Open Governance

$Revision: 1.11 $
$Date: 2005/11/05 18:25:55 $

Abstract: Open Governance is a form of security whereby a business engages partners and the user public in protecting assets under management. Open governance arose in the unregulated environment of Internet Payment Systems.

Yet the techniques developed are universally applicable, and in some cases have decided advantages, even when applied to the regulated or non-payment sectors. Use of these techniques and the overall philosophy, in concert with conventional techniques, can reduce dramatically internal risks and costs.

Introduction

Preamble

Open Governance is the protection policy whereby a business engages partners and the user public in protecting assets under management [OG]. It does this by using a set of classical techniques, updated and applied to the Internet world. Payment systems especially can use these techniques, in concert with their other more conventional techniques, to reduce internal risks and other costs.

Open governance arose in an unregulated environment. Yet the techniques developed are universally applicable, and in some cases have decided advantages, even when applied to the regulated world. This presentation hopes to make that case.

Structure

Firstly, a survey of key factors impressing upon the world of payments systems is undertaken. Then, open governance is described, as it has evolved in the payments world. Finally, the two are brought together, and a list of useful and universally applicable techniques is presented.

The Environment of the Payment System

Key Forces

There are several key forces pushing at payment systems:

- Scandal in the audit field - are audits all they are cracked up to be?
- Communications is now free.
- The end of secrets - discovery and the email backup.
- Regulatory uncertainty over two key questions:

    1. should banks be the only payment systems? In US-centric circles, no. In Frankfurt-centric circles, yes.

2. how much regulation should be imposed? In single purpose, reserve based systems, not much. in complex balance sheet scenarios, a lot is required.

- Arisal of challengers to the payment systems field: telcos, couriers, mass transits, startups.

The Scandal of the Audit

The Auditor's Independence

If the professional auditor is selected by the management of the company, there is a clear conflict of interest. In the presence of fraud, by those same managers, there is an incentive to employ an auditor who is easy to manipulate. As there are large fees involved, it is easy to increase fee income and divert an auditor's attention. A sophisticated manager may even be able to do it without the auditor noticing.

Further, auditors generally employ consultancy divisions, and spend a lot of their energy in selling the consultancy into their customers business. The efficiency motive for this is easy to understand. If an auditor must understand large swathes of business in order to prepare accounts and watch for trouble, they can also easily identify areas that need fixing. Why pay twice for that knowledge? Bring in the auditor as a consultant at the same time and reduce the fee to a quantity discount.

Yet these two forces mean that whilst a given auditor may act honourably and professionally, the temptation exists to not be too harsh on the potential for fraud. Or, to concentrate on surfacing problems for which an auditor already has a paid solution.

This is no unique or isolated issue. Mark Everson, commissioner for the US Internal Revenue Service, recently commented [IRS]:

> There's no doubt that one of the things that has contributed to our recent problems is a change in the way the financial professions have approached their responsibilities. I started out my career in the mid-1970s with Arthur Andersen, which at the time had an impeccable reputation. I was on the audit side, not the tax side, but we all knew that the No. 1 obligation was to help your client follow the law. It was important not just because of the penalties associated with misconduct, but because the reputation of the firm and client was the top priority. The financial community's more recent emphasis on value creation and risk management unfortunately gave rise to a number of attorneys and accountants who wanted their fees based on value creation. And they obviously felt there wasn't significant risk of a transaction being questioned or of illegal conduct being uncovered. That constituted a total deterioration of the old model, which I think we have to try to return to, and why one of our top enforcement priorities is to assure that attorneys and accountants adhere to professional standards and follow the law.

Much attention has been focused on the independence of the auditor and many solutions have been proposed. In 199x, Arthur Anderson split off from its consulting divisions, which renamed themselves Anderson Consulting. In this way independence was regained, but the pressure had been financial - the consulting division partners were bringing in the lion's share of fees, and they wanted to keep more of it.

Collapses in the face of Audits

Enron, Arthur Anderson, Worldcom, Ernst & Young ...

In response to the scandals in the field of the professional audit, there has occurred:

- massive restatement of earnings in the US.
- ever increasing regulatory burdens - Basel II, Sorbanes-Oxley.
- finally, a willingness to seriously address the conflicts of interest in the process.

