bdoc

Abstract:

The recent increase in incidents of document forgery gives rise to third parties that collect, validate documents. There are many ways to verify the authenticity of paper documents, including watermarks, signatures and embossed seals. But digital assets present a problem. Documents in digital form can be modified and copued with no one being the wiser. That makes them difficult to trust. There are many products and services that provide secure and verified document management, but they can be expensive and often require the involvement of a third party. Blockchain has demonstarted that trusted, auditable computing is possible using a decentralized peer-to-peer distributed ledger. A blockchain can be used to certify the existence, inntegrity and ownership of a document. In this paper, we describe a digital document format named bdoc on top of blockchain.

Keywords:

Blockchain, IPFS, Documents, bdoc, authentication

Introduction:

To create trust, in todays digital document verification, validation and sharing process, requires the devotion of a tremendous amount of resources to audit and verify documents. This leads to reducation in efficiency and accuracy. The current document verification & validation processes are also terribly inaccurate and prone to failure.

It is quite challenging to protect the documents, and impossible to truly verify the existence & ownership of the document because of the manual efforts required for the same. Software programs have helped to automate some of these tasks, but they are even harder to protect, synchronize, and verify because computer records are easy to change and have single point of failure , if not managed properly & protected securely.

Proving the authenticity of a documet at a certain point in time can be very useful for educators, entrepreneurs, and attorneys. Timestamping data in an unalterable state while maintaining confidentiality is perfect for legal applications. Users can use it to prove the ownership and authenticity of any documents including a will, deed, power of attorney, health care directive, promissory note, satisfaction of a promissory note, and so on without disclosing the contents of the document.

Blockchain provide a mechanism to store the data in a peer-to-peer decentralised distributed ledger and makes it independently auditable. Blockchain is a continuously growing distributed ledger of transaction records. Each participating node in the blockchain network maintains a copy of the ledger. The distributed nature of the ledger prevents tampering and revision, which makes it easy to confirm the authenticity and security of every transaction recorded on the chain. This feature can be used for documents too. In this paper, we have describe how the distributed ledger technology along with smart contract can be used to create a document format “bdoc” that makes it faster, cheaper for document creation and validation.

Proposed Solution:

All kinds of collaborative and business operations require some type of document sharing. Blockchain is a digital mechanism that enables people who do not know each other to engage in trusted transactions with full confidence in the integrity of the assets being exchanged.

Bdoc can be used to solve the existing problem of verifying the validity of digital assets such as a picture of your birth certificate, a pdf document stating your will or a signed legal document specifying a business deal very efficiently and at a very low implementation cost.

bdoc is a blockchain based file format developed to address the authenticity, integrity, security and transaparencey of the document. This is done by embedding authentication, ownership information into the document itself and using a smart contract to keep tracking the system to protect against tampering or modification. The actual content of the document will not be uploaded on the blockchain network.

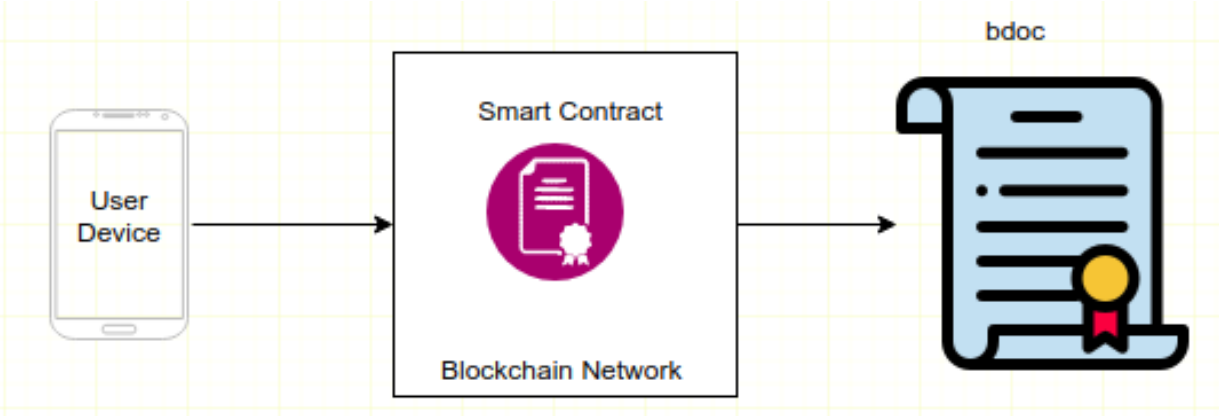

Fig. 1 Blockchain Document Creation Overview

The following process is used to create a blockchain document:

Process for document creation :

i) The content of the document is hashed using sha256 or equivalent method

ii) A smart contract method creates the record and returns a unique Id for the document. On blockchain a smart contract is used to store following information:

a) document name ,

b) document hash ,

c) user id of the person creating the file .

iii) A metadata is created about the document including

a) the unique id returned by smart contract ,

b) blockchain Id (can connect to any blockchain) ,

c) type of blockchain .

iv) Metadata created in step 3 and document is encrypted with user public key & encapsulated in a zip file .

