

STRATIS
BLOCKCHAIN SOLUTIONS

White paper

Contributors: Chris Trew, Guy Brandon
and Nicolas Dorier (Stratis Bitcoin Full Node)

Table of Contents

Summary	2
Blockchain: a distributed ledger.....	3
What is the blockchain?	3
Bitcoin, blockchain 2.0 and the growth of distributed ledger technology	4
Cloud computing	5
What is cloud computing?	5
What is the Stratis platform?.....	6
Overview	6
Architecture and development	7
Architecture of the Stratis Bitcoin Full Node.....	8
Stratis Bitcoin Full Node.....	9
Stratis: key features	10
Stratis Private chains	10
Stratis blockchain-as-a-service (BaaS)	11
Decentralised app hosting	11
Bitcoin, Ethereum, LISK node provisioning	11
One-click deployment	12
Fiat gateway integration	12
Three-tier architecture	13
Stratis consultancy	13
Blockchain consultancy	13
Active development for the Bitcoin ecosystem	14
Scalability.....	15
Bitcoin compatibility.....	16
Conclusion	16
Case Studies	17
Proof of Existence	17
Clearing and settlement.....	17
Creating a private blockchain	18
Fiat gateway	19
Blitz sidechain	19
References.....	20

Summary

Blockchain or Distributed Ledger Technology (DLT) offers a radically different paradigm of storing and managing information online. Decentralised ledgers lack the points of failure and associated security issues of traditional databases and top-down protocols, whilst at the same time posing their own unique challenges for effective deployment and maintenance.

The advantages in terms of costs, transparency, immutability, security and confidence that are characteristic of blockchain solutions mean that financial businesses, government departments and other organisations are exploring applications of all kinds with a view to delivering services more profitably and efficiently. However, reliable deployment of a new blockchain fit for purpose entails extensive overheads in terms of network infrastructure, development, security and ongoing maintenance. Moreover, use of an existing blockchain (such as Bitcoin) comes with numerous problems for a mainstream business, not least because users have no control over blockchain features or future development.

An attractive model for blockchain service provision exists in cloud computing. Cloud services may be tailored according to the needs of the organisation and infrastructure, platforms and software provided as services via web interfaces - without businesses having to take on the maintenance of these themselves.

Stratis will take a similar approach to blockchain deployment, enabling organisations to provision their own private blockchains, tailored to their precise needs but secured on the parent Stratis chain. This approach means there are few unnecessary overheads whilst allowing businesses to secure the benefits of a blockchain-based solution, developing services via powerful APIs and lite web-based clients.

Blockchain: a distributed ledger

What is the blockchain?

A blockchain or distributed ledger is new way of storing and transferring information. Centralised databases have been employed for many years by financial corporations and other organisations to store customer details and record transactions of one kind or another. These are carefully-guarded and closed systems in which only privileged operators are allowed to make entries. When a customer transfers money from one bank account to another, they make a request to the bank to do so on their behalf rather than engaging directly with the database that holds information about balances. Centralisation is inherent in the paradigm.

This carries certain implications. A centralised system is one that by definition has a point of failure. It is also one that implies a power differential because the privileged operators have the prerogative to intervene - for example, by unilaterally reversing a transaction or imposing new charges.

The blockchain offers a radically different approach. The Bitcoin protocol,[\[1\]](#) launched in 2009, established for the first time the viability of transferring value on a peer-to-peer basis over the internet, without the need for a trusted intermediary. Satoshi Nakamoto, the pseudonymous creator of Bitcoin, solved the 'double spend' problem: the issue that digital information can easily be copied, and therefore a centralised authority was previously required to reflect where funds were located.

At its simplest, the blockchain is a digital record stored on a network of computers around the world. Instead of securing information by restricting access, the blockchain shares information amongst all users. Ownership of funds (for example) is cryptographically verified, and the full transparency and mutual ownership of the system means that a bad actor is immediately recognisable as such and any transactions submitted by such a node are ignored.

The decentralised structure of the blockchain brings several key features in contrast to traditional centralised approaches:

- **Transparency:** it is possible for anyone to track the movement of funds from one account to another.
- **Immutability:** once confirmed, a transaction cannot be reversed. No one can interfere with a completed transfer.
- **Low cost:** transaction fees are minimal.
- **Cross-border:** funds can be sent as easily to someone on the other side of the world as they can to someone in the next room.
- **Speed:** due to the flat and transparent nature of the blockchain, transfers show up almost instantly and are typically confirmed in minutes, rather than hours or days.