Lack of faith is at an all time low.

The independence of auditors has been on the discussion agenda for a decade or more. The size of the consulting revenues dwarfs the audit revenues, so why do we believe that they cannot have an effect?

Consider the Audit. A summary of its principles is in order. Firstly, an independent professional auditor is employed because it can do the checks that others want, but more efficiently. The auditor can visit places, observe events, create records, and prepare a summary to broadcast. Secondly, the auditor can be given access to secret information. Thirdly, by design and presumption an auditor is an independent party.

The Cost of Talking to the Customer

As is almost too passe to mention, the marginal cost of a message has shrunk to zero. That is, it may cost to send to the first customer, and it may cost to send the first message to any customer, but every one thereafter is essentially free of externally imposed costs.

Consider the Internet's effect on the talking to the customer. If communication is free, the customers can now receive as much information, when they want it, how they want it, and the marginal cost of that information is zero. The inevitable result of this is per-transaction distribution of information. That means, an email every time someone access their account.

The End of Secrets

Discovery

Several high-profile cases (Microsoft, Arthur Anderson) have underscored the importance of documents in discovery. Vast amounts of documents are pored over by examiners. Evidence is searched for in the documents of the victim, cases launched, costs incurred.

In any sophisticated place of business, it is no longer customary to just send an email describing secret activity. Any employee now routinely expects that all emails are subject to scrutiny, and conduct follows that risk.

A less noticed effect is the change in environment. What happens to secret activity? Is it now conducted verbally? Do other means of communication get used?

Obviously, secrets still exist, but activity with some fear of wider scrutiny shifts to other media. Telephone and face-to-face meetings remain popular, perhaps defying the predictions of net watchers that all will go digital, and ad hoc communication methods such as chat (instant messaging) and

employee-owned mobile/cell phones cause difficulties in the securities sector where all communications generally have to be recorded.

Yet the limits on organisation remain; secrets can only be small if they can not be recorded.

The Cash-flow Basis

Any company that borrows from external stakeholders, be they lenders or shareholders, will have faced the the real time cash-flow dilemma. Banks, especially, analyse a company from the point of view of the internal cash flow and the internal books. Shareholders want the same, but rarely are given that privilege.

Yet public companies are moving inexorably in that direction. Either regulation, or best practice, or better availability of capital is driving them in the direction of more and better information available, direct, online to a large group of outsiders.

Likewise, user-base numbers are becoming the key to analysing a company. Yet, companies have responded by inflating and forging numbers. As time goes on, the need to present verifiable, auditable reports on activity increases.

need some examples here...

Whistleblowing

The increase in high profile whistle blowing cases, and the whistle blowers protection acts, means that internal secrets could leak if those secrets are against the interests of the public.

The Public Sector experience

http://www.theregister.co.uk/2006/05/05/secret_folly/

> *But private provision does not do away with the need for scrutiny. According to this paper, it begs for more. Official Australian reports prior to the 2003 decision found that a vast majority of public contracts were obscured by commercial-in-confidence, most often at the behest of the government, and not, as is usually claimed, the private partner. Yet few contracts could justify the secrecy, so it was recommended that transparency be the rule and commercial-in-confidence should be justified whenever it was called upon. Secrecy had become a political reflex because, "[It] suited the personal interests of ministers and senior bureaucrats in avoiding the onerous task of being accountable for their activities."*

Living and financing in an open world

As more and more forms of communication are made more and more subject to scrutiny, business is forced to shift in a more open direction. Now, it is routine to think in terms of "doing the right thing" because the risk of future liability is lower.

The end result of this is that business can and is shifting to a point where substantial amounts of its activity can be dynamically reported. There are no more forever secrets across the corporation, and even short term secrets are informed for eventual scrutiny.

The Forces, Summed, Equals ... the Fall of the Audit?

All of the above come to bear at the point of the audit.

If the customer can receive information, for zero marginal cost, then they can also *conduct auditing checks for free*. Observation of remote places can be achieved by direct accessibility of assets over the Internet. Events can be encoded and distributed as signed records, automatically and immediately. Summary reports can be made to all immediately, as easily as to one, or individuals can conduct their own report generation by working from the raw data.

