IJARASEM

ISSN: 2395-7852

# International Journal of Advanced Research in Arts, Science, Engineering & Management

Volume 10, Issue 2, March 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 6.551

International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 2, March 2023 |

# Atomic Swap of Cryptocurrencies Using HTLC

**Prof. Pandu Naik, Suchithra Nayak, Neha Shiramagond, Rakshith Nayak, Vikas Shettigar**

Dept of Computer Science, Yenepoya Institute of Technology, Moodbidri, Mangalore, India

**ABSTRACT**: Atomic swapping is a technology that makes it possible to trade two different cryptocurrencies without the use of a centralized exchange. By locking up the assets until the terms of the trade are satisfied, smart contracts are used in the procedure to facilitate the exchange. One of the most widely used cryptocurrencies is Bitcoin, and another is Ether. Recently, atomic exchanging between these two has gained popularity. Customers can do this without an intermediary or exchange platform, exchanging one currency for another. Atomic swapping is a procedure where two parties agree to exchange assets, define the parameters of the deal in a smart contract, and then carry out the trade via a decentralized protocol.

**KEYWORDS**: Blockchain, Decentralized, Centralized, Bitcoin, Ethereum, Smart Contract, SHA256, HTLC.

## I.INTRODUCTION

Blockchain is a technology that was created by fusing several different methods. Under the alias Santoshi Nakamoto, computer programmers created it in January of 2009. In order to give everyone equal access to economic prospects without having to worry about being seized or using an intermediary, as well as to stop the scam being used in this transaction, it was introduced. It is essentially described as a digital, decentralized ledger of all cryptocurrency transactions. These days, cryptocurrencies are decentralized virtual currencies that are based on the internet. Blockchain runs on a decentralized computer network. It records every transaction that involves money. Simply said, it is a peer-to-peer network that enables value transfers without the need for intermediaries.

Digital or virtual currencies that use cryptography to protect transactions are known as cryptocurrencies. The Secure Hash Algorithm (SHA-256), which reduces communications to 256 bits, is one of the most popular mincing techniques utilised by numerous cryptocurrencies. The verification of digital signatures, limiting the production of new units, and attesting asset transfers are all regularly carried out using this algorithm. They are distributed and constantly run on the blockchain distributed census technology, which keeps track of all transactions across a network of computers. In 2009, the most widely used cryptocurrency, Bitcoin, was created. Since then, a number of new cryptocurrencies—often referred to as "altcoins"—such as Ethereum, Ripple, Litecoin, and numerous others have emerged.

### Brief about blockchain and swapping

How does a trasaction get into the blockchain?

The following parties are involved in a series of processes that lead to a transaction being added to a blockchain:

• Sender: The person who wants to send digital assets, such as cryptocurrency, from their wallet, sometimes referred to as the sender or the party starting the transaction.

• Recipient: The person who will receive the digital assets after the transaction, also known as the recipient or the user.

• Transaction Creation: When sending digital assets, the sender must first define the transaction's specifics, including the quantity to be sent, the recipient's address, and any transaction costs.

• Block Propagation: The mined/validated block is subsequently transmitted to more nodes for additional verification via the network.

Confirmation: The transaction is regarded as confirmed after the block is uploaded to the blockchain. Depending on the blockchain network and desired level of security, a different number of confirmations may be necessary. A higher level of security is often indicated by more confirmations.

• On a public blockchain, a consensus is reached before a transaction is added to the chain. This indicates that the majority of "nodes" (or computers) in the network must agree for a transaction to be valid. Rewards are used to encourage the network's computer owners to verify transactions.

