Cryptography (BITS F463)
Programming Assignment 2 (Term Project) 2024

Weightage 15%

1 Introduction

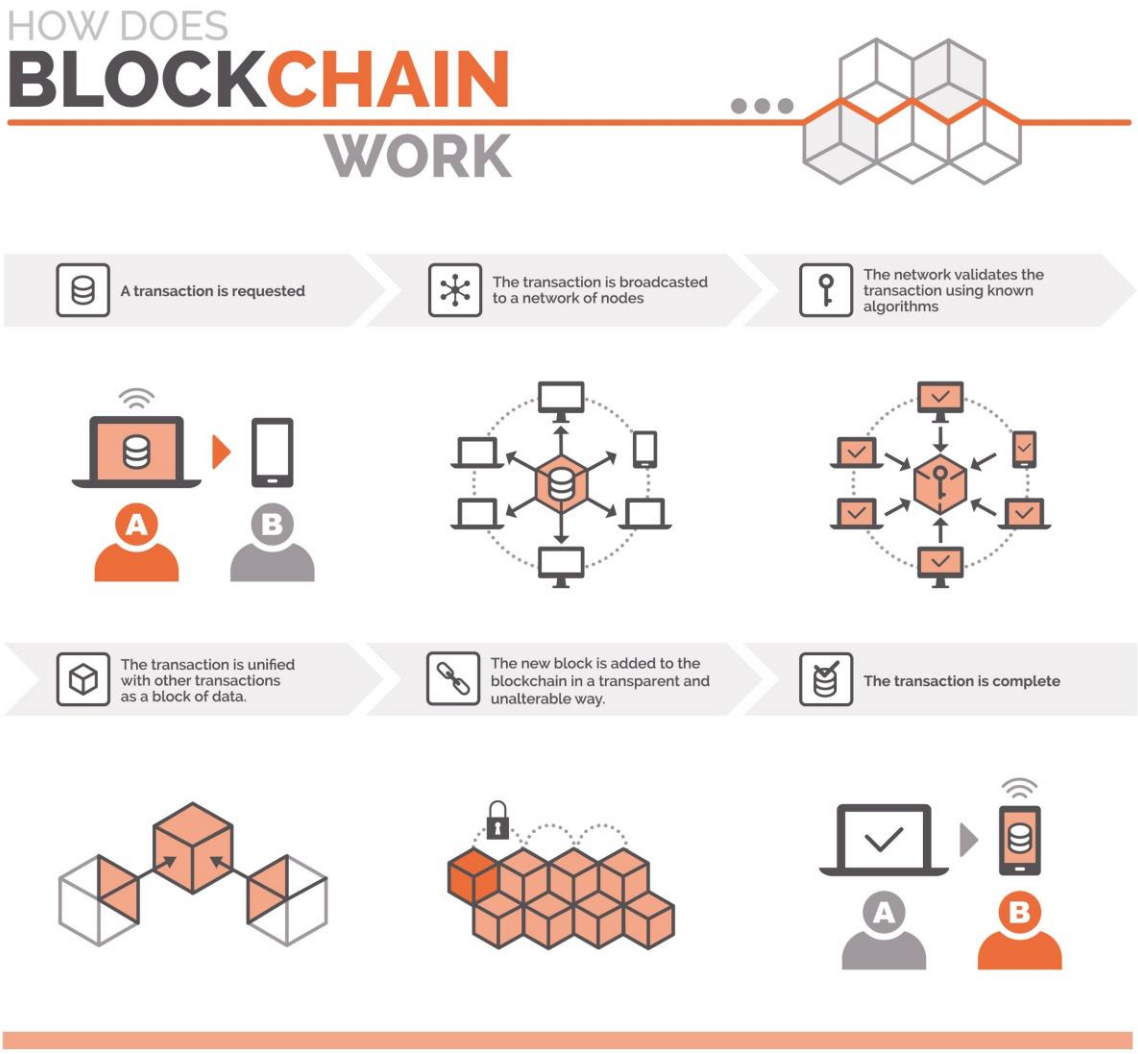
There has been a lot of buzz around blockchains in recent years, ever since Bitcoin became popular. Blockchain technology offers new tools for authentication and authorization in the digital world that preclude the need for many centralized administrators. The scope of this project is to help you get accustomed to blockchain development. You are required to identify one problem that you feel can be solved with the help of blockchain and then implement your solution. You can work in teams which you have already formed earlier.