Why can't the same transaction records that generate fee income be sent immediately to a user, the same way a user is notified of a package delivery or an airline change? And, why have a summary prepared when the user can see all the raw info himself, and potentially pay out of his own pocket for some external analysis?

Certainly for a payment system, vast amounts of the auditor's role can be conducted by the user, as efficiently as any one else. This removes one of the pillars of fundamental support for the audit - it is no longer inefficient for users to conduct their own checks.

What about the other fundamentals?

Auditors may be independent on paper, but they don't seem to be acting that way in practice. And, any theory of fee taking value added would explain this - what auditor would risk aprobum, ruin, disgrace to protect his fee income? Is an auditor independent in fact, or is it dependent on fees?

An auditor may be independent, but is not free of conflicts of interest. The fees for both audit services and value added services represent a vast and unassailable conflict of interest. In contrast, every customer has interests more closely aligned to their auditing role - they care for their goods, as they own them. Thus, the auditor may retain independence, but this is trumped by the owners' interests.

This leaves the first fundamental, that of access to secret information. The auditor may still have an advantage is that he may be cleared to read, analyse and audit information of sensitivity, which could not be disclosed to general customers.

Yet, much information is secret for uncertain reasons. And, as time goes on, more and more information is designated as "must be safe for liability purposes". The difference between that and publishing it totally is not that far. In fact, publication immediately of much information for auditing purposes may be the only way to be sure that it is safe, for liability purposes.

The existance of all these forces may not only explain the robustness of payments systems under open governance, but also may predict their dominance in the future. The critical underpinnings of a regulated system are that the regulator be needed to supervise, and the auditor be needed to check the detail. If the latter has lost the foundations, what about the former?

The Regulatory Question

Regulators have long paid lip service to competition. But, they have also had their blind spots, those industries that have been spare the full force of the breakup mania. There are many reasons oft listed as to why these particular industries should be spared:

- strategic or defence importance,
- national treasure,
- natural monopoly,
- consumer protection...

Yet these reasons are slowly being eroded. All the national treasures are up for grabs.

One of the last to go is payment systems. Once thought critical for systemic risk and monetary policy reasons, it is no longer radical to ask whether a telco or a mass transit should run a payment system. Indeed, it is now routine amongst Central Banks around the world to question whether the 20th century dogma of the monopoly of currency issuance had been overdone.

Having raised the doubt, there remains the detail. Changing a policy that dominated public thinking for the entirety of the last century is no small change. Yet some steps have been made. The European Directive on eMoney envisages compromises between an issuer of eMoney and a bank. Small, single purposes systems can be effectively left to ad hoc national supervision, and larger ones can secure a half-way-house: the eMoney licence.

The US has gone further. The lead agency in matters of currency issuance, the Federal Reserve, has staunchly declined to pressure regulation on gold issuers and derivative dollar issuers. Other agencies, following the lead of the all-powerful Fed, have concentrated on molding the new breed of issuers into one or other model, rather than assuming that they have to be closed down. Evolution of regulation proceeds...

"If regulation?" has been answered - maybe. "How much regulation?" is being addressed in experiments across the world. One criticism of the European Commission's early, heavy handed approach was that it stymied the arisal of new solutions indigenously. [G2]. The Journal of Internet Banking and Commerce, Vol 2, Num 2 March 1997. Was the Paypal Invasion of Europe inevitable? I argued then that the eMoney directive made it so.

Techniques

The Challenge of Open Payment Systems

Several open payment systems have arisen to challenge conventional markets. They have not yet made their mark in volume terms, although the market size of Paypal is impressive. What has been of interest is how they have faced the challenge of governance, which is the subject of the next section.

In the halcyon days of the Internet, the latter half of the 1990s, countless Internet money issuers arose and fell. Almost all succumbed to the complexity of the financial cryptography, as Internet people generally with little business and financial experience stumbled onto the possibility of issuing their own value, and failed to realise their own limitations [FC7.2].

To some extent lucky or statistical, two models arose. One model, which might be called the Paypal model, filled a hole in the market - that of facilitating credit card purchasers for small merchants. As a meta-credit card merchant or banking facilitator, their structure should be similar to those they imitate, and are not covered further here.

