Visit our website

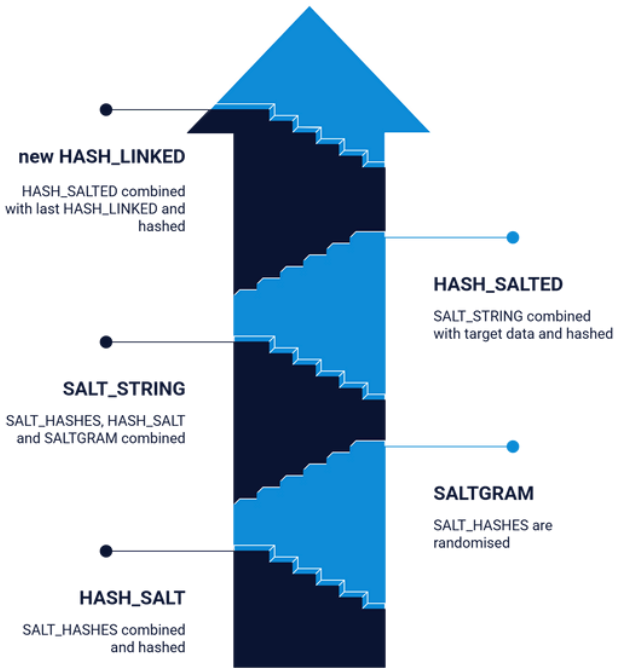
Codel Hash-Chain Technical Summary

The Secret is in the Salt

The **Codel Hash-Chain** is a novel variant on hash lists, hash chains and commitment schemes, featuring elements of all three.

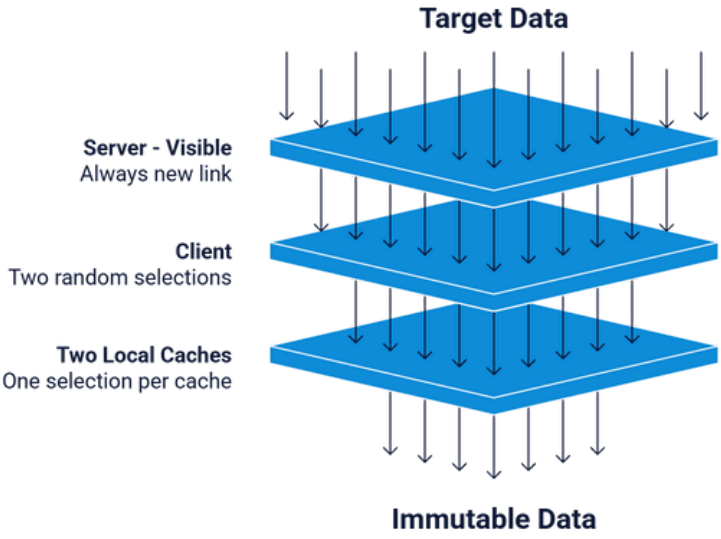
The key concept described in our patent is the entanglement of selected elements of the chain (SALT_HASHES), which are combined and hashed to HASH_SALT. They are then randomised into a SALTGRAM (an anagram with minimum length of 96 bytes).

The SALT_HASHES, HASH_SALT and SALTGRAM are then combined into a single SALT_STRING and appended to the target data whose immutability we wish to protect. The HASH_SALTED of that combination is combined with the most recent HASH_LINKED on the chain and hashed to created the new HASH_LINKED.



The way SALT_HASHES are selected is crucial to the purpose of the entanglement. In order to ensure that every new Link is incorporated, as soon as possible, into a SALT_STRING, each new Link is assigned as one of the SALT_HASHES to the first (slightly older) link which requests it. This ensures that all new Links become **entangled within less than a second**. However, as this assignment takes place on the Server, it is visible to any potential attacker who has access to the growing chain.

Even though it will be randomised into an anagram, we prefer to make all attempts at brute forcing a match not just difficult but "computationally infeasible".



