SCALABILITY AND PRIVACY CHALLENGES

From : Mastering Blockchain

By – Imran Bashir

www.packet.com

Blockchain Challenges

- At the top of the list these issues comes scalability and then privacy.
- Both of these are important limitations to address, especially as blockchains are envisioned to be used in privacy-demanding industries too.
- There are specific requirements around confidentiality of transactions in finance, law and health, whereas scalability is generally a concern where blockchains do not meet the adequate performance levels expected by the users.

Blockchain Challenges

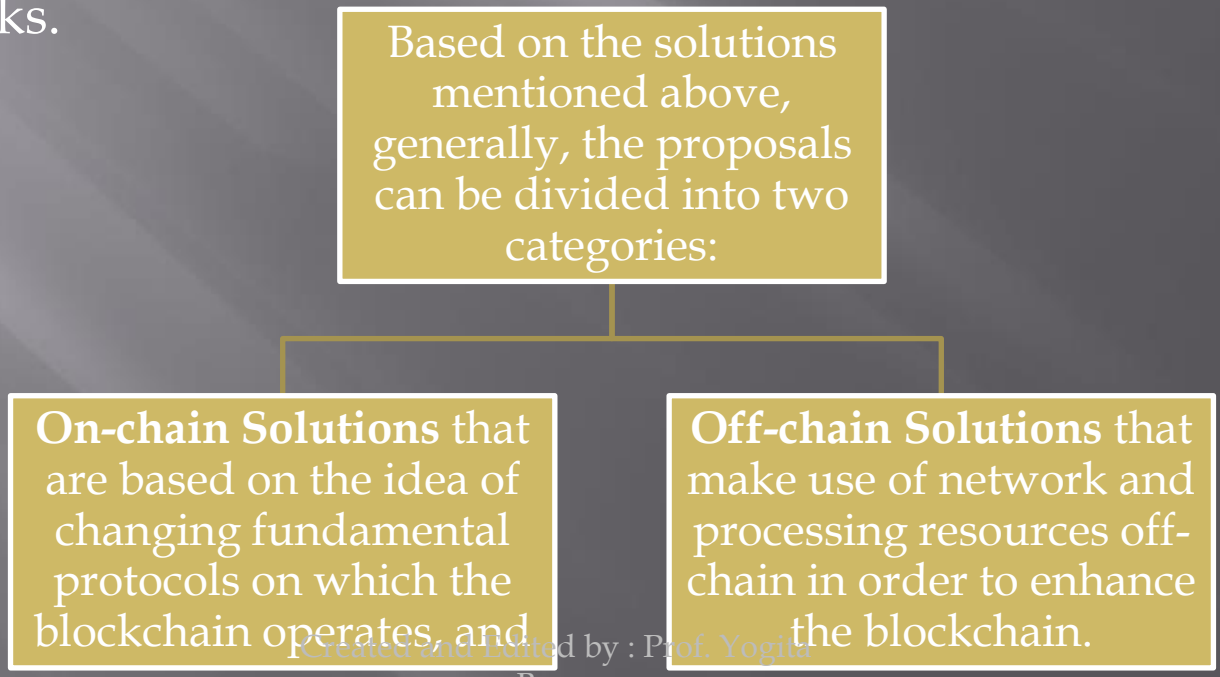
- These two issues are becoming inhibiting factors toward blockchain technology's wider acceptance.
- A review of currently proposed and ongoing research in these two specific areas will be presented in this chapter.
- In addition to privacy and security, other challenges include regulation, integration, adaptability, and security in general.
- Although, in bitcoin blockchain security is provably bulletproof and has stood the test of time, there still are some caveats that may allow security to be compromised to an extent in some subtle scenarios.
- Also, there are some reasonable security concerns in other blockchains, such as Ethereum, regarding smart contracts, denial of service attacks, and large attack surface.

Scalability

- This problem has been a focus of intense debate, rigorous research, and media attention for
- the last few years. This is the single most important problem that could mean the difference
- between wider adaptability of blockchains or limited private use only by consortiums. As a
- result of substantial research in this area, many solutions have been proposed, which we will discuss further.
- Fun reading :
  - https://en.bitcoin.it/wiki/Scalability

Proposed Solutions

- From a theoretical perspective, the general approach toward tackling the scalability issue generally revolves around protocol-level enhancements. For example, a commonly mentioned solution to bitcoin scalability is to increase its block size.
- Other proposals include off-chain solutions that offload certain processing to off-chain networks, for example, offchain state networks.



