Introduction to Bitcoin Enterprise Summary

Learn how Bitcoin and the BitcoinSV network can radically change how digital services are provided.

The purpose of this course is to give answers to questions such as:

- What is the difference between BSV and Cryptocurrency?
- What are blocks?
- What are transactions?
- Separation of blockchain vs transaction ledger
- Working blockchain - Pruning vs SPV and block linked databases
- Why fixed protocol?
- What is a 'private blockchain'?
- Why is Proof of Work superior vs Proof of Stake/Authority?
- Why is proof of work inefficient for BTC but efficient for BSV and more efficient at scale?

About BitcoinSV

Introduction

- Rapid change is taking place across fields of information technology, traditional systems are being digitised.
- The success of bitcoin enabled the disintermediation of our digital financial and data activities, allowing a global network of third-party nodes to manage a single ledger of all business activities.
- The ledger is efficient and its ability to scale, enables transaction cost to be reduced to unseen levels.
- Correct use of the ledger can facilitate triple entry accounting.
- Bitcoin was designed from first principles to act as a high performance, reliable and low-cost public network and ledger.

> BitcoinSV manages the Bitcoin ledger, focusing solely on building for performance.

Safe, Instant Transactions at a Predictably Low Cost

- From the outset, Bitcoin was designed with scalability in mind.
- In order to scale to a system capable of managing global demand, some less intuitive design choices were made.
- Thanks to tremendous contributions from professional research and development teams the changes made to the underlying Bitcoin protocol under erroneous assumptions have been almost entirely reverted, and the protocol in use on the BitcoinSV network has been returned to as close to the original Bitcoin protocol as possible.
- Development of the node client software (Blockchain) has leveraged Satoshi's seemingly unconventional design choices leading to massive breakthroughs in network throughput, capacity and capability.

> The development of infrastructure and software continues with the upcoming release of **Teranode, a completely reworked node client particularly suited to cloud micro-service architectures.**

Reliably Low Fees

- The bitcoin network is capable of accomodating large/enormous transactions so that there is no market-based fee pressure.
- This allows miners to set low, stable transaction prices for users.

> Bitcoin was always meant to scale without limits, and it's this scaling that drives a positive user experience, and a sustainable block reward.

> As more transaction volume is processed by the network, fee revenue increases for the miners and competitive forces imply that transaction processing will be offered by more capable nodes at the best possible rate.

Comparison to Legacy Transaction Systems

- Valid transactions which are submitted to the network can be considered cleared and settled within just a few seconds of their submission to network nodes.
- Checking the status of a transaction is also quick and easy and can be automated within wallet software.

> BitcoinSV network cost approximately 0.01c USD, allowing for 1,000,000 transactions to be processed for just $100.

Payment Channels

- BitcoinSV allows users to leverage payment channels.
- A **payment channel** is a is a valid transaction, but will not be accepted into a block until some future time and date.
- In the **intervening period**, the parties to the transaction have the freedom to publish new updates which change aspects of its contents such as data packets being shared, amounts being paid and much more, enabling innovative and highly compelling digital services to be managed within the transactions themselves.
- Payment channels are a ground-breaking new technology, only supported by the BitcoinSV network.

Scalability to Accommodate Global Demand

- One of the most important aspects of the Bitcoin system is its ability to scale without bounds, giving it the potential to manage hundreds of millions or even billions of transactions every second.
- In 2009, Bitcoin was released with no limits on block-size, transaction size, script complexity or use of opcodes. Between 2010 and 2017, numerous changes were made to the base protocol that restricted its ability to scale.
- However, since 2018, teams developing the BitcoinSV node client software have worked to restore Bitcoin to its original unbounded protocol design.
- Bitcoin script also comes with `op_codes future proofing it to work well with IPV6, and extra op_codes` to add additional hashing functions if needed. Furthermore, as IPV6 subsumes IPV4, Bitcoin will become instrumental in supporting the anticipated billions of IoT devices expected to come online.
- By way of micro-transactions, Bitcoin will be the global validation and timestamping service providing an effective way to clean data and communications, maintaining integrity and supercharging AI & Machine Learning.

