Tailoring Identity For You

privacy by demand

Barely a day passes without news of another high-profile **data breach** or mass **identity fraud** and even household names have fallen foul to criminal hackers.

In response to the public outcry ambitious regulations have been introduced such as the European Union's **GDPR** and the Payment Card Industry's **PSD2** which aim to safe-guard privacy and reduce security breaches.

You already understand how you need to use identity to service the needs of your business and customers, the question is how do you adapt existing solutions to comply with these regulations?

The **GDPR** will take effect for all UK businesses on **25 May 2018** and reports are already circling of top-tier law firms preparing high=profile test cases for that date with the first rulings likely to be delivered in **October 2018**. **Big name brands** will be amongst those feeling the regulation's bite.

"If your organisation can't demonstrate that good data protection is a cornerstone of your business policy and practices, you're leaving your organisation open to enforcement action that can damage both public reputation and bank balance."

– Elizabeth Denham, Information Commissioner

Whenever your organisation processes **personal data** for **individuals** living in the EU the **GDPR** rules and restrictions apply even if that processing happens in another jurisdiction.

Personal data encompasses everything relating to **genetic**, **mental**, **cultural**, **economic**, and **social** identifiers.

Whenever your organisation **processes** any **personal data** you must have **explicit consent** from its **subject** or their **legal guardian** and you may be called upon to **prove** their consent in a **court of law**.

If this weren't onerous enough, not only can the subjects of processing **demand** all **personal data** held on them at any time, delivered in a **portable data format**, they also have the **right to be forgotten**.

The implications of these **guaranteed rights** for existing IT systems are far-reaching.

Day-to-day operations must be brought under **internal governance** procedures **proving compliance** to standards such as **ISO 27001** and **BS 10012**.

More significantly **software development processes** must embrace **privacy by design** principles from their very earliest stages. A generation of developers will need **training** and many **industry practices must change**.

distributed ledgers

For as long as mankind has been a trader of goods and services there's been a need to keep accurate records of profit and loss, or liabilities incurred and of safeguards deployed.

Our language is replete with audits: to take stock of a situation; to settle our accounts; to pay the final reckoning.

Sumerian accounting tablet

For centuries we've recorded our commercial transactions in ledgers tracking paper artefacts which we know are can be falsified, with independent auditors to confirm their integrity.

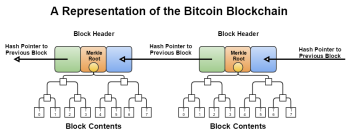

multi-column spreadsheet

The switch to digital technology was heralded as a chance to do away with all this paper. But how can we do that when so much of it's needed to prove our records are telling the truth?

Distributed ledgers are a new development aimed at addressing this problem.

The aim of a distributed ledger is to store digital records in a vast computer network with at least the same integrity we expect from our existing paper records.

They do this by leveraging techniques developed for secure communications to create audit trails which becoming increasingly difficult to alter as they grow in size.



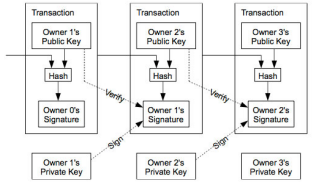
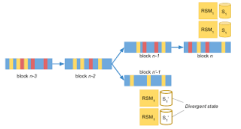


Diagram of a Bitcoin
from *Bitcoin: A Peer-to-Peer Electronic Cash System*, published in 2008 by "Satoshi Nakamoto".

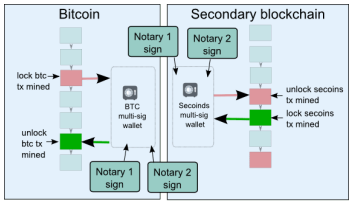
The most popular ledger design is the **blockchain** first popularised by the **Bitcoin** electronic currency system. This presents an immutable structure in which each block not only references its predecessor, it also includes a cumulative proof of the integrity of each preceding block.

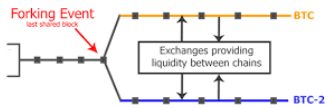
The Bitcoin network is a **peer-to-peer** design in which a majority of the participating computers reach a consensus about which transactions have occurred.



When the network is interrupted multiple forks are created which need to be resolved somehow when communication is restored. In the case of Bitcoin only the most active fork will be preserved with others abandoned.

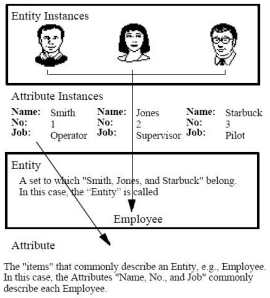
One way of mitigating the effect of forks is to use **side chains**. These are links between disparate blockchains which can be used to preserve these phantom forks.





identity is exchange

Throughout history humans have defined each other in terms of **attributes** such as whom they associate with, which goods they possess, how they present themselves, and what they believe.



The "items" that commonly describe an Entity, e.g., Employee. In this case, the Attributes "Name, No., and Job" commonly describe each Employee.

For the most part these attributes arise from subconscious judgements about inferred membership of a group or eligibility to engage in some restricted activity.

This is easily managed in small groupings where all the members and their attributes can be generally known, whilst in larger tribal groups permanent markings earned throughout life make this knowledge more explicit.

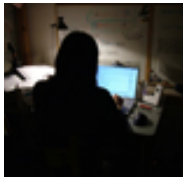
However as societies grow larger and more complex this is no longer sufficient and physical **tokens** become increasingly important to asserting membership rights and status. But tokens suffer from two serious shortcomings.

Not only can they easily be stolen, they can also be counterfeited.

The authorship of tokens is often asserted by **signing** them with an accepted **trust mark** which is equally prone to misuse so these are often further enhanced with features which are difficult to copy.

