and we demonstrated it in public (http://www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-first-ever-public-demo-r3s-corda-platform-1555329) for the first time a few weeks later. Since then, we've been continuing to develop the code base in collaboration with our members, trialling it through an ongoing series of proofs-of-concept, prototypes and more advanced deployments, refining the design and maturing our thinking.

As part of this process, we wanted to share more information with the broader community about what we're doing. I'm pleased to announce the release of our first whitepaper on Corda (http://r3cev.com/s/corda-introductory-whitepaper-final.pdf): an introductory, non-technical overview that explains our vision, some design choices and outlines the key concepts underpinning the platform. We'll follow this up in the coming months with a more detailed technical whitepaper.



Corda: An Introduction

Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn

August, 2016

Abstract

A distributed ledger made up of mutually distrusting nodes would allow for a single global database that records the state of deals and obligations between institutions and people. This would eliminate much of the manual, time consuming effort currently required to keep disparate ledgers synchronised with each other. It would also allow for greater levels of code sharing than presently used in the financial industry, reducing the cost of financial services for everyone. We present Corda, a platform which is designed to achieve these goals. This paper provides a high level introduction intended for the general reader. A forthcoming technical white paper elaborates on the design and fundamental architectural decisions.

The whitepaper, which you can download here (http://r3cev.com/s/corda-introductory-whitepaper-final.pdf), explains how we set ourselves the challenge of starting with the financial industry's pain points: duplicated, inconsistent data and business logic and redundant business processes – and asked ourselves if we could apply breakthroughs in distributed ledger and blockchain technology to solve them.

Our conclusion is that distributed ledger and blockchain technology represents a once-in-a-generation opportunity to transform the economics of data management across the financial industry. But there's a problem because the blockchain and distributed ledger platforms that led us to this exciting moment were never designed to solve the problems of financial institutions and do not meet all our needs: we need tight linkage to the legal domain; we have an obligation to prevent client data being shared inappropriately and so can't send all transactions to all network participants; we must integrate and interoperate with existing financial infrastructure; and more.

Corda is the outcome of the analysis we did on how to achieve as many of the benefits of distributed ledger and blockchain technology as possible but in a way that is sympathetic to and addresses the needs of regulated financial institutions. Corda is intended to be a contribution to the plurality of technologies that will be adopted in the coming years, one that is targeted specifically and with a laser-focus on the needs of financial institutions.

I hope you find the whitepaper interesting and illuminating and we would love to hear your feedback.

POSTED BY

GENDAL
POSTED ON

APRIL 5, 2016
POSTED UNDER

BLOCKCHAIN, CORDA, DISTRIBUTED LEDGER, R3
COMMENTS

42 COMMENTS

Introducing R3 Corda™: A Distributed Ledger Designed for Financial Services

As reported in Bloomberg (http://www.bloomberg.com/news/articles/2016-04-05/protecting-trade-secrets-challenges-wall-street-blockchain-play) this morning, I'm delighted to confirm that R3 and our member banks are working on a distributed ledger platform for financial services: ***Corda***™. I explain it on our official R3 blog (http://r3cev.com/blog/2016/4/4/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services) and reproduce it here.

For the last six months, my team and contributors from our membership have been building a distributed ledger platform prototype from the ground up, specifically designed to manage *financial agreements* between regulated financial institutions. I am massively excited by the progress our team, led by James Carlyle, our Chief Engineer, and Mike Hearn, our Lead Platform Engineer, are making and I think the time is right to share some details.

Corda: A Distributed Ledger for Recording and Managing Financial Agreements

Corda is a distributed ledger platform designed from the ground up to record, manage and synchronise financial agreements between regulated financial institutions. It is heavily inspired by and captures the benefits of blockchain systems, without the design choices that make blockchains inappropriate for many banking scenarios.

Corda's key features include:

- Corda has no unnecessary global sharing of data: only those parties with a legitimate need to know can see the data within an agreement
- Corda choreographs workflow between firms without a central controller
- Corda achieves consensus between firms at the level of individual deals, not the level of the system
- Corda's design directly enables regulatory and supervisory observer nodes
- Corda transactions are validated by parties to the transaction rather than a broader pool of unrelated validators
- Corda supports a variety of consensus mechanisms
- Corda records an explicit link between human-language legal prose documents and smart

contract code
- Corda is built on industry-standard tools
- Corda has no native cryptocurrency

Corda's design is the result of detailed analysis and prototyping with our members and will be open sourced when the code has matured further.

In the remainder of this post, I want to share some insight into our thinking. Why are we building Corda? Why have we made some of the design decisions we have? When will the code be ready for others to examine and build upon? How does this relate to other platforms and projects?

A thought experiment

When I joined R3 from IBM in September 2015, I forced myself to stop and think. The blockchain bandwagon was running at full speed, I'd just been appointed CTO of a project intended to bring blockchains to finance but there was a nagging worry at the back of my mind… how could I avoid falling into the trap of believing all the hype?!

I imagined myself sitting in front of the CIO of one of our member banks some time in the future. I imagined we had naively selected a "blockchain for finance" based on what was popular at the time and widely deployed a range of products and services on top of it. And I imagined we had believed the hype, had suspended our critical faculties and had omitted any engineering. In this imagined scenario, I now found myself facing an angry CIO, who wanted to know why the system I had built had just failed calamitously. *Why on earth did I build it the way I did?!*

I concluded that an entirely inappropriate answer to that question would be: "because blockchains were cool in 2015"! No. That simply won't do.

The reality is that solutions based on selecting the design first and then trying to apply it to arbitrary problems never work out well. Every successful project I've worked on started with the *requirements*, not some cool piece of technology, and I was determined to bring that discipline into our work at R3.

