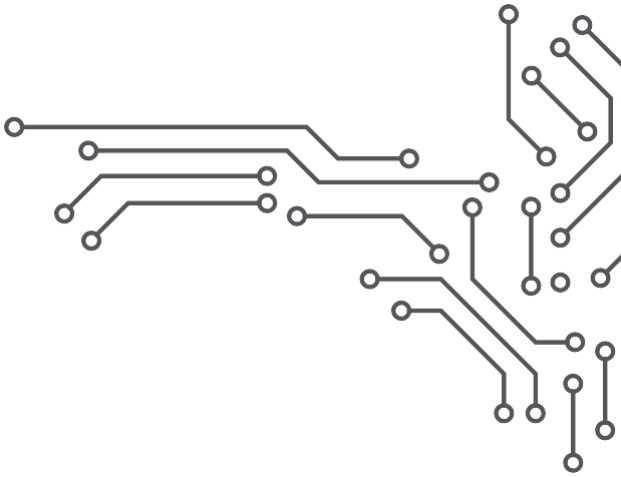
SHARIYAH
REVIEW BUREAU

SHARIA ANALYSIS

Bitcoin

INTRODUCTION



Bitcoin at its most basic is an autonomous public key cryptosystem that facilitates the exchange of digital value among peers via a sequence of digitally signed transactions rather than messages. As Satoshi Nakamoto, the creator of Bitcoin, says in its white paper, “An electronic coin is a chain of digital signatures.” The platform allows anyone to deploy permanent and immutable decentralized applications

Ticker	BTC
Consensus mechanism	Proof-of-work
Network type	Open source, Decentralized
Maximum Supply of Tokens	21 Million
Platform Function	Peer-to-Peer payments
Token Function	Payment

BITCOIN

Bitcoin at its most basic is an autonomous public key cryptosystem that facilitates the exchange of digital value among peers via a sequence of digitally signed transactions rather than messages. As Satoshi Nakamoto, the creator of Bitcoin, says in its white paper, “An electronic coin is a chain of digital signatures.” The platform allows anyone to deploy permanent and immutable decentralized applications

BITCOIN BLOCKCHIAN

Satoshi realized that for a P2P transaction system to work, all transactions must be publicly auditable via a shared database, or ledger, containing the history of all previous transactions. Satoshi’s solution: a P2P distributed “timestamp server” shared in common throughout the network. This timestamp server works by continuously hashing blocks of information (messages, transactions, etc.), which are timestamped and published widely to the network. Each timestamp of a block references the hash of the previous block, creating a chain of cryptographically secure, verifiable data that is more secure with each subsequent block. This distributed timestamp server as described by Satoshi has come to be known popularly as “blockchain.”

PROOF-OF-WORK MINING AND NAKAMOTO CONSENSUS

For this P2P transaction system to remain secure against malicious attacks and faulty nodes, there needs to be a method to counter Sybil attacks (when one entity fabricates many identities to compromise a network) and ensure consensus as nodes freely join and leave the network. To mitigate these risks, Satoshi implemented a proof-of-work, or PoW, system inspired by Adam Back’s Hashcash, which was also applied within Bitcoin precursors B-money and Bit Gold but with notable differences.

For this P2P transaction system to remain secure against malicious attacks and faulty nodes, there needs to be a method to counter Sybil attacks (when one entity fabricates many identities to compromise a network) and ensure consensus as nodes freely join and leave the network. To mitigate these risks, Satoshi implemented a proof-of-work, or PoW, system inspired by Adam Back’s Hashcash, which was also applied within Bitcoin precursors B-money and Bit Gold but with notable differences.

This process by which the network continuously validates broadcasted transactions and records them in the distributed ledger in the form of linked “blocks” of transaction data, producing a cryptographically secure, verifiable history of transactions over time, has since become known as mining, as this is how new Bitcoin is minted and put into circulation.

This is where Bitcoin’s design diverges from previous iterations of digital cash. While former proof-of-work tokens were issued and valued based on the work done to produce them or some other set of rules, the Bitcoin protocol rewards miners that solve a proof-of-work with a predetermined amount of Bitcoin in predetermined intervals, resulting in an autonomous, automated mint for BTC, whose value is intrinsic to the system rather than in relation to some other metric or resource.
The time, energy and resources put into securing the network and validating transactions is rewarded with the protocol currency and accumulated transaction fees, providing an economic incentive for miners to remain good actors despite particular groups possibly obtaining a majority of the hashing power and thus becoming capable of compromising the entire network.

