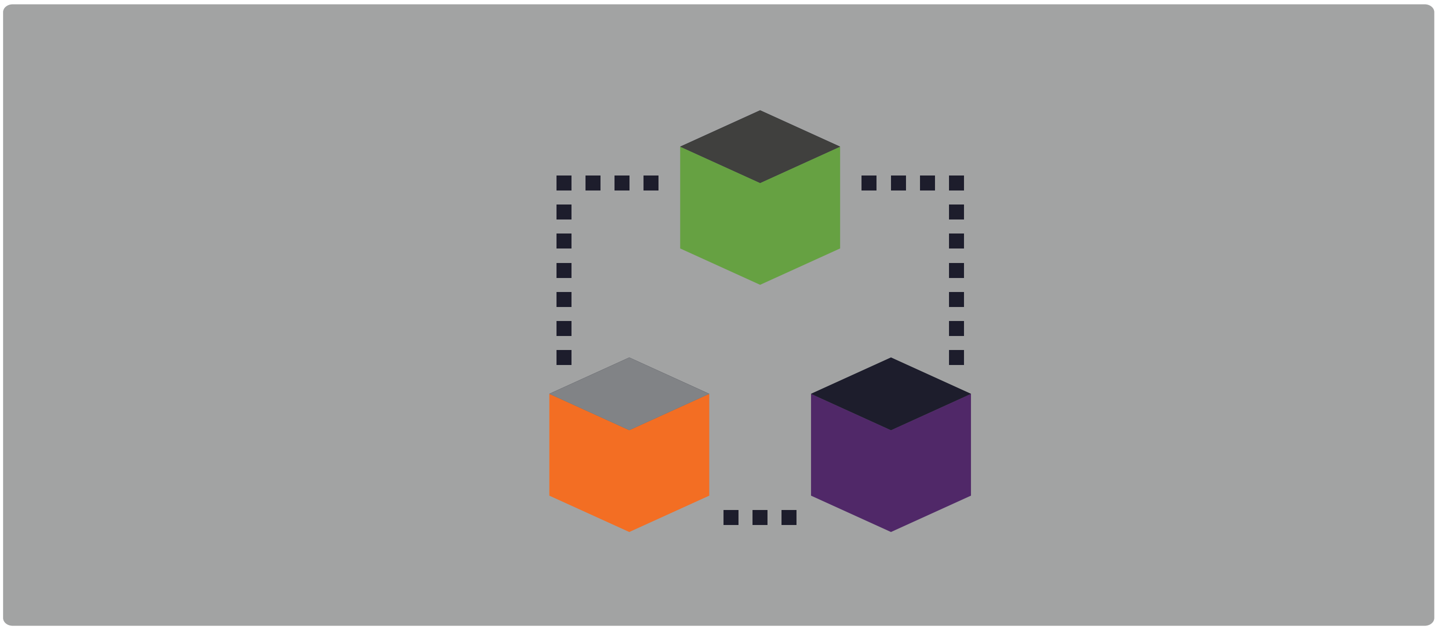
WHITEPAPER

Identity based eSignatures for Blockchain transactions

Combining the power of legal non-repudiation with transaction immutability



INTRODUCTION

Blockchain has been a buzzword for a last couple of years arising out of the hype from Bitcoin. No doubt, the technology is promising as it allows for trust less-consensus between multiple parties based on peer-peer networking and secure hashes that cannot be altered by design. While there have been debates about Blockchain implementation (Public vs Private vs Protected), the fundamental question remains and given Bitcoin's legacy of driving anonymity, Blockchain based Smart Contracts and Cryptocurrencies in general suffer from the same misunderstanding – how does one validate Identities? What happens if Private Keys are compromised? Will it be legal?

This Whitepaper suggests an approach based on existing Digital infrastructure available as part of India Stack – eKYC, eSign where a digital KYC and digital signature can be used to sign transactions on a Block thereby resulting in legal validity, non-repudiation and transaction immutability

THE CHALLENGE

As Governments embark on the Digital Transformation journey, increasingly Blockchain is part of conversations for providing immediate consensus, real time information sharing and smart contracts which can trigger payments based on preset conditions. While a lot of this is still conceptual, practical implementations have largely been driven on two technologies – Ethereum and Hyperledger.

But in order for this technology to succeed, the biggest challenge is around identity verification and ability to prove ownership in the digital world. Social Identities are restrictive and subject to fraud. Regulators look for identities that are more trustworthy – Federated Government Id's, Bank Id's.

Also, the fact that in the current system, lost identities are recoverable. We can always a recover a stolen/lost Bank card while in Blockchain, if a private key is lost, access to assets on the corresponding Blockchain is lost forever.

If a malicious party gains access to keys, they can transfer assets to their account. Although transactions are registered on a Blockchain, there is no association of the Blockchain to a trusted identity. While anonymity is a strength of the technology, ability to marry it with verifiable identities and ensuring restricted access is what will drive Blockchain's adoption in the future.