Remind me again why a system designed to replace banks is also supposedly their saviour?

And there is a second reason for this caution: the technology and finance industries collectively "decided" some time in early 2015 that "blockchain technology" was somehow the future of financial services.

Indeed, I am one of the most active proponents of precisely that claim. But the *reason* for blockchain technology's importance is extremely subtle – and this subtlety is something that most people seem to have missed.

To understand this, we need to look at Bitcoin.

Bitcoin's architecture, as I have often written, is a marvel. Its interlocking components are one of those rare examples of something so elegant that they seem obvious in hindsight, yet which required a rare genius to create.

But what is often missed is that the cleverest part of Bitcoin isn't actually its architecture; I think the cleverest part was to articulate the *business problem*. We don't tend to think of Bitcoin as being the solution to a "business problem" but it can perhaps be thought of as a wonderfully neat solution to the problem of: "how do I create a system where nobody can stop me spending my own money?" Now, I can't claim to know the mind of Satoshi and he certainly didn't write the whitepaper in this way but it triggers a very useful thought-experiment.

In fact, once you write this 'business problem' down, the design drops out almost trivially! (Almost…) You want always to be able to spend your own money? Then you can't have a central point of control. It could be shut down by the authorities. You can't even have a collection of validators with known identities as they could also be shut down with concerted effort. Very quickly you realise you need a massively replicated consensus system and, if you don't want to tie actions to real-world identities, you need something like Proof of Work to make the voting work. You work the logic through and pretty much the whole design (the blockchain, the need for mining, block rewards, maybe even the UTXO transaction model, etc., etc.) drops out. Of course, it does push a lot of work onto the users: confiscation of somebody's bitcoins is easy if you know their private key… but let's leave that to one side for now.

And this way of looking at it is important because it highlights how Bitcoin's blockchain can be thought of as the *solution* to a business problem. Satoshi Nakamoto didn't wake up one morning wanting to "apply Blockchain to finance". Blockchain was the tool that was invented to solve a real problem.

So we have a conundrum, right? If that's the case, then *what on earth* is the argument that says blockchain has *any* relevance at all to banking?!

Indeed, last time I checked, banks have the *inverse* of my Bitcoin problem statement!

What is the defining characteristic of blockchain systems?

So I spent most of October sitting in a dark room (really! This was our first London office… a tiny four-person room in a shared working space in the City of London) questioning some of the most fundamental assumptions about blockchains. *What is it exactly that makes them interesting to banks?*

Most people had already made the mental leap that the "bitcoin package" was unacceptable as a take-it-or-leave-it deal: proof of work is unnecessary for private deployments, for example. But, as I looked around, all I could see was firms who had accepted everything else… It seemed strange to me that, as an industry, we could tease apart *one* part of the "blockchain bundle" but then stop there.

I spent several of my earlier, formative years at IBM in a role called "technical sales". If you've ever bought technology from a large IT vendor, you'll have met somebody like me. We're the people who visit clients with the sales rep and act as the technical expert: we explain how the product works, make sure we're proposing the right solution to the client and ensure there is no technical barrier to closing the deal.

A lesson I learned very early in that role was: it doesn't matter how hard you wish or how many client meetings you schedule or how aggressive the sales rep gets, if you can't show how your solution is going to solve the client's business problem then the deal almost certainly won't close. And those that do are the ones you'll live to regret…

Fast forward a decade, and as I surveyed the blockchain landscape in October 2015, all I could see was excitable (and vocal!) firms touting solutions that made very little sense to me for the kinds of problems I was trying to solve. I will confess to many moments of self-doubt: maybe they were all sane and *I* was the mad one..?!

But I ploughed on: even if they *are* right that a "take it or leave it" blockchain design is the saviour of the financial industry, I'll be doing our members a favour if I could explain *why*.

So we started picking away at what can perhaps be called the "blockchain bundle": the collection of services that blockchains provide to those who use them.

We concluded that a blockchain such as the ones underlying Bitcoin or Ethereum or any of the private variations actually provide at least five interlocking, but distinct, services. And the right approach is to treat them as a *menu* from which to select and customise… different combinations, in different flavours, for different business problems.

CONSENSUS

The first, and most important, feature of blockchains – and the thing that is probably genuinely new in terms of scale and scope – is that they create a world where *parties to a shared fact* know that the fact they see is the same as the fact that other stakeholders see:

"I see what you see… and I know that what I see is what you see"

And, critically:

"I know that you know that I know"!

And:

"I know that you know that I know that you know…"

And so on…

And it makes this promise across the Internet between mutually untrusting parties. Sure: consensus systems and replicated state machines have existed for years but consensus systems at Internet scale, between untrusting actors, that work in the face of powerful adversaries? That's a step forward.

In Bitcoin, the shared facts are things like: "What are all the bitcoin (outputs) that have not yet been spent and what needs to happen for them to be validly spent?". And the facts are shared between all full node users.

In Ethereum, the shared fact is the state of an abstract virtual computer.

But notice something interesting: there isn't some law of nature that says the set of people who have to be in consensus is the whole world. Bitcoin just happens to work that way because of its unique business problem. If you don't have Bitcoin's business problem then be very wary of those trying to sell you something that looks like a Bitcoin solution.

VALIDITY

The second feature in the "blockchain bundle" is *validity*. Tightly linked to consensus, this feature is the one that allows us to know whether a given proposed update to the system is valid. It is how we define the *rules* of the game. What does a valid "fact" look like in the system? What does a valid update to that fact look like?

UNIQUENESS

The third feature in the blockchain bundle is its "uniqueness service". I can quite easily create two perfectly *valid* updates to a shared fact but if they *conflict* with each other then we need everybody who cares about that fact to know which, if either, of those updates we should select as the one we all agree on. The "anti-double-spend" feature of blockchains gives us precisely this service and it's hugely important.