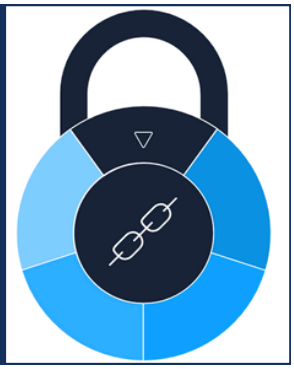
This is achieved by leaving the assignment of the next two SALT_HASHES to the Clients themselves. They make random selections from two caches they build on their local devices.

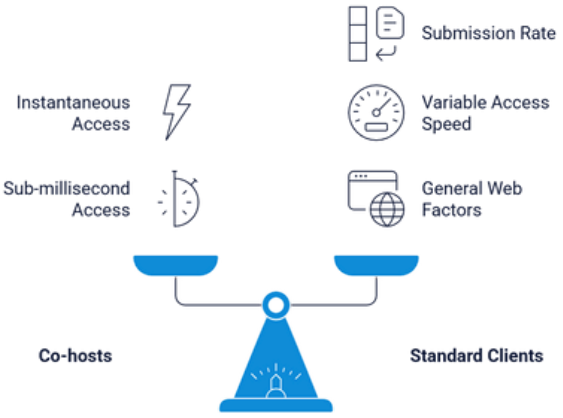
Unless the attacker has simultaneous access to ALL active Clients, they cannot learn which SALT_HASHES have been selected.

Attackers only have a few seconds in which to acquire that information before the results of Client Selections all become **immutable**.

The subsequent randomisation of the SALT_HASHES' 96 (minimum) characters into the SALTGRAM, renders any prospect of brute forcing completely beyond any current or feasible future computing technology. This blocks any attempt by an attacker to achieve "Chain Replacement" which is the main significant weakness in most commitment schemes.

This is what all the Consensus mechanisms (Proof or Work, Proof of Stake etc) implemented by Block-Chains are also designed to prevent, but our algorithm provides **greater guarantee of protection**, far faster, far more effectively and at a tiny fraction of the cost.





As the effect is instantaneous (no attack can successfully replace a new Link and still pass the validation tests) from the moment the new link is added to the chain, we have also **eliminated Verification Latency**.

However, the logistics of chain publication and the need to protect it from other attacks (eg DDoS) do create a "Publication Latency" which delays validation for a period depending on how well you are connected to the chain.

Co-hosts (those organisations large enough and with an interest in either access speed or the promotion of digital trust - to become one of the Chain Builders) will have **instantaneous access** to those links they create themselves and sub-millisecond access to links created by other Co-hosts.

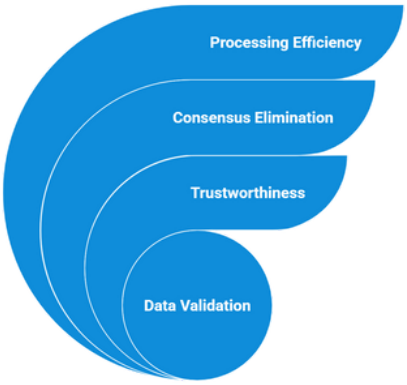
Counter intuitively, the speed of publication is increased by increasing submission rates. This is because, we only allow public access to the data when blocks of 10,000 are completed and protected by a further link on the chain (which appears in a later block). The higher the rate of submissions, the faster we reach the 10,000 target. If, for example, the submission rate exceeds 100,000 per second, blocks would be published about 1 tenth of second after the first link in the block appeared on the chain. At that point, all the publication latency is really down to local conditions such as broadband and device performance.

Standard Clients access speed will depend on all the factors which influence web access more generally (bandwidth, contention, local OS issues etc).

No Consensus Required

As presaged above, a significant consequence of this approach is that **no "consensus" is required to ascertain the validity of any protected data**.

Either it validates and can be trusted or it doesn't and cannot. The Relying Party does not have to consult any other party to reach a reliable conclusion.