2.1 Blockchain Fundamentals

A blockchain is a digital and distributed ledger of transactions, recorded and replicated in real-time across a network of computers or nodes. Every transaction must be cryptographically validated via a consensus mechanism executed by the nodes before being permanently added as a new “block” at the end of the “chain.” There is no need for a central authority to approve the transaction, which is why blockchain is sometimes referred to as a peer-to-peer trustless mechanism.

Blockchain can be thought of as a linked list with each node containing multiple transactions. Each transaction has a hash that depends on the previous transaction's hash as well. So, we can see that the order of transactions is important. If we were to change one transaction somewhere, it would have a ripple effect and change the hash of all subsequent transactions. This is one of the reasons why blockchain is a powerful medium for storing transactions.

The placing of a transaction in a block is called a successful conclusion to a proof of work challenge, and is carried out by special nodes called miners. Proof of Work is a system that requires some work from the service requester, usually meaning processing time by a computer. Producing a proof of work is a random process with low probability, so normally a lot of trial and error is required for a valid proof of work to be generated. When it comes to Bitcoins, hash is what serves as a proof of work. Miners on a Blockchain are nodes that produce blocks by solving proof of work problems. If a miner produces a block that is approved by an electronic consensus of nodes then the miner is rewarded with coins. This essentially is the crux of blockchain. Proof of Work is what is keeping all transactions on the blockchain secure and protecting it from malicious attempts to alter these transactions.



This is just a high-level introduction. You are expected to dig deep and understand how the blockchain truly works. Different applications might implement it differently, but the core ideas remain the same.

2.2 Quick Introduction to HMAC

Challenge-Response Authentication with HMAC (Hash-based Message Authentication Code) can be implemented in a scenario where a user wants to prove their knowledge of a secret key without revealing the key itself.

Scenario:

In a secure messaging system, Alice wants to prove to Bob that she possesses a secret key without disclosing the key itself. They decide to use a Challenge-Response Authentication mechanism with HMAC. The scenario is as follows:

1) Alice generates a random challenge and sends it to Bob.
2) Bob, acting as a verifier, sends back a random bit (0 or 1) to Alice.
3) Alice creates an HMAC (using a secret key) of the challenge combined with the bit received from Bob.
4) Bob, with the knowledge of Alice's public key, verifies the HMAC to check if Alice knows the secret key without revealing the key itself.

As part of the assignment, you will implement this Challenge-Response Authentication with HMAC in your blockchain application. Decide on the appropriate number of rounds for the challenge-response exchanges.

Algorithm steps:

1) Alice generates a random challenge (generate_challenge()) and sends it to Bob.
2) Bob sends back a random bit (0 or 1).
3) Alice creates a response (create_response()) using HMAC with the challenge and the bit received from Bob.
4) Bob verifies the response (verify_response()) by recomputing the expected HMAC and comparing it with the received response.

Notes:

1) Choose a secure hash function and HMAC library for implementation.
2) Ensure that the implementation adheres to best practices for cryptographic protocols.

In your blockchain application, incorporate this Challenge-Response Authentication with HMAC for secure user authentication without revealing the secret key.

3. Deliverables

Stage 2 evaluation:

1. Every group should write the topic name in the group formation spreadsheet before 11.59 pm, March 17th, 2024.
Topic submission link: Problem statement sheet

2. A brief presentation (2-3 slides) on the chosen topic should be prepared and presented during the stage 2 evaluation. Please note that stage 2 assessment carries 5% weightage. The slides should mention the problem that you have identified and how it can be solved through the use of blockchain. The presentation should also include details of all team members.

Stage 3 evaluation:

1. You are free to code in any language but your solution must implement the following methods:

   -- createBlock()
   -- verifyTransaction()
   -- mineBlock() or something equivalent for proof of work
   -- viewUser()

2. All transactions must be verified before they can be added to a block. As part of the verification process, you are required to use HMAC (as described in section 2.2) to verify at least one attribute.

3. viewUser() should list all (successful) transactions against the user.

4. For your final submission, submit your source code & readme as a single .zip or .tar file in the final submission link given below. Please name your file as bitsf463_team99 (assuming your team number is 99. You can find your team number from the google sheet you filled earlier). The readme should contain a brief explanation of the project, steps to run the code, and the list of team members. The deadline for the same will be 11:59 PM 17th April 2024. The exact date and demo schedule will be intimated later. From a team, only one team member needs to do the submission.
Final Submission Link:
BITS F463 TERM PROJECT 2024 FINAL SUBMISSION

4. Further Reading

-- What A Blockchain Actually Is, Written In Blockchain
-- Bitcoin White Paper
-- How Do Bitcoin Transactions Work?
-- WTF is The Blockchain
-- Creating Your First Blockchain
-- Lectures & Slides on Cryptocurrency from Princeton