ConsenSys Academy

a signed blockchain transaction (simplified)

The first, unsigned hash is formed by making a cryptographic hash of the `Sender`, `Receiver` and `Amount` data. The second, signed hash is formed by combining the `Sender` `Receiver` `Amount` and, most importantly, `Hash` data and signing all *those* fields.

By creating these two successive hashes, we are creating a series of protective wrappings. A message that has a valid digital signature on it provides three different confirmations. It confirms:

- **Origin:** From what we learned about public key cryptography, we can infer that if a private key digital signature is valid then the signed message really did come from the account associated with the public key.
- **Message Integrity:** From what we learned about cryptographic hash functions, we know that the message has not been tampered with by anyone else
- **Intent:** By signing the first hash, the owner of the private key is signalling their intent to execute whatever commands or agreements are contained in the message.

In the non-blockchain world, the idea of capturing intent may seem fairly useless since you can't legally force someone to do something they do not want to do. Someone can sign a string saying, "I'll pay you 100 pounds" but you can't really *do* anything with that string. It's just pixels on a screen.

The real power of digital signatures comes when the message within that digital signature can be executed, say on a blockchain protocol. In fact, the only signficant messages in the blockchain world are bits of code that, when signed and validated, can be executed automatically by the blockchain protocol. (If this feels like a leap for you, that's okay, we're going to keep explaining it more.)

Conclusion

The decentralization of intent is the last piece of cryptographic primitives in this section. It's important for capturing intent but it's also significant because it relies entirely on two other primitives (public key cryptography and hash functions) for its existence. Digital signatures are *emergent* in this way, arising from simple-yet-powerful features to create something with equal importance. It's a good microcosm or analogy for the broader ecosystem and yet another example of emergence.

Additional Resources

- Article: The Magic of Digital Signatures (MyCrypto)