BSV BLOCKCHAIN

Enterprise blockchain products using the BSV blockchain

TABLE OF CONTENTS

ABOUT THE AUTHORS

Manisha Arora and Kapil Jain are technology professionals with experience in enterprise software development across the globe in finance, healthcare and SCM domains. They collaborated for this eBook to explain Bitcoin protocol and the BSV blockchain in terms of enterprise application development considerations.

Both have been associated with the Association for the BSV blockchain and BSV Academy for creating educational content for effectively teaching blockchain to a wider audience.

Manisha Arora

LinkedIn

Kapil Jain

LinkedIn

ABSTRACT

The BSV blockchain implements the Bitcoin protocol in its original design and offers a varied set of capabilities which can be harnessed by enterprises to gain enhanced and novel capabilities which were not possible before the invention of this protocol.

This innovation allows creation of a distributed global network for value exchange which runs based on a competitive process rather than a set of trusted entities.

Beyond the buzz and hype about blockchain technology being revolutionary, the current state of enterprise application development using blockchain as a whole has not progressed beyond experimental phases. There are two main reasons for this situation: one, enterprises being skeptical, have focused towards the various implementations of private or permissioned blockchains and second, the limited scalability provided by available blockchains.

The BSV blockchain (BSV) is the only public blockchain which has potential to handle not thousands but millions of transactions per second. It is not just the provision of throughput capacity, but the BSV blockchain also processes transactions for tiny fees, consistently less than a hundredth of the US cent for payment transactions.

With a stable base protocol and technical plumbing in place, this innovation has potential to power the emergence of new data business models in varied industries such as healthcare, eSports, supply change management, Internet of Things, Big data applications, remittance, distributed network intelligence, privatised identity system and many more.

In this eBook we will explore:

- The properties of the BSV blockchain that makes it distinguishable from other enterprise-scale blockchains
- Applications and products that can be built using the BSV blockchain

Keywords: Blockchain, application development, software, digital transformation, digital cash system, electronic payments, metanet, peer-to-peer payments, smart contracts, micropayments, distributed ledger, public blockchain, proof-of-work consensus algorithm

Introduction to the protocol behind the BSV blockchain

Bitcoin is a peer-to-peer electronic cash system[1]. It is a protocol by which two parties can transact i.e. exchange value over the Internet without involving a trusted intermediary. It utilises cryptographic tools - digital signatures and hash functions to enable and record the exchange. Either the sender or the receiver of each transaction broadcasts it to the network of nodes / miners. Within the network, all transactions that are broadcasted within a certain time frame are grouped together. The staging area where miners pool these transactions broadcasted to the network is called a mempool.

The miners compete and cooperate with each other within the ecosystem. They compete with each other to verify the integrity of each transaction, received within a certain timeframe, and solve a hash puzzle using a technique similar to brute force. The miner who solves the hash puzzle first proposes the block to the network, as a candidate to be added as the next block in the blockchain, along with the proof-of-work.

Other miners co-operate by validating the proof-of-work and integrity of transactions, accepting it as a valid block in the chain. These validated transactions are grouped together as a block and the solution to the hash puzzle is recorded in the block header.

When the next block is mined, validated and accepted the block header of the previous block is referenced in the next block header. This process subsequently generates a chain of blocks. Though the data structure that evolves from the protocol implementation is as a blockchain, it is essentially a timestamp server, which timestamps each block in a chronological order, and the timestamp for a block is attributed to each transaction that is part of that particular block. The transactions within a block are recorded in the chronological order and nodes implement the 'first seen rule'[2] to overcome conflicts.

The diagram below displays an example of payment settlement process which shows an exchange between two entities, Alice and Bob.

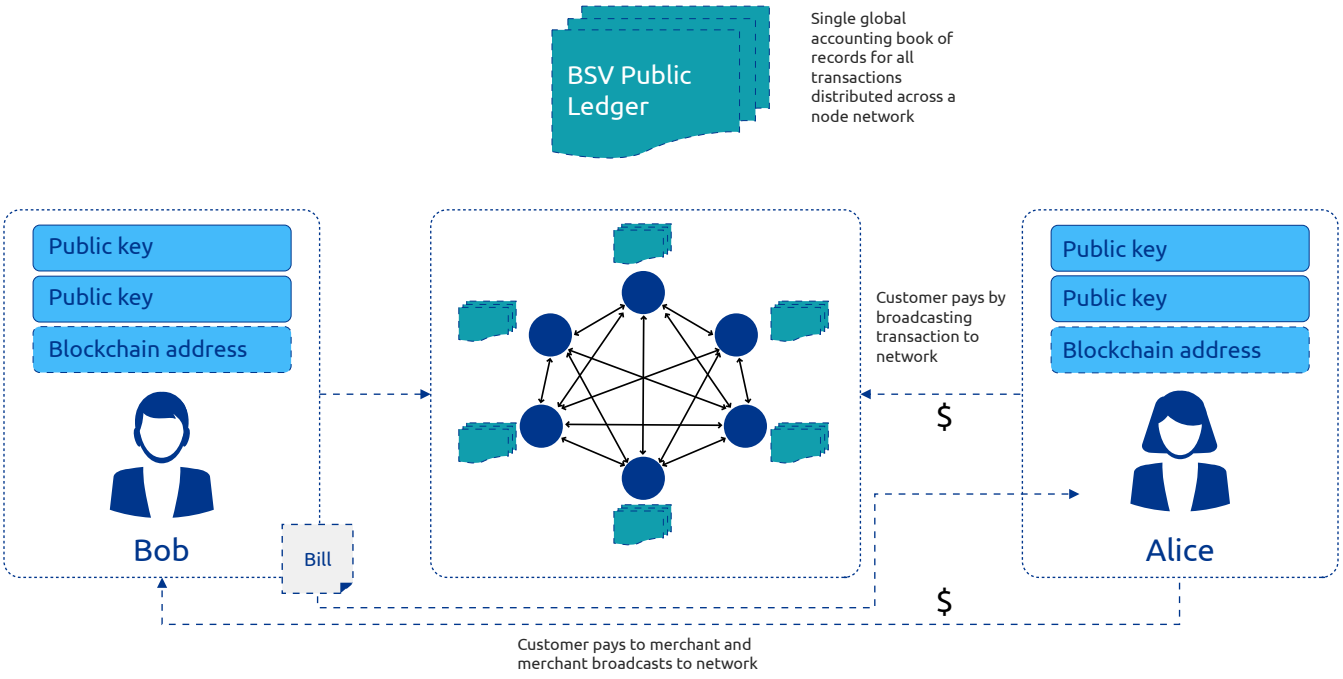


Figure 1 : Reference implementation of blockchain-based payment and settlement process used in e-commerce[3]

There are several options available to be used as enterprise blockchain, a number of them implementations of the Bitcoin protocol. However it is essential for enterprises to realise the distinguishing capabilities BSV blockchain provides from other blockchains and Bitcoin node implementations. Before we look at details of why the Bitcoin protocol stands apart, let's list the critical decision parameters for enterprise to consider:

Attributes	BSV blockchain capabilities
Authorisation speed for transaction	1 sec
Transaction clearing and settlement	10 mins
Throughput	3,987 TPS as of today
Median transaction fees	$0.00011

By end of 2022, the throughput capability is planned to expand to 50,000[5].

BSV blockchain features

Before we deep dive into important features, it is critical to understand that the Bitcoin protocol is 'set in stone' and cannot be altered by any centralised authority. It draws parallels from the TCP/IP Internet layer on which the complete digital economy relies today. Enterprises require the protocol to be stable as change in the same will have a cascading effect on the products. Like any other protocol, the Bitcoin protocol is nothing but a set of rules, categorised as immutable, mutable rules and communication rules.[6]

There is a large set of features that the Bitcoin protocol comes with which are a straightforward capability which can be used by enterprise applications without building any complicated layer on top. Though the features are listed individually, the best way to understand these is together, as each feature compliments the other and works together for the completeness of the protocol.

The salient properties of the Bitcoin protocol, as implemented by the BSV[1] blockchain that make it a transformative innovation are:

Immutability

The BSV blockchain is an immutable ledger of transactions and data, with each block timestamped[7]. In mathematical terms, blockchain records permanent evidence that an event 'e' occured in time 't'. The BSV blockchain relies on two concepts to achieve immutability, one is a distributed timestamp server and other is proof-of-work[8].