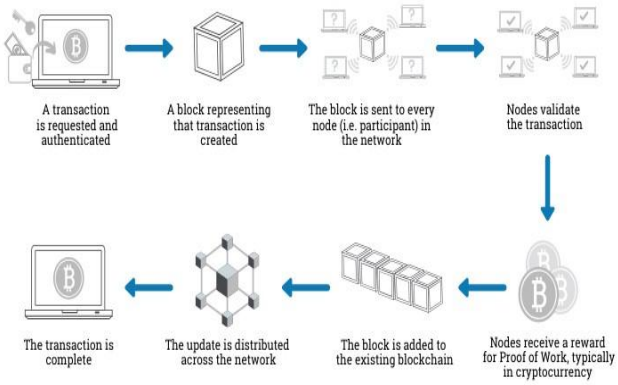



Fig1: Transaction into blockchain

It's important to remember that depending on the blockchain network and its consensus algorithm, the specifics and stages of how a transaction enters a blockchain may differ. To validate a block, for instance, miners in Proof of Work (PoW)-based blockchains like Bitcoin compete to solve a challenging mathematical puzzle, but in Proof of Stake (PoS)-based blockchains like Ethereum 2.0, validators are selected based on their stake in the network. The majority of blockchain networks, however, continue to use a same general notion for transaction origination, propagation, verification, consensus, and confirmation.

What is an atomic swap?

Atomic swaps have built-in features that must be completed by both participants in order for a transaction to be finalized. Atomic swaps use a type of contract known as a Hashed Time Lock Contract (HTLC), which imposes specific trading requirements and a deadline that must be satisfied. A transaction from Bitcoin to an Ethereum address is possible, as well. Atomic swaps, a peer-to-peer way of swapping cryptocurrency across two independent blockchains without the need for any third-party intervention, are necessary to securely execute a trade across blockchains.

By using the scenario in which Alice and Bob have decided to trade her 25 ETH for his 1.5 BTC. Before sending his BTC, Bob must first construct a smart contract address. To access the funds, a special cryptographic key that is generated by the contract must be used. The smart contract also creates an encrypted (hashed) version of the key based on this key, which Bob gives to Alice. Alice can confirm that Bob has indeed deposited his money by using the hashed key. She won't be able to withdraw the money, though, until all of the swap's requirements have been satisfied. Based on the hashed key, Alice must create her own contract address where she can send ETH. The password Alice needs to access Bob's deposit is automatically disclosed whenever Bob claims the money Alice locked up in the smart contract.

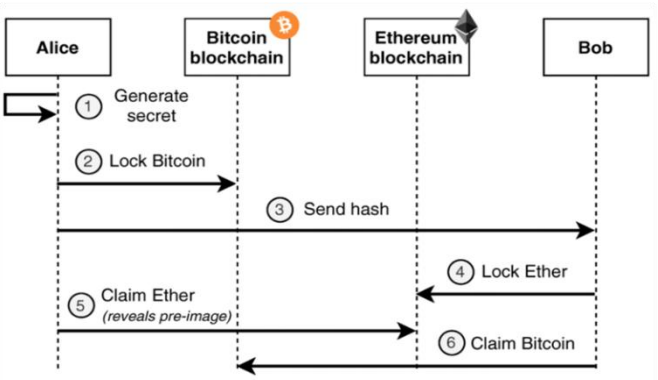



*Fig2: Exchange between Alice and Bob*

Is swapping of cryptocurrencies taxable?

According to trading custom, there is a tax if the transaction is made with the Revenue Service (RS) in mind, which serves as a centralized network. A decentralized switching does not include an exchange tax. A decentralized network is one in which there are no trusted third parties and where it is not necessary to know the opponent in order to complete a transaction.

Centralized and decentralized exchange

Centralized bitcoin exchanges serve as a middleman between buyers and sellers, as the name implies. The majority of cryptocurrency transactions happen on centralized exchanges because they provide more reliability. On centralized exchanges, users can buy and sell cryptocurrencies for fiat money like the US dollar or digital assets like BTC and ETH. They operate as reliable brokers and frequently as custodians in transactions, preserving and protecting your money.

Decentralized exchange, as contrast to centralized exchange, is non-centralized and involves multiple parties managing the assets. Smart contracts and decentralized apps are used to automate transactions and trades as opposed to conventional centralized exchanges. This approach is much safer since, as long as the smart contract is made properly, there can be no security breach. Decentralization is the practice of spreading control, authority, and decision-making across a number of organizations or people as opposed to concentrating it in a single body.In numerous fields, decentralization has many benefits, such as; Greater transparency is encouraged by decentralization because decisions and actions are spread out among various entities. This makes it more difficult for any one organization to manipulate or control information, resulting in more open and transparent decision-making. Decentralization promotes higher efficiency and agility by enabling quicker decision-making. Local decision-makers don't need to rely on the lengthy and cumbersome procedures associated with centralized decision-making, which allows them to respond more swiftly to changing circumstances and make judgements that are best suited to their particular context.Local communities are empowered by decentralization because it gives them more autonomy over their own issues. It gives individuals the chance to take part in decision-making, express their concerns, and influence programs and policies that have a direct impact on them. Better outcomes for local communities and more inclusive and representative governance may result from this.