Big Blocks Show Big Potential

-As of 2021, BitcoinSV nodes are already regularly processing blocks containing over one million transactions and over 2GB in size.

- To ensure the network scales smoothly the BitcoinSV node software team's focus is on optimizing software performance - and keeping the underlying base protocol consistent helps them do this.
- In addition to helping nodes scale, the continuous efficiency improvements, and unchanging base protocol of the BitcoinSV node software help ensure the network is robust in the event it loses significant processing power. Scaling the node client and the systems that run it is a key pillar of the network's robust architecture and capability.
- Importantly, because nodes must win blocks to get paid, and the probability of getting paid goes up significantly when nodes who have significant capacity and processing power are well-connected to each other, the network will always be able to accommodate demand, no matter how much it grows.
- Bitcoin's sophisticated economic incentives also encourage nodes to be assertive in their strategies to increase their throughput capabilities to attract more fee revenue.
- Yet, at the same time, the incentive structure is designed to ensure that they cannot do this in a fashion that outpaces the rest of the nodes on the network.
- Bitcoin is a co-operative meritocratic system. The more ambitious and competitive a node is, the greater the reward they can win, with the caveat that nodes must also be completely open and honest with each other to maximize their efficiency

A Plan for Regulatory Acceptance

- Cryptocurrency and blockchain landscape, there is evidence of scant regard for legal process and regulations.
- Bitcoin can work within the frameworks of current laws and regulations. It was designed in such a way as to make adherence to legal requirements both simple and affordable.
- Bitcoin was never created to subvert the legal system or destroy central banks, but rather as a tool to be used to build new platforms and services in ways that are far more efficient, scalable and profitable.
- Micropayment based business models are only possible with efficient, ultra-low-cost, payments.

Ready-made Compliance Tools

- Technical Standards Committee (TSC) is implementing and servicing a set of ready-made tools that help enterprises building platforms remain compliant with stringent regulations easily and cheaply, including internationally applied, 'Know Your Customer' (KYC) and 'Anti Money Laundering' (AML) rules.
- Every Virtual Asset Service Provider (VASP) must comply when dealing with high value transfers.
- The TSC is constantly developing new standards to deliver fast, low-cost digital services that exceed the functionality of their legacy counterparts to ensure every platform built on Bitcoin is ready for the regulations of today and the future.

The Open BSV License

- The Open BSV License (https://bitcoinassociation.net/open-bitcoinsv-license) has been created for use by developers, projects or companies who wish to make their software or applications available for open (free) usage only on the Bitcoin SV blockchain.
- It is a modified version of the MIT license that allows free usage and modification of open-source software only on the BitcoinSV blockchain and its related testnets. Since its creation, there have been numerous protocols, toolkits and software elements released under the Open BSV Licence including: Nakasendo Go-SVDB ElectrumSV Bitbus Many more

The Bitcoin White Paper

- In 2020, Dr Craig Wright (AKA Satoshi Nakamoto) was awarded copyright over the Bitcoin white paper (www.bitcoinsv.io/bitcoin.pdf) he published in 2008 by the United States copyright office.
- This copyright is essential to the protection of Bitcoin against other projects who lay claim to being the original Bitcoin and protects the white paper as a foundational document outlining the functionality of Bitcoin as a system, a network and a ledger of exchange.

Protocol Stability

- One of the most important aspects that will contribute to the uptake, longevity and reliability of Bitcoin is its stability as a protocol.
- In the period from 2010 to 2018, the Bitcoin protocol was changed in several fundamental ways by node client developers seeking to 'fix' what they erroneously perceived to be 'problems' with the system.
- The fixing created further downstream problems in many areas and generated significant angst for developers building applications and businesses on Bitcoin at the time.

> With the release of the BitcoinSV node client, node operators, the arbiters of the network, have committed to a policy of making no further changes to the protocol save those which undo changes already made such as the removal of transaction and block size limits and the re-enabling of disabled functionality in the scripting language.