IMMUTABILITY

The fourth feature in the "Blockchain Bundle" is often, if misleadingly, termed "immutability": data, once committed, cannot be changed.

This isn't quite true: if I have a piece of data then *of course* I can change it. What we actually mean is that: once committed, nobody *else* will accept a transaction from me if it tries to build on a modified version of some data that has already been accepted by other stakeholders.

Blockchains achieve this by having transactions commit to the outputs of previous transactions and have blocks commit to the content of previous blocks. Each new step can only be valid if it really does build upon an unchangeable body of previous activity.

AUTHENTICATION

The final critical feature in the "Blockchain Bundle" is authentication: every action in the system is almost always associated with a private key; there is no concept of a "master key" or "administrator password" that gives God-like powers. This is quite different to traditional enterprise systems where these super-user accounts are prevalent and petrifying from a security perspective.

So what is the *financial services* business problem?

So why did I take us through this analysis? Because it gets us to the heart of the distributed ledger domain: the thing that is *genuinely new* is the emergence of platforms, shared across the Internet between mutually distrusting actors, that allow them to reach consensus about the existence and evolution of facts shared between them.

So if that's what this is all about, then what are the "shared facts" that matter in finance? What business problem would we need to have for any of this work to be of any use at all?

And this is the light bulb moment *and the fundamental insight driving the entire Corda project*:

The important "shared facts" between financial institutions are *financial agreements:*

- Bank A and Bank B agree that Bank A owes 1M USD to Bank B, repayable via RTGS on demand.
- *This is a cash demand deposit*
- Bank A and Bank B agree that they are parties to a Credit Default Swap with the following

characteristics
- *This is a derivative contract*
- Bank A and Bank B agree that Bank A is obliged to deliver 1000 units of BigCo Common Stock to Bank B in three days' time in exchange for a cash payment of 150k USD
- *This is a delivery-versus-payment agreement*
- … and so on…

The financial industry is pretty much *defined* by the agreements that exist between its firms and these firms share a common problem: the agreement is typically recorded by *both* parties, in *different* systems and *very large* amounts of cost are caused by the need to fix things when these different systems end up believing different things. Multiple research firms have postulated that tens of billions of dollars are spent each year on this problem.

In particular, these systems typically communicate by exchanging *messages*: I send an update to you and just *hope* you reach the same conclusion about the new state of the agreement that I did. It's why we have to spend so much money on reconciliation to check that we did indeed reach the same conclusions and more money again to deal with all the problems we uncover.

Now imagine we had a system for recording and managing financial agreements that was *shared* across firms, that recorded the agreement consistently and identically, that was visible to the appropriate regulators and which was built on industry-standard tools, with a focus on interoperability and incremental deployment and which didn't leak confidential information to third parties. A system where one firm could look at its set of agreements with a counterpart and know for sure that:

"What I see is what you see and we both know that we see the same thing and we both know that this is what has been reported to the regulator"

That's Corda.

How does Corda choose from the "Blockchain Bundle" Menu?

So now we understand the financial services requirement, we can look again at the "Blockchain Bundle" menu from above and outline the choices we've made.

CONSENSUS

A critical piece of the Corda philosophy is that our problem is to ensure that "I know that you see the same details about a shared fact that I see".

But this *does not* mean that a third party down the road also needs to see it: our consensus occurs between parties to deals, not between all participants.

VALIDITY

Furthermore, in Corda, the only people who need to be in agreement about a fact are the stakeholders to that fact: if you and I agree about something that pertains only to us then why should we care what some completely unrelated third party thinks? And why would we even **think** of sending them a copy so they could opine on it? So, in Corda, we let users write their validation logic in time-tested industry-standard tools and we define who needs to be in agreement on a transaction's validity on a contract-by-contract basis.

UNIQUENESS

Just like every other distributed ledger out there, we need to be sure that two valid, but conflicting, transactions cannot both be simultaneously active in the system. But we also recognise that different scenarios require different tradeoffs. So Corda's design allows for a range of "uniqueness service" implementations, one of which is a "traditional blockchain". But it doesn't need to be and, for our purposes, we also need implementations that make different tradeoffs under Brewer's CAP theorem (https://en.wikipedia.org/wiki/CAP_theorem): in particular, some financial services use-cases need to prioritise consistency at the expense of availability in the event of a network partition.

IMMUTABILITY AND AUTHENTICATION

Here, Corda's design departs very little from existing systems: our data structures are immutable and our building block is the exchange of digitally-signed transactions.

So Corda is very traditional in some respects – we directly apply the "authentication", "immutability" and "uniqueness service" features of blockchains but we depart radically when it comes to the scope of "consensus" (parties to individual deals rather than all participants) and "validation" (the legitimate stakeholders to a deal rather than the whole universe or some arbitrary set of 'validators').

How is Corda Different?

Hang on? Isn't this the same pitch that every other blockchain firm is making? Not quite.

Notice some of the key things: firstly, we are *not* building a blockchain. Unlike other designs in this space, our starting point is individual agreements between firms ("state objects", governed by "contract code" and associated "legal prose"). We reject the notion that all data should be copied to all participants, even if it is encrypted.

Secondly, our focus is on agreements: the need to link to legal prose is considered from the start. We know there will still always be some disputes and we should specify right up front how they will be resolved.

Thirdly, we take into the account the reality of managing financial agreements; we need more than just a consensus system. We need to make it easy to write business logic and integrate with existing code; we need to focus on interoperability. And we need to support the *choreography* between firms as they build up their agreements.