On Scaling Decentralized Blockchains

- Another approach to addressing limitations in blockchains has been recently proposed by *Miller* and others in their position paper *On Scaling Decentralized Blockchains*.
- In this paper, it is shown that a blockchain can be divided into various abstract layers called **planes**.
- Each plane is responsible for performing specific functions.
- These include the network plane, consensus plane, storage plane, view plane, and side plane.
- This abstraction allows bottlenecks and limitations to be addressed at each plane individually and in a structured
- manner.
- A brief overview of each layer is given below with some references to the bitcoin system.

On Scaling Decentralized Blockchains

- First the network plane is discussed.
- A key function of the network plane is transaction
- propagation.
- It has been identified in the mentioned paper that in bitcoin, this plane underutilizes the network bandwidth due to the way transaction validation is performed by a node before propagation and duplication of transaction propagation, first in the transaction broadcast phase, and then after mining in a block.
- It should be noted that this issue was addressed by **BIP 152** (**Compact Block Relay**).

On Scaling Decentralized Blockchains

- The second layer is called the consensus plane.
- This layer is responsible for mining and achieving consensus.
- Bottlenecks in this layer revolve around limitations in Proof of Work algorithms whereby increasing consensus speed and bandwidth results in compromising security of the network due to an increase in the number of forks.

On Scaling Decentralized Blockchains

- The storage plane is the third layer, which stores the ledger.
- Issues in this layer revolve around the need for each node to keep a copy of the entire ledger, which leads to certain inefficiencies, such as increased bandwidth and storage requirements.
- Bitcoin has a method available called pruning, which allows a node to operate without the need to download the full blockchain.
- This functionality has resulted in major improvements from a storage point of view.

On Scaling Decentralized Blockchains

- Next on the list is the view plane, which proposes an optimization.
- This is based on the proposal that bitcoin miners do not need the full blockchain to operate, and a view can be constructed out of the complete ledger as a representation of the entire state of the system, which is sufficient for miners to function.
- Implementation of views will eliminate the need for mining nodes to store the full blockchain.

On Scaling Decentralized Blockchains

- Finally, the side plane has been proposed by the authors of the above-mentioned research paper.
- This plane represents the idea of off-chain transactions whereby the concept of payment or transaction channels is used to offload the processing of transactions between participants, but is still backed by the main bitcoin blockchain.

On Scaling Decentralized Blockchains

- The above-mentioned model can be used to describe limitations and improvements in current blockchain designs in a structured manner.
- Also, there are several general strategies that have been proposed over the last few years which can address the limitations in current blockchain designs such as Ethereum and bitcoin.
- These approaches are also characterized and discussed individually in the following section.

Block size increase

- This is the most debated proposal for increasing blockchain performance (transaction processing throughput).
- Currently (till 2017), bitcoin can process only about three to seven transactions per second, which is a major inhibiting factor in adapting the bitcoin blockchain for processing micro-transactions.
- Block size in bitcoin is hardcoded to be 1 MB, but if block size is increased, it can hold more transactions and can result in faster confirmation time.
- There are several **Bitcoin Improvement Proposals** (**BIPs**) made in favor of block size increase. These include BIP 100, BIP 101, BIP 102, BIP 103, and BIP 109.

Block size increase

- In Ethereum, the block size is not limited by hardcoding; instead, it is controlled by gas limit.
- In theory, there is no limit on the size of a block in Ethereum because it's dependent on the amount of gas, which can increase over time.
- This is possible because miners are allowed to increase the gas limit for subsequent blocks if the limit has been reached in the previous block.

Block interval reduction

- Another proposal is to reduce the time between each block generation.
- The time between blocks can be decreased to achieve faster finalization of blocks but may result in less security due to the increased number of forks.
- Ethereum has achieved a block time of approximately 14 seconds and, at times, it can increase.
- This is a significant improvement from the bitcoin blockchain, which takes 10 minutes to generate a new block.

Block interval reduction

- In Ethereum, the issue of high orphaned blocks resulting from smaller times between blocks is mitigated by using the **Greedy Heaviest Observed Subtree** (**GHOST**) protocol whereby orphaned blocks (uncles) are also included in determining the valid chain.
- Once Ethereum moves to Proof of Stake, this will become irrelevant as no mining will be required and almost immediate finality of transactions can be achieved.