Building Foundations on a Bedrock of Stone

- When businesses depend on a technology and that technology is continuously changing, it creates situations where their applications and processes become inoperable.
- When it comes to Bitcoin, this can mean the network becomes inaccessible for applications or services that depend on it, or worse, pre-signed transactions scheduled to take place at some point in the future can no longer be processed.

Technical Details

The Network

- The Bitcoin network is the infrastructure all network users (applications, services, and users) rely upon, with the nodes sitting tightly connected at its core.
- Nodes are defined as systems which gather and process transactions, timestamping them into blocks through the process defined in Section 5 of the Bitcoin white paper.
- Driven by Bitcoin's game changing economic incentives, the network spontaneously forms into a densely connected and highly robust small world network which allows the most capable nodes in the system to succeed in their roles as transaction validators by building blocks to extend the public ledger.
- It is the role of these operators to use these highly capable, purpose-built machines to construct the blockchain at the core of the system as part of a competitive enterprise within which they compete in a rapidly repeating game.

The Small World Network

- As the network grows, the nodes who demonstrate their capability to generate blocks reliably and honestly are incentivised to create a **dense web of high-bandwidth connections** to each other to ensure that they are able to both transmit and receive new transactions and block announcements in as close to real time as possible.

- **This highly interconnected core at the centre of the network forms what is known as a 'small world network' and enables a level of hyper-awareness of the activities of other nodes.**
- This collective awareness allows each node to show openly their intent regarding any particular transaction or block and is a major incentive in the development of the network's structure.
- Within this small world network, nodes manage each other, and their connections with each other.
- Despite a lack of central direction, this method of reaching consensus ensures that only the most honest and capable systems who will benefit from investments in connectivity from their peers.

Robust In Its Unstructured Simplicity

- Thanks to the simple nature of Bitcoin's protocol and the very high density of connections at the network's core, the functionality of the system remains robust even under extreme modes of failure such as the loss of a majority of nodes on the network.
- The simple nature of Bitcoin's protocol and the very high density of connections at the network's core, the functionality of the system remains robust even under extreme modes of failure such as the loss of a majority of nodes on the network.
- Thanks to Bitcoin's unbounded block size, the impact to users of the system in such a scenario is minimal.

The Bitcoin Satoshi Vision Node Client

-**This client is a direct descendant of the original Bitcoin node client** released by Satoshi Nakamoto in 2009, and extensive efforts have been made to maximize scaling within the limits of its single server architecture.

- **The node client offers features such as Remote Procedure Call (RPC) functionality to broadcast and analyse transactions and analyse blocks and other network activity.**
- **The client has been optimised to focus on the utilities required to operate a node which is actively working to extend the blockchain by building blocks and performing by building blocks and performing proof of work**, rather than as a wallet for network users to send and receive funds.

Teranode - The Future of Bitcoin

- The Bitcoin Association also funds development of the Teranode project which is a next generation BitcoinSV node client.
- Teranode's design leverages microservices to create a highly extensible cluster-based system.
- It has become abundantly clear that demand for transaction validation and timestamping will continue to grow exponentially for many years.
- The Bitcoin Association has taken a leadership role in undertaking the development of next generation node clients for node operators as we transition to a future where millions of transactions per second are submitted to the network.
- **The Teranode project is being designed to manage multi-terabyte-sized blocks** which will allow the network to process tens of millions of transactions per second.
- A single terabyte block produced every ten minutes can contain up to 4 billion transactions, giving the network a daily capacity of over 500 billion transactions.
- This will allow BSV to accommodate more than just monetary transactions to support machine-to-machine data exchange, smart contracts, enterprise applications and more with ease.

The Protocol - Simple, Robust and Unbounded

- As a foundational technology for tomorrow's financial products and services, it is of vital importance that people building on the Bitcoin protocol have certainty that the systems and software they produce today will continue to operate for many years into the future without having

to worry that node client developers might decide to modify the protocol in such a way that those products and services cease to function.
- This has been an issue in the past, and while changes were introduced into the protocol during its first 10 years, network node operators are much more aware of their responsibility as stewards of the system and have made a commitment to make no further changes to the protocol beyond those needed to restore it back to its original functional capability.

