JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Comprehensive Study on Asymmetric Cryptography Signatures and Smart Contract

[1] Dr. R. NAVEEN KUMAR ,

[1] Asst Professor , Department of Computer Science ,

Sri Krishna Adithya College of Arts and Science, Coimbatore.

Email: [1]naveenkumarr@skacas.ac.in.,

ABSTRACT

Digital signatures are a restrained technique is used to validate the secrete document without any tampering. The hand-written signatures and Digital signature are both rely on the fact that it is very hard to find two signatures with the same person. Nowadays People use public-key cryptography to compute digital signatures by connecting something unique with another person's signature. Sometimes this digital signature called an electronic signature used for acknowledging online transactions. These signatures are commonly used for financial transactions, online transactions, software distribution, and in some common cases these signs are used for security purposes. The digital signatures are using different algorithms and procedures for cryptocurrency and other applications. This paper performs security analysis and the understanding of Digital Signature.

Keyword : Digital Signature , Smart contract , Distributed ledger and Cryptographic keys

I . INTRODUCTION

A digital signature is a measurement technique used to validate the authenticity and integrity of a message, software or digital document. A digital signature is equivalent to a handwritten signature or a stamped seal. A digital signature offers inherent security and has intended to solve the problem of tampering and personification in digital communication. It provides assurances of evidence of origin, identity and status of electronic document, transaction or message and also can acknowledge informed consent by the signer[1].

In countries like United States, digital signatures are considered as legally binding in the same way as traditional document signatures. Digital signatures are an electronic document that is used to identify the person who is transmitting the data. A valid digital signature gives a clients reason to believe that the message was created by a claimed sender and the sender cannot deny having sent the message and the message was not altered in transit[2].

II . How digital signature work

Digital signature is based on public-key cryptography which is also known as asymmetric cryptography. Digital signatures employ asymmetric cryptography which is also known as public-key cryptography (PKI). The PKI uses public and private keys to encrypt and decrypt data. The keys are of large numbers that have been paired together but the keys are not identical. One key in the pair can be shared with everyone, it is called a public key. The other key in the pair is kept secret which is called a private key. Using a public key

algorithm such as RSA, a person can generate two keys that are mathematically linked with each other: one private key and one public key[3].

RSA Algorithm : The RSA Signature is a deterministic digital signature scheme that provides message recovery.

For the RSA public-key encryption scheme,

the message space M and the ciphertext space C are Zn= {0, 1, 2, ... , n-1}.

Key-Generation In RSA public-key cryptosystems each user 1.

Generates two large distinct random primes p and q, 2.

Computes n = pq and Φ = (p-1)(q-1) 3.

Selects a random integer e,1 < e < Φ, such that gcd(e,Φ) = 1 4.

Computes the unique integer d,1 < d < Φ,

such that ed ≡1 mod Φ Now the public key of Alice is (n,e) and the private key is d.

Signature Generation To sign a message m Є M, Alice 1.

identifies m with a number ~ m in Zn through a map R : M → Zn. 2.

computes the signature s = ~ md mod n

Digital signatures work through public-key cryptography's two mutually authenticating cryptographic keys. The person who is creating the digital signature uses his own private key to encrypt signature related data. The only way to decrypt the data is with the signer's public key. This is the process of authenticating digital signatures[4]. This technology requires all the parties to trust on the individual creating the signature has been able to keep their own private key secret. If some other person accesses the signer's private key, the party could create fraudulent digital signatures in the name of the private key holder. Public key cryptography system where you have two keys namely public key (Pu) and private key (Pr). The person will give out the public key to the entire world and the person will keep the private key themselves.