When we decide that a token is validly signed we're placing confidence in the issuer to be authoritative. How much confidence we should have depends on how easy it is to duplicate the signature.

When a token arrives in a package with an intact **seal** we can be reasonably confident that it's not been interfered with in transit, especially if we also have a high level of trust in whoever delivers it.



Tokens in their simplest form provide a statement of authority without revealing anything about personal identity and this is sufficient for many purposes.

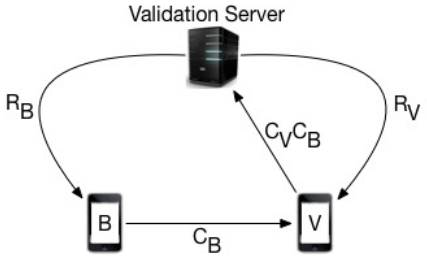
After all, transactions involving cash are often anonymous in this manner and experiments with ways of replicating this in the digital realm are a key motivator for **fintech** innovations such as **Bitcoin**.

When accepting a token it's often desirable to provide proof in the form of a **receipt** that the transaction occurred. Receipts usually come in pairs or triples and unsurprisingly are also tokens.

Annotating tokens with attributes is a powerful way to share knowledge with those who need to trust it.

transactional identity

Let us start with the simple proposition that to create trust between two strangers they need to share a common connection.



The simplest way for these strangers named **B** and **V** to confirm that they share a common connection is for **B** to give a token to **V** and for **V** to then give this token and a second token to the shared **trust anchor**.

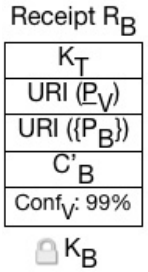
If the trust anchor then contacts both **B** and **V** to confirm **receipt R** of the tokens **C**, each can be certain that the other is trustworthy.

This **triangle of trust** relies on a one-way directed traffic flow where only the **trust anchor** can identify **B** and **V** who remain **anonymous** to each other.

The primary capability the **trust anchor** requires is the ability to convert **tokens** into **destination addresses**.

From this foundation in **anonymity** and **trust** we can build a functional **identity system**. We do this by annotating the **receipt** delivered to **B** with information authorised by **V**, and by annotating the **receipt** delivered to **V** with information authorised by **B**.

Our **trust anchor** has now transformed into a split-horizon **dead-letter drop** through the added capability of converting **tokens** from **B** into messages for **V** and vice versa.



The implementation we demonstrate here takes this idea further and requires some explanation.

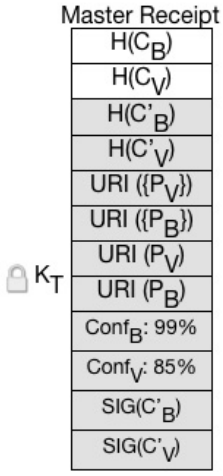
Firstly we have a unique shared key K_T which identifies a **transaction**. This can be used to encrypt any information sent to **B** or **V** so that either can decrypt it.

The **receipt** also contains a new unique token C'_B which replaces the token consumed by this transaction.

Other fields are application specific **URI**s pointing to network resources and a **confidence value** for the data source.

In this example we encrypt each receipt with a key K_B or K_V previously registered with the **trust anchor** though the transaction protocol could be extended to include key transmission.

The **trust anchor** has a privileged position and we can make use of this to do something rather clever by introducing a transaction **master receipt**. This contains the information sent to **V** and **B** with metadata identifying the immediately previous **receipts** issued to each.



The shaded fields are encrypted with the transaction key K_T so either **B** or **V** can decrypt them.

$H(C_B)$ and $H(C_V)$ are the cryptographic **HMAC** message signatures for the respective tokens C_B and C_V. These form links in two fine-grained block chains.

the bespoke experience

There are two kinds of people in this world: those forced to buy their garments **off the peg**, and those who can choose **made-to-measure**.

The made-to-measure route is far more effective when introducing a modern **digital identity** system.

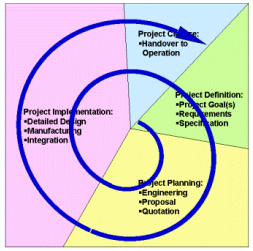
Your organisation already has numerous ways to represent identity tailored to its **domain knowledge**, **auditing**, **customer relationship**, **access**, and **capability management** needs.

Right now your IT teams address these with **legacy systems** no one dares to retire and one-size-fits-all **enterprise applications** with configuration options to match.

Isn't it time **your organisation's needs** take precedence over those of vendors?

At **InIdSol** we're passionate about the **science** of **digital identity** and place **privacy by design** at the centre of both commercial practice and research endeavours.

We use proven **iterative methods** to keep costs and risks low as we explore our clients' needs, and apply our scientific understanding to find viable tailored solutions.



This flexible approach works equally well with traditional **waterfall** development and newer **agile** methodologies.

As a design house our main outputs are **system design documents** explaining our proposed solutions for a general audience. The most important of these are **detailed specifications** intended for implementation but we can also provide **proofs of concept** and **mockups**.

Our designs are always supported by onsite **training** to ensure you gain the necessary **skills** and **institutional memory** necessary to **maintain** a **state-of-the-art** digital identity **infrastructure**.

Aside from design we also provide a **code auditing** service aimed at identifying weaknesses in your existing applications and providing remedial advice for privacy hardening.

Our many years implementing digital identity systems allows us to work with recruiters to **screen** potential **candidates** for suitable **experience** as you **build** your **developer** or **support base**, focusing on **security**, **biometrics**, and **machine learning**.

As an added bonus we have extensive experience developing **patents** so where commercial considerations make this a high priority we will introduce you to respected **patent attorneys** to oversee the process.