Innovation and creativity: By promoting a diversity of viewpoints and ideas, decentralization promotes innovation and creativity. Distributed decision-making promotes experimentation and fosters many methods to problem-solving, which results in more creative solutions. Resilience and robustness: By minimizing single points of failure, decentralization can improve a system's resilience and robustness. If a single node or entity fails in centralized systems, it may have far-reaching effects. The impact of failures is reduced and the system as a whole is more resilient in a decentralized system, nevertheless.

## II.PREDICAMENTS

Smart contract

A smart contract is a distributed program that executes business logic in response to events. A smart contract's execution can result in a money exchange, the delivery of services, the release of digitally secured content, or other types of data modification, including changing a land title's name. Smart contracts can also be used to enforce privacy protection, for example by allowing the selective release of data that is privacy-protected in order to fulfil a specific request. A number of architectures can be used to develop, distribute, maintain, and update the software that support smart contracts. They can be used as part of a blockchain and stored on various digital exchanges and payment systems, including those that accept bitcoin and other cryptocurrencies. Smart contracts, despite their name, are not enforceable contracts. Their primary duty is to programmatically carry out business logic, which has been programmed into them to carry out different tasks, processes, or transactions in response to a specific set of conditions. To connect this execution to legally enforceable agreements between parties, legal action must be done. Many technologies are thought to consider it to be a trustworthy transaction. It is possible to create, distribute, maintain, and update smart contracts.

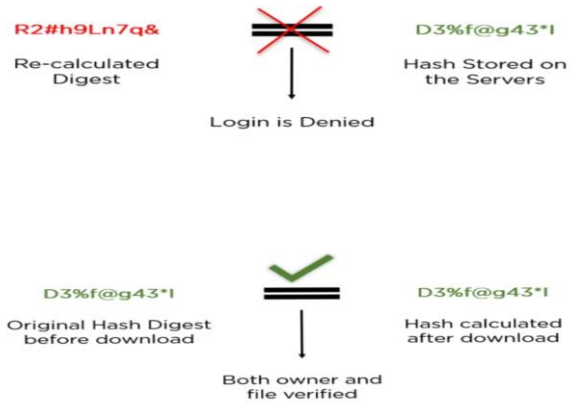
**HASHING**

Raw data is scrubbed by hashing until it can no longer be reconstructed in its original form. It takes a set of data and passes it through a function to numerically modify the plaintext. A hash value is the output of the hash function, which is also known as a result or digest. The hash function is used to convert the plaintext into the proper hash digest. Your

digest should never give you access to the original plaintext because they are designed to be irreversible. Hash functions always yield the same result when the input is left unchanged, regardless of how often they are employed.

There are two primary applications of hashing:

- Password Hashes: Prior to being kept on a website server, most servers translate user passwords into a hash value. For validation, it makes a comparison between the hash value recalculated after login and the one saved in the database.
- Integrity Verification: When uploading the file to a website, it also delivered the file's hash as a bundle. It can recalculate the hash and compare it when a user downloads it to ensure data integrity.




HTLC(Hash Timelock Contract)

• A transactional agreement called a "Hashed TimeLock Contract" (HTLC) is used in the cryptocurrency sector to provide conditional payments. In essence, it is a payment where the recipient or beneficiary must acknowledge receiving the funds prior to a set date or predefined period.
• The recipient must acknowledge this payment by providing a cryptographic proof of payment; otherwise, they lose the right to do so and the payee receives their money back.So in the crypto world, an HTLC essentially implements time-bound transactions. The recipient will not receive any money, and the transaction is void, if they fail to produce cryptographic proof of receipt of payment within a set window of time.