The second model might be called the *Internet Gold* model ("IG"). This model is more of a true innovation, and its arisal has also sparked issuances in other instruments such as national currency.

The model in brief is as follows. An issuer promises by contract to escrow gold in behalf of owners. In order to give access to the benefit of the owner's gold, an accounting system is made available on the net. If an owner sends in a one kilogram bar, then 1000 grams are credited to her account.

As the account also has the facility to do user-to-user transfers, the system serves as a payment system. In time, merchants arise, selling product for grams of gold. Further, independent third party *exchangers* or *cambios* arise to facilitate movement of value between the gold unit and convenient national units such as dollars or euros.

The model is simple, and well understood. It is solid, and is the basis for approximately 20 issuers around the world. However, the question of safety arises, and the governance equation can be posed as "how do I, as user, know that the gold exists to back my account balance?"

The Characteristics of an IG

Internet Gold issuances have many important characteristics, some of which are mentioned above. Follows is a brief survey of the salient characteristics.

1. Internet startups have very small initial capital. Most IGs start out with less than a million dollars of capital, some with less than $100,000. Out of this capital has to come purchase of software, salaries (tech, marketing, managerial), costs (Internet servers, warehousing fees) and some small bootstrapping amount of issuance.

2. Small initial amounts of gold issuance. Total issued gold can start as low as $10,000 worth. Generally, this amount comes out of capital, and is sold off to early users.

3. 100% reserves position of physical metal. Most IGs take in an exact amount of metal, and deliver that exact amount of digital units, less fees. This results in a balance sheet where metal exceeds or equals the amount of total issed digital.

4. Requirement to enter the business of primary sales. The Issuer should be passive, and simply bail in or redeem the physical metal. Yet, for a variety of reasons, the Issuer must generally take the initiative in initial sales of digital gold by bailing in a small amount of capital and acting as the first cambio.

What has to be Protected?

To protect the issuance of gold, we are fundamentally concerned with two things:

- the protection of the physical metal (that is, the underlying), and
- the protection of the digital issue, (that is, the derivative).

Further, both of these have to be matched to each other according to the contract. Generally, this means that they have equal amounts under management, but this is not a certainty.

It is useful to list out the key risks that might occur to bedevill the IG. There is the risk of theft of the gold, by simple theft, by substitution, or by hiding a loss between the cracks of a complex system. Likewise, there is the risk of theft of the digital value, either from an account, or by inflation of the digital amounts by system corruption of some form (we can ignore the "inflation" of gold reserves as

alchemy remains elusive). Finally, we must recognise several classes of thief: the plain or common crook working from outside, the insider, and the legal challenger armed with a court order.

The Development of Open Governance

Open governance arose as a blanket term for a host of techniques developed to ensure safety of customer funds in an unregulated environment. Issuers of digital assets in the mid 90s faced the dilemma of regulators declining to advise on their activities, and observers asking the obvious question of how the money was safe.

As no advice was available, nor easily accessible in an understandable format (from the perspective of the builders of early financial cryptography applications) methods of governance were invented from scratch. From first principles, as it were. It may be that this might have led to a hotchpotch of temporary arrangements, but the results have stood the test of time. Not only do they go a long way towards protecting assets, they stack up well against the alternate, regulated methods.

Introduction to Open Governance

1. Separation of powers using 5PM - Issuer, Co-signatory, Repository, Manager and Public:
    - Splitting custodial control out into Repository,
    - Co-signatory as a separate governance partner,
    - Publication of instructions to governance partners,
    - Using the public to audit the chain of events in real time.

    5PM consists of 4 parts standard *separation of roles* and 1 part coopting the public as an unpaid, real time auditor.

2. Drawing the public in as auditor can benefit from:
    - Balance sheet:
        - Total value of digital float,
        - minus, Amounts held in the treasury and other internal accounts,
        - Equals, Total summed amount of external customer accounts.
    - Instructions to enact issuance activities.
    - Transactions of key events such as float creation, pursuant to issuance actions.

3. Isolating the digital assets under the same strong governance: Issuer, Mint, Operator, Manager and Public.

4. Creation of strong contracts that can be immobilised and thence spread their pervasiveness such that even the end user comprehensively has the documentation.