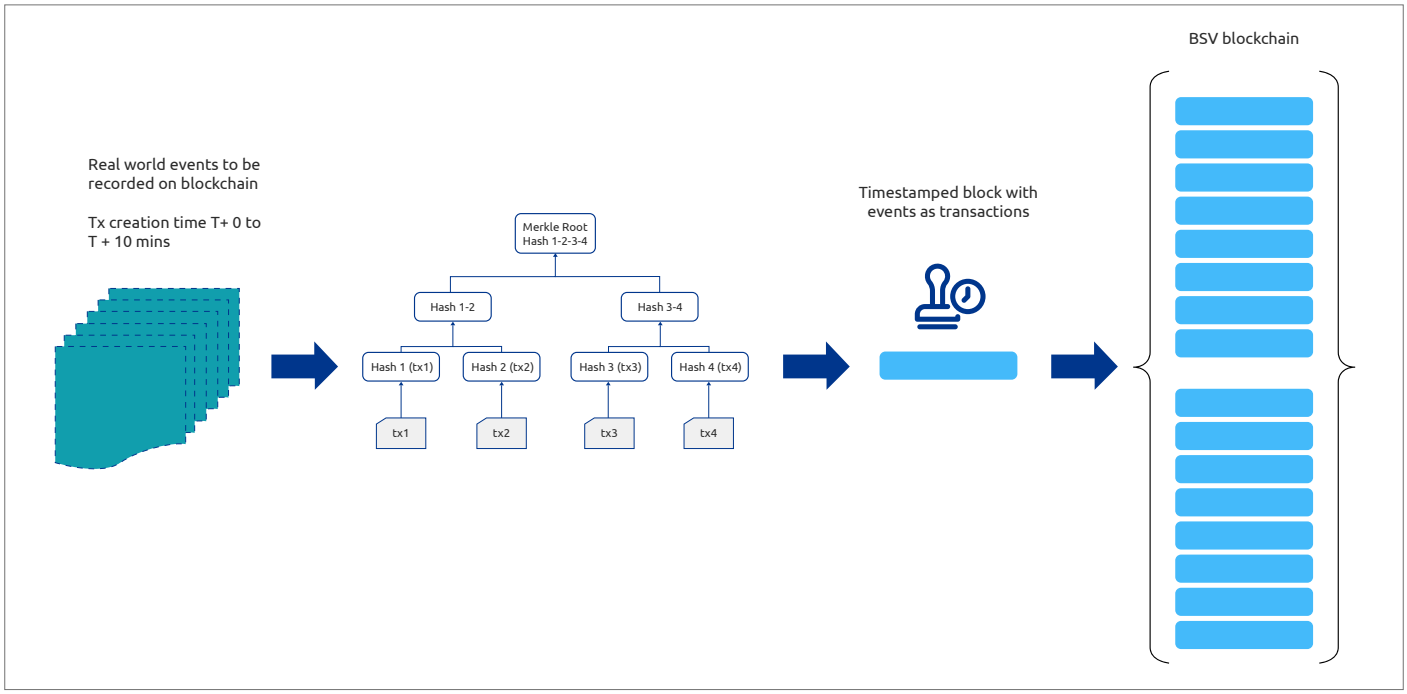


Figure 1.1. BSV as a timestamping server

As a distributed timestamp server, the BSV blockchain hashes the transactions of the block and associates it in the block header along with a unix time value of the formation of the block. This hash is unique to the block and since it is generated from the contents of the block, changing the contents would invalidate the hash stored in the block header at the time of block creation.

[1] As some of the Bitcoin node implementations have altered its fundamental qualities, we focus exclusively on the BSV blockchain's properties.

Generation of this hash requires miners to invest in CAPEX and spend on considerable OPEX in forms of recurring electricity bills. For a miner to prove that the block was mined by it, it needs to exhibit proof-of-work, which is easily verifiable by other miners in the network. Proof-of-work is a form of cryptographic challenge or puzzle, which requires extremely high hashpower (computational resources) to solve and at the same time very easy to verify once a solution is available. As the name suggests, it proves to the network that the miners have spent a significant amount of computational efforts

Distributed system

For consumers and businesses, a node network is a distributed network. The protocol mandates for each node to agree and have an identical copy of the blockchain. Each node executes an identical set of immutable rules, i.e. programmed as part of node software. This provides resilience to the network as there can never be a single point of failure affecting end users.

It also adds trustlessness to the network, as end users do not have to trust a single node for validating integrity of transactions.

Lastly it makes the system economical for end users, specifically for businesses as they would be charged a fee for each transaction, which in turn can be negotiated as miners compete with each other to get more and more transactions. The nodes within themselves are hyper-connected and form a small world network and as the ecosystem grows and matures the network topology between the nodes will emerge as small world network, or Mandala network. A visualisation of the overall network that forms is shown in Figure 1.2.

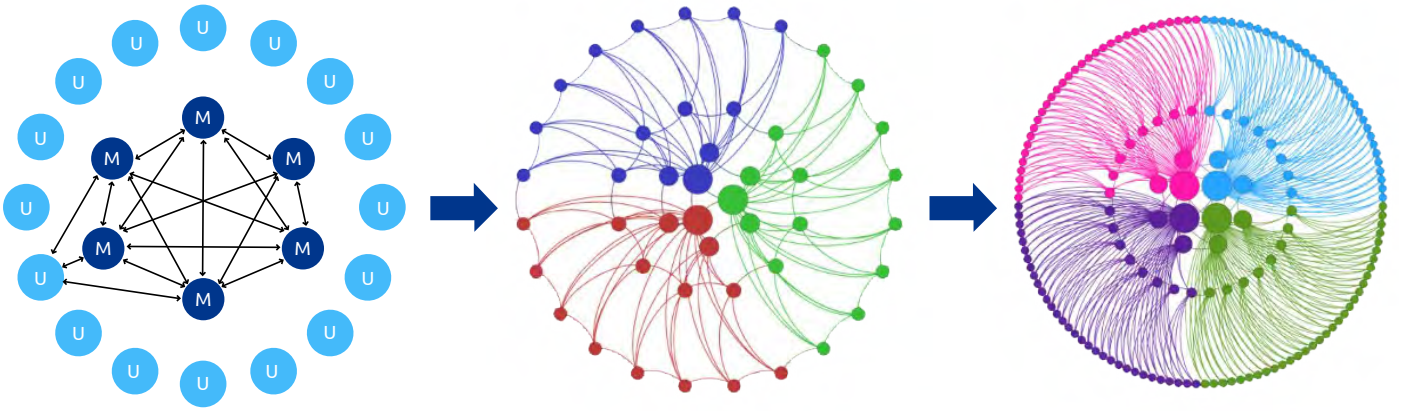


Figure 1.2. BSV's distributed small world network

As shown in the image, the peer node network becomes the core of the BSV network. User nodes are lightweight nodes which come and go based on their need, accessing the BSV network using their connectivity with one or more miner nodes.

Privacy and accountability

BSV handles privacy by separating identities of the two parties transacting from the transactions. For transferring bitcoin, the sender needs to sign the ownership of the coins using a private key and in the same transaction, the receiver's public key is associated with the transferred coins. This provides pseudonominity to the users while the ledger remains transparent and auditable. Additionally, the immutability of the ledger implies accountability.

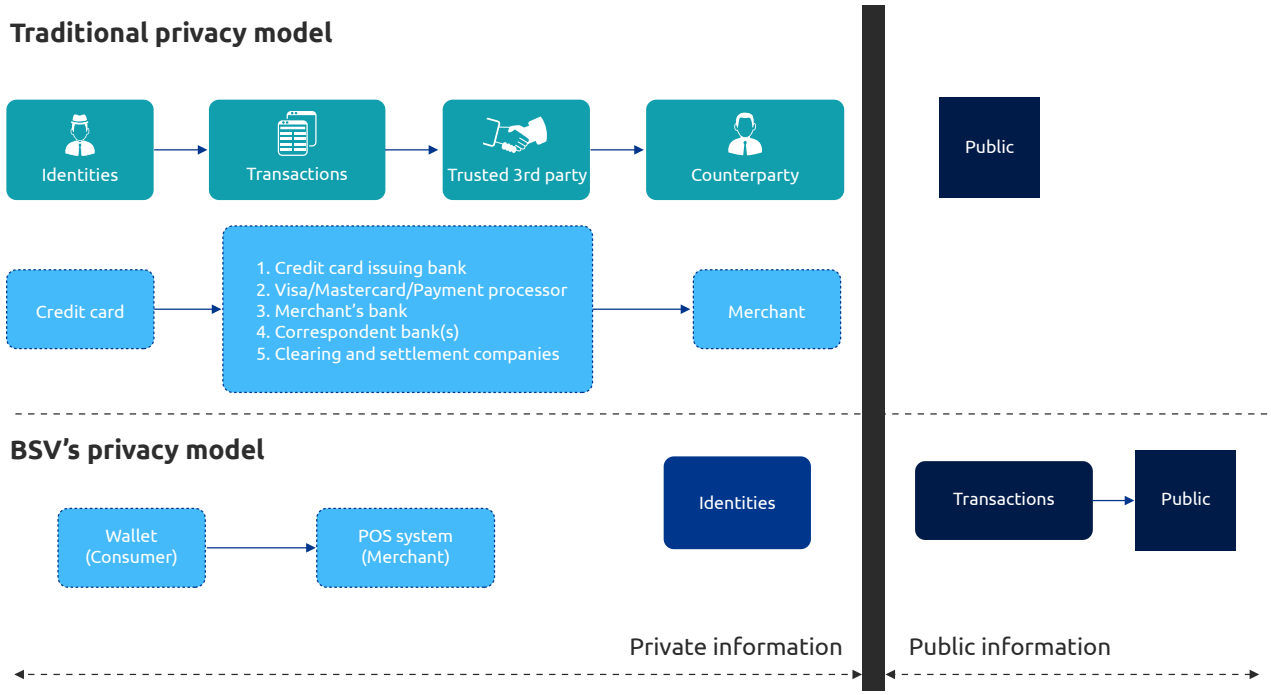


Figure 1.3 : Information flow exhibiting privacy model in current digital ecosystem versus the BSV blockchain