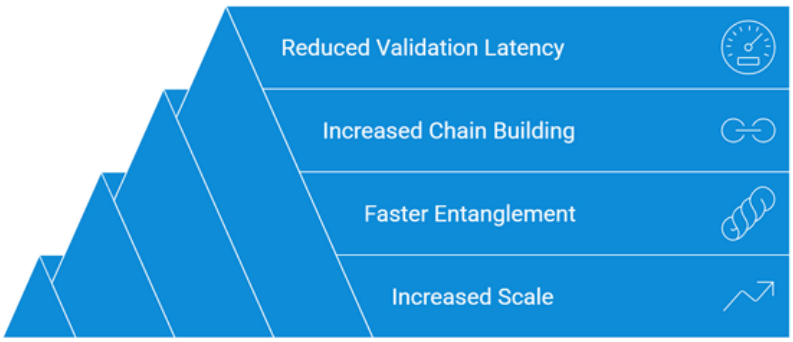


As a result, **far less processing power** is required to generate the Hash-Chain than standard Block-Chains, all of which, so far as we know, require some kind of consensus mechanism to confirm their collective integrity.

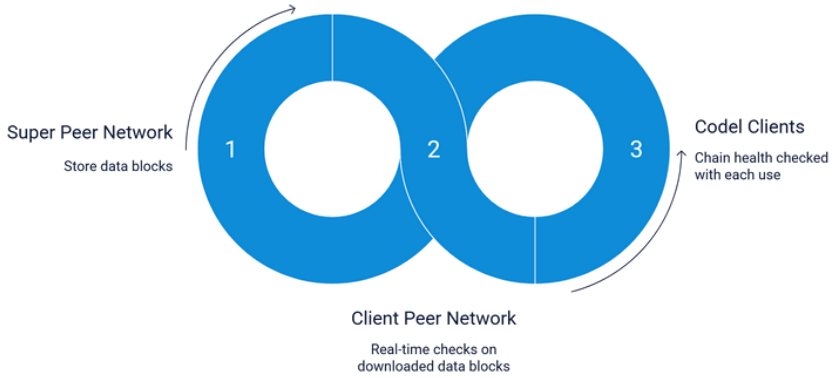
All means of achieving that consensus impose much more significant computing overheads than our Entanglement Algorithm.

To hammer the point home: NO Attack on the Chain can result in the deception of either the Author whose Client created the Link or the Relying Party who seeks to validate the relevant data. The worst case scenario is a "false negative" where an attack on the chain might cause validation to fail. **No "false positive" is EVER possible**.

One of the consequences of the Chain logistics is that the speed of chain building and, to some extent, validation actually increases with scale.



We do, however, use a much cheaper form of Consensus, in the form of a "**Client Peer Network**" (CPN), to surveil the "**Super Peer Network**" (SPN) of Co-hosts. Those active on the CPN perform routine real time checks on all Blocks of data downloaded from the SPN and share their results.



This is NOT required to confirm the validation of any given protected item but to identify and interdict any attempts by attackers to disrupt the system or corrupt the data before it can significantly impact the service. This process ensures that any attempted attack on the growing chain will be detected in as little time as it takes to download the data.

We WILL be Attacked

We DO anticipate such attacks once the reliability of our integrity protection is widely understood. Why? Because if the only way to conclude a transaction, access resources, cross borders etc is to validate documentation protected by the **Codel Hash-Chain**, then one obvious way to bypass that obstacle is to try to take down the Chain for long enough for Relying Parties to conclude that they'll have to ignore the validation procedure and take the risk of accepting relevant documentation at "face value".

Our protection against such **DDoS attacks** will start with the highest standards currently implemented by all the major Cloud providers but will be supplemented with additional measures of our own - such as permanent "Red and Blue" teams alternating between attack and defence in every Penetration Testing scenario they can imagine.