Different Solutions for Different Problems

But… we should be clear. We are not viewing Corda as a solution to all problems. This model is extremely powerful for some use-cases but likely to be less well suited to others. It's why we continue to engage extremely deeply with all our partners who are working on complementary platforms in this space; we are not omniscient. Moreover, there are still many significant design and research questions we have to resolve: there is still a great deal of work to do.

Furthermore, I have been deeply impressed by the quality engineering embodied in the many platforms that have passed through our labs and you will continue to hear about projects we are delivering on platforms *other* than Corda: different solutions for different problems is our mantra. Indeed, those who have attended panels or workshops in recent months will have heard me saying this for some time now.

Corda does not seek to compete with or overlap with what other firms are doing: indeed, we are building it because no other platform out there seeks to solve the problems we're addressing. That's what makes this space so endlessly exciting.

What next?

In the coming weeks and months, you'll hear more about Corda, about our initial projects and about its design. We will also be gearing up to release the core platform as open source, possibly as a contribution to other endeavours. Watch this space.

And… we're still hiring (https://jobs.lever.co/r3cev.com): there is a great deal of work still to do!

POSTED BY

GENDAL
POSTED ON

JANUARY 4, 2016
POSTED UNDER

BLOCKCHAIN, CAREERS, DISTRIBUTED LEDGERS, R3, SHARED LEDGERS
COMMENTS

6 COMMENTS

It's New Year… Time to change the world

We're hiring! (http://r3cev.com/careers)

- Are you a talented developer?
  - … who has experience of banking technology *and* a passion for blockchain technology?
- Can you tell your nostro from your vostro?
  - … and do you have an intuitive understanding of why it's quite so hard to change *anything* in a bank?!
- Do you understand why Bitcoin works the way it does?
  - … and can you explain the block size debate in a way that *all sides* would agree was fair?
- Can you explain why $100 at Chase is different to $100 at Wells Fargo?
  - … and can you design a data model that reflects this reality?
- Do you have a passion to transform the world of finance by applying insights from the worlds of cryptography, blockchain technology and distributed systems?

If so, we should speak.

At R3 (http://r3cev.com/careers), we're working on what I think is the most interesting and exciting technology project in finance for years and we're hiring talented, motivated professionals to turn our vision into a reality.

If you think "a blockchain" is the answer to every question then you probably shouldn't apply. But if you think the application of modern cryptography, consensus techniques and modern internet-scale technologies to some of the thorniest problems in financial technology sounds exciting, please email me (mailto:richard@r3cev.com).

Before you do, however, some background. Because I'm convinced many people are thinking about the problems and opportunities completely back to front…

The reality is that banks were amongst the earliest adopters of information technology and, contrary to popular belief, they have done a good job in automating previously manual processes and in digitising previously physical processes.

But there *are,* of course, significant opportunities to improve the cost and efficiency of the architectures that have emerged – and today's developments in blockchain technology and distributed ledgers are showing us how.

At core, this is all about moving from *firm-level* systems to *industry-level* systems.

Today, each bank has its own ledgers, which record that firm's view of its agreements and positions with respect to its customer set and its counterparts – and its counterparts, in turn, maintain their views. This duplication, whilst robust, is expensive and can lead to inconsistencies, and it drives a need for costly matching, reconciliation and fixing of errors by and among the various parties to a transaction. To the extent that differences remain between two firms' views of the same transaction, this is also a source of risk, some of it potentially systemic.

The maturation of cryptographic techniques, exemplified in part by "blockchain technology", provides a new opportunity: the possibility of authoritative systems of record that are securely *shared* between firms. This provides the opportunity to implement new shared platforms for the recording of financial events and processing of business logic: one where a single global logical ledger is authoritative for agreements between firms recorded on it, even though the relationships and obligations recorded remain between those firms.

I believe successful, transformational, large-scale deployments of shared ledger technologies in finance depend on the adoption of an architecture that is designed from the ground up to address the functional and non-functional requirements of banks. And the non-functional requirements are really, *really*, exacting.

It's why I hired James Carlyle, Mike Hearn and Ian Grigg (https://gendal.me/2015/11/19/introducing-the-r3-technical-leadership-team/) to start building out our technical leadership team: I might be CTO but I'm not remotely clever or experienced enough even to *begin* to figure out the answers to these questions.

And it's also why we're hiring talented developers, designers and architects to join our team.

So, if you're experienced, intelligent, curious and motivated by solving difficult problems in distributed systems in finance, I can think of no better places to be working right now.

email me at richard@r3cev.com (mailto:richard@r3cev.com) if you want to talk.

POSTED BY

GENDAL
POSTED ON

NOVEMBER 19, 2015
POSTED UNDER

UNCATEGORIZED
COMMENTS

40 COMMENTS

Introducing the R3 Technical Leadership Team

I joined R3 in September as our Chief Technology Officer. Regular readers may have noticed a drop-off in my blogging at precisely the same time. It turns out that joining a high-profile, fast-growing startup consumes a lot of time..!

In this post, I want to share some early thoughts and to introduce my senior leadership team (http://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/564dd802e4b0dff76870e198/1447942146527/PRESS+RELEASE+R3+tech+maangement+team+%2811-19-15%29.pdf). Regular readers of my blog will know that I have thought deeply and written often about the applications of blockchain and distributed ledger technology in finance. But as I set out on my journey at R3, I tried to imagine myself in a few years, sitting in front of the CIO of one of the world's largest banks, having a conversation about our project. What would we talk about? How would I describe what we had built? How would I explain why we built it one way rather than another?

I figured it would be an *extremely* difficult conversation if my opening line was: "well… you know…. I built the platform like this because blockchains were cool in 2015"… No. That simply won't do. The rules of engineering and architecture don't fly out of the window just because somebody pulls out the "shared ledger" trump card.