Not only did Satoshi use the proof-of-work algorithm as a mechanism for issuing a currency, but also used it as a consensus mechanism, as the longest chain of confirmed blocks is always the leader. This has since become known as Nakamoto consensus.

BITCOIN UTILITY

The utility of Bitcoin is transfer of value and functioning as a medium of exchange. It is by design, a means of payment.

BITCOIN NETWORK

The Bitcoin network is an open-source, multistakeholder system that maintains and facilitates a global settlement layer and accounting system for borderless, peer-to-peer transactions. The stakeholders consist of miners, developers, merchants/companies and users all working in concert to provide security and up-time to the network, improve the protocol, build services on the network, and ultimately, use the network.

Unlike credit card networks like Visa and payment processors like Paypal, bitcoin is not owned by an individual or company. Bitcoin is the world's first completely open payment network which anyone with an internet connection can participate in. Bitcoin was designed to be used on the internet, and doesn't depend on banks or private companies to process transactions.

One of the most important elements of Bitcoin is the blockchain, which tracks who owns what, similar to how a bank tracks assets. What sets the Bitcoin blockchain apart from a bank's ledger is that it is decentralized, meaning anyone can view it and no single entity controls it.

Here are some details about how it all works:

- **Specialized computers known as 'mining rigs' perform the equations required to verify and record a new transaction.** In the early days, a typical desktop PC was powerful enough to participate, which allowed pretty much anyone who was curious to try their hand at mining. These days the computers required are massive, specialized, and often owned by businesses or large numbers of individuals pooling their resources. (In October 2019, it required 12 trillion times more computing power to mine one bitcoin than it did when Nakamoto mined the first blocks in January 2009.)

- **The miners' collective computing power is used to ensure the accuracy of the ever-growing ledger.** Bitcoin is inextricably tied to the blockchain; each new bitcoin is recorded on it, as is each subsequent transaction with all existing coins.

- **How does the network motivate miners to participate in the constant, essential work of maintaining the blockchain—verifying transactions?** The Bitcoin network holds a continuous lottery in which all the mining rigs around the world race to be the first to solve a math problem. Every 10 min or so, a winner is found, and the winner updates the Bitcoin ledger with new valid transactions. The prize changes over time, but as of early 2020, each winner of this raffle was awarded 12.5 bitcoin.