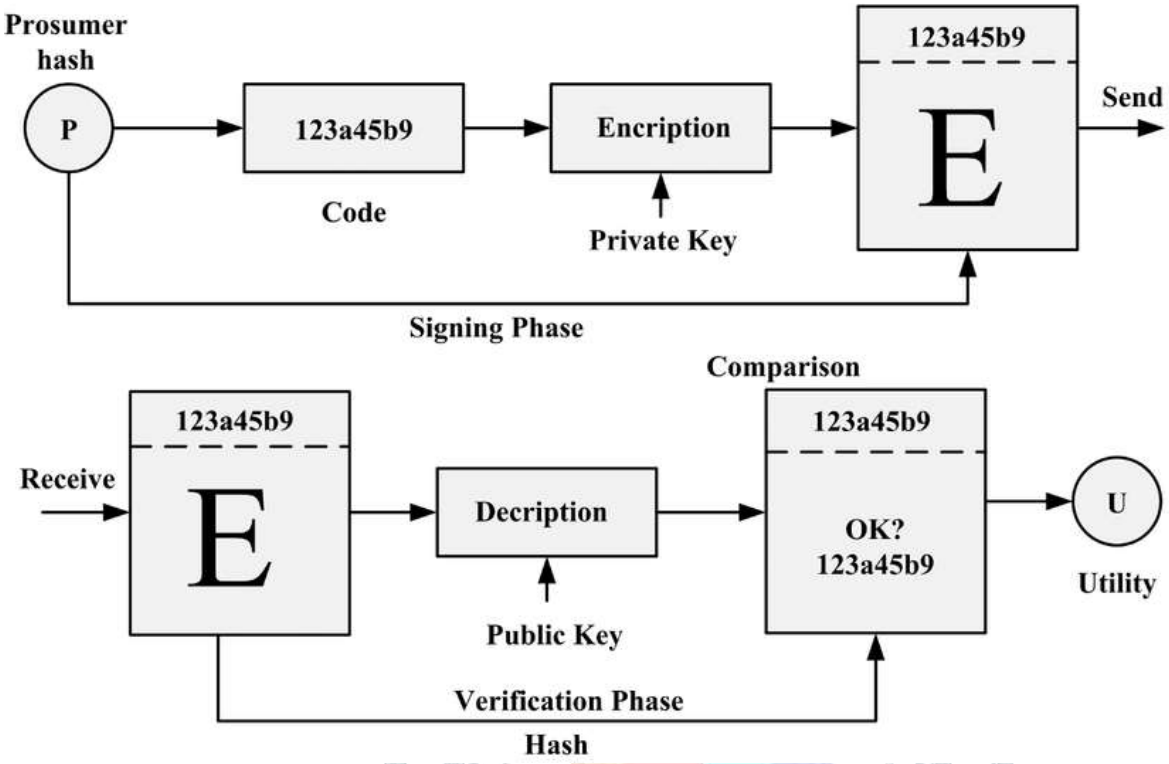
For example, your Etherem address is a public key and your private key is stored in a browser or mobile or hardware wallet. We can consider a public key like a bank account number, for someone to send you money (Ether), they just need to know your account address. However, only you can access the funds in your account because you are the only one who knows your private key, which is similar to your bank account password[7].

III . Process of digital signature

The first step in the digital signature is to generate the hash of the data. After the person generates the data, it will produce a digital signature. Once the digital signature is produced, the public key will be sent to the recipient. Once the receiver receives, the receiver will check the value has been generated by the sender. The final process is to regenerate the hash value from the data and the receiver will match it with the hash sent by the sender.

Practical applications of digital signature:

A digital signature is widely being used during these pandemic days. The various practical applications of digital signature are, it is used in software programs, which need to establish a secure connection over an insecure network like the internet. Users and systems need to be certain that a public key is authentic, that it belongs to the person or entity claimed, and that it has not been tampered with or replaced by a third party.



As shown above Zahid Ullah in his Smart Grid Block-Chain (BC) Conceptual Framework he had insisted that the public key verification phase is used to protect the descriptive data from the receiver, this shows that the encryption data is sent to receiver using public key through single phase with a secured verification phase[11].A digital signature is widely used by The United States Government Printing Office publishes versions of the budget, public and private laws, and bills with digital signatures. It can reduce the time to close the contracts that require many parties to validate and sign them.

Digital signatures can be used for B2B communication and transactions, that can validate the source and can be sent to only the intended party without any middle man. A digital signature is widely used to send and receive encrypted emails, that are digitally signed and secured. It is also used to carry out secure online transactions because the signature cannot be known by any others other than the sender and receiver.
And it also helps to identify the persons who are taking place in online transactions. Digital signatures are widely used to apply tenders, efiling with Register of Companies, filing of income tax returns, and other relevant applications. A digital signature is also used in various documents like word, excel, and PDF documents to sign and validate the text written in them.

IV . SMART CONTRACT

A smart contract is a transaction protocol that is intended to automatically execute, control, or document legally relevant events and actions according to the terms of a contract or an agreement. The objectives of smart contracts are the reduction of need in trusted intermediaries, arbitrations and enforcement, costs, fraud losses, as well as the reduction of malicious and accidental exceptions. Since a smart contract is a self-executing contract with the terms of the agreement between buyer and seller being directly written into lines of code.

Traditionally the code agreements contain the decentralized blockchain network around the distributed technology. The code controls the execution and gives the details of the transaction. Smart contracts trusted transactions had permitted the agreements holders to carry out the disparate, without the need for a central authority, legal system, or external enforcement mechanism. The virtual currency called “Bit Gold” in 1988, defined smart contracts as computerized transaction protocols that executed the terms of a contract. He wanted to extend the functionally of electronic transaction methods, such as POS (point of sale), to the digital realm. Smart contracts are a type of Ethereum account. where they can they can send transactions over the network. However, they are not controlled by a user, instead, they are deployed to the network and run as

programmed. All the client's accounts can directly interact with a smart contract while submitting the transaction details for executing a function defined on the smart contract. Smart contracts can define rules, as a regular contract and automatically enforce them via the code.

This automation tool works independently without any human interpretation. Each client has their own contract that contains some code that spells out the conditions of the agreement, so two parties can complete their transaction on their own without costly third parties.