As the transactions in the block cannot be erased or changed, it stores the digital karma of individuals and businesses forever, bringing all to accountability. Any illegal or criminal activities done using BSV can be easily traced via the immutable evidence trail and hence subject to action by the law enforcement system.

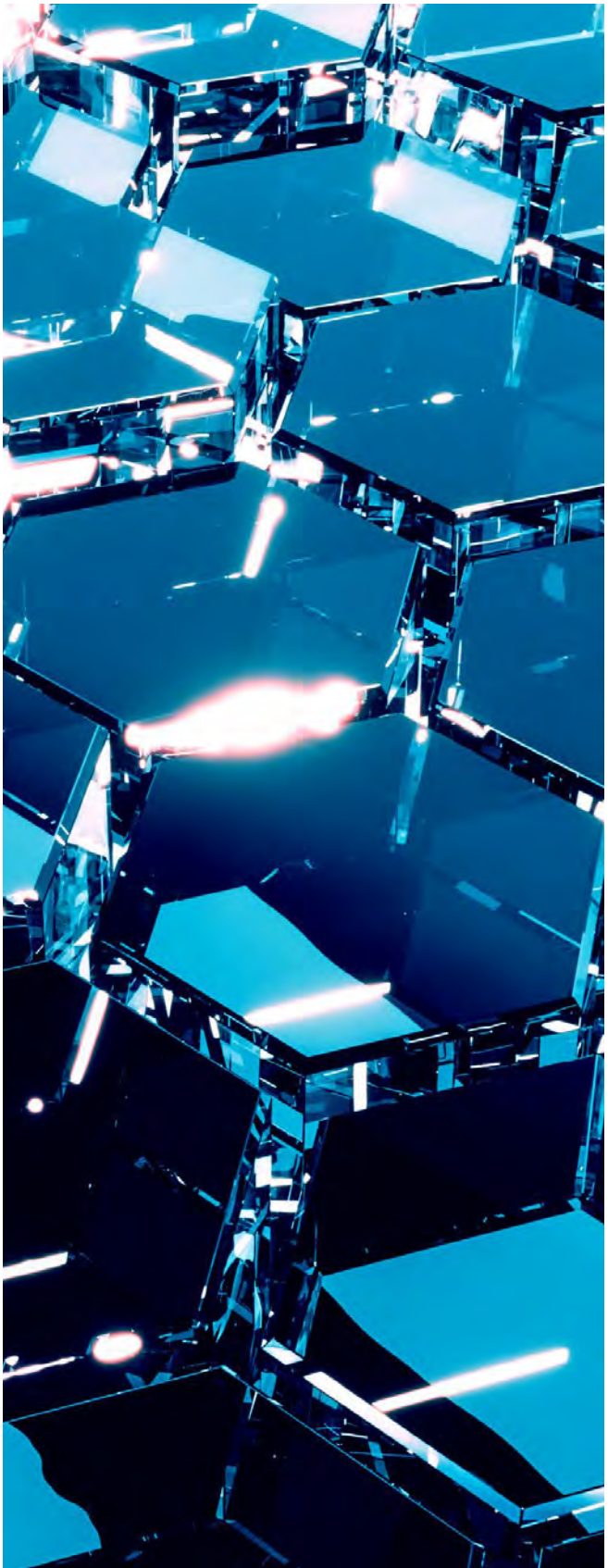
Security

Like many existing systems, security is both the responsibility of users and protocol. For individuals and business, there are recommended best practices to be followed which are not in the scope of this topic. From the protocol perspective, BSV implements the philosophy of economic security[9]. There are multiple facets to it.

1. **The keys that provide access to ledger databases**, are not stored in the blockchain itself and are distributed across diverse systems which makes it infeasible for any adversary to attack the system. This is unlike existing systems in which sensitive information such as credit card details are stored in a centralised database which makes it easy to hack.

2. **Integrity of the transaction, specifically double spend**, is the responsibility of the miners and protocol mandates that not only the miner who mines the block validates it but also the majority of nodes perform the same validation before the block is accepted as valid.

3. Finally, the aspect of **economic incentives is tied to the proof-of-work**. It takes huge investment, in terms of hash power, from nodes to mine blocks and keep running their business profitably. The protocol mandates nodes abide by the same set of immutable rules to form a consensus. If a node decides to waste hash power, in attempting to get a invalid transaction accepted in the block, they limit their revenue generating ability, as other nodes will not accept the block. If any node decides to overwrite the transaction in blockchain, protocol requires it to build a new proof-of-work chain and outpace the constantly lengthening chain-tip of their blocks to be considered as valid. This makes it computationally impractical to change or erase transactions captured in a block



Byzantine Fault Tolerance (BFT)[10]

In distributed computing, the Byzantine Generals Problem deals with establishing consensus among nodes so that reliability of the system remains intact. The protocol for validation and validations of transactions by miners provides the game-theoretic solution and also challenges assumptions made to simplify the stated Byzantine Generals Problem. The consensus mechanism used in BSV is 'one CPU one vote', which implies the percentage of voting share for miners in the network depends upon the number of CPUs that miner has and utilises continuously.

In terms of Byzantine Generals problem, where each node or miner is a General, the vote share is directly proportional to the strength of army, i.e. the number of CPU, a miner has invested in and utilises to solve the puzzle to compete with other miners. This investment, referred to as 'having skin in the game' in layman terms, ensures the honesty of miners towards the network and they act to keep their incentive intact, effectively providing an economic solution for the BFT problem.

Scalability

With respect to scalability of Bitcoin, enterprise product design needs to be cognisant about two facets - block size and individual transaction size.

Block size

In 2020, BSV main network processed 309 MB containing over a million transactions which was quickly followed by 369 MB containing 1.3M transactions. At the time of writing[2] the biggest block mined was 3.8 GB in size and currently the network maintains an average block size of 100 MB. The main network has comfortably handled a peak of 5,124 TPS and the scaling test network has handled a peak load for 19,308 TPS.

By the end of 2022, re-architecting of node software from a monolith to Microservices, known as Teranode is planned to be released which aims to deliver exponentially scaling capabilities. Currently a minimum TPS of 50,000 to maximum 100,000 capability already demonstrated in testing environments using Teranode.

Teranode release employs horizontal scaling which can enable further higher throughput from these test results making it the most scalable blockchain that exists as of today[11].