Bitcoin, blockchain 2.0 and the growth of distributed ledger technology

Although Bitcoin is very successful at transferring value and is an effective form of decentralised money, from the outset it was recognised that the same approach could be used to record information of almost any kind on the same shared basis. As well as cash, strings of characters on the blockchain could represent simple messages, ownership of physical or digital assets or securities, voting decisions, and so on.

This broader application was developed by a number of '2.0' platforms including Nxt and BitShares, amongst others. To date, however, all of these have been relatively limited in one way or another, and lack suitability in their current forms for adoption by real-world financial businesses.

The rise of Bitcoin and similar protocols was accompanied by a rapid re-evaluation by governments, regulators and the financial services industry of the existing paradigms. Due to Bitcoin's position outside of the control of state and financial authorities and its potential for misuse as a tool of fraud, money laundering and other illegal activity, as well as other concerns such as its volatility and the unregulated nature of the exchanges on which it traded, the first reactions tended to be scepticism and concern. However, an increasing number of actors have also recognised the potential of blockchain technology and the broad range of use cases to which the distributed ledger lends itself.

A noticeable shift has occurred towards the end of 2015 and in 2016, with a series of national governments and major banks now actively undertaking research into distributed ledger technology (DLT) as a means of creating more effective money and delivering more efficient public services - not least the UK government^[2], China, South Korea, Goldman Sachs and UBS, amongst others. Around \$1 billion was invested in Bitcoin-related companies in 2015 alone.^[3]

The benefits of blockchain technology for companies and organisations of all sizes and types are becoming ever clearer. However, until now there have been few options for those who wish to deploy or use blockchain technology. They either have to invest the time and funds to create and maintain their own protocol from scratch, or use an existing open platform (such as Bitcoin itself), with all the limitations and problems that entails.

Case study:

Proof of Existence

The immutable and transparent nature of the blockchain lends itself to applications in which the existence of a file or document must be proved for a particular point in time.

Blockchain solutions are already informally used as a kind of digital copyright. Users take a 'hash' - a cryptographic digest of a file that serves as a unique fingerprint - and upload it to the blockchain.... [Read More](#)

Cloud computing

What is cloud computing?

Cloud computing refers to the practice of accessing data and IT resources via a remote provider, rather than relying solely on in-house hardware and software.

In the internet era, businesses and individuals no longer need to purchase and maintain their own hardware, or even run their own software platforms. Instead, these can be housed by third parties in dedicated data centres and accessed as and when required.

The benefits of such an approach are extensive. It means that resources can be allocated and paid for according to need, rather than purchased inefficiently and in advance; economies of scale are inherent in cloud provision. This allows for far greater flexibility and control over budgets, as well as enabling companies to scale rapidly when required. Consequently, almost all of us now use cloud computing in some form, particularly for email (including popular webmail platforms like Gmail and Yahoo) and storage (cloud drives such as AWS, OpenDrive, iCloud, Dropbox and so on).

Although storage is one of the most popular applications of cloud computing, almost any IT resource an organisation needs can be provided in this way. Over and above Infrastructure-as-a-Service (IaaS), which includes servers, storage and network provision, there is a growing move to meet all computing needs via the cloud. Platform-as-a-Service (PaaS) comprises the delivery of development tools and frameworks, databases and execution environments, whilst Software-as-a-Service (SaaS) allows applications to be run from the cloud.

What is the Stratis platform?

Overview

Stratis is a powerful and flexible blockchain Development Platform designed for the needs of real-world financial services businesses and other organisations that want to develop, test and deploy applications on the blockchain. Stratis blockchain apps can be developed in pure C# and can also utilize the Microsoft .NET framework, while also taking advantage of the powerful Stratis APIs and framework. Stratis significantly simplifies the development process for creating Blockchain applications and accelerates the development lifecycle for blockchain development projects. Stratis private chains allow businesses to deploy their own customised blockchains without the overheads inherent in running their own blockchain network infrastructure. Stratis's turnkey solution enables developers and businesses to create, test and deploy blockchain-based applications quickly and easily, all without the costs and security concerns that would otherwise arise from an in-house implementation.

Stratis will be developing a Bitcoin full node in C# utilising the trusted and proven architecture of Bitcoin. The Stratis Platform will then be built on top of this innovative C# fully validating node (tailored to Stratis's own needs) whilst also adding a broad range of powerful new features on top of it. In addition, Stratis will enable the deployment of customisable sidechains.

