evp
evident proof

An introduction

Dr Ken Boness

Evident Proof is...

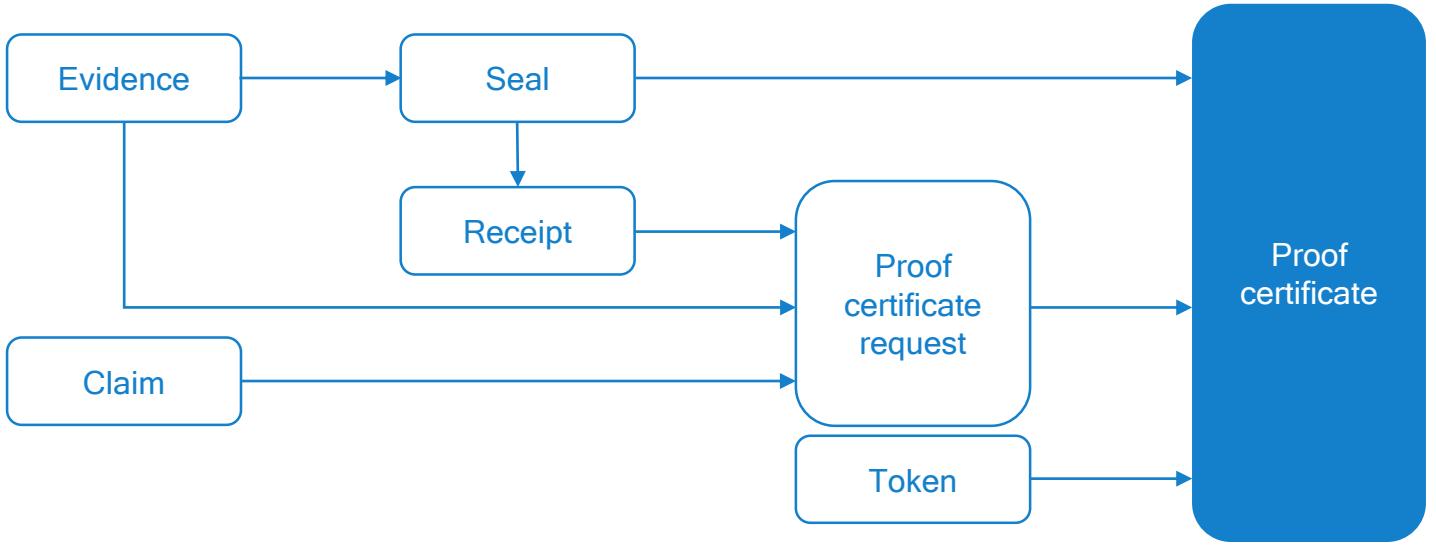
A digital platform, underpinned by blockchain technology, which ensures that data transactions, events and documents can be used as dependable evidence

Immutable proof for organisations and individuals

What the platform does

Evident Proof:

- Takes digital records, such as data transactions, events and documents, and creates a unique signature – a seal - for each.
- Stores these seals in an immutable ledger, called a proof chain, from which reliable proof certificates can be obtained on demand
- Generates the proof certificate - a report that verifies the correctness, completeness and time-order of digital records submitted as evidence



How it works: setting up the proof

The organisation (service user) delivers digital records	• Transactions • Data events • Documents
Evident creates unique signatures (seals) of the data	The seals will be used to verify the evidence
Evident places encrypted seals and identity tags on the proof chain	The proof chain uses two blockchains – one private and one public – to ensure immutability
A receipt and token for each seal successfully added to the proof chain is sent to the organisation	Each receipt is kept by the service user as the key to invoking the use of an associated seal in a proof certificate request The token (or fraction of a token) gives the organisation, or a third party, permission to request proof certificates in future

How it works: verification of evidence

Organisation sends proof request and token (which indicates permission to view the verification)	A proof request is a request for a proof certificate to be created by the service. Each request includes a submission of the digital data items being used as evidence **paired** with the receipts to their seals, **together with** the scope, order and time period of the proof required
Evident compares proof request data with seals held on the private blockchain	
Evident generates proof certificate	The proof certificate verifies the accuracy, completeness and time order of digital records submitted as evidence. It indicates if there is any difference between the original records and the seals
Proof certificate information can be further verified on the public blockchain	

Proof certificates

Proof certificates can be generated to verify any document, data event or transaction where a seal is held on the Evident proof chain

A certificate has several parts:

- **Header information** with requestor contract details, date of request, purpose of request including reference to the proof request.
- A **primary table of results** which compares the information originally supplied to that in its seal. Any variations in either the content or chronological order of the data will be shown.
- A **secondary table with reference data** that can be used to independently verify the primary table from the public blockchain.