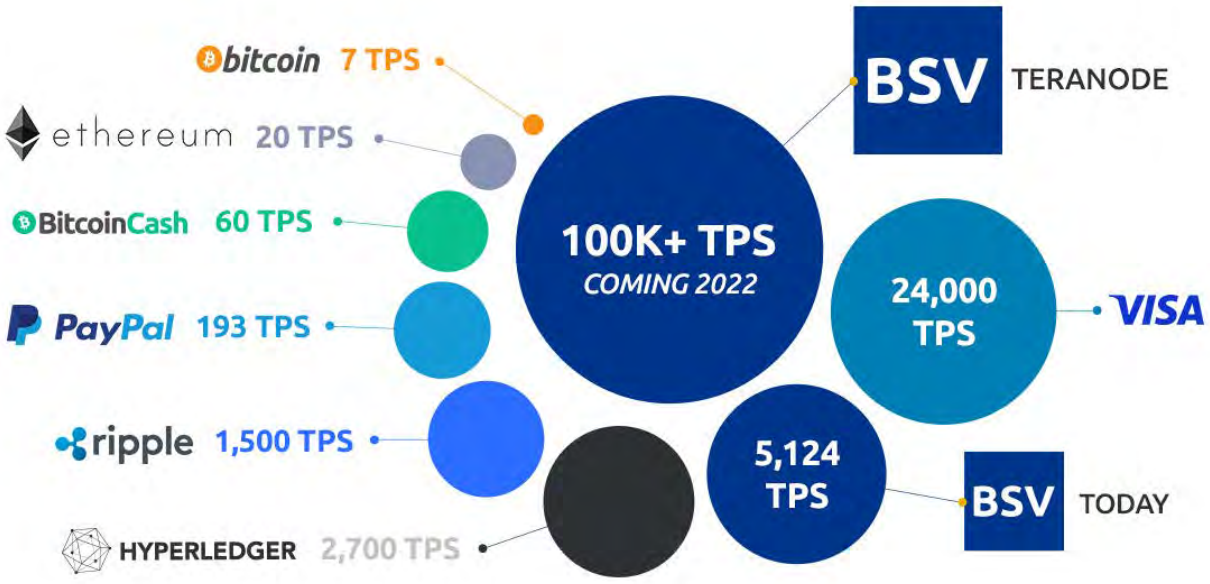


Figure 1.4 : Transaction processing capability comparison of BSV with other blockchains and existing PSPs

One of the pivotal consequences of allowing big blocks is that it reduces the transaction fees for the miners and in turn enables microtransactions and nano-transactions.

[2] March 2022

Individual transaction size

The BSV blockchain also offers scalability on transaction level where it uses a native language called Script for supporting various contract types between entities exchanging value in the transaction. These scripts present in transactions contain not just payment information (digital signatures, value etc.) but also can contain data. There is no limit imposed in the protocol on the number of inputs, or outputs and each script can have up to a maximum of 4.2 GB data items using something called the OP_PUSHDATA method. Of course in reality it is restricted by miners who define local transaction processing rules limiting the supported sizes of data in input/outputs. Miners also support zero value outputs which can have supported data blobs present in them called the OP_RETURN method. This allows BSV transactions not just to work as payment but also data transactions using the BSV ledger to become a real data ledger.

Trustless peer-to-peer (P2P) exchange

There are two important features of the protocol which enable P2P transactions between non-trusted parties. One is Simplified Payment Verification (SPV) and the other is nSequence value for an input in a transaction. It is notable that both these features enhance scalability and cost-effectiveness for an enterprise using the Bitcoin protocol.

SPV - Simplified Payment Verification

SPV provides a proof of publication in the blockchain[12, 13], hence giving certain assurance to merchants for performing the transactions with a non-trusted party. To prove the integrity and ownership of the transaction, SPV relies on validating the Merkel proof of the previous transaction against the Merkel root of the block which contains the transaction. This feature of the protocol lets the product, built using blockchain, validate transactions, without running a full node and hence save cost. It also brings in processing efficiency by providing validations at client side for merchants and businesses, before a transaction is submitted to the miner.

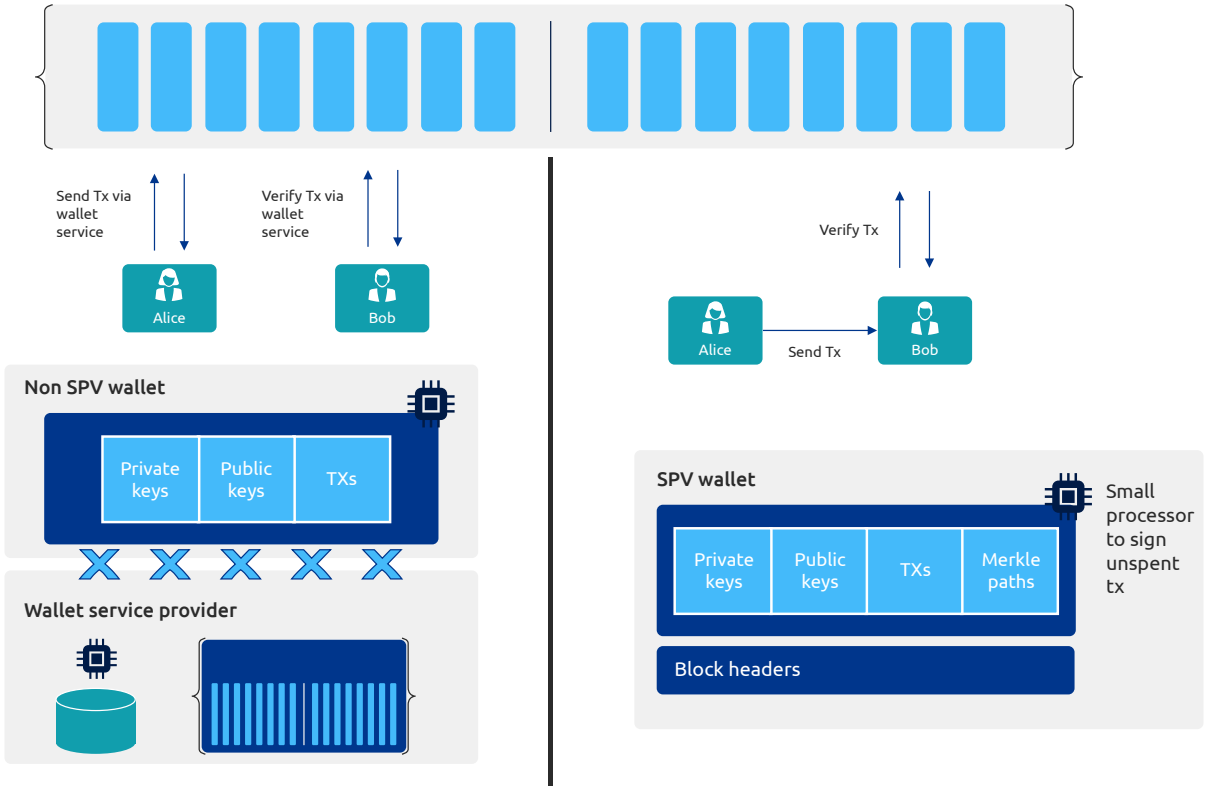


Figure 1.5 : SPV and non-SPV peer-to-peer Exchange

This in turn leads to enhancing scalability for both enterprise product and network, as the number of requests to the nodes are reduced, resulting in less network throttling. Despite the name, SPV can be used for both payment and data transactions.

nSequence number

nSequence number lets create versions of non-finalised transactions (Payment Channels[14, 15]) and enables two non-trusted parties to negotiate and perform trade.

Each transaction in BSV can have more than one input and each input has a parameter nSequence. If the value of nSequence is anything other than UINT_MAX i.e. 0xFFFFFFFF then the miner will not recognise this transaction as final and persists it in the mempool. The miner will further check for the value of parameter nLockTime which specifies a time in future when the transaction becomes valid.

The two parties negotiating can submit multiple versions of the transaction and the transaction version with highest value of the sequence number is considered final at the time of maturity i.e. when nLockTime expires. Alternatively if the transaction is submitted with nSequence number as UINT_MAX, the transaction is committed to blockchain irrespective of the nLockTime expiration. This provides scalability as all transactions are peer-to-peer and also cost effective as there is no transaction fee charged unless the transaction is committed to blockchain.

The BSV blockchain as a global enterprise blockchain

From the inception to design to implementation, the BSV blockchain considers the requirements for enterprise adoption. Currently there are 400+ enterprises[16] of varied sizes within the ecosystem, across a broad range of domains.

Looking at the current OSI model of the Internet, the session, presentation and application layer are seen to be already starting to be disrupted by the Bitcoin protocol. Currently, work is in progress with 1,000s of patents and many emerging technology companies who are envisioning and building new types of business applications where micropayments are the norm and a pay-per-action revenue model of operations is starting to develop. Metanet and the below diagram captures a vision of what future that this ecosystem is building and in future this disruption could even impact the further layers of the model.