SOLUTION

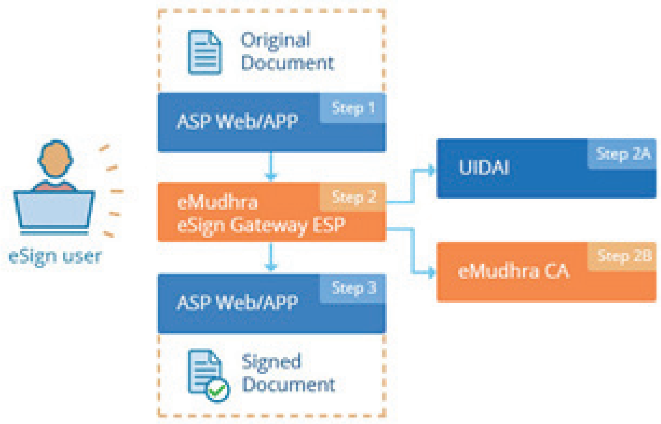
In India, AADHAAR (National ID) is issued to 1.3bn residents. A stack built of top of this allows of digital KYC retrieval and server side digital signatures issued by trust service provider like eMudhra under a regulated architecture.

These digital signatures are generated for each transaction requiring biometric/mobile authentication for each transaction using the federated identity AADHAAR. After every transaction private keys are destroyed. This architecture is legally valid under the Information Technology Act giving sanctity to the use of Digital Signatures.

Extending this approach to Blockchain, as a Trust Service Provider eMudhra's approach is to leverage Federated identity combined with server side one time digital signatures to sign transactions on a Block. This results in a more secure system where identities are verified, transactions are traceable and transaction records are immutable.

So far, while a lot of projects are within specific domains such as Banking where identity verification is part of customer onboarding , such an architecture can cut across industries and be even used for cross border trade with mutual recognition of digital signatures in place where two parties need to rely on intermediaries for identity verification.

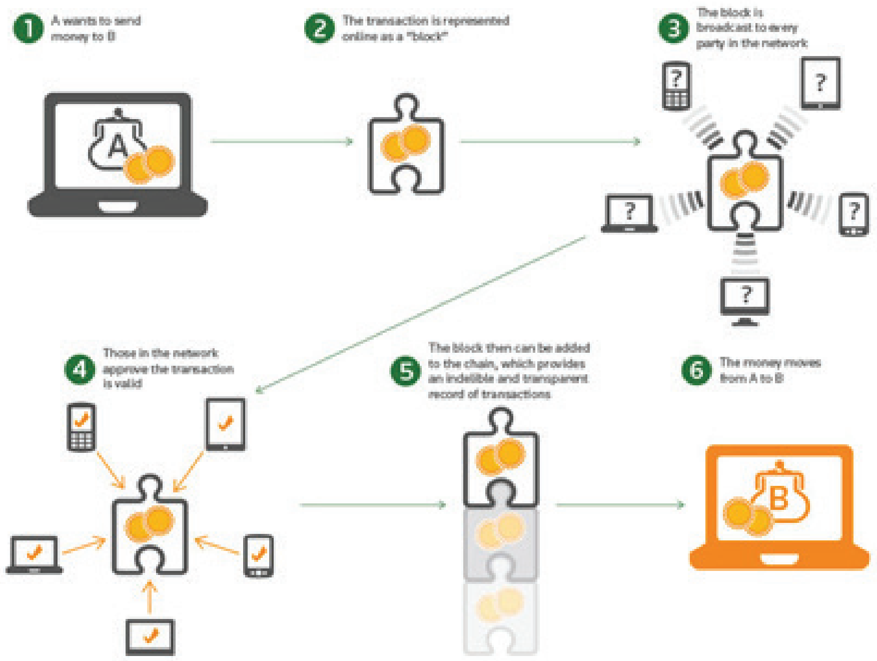
One would argue that this places dependence on a Trust Service Provider to manage keys but can a Blockchain other than Bitcoin exist without trusted parties? Will such a concept gain acceptance among regulators for large scale public use? These are questions that will get answered over the course of time as Blockchain evolves.



FACTS

- 90% Top Banks in US and Europe are experimenting with permissioned Blockchain
- Banks a cost reduction of upto 33% by using Blockchain
- Blockchain market is expected to be worth USD 20bn by 2024

AN ILLUSTRATIVE WORKFLOW


1 A wants to send money to B
2 The transaction is represented online as a "block"
3 The block is broadcast to every party in the network
?
4 Those in the network approve the transaction is valid
5 The block then can be added to the chain, which provides an indelible and transparent record of transactions
6 The money moves from A to B
A
B

ABOUT THE AUTHOR

Mr.Kaushik brings 12 years of experience in the technology domain currently driving growth and positioning of eMudhra as a Senior Vice President. businesses. Prior to this, he has worked at Hedge Funds and Financial Institutions driving algo trading, portfolio management using technology

ABOUT EMUDHRA

eMudhra Limited is a Certifying Authority licensed by Controller of Certifying Authorities, under Government of India. eMudhra operates under the guidelines set by Information Technology Act. With more than one million certificates issued, eMudhra caters to all kinds of subscribers who use Digital Certificates for Income Tax, MCA (ROC), Tenders, Foreign Trade, Banking, Railways and many other needs.