Literature Survey 2:

**Blockchain-Enabled Applications in Next-Generation Wireless Systems: Challenges and Opportunities**

The research issues addressing some of the challenges faced by blockchain-enabled wireless applications. As a potential solution, a wireless blockchain middleware architecture (BlockWare) is proposed, based on a blockchain middleware layer connecting wireless applications and underlying blockchain infrastructure. The blockchain workflow innovatively integrates and enable a system which can achieve advanced features such as decentralization, immutability, transparency, and security. BlockWare interact with underlying blockchain networks on behalf of wireless applications. The common functions provide extra intelligent services to wireless applications and lower their complexity and promote large-scale deployment of blockchain-based wireless applications.

Literature Survey 3:

**Adoption of Blockchain With 5G Networks for Industrial IoT: Recent Advances, Challenges, and Potential Solutions**

Blockchain and IIoT, enabled by 5G, is a viable option to fully explore the potential of contemporary industry. The main issue for Industry 5.0 is to enable massive data transmission while preserving high levels of security, transparency, and trustworthiness. 5G networks integrated with blockchain are capable to resolve these issues. It has many advantages such as Improved consensus mechanism, Higher throughput and low latency, Off- chain storage, Standardization of blockchain-enabled IIoT, Privacy protection. Through inherent characteristics such as decentralization, privacy, and transparency, blockchain offers the ability to overcome the shortcomings of resource-constrained IoT devices.

**Blockchain Architecture:**

Blockchain is a decentralized technique for storing and sharing information that a single party does not control. Its architecture is similar to a public accessible distributed database. The technical concept of its operation is selfevident: Blockchain comprises a group or series of blocks linked together by cryptographic strings of characters called ‘‘hash’’. The Genesis Block is the first block in the chain, and it allows us to start the chain by constructing and establishing the first hash. A cryptographic hash is a string formed by running it through a hash function, transforming it into another string. The number of characters in the hash remains constant regardless of the length of the encrypted string. Also even a single comma in a string can totally change the hash.

Block version: specifies which set of block validation criteria should be used.

• Merkle tree root hash: the sum of all transactions in the block’s hash value.

• Timestamp: current time as seconds in the universal time since January 1, 1970.

• nBits: target threshold of a valid block hash.

• Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation

• Parent block hash: a 256-bit hash value that points to the previous block.

The block’s body is then made up of a transaction counter and transactions. The maximum number of transactions a block can contain is determined by the block size and the size of each operation. The Blockchain’s cryptography is an asymmetric approach for verifying transaction authenticity.

**SMART CONTRACTS**

All complicated protocols and applications are built based on smart contracts. Smart contracts are small applications that are saved on a blockchain and operated in parallel by many validators. Typically, smart contracts are connected to the Blockchain in computer codes and recorded in the Blockchain after being propagated by the P2P network and validated by the nodes after signing by all parties. A smart contract has several pre-defined states and transition rules, scenarios that trigger contract execution (for example, when a specific event occurs), answers in a particular scenario, and so on. The Blockchain keeps track of smart contracts in real-time and executes them when special trigger conditions are satisfied.

**Consensus Algorithm:**

**Proof of Work (PoW):** This consensus algorithm is used to select a miner for the next block generation. Bitcoin uses this PoW consensus algorithm. The central idea behind this algorithm is to solve a complex mathematical puzzle and easily give out a solution. This mathematical puzzle requires a lot of computational power and thus, the node who solves the puzzle as soon as possible gets to mine the next block.

**Proof of Stake (PoS):** This is the most common alternative to PoW. In this type of consensus algorithm, instead of investing in expensive hardware to solve a complex puzzle, validators invest in the coins of the system by locking up some of their coins as stakes. After that, all the validators will start validating the blocks. Validators will validate blocks by placing a bet on them if they discover a block that they think can be added to the chain. Based on the actual blocks added in the Blockchain, all the validators get a reward proportionate to their bets, and their stake increase accordingly.

**Proof of Authority (POA):** In PoA, rights to generate new blocks are awarded to nodes that have proven their authority to do so. These nodes are referred to as **“Validators”** and they run software allowing them to put transactions in blocks. Process is automated and does not require validators to be constantly monitoring their computers but does require maintaining the computer uncompromised. PoA is suited for both private networks and public networks, like POA Network, where trust is distributed. PoA consensus algorithm leverages value of identities, which means that block validators are not staking coins but their own reputation instead. PoA is secured by trust on the identities selected.

**Decentralized Microservices:**

Web services’ principal purpose is to transmit data in an easy-to-understand manner. Web services come in two flavors: REST and SOAP. The most common type of web service is the REST technique. The HTTP protocol is used to consume REST (Representational state transfer), which manipulates services using the four methods POST, GET, PUT, and DELETE [27], [34]. SOAP (Simple Object Access Technology) is a protocol that enables decentralized and distributed XML communication between peers [35]. Input, output, and service parameters are all part of the web service setup. A SOAP service may be consumed using WSDL (Web Service Description Language), while a REST service can be consumed using WADL (Web Service Description Language) (Web Application Description Language).