Visit our website

Anonymity AND Full Disclosure fully supported

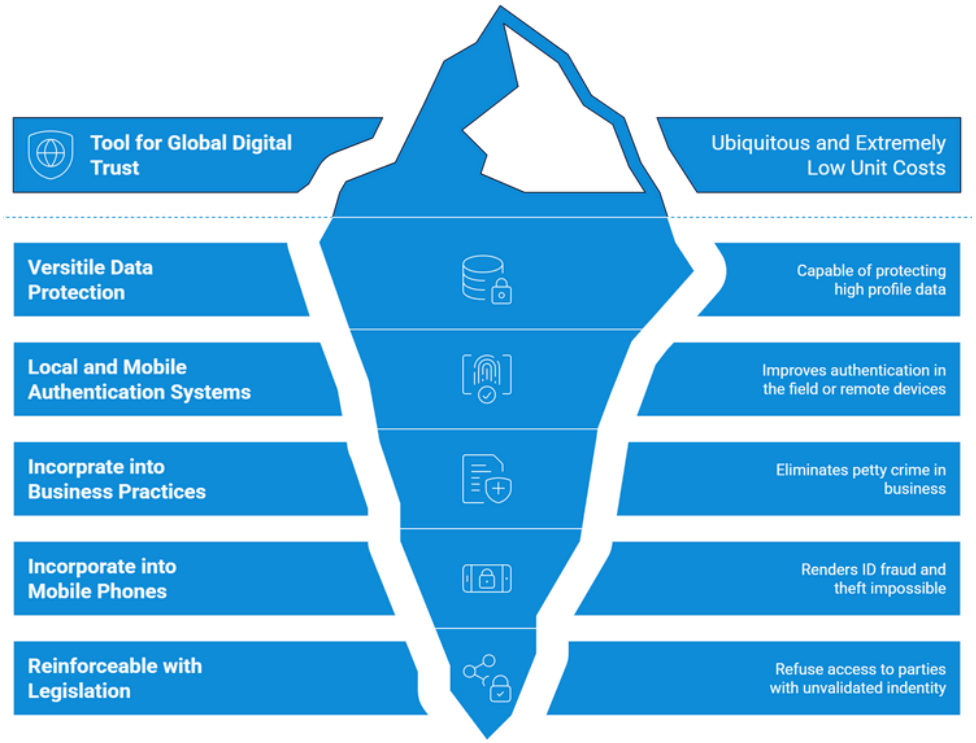
All data on the chain is **anonymous by default**. It is left up to the Authors and Relying Parties to agree on the level of disclosure they require.

The Codel Client implements **7 levels of authentication** from complete anonymity through to multiple witnessed transactions supported by strong biometrics. Probably stronger than that required for the launch of nuclear missiles.

A solid basis for Global Digital Trust

The overall effect is that the system has **extremely low unit costs**, which makes it ideal for both **bulk data protection** (protecting the integrity of vast numbers of data) and **trivial data protection** (family snapshots, diary entries, life logging etc) as well as all data in between. That **ubiquity** makes it an obvious tool to create the infrastructure for **global digital trust**.

As well as protecting all the high profile data like large financial exchanges and asset transfers, it can trivially protect and improve all authentication systems to verify not just the integrity of data but, when tested in the field or by remotely trusted devices, to prove the identity of individuals and autonomous systems.



Incorporated into **routine business practices** such as invoice and statement production, identity, attribute and authority documentation etc, it can eliminate most of the widespread but relatively "petty" crime such as "push fraud".

Incorporated into **Mobile Phones**, it will render the vast majority of ID fraud and theft impossible and make it trivially straightforward for users to confirm the identity of any kind of caller or agent, from meter readers, through Uber Drivers, to Security personnel.

Reinforce our protection with legislation to allow relying parties to refuse access or co-operation to any parties who refuse or are unable to validate their identity on demand and another swathe of criminal activity is dramatically reduced, or even eliminated.

All of which is why we believe Codel can dramatically improve the Human Condition and help to save the world from a large number of its serious problems.

For more information or to discuss your requirements in greater detail, please contact
email: james.zorab@codelmark.com | phone: +44 7730 456 463