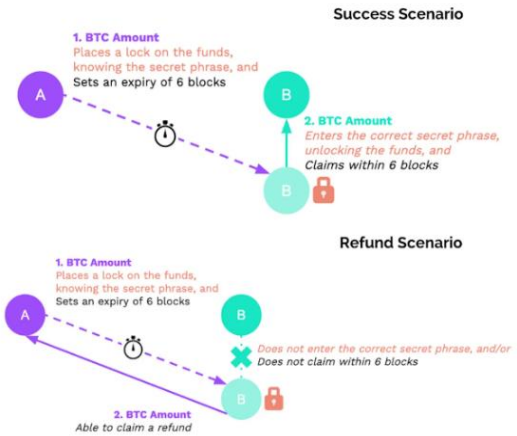



*Fig3: Success and Refund scenario of HTLC*

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 2, March 2023 |

## III.GRIEFING ATTACK IN TIMELOCKED CONTRACTS

When an attacker purposefully delays the execution of a transaction or the release of funds by taking advantage of the time lock mechanism, this is referred to as a griefing attack in a timelocked contract. Certain actions in a timelocked contract can only be carried out after a predetermined amount of time has passed. For instance, a smart contract may be set up to release payments to a beneficiary after a predetermined period of time. This is done to make sure the receiver only gets the money after fulfilling specific requirements. However, a griefing attack can happen when a perpetrator tries to stop the money from being released.In order to postpone the execution of the release transaction until after the time lock has expired, the attacker could, for instance, generate a transaction that cancels the release of funds or submit several transactions with little amounts of gas. The recipient, who may have relied on the prompt release of funds to fulfil their responsibilities, may suffer severe harm as a result.It is crucial to carefully construct the contract to take into account potential attack vectors in order to prevent griefing assaults in timelocked contracts. Implementing extra security measures, such as multi-factor authentication or multi-party clearance for certain actions, may be necessary to achieve this. Security professionals should also evaluate the contract to find and fix any potential weaknesses.

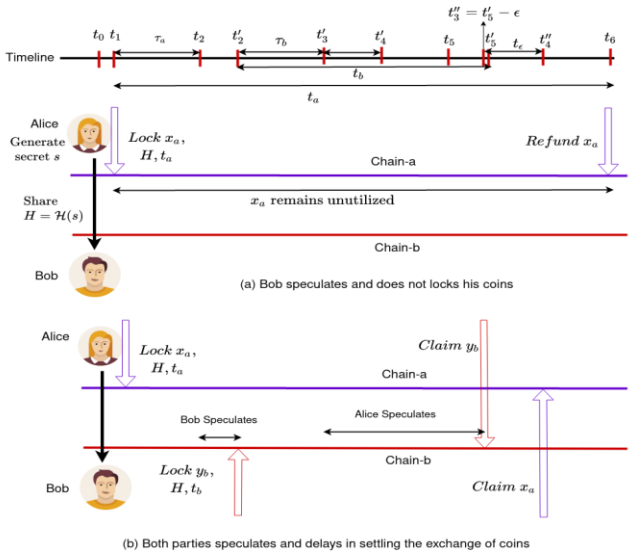



Fig 4: Coins remain unutilized in HTLC-based atomic swap

due to (a) Bob speculates the deal and does not lock his coins and (b) Bob speculates, finds favourable for locking his coins delaying, and Alice speculates to finds favourable for claiming the coins from Bob

Let's take a look at a mathematical illustration of a timelocked contract that mandates a user wait a certain amount of time before being able to withdraw money. According to the contract, the user can only take money after waiting T blocks have passed. If an attacker decides to employ the time lock method to stop the user from withdrawing the funds, this could result in a griefing assault. Let's say that after T blocks have passed, the user creates a transaction to withdraw the money. The attacker might then utilize small amounts of gas to make several transactions to delay the user's withdrawal transaction's execution until after the time lock has passed. Let's take an example where the customer requests to withdraw 10 ether after waiting T = 5 blocks to demonstrate this. After 5 blocks have passed, the user creates a transaction to withdraw the money. To prevent the user's withdrawal transaction from being processed, the attacker instead makes numerous smaller-sized transactions. Let's say the attacker sends 10 transactions, each containing 0.1 ether, and they all reach the contract before the waiting period expires. These transactions take longer to complete than the user's withdrawal transaction because each one requires a little amount of petrol. The user cannot withdraw the money because their transaction is postponed until after the time lock has passed. In this case, the attacker used the time lock technique to successfully stop the user from withdrawing the money. The timelocked contract should be evaluated by security professionals to discover and fix any potential flaws and should be structured to account for potential attack vectors, such as implementing multi-factor authentication or setting gas limitations.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 2, March 2023 |