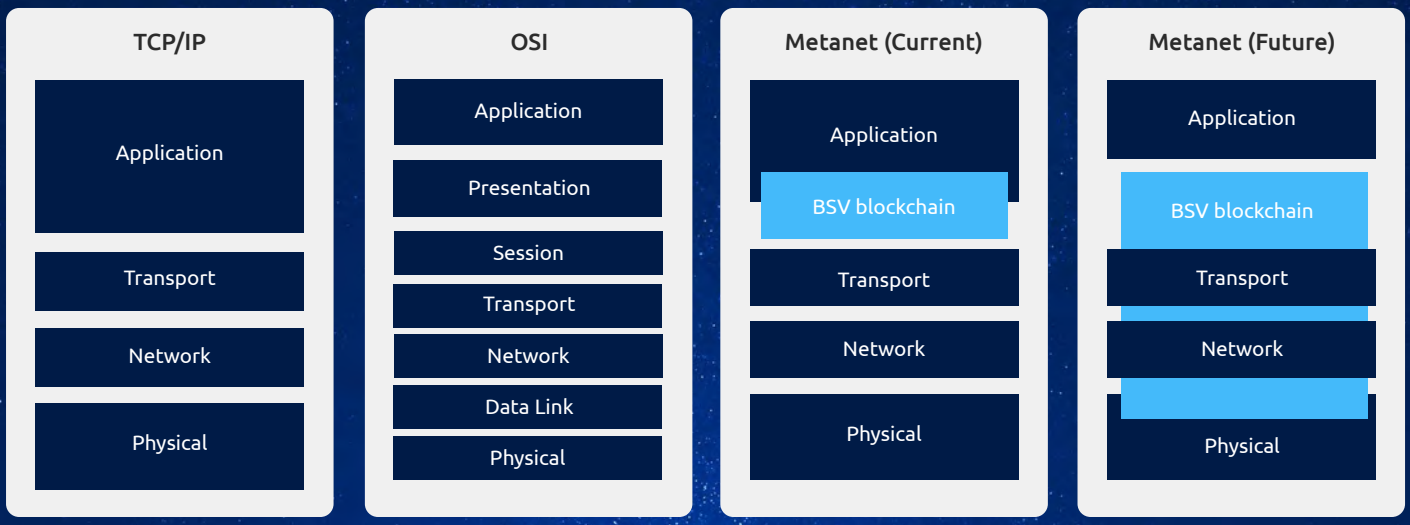


Figure 2.1 BSV disrupts various layers represented using the OSI model of the internet, today and in future.

To understand the enterprise products that can be built using the BSV blockchain, we can abstract the idea of product category and it would provide a broader perspective for further enhancement and creativity.

Products that are built or can be built using the BSV blockchain can be grouped based on the capabilities that are implicit or explicit. Let us look at it in a bit more detail as described in the table below.

Product category	Description	Properties	Industries
Implicit	Protocol native features that can be used in many domains and benefit enterprises straight-forwardly	Immutability, privacy and accountability	Triple accounting ledger, healthcare, banking financial service and insurance, supply chain management, public sector
Explicit	These products are not very apparent for businesses but the benefits are game-changing	Microtransactions, scalability	Social media[17], metanet, decentralised autonomous corporations, big data and AI, internet of things

Table 2.1 : Capabilities gained by enterprises with the BSV blockchain

The BSV blockchain's implicit capabilities

Recalling the features listed above for the protocol, it is not far-fetching to claim the plethora of enterprise products can be envisioned using bitcoin. Below are a few native features of the protocol which many domains can benefit from straight away.

Notarisation

A notary[18] provides authentication helping to secure records allowing nearly any format of transaction, document or event to be verified. Since the process involves law and is as per the jurisdiction of every country, public blockchain can help facilitate the process and automate in a manner due to public timestamped immutable recording of an event, which was not possible in the past.

While the documents can be stored on more suitable datastores, the proof of existence of the signed and validated document can be hashed and stored on the blockchain. The verification of this proof of existence becomes seamless as blockchain is public and hash provides the integrity.

The ownership of the document, at a particular time, when the transaction is recorded on blockchain, is provided by the fact that document signing is witnessed as per the laws. This domain can be applied to use cases where transfer of document ownership is required or KYC/KYB is needed. Together with features of payment channels, the business workflows can be automated.

Triple entry accounting ledger

Current commerce and accounting uses double entry accounting which is prone to fraud due to lack of governance and traceability. In order to circumvent the gap, an audit strategy governed by laws is required. This makes accounting laborious, costly and time-consuming.

With the demands of Internet commerce, digital cash and trade between more than one party, the solution popularised by Ian Grigg[19], was a triple entry accounting ledger. In this system, an agent keeps the record of complete transactions and hence maintains the ledger, apart from the two or more parties maintaining their individual bookkeeping ledgers.

The requirements of psuedonominity, transaction signing, peer-to-peer communication, transaction permanency and most importantly timestamping all the transactions chronologically are natively supported by the BSV blockchain. Not only it gives huge benefits to enterprises to prevent insider fraud but it also provides an accessible and easy tool for government and external agencies to audit the accounting.

Further, the same[20] system can be used to create sub-ledgers by account and miners or another service provider can be engaged to maintain, enforce a set of rules, and generate reconciliation reports.

Electronic Data Interchange (EDI)

EDI or Electronic data interchange is a fundamental technology that has existed since the 1970s and is at the heart of finance, commerce and supply chain. There are a large number of EDI standards and messages based on usage, jurisdiction and industry that are heavily used today in every transaction that happens.

One problem with regards to security and privacy while using EDI is the usage of Interchange envelope/message which is a trusted middleman in the exchange. Bitcoin's data transaction capability mimics EDI but with all the benefits that the Bitcoin protocol brings. Using Bitcoin, the same EDI schema (X12, EDIFACT etc.) of a message can still be used by embedding it in a transaction and using hierarchical keys[21] which firewalls the identity to exchange these messages. In a typical exchange, One entity can prepare the Group envelope[22] and send that directly to the receiving entity without the usage of an Interchange envelope[22]. Such implementations will transform the electronic message exchanges and hence the way trade is done as we know it, globally.

Public sector [23,24]

Given the transparent immutable ledger that the BSV blockchain is, it provides a powerful tool to honest governments in implementing a traceable yet private ledger.

Tracing money with blockchain not only enables legal and legislative controls within the country but also operates across international jurisdictional lines. This enables the government to not only utilise the easiest platform for governments and tax authorities to ensure compliance but also stops corruption and fraud. In particular, the traceability of all payments in BSV provides a scenario where any individual that attempts to falsify tax records, or to underpay tax illegally, could be quickly determined. Additionally, payment of owed taxes, such as income tax, VAT/GST etc. can be automated and settled instantly.

Combined with monetary transactions, the government can implement asset tracking on blockchain such as land registry, which would give them a transparent, auditable view for ownership and movement of assets. Regulations such as Anti-money laundering (AML) and Know Your Customer (KYC) can be easily implemented as it exists today. Using features such as tokenisation, sub-ledgers and payment channels, sophisticated products can evolve.

The consequential benefits that follow for governments using blockchain based products are that businesses can remit tax instantly to the government, remove dependencies on intermediaries, and cut the government's need to establish a large bureaucracy to seek and punish offenders. From the citizens perspective, since the ledger is open and transparent, blockchain can be easily used to monitor government actions to align and spend funds for the benefits of the country or state.

Further, the BSV blockchain can be used to transform press/media as it exists today. In the current ecosystem, with multiple sources of information available, it creates a demand for countries to hold people accountable for activities such as anonymous trolling, spreading fear via fake news, and more seriously countering controversial scenarios on manipulating information during election campaigns. Using blockchain as the platform for all such agencies, it guarantees privacy to the users and businesses, giving them freedom but also holds them accountable as all the actions are traceable.

The BSV blockchain's explicit capabilities: scalability, public yet private

In the current ecosystem of blockchain providers, either blockchains have scalability issues which make it unsuitable for enterprises or they've steered away to a 'private' or 'permissioned' model that defies the benefits of the technology.

And so, the BSV blockchain's distinguishing characteristics in this category are its scalability and public nature.

While scalability has been discussed above, public blockchain helps achieve interoperability between products. When data silos or data monopoly are one of the biggest challenges enterprises face in the current digital world, the BSV blockchain can be effectively used to address the challenge. Let us look at some of the capabilities that come to life when the BSV blockchain network is used for trade and commerce.

Tokenisation[24]

Tokens are a way to track assets. The most common implementation in the software industry is security tokens or access tokens, which give authorisation to software resources such as API for a predefined amount of time, given the user satisfies authentication criteria. Alternatively the most common implementation in financial markets is tokenisation of a company's shares.

Tokens in isolation do not hold any value, but they provide an immense level of traceability and transparency when associated with other systems. Consider a token associated with each part of the car at the time of manufacturing, from small to big, windshields to engine - every part is tokenised. The utilisation of tokens becomes important for the requirements of validating the authenticity of each part during sale, resale, insurance, etc.

The way to store this big data on blockchain is a series of meta structures pointing to tokens, possibly Merkelised structures. With the Internet of things becoming mainstream, it adds value to not look at every device, but rather at individual components. Organisations could view manufacturing information as when they perform customer surveys about reliability over time, such as if parts of a car work after a recall event. It is not only granularity of data that adds value here, it is also honest data as it would utilise blockchain's native features.

Though the example of tokenising the parts of a car is pretty simple, the concept becomes very interesting when applied to industries such as finance and supply chain management. Within the highly regulated financial industry, any asset which is tradable can be tokenised i.e. currencies, securities, goods, stocks, real estate, equity shares etc.