**BLOCK OF SUB-LEDGER OPERATIONS:**

the TSLO Block (Trusted SubLedger Operations), is made up of the same elements as a traditional block, except for one feature: the grouping of operations or transactions, which changes the block’s structure.

• Block version

• Merkle tree root hash: the hash value of all the transactions in the block. The tree may have a new layer with the root node, the asset node.

• Timestamp

• nBits

• Nonce: There is no need for the nonce on the first stage, only in the case of implementing the PoW mechanism.

• Parent block hash

**Main Architecture: Trusted Sub-Ledger Operations and Decentralized Microservices:**

the existence of an ecosystem involving three businesses and their information systems. Each IS having three or more databases, either SQL or NoSQL, that act as data sources and targets for internal microservices representing each sub-ledger. In our schema, we have two microservices for each of our three ISs, which could be account payable and account receivable subledgers, respectively. Our operations will start from their SLs. Microservices 1 and 2 will be in charge of storing transactions on the database and then transmitting them to the DMST (Decentralized Microservices Tree) via gRPC messages. The DMST creates DSLs, decentralized sub-ledgers containing SLOs (Sub-Ledger Operations), which are not verified because they have not yet been submitted to the PoSaA to become TSLOs (Trusted Sub-Ledger Operation). The SLO encapsulates the conditions (by asset family or asset, more specifically) implemented on the microservices tree. Decentralized Sub-Ledgers are displayed as a pool of elements at the start of the leading Blockchain. We believe that every business needs at least one information system to concentrate its activities through modules (Purchase – Sale – Stock, and so on). Each module is linked to a sub-ledger that communicates with decentralized microservices using the gRPC protocol. Decentralized microservices are instances with two primary parts: the blockchain part, which contains the replication of the shared chain on a peer-to-peer network, and the part code, which is in charge of the impact code of our accounting concept: TRUSTED SUB-LEDGER OPERATION. The operation is sent from the sub-ledger to the decentralized microservice to insert the effect code and then to p2p for validation and blockchain chaining. Finally, the operation is retransmitted to the general ledger as a verified operation after it has been validated.

**Blockchain Wireless Applications:**

Many emerging wireless applications are based on unique requirements such as edge data processing, distributed trust, and automation, which can be provided and enabled by blockchain technology through decentralization, transaction accountability, and smart contract-based automation. 5GS capabilities for hosting blockchain middleware, emerges as an important issue to be addressed for applications integrating blockchain. Multiple parties use a permissioned blockchain network (e.g., Hyperledger Fabric) for better blockchain access control and governance.

**Wireless Blockchain Middleware Architecture:**

A wireless blockchain middleware architecture (BlockWare) is a layered (i.e., three-layer) architecture, with several new entities, each with different roles and functionalities, being introduced. Blockchain Client application (BCA) and Blockchain Client (BCC) could be hosted on the UE side, while Blockchain Function (BCF) and Blockchain Network Application (BNA) may be hosted on the communication infrastructure side. The top-most layer of BlockWare is the vertical (or vertical-specific) application layer and BCA and BNA reside on this layer. BCA and BNA conduct client-side and server-side application logic processing for specific vertical wireless applications, respectively. The middle layer of BlockWare is the middleware layer or blockchain application enablement layer. BCC and BCF reside on this layer. BCC acts as a service interface for a BCA to interact with blockchain services (exposed by BCFs). BCF provides blockchain as a service. BCF acts as glue and a middleware, providing blockchain capabilities as a service to BCAs/BNAs. First, BCF can encapsulate the capabilities of the underlying BCNs, independent of the associated blockchain system. Second, the BCF provides abstraction, translating the various operation requests sent from the BCAs or BNAs to the BCNs (e.g., to store a transaction onto a blockchain) to the specific commands/calls of the specific underlying blockchain systems. The bottom layer of BlockWare is the blockchain infrastructure layer, with underlying Blockchain Nodes (BCNs) residing on this layer. In various deployments the BCN may either be deployed within the communication infrastructure directly, such as a 3GPP system, or be deployed externally. Accordingly, the BCC and BCF residing on the middle layers need to interact with and manage the underlying BCN for usage of its blockchain-related resources.

**Future Scope:**

Next stage and vision will cover some enhancements to the current architecture then propose a concrete stable version for individual entities or corporations according to governmental standards and policies. We have many other projections concerning the implementation of this architecture by setting up a platform under a middleware that will be grafted to any information system, which gives us a new challenge of adaptability, and which constitutes work of theoretical and technical improvements of our approach.

**Conclusion:**

Advances in blockchain technology present opportunities for CPA auditors and assurance providers to grow, learn and exploit their proven ability to adapt to the needs of a rapidly changing corporate world. We have established a complete architecture that offers a solution to the challenges mentioned above, and we have illuminated the solution’s major components. We are sure that integrating our technique is a first step toward integrating blockchain technology into the financial auditing industry and that we can now move on to studying the developing limits of this union.