OpenSig: Digital Signature Technology

David Potter
dnpotter@opensig.net
OPENSIG−121GfwxgvdEUck7Xb4d5wbMnf7Xm2b4zw3−btc

www.opensig.net

Abstract

Systems and processes exist for signing documents and files electronically for authenticity, integrity and non-repudiation purposes but their benefits are limited when the file itself needs to be modified to contain the signature or if a third party company is required to hold the signature in trust. Following the invention of blockchain technology in 2008[2] it has become possible to store small records on a publicly owned, decentralised, global network, without the need to trust any particular individual or company to keep those records secure. This paper outlines a proposal for the OpenSig standard, which utilises blockchain technology to provide a simple, secure, global and trustless mechanism for signing and verifying any type of digital file.

1. Introduction

This paper introduces OpenSig, an open digital signature scheme. The objective of OpenSig is to define a standard for using blockchain technology as a trusted third party register of digital signature records, allowing anyone to sign any file and for others to verify its authenticity and integrity. This paper introduces the technology; the requirements of the OpenSig standard will be released to developers in a separate document on opensig.net.

To digitally sign a file, electronic signature schemes produce a signature record from a cryptographic hash of the file contents that is signed by the signer's private key. The resulting record is then made available to whoever needs to verify the file either by modifying the file to hold the signature inside or by storing the signature separately and making it available on request, usually using the services of a trusted third party company. These approaches can have unwanted technical consequences or security and privacy risks. Examples of problems resulting from existing digital signature schemes are:

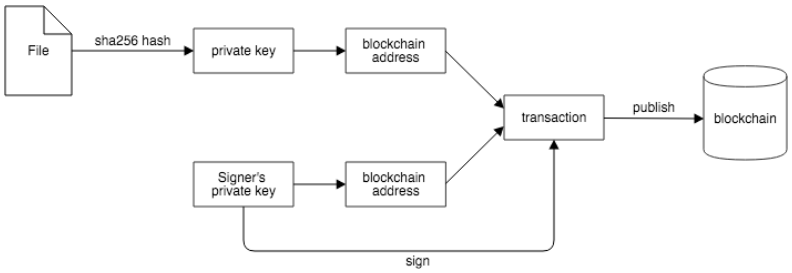
- **Restricted**: modifying the file, either by inserting the signature or by wrapping it in a container, may restrict the type of file that can be signed

or can render the file unreadable to any software that does not support the specific signing technology;
- **Trust**: for some, trusting a third party company to hold their signature records indefinitely, and not to accidentally or maliciously discard or corrupt them, may not be an acceptable risk;
- **Privacy** some digital signature services require the file to be uploaded to their cloud server for signing, resulting in privacy issues.

OpenSig technology attempts to solve these problems by allowing the user to sign any file within the privacy of his device, recording the signature on a public blockchain maintained by a publicly owned, decentralised, global network of computers. The blockchain provides the role of a trusted, independent third party by storing the signature records indefinitely and making them available to anyone, anywhere, at any time.

2. Signing

To sign a file, an OpenSig compliant client first passes the file through a secure hashing algorithm to produce a SHA-256 hash. This hash is used as the file's private key[1] from which its public blockchain address can be generated (in a sense the file is its own private key and so anyone in possession of the file can derive its blockchain address). To sign the file the signer sends a small amount from his blockchain address to the file's blockchain address, signing the transaction with his private key. The transaction is the signature and is published on the blockchain.



The transaction links the public blockchain addresses of the signer and the file at the approximate date and time it was signed.

2.1. Cost

There is a cost associated with publishing any transaction on the blockchain. The cost is made up of two parts: the amount sent to the destination address(es) and a fee paid to the miner for maintaining the network. The cost of publishing

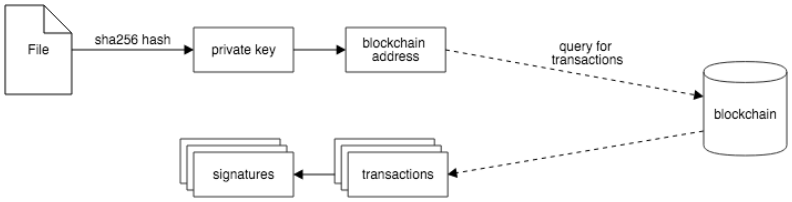
[1] If the hash is outside of the range of valid ECDSA private keys additional zero bytes are appended to the file's data one at a time until a valid key is found.

a single OpenSig signature transaction on the blockchain will depend on the specific blockchain technology. In the case of the Bitcoin blockchain, at the current time and price ($420/btc) it costs between $0.02 and $0.07, depending on how quickly the user wants the signature to be recorded on the blockchain[2]. The following table shows the time that a user could reasonably (with 90% probability) expect to wait for a signature to be recorded based on the overall cost of the signature transaction[3] (this is an indication only as the figures will vary over time):

Cost	Approximate time of confirmation
$0.02	3+ hours to ∞
$0.03	25 minutes to 5 hours
$0.04	0 minutes to 2 hours
$0.05	0 to 45 minutes
$0.06	0 to 35 minutes
$0.07	0 to 30 minutes

3. Verifying

Anyone in possession of a file can pass it through the same hashing algorithms as the signer to generate its public blockchain address. The blockchain can then be queried to obtain a list of all the input transactions for the file's blockchain address. These transactions (if any) are the signatures of all the people who have signed the file, from which each person's public blockchain address and time of signing can be extracted.