Recording transactions on blockchain would provide transparency, reliability due to immutability, auditable title transfers and revenue flows. It could even reduce the entry barrier for small investors, for example if a share value for one share for a particular organisation is too high for one investor, tokenising the share would mean investors can invest only in a part of the share, as per capacity. In fact, every dematerialised financial derivative and security is already tokenised. But by using blockchain, it becomes transparent and easily auditable.

In the supply chain industry, visibility is a challenge given the nature of complex transactions involving information flows, inventory flows and financial flows. The synchronisation of these flows is generally manual and involves costs for audits and inspections, increasing both cost and time-spent. When blockchain is used, all the units of inventory, orders, loans, bills of lading are tokenised, giving each a unique identifier.

Since the transactions are recorded on global blockchain, the multiple parties transacting for exchange of value benefit as they get access to accurate and one single view on the flow of information. This visibility is not limited to the partners within the supply chain, it also gives transparency to the end user, by giving them information like transparent details of ingredients used in the dish served in dining, which serves as a business differentiator.

Decentralised Autonomous Corporations (DAC[25, 26])

Currently the structure in organisations is hierarchical, with decisions made by top tier leaders which percolates downwards within the defined hierarchy. The concept of DAC challenges this idea and is defined as an organisation which runs via code and software, minimising human involvement, for both strategic decision making, governance and operational processes.

DAC are distributed and are not vulnerable to single point of failure. There are two necessary but not sufficient components that collaborate to form a DAC.

Autonomous Agents

The requirement to implement a mechanism of self-regulation necessitates the use of an Autonomous Agent (AA). In simple words, AA is a software capable of taking autonomous actions in order to meet its design objectives.

There are two classes of AA required for any organisation to attain autonomy - Voting AA and Task AA. Voting AA as the name suggests has the power to vote. The shares of an organisation are represented as tokens which grant its holder ownership and voting rights. These tokens can be exchanged, transferred or generated newly for newly joined members and are issued on blockchain. Task-AAs search for vacant tasks guided by its own preference orders over available tasks. For example, it can select a contractor and submit the contractor's proposal for voting either to the voting-AAs or to the DAC members.

Contractors

AAs do not have the capabilities to manufacture a product, write code, and develop hardware. They require actors in the physical world for this purpose, called contractors.

Using Artificial Intelligence (decision trees, neural networks) and feedback loop incorporated by questionnaires, reputation system, further, a more sophisticated system can be achieved. Also it is important to note that DAC is not about handing over authority and control to algorithms, but to provide more freedom to humans by automating coordination in distributed global organisations.

With respect to implementation, DAC boils down to secure multi-party computation, synchronised using blockchain. The agents are coded as payment channels or famously known as smart contracts.

Enterprise products enabled by microtransactions [27]

In the current ecosystem microtransactions are not feasible as the transaction fee does not support exchanging value as low as 1/100th of the cent, whereas in BSV, this constraint does not apply. Microtransactions enabled by the BSV blockchain are bound to bring forth new business models across various industries.

Applying microtransactions to Social Media applications

In the context of social media, the current ecosystem provides the exchange of information without charging any monetary value from the users. This forces the organisations to generate revenue by sharing and selling personal information of the users, displaying unwanted advertisements, and at times, psychologically manipulating the users by influencing their choice. Another aspect to consider here is that the owner of content is the platform hosting the content, giving no value or benefit to the content creator. The simplest way to look at this situation is that when a content creator publishes anything on social media, the reward given in terms of 'likes' or 're-publishing' has no tangible value.

The BSV blockchain solves the above two issues - first by providing immutability to anything written on blockchain and hence content cannot be modified or manipulated, second by enabling microtransactions. A real world transaction at the time of writing demonstrates a microtransaction is shown below.

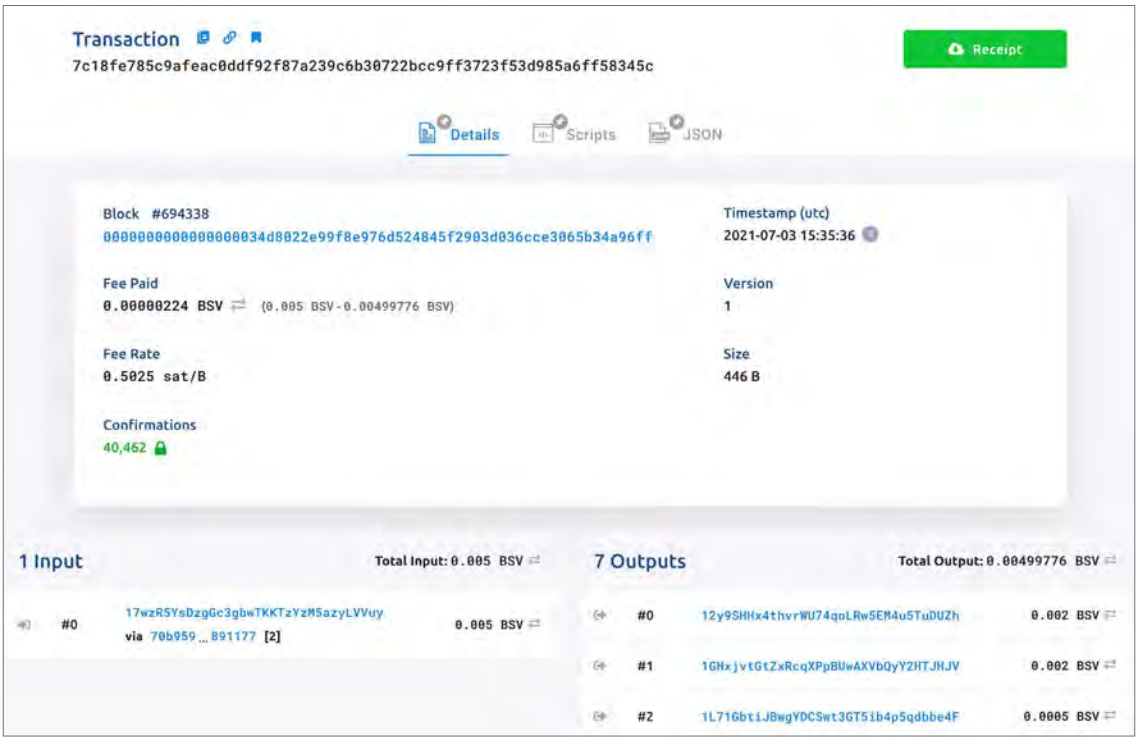


Figure 2.2 A typical Bitcoin SV (BSV) transaction : Source

The capability of microtransactions vis-a-vis micropayments provided by the BSV blockchain lets content owners monetise the content and gives users the power to own their private and personal information.

Social media is just one such industry. Let's briefly consider other domains that could be disrupted by the enablement of microtransactions.

Applying microtransactions to healthcare

Within healthcare, patients' data is currently owned by the digital platform they subscribe to. By utilising blockchain, the owner of a patient's record is the patient itself and using microtransactions, they can even monetise the data by selling the same for research.

Applying microtransactions to software development and IoT

In the developer ecosystem, open-source libraries, frameworks etc., can be charged via microtransactions benefitting the whole community.

With the Internet of Things becoming more and more pervasive, monetising API calls at granular levels is just one of the capabilities blockchain provides. One such implementation uses micropayments to measure the uptime of the websites and overall network monitoring services. It uses devices such as mobile phones of common people, the service provided by devices is monetised using microtransactions, enabling distributed network intelligence in the most accurate sense.

Microtransactions open up a whole new set of opportunities for enterprises by providing a strategic advantage of benefiting the users in the ecosystem.

Metanet - an Internet built on BSV [28, 29, 30]

BSV is effectively a Mandala network. At the core is hyper connected nodes which is the centre of the multi-layer mandala. On top of it will be the business network who organise keys and sell information access, i.e. wallets commercial, social Internet apps etc. The third outward layer would be simple, lightweight protocol SPV, which will enable peer-to-peer transactions. The outermost layer is of users of the BSV blockchain protocol.