Stratis will continue to maintain and further develop the Bitcoin version of the NStratis Full Node. The Stratis Bitcoin Full Node and the NStratis framework will be open source, so anyone can inspect it, clone/modify it and use it for their own purposes – contributing to a healthy ecosystem and the mutually beneficial sharing of ideas and development efforts.

Architecture and development

The Stratis platform will be built on the C# Stratis Bitcoin Full node platform and framework. The Stratis Bitcoin Full node will be developed on top of the NBitcoin library, [\[6\]](#) a near-complete port of Bitcoin Core written in C# and .NET by blockchain developer Nicolas Dorier. There will also be a C++ Wallet and full node version based on Bitcoin Core, though the majority of nodes on the network will be NStratis (C#) nodes. NBitcoin is a complete and proven blockchain framework that is already in use, and will enable accelerated development.

Stages in NStratis development will include:

1. Development of the Stratis Bitcoin Full Node
2. Fork the Stratis Bitcoin Full Node for NStratis
3. Implement the required changes to NStratis and port Elements sidechains to C#.

Benefits

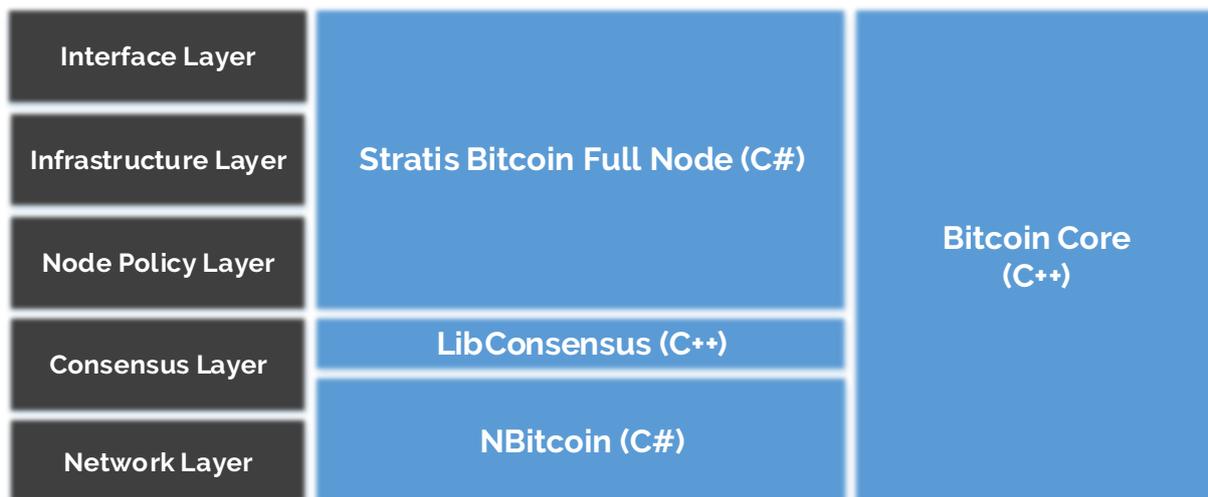
There are several advantages to building Stratis on the NBitcoin platform. [\[7\]](#)

- It was developed in pure C# and it utilizes the Microsoft .NET framework, which is easier to maintain and develop further than the traditional C++ Bitcoin Core source code.
- C# is one of the dominant languages in business application development and it offers several advantages over C++.
- NBitcoin is currently the only cross-platform alternative Bitcoin implementation available. Stratis will upgrade the code base to .NET Core, Microsoft's latest version of .NET that can run natively across even more devices.

Architecture of the Stratis Bitcoin Full Node

A full node is an application whose goal is to keep track of valid blocks in the blockchain. It is essentially composed of several layers:

- **Network Layer** - this deals with which messages are exchanged between full nodes, and how.
- **Consensus Layer** - this sets the (blockchain-wide) rules for what is considered a valid block.
- **Node Policy Layer** - this adds more restrictive rules than the Consensus Layer to prevent DDoS (node-wide rule).
- **Infrastructure Layer** - governs how to store and verify blocks and transactions efficiently.
- **Interface Layer** - API for developers to query the state of the node, and/or user interface.



While Bitcoin Core deals with all these layers in the same source code, Stratis Bitcoin Full Node will only have to deal with the Node Policy Layer, Infrastructure Layer and Interface Layer.