If we aspire to reduce cost, free up capital, improve controls and enable innovation in finance and beyond, we need to build our vision on more than hype and hope. So I've gone back to basics: what properties does a technology platform need to possess if it is going to enable the world's banks – and

other firms – to deploy shared platforms to record, manage and report on their contractual agreements with each other and with their customers? What is the irreducible set of functional requirements we must provide? What are the non-negotiable non-functional requirements?

So I've spent my first few weeks building my leadership team, establishing an Architecture Working Group with our members and developing a detailed view on what a shared ledger for financial firms needs to look like if it's going to gain widespread adoption and solve real business problems.

In the coming weeks, I'll share thoughts on these questions. I'm probably wrong about huge portions of it (I usually am…). But my strong desire is to have this debate in the open: just as we're driving this discussion with our members, we also want to debate this with other practitioners, firms and projects. Not least, because it's *manifestly obvious* that a base "fabric" for the recording of financial events and execution of logic has to be open and if I can persuade you of my vision (or you can persuade me of yours…), perhaps we can work together to drive some standardisation too. Watch this space.

In the meantime, I'd like to introduce my senior leadership team.

First, I'm delighted to announce that James Carlyle (https://twitter.com/jwgcarlyle), formerly Chief Engineer at Barclays Personal and Corporate Bank, is joining R3 as our Chief Engineer. He is almost too-good-to-believe: he built hugely complex systems for a hugely complex bank, founded two startups *and* he happens to to be one of the few people I know who can both *talk* about ethereum *and* develop for it.

Secondly, I am beyond excited that Mike Hearn (https://github.com/mikehearn) has joined us as our Lead Platform Engineer. He brings half a decade of experience of blockchain and cryptocurrency development and over seven years of experience helping run some of Google's most heavily-trafficked websites. The combination of deep understanding of blockchain technologies and real-life experience of building rock-solid internet-scale production platforms is truly unmatched in the industry. And his involvement in the recent bitcoin blocksize debate gives me confidence he can hold his own against a group of *very* opinionated bank architects…

Thirdly, I would like to welcome Ian Grigg (http://www.financialcryptography.com/), our Architecture Consultant. Ian has been building cryptographic ledger platforms for *over two decades*. He invented the concept of the "Ricardian Contract (http://iang.org/papers/ricardian_contract.html)", co-invented the concept of triple-entry accounting (http://iang.org/papers/triple_entry.html) and astounds me every day with the experience and perspective he brings to the team. You would be amazed how many of the concepts in the shared ledger space today can be traced back to Ian's work.

Fourthly, Tim Swanson (https://twitter.com/ofnumbers) joins as our Head of Research. I have to believe there are people in this space who Tim *doesn't* know, but I've not met one yet. He teaches me every day that it's OK to be opinionated, provided you can justify the opinions. And Tim can; his most recent report (http://www.ofnumbers.com/2015/11/18/watermarked-tokens-and-pseudonymity-on-public-blockchains/) is a fascinating demonstration. I lean on him heavily for advice and insight and am delighted to have him as a colleague.

They join a fast-growing team, which also includes Jo Lang (http://www.femtechleaders.com/north-america/jo-lang/) and Ayoub Naciri (http://www.fifthmoment.com/author/ayoub-nacirigmail-com/), amongst others.

… and what about you? **We're hiring!**

We are working on the most interesting and exciting project I can imagine in technology today. We'll be sharing details of our open roles and how to contact us shortly. In the interim, if you're interested in working with us, I'd encourage you to think about a few questions that just might come up in interview…

- If you were building a system to enable multiple parties to come to consensus about the state of an agreement between them and maintain that in lockstep for the life of that agreement, what are some of the most important non-functional requirements you would want to explore to validate your design?
- If you were building a shared ledger system between large numbers of regulated financial entities with hugely sophisticated IT infrastructures, what would be your approach to co-existence and integration?
- What would be your answer to the CIO's *follow-up question?* "Tell me… why *did* you build your shared ledger using a blockchain rather than another technology?"

POSTED BY

GENDAL
POSTED ON

AUGUST 26, 2015
POSTED UNDER

ADVICE, ARCHITECTURE, BLOCKCHAIN
COMMENTS

18 COMMENTS

Free advice can be valuable… but only if you take it

If a client tells you your solution doesn't solve their problem, it may not be the problem that needs to change…

I often argue for the importance of blockchain and distributed ledger technology by using the following chain of logic:

- Bitcoin's architecture solved the problem of censorship-resistant digital cash
- But few, if any, financial firms are interested in censorship-resistant digital cash
- So why are they looking at this technology?
- Because some principles underpinning Bitcoin's architecture – shared ledgers, for example – could be relevant to problems that banks face.

Sure, a blockchain or a replicated shared ledger *could* indeed be useful to banks. Perhaps it could reduce the need for reconciliation between firms if they all ran off a single ledger, for example. But this says nothing about whether blockchains are the *optimal* solution to any particular problem in banking. That still has to be argued, of course.

Recall: the bitcoin architecture was a solution to a very specific, very carefully framed problem – how to transmit value without the risk of censorship. Just because the underlying architecture *could* be used to solve some pressing problems in banking doesn't mean it's the best way to do so. Indeed, although the interlocking aspects of the Bitcoin solution are in some ways quite elegant, there are also some compromises. After all, it is an engineering solution to a set of very specific constraints and so it has to be demonstrated that it's the right solution when the constraints are different.

Lee Braine, of Barclays Investment Bank CTO Office, made an important contribution to this debate when he spoke at London Blockchain Conference 2015 recently. The video is now available and I urge anybody working in this space to watch it and to internalise its message.