What is the Bitcoin Protocol?

There are two message types that comprise the Bitcoin protocol:

1. Block Headers

- Block headers are just 80 bytes long and represent a node's proposal to the network for the extension of the ledger.
- In order to validate a block header, other nodes must first check the following:
- That it forms a new longest chaintip by building on the most recent previous block.
- That its timestamp is valid and within the allowed precision.
- That the difficulty target is correct.
- That its proof of work is valid - this simple check is done by double hashing of the 80-byte header
- using the SHA256 algorithm and checking that the resultant value is below the difficulty target.
- That the transactions contained within the block are valid and that the Merkle tree whose root value is in the block represents a valid interpretation of recent events on the network.
- These final checks involve ensuring each transaction in the block is valid and does not spend any previously spent inputs, and that a reconstruction of the complete Merkle tree generates the root hash which is contained in the block header.
- Once these checks are complete, the node can accept the block as valid and begin building a new block that references this block as the highest valid chain tip.
- The small size of block headers is an important aspect of the efficiency of using working blockchains, a concept we will cover in a later section.

2. Transactions

- Each transaction must reference one or more existing outpoints containing spendable satoshis on the Bitcoin ledger and generate one or more new outputs that place those satoshis into newly created scripts which can be consumed in future transactions.
- Each output generated within a transaction defines a predicate or 'puzzle' which locks the satoshis it contains into place. In order to spend the satoshis, the user must provide a valid solution as a transaction input. The scripting language used within the Bitcoin protocol is highly flexible and can be used to capture and inscribe any requirements related to the activity generating the transactions. Importantly, transactions are not necessarily limited to financial activity, and things like sensor data, user selection information and much more can be captured in a transaction script. There are no protocol level limits on the size or complexity of transaction scripts.

Proof of Work

- Bitcoin uses a Proof-of-Work system that requires nodes competing to extend the blockchain to solve a computationally demanding and energy intensive puzzle as part of the block creation process.
- Verifying the proof to the puzzle is the first thing that nodes do when they are validating a proposed block received from another node. While it takes a lot of computing power to find a valid Proof of Work solution, it is very quick and easy to check.

- This system serves as a gating function by galvanizing nodes to invest money in their block production systems, precipitating the formation of the small world network discussed previously.

The Algorithm

- The proof of work mechanism is controlled by an algorithm which modulates the difficulty of the puzzle so that no matter how much computing power or energy is applied to the solution, the block discovery rate is kept as close to 10 minutes as possible.
- This timeframe is important as it provides enough time between blocks to minimise the emergence of competing blocks (and the resultant orphans), while still allowing for a significant number of competing nodes to participate in the network.

Efficiency of Proof of Work

- While it may seem that Proof of Work is an inefficient system which consumes vast amounts of energy, this is not the full picture.
- . Since the inception of the network, Bitcoin has distributed its base tokens of account (Satoshis) by including them as a block reward subsidy, with the intention of bootstrapping node operations.
- As per the Bitcoin white paper, the block reward will eventually entirely transition to transaction fees. As this occurs, nodes will be incentivised to get as many transactions as possible inside each block.

Privacy and Identity

- l data committed to the ledger is public, however thanks to Satoshi's choices in picking his elliptic curve and signature algorithm, best in class encryption is possible.
- Identity in this scenario is kept completely off-chain. The ability to read and write data on a particular part of the blockchain will be managed by the user's device and will be dependent on the device having the particular keys needed.

Permissions, Privacy and the Metanet

- Through Bitcoin's highly flexible and expressive scripting language, people using Bitcoin can express any type of spending condition or permission-based requirement and place it on the objects they are using within their platform.
- With this flexibility, and the use of a second layer data protocol that nests within Bitcoin transactions, it becomes simple to imagine, design and then build applications for diverse use cases on the blockchain.