The proof chain

The proof chain is maintained simultaneously on two blockchains

A private blockchain

- For all regular service support
- The first choice for generating proof certificates for primary service users

A public blockchain

- A public blockchain to act as a guarantor of the integrity of the private blockchain
- Locks in the immutability of the proof chain
- The method for generating proof certificates for secondary service users

Using two blockchains: immutability

evp
evident proof

Public blockchains

Replicated on countless numbers of separate computers accessed by unknown people known as miners

Miners

Paid for adding blocks of data to the blockchain, miners work independently and competitively. The consequence is that no middleman needs to be trusted – falsifying records on the blockchain is computationally too expensive to contemplate AND it will be discovered

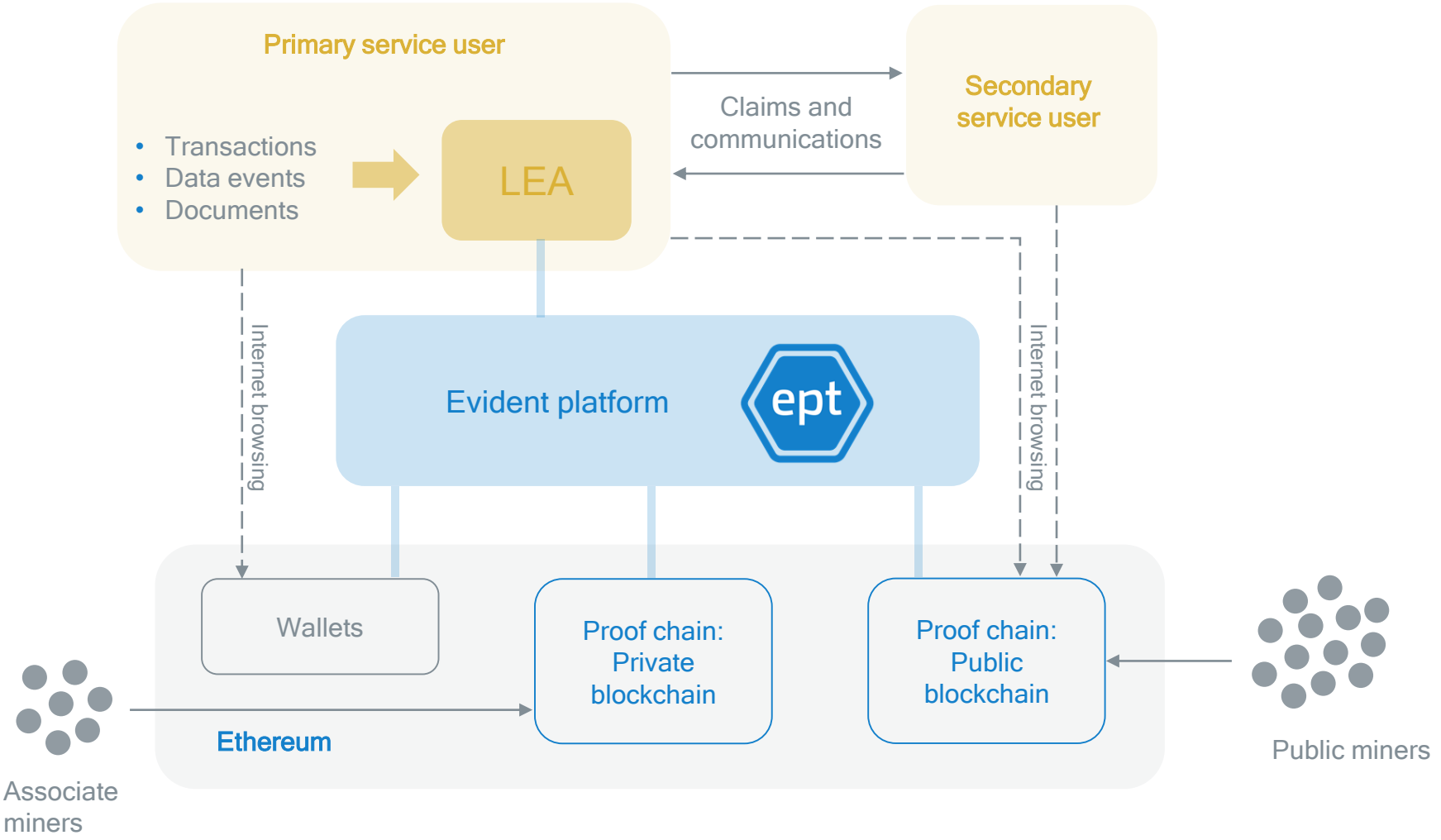
Private blockchains

Allow the cost of mining to be controlled and the speed of service to be maximised. However, the miners are collaborators in the service and the 'trustless' quality of a private blockchain is solely dependent on the computational cost of attempting to change records

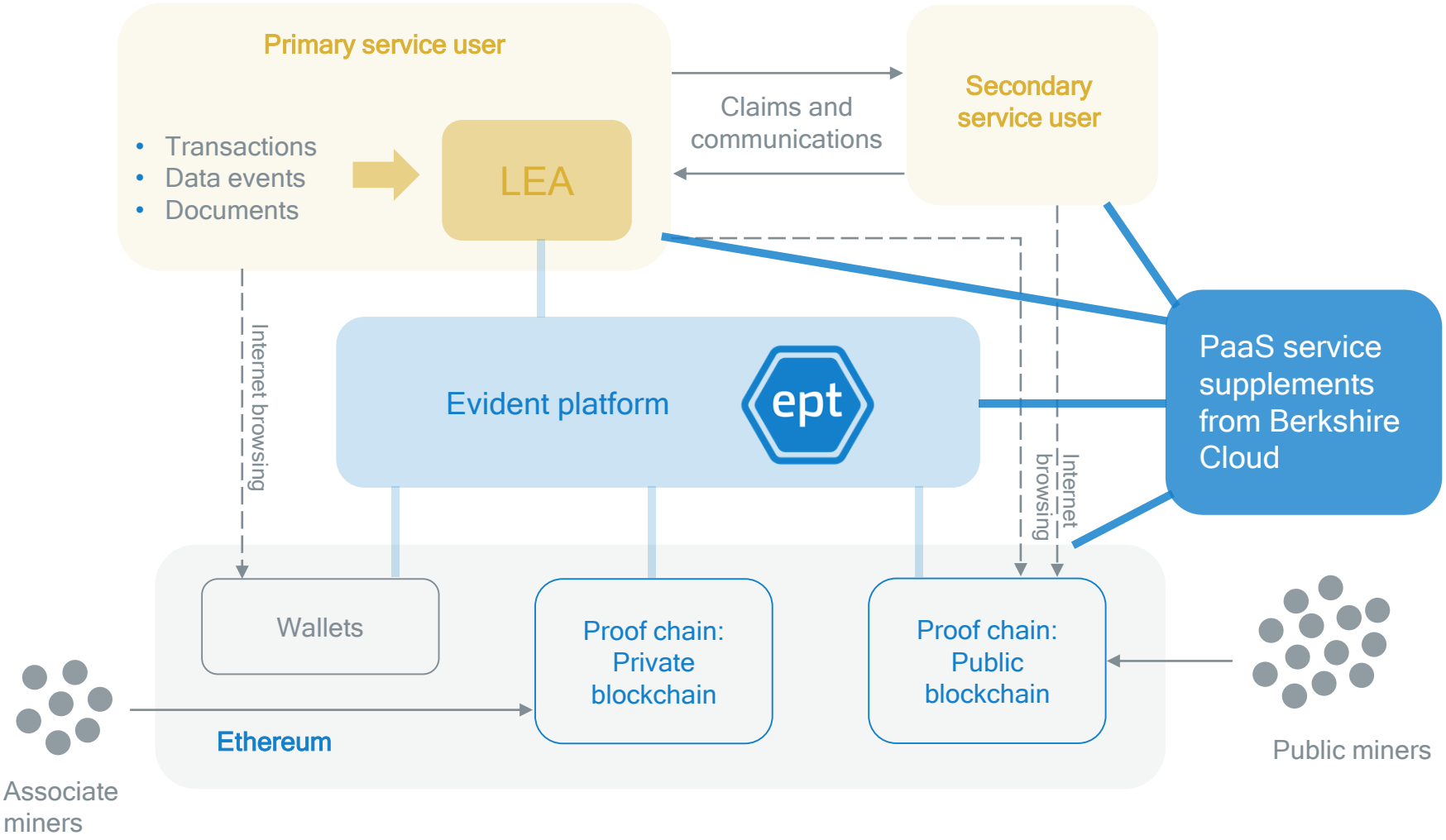
By always offering proof certificates on the public, as well as the private, blockchain