[vimeo 137190236]
We all too often "talk past each other" in the distributed ledger world and we are quick to assume the other person just "doesn't get it". I can assure you that Lee *does* get it and it would be a brave startup in this space that chooses to disregard what he said. *He's giving us free advice! Take it!*

Like I say, watch the video for yourselves.

I think another way to capture the chain of logic in the video is as follows:

- Assume the ongoing interest in the application of blockchain technology continues
- Assume further that some banks identify some compelling business opportunities in deploying a cryptographically-secure shared ledger between themselves.
- What is the probability that a derivative of Bitcoin or Ethereum or any other current platform will be the best solution to that specific problem?
- Given that none of them were invented to solve that problem, surely it's quite low, right?

So we could find ourselves in the situation that bitcoin and blockchain technology have catalysed an orgy of activity, that this activity has identified countless high-quality business problems and yet none of those opportunities are best addressed with the technology that triggered the excitement in

the first place!

The theme of this blog is “free advice” and the free advice I’m taking from Lee’s comments includes:

First, we shouldn’t get enamoured by a *particular* implementation of a technology. Sure: if you have an implementation then you may have bought a place at the table. But don’t make the mistake of assuming that if the business problem doesn’t fit the technology then it’s the business problem that needs to change!

Secondly, if you’re working in a financial institution, be careful to distinguish between the *principles* embodied in these technologies. Shared ledgers? Yes. That seems to be at the heart of this domain. Indiscriminate replication? Perhaps. Cryptographically-secured access down to the “row” level? Probably. And so on.

Thirdly, consider the complexity of banks’ existing IT environments. An idealised, “wouldn’t the world be perfect if…” solution is no use to anybody if it requires the whole world to move at once and/or if there is no credible migration path. This points to a need to listen to the incumbents when they object. Furthermore, consider the *non-functional requirements* which are simply a given in this space.

Fourthly, if we assume that today’s current hyperactivity will lead to a new understanding of the possibilities for banks but don’t assume that today’s blockchain platforms (permissioned or permissionless) are the (whole) answer, then surely we’re back in the land of engineering, architecture and hard work? Perhaps this means that the combination of persistence, data models, APIs, consensus, identity and other components that we need won’t all come from one firm. So a common language, some common vision and an ability to collaborate may become critical. Where is your distinct differentiation? Where would you fit in an overall stack?

POSTED BY

GENDAL
POSTED ON

AUGUST 17, 2015
POSTED UNDER

BITCOIN, BITCOIN XT, BLOCK SIZE, GOVERNANCE
COMMENTS

33 COMMENTS

Brief thoughts on the Bitcoin block size debate

I've kept well away from the block size debate but the launch of Bitcoin XT (https://medium.com/@octskyward/why-is-bitcoin-forking-d647312d22c1) is worth a quick mention.

My reasons for staying out of the debate are pretty obvious: I'm not a miner, I'm not a core developer, I don't run a wallet service, I have no particular insight into the engineering trade-offs and, perhaps most importantly, I'm ***not mad***. If I wanted to argue with people on the internet, there are far more interesting topics than Bitcoin's block size…

But I've been asked by several people what I think. And, at core, I think it might come down to three issues: 1) fear of two different types of failure, 2) a clash of visions and 3) no process for reconciling the first two issues.

Fear of Two Different Types of Failure

Fear of technical failure

I don't contribute, but I do read the Bitcoin Development (http://lists.linuxfoundation.org/pipermail/bitcoin-dev/) mailing list. I find it immensely helpful in keeping up with much of the day-to-debate debate. What becomes clear when you read it is that there are (at least!) two distinct cultures at work.

First, there is a very strong security engineering (http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c01.pdf) culture. I sometimes think the trick to being a good security engineer is to think like a software tester (and vice versa): "How could I break this?"… "How could an attacker get round this?"… "What could go wrong here?"… "How could I force the provider of this service to waste all their resources" And so on. Your job is to figure out all the ways something could fail, and fix it.

So, when presented with something like an increased block size, you obviously focus on all the things that could go wrong: miners on slow connections could get out-of-sync with those on the other side, the increased cost of running a node could create a centralisation pressure and so on. And when you compare this against the potential benefits, you might not think the change makes sense: there's an increased technical and security risk but you haven't fixed the underlying scalability issue at the heart of the system… you have, in some ways, just kicked the can down the road. So you might say that a driving issue here is "**fear of technical failure"**: the change, which has uncertain benefits, could cause catastrophic harm. Better not do it just yet.

Fear of practical failure

But, on the other side, is a somewhat different culture, one that comes from a world where there are problems everywhere you look and they all need fixing. So you pick the biggest one, fix it and move on. The engineering functions of large companies are often like this. You know your change might cause problems but if you believe "doing nothing" is not an option then it comes down to making the least-worst decision. There are, after all, usually no good solutions, just compromises.

So, if you're faced with a problem like blocks getting full in some foreseeable timeframe, it is natural to ask yourself: what is the risk of doing nothing? If your belief is that consumers mostly have *choices* and will simply abandon a system that can't guarantee transaction confirmation in a reasonable period then you'll likely see failure to increase the block size as something that will lead to a catastrophic exodus of users and your bias will likely be towards making the change. For you, the issue is "**fear of practical failure"**: failing to increase the blocksize, a change which has uncertain risks in any case, will drive away users and make the system a failure in all practical cases.