Resources and Tools

The Technical Standards Committee

- Part of the work undertaken by the Bitcoin Association includes the formation and management of a Technical Standards Committee focused on delivering a robust and feature-packed set of standards, which will simplify the process of interconnecting services and products operating on the Bitcoin network.
- The committee promotes technical excellence and furthers Bitcoin SV's utility by enhancing interoperability through standardisation, facilitating industry participation in the development of global standards, and ensuring technical standards are maintained and freely available.
- Working groups are formed to evaluate and progress each separate standard, with current developments covering a wide array of service needs and requirements in parallel.

- The committee itself does not decide when to develop a new standard, but allows the process to be industry-driven. Individuals or companies who wish to develop or accelerate proposals are encouraged to come forward and participate

TSC Principles

The TSC operates under a set of 4 principles defined to ensure the committee operates to a very high standard, and always looks to make the best decision for the ecosystem at large. These principles are defined as follows:

1. Industry-driven: experts and companies, in response to a perceived need in their industry, take the lead deciding which standards should be developed, not the TSC.
2. Created by experts: industry experts are involved at all stages of the standard development process, from deciding whether a new standard is needed, to defining all the technical content and reviewing and monitoring industry adoption once published.
3. Collaborative and objective: an open process to ensure that all parties interested are offered the opportunity to be actively involved in the standard development. The recommended solution is a result of a consensus-based approach that fully considers comments gathered from stakeholders during both the internal and public review phases.
4. Accountable and open: TSC standard development follows transparent procedures. The implementation of standards is monitored and recorded internally with a summary of technical decisions and comments received made publicly available.

Standard Development Process

Technical standards are created by working groups formed from experts in the necessary subject matter. A strong focus is placed on meeting the needs of the organisations and sectors that they represent and of the wider ecosystem. These industry experts drive the standardisation process, and are involved at all stages of standard development, the initial decision whether a new standard is needed, the subsequent definition of technical content, final review process and post-publication monitoring of industry adoption. The TSC oversees the process, acting as facilitators and offering the platforms, rules, governance, methodologies, and access to specialists such as technical writers to objectively address the standards development lifecycle. Each standard's working group is assigned a TSC sponsor to guide its development lifecycle. The sponsors independently oversee the working group using their own methods while ensuring policies and processes are maintained and guaranteeing high quality outputs that reinforce the relevance of industry and technology standards.

The standard development process is split into three stages:

1. Submission: The submission phase of the standardisation process describes the activities undertaken from initially identifying a business need through to the formation of a working group that will drive the standard forwards to completion.
2. Drafting and Review: The drafting and review phase of the standardisation process describes the activities undertaken from the successful formation of a working group through to completion of a final, reviewed draft.
3. Standardisation: During the standardisation phase, the standard is published on the TSC website. A period of time is allowed for during which the TSC and the working group monitor adoption and implementations. This period of time is determined by the scale and scope of the standard. Once elapsed, the TSC make a final decision (through majority vote) on whether to promote the publication to recommended, make further modifications or to withdraw the standard.

Status of Current and In-progress Standards

With new standards being added, and standards that are being worked on moving through the different stages of development, the status of various standards being worked on changes on a monthly basis. To see a list of the currently published and in-progress standards, please visit this website: https://tsc.bitcoinassociation.net/library/

Future Roadmap

The TSC roadmap summarises the current standardisation landscape for the Bitcoin SV ecosystem. In line with its mission to promote technical excellence and improve the utility of BitcoinSV, the TSC aims to enhance interoperability through standardisation.

- It is intended to help people navigate emerging standards and includes several proposed areas for future development based on feedback received from stakeholders.
- To learn more about the TSC roadmap, please visit this website: https://tsc.bitcoinassociation.net/roadmap.

The Working Blockchain

- As stated before, the protocol is unbounded, and blocks can accommodate vast quantities of data and transactions. As the network grows, it will become increasingly impractical for users to need to manage the full blockchain in order to interpret their own situation.
- Thankfully, in sections 7 and 8 of the Bitcoin white paper, entitled 'Reclaiming Disk Space' and 'Simplified Payment Verification' respectively, there are defined solutions that allow every entity connected to the network to manage only the data that they need to manage, rather than all of the data at once.