## IV.RESULTS

The outcomes of cryptocurrency atomic swapping using hash time locked contracts (HTLC) have been highly encouraging. Atomic Swapping is a more secure and trustless trading alternative since it enables two parties to trade various cryptocurrencies without the need for a centralized exchange or a reliable third party. The possibility of counterparty fraud is eliminated, which is one of the key advantages of adopting HTLC for atomic swaps. It makes sure that both parties keep their end of the agreement before the transaction is finished by using cryptographic methods and time-locks. This offers a high level of protection and does away with the requirement for a reliable middleman. Atomic Swapping is also a lot quicker and more effective than conventional trading techniques. Since a centralized exchange is not required, the transaction can be finished almost immediately, which is crucial for traders who must act quickly to seize market opportunities. Atomic Swapping also has the enormous benefit of enabling cross-chain trading, which frees traders from the requirement to use a centralized exchange that only supports the currencies they intend to trade. It also makes it simpler for traders to diversify their portfolios by creating fresh trading possibilities. Atomic Swapping is still a relatively new idea, thus there might be obstacles in the way of its general acceptance, it's crucial to remember. The requirement for standardized protocols, user adoption, and regulatory barriers are a few of these difficulties. However, Atomic Swapping with HTLC is a fascinating development in the world of cryptocurrency trading due to the potential advantages.

## V.RELATED WORKS

At the time of [TN1(2013)], the HTLC-based atomic swap was first proposed. However, the design is unjust and is expected to be open to griefing attacks. Later, Hao et al. (Han et al., 2019) recommended using premium to defend against griefing attacks. However, the protocol made the assumption that only Alice could be at fault in a two-party scenario where Alice wants to exchange money with Bob. Bob is not obligated to lock premium, so she must. Even though Alice starts the swap on time in an option-based swap in the American way, Bob receives the premium. If Alice doesn't answer within the agreed-upon time frame, Bob receives the premium in a currency exchange-based atomic swap. The protocol is unfair because Bob can also sorrow. The construction requires the addition of an additional opcode, hence it cannot be implemented with Bitcoin scripts.Both parties involved in currency exchange have written similar works that discuss locking premium [Xue and Herlihy(2021)]. The protocol, however, has issues with misaligned premiums, lacks fairness, and is incompatible with Bitcoin scripts. Additionally, the authors bootstrapped the premium, locking small valued premiums first and increasing the premium amount with each iteration. As a result, there are more communication rounds, more contracts are created for each iteration, and the lock time is greater than in [TN1(2013)]; also, griefing on the locked-up premium is feasible [Nadahalli et al.(2022)].A protocol that is trouble-free and appropriate for use with Bitcoin scripts has been proposed by Nadahalli et al. [Nadahalli et al.(2022)]. The protocol is effective in terms of both the volume of transactions and the maximum amount of time that funds can be locked. The issue of mismatched premium does, however, exist. Due to the coupling of the premium and the principal amount, the model lacks flexibility and cannot be applied to multi-party atomic swap settings involving more than two blockchains [Herlihy(2018)]. Our suggested protocol fixes several of these issues. However, compared to [Han et al.(2019)] and [Nadahalli et al.(2022)], there is a constant factor increase in the overhead of the transaction and communication round.