Invertible Bloom lookup tables

- This is another approach that has been proposed to reduce the amount of data required to be transferred between bitcoin nodes.
- **Invertible Bloom lookup tables (IBLTs)** were originally proposed by *Gavin Andresen*, and the key attraction in this approach is that it does not result in a hard fork of bitcoin if implemented.
- The key idea is based on the fact that there is no need to transfer all transactions between nodes; instead, only those that are not already available in the transaction pool of the synching node are transferred. This allows quicker transaction pool synchronization between nodes, thus increasing the overall scalability and speed of the bitcoin network.

Sharding

- Sharding is not a new technique and has been used in distributed databases for scalability such as MongoDB and MySQL.
- The key idea behind sharding is to split up the tasks into multiple chunks that are then processed by multiple nodes.
- This results in improved throughput and reduced storage requirements.
- In blockchains, a similar scheme is employed whereby the state of the network is partitioned into multiple shards.
- The state usually includes balances, code, nonce, and storage. Shards are loosely coupled partitions of a blockchain that run on the same network.
- There are a few challenges related to inter-shard communication and consensus on the history of each shard. This is an open area for research.

State channels

Lightning Network

- Suppose Cam buys a coffee regularly at Starbucks
- It is inefficient to use the main blockchain for small transactions
- The solution is to set up a multi-signature address that is shared by Cam and Starbucks

CNBC

BITCOIN

Starbucks' Howard Schultz: A 'trusted' digital currency is coming, but it won't be bitcoin

- "One or a few legitimate" cryptocurrencies are coming, but bitcoin is not one of them, according to the Starbucks executive chairman.

https://www.cnbc.com/2018/01/26/starbucks-schultz-a-digital-currency-is-coming-but-wont-be-bitcoin.html

State channels working

State channels work by performing the following three steps:

1. First, a part of the blockchain state is locked under a smart contract, ensuring the agreement and business logic between participants.
2. Now off-chain transaction processing and interaction is started between the participants that update the state only between themselves for now. In this step, almost any number of transactions can be performed without requiring the blockchain and this is what makes the process fast and a best candidate for solving blockchain scalability issues. However, it could be argued that this is not a real on-blockchain solution such as, for example, sharding, but the end result is a faster, lighter, and robust network which can prove very useful in micropayment networks, IoT networks, and many other applications.
3. Once the final state is achieved, the state channel is closed and the final state is written back to the main blockchain. At this stage, the locked part of the blockchain is also unlocked.

Private blockchain

- Private blockchains are inherently fast because no real decentralization is required and participants on the network do not need to mine; instead, they can only validate transactions.
- This can be considered as a workaround to the scalability issue in public blockchains; however, this is not the solution to the scalability problem.
- Also, it should be noted that private blockchains are only suitable in specific areas and setups.

Proof of Stake

- Instead of using Proof of Work, Proof of Stake algorithm based blockchains are fundamentally faster.
- But again the question is still up for debate - ***is proof-of-stake better than proof-of-work?***
- Fun Reading:
  - *https://www.coindesk.com/proof-of-stake*
  - *https://consensys.net/blog/blockchain-explained/what-is-proof-of-stake/*
  - *https://goodmenproject.com/the-good-life/money-the-good-life/ethereum-proof-of-stake/*

Sidechains

- Sidechains can improve scalability indirectly by allowing many sidechains to run along with the main blockchain while allowing usage of perhaps comparatively less secure and faster sidechains to perform transactions but still pegged with the main blockchain.
- The core idea of sidechains is called a two-way peg, which allows transfer of coins from a parent chain to a side chain and vice versa.

Subchains

- This is a relatively new technique recently proposed by *Peter R. Rizun* which is based on the idea of weak blocks that are created in layers until a strong block is found.
- Weak blocks can be defined as those blocks that have not been able to be mined by meeting the standard network difficulty criteria but have done enough work to meet another weaker difficulty target.
- Miners can build subchains by layering weak blocks on top of each other, unless a block is found that meets the standard difficulty target. At this point, the subchain is closed and becomes the strong block.

Subchains

- Advantages of this approach include reduced waiting time for the first verification of a transaction.
- This technique also results in a reduced chance of orphaning blocks and speeds up transaction processing.
- This is also an indirect way of addressing the scalability issue. Subchains do not require any soft fork or hard fork to implement but need acceptance by the community.