I exaggerate for effect, of course and I've ignored many aspects of the argument (e.g. the fee market, etc). And I'm sure some of the details are simply wrong. But note: even under this simplistic model, it doesn't mean either side is "wrong" or "bad": it is possible to hold either view quite legitimately and to passionately believe the other side is wrong

A Clash of Visions

Where it gets more complex is when it comes to vision: if there was common agreement on what outcome was desired (e.g. "x transactions per second across the blockchain by 2017" or "the system should support this number of consumer wallets") then the discussion would be a pure engineering discussion: "what is the best way to achieve this goal?" But it strikes me that there isn't agreement on this underlying vision.

And so, the engineering discussions get lost in the sound of people talking past each other or, worse, resorting to ad hominem arguments. If you're arguing from different premises, you never get anywhere, sadly. It's what makes political discussions on the internet so tedious..!

Process

In most projects, these issues can be resolved, ultimately, through the "benevolent dictator" model. Linus just decides (https://en.wikipedia.org/wiki/Benevolent_dictator_for_life). Unfortunately, that process just doesn't work in a system like Bitcoin. It's not enough to control which code goes into the "core" distribution: the prevailing network rules are a complex function of miner adoption, full node adoption, wallet adoption, major merchant/processor adoption, and more. It's an inherently messy and political process. So the block size debate is likely to just be the first of many such controversies in this world. The launch of Bitcoin XT is an interesting way to force the debate towards a conclusion but it's likely to be messy.

And I hope those looking at "private blockchains" aren't feeling smug as they read this. Managing the maintenance and upgrades of shared ledger systems between firms won't be a walk in the park, either.

I have no particular insight into where this will go or which vision of the future will prevail. But I hope (perhaps forlornly) that it will be resolved through the actions of professionals acting in good faith and that neither side will resort to “dirty tricks”.

POSTED BY

GENDAL
POSTED ON

JULY 23, 2015
POSTED UNDER

BITCOIN, BLOCKCHAIN, LEDGERS, MODELS
COMMENTS

30 COMMENTS

Bitcoin and Blockchain: two revolutions for the price of one?

I gave a brief talk on Bitcoin and blockchain technology to an audience of non-specialists at a dinner last week. It covers many of the themes I've explored on this blog before. But the short, fifteen-minute, format forced me to be brief and clear. This is an edited version of the speech

A £20 note has an obvious, yet extraordinary super-power. I can hand it to anybody in this room and £20 of value will be transferred instantly, directly, peer-to-peer, person-to-person. Settlement, with finality, in central bank money! And nobody else need know. And nobody can stop me.

(https://gendal.files.wordpress.com/2015/07/super20.png)

Super £20!! [I really hope there's no law against posting photos of money…]

But this super-power only works at close distance. If I want to transfer £20 of value to somebody in a different town or in a different country, I need to trust other people. Sure: I could put the £20 in an envelope and post it. But even then I'd have to trust the postal service.

Or I could use a bank. But I'd be trusting them to be good for the money. And I'd have handed over control: if my name's on the wrong list, the bank would be obligated to seize my funds. And if *you're* on the wrong list, the bank will refuse to transfer the money to you…

"Digital" money is not the same as physical cash.

And the world's financial plumbing – payments systems, correspondent banking, SWIFT, … – is a direct consequence of this observation: physical cash really is fundamentally different to every other form of money: only *physical* cash is a bearer instrument. And only *physical* cash can be transferred without permission – *censorship-resistant*.

Or so we thought.

Because a curious email to an obscure cryptography mailing list (https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html) at the end of 2008 said something quite audacious. The email, from the hitherto unknown Satoshi Nakamoto heralded the arrival of Bitcoin and the advent of "purely peer-to-peer electronic cash".

Bitcoin P2P e-cash paper

Mail-Archive, Inc. (US) https://www.mail-archive.com/cryptography@metzdowd.com/msg09959.html

Bitcoin P2P e-cash paper

Satoshi Nakamoto | Sat, 01 Nov 2008 16:16:33 -0700

I've been working on a new electronic cash system that's fully
peer-to-peer, with no trusted third party.

The paper is available at:
http://www.bitcoin.org/bitcoin.pdf

The main properties:
 Double-spending is prevented with a peer-to-peer network.
 No mint or other trusted parties.
 Participants can be anonymous.
 New coins are made from Hashcash style proof-of-work.
 The proof-of-work for new coin generation also powers the
    network to prevent double-spending.

Bitcoin: A Peer-to-Peer Electronic Cash System

Abstract. A purely peer-to-peer version of electronic cash would
allow online payments to be sent directly from one party to another
without the burdens of going through a financial institution.
Digital signatures provide part of the solution, but the main
benefits are lost if a trusted party is still required to prevent
double-spending. We propose a solution to the double-spending
problem using a peer-to-peer network. The network timestamps
transactions by hashing them into an ongoing chain of hash-based
proof-of-work, forming a record that cannot be changed without
redoing the proof-of-work. The longest chain not only serves as
proof of the sequence of events witnessed, but proof that it came

(https://gendal.files.wordpress.com/2015/07/super202.png)

"A purely peer-to-peer version of electronic cash"

We all know the story of what happened next.

Except… what many people have missed is that the choice of the word "cash" in that email was absolutely critical and absolutely deliberate. What this email announced was the arrival of a ***digital*** bearer asset that is censorship resistant. Digital cash. A digital asset that you can hold outright, with no risk of confiscation, and which you can transfer to anybody you choose with no permission from anybody else.

And the funny thing is: the architecture of Bitcoin flows almost trivially (*almost…!*) from this requirement. Proof-of-work, the peer-to-peer gossip network, mining, the mining reward, the *blockchain*. The lot. It's as if the genius of bitcoin was to *ask the question*.

But why am I saying this in the summer of 2015? This exact same thing could have been said at any point from 2009 until now. There's nothing new here.

Except…

Nobody asks the obvious question:

Who actually wants a censorship resistant digital bearer asset?!

