STONEBLOCK

The Future of e-Government is Now

Technical Sheet

The Use Case

Digital registration of government-issued documents
Stoneblock is a blockchain-based digital registry, securing the key criteria of the documents issued by a government to citizens using strong cryptograhy and distributing the documents using a peer-to-peer distributed ledger.

By ensuring the integrity of the documents using a blockchain, Stoneblock provides a simple and straightforward mechanism for guaranteeing that documents have not been tampered with, are attributable to the citizen and cannot be repudiated, while providing a platform for making that data open to others in the government and economy (while remaining under the control of the citizen and adhering to local regulations on data privacy).

Stoneblock can be used, for example, to store a citizen's birth certificate and other life-event certificates, social security records, immigration records and naturalisation events, and criminal records - in a single data view. Stoneblock can be used to record land titles, health records, tax payments and refunds, driver's license and vehicle registration, and votes cast in public ballots. Stoneblock's 'general' nature makes it a capable vehicle to move from existing federated database infrastructure and the e-government services that use them, to the robust, distributed, and secure blockchain architecture.

Whole-of-government ready
Stoneblock can be used across multiple levels of government and across multiple portfolios of government (subject to the legislation and regulations of the respective jurisdiction).

Complete chain of attribution
Stoneblock enables a complete chain of attribution for how documents are authorised by the government and issued to a citizen. Documents issued by the government are signed using a hardware-based key. Citizens sign their documents using their mobile device. Information is immediately private to the citizen and under their full control, whilst the government agency and officers remain an irrefutable party to the issuance of the document.

Perpetual data store with migration tools
Stoneblock provides a perpetual data store, capable of outlasting the lifespan of a citizen and therefore ideal for the nature of government. To migrate legacy data stored in traditional systems of federated database, a secure application programming interface (API) is exposed by Stoneblock to allow existing e-government services and systems to make requests to store and retrieve information from the Stoneblock blockchain. This effectively provides a straightforward pathway to migrate from traditional centralised digital registry services to a distributed one.

Built upon strong identity
In the case a jurisdiction has no existing identity scheme for citizens, Stoneblock provides one. An important precondition for use of Stoneblock is, an identity scheme must exist, in order to preserve the complete attribution of all digital documents it stores.

How Does It Work?

Key concepts in a Stoneblock ecosystem
The key entities in a Stoneblock ecosystem are: (a) government *agencies*, (b) government *officers*, (c) public *citizens*, and (d) *document types*. To maintain a full chain of attribution over all data in Stoneblock, government agencies are setup at the highest level by the country's Cabinet of Ministers, who in turn is instantiated by the Prime Minister. These government agencies represent the statutory bodies responsible for issuance of particular document types.

Once government agencies are instantiated and head officers nominated, those head officers setup the other respective officers in the agency - these will be the people authorised to sign government issued documents on behalf of the state. This method of delegation with attribution keeps the chain of attribution in tact through the executive branch of government.

Key storage
Being a fully-permissioned ecosystem means that at all times a user of Stoneblock is clearly and legally identifiable by their private-public keypair. Government officers store their private keys on a heirarchical deterministic (HD) hardware wallet with mnemonic passphrase recovery, compliant with BIP-0032/39, and must be used to sign all document workflows they are responsible for issuing on the platform. Citizens store their private keys within the Stoneblock Android mobile appplication.

Architecture

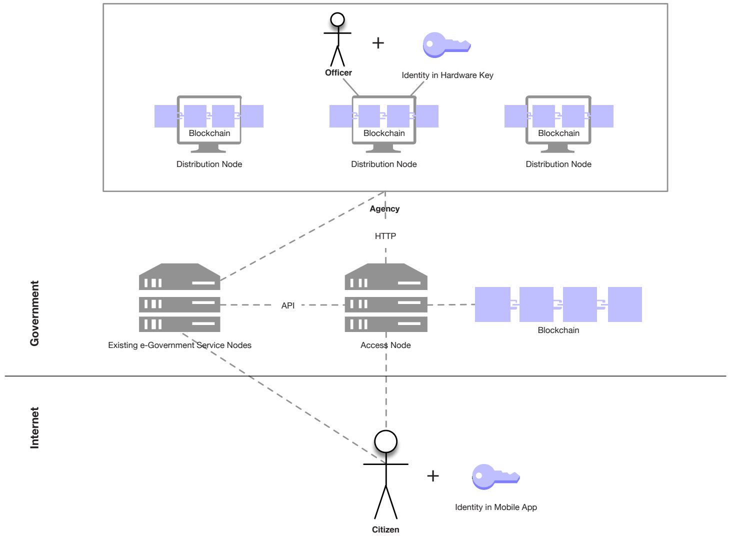
Stoneblock comprises a number of software and hardware components: (i) *distribution* nodes; (ii) an *access* node; (iii) a browser-based application; (iv) an Android mobile application; and (v) a HD hardware wallet.

The main component of the Stoneblock ecosystem is a modified implementaton of the Ethereum Foundation's Ethereum node software based on the Go source code (1.7.0 stable release), configured to run a private blockchain.

The middleware or access node comprises a RESTFUL API written in Node.js and is used to marshall requests to access the private Ethereum blockchain, from the browser-based Stoneblock application and citizen's mobile application. This component sits aside existing e-government web services infrastructure.

The browser-based application runs on each of the government officer computers within an agency, communicating with the private Ethereum blockchain via requests made of the access node, and providing the compute power to validate transactions being processed by the Stoneblock ecosystem.

Business logic for indiviudal government document types is securely and transparently implemented as 'smart contracts' written in Ethereum's Solidity (version 0.4.0) language and stored on the blockchain.



The Android mobile application is made available to citizens to generate their self-sovereign identity (a public-private key pair), and then using the application, verify and sign documents issued by the government and directed to the citizen. Once signed by the citizen on the mobile device, the documents are registered on the blockchain and a view of that document stored in the mobile application for the citizen to refer to and present to other interested parties during the course of transactions that involve government-issued document.

Contact Us

Neocapita is a privately--owned firm incorporated in Estonia with offices in Vienna, Austria and Bucharest, Romania. Connect with us via email: info@neocapita.com, to learn more about Stoneblock and to arrange a demonstration.

Visit us on the web: neocapita.com.

NEOCAPITA