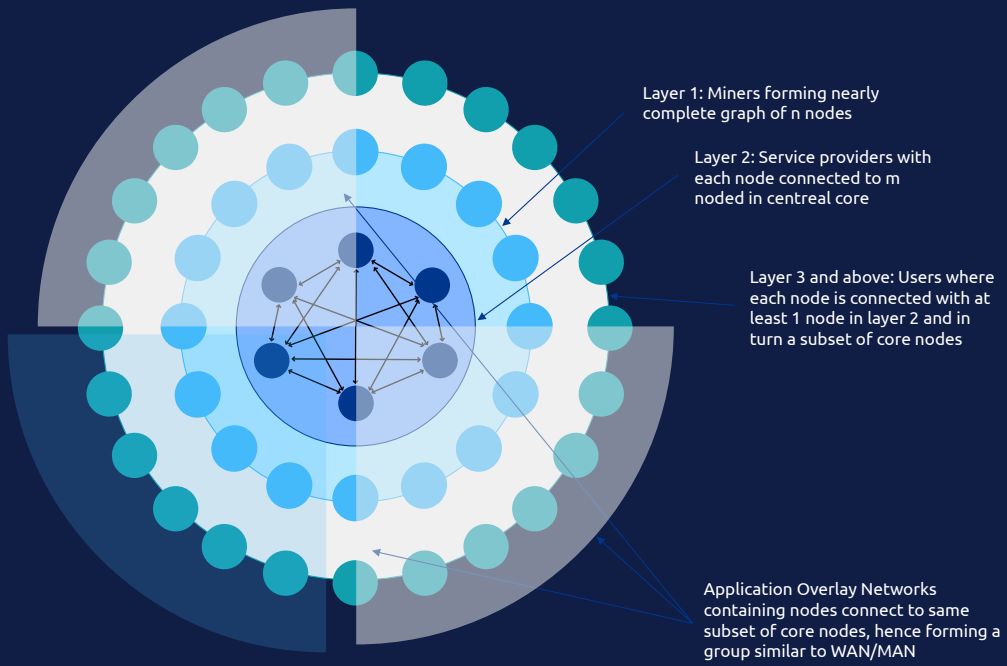


Figure 2.3 : The vision of BSV's Layered Network

Above is the high level ecosystem topology which will emerge with time. Getting into the details of the second layer i.e. business network, it is imperative that enterprises will require a mechanism to collate and organise data efficiently and exploit the commercial usage of underlying BSV ledger.

This is where Metanet and the Metanet protocol plays a crucial part. Metanet, is the term given to value-based Internet. It utilises native capabilities of the Bitcoin protocol, such as immutability, right ownership of data and micro transactions.

Metanet protocol is a protocol for structuring data within the on-chain Internet architecture. Digging deep into the native data structures of the BSV blockchain, it can be inferred that blocks and transactions are nothing but directed acyclic graphs (DAG). In the steady state, blocks have an in-degree and out-degree of 1 whereas transactions can have both in-degree and out-degree 1 or more. Metanet protocol uses the same native properties of data structure and provides an extremely efficient mechanism to store and retrieve data.

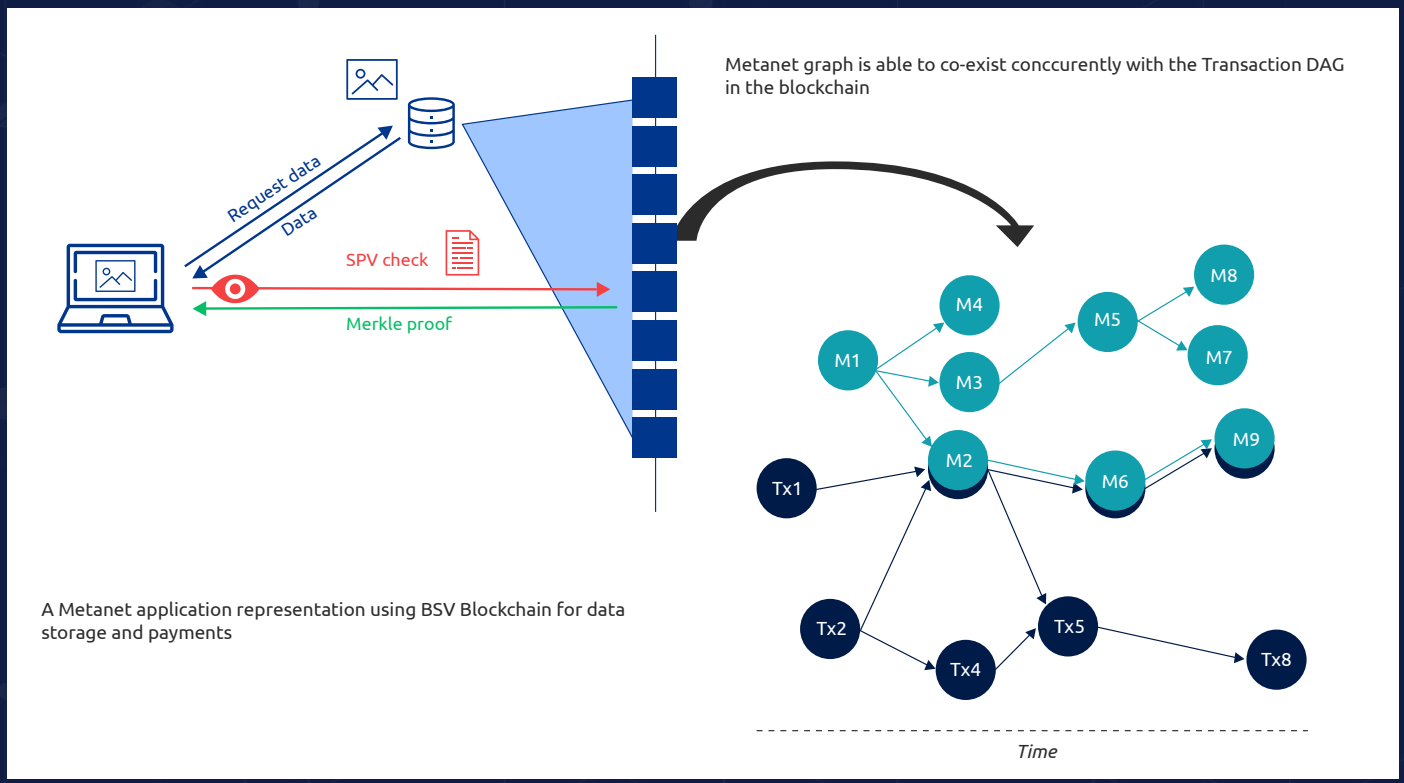


Figure 2.4 Metanet application architecture and Metanet DAG built on top of Transaction DAG

Applying Metanet to securing the integrity of University qualifications

Consider an example of a university storing the records of students such as credits using a DAG and another social media website storing user profile, its network in one DAG and timeline in another. Both being on blockchain, provide integrity of information which is easily verifiable without involving intermediaries or any third party service as it is achieved in the current ecosystem. The differentiator here is that every node has access control via permissions controlled by the owner of the data, rather than the platform such as social media.

Applying Metanet to the healthcare and public sectors

The capabilities of Metanet can be further applied in industries such as healthcare and public sector too, but it is not limited to these domains. Within healthcare, the patient's medical records and history can be stored using metanet protocol which not only provides one view to all the associates such as medical practitioners, pharmacy, health insurance etc. but also it has potential to resolve much more critical aspects such as the opioid crisis.

Within the public sector extending metanet protocol, an establishment such as the central government can create separate sub-ledgers such as election ledger, real estate registry ledger, cash ledger, healthcare ledger and so on and link these to its citizens. Each ledger is inherently a graph structure and provides native benefits of blockchain.

Within the digital world, it is difficult to see data in silo, most of the data[31] is highly correlated and can be structured in a hierarchy vis-a-vis graph. It could be as simple as a version control repository, content management system, or organisational hierarchy, as complex as an e-commerce site, financial data, healthcare etc. Metanet protocol provides efficiency to the complete ecosystem as whole, by using native features of a turing complete machine[32, 33] known as the BSV Blockchain.

Conclusion

In terminologies of artist and aesthetics there is a famous saying ‘Simple is hard’. The same principle applies to the core foundations of the BSV blockchain.

With the evolution of the Internet, the current digital ecosystem is hampered by

- Increase in cost due to sophisticated security measures
- trusting the intermediaries and
- data and money operating separately

These aspects not only make building enterprise products a complex affair but have led to a saturation with respect to new business models.

Redefining security

The lesser known fact about security is that security is about economics. Though counter-intuitive, it is simple to understand ‘Criminal groups act as profit seeking enterprises, and the ability to shift the economic returns away from this activity results in a lower amount of crime’. [34]

The network processors aka miners abide by a centralised, stable, set in stone, protocol like the Internet and compete with each other to earn incentives. These incentives are aligned to the securing of the network. The larger the network grows, the more secure it becomes. For global enterprises, it means less cost on security.

Expanding the cost savings, the sheer nature of distributed, immutable, verifiable, auditable ledger can save huge amounts of operational costs on governance, compliance. With distributed global economy, organisations rely on data for decisions, flowing in from multiple data sources. The aspect of one global chain, having immutable data makes it trustworthy and reduces the friction between multiple parties giving enterprises visibility and one view of records.