Tree chains

- There are also other proposals to increase bitcoin scalability, such as tree chains that change the blockchain layout from a linearly sequential model to a tree.
- This tree is basically a binary tree which descends from the main bitcoin chain.
- This approach is similar to sidechain implementation, eliminating the need for major protocol change or block size increase.
- It allows improved transaction throughput.
- In this scheme, the blockchains themselves are fragmented and distributed across the network in order to achieve scalability.
- Moreover, mining is not required to validate the blocks on the tree chains; instead, users can independently verify the block header. However, this idea is not ready for production yet and further research is required in order to make it practical.

An elegant solution to scalability

- An elegant solution to scalability issues will most likely be a combination of some or all of the above-mentioned general approaches.
- A number of initiatives taken in order to address scalability and security issues in blockchains are now almost ready for implementation.
- For example, bitcoin segregated witness is a proposal that can help massively with scalability and only needs a soft fork in order for it to be implemented.
- The key idea behind so called *segwit* is to separate signature data from the transactions, which resolves the transaction malleability issue and allows block size increase.

Ethereum Devcon 2

- On the other hand, recently, an Ethereum mauve paper written by *Vitalik Buterin* has been presented at Ethereum Devcon 2 in Shanghai; it describes the vision of a scalable Ethereum.
- The mauve proposal is based on a combination of sharding and implementation of Proof of Stake algorithm.
- Certain goals such as efficiency gain via Proof of Stake, maximally fast block time, economic finality, scalability, cross-shard communication, and censorship resistance have been identified in the paper.

Bitcoin NG

- Another proposal, Bitcoin NG, which is based on the idea of micro blocks and leader election, has gained some attention recently.
- The core idea is to split blocks into two types, namely leader blocks (also called key blocks) and micro blocks.
- Leader blocks are responsible for Proof of Work whereas micro blocks contain actual transactions.
- Micro blocks do not require any Proof of Work and are generated by the elected leader every block-generation cycle.
- This block-generation cycle is initiated by a leader block.
- The only requirement is to sign the micro blocks with the elected leader's private key.
- The micro blocks can be generated at a very high speed by the elected leader (miner), thus resulting in increased performance and transaction speed.