## VI.CONCLUSION

The use of atomic swapping with hash time locked contracts (HTLC), a potent method that permits secure and trustless cryptocurrency exchange between two parties without the need for a centralised exchange or a reliable third party, is explained in this paper. By utilizing cryptographic methods and time-locks, it makes sure that both parties keep their half of the contract. Atomic Swapping is the perfect solution for peer-to-peer cryptocurrency trading since it offers a high level of security and removes the possibility of counterparty fraud. It may help blockchain technology become more widely used in the financial sector and completely change how individuals trade cryptocurrencies. However, it's important to note that Atomic Swapping is still a relatively new concept and there may be challenges to its widespread adoption, including the need for standardized protocols, user adoption, and regulatory hurdles. Nevertheless, the potential benefits of Atomic Swapping using HTLC make it an exciting development in the world of cryptocurrency trading. Atomic Swapping is vast and exciting. As the adoption of cryptocurrencies and blockchain technology continues to grow, the need for secure and trustless methods of trading cryptocurrencies becomes more crucial. Atomic Swapping using Hash Time Locked Contracts (HTLC) has the potential to address this need and revolutionize the way people trade cryptocurrencies.

| ISSN: 2395-7852 | www.ijarasem.com | Impact Factor: 6.551 |Bimonthly, Peer Reviewed & Referred Journal|

| Volume 10, Issue 2, March 2023 |

**ACKNOWLEDGEMENT**

We thank Mr. Pandu Naik, Assistant Professor at Yenepoya Institute of Technology, for his initial valuable comments onthis work.

**REFERENCES**

[1] [Nadahalli et al.(2022)] Tejaswi Nadahalli, Majid Khabbazian, and RogerWattenhofer. 2022. Grief-free Atomic Swaps. In 2022 IEEE InternationalConference on Blockchain and Cryptocurrency (ICBC).

[2] [TN1(2013)] 2013. TierNolan. Technical Report.

https://github.com/TierNolan.

[3] [Eizinger et al.(2021)] Thomas Eizinger, Philipp Hoenisch, and Lucas Sorianodel Pino. 2021. Open problems in cross-chain protocols.arXiv:2101.12412 [cs.CR]

[4] [Han et al.(2019)] Runchao Han, Haoyu Lin, and Jiangshan Yu. 2019. On the optionality and fairness of Atomic Swaps. In Proceedings of the 1st ACM Conference on Advances in Financial Technologies. 62–75.

[5] Lys, Léonard, Arthur Micoulet, and Maria Potop-Butucaru. "Atomic swapping bitcoins and ethers." *2019 38th Symposium on Reliable Distributed Systems (SRDS)*. IEEE, 2019.

[6] Hoenisch, Philipp, et al. "LightSwap: An Atomic Swap Does Not Require Timeouts at both Blockchains." *Data* Privacy Management, Cryptocurrencies and Blockchain Technology: ESORICS 2022 International Workshops, DPM 2022 and CBT 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers. Cham: Springer International Publishing, 2023

[7] Mazumdar, Subhra. "Towards faster settlement in HTLC-based Cross-Chain Atomic Swaps." arXiv preprint arXiv:2211.15804 (2022).

[8] Malavolta, Giulio, et al. "Concurrency and privacy with payment-channel networks." Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. 2017.

[9] [Moreno-Sanchez et al.(2020)] Pedro Moreno-Sanchez, Arthur Blue, Duc Viet Le, Sarang Noether, Brandon Goodell, and Aniket Kate. 2020. DLSAG: Non-interactive Refund Transactions for Interoperable Payment Channels in Monero. In Financial Cryptography and Data Security - 24th International Conference, FC 2020 (Lecture Notes in Computer Science, Vol. 12059), Joseph Bonneau and Nadia Heninger (Eds.). Springer, 325–345.

[10][Thyagarajan et al.(2022)] S. Thyagarajan, G. Malavolta, and P. Moreno-Sanchez. 2022. Universal Atomic Swaps: Secure Exchange of CoinsAcross All Blockchains. In 2022 2022 IEEE Symposium on Securityand Privacy (SP) (SP). IEEE Computer Society, Los Alamitos, CA,USA, 1083–1100.

[11] Masuzawa, Toshimitsu. "Atomic Cross-Chain Swaps with Improved Space and Local Time Complexity." Stabilization, Safety, and Security of Distributed Systems: 21st International Symposium, SSS 2019, Pisa, Italy, October 22–25, 2019, Proceedings. Vol. 11914. Springer Nature, 2019.


# International Journal of Advanced Research in Arts, Science, Engineering & Management (IJARASEM)

| Mobile No: +91-9940572462 | Whatsapp: +91-9940572462 | ijarasem@gmail.com |

www.ijarasem.com