Redefining trust

The BSV blockchain shifts the paradigm of trust by providing capability to perform transactions peer-to-peer, in a transparent manner, which is not possible in the current ecosystem without involvement of central banks for payment processing and settlement, or third parties for audit, reputation, contract negotiations etc. The scalability and robustness of the system provides instinct transactions rather than relying on end of day settlements or batch processing. Not only this, micropayments which was never possible ever today, due to high transaction fees, is a game-changer. It augments the current customer base giving a strong[35] strategic advantage to businesses.

Unification of Bit and Coin

The Internet was built with the gap of keeping data and money as separate systems, which lead to organisations seeking profits from the privacy of users. It is one system that records events globally and immutably, making payments just a specific type of events and bridges the existing gap of monetising the data for a value as small as 1/100 of the cent. Bitcoin as the name has both 'bit' and 'coin' i.e. data and money. Given data is the most important commodity in the current world, the BSV blockchain revolutionises the way this commodity is traded.

Built on the strong foundation of scalability, stability, security and instant transactions, the BSV blockchain promises to be the right choice for enterprises. It not only revolutionises business models but also safeguards the reputation of enterprises by providing them with fraud-proof capabilities.

REFERENCE LIST

[1] Wright, Craig S, Bitcoin: A Peer-to-Peer Electronic Cash System (August 21, 2008).
Available at SSRN: https://ssrn.com/abstract=3440802 or http://dx.doi.org/10.2139/ssrn.3440802

[2] Bitcoin Wiki accessed on 3rd of July 2021:
https://wiki.bitcoinsv.io/index.php/First_seen_rule

[3] Wright, Craig S, Investigation of the Potential for Using the Bitcoin Blockchain as the World's Primary Infrastructure for Internet Commerce (November 6, 2017).
Available at SSRN: https://ssrn.com/abstract=3065857 or http://dx.doi.org/10.2139/ssrn.3065857

[4] Bitcoin Scaling news release accessed on 3rd July 2021: https://bitcoinassociation.net/bsv-proves-that-bitcoin-scaling-works-surpasses-btc-blockchain-in-accumulated-data-size/

[5] Live demo of Teranode node software's scaling capability in a Bitcoin conference on 9th June 2021: https://www.youtube.com/watch?v=i3As9-9uSXs

[6] Bitcoin Wiki accessed on 3rd of July 2021:
https://wiki.bitcoinsv.io/index.php/Protocol

[7] NCHAIN HOLDINGS LIMITED, Time-Locked Blockchain Transactions and Related Blockchain Technology (April 1, 2021).
Available at Google Patents: WO2021059091A1.pdf (storage.googleapis.com)

[8] Wright, Craig S, Proof of Work as it Relates to the Theory of the Firm (June 27, 2017).
Available at SSRN: https://ssrn.com/abstract=2993312 or http://dx.doi.org/10.2139/ssrn.2993312

[9] Wright, Craig, myth and reality - security is really about economics (23 May 2017) accessed on 3rd July 2021:
https://craigwright.net/blog/bitcoin-blockchain-tech/myth-and-reality-security-is-really-about-economics/

[10] Wright, Craig - Satoshi and the Byzantine Generals (24 March 2020) accessed on 3rd of July 2021:
https://craigwright.net/blog/bitcoin-blockchain-tech/satoshi-and-the-byzantine-generals/

[11] BSV Academy: BSV and the promise of enterprise blockchain - accessed on 3rd of July 2021:
https://bitcoinsv.academy/bitcoin-sv-what-it-is-and-how-it-restores-the-promise-of-enterprise-blockchain

[12] Wright, Craig - Merkle Trees and SPV - accessed on 3rd of July:
https://craigwright.net/blog/bitcoin-blockchain-tech/merkle-trees-and-spv/

[13] BiSV wiki - accessed on 3rd of July 2021:
https://wiki.bitcoinsv.io/index.php/Simplified_Payment_Verification

[14] BSV wiki - accessed on 3rd of July 2021:
https://wiki.bitcoinsv.io/index.php/Payment_Channels

[15] BSV wiki - accessed on 3rd of July 2021:
https://wiki.bitcoinsv.io/index.php/NLocktime_and_nSequence

[16] BSV Development Grows To Nearly 400 Ventures, published 21 January 2020 - accessed on 3rd of July 2021:
https://bitcoinassociation.net/bitcoin-sv-bsv-development-rapidly-grows-to-nearly-400-ventures-projects-worldwide/

[17] Charles Ryan X, Video Presentation : Money Button is like the Facebook 'like' button, but it's money, published 08 January 2019 - accessed on 3rd of July 2021:
https://www.youtube.com/watch?v=-2MQEh8Iimc

[18] Wright, Craig - Bitcoin as a Notary (01 Oct 2018) accessed on 3rd of July 2021:
https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-as-a-notary/

[19] Grigg, Ian - Triple Entry Accounting (25 Dec 2005) accessed on 3rd of July 2021:
https://iang.org/papers/triple_entry.html#ref_IG2

[20] Wright, Craig - Ledgers and design (18 Mar 2020) accessed on 3rd of July 2021:
https://craigwright.net/blog/alternative-coins-systems/ledgers-and-design/

[21] BSV wiki - accessed on 3rd of July 2021:
https://wiki.bitcoinsv.io/index.php/Private_Keys

[22] EDI Basics Website - accessed on 3rd of July 2021:
https://www.edibasics.co.uk/what-is-edi/what-comprises-an-edi-document/what-are-edi-envelopes/

[23] Wright, Craig - Bitcoin and Tax (18 Mar 2020) accessed on 3rd of July 2021:
https://craigwright.net/blog/law-regulation/bitcoin-and-tax/

[23] Wright, Craig - Bitcoin is not anti-state - it is pro honest government (18 Mar 2020) accessed on 3rd of July 2021:
https://craigwright.net/blog/bitcoin-blockchain-tech/bitcoin-is-not-anti-state%e2%80%8a-%e2%80%8ait-is-pro-honest-government/

[24] Wright, Craig S and Stephane Savanah, Tokenisation method and system for implementing exchanges on a blockchain (February 14, 2017). Available at Google Patents:
https://patentimages.storage.googleapis.com/16/77/00/b90ef28a5939c3/US20190043048A1.pdf

[25] Wright, Craig S, Decentralized Autonomous Corporation (February 2, 2016).
Available at SSRN: https://ssrn.com/abstract=3305528 or http://dx.doi.org/10.2139/ssrn.3305528

[26] Wright, Craig - blockchain based decentralised autonomous corporations - an overview (17 Oct 2018) accessed on 3rd of July 2021:
https://craigwright.net/blog/bitcoin-blockchain-tech/blockchain-based-decentralised-autonomous-corporations-an-overview/

[27] Sewell, Martin and Joseph, Daniel, System and method for distributing data records using a blockchain (April 10, 2018).
Available at Google Patents:
https://patentimages.storage.googleapis.com/c7/7c/a6/15505725ea9f40/US20210124731A1.pdf

[28] BSV wiki - accessed on 3rd of July 2021:
https://wiki.bitcoinsv.io/index.php/The_Metanet

[29] Lee, Brendan, Elas Ledger: A journey of understanding (July 21, 2020) - accessed on 3rd of July 2021:
https://www.elas.digital/blog/elas-ledger-a-journey-of-understanding

[30] Davis, Jack, Edge Cases: The Metanet Blog(2nd Sept 2019) - accessed on 3rd of July 2021:
https://medium.com/nchain/edge-cases-the-metanet-blog-c0e794d1c9c5

[31] Wright, Craig S, There's Nothing but Data out There (July 24, 2012).
Available at SSRN: https://ssrn.com/abstract=3442166 or http://dx.doi.org/10.2139/ssrn.3442166

[32] Wright, Craig S, A Proof of Turing Completeness in Bitcoin Script (October 12, 2017).
Available at SSRN: https://ssrn.com/abstract=3265157 or http://dx.doi.org/10.2139/ssrn.3265157

[33] Wright, Craig S, Bitcoin: A Total Turing Machine (October 12, 2017). Available at SSRN: https://ssrn.com/abstract=3265146 or http://dx.doi.org/10.2139/ssrn.3265146

[34] Wright, Craig S, Criminal Specialization as a Corollary of Rational Choice (2012) - accessed on 3rd of July 2021:
https://asmedigitalcollection.asme.org/ebooks/book/136/chapter-abstract/24141/Criminal-Specialization-as-a-Corollary-of-Rational?redirectedFrom=fulltext

[35] Wright, Craig - Bitcoin as a Notary (11 Jan 2021) accessed on 3rd of July 2021:
https://craigwright.net/blog/economics/strategic-advantage-and-finding-opportunities/