The Consensus Layer is an integral component in the Full Node architecture that should ideally not be modified without industry-wide consensus, since a bug in this layer could cause a fork in the Blockchain and result in loss of funds. As a result of this risk Consensus Layer should be as close to Bitcoin Core as possible.

Bitcoin Core provides part of the consensus code in a library called LibConsensus. NBitcoin will be used to fill in any gaps. To simplify the transition to the Stratis Bitcoin Full Node, all of the RPC API endpoints available in Bitcoin Core will be provided, so users and businesses will not have to rewrite their software to utilise the Stratis Bitcoin Full Node. Stratis Bitcoin Full Node in C# and Microsoft's .NET Framework

Stratis Bitcoin Full Node

Bitcoin was originally developed by Satoshi Nakamoto as a piece of software that bundled together several different functionalities. What users called 'Bitcoin' was at the same time the protocol, the wallet, the key storage, the mining software, the infrastructure for other apps, and the full node.

As with all maturing technology, the Bitcoin industry became more and more specialised, and the functionality once provided only by Bitcoin Core has now been diffused among different players in the industry. An all-purpose piece of software has now been replaced and complemented by multiple specialised parties and applications.

The most basic layer of Bitcoin on which everybody depends is a full node. Changing the code of a full node is a controversial matter, as the consequences impact virtually every company in the ecosystem. On the other hand, if consensus about an improvement to Bitcoin is reached and a new feature is successfully implemented in the full node, then the benefits ripple out across the whole industry. A typical example is the new OP_CSV and Segregated Witness improvement that will allow the development of off-chain payments, which will permit Bitcoin to scale as a currency.

At present, the most popular Bitcoin node is called Bitcoin Core and is developed in C++. The Bitcoin Core team is a group of highly skilled developers who generally adopt a very conservative approach to accepting improvements. One of the reasons for this is that a full node is such a critical component for Bitcoin that any new features require extensive reviews and testing. Contributors to Bitcoin Core generally work on it for free, and their review time is valuable but limited.

We believe that one way to allow improvements to be implemented faster is to develop a full node in C# instead of C++. Highly skilled C++ engineers are in short supply in the corporate world, which tends to prefer higher-level languages like C# or Java. Higher-level languages are also easier to review and learn, and it is harder to make coding mistakes.

As such, we propose that the Stratis Bitcoin Full Node will be based on the NBitcoin framework, which is the most complete and portable library for developing blockchain applications and platforms in C# and Microsofts .NET.

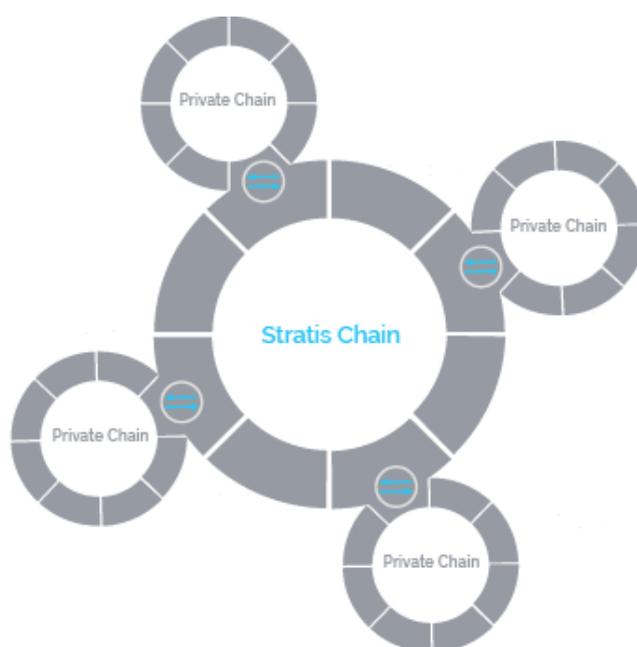
Stratis: key features

Stratis allows the creation of distinct, private blockchains, launched by third party organisations and tailored to their needs but secured on the main Stratis blockchain. They can be accessed via lite clients and simple but powerful APIs. Because these Private chains are based upon the code of the main Stratis chain and side chains are compatible and transfer between the two is straightforward.[\[8\]](#)

Stratis Private chains

A secure blockchain network will typically consist of hundreds or even thousands of computers running the same protocol. Consequently, there are significant advantages to employing an established network with proven stability and security, rather than starting from scratch. Although it is possible to develop applications on top of the Bitcoin blockchain, the first and still the best-known and most secure cryptocurrency network, there are good reasons why few businesses would want to do so. Bitcoin has comparatively slow 10-minute confirmation times, and periodic attacks on the network means that transactions can be delayed for hours; addressing these effectively requires a controversial hard fork and the pace of development is slow. Businesses have no control over upgrades or other changes to the network such as the capacity of each block and the rate that transactions that may be processed. Thus Bitcoin's security advantages come at a cost of significant rigidity and unpredictability.