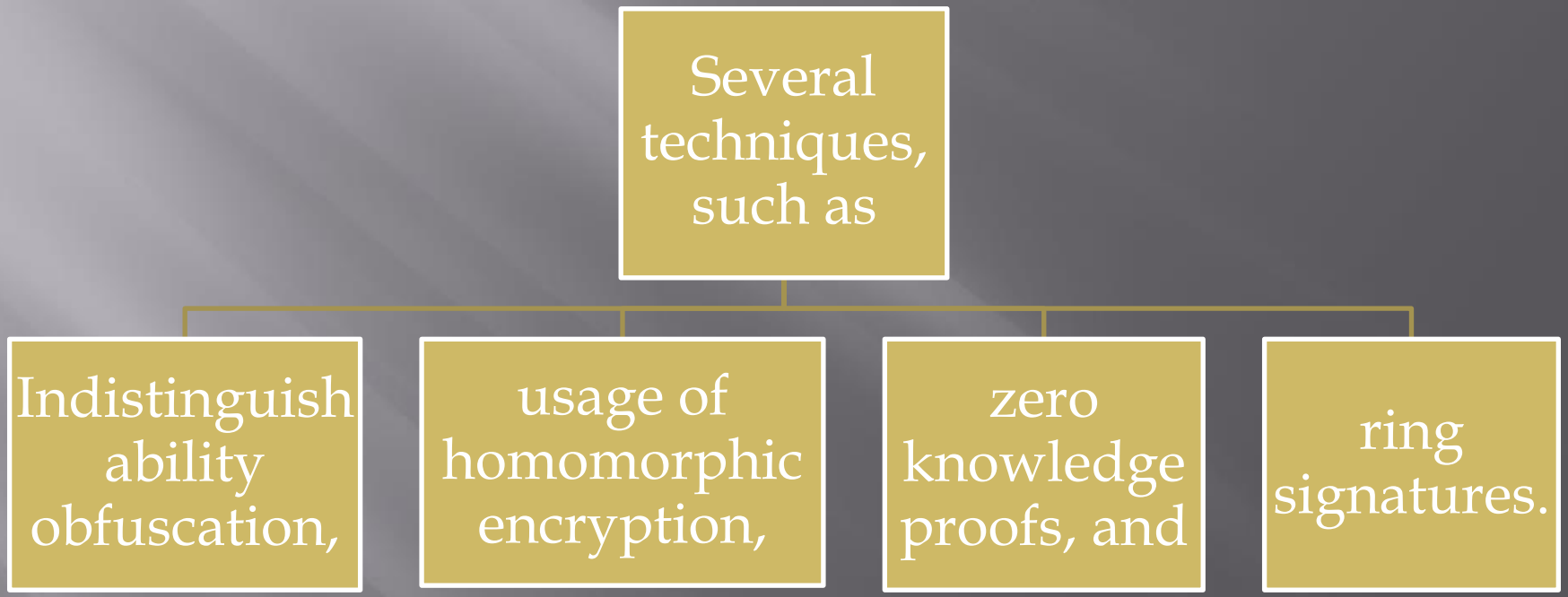
Security

- Even though blockchains are generally secure and make use of asymmetric and symmetric cryptography as required throughout the blockchain network, there still are few caveats that can result in compromising the security of the blockchain.
- There are a few examples of transaction malleability, eclipse attacks, and possibility of double spending in bitcoin that, in certain scenarios, have been shown to work by various researchers.
- Transaction malleability opens up the possibility of double withdrawal or deposit by allowing a hacker to change a transaction's Unique ID before the bitcoin network can confirm it, resulting in a scenario where it would seem that transactions did not occur.
- BIP 62 is one of the proposals along with segregated witness (segwit) that have suggested solutions to solve this issue. It should be noted that this is a problem only in the case of unconfirmed transactions, that is, scenarios where operational processes rely on unconfirmed transactions.

PRIVACY

- Privacy of transactions is a much desired property of blockchains.
- However, due to its very nature, especially in public blockchains, everything is transparent, thus inhibiting its usage in various industries where privacy is of paramount importance, such as finance, health, and many others.
- There are different proposals made to address the privacy issue and some progress has already been made.
- Several techniques, such as indistinguishability obfuscation, usage of homomorphic encryption, zero knowledge proofs, and ring signatures.
- All these techniques have their merits and demerits and are discussed in the following sections.

Privacy Preservation



Indistinguishability obfuscation

- This cryptographic technique may serve as a silver bullet to all privacy and confidentiality issues in blockchains but the technology is not yet ready for production deployments.
- **Indistinguishability obfuscation** (**IO**) allows for code obfuscation, which is a very ripe research topic in cryptography and, if applied to blockchains, can serve as an unbreakable obfuscation mechanism that will turn smart contracts into a black box.
- The key idea behind IO is what's called by researchers a *multilinear jigsaw puzzle*, which basically obfuscates program code by mixing it with random elements, and if the program is run as intended, it will produce expected output but any other way of executing would render the program look random and garbage.

Homomorphic Encryption

- This type of encryption allows operations to be performed on encrypted data.
- Imagine a scenario where the data is sent to a cloud server for processing. The server processes it and returns the output without knowing anything about the data that it has processed.
- This is also an area ripe for research and fully homomorphic encryption that allows all operations on encrypted data is still not fully deployable in production; however, major progress in this field has already been made.
- Once implemented on blockchains, it can allow processing on cipher text which will allow privacy and confidentiality of transactions inherently.

Zero knowledge proofs

- Zero knowledge proofs have recently been implemented in Zcash successfully.
- More specifically, SNARKs have been implemented in order to ensure privacy on the blockchain.
- The same idea can be implemented in Ethereum and other blockchains also.
- Integrating Zcash on Ethereum is already a very active research project being run by the Ethereum R&D team and the Zcash Company.

State channels

- Privacy using state channels is also possible, simply due to the fact that all transactions are run off-chain and the main blockchain does not see the transaction at all except the final state output, thus ensuring privacy and confidentiality.

Secure Multiparty Computation

- The concept of secure multiparty computation is not new and is based on the notion that data is split into multiple partitions between participating parties under a secret sharing mechanism which then does the actual processing on the data without the need of the reconstructing data on single machine. The output produced after processing is also shared between the parties.