5. Entanglement with crypto - creating a chain of auditable records, wherein each record is unchangeable, and cannot be hidden without the gaps being obvious.

6. Arbitration as Support and as Governance.

The Five Parties Model

In 1995 I drew from a wide variety of classical sources such as accounting to construct a model to protect the escrowed or accounted value in an unregulated issuance. This model was subsequently adopted as a *defacto* standard by which governance was measured in the IG world.

Any issuance of digital value may be easily thought of as an Issuer as the business owner seeking to attract the custom of Users. The Five Parties Model ("5PM") seeks to augment these two actors for governance purposes and is based on the following elements. Firstly, there is a Separation of powers by the creation of five distinct roles: *Issuer*, *Co-signatory*, *Repository*, *Manager* and finally the *User*.

Physical	Issuer	Repository	Co-signatory	Manager	User
Digital		Operator	Mint		

Fig 1. The Five Roles and Their Alternative Terms

Value in its haptic (gold) form is escrowed with the Repository as one Role, and when this is digital value, the Role is termed *Operator*, being a hoster of a system of digital accounts. The Co-signatory splits custodial control out from the Repository, such that no value can move without that special oversight. When in the digital domain, we term this role the *Mint* which has the special duties of creating new digital value where before there was none, and in this way the Operator is relieved of any need whatsoever to conduct transactions in the system he is operating.

To insulate the Issuer from any actual transactions, a Manager role is created from which new and old value is disbursed. This is generally an employee of the Issuer, but internally, tight separation is indicated so that Issuer duties are cleanly separated from day to day transactions.

The User as Auditor

Those four roles are very standard uses of separation of powers and accountants will recognise them immediately. It is the fifth role that is innovative, the User. In order to provide a further check on the four powerful roles, the User is encouraged and exhorted to observe and prove every transaction of governance importance. In order to do this, the business must make its governance actions publically viewable, and the Roles should likewise publish their actions and results. In practice this means a combination of:

- The Issuer publishes instructions to governance partners, for example PGP-signed emails.

- The Repository publishes a real-time statement of the assets under management. For a gold repository, this would be a list of bar numbers and bar weights, and include a convenient but checkable total.

- The Operator of digital accounts publishes a complete balance sheet of the issuance, including the open presentation of special accounts (typically the Mint account which might be shown as negative, and the Manager’s account which equates to "treasury" or own capital).

The User could then run through a checklist to audit a typical bar increase: The arrival of a bar would cause the Repository's statement to change. Downloading and checking the totals, this total could then be checked against the balance sheet offered by the Operator. Another level of checks is to examine the instructions. Firstly, the Issuer might instruct the Repository to accept a new bar. When so confirmed by the Repository to the Co-signatory, the Issuer can also instruct the Mint to issue new float. This float would transfer to the Manager for eventual disbursement to the owner of the gold that was accepted by the Repository.

The precise flow of such messages would vary, but what should be clear is that there is little to be gained by keeping them private, and much to be gained by making them public. If each and every message is open and digitally signed, then the entire balance sheet and assets registry can be constructed on the fly by any User.

This mechanism is very powerful! It forms one corner of a foundation of strong governace, and it does so without involving regulations or auditors. Even better, it aligns the interests of the User in good governance with her own actions and capabilities, and does so at only minimal costs of the Roles to the Issuer.

The Problem of Exchange

By looking at the 5PM above, it can be seen that the day to day costs are in the Manager's domain. If the Manager is also buying and selling for other financial assets then he is also attracting risk to the business. For example, in the IG world, the manager may buy and sell digital gold for national units such as dollars or euros.

Although not necessary from a theoretical point of view, this inevitably introduces risk into the system. Once mismatched instruments are traded, the temptation to cut corners and deliver credit appears, and in practice, governance becomes weak because it is never clear that credit isn't being created.

This grave issue was initially addressed by encouraging the Issuer to create a separate organisation with separate staff and assets to do sales. The intention was to create a risk-free Issuer operation alongside a risky exchange operation.

In the closing months of the year 1999, the IG community experienced a dramatic market shift. It started with a single trader offering to make a market between digital gold from one Issuer and national currencies, arbitraging the flooded support team of major Issuer. At first this was received with coolness by the Issuer, but he also had his own problems and decided to hand over all small cheque payments to a former employee.