Pruning to Create a Working Blockchain

- Thanks to Bitcoin's use of Merkle trees, the full contents of a block (unbounded in size) is hashed down to a single 32-byte value which is included as part of the block header. To validate a block, nodes must check that the block's Merkle root is correct.
- The only way to do this is to take every single transaction in the block and hash them to create the full Merkle tree structure. Once the block is validated, the node can then freely prune unneeded content without damaging the integrity of the remaining parts.
- As such, a miner's Working Blockchain is generated by taking the full content of each block and cutting it back to only that which they determine is needed to most effectively validate future actions.

Building a Working Blockchain from a List of Block Headers

- Building a Working Blockchain from a List of Block Headers. For users interfacing with the network, Simplified Payment Verification, or SPV, provides a means by which a user can start from a list of block headers and add individual transactions with their corresponding Merkle path, effectively reconstructing a partial Merkle tree.
- Storing transactions in this way gives users the ability to prove to anyone that records presented have been accepted by the network without having to manage even a tiny fraction of the network's total throughput.
- Users simply hold what they need and no more. When they no longer need the information, it can be pruned in the same manner used by miners to reclaim disk space.

A World View Backed by Proof of Work

The Metanet and the New Internet of Value

- In 2019, Dr Craig Wright published a white paper detailing a system for creating an on-chain internet of value, allowing content and content management frameworks to be embedded directly into Bitcoin transactions and indexed to allow simple navigation and service.
- **The Metanet is a protocol that describes a means of embedding this data in transactions in ways that allow it to be both easily retrieved and verified to establish provenance. This gives data on the Metanet the immutability, security and scalability of Bitcoin.**
- Key to the Metanet is the Elliptic Curve Digital Signature Algorithm (ECDSA) that is used to secure millions of Bitcoin transactions every day. Using elliptic curve signatures as part of a second layer protocol allows us to generate detailed information systems on the public ledger and then serve them up to users/viewers/customers via Metanet gateways.
- Thanks to the fact the information isn't stored via a central server or domain-based system, it can remain accessible even when individual metanet gateways are taken offline.
- The model gives the data being served the same immutable properties as the Bitcoin transactions it is wrapped in, with the security of Elliptic Curve Digital Signatures which allows any user viewing the data to quickly and easily validate the source of the material.

The Metanet Protocol

- The Metanet protocol defines various ways that we can build linked informational databases on the public ledger for use in the Metanet.
- These databases closely resemble the hierarchical systems used in today's internet services, but rather than these being hosted on servers that can be attacked and taken off-line, they are written to the public ledger and become immutable records available to anyone with access to the internet.
- The protocol uses ECSDA signatures to form edges from child nodes back to their parents.
- An individual parent node can have an unbounded number of children, but the current version of the Metanet protocol limits each child to one parent, or zero parents in the case of the root node of a Metanet graph.
- By using this simple and extensible element, we can create complex structures comprising of large numbers of connected nodes forming a database of information which can be simply and quickly scanned, validated and visualised by Metanet users.
- The Metanet brings the idea of microtransactions to the fore, giving platform operators and application builders the power to manage individualised services for millions of users with microtransactions. This could include serving content, calculating computer-based outcomes or any of a multitude of other activities. A technical summary of the protocol is available here: https://5thwork.com/courses/course-v1:NITDA+NITDA0005+2022Q3/courseware/bfcd0622f83c4ea195e5d9d89bc6c9b9/c95358c6d72d431d8753b37adf28300a/?child=first

Node Software

Reliable open source software that provides the fundamental requirements for transaction processing enterprises to mine efficiently and effectively for greater profitability.

Lite Client

Bitcoin SV's LiteClient makes Simplified Payment Verification (SPV) communications faster and more secure, allowing for services to deal only with transactions deemed relevant for their own activities, without the need to retain records for the entire network.

Teranode

Teranode is Bitcoin SV's solution to the challenges of vertical scaling by instead spreading the workload across multiple machines. This horizontal scaling approach enables network capacity to grow with increasing demand through the addition of cluster nodes, allowing for Bitcoin scaling to be truly unbounded.