This also gets rid of some of the busywork involved in drafting contracts because the system is autonomous, and since the system is decentralized and verified by a series of nodes, there is no chance of fraud or system failure. Smart contract in the blockchain: Smart contracts on blockchain can do is streamline this complex process that involves several intermediaries because of a lack of trust among participants in the transaction. With your identity stored on a blockchain, lenders can quickly make decisions about credit[10]. Then, a smart contract would be created between your bank, the dealer, and the lender so that once the funds have been released to the dealer, the dealer can hold the booked item after paying the balance repayment amount as per the agreed terms. The transfer of ownership would be automatic as the transaction gets recorded to a blockchain, is shared among the participants, and can be checked at any time.

As shown above How do smart contracts work: Smart contracts work by cryptography code on blockchain units. The group of computers executes the actions releasing funds to the appropriate parties, registering a home, sending notifications, issuing a ticket when predetermined conditions have been met and verified. The blockchain is then updated when the transaction is completed. For example, here we take a supply chain example. If a client wants to buy something from a seller, so he puts money in an escrow account. Seller will use Shipper x to deliver the product to the buyer when the buyer receives the item, the money in escrow will

be released to seller and shipper x. if the buyer doesn't receive the shipment by date, the money in escrow will be returned.

When this transaction is executed, manufacturer G is notified to create another of the items that were sold to increase supply. All this is done automatically. The advantages of a smart contract: The well-begin of smart contracts go from clients to clients with blockchain. Smart contracts are digital and automated, Because of using automation, there is no need for spending more time on processing paperwork or correcting the errors that are often written into documents that have been filed manually. Computer coding and encoding are too accurate than the legalese than traditional contracts. Smart contracts impulsive execute transactions follow certain rules and the encrypted records of those transactions are shared to the clients across the limit. Blockchain records are encrypted and the makes them very hard to hack. Smart contracts eliminate the intermediates because participants can trust the transparent data and the technology to execute the transaction.

Smart contract in the blockchain: Cryptographic signatures are a fundamental building block of blockchains. Transactions are signed with the private keys corresponding allowing the transactions senders to be linked to their account. Without this feature, the block chain's bookkeeping would simply not work. Digital signatures are also often verified directly in smart contracts deployed on Ethereum, in order to allow one or more verifies to authorize actions by submitting signatures created off-chain (or even signatures generated by another smart contract).This is used in different voting systems, in order to submit various signatures together or delegate others this had been followed by the authorization party.

Real-life examples of smart contracts: Here we can take a look at some real-world examples to see a smart contract in action. They are supply chain and product tracking, insurance policies and payments, stock trading, trade finance, records, property ownership, mortgages, medical research, voting, peer-to-peer transactions, product development, stock taking, and intellectual property rights.

V. CONCLUSION

This paper has discussed the Digital signature and smart contract Techniques along with Distributed ledger network using the Private and Public Blockchain concept and its future projects. In this study, it is evident that the construction of Digital signature technology is used for improvising and securing the fraudulent challenges using smart contracts without considering the third parties.

VI . REFERENCE

[1] Julio Lopez and Ricardo Dahab, "An overview of elliptic curve cryptography", May 2000.

[2] El-Kassar, A.N., M.Rizk, N.Mirza and Y.Awad,2001.ElGamal public-key cryptosystem in the domain of Gaussian integers.Intl.J.Appl.Math.,7:405-412.

[3] Haraty, R., O. Otrok and A.N.El-Kassar,2004.A comparative study of ElGamal based cryptographic algorithm. Proc. Sixth Intl. Conf. Enterprise Information Systems (ICEIS 2004),3:79-84.

[4] Rivest,R.L.,Shamir,A.,and Adleman,L.," A method of obtaining Digital Signatures and Public key cryptosystems",Comm.ACM,21,1978.

[5] Nathanson, Melvyn, B.,Elementary Methods in Number Theory, Springer, 2000.

[6] William Stallings, Cryptography and Network Security: Principles and practice.Tsinghua press,2002,253-299.

[7] Dr. R. Naveen Kumar "The Future Impact of Blockchain Technology using Decentralization Networks" (IJARESM), ISSN: 2455-6211 Volume 8, Issue 9, September-2020, Impact Factor: 4.597.

[8] Rabin, M.O., Probabilistic algorithms. In Algorithms and Complexity, J. F.Traub,Ed., Academic Press,New York,1976,pp.21-40.

[9] A. Jurisic, A. Menezes, "Elliptic Curves and Cryptography", 2003,http://www.certicom.com/whitepapers.

[10] Dr. R. Naveen kumar "The Persistence of Blockchain Technology using Digital Signature and Hash Functions" (IJARESM), ISSN: 2455-6211 Volume 8, Issue 11, November-2020, Impact Factor: 7.429.

[11] Zahid Ullah , Geev Mokryani , B. Khan " Smart Grid Block-Chain (BC) Conceptual Framework: Bi-Directional Models for Renewable Energy District and Utility, Dec 2019.