we achieve immutability

Simplified architecture



Simplified architecture:
Enhanced by Berkshire Cloud PaaS supplemental products



Glossary

Batch identifier: Seals and their meta-data are put on the public blockchain in batches. This saves operating mining expenses. In order to maintain a quick link to the unbatched seals on the private blockchain a batch ID is included in each receipt. It is assumed that all the seals associated with a single dispatch are kept in the same batch

Dispatch: A transmission of data from the LEA. Always sending a set of evidence data.

Evidence data record: A set of data collected into KeyName/value pairs that is deemed to be potential evidence in some future warrant or rebuttal. It typically concerns things, events and providence.

Immutable proof chain: This is a general term characterising the evident service. It is an informal expression of the feature that evidence seals that verify actual evidence are held in a temporal chain that is immutable in order and content.

Local Evident Agent (LEA): A software element, middleware, that joins the primary service user's IT system to the Evident service. Its primary purpose is to send dispatches into the service over the Internet. It may also be interfaced into the primary service user's database with bespoke business rules for identifying and preparing data to be sent as evidence in a dispatch. How it is designed and constructed is outside the scope of this paper.

Primary Service User (PSU): An organisation that uses the service. They will have a unique service identifier, a service agreement with the service provider, and responsibilities under that agreement.

Proof Certificate: The result of executing a proof request. It shows completeness, or otherwise, of pertinent evidence data and the correctness of submitted evidence documents.

Proof Certificate Request: A request by a primary or secondary service user for the service to provide a proof certificate in regard to identified aspects of evidence data. Usually it is accompanied by the identities of the required seals, pertinent metadata, evidence data documents and temporal constraints.

PSUXRef: A unique reference code meaningful to the PSU. It is constructed to give context to dispatch data.

.

Receipt: Proof that the seal associated with a particular evidence key, with a particular PSUXRef received by the service on a particular dispatch has been saved on the blockchains.

RCID: A systemwide unique identifier for every issued receipt

SAID: Service Agreement unique ID. An identifier uniquely identifying a particular service agreement with a particular PSU.

Seal: A hash encoded (e.g. 256 or 512 digit SHA-3) version of the value field of a KeyName/Value pair in the evidence data. Appended to this is meta data of the dispatch and the KeyName.

Secondary Service User: An organisation with the time-limited permission and enablement of a primary service user to generate proof certificates.

Service Agreement: An agreement between the primary service user and the service provider which defines the service utility and warranty obligations on the service provider and the responsibility obligations on the primary service user.

SHA-3: Secure Hash Algorithm 3 is a cryptographic hash function. It is based on the competition winning Keccak algorithm. Like SHA-2 which it supersedes it allows a digital record of any size to be uniquely summarised by a short digital 'digest' of fixed length.

Temporal Constraint: A set of time rules and conditions for filtering, ordering and selection of seals in the production of a particular Proof Certificate.

Token (EVT): A Token is: (a) A value in ERC20 format for transacting in Ethereum *wallets*. (b) A promissory note related to seal receipts and Proof Certificates. When a receipt is sent a fixed fraction of a Token is passed into the seal owner's wallet. The actual fraction is a matter for operational control but let us designate it as f. When a Proof Certificate is requested it must be accompanied by an assignment of Tokens. If s seals are involved in a required Proof Certificate then s*f Tokens will be taken from the owner's wallet.

Virtual Immutability: The immutability of data in blocks on a public blockchain asymptotically approaches total immutability as the number of independent public miners increases. Whilst to all practical purposes immutability is strongly assured it would be more correct to talk of virtual immutability.