This move was instantly successful, and signalled that the Issuer would accept third party exchange operations without using his "market power" to squash these operations. By the time 12 months had passed, 30 or so independent operations had opened up around the world, and the model of independent exchange was firmly established. (This model has far-reaching effects on the costs structures of payment systems as the independence also means that the costs of exchange can be properly accounted for in the market.)

The governance aspects are important. By outsourcing the function of exchange - the risky component - this leaves the Issuer clear to concentrate on the risk-free business of of running the systems, issuing instructions to mint and bail in new value, and other support operations. In essence, the business of Issuance is now reduced to a series of checklists and digital operations. This makes it risk free in the financial sense, and extremely cheap to run - both stunning governance benefits.

The Verdict is In!

We now have a useful body of experience to match the theoretical basis of the 5PM techniques. These lessons can be summarised such:

- 5PM is a model, and not a prescription. Understanding it is essential to implementing it, but more importantly, it is necessary to vary the perfect design to match the business.

- One of the most important variations is that impressed by completness *versus* cost. When a business of issuance starts out, it does not have the cash to invest in an entire 5PM, and nor does the value carry the risk worth the effort. So businesses are advised to start with only light attention to the roles, and ramp them up as time goes on. Typically the Co-signatory or Mint roles are added later on, and reporting to the User is minimal at first.

- Each single asset might need a 5PM to protect it. This means that in the gold world, there are two distinct implementations, one to protect the gold, and one to protect the digital accounting balances.

- Overall, the result has proven more cost-effective than third party professional audits. Where companies have conducted audits and also implemented 5PM, the respect of the net community seems more oriented towards the 5PM, whereas the respect of traditional observers has oriented towards the professional audits. But it is hard to escape the cost-effectiveness of 5PM as against the lack of clarity of audits, and it seems that over time, professional audits are being relegated to a compliance role only.

- Once criticism of the 5PM and especially the User's role was that Users are not competent to the task. This has been disproved, and while only a few users in any area have taken on the role of the 5PM auditor, they have been exceptionally well educated and eagle-eyed, often more so than any Issuer, and often participating in other Issuances.

- Systems that have employed elements of 5PM have survived. Systems that did not employ 5PM have crashed. This is not a necessary rule but an observed result with some limitations:

    - One Issuer claimed elements of 5PM but the eagle-eyed pointed out that the claims were no more than words. That system collapsed, as many predicted.
    - Another Issuer claimed elements of 5PM but refused to reveal details. That system has struggled to maintain credibility, due to its quixotic claims.
    - One Issuer has put in place only a few elements of 5PM and has struggled to survive due to a variety of factors.
    - And, one Issuer has famously decided that 5PM is too expensive and has deferred it indefinately. That Issuer is doing well but is small.
    - One Issuer implemented the full 5PM before opening the doors, but has struggled to gain growth and remains a minor player.

  Perhaps, in the best endorsement of all, some exchange-traded funds in escrowed gold have adopted some of the elements in addition to their regulated regime.

- Few Issuers chose to let the Exchange business go to a totally independent party or a market process. This was essentially because the primary or 'monopoly' were a main source of income for the business, and few Issuers had the capital to reach profitability without this revenue.

Early days yet!

Triple Entry Accounting

Entanglement with crypto - creating a chain of auditable records, wherein each record is unchangeable, and cannot be hidden without the gaps being obvious.

There is a hole in the 5PM that canny accountants will spot immediately. No matter how complete the model, the Repository or Operator can still perform an inside theft. In the case of Repositories, protection mechanisms for gold vaults and banks are well described elsewhere. We now turn briefly to how we can protect the digital balances managed by the Operator.

The basic building block that allows us to proceed is the art and tools of cryptography, and in particular the conceptual notion of the digital signature. With this facility, we can chain the following actions together.

The User in her use of the system creates a request for a transaction. Using cryptography she can sign this request. Primarily this can be used to properly authenticate her instructions, but there is a very important additional benefit as described here.

On receipt of the signed instruction, the Operator's software can routinely check the signature and thus authenticate the instruction. It then creates the transaction so ordered. The Operator may then create a Receipt which can be sent back to the two parties to the transaction.