By contrast, Stratis private chains allow developers complete freedom to customise their implementation for their specific needs, whilst the underpinning 'parent' blockchain is established enough to give users a high degree of confidence in its security. For example, if a business requires large block sizes to accommodate a high volume of transactions; rapid block times to enable low-latency trading; controlled transactions so that only approved users can submit a request to the network; a given rate of inflation; or additional space for metadata in each block, any or all of these can be specified at launch. The private chain can be accessed by straightforward APIs, meaning that stand-alone applications can rapidly be developed.



Stratis blockchain-as-a-service (BaaS)

Given both the advantages of cloud computing and the benefits of blockchain technology, there is a strong business case for deploying distributed ledgers in the same way, tailoring them according to the needs of the organisation in question. As with other forms of cloud usage, this allows an on-demand payment model, as well as scalability and removing the need for costly hardware and specialist expertise. BaaS enables an off-the-peg approach to blockchain use, placing it within the reach of any organisation.

The nature of the blockchain means that it cannot readily be located within the traditional framework of IaaS/PaaS/SaaS. Blockchains are software, run on distributed networks of computers. Moreover, 'blockchain' is a catch-all term for an approach to storage and consensus; blockchain protocols can provide a breadth of services as straightforward as value transfer (Bitcoin) to the execution of smart contracts (Ethereum). Thus there is a case for considering BaaS as the provision of infrastructure, platform and software at the same time.

Specifically, BaaS allows developers to test and deploy their bespoke blockchain-based applications in the cloud, without having to maintain the network or full clients themselves. The implementation of the blockchain can be tailored to their needs and accessed via lite clients or APIs.

Decentralised app hosting

As well as offering the services integrated in its own blockchain, Stratis will specialise in providing hosting and consultancy for decentralised applications (Dapps) on top of the Ethereum blockchain. This enables a complete off-the-peg approach to smart contracts. Stratis will work closely with businesses to determine their needs, before deploying nodes if required and organising hosting. This allows clients to focus solely on creating dapps without expending time and resources on infrastructure.

Bitcoin, Ethereum, LISK node provisioning

These solutions will not be confined to the Stratis chain and private chains. Stratis will enable one-click provisioning of other major blockchain platforms aside from its own, including Bitcoin, Ethereum, BitShares and LISK – each of which has its own character, community of developers and use cases. Thus if an organisation wishes to test out different networks, or use them in parallel to employ different functionality, there is nothing to stop them doing so quickly and easily.

For example, Ethereum's smart contracts and the WAVES decentralised asset exchange offer functionality not implemented by Stratis but that will be useful to certain businesses, either in combination with Stratis or on its own. Stratis Consultancy will provide consultancy services for many different blockchain solutions and can advise on which blockchain-based solution is most appropriate, and how businesses might go about deploying this, as well as installing required software and provisioning nodes if required.

This off-the-peg provisioning reduces the unnecessary overheads for blockchain deployment to near zero and makes Stratis the most convenient and cost-effective solution currently available.

One-click deployment

Stratis makes it easier than ever before for organisations to deploy private blockchains, taking a cloud services approach to provisioning. A one-click process means that new chains can be launched with unprecedented speed, tailored for the needs of the organisation. A broad range of variables including block time, size and space for metadata are customisable, making it incredibly flexible. Essentially, an entire network can be bootstrapped on the back of the main chain, giving a ready-made cryptocurrency ecosystem for developers to use out of the box.

Fiat gateway integration

Although blockchains allow for the transfer of value in the form of their native tokens, these have numerous problems from the perspective of a commercial enterprise, including compliance issues and the fluctuation in price that is a result of normal market supply and demand.

Stratis is designed with the integration of fiat gateways in mind from the outset. It allows financial organisations to use the blockchain for the transfer of existing currencies that are both readily accepted by mainstream consumers and are not subject to damaging volatility: tokens of value that are simply digital equivalents of regular money. This 'best of both worlds' approach means that businesses can maintain compliance in whatever way they see fit, according to jurisdiction and organisational policy, whilst simultaneously using the blockchain as a store of value – with all the advantages for speed, cost, transparency and stability of currency such a dual strategy allows.