Provided each signee has shared his public blockchain address with the verifier - thereby declaring himself as the owner of the key - then the verifier is able to identify who signed the document and when. A user's public keys are freely shareable with no security risk. They may be shared by any unsecured method, for example by email, on social media, on a website or on a business card.

If the file has been modified since it was signed then the public blockchain

[2]A miner will usually mine transactions with the highest fees first so how quickly a signature transaction is accepted by the network depends on the value of the fee and the values of the fees in other transactions waiting to be mined. The optimum fee for ensuring (with high probability) that the transaction is included in the next block candidate varies, but is assumed to be 45 satoshis per byte for the purposes of the cost calculation. The minimum valid amount payable to an address is 5430 satoshis so the total transaction value can range from 5430 to 16680 satoshis, given a mean transaction size of 250 bytes.

[3]Data from cointape.com 15th April 2016.

address generated by an OpenSig client will be different from the original and a blockchain query will not return the original signatures. In this way the integrity of a signed file is assured.

4. Privacy and Security

When signing or verifying a file all private data, including the file and all private keys, are contained on the local device and do not pass beyond the OpenSig compatible client software - only the public keys of the file and the signer are published. Due to the asymmetric nature of the cryptography used by blockchain technology it is practically impossible for any information about the file contents or its private key to be reverse engineered from its public key.

Once a signature is published to the blockchain it is, in practice, impossible for it to be removed or corrupted, and, being decentralised, the network that maintains the blockchain is available 24 hours a day.

5. Use Cases

5.1. Keys for different roles

Private and public keys can be easily created and so there is no practical limit to how many public keys an individual can have. Like email addresses a public key is a token of identity and a person may choose to use different identities for different roles, such as for personal and for office use. The different keys may then be shared with different groups of people.

5.2. Blockchains for different roles

The OpenSig standard does not specify one particular blockchain to use to record signatures, rather it encourages OpenSig compatible clients to support multiple blockchains allowing the user to choose which blockchains they want to publish their signatures on. This frees the user to choose blockchains that are compatible with, for example, their roles, their specific technical requirements or their moral sensibilities.

5.3. Signature Pages

For documents with a signature page the public keys of the signees can be inserted into the document in place of their manual signature. The verifier will be able to verify the signature page against the corresponding signatures on the blockchain.

6. Limitations

6.1. Signature Timestamp

The timestamp for a signature returned by the OpenSig verification process is dependent on the technical specification of the blockchain on which the signature was published. In the case of the bitcoin blockchain the timestamp is that of the block that mined the signature transaction. This is an approximate time, known as the network-adjusted time, which is dependent on the accuracy of the miner's local system time and those of its neighbouring network nodes[1].

When the optimum fee is used and the network is not overloaded, the user can expect the signature to be included in next block candidate, which will, on average, be 5 minutes after the file is signed. Assuming the network takes a further 10 minutes to mine the block, and the block timestamp is reasonably accurate, the user can reasonably expect, as a best case, for a signature to be timestamped approximately 15 minutes after the actual time the file was signed. When a lower non-zero fee is used the user may reasonably expect the network to take a few hours to timestamp the signature.

In extreme cases, when a very low or zero fee is used, it is conceivable for a transaction to take days or longer to be accepted by the network. It is also theoretically possible for a block's timestamp to be inaccurate by $\pm$1-2 hours without the block being rejected by the network[1], or for the miner's node to be subject to a 'timejacking' attack[3]. In these extreme circumstances it is possible for a signature's timestamp to mislead the verifier; for example for a signature to be dated the day before the document if it was signed just after midnight. There are steps that can be taken to improve accuracy, for example by using higher transaction fees and by developing a client that examines the timestamps of the signature's neighbouring blocks.

These limitations and examples demonstrate that if precision of the signature's timestamp is critical to an application then OpenSig technology may not be appropriate.

6.2. No Signing Restrictions

There are no restrictions on who can sign a file, when it is signed or how many times it can be signed - anyone in possession of the file can sign it at any time in the future. Indeed, since the blockchain is public it is, at least in principal,

possible for anyone to sign any file, although they would not know what they are signing or even if they are signing a file at all.

7. Conclusion

Using OpenSig technology to record digital signatures allows anyone, anywhere in the world, to digitally sign any file in the privacy of their device without the need to register their details with a third party or pay high up-front costs. It provides signers and verifiers with a digital signature strategy that does not require trust in each other or in a third party. OpenSig technology is simple, secure and global.

References

[1] "Bitcoin Specification: Block Timestamp." https://en.bitcoin.it/wiki/Block_timestamp.

[2] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System." Nov. 2008. https://bitcoin.org/bitcoin.pdf.

[3] "Timejacking & Bitcoin." May 2011. http://culubas.blogspot.co.uk/2011/05/timejacking-bitcoin_802.html.