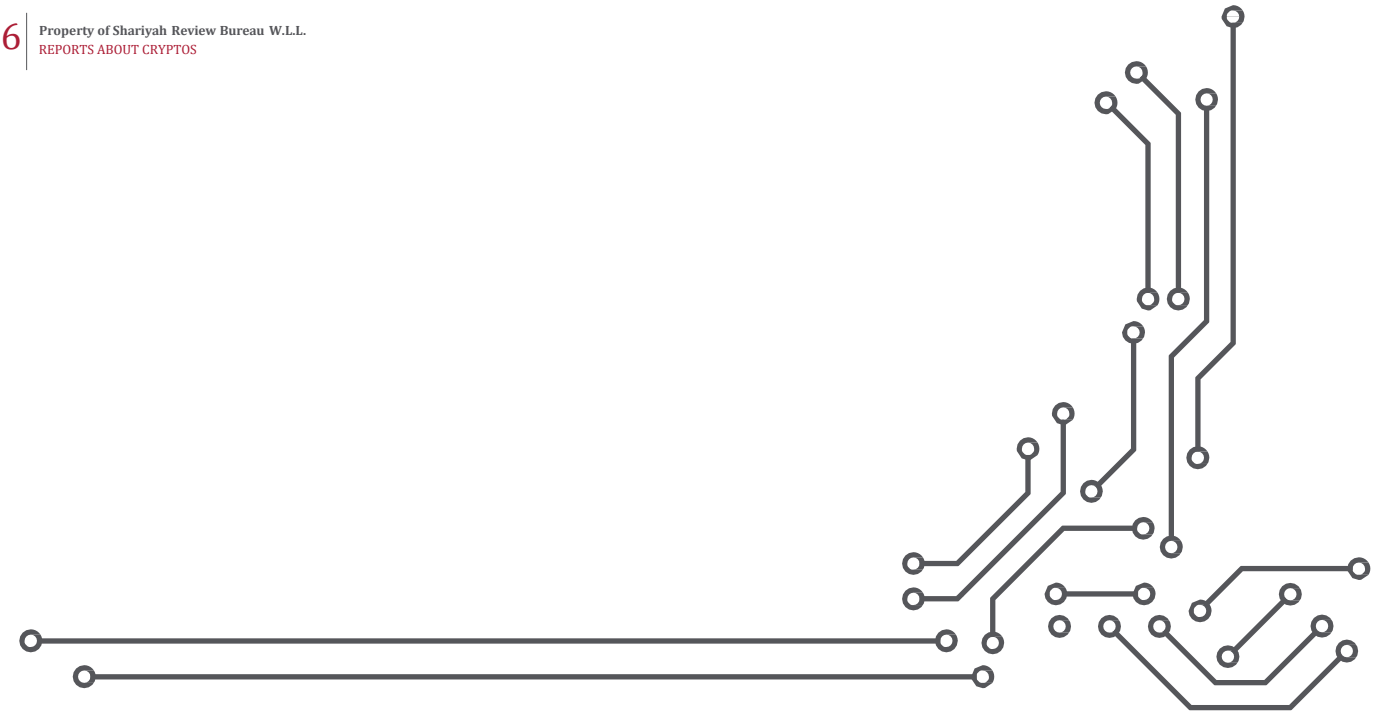
BITCOIN ANATOMY

What is a Bitcoin?" This question seems simple enough given what was covered so far, yet it is not all that obvious on the surface. What is this asset we are transacting across this P2P global financial network? When looking at the BTC balance in a digital wallet, what does that number represent?

As we've established, the means by which the Bitcoin network facilitates the transfer of value is not as simple as Alice sending a single transaction to Bob's account with a central server updating their respective balances. The Bitcoin total visible in one's public key address, or wallet, actually consists of multiple unspent transaction outputs, or UTXOs, of previous transactions received in the past that can be spent in the future. Recall Satoshi's basic definition of an electronic currency as a "chain of digital signatures." The amount of Bitcoin visible and accessible at a certain address is the sum total of the combined value of multiple chains of ownership implemented via digitally signed transactions.

CONSENSUS MECHANISM

Mining is a distributed consensus system that is used to confirm pending transactions by including them in the block chain. It enforces a chronological order in the block chain, protects the neutrality of the network, and allows different computers to agree on the state of the system. To be confirmed, transactions must be packed in a block that fits very strict cryptographic rules that will be verified by the network. These rules prevent previous blocks from being modified because doing so would invalidate all the subsequent blocks. Mining also creates the equivalent of a competitive lottery that prevents any individual from easily adding new blocks consecutively to the block chain. In this way, no group or individuals can control what is included in the block chain or replace parts of the block chain to roll back their own spends.



CONCLUSION

Bitcoin was setup as a P2P transaction system. The network is an open-source, multistakeholder system that maintains and facilitates a global settlement layer and accounting system for borderless, peer-to-peer transactions. From a Shariah compliance perspective, the Shariah has not defined or enforced any one article to be the medium of exchange.

Ibn Taymiyyah (d. 728 H) states that, the Shariah has not defined any specific condition nor definition for currency and money and has instead left it to the 'Urf and understanding of the people [Majmu' al-Fatawa]. It is upto the people to come to an agreement and understanding of what they accept as a medium of exchange and what they do not. Further, two people may agree to exchange something, but that does not mean that what is exchanged is equivalent to currencies either. It is simply a medium of exchange. As such, people agree on the Bitcoin network to use bitcoin as the medium of exchange. Bitcoin has a lawful and Shariah compliant utility which is to function as a medium of exchange, facilitate payment and the transfer of value; as such Bitcoin is Shariah compliant.

RESOURCES

Website: https://bitcoin.org/en/
Whitepaper: https://bitcoin.org/en/bitcoin-paper
Learning Resources: https://bitcoin.org/en/resources

Secondary sources:
https://www.coinbase.com/learn/crypto-basics/what-is-bitcoin
https://cointelegraph.com/bitcoin-for-beginners/what-is-bitcoin

ABOUT SRB

Since our humble beginnings 17 years ago in the Kingdom of Saudi Arabia we've grown to include +100 companies across a host of industries, 5,000 transactional programs, 5 interdisciplinary teams and a combined scholarly workforce of 31 Sharia Scholars from 16 countries. And we're not done yet: our Sharia Audit and Sharia Advisory services will continue to improve—serving local and international businesses to help them maintain and manage Shari'a compliance.

Our combination of international and local market knowledge and multi-disciplinary perspective of Sharia give us an edge in the professional Sharia Advisory and Sharia Audit services industry in the GCC. The scope and value of our services, and the help they offer in building a thriving economy, keeps us excited.

The future of Sharia Advisory and Audit is exciting, and we are very lucky to be a part of this business!