Usage of hardware to provide confidentiality

- Trusted computing platforms can be used to provide a mechanism by which confidentiality of transaction can be achieved on a blockchain.
- For example, by using Intel **Software Guard Extension** (**SGX**), which allows code to be run in a hardware-protected environment called an *enclave*.
- Once the code runs successfully in the isolated enclave, it can produce a proof called a *quote* that is attestable by Intel's cloud servers.
- However, it is a concern that trusting Intel will result in some level of centralization and is not in line with the true spirit of blockchain technology.
- Nevertheless, this solution has its merits and, in reality, many platforms already use Intel chips anyway, therefore trusting Intel may be acceptable in some scenarios.

Usage of hardware to provide confidentiality

- If this technology is applied on smart contracts then, once a node has executed the smart contract, it can produce the quote as a proof of correct and successful execution and other nodes will only have to verify it.
- This idea can be further extended by using any **Trusted Execution Environment** (**TEE**) which can provide the same functionality as an enclave and is available even on mobile devices with **Near Field Communication** (**NFC**) and a secure element.

Coinjoin

- Coinjoin is a technique which is used to anonymize the bitcoin transactions by mixing them interactively.
- The idea is based on forming a single transaction from multiple entities without causing any change in inputs and outputs.
- It removes the direct link between senders and receivers, which means that a single address can no longer be associated with transactions, which could lead to identification of the users.
- Coinjoin needs cooperation between multiple parties that are willing to create a single transaction by mixing payments.

Coinjoin

- Therefore, it should be noted that, if any single participant in the Coinjoin scheme does not keep up with the commitment made to cooperate for creating a single transaction by not signing the transactions as required, then it can result in a denial of service attack.
- In this protocol, there is no need for a single trusted third party.
- This concept is different from mixing a service which acts as a trusted third party or intermediary between the bitcoin users and allows shuffling of transactions.
- This shuffling of transactions results in the prevention of tracing and the linking of payments to a particular user.

Confidential Transactions

- Confidential transactions make use of Pedersen commitments in order to provide confidentiality. Commitment schemes allow a user to commit to some value while keeping it secret with the capability of revealing it later.
- Two properties that need to be satisfied in order to design a commitment scheme are *binding* and *hiding*.
- Binding makes sure that the committer is unable to change the chosen value once committed, whereas the hiding property ensures that any adversary is unable to find the original value to which the committer made commitment.

Confidential Transactions

- Pedersen commitments also allow addition operations and preserve commutative property on the commitments, which makes it specifically useful for providing confidentiality in bitcoin transactions.
- In other words, it supports homomorphic encryption of values.
- Using commitment schemes allows the hiding of payment values in a bitcoin transaction.
- This concept is already implemented in the Elements Project (h t t p s ://el e m e n t s p r o j e c t . o r g /).

MimbleWimble

- MimbleWimble extends the idea of confidential transactions and Coinjoin, which allows aggregation of transactions without requiring any interactivity.
- However, it does not support the use of bitcoin scripting language along with various other features of standard Bitcoin protocol.
- This makes it incompatible with existing Bitcoin protocol. Therefore, it can either be implemented as a sidechain to bitcoin or on its own as an alternative cryptocurrency.

MimbleWimble

- This scheme can address privacy and scalability issues both at once.
- The blocks created using the MimbleWimble technique do not contain transactions as in traditional bitcoin blockchains; instead, these blocks are composed of three lists: an input list, output list, and something called *excesses* which are lists of signatures and differences between outputs and inputs.
- The input list is basically references to the old outputs, and the output list contains confidential transactions outputs.
- These blocks are verifiable by nodes by using signatures, inputs, and outputs to ensure the legitimacy of the block.
- In contrast to bitcoin, MimbleWimble transaction outputs only contain pubkeys, and the difference between old and new outputs is signed by all participants involved in the transactions.

Summary

- In this chapter, readers have been introduced to the security, confidentiality, and privacy aspects of blockchain technology.
- Privacy was discussed, which is another major inhibiting factor in adapting public blockchains for various industries.
- Next, smart contract security, which is a very hot topic currently, was discussed.
- It is a deep and extensive subject but a brief introduction on various aspects has been given, which should serve as a solid ground for further research in this area. For example, formal verification on its own is a vast area for research.
- Also, documentation is quite scarce; therefore, readers are encouraged to keep an eye on developments, especially around formal verification and developments related to the Ethereum mauve paper, as it is going to develop rapidly very soon.
- The field of blockchain security and especially smart contract security is so ripe now that a whole book can be written on the subject.
- There are many experts and researchers in academia and the commercial sector exploring this area and soon there will be many automated tools available for the verification of smart contracts.