The Operator can create the Receipt by including the original Request from the User. This then makes the Receipt a *dominating* record, and both parties can then dispose of the earlier weaker record of the original request. Further, the Operator can then also sign the Receipt, which binds that transaction tightly to the Request.

In this way the Receipt becomes the most powerful evidence of the transaction, and indeed in our designs, the *Receipt becomes the transaction*. For our present purposes, this Receipt also is unforgeable by the Operator, and thus puts a practical and auditable limit on the Operator creating or manipulating the transactions. He may create bogus transactions but they are easily shown as bogus because he does not have access to the User's key, and thus cannot forge her Request.

Classically, double entry accounting is used to control the Operator from forging or losing entries. It can be seen that a digitally signed Receipt that has all the information included is a stronger single entry than the double entry form of classical accounting. Yet for various reasons, double entry still adds value, and when combined with the single entry of the digitally signed Receipt, the result is a powerful advance on the classical model of accounting. I introduce this as *triple entry accounting* in a draft paper [TEC].

The Contract or User Agreement

One innovation that has not as yet emerged into widespread practice is the digitally signed contract. One form, indeed the only form is that of the Ricardian Contract, which shows how to create a single defining contract that can participate in a transaction [TEC].

This invention was created to fill the gap between loose corporate adherence to contracts, including frog boiling, and the lack of jurisdictional and regulatory context found in early payment systems work. As it has always been uncertain whether any particular Issuance is sanctioned by any particular state, it has also been harder than normal to identify a body of law to apply to disputes.

Issuers in the IG world have responded to this lack by taking the User Agreement seriously as a contract between themselves and the Users. In general, the more credible Issuers have carefully crafted their agreements, stuck to the spirit of the clauses, and only relatively occasionally changed them. Thus the agreements have been effectively immobilised. This attention to stability and willingness to stick to the written agreement has been foundational in moving to the next stage, alternative dispute resolution.

Alternative Dispute Resolution

Alternative Dispute Resolution ("ADR") is emerging as a cost-effective way of resolving disputes on the Internet. It is however ADR with a difference from the conventional model.

In any analysis of payment systems, it becomes clear very quickly that each additional payment within the system is costless. Following economics, the capital investment is sunk costs, so the cost drivers of the system are then what remains: support and sales. In theory at least we have already disposed of sales by pushing exchange out of the core Issuance, above, which leaves support costs.

Support costs are basically about transactions or accesses that go wrong. So the fundamental cost driving equation is one of the ratio of bad transactions and the average costs of each such transaction.

Reducing the costs of disputes is one way forward, and innovations such as the strong user agreement and triple entry accounting reduce uncertainty and thus costs in any dispute. In practice they dramatically reduce the number of disputes because all sides have the same evidence, and that evidence is generally very clear.

One Issuer made a dramatic step forward. In dealing with the rapidly escalating costs of scams and other frauds, the Issuer set a new policy of not offering any *extraordinary actions* except when ordered to by a court of competant jurisdiction. In effect, the Issuer threw up its hands in horror, and said "no more without a court order!"

This draconian step was of course unpopular with users, but in one fell swoop reduced support costs dramatically as it was no longer necessary to pass judgement on the rising tide of disputed transactions. Unfortunately it was only half the answer as the courts in the approximate jurisdiction of the USA are notoriously expensive (primarily because of the perverse incentives imposed on and by the legal industry) so only the largest of cases could generate the required court order.

Another issuer, this time in Russia, faced the same tide of rising fraud. [1]. It also instituted the rule of only juridically ordered exceptions. But it went one step further and specifically encouraged and enabled the arisal of cheap arbitration to provide those orders.

In this system, any User could file a dispute on the payment of a fee of 10% of the arbitrated amount, but this is deliberately kept flexible so that any amount can start an action, the funds stolen were a barrier to even filing. The dispute would then be referred to one of a list of arbitrators who are drawn not from the (expensive) legal fraternity but from the (cheap) user community. The arbitrator has extended powers in the system and can even breach privacy by tracing transactions.