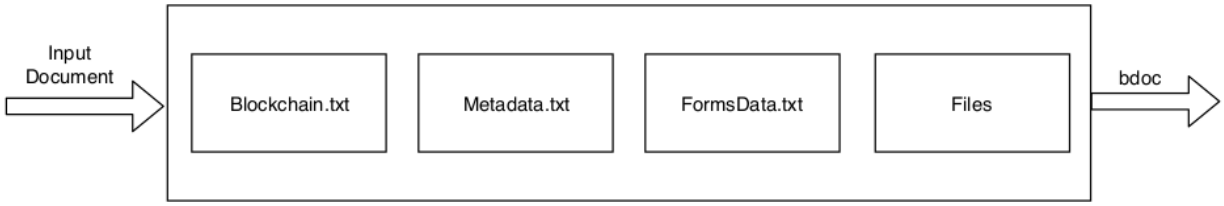

Fig. 2 An Overview of internal file structure of bdoc

A bdoc compromise of blockchain.txt, metadata.txt, formsdata.txt and the acutal document. Blockchain.txt contains the information about the documentId, document hash and information of the blockchain. Metadata.txt contains the information about the dfifferent pages of a document. Formsdata.txt contains information about the ownership of the document and files have the actual document.

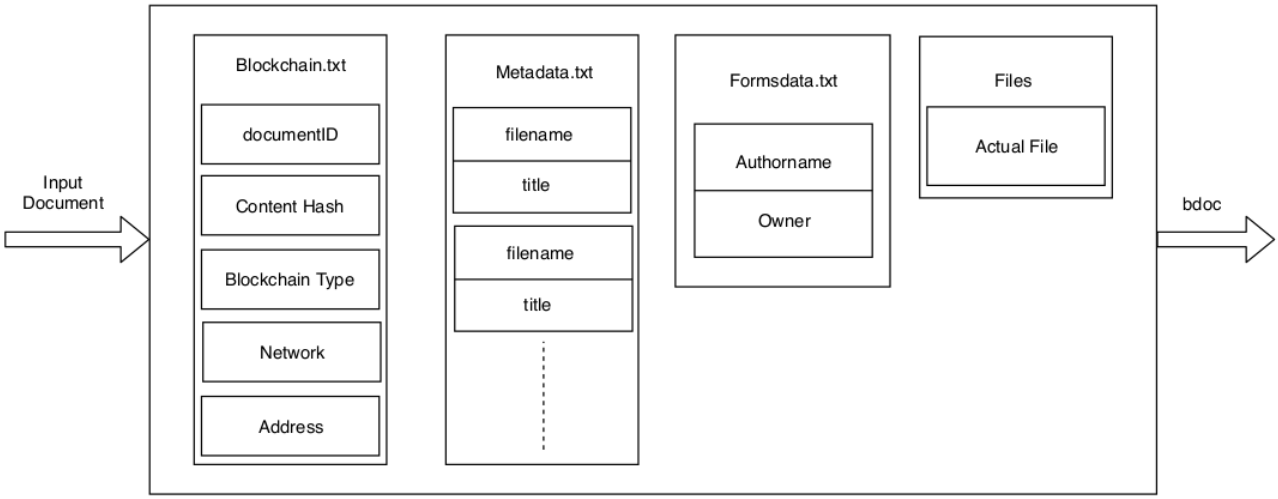

Fig. 3 Internal file structure of bdoc

Process for document verification

i) Document is un zipped and decrypted with user private key

ii) Metadata and content is extracted

iii) Blockchain information is used to connect to the blockchain

iv) Content is hashed and compared with hash stored on blockchain .

v) Metadata is hashed and compared with the hash stored on blockchain .

Due to the characteristics of the Blockchain, bdoc can be accessed by anyone having the permission/ownership of the document and can be easily verifed by others by digital signatures of the document without having to rely on trusted intermediaries. The use of digital signatures encoded into documents, as opposed to physical signatures printed with physical ink, provides assurance that the document was not modified after the signing.

Using the bdoc now it become eaiser to answer the following:

Authenticity : How do i know this is the document created by a said person?

Integrity : How do i know the content of the document has not been changed?

Security : How do i make sure that this document will not be read by an unauthorized person?

Transparency : How do i know that this document has been read by said person or if the document has gone through a due workflow process?

Conclusion

Personal documents should not be trusted in the hands of third-parties, where they are susceptible to attacks and misuse. Instead, users should own and control their documents without compromising security. The proposed document format in this paper achieve this by creating a specific document format bdoc on blockchain, where actual document is stored in user device or off-chain. Users always have the control of their documents and can grant permissions to organisation to access documents using the application. It also makes collecting, storing and sharing of documents simpler and all operations can be easily tracked on blockchain.