Well… some people do, of course. But none of them are banks or corporates. At least, *I've* not yet met a bank that wants this.

So *why are so many banks, corporates, VCs and startups spending so much money in this space?!*

I think there are two completely distinct reasons and that that the world of "blockchain technology" is actually two completely different worlds, with different opportunities and different likely winners. And those who don't realise this might be about to lose a great deal of money.

First, let's look at Bitcoin.

We should probably be realistic here. Bitcoin is not the solution to Greece's crisis and it won't bring finance to the world's poor. But it turns out that censorship resistance *is* extremely valuable, even for people who don't think they need it.

Because censorship resistance implies *openness*.

Anybody or *anything* can connect to an open network like Bitcoin to own and transfer value. And anything that is open, standardised, owned by nobody and useful smells very much like a platform. And we've seen how those stories play out.

But notice something else: Bitcoin is *worse* than existing solutions for all the use-cases that banks care about. It's expensive. It's slow. And it's "regulatorily difficult". And this is *by design*.

So this makes it doubly interesting.

Because it means Bitcoin is probably worse than existing solutions for all the things *most* people and firms care about but *vastly* better for one single use-case (open access to value transfer) that could be very useful for *some* people.

Isn't that pretty much the definition of a disruptive innovation? Something that's worse for existing use-cases but solves a niche use-case very well?

So, if this is true, we should expect to see adoption of Bitcoin come from the margins, solving marginal problems for marginal users.

But disruptive innovations have a habit of learning fast and growing. They don't stop at the margins and they work their way in and up.

So this is why I think so many of the big-name VCs are so excited about it.

So the incumbents should be keeping a very close eye on what's going on. If anything in this space is going to disrupt them, it will probably come from this world. But it's perfectly understandable that vanishingly few of them are actually *engaging* deeply in this world.

So if Bitcoin isn't why banks are looking at this space, what *are* they looking at?

> How have so many people convinced themselves that there is something of interest here that is "separate" to Bitcoin or systems like it?

At this point, it's customary to observe sagely that "of course, the real genius of bitcoin was the blockchain; that's where the value is".

But I've discovered something rather amusing. If you push the people who say this, and ask them what they *actually* mean, most of them can't! And yet… whether they understand why or not, they are actually on to something.

It comes down to how bitcoin delivers on the design goal of "censorship resistant" cash.

Imagine Bitcoin didn't already exist and you were asked to design a system of censorship-resistant digital cash. How would you do i?

Well… you couldn't build it around a central database: the government could shut it down. That doesn't sound very censorship resistant.

And you couldn't rely on a network of trusted people around the globe since law enforcement could simply collaborate to shut them down too. And in any case, who would control the identity system that helped you be sure these people were who you thought they were in any case?

It turns out that the answer is quite unexpected… and it's something I'd bet almost *all* engineers would consider *completely mad.*

The answer is that you get everybody who fully participates in the system to maintain a full copy of the ledger. And every time somebody, anywhere in the world, spends some bitcoin, we're going to inform everybody who's maintaining this ledger and they're going to store a copy of that transaction too.

Bitcoin essentially runs on a MASSIVELY replicated, shared ledger. (The trick is in keeping it consistent, of course…)

It sounds insanely inefficient and expensive… and perhaps it is. But we also have to ask ourselves: inefficient and expensive as compared to *what*?

And this leads us to the *other* world

Just look at the state of banking IT today… Payments, Securities, Derivatives… Pick any one. They all follow the same pattern: every bank has built or bought at least one, usually several, systems to track positions and manage the lifecycle of trades: core banking systems, securities settlement systems, multiple derivatives systems and so on.

Each of these systems cost money to build and each of them costs even more to maintain.

And each bank uses these systems to build and maintain its view of the world. And they have to be connected to each other and kept in sync, usually through reconciliation.

Take even the simplest OTC derivative contract: it is recorded by both sides of the deal and those two systems have to agree on everything for years. Very costly to operate.

But what if… what if these firms – that don't quite trust each other –used a *shared* system to record and manage their positions? Now we'd only need *one* system for an entire industry… not one per firm. It would be more expensive and complicated to run than any given bank-specific systems but the *industry-level* cost and complexity would be at least an order of magnitude less. One might argue that this is why industry utilities have been so successful.

But a centralised utility also brings issues: who owns it? Who controls it How do the users ensure it stays responsive to their needs and remains cost-effective?

The tantalising prospect of the blockchain revolution is that perhaps it offers a third way: a system with the benefits of a centralised, shared infrastructure but without the centralised point of control: if the data and business logic is shared and replicated, no one firm can assert control, or so the argument goes.

Now, there are lots of unsolved problems: privacy, performance, scalability, does the technology actually work, might we be walking away from a redundant (antifragile (https://en.wikipedia.org/wiki/Antifragile)?) existing model? Who will build these platforms if they can't easily charge a fee because of their mutualised nature? Difficult questions.

But see: this has nothing to do with funny internet money, bitcoin or censorship-resistant digital cash. It's a completely different world

Two revolutions for the price of one

So… the blockchain revolution is so fascinating because it could actually be TWO completely different revolutions… both profound in their implications:

- Censorship-resistant digital cash providing a new platform for open, permissionless innovation driven from the margins
- And industry-level systems of record driving efficiencies for incumbents.

Neither of these are "sure things"… they are both high risk speculative bets… but they're also very DIFFERENT bets…

[EDIT 2015-07-23 Gideon Greenspan has written a great piece that comes at this argument from a very different angle (https://www.linkedin.com/pulse/ending-bitcoin-vs-blockchain-debate-gideon-greenspan?trk=prof-post)]

As ever, the thoughts and comment on this blog are mine alone and don't represent the view of my employer….