In this concept, the arbitration’s "award" becomes an order that the Issuer can respect, as it is independent and already paid for. This independant accounting of the costs of dispute resolution then lead to clear signals as to where to deploy resources in fighting overall fraud - something that no other system enjoys.

How to Use it

How it Stacks up

The IMF’s Code on Transparency

It is difficult to compare the results of governance structures as it is hard to run the experiment without it being spoilt by the existance of other methods. The notion of self-governance is perhaps rarer than expected, although the words appear frequently enough.

However, some elements of open governance are found in other models. The International Monetary Fund ("IMF") has created a "Code of Good Practices on Transparency in Monetary and Financial Policies" that mirror many elements of open governance [IMF]. Perhaps surprisingly, the structure of the IMF and the targetted international financial agencies and central banks correlates well with our present target unregulated issuer: both are effectively self-governing organisations with no assistance or oversight from a higher body.

Specifically, the IMF code promotes the publication of the balance sheet, aggregated market transaction data, and any audited financial statements, all on a reliable basis. It quite clearly indicates that governance procedures, independent audits, and internal audit arrangements should be publically disclosed [IMF2]:

8.2	**Where applicable, financial agencies should publicly disclosed audited financial statements of their operations on a preannounced schedule.**
8.2.1	Financial statements, if any, should be audited by an independent auditor. Information on accounting policies and any qualification to the statements should be an integral part of the publicly disclosed financial statements.
8.2.2	Internal governance procedures necessary to ensure the integrity of operations, including internal audit arrangements, should be publicly disclosed.

The IMF is saying to the users of this code (which it defines as those with oversight over payment systems) that the words "trust me, we’re audited" are inadequate - only information published to the public is acceptable.

The only significant area where the code differs from the model of open governance is that it insists that financial statements should be audited, whereas in open governance, we leave this as an option to the Issuer. The difference here is in the size of the constituent - a central bank can easily afford an audit of its financials. On the other hand, an unregulated issuer of money starts out small and lean. Many are happily doing business with less than a million dollars in issued float, an amount that is too small to be attractive for an insider theft. Further, they can ill-afford to spend money on an audit when the audit cost will exceed its income by an order of magnitude.

Bernard Newman suggests that the code may have resulted from the trial by fire of the IMF’s own corruption record [BN]. From the abstract:

> Faced with the crises and scandals of recent years the IMF has determined to strengthen "the architecture of the international financial system," thus to create a possible solution to the problem.

Either way, the public disclosure aspects of IMF's view of governance are stressed.

Conclusion

Some Examples

Open Scrutiny

Open scrutiny is no stranger to us: it is a fundamental leg of the process of democracy. All public institutions benefit in meeting their mission by scrutiny from their very same served public.

http://www.icannwatch.org/

References

[OG] The first reference to the term Open Governance is this article that equates it more to caveat emptor: Martin Wilcock, OPEN GOVERNANCE: The Case For Unregulated E-Commerce, Journal of Internet Banking and Commerce (JIBC), June 2000, vol. 5 no 1.

[FC7] Ian Grigg, Financial Cryptography in 7 Layers, Proceedings of the 4th Conference in Financial Cryptography, 2000, Anguilla, East Caribbean.

[IRS] Big-money tax evaders in IRS cross hairs, August 5, 2004

[G2] Ian Grigg, Critique on the 1994 EU Report on Prepaid Cards,

[FC7.2] The disciplines required for a successful money are suggested in Financial Cryptography in 7 Layers, Op Cit,

[TEC] Ian Grigg, Triple Entry Accounting, Draft paper.

[TEC] Ian Grigg, The Ricardian Contract, Workshop on Electronic Contracting, 2004.

[1] Nikita Sechenko, Save Thyself - Russia's WebMoney Payment System (translated) Translated from the original Russian by Daniel Nagy.

[IMF] International Monetary Fund, Code of Good Practices on Transparency in Monetary and Financial Policies: Declaration of Principles

[IMF2] Ibid, 8.2

[BN] Bernard H. Newman, International Monetary Fund Corruption Victim: is Accounting/Auditing the Solution? Lubin School of Business, Pace University, New York. This paper may have been published by the American Accounting Association, no full paper has been found. http://aaahq.org/NERegion/2001/Accepted/bnewman.pdf