Case study: Fiat Gateway

Financial services company RemitCo wishes to facilitate the remittance of funds by migrant workers in the Middle East back to their families at home. Although remittance is a \$600 billion market, there is little competition in many locations and low-income workers may be heavily penalised in various ways.

[Read More](#)

Three-tier architecture

The Stratis platform uses a three-tier architecture typical of the Microsoft® ASP.NET application style. This is a good fit as the Stratis Full Node, Stratis Blockchain API and the Stratis SPV technology are developed in C# and run within the Microsoft .NET Framework and common language runtime.

In the client tier, Browsers, Desktops, Mobiles, and IOT (Internet of Things) devices connect to the various services in the application tier. They receive blockchain data by querying the Stratis Chain API via HTTPS.

The application tier is composed of the Stratis Chain API, Cloud Stratis Management portal, Cloud Stratis API and Secure Payment Verification (SPV). All of the components in the application tier are developed in C#. The application tier handles Blockchain requests and SPV proofs for Lite clients that do not download the full blockchain. It also provides access to the Stratis Cloud management portal and API.

The server tier consists of the Stratis Full blockchain Node, the Cloud Stratis hosting layer and the Stratis payment protocol.

Stratis consultancy

The Stratis's headquarters will be based in London, a global financial centre and a hub for fintech services.

As thought leaders and practitioners of distributed ledger technology, Stratis will leverage its own expertise by offering consultancy services to other businesses working in the sector, thereby driving forward blockchain adoption and forging key partnerships where opportunities are presented.

London's light-touch approach to regulation means that many other cryptocurrency businesses are choosing the city for their headquarters and there is a growing concentration of skills and experience, as well as extensive access to traditional financial services businesses. Although Stratis's consultancy work will predominantly be within the UK, it will be expanded worldwide if there is demand. The work will focus on several key areas:

Blockchain consultancy

Stratis's consultancy arm will work with businesses to help them explore how blockchain technology can help them. Distributed ledger technology offers numerous specific benefits, but it is not a panacea and is not necessary or helpful in all cases. Stratis will help businesses and organisations of all sizes to pinpoint where they can save money

and increase efficiency, transparency and security using blockchain technology, and the solutions that are best suited for their circumstances and needs.

Active development for the Bitcoin ecosystem

Stratis's developers will actively contribute to the development of Bitcoin Core and Elements side chains,[\[9\]](#) while also further developing NBitcoin, the most complete C# .net Bitcoin library. The team will develop the Bitcoin version of NBitcoin while also creating their own NStratis version, rather than forking the code and developing this independently. Core to the aims of Stratis is to contribute to the ongoing development of other key projects in the relevant space.

This will not only help to advance blockchain technology more broadly, but will position Stratis as one of the top blockchain companies. Stratis will be based on the latest version of Bitcoin, so it will be a simple matter to implement any technology developed for Bitcoin (and in many cases from Stratis to Bitcoin).

Scalability

Scalability is a major issue for cryptocurrency protocols. Because every transaction is stored on the blockchain for transparency and immutability, in an unoptimised blockchain the size of the chain is a function of the number of transactions. This can cause serious issues. Bitcoin's 1 MB block sizes limit it to a low throughput of transactions per second (tps), and tensions between different stakeholders in the Bitcoin ecosystem (including miners, large holders/advocates and end-users) have meant that the problem has proven extremely difficult to fix. The result has been that there have been periods when transactions have been delayed because there is not enough space in a block. Consequently, few serious businesses would voluntarily expose themselves to the risks of using the Bitcoin blockchain for third-party applications, having no control over the future of the protocol and no influence over any improvements that might be made.

For Bitcoin, the problem of transaction volumes may yet be solved by a hard fork to enable larger blocks, but this is still a suboptimal solution. As transaction volumes grow exponentially with greater adoption (in the best case scenario), block size will also have to grow exponentially. This places greater demands on full nodes in terms of bandwidth and disk space. Despite expected advances in storage and connectivity technology, this will likely lead to an even greater centralisation of mining, in which only the best-resourced nodes can afford to maintain the network. Aside from any political and ideological concerns, this has implications for network security.

Stratis addresses these problems in several different ways. Firstly, every private blockchain is configurable, meaning that an organisation can choose how large blocks should be - reflecting their own needs and resources.

Related to this, instead of using a single ledger for every application, Stratis comprises a host chain from which financial businesses can deploy their own ledgers depending on their specific requirements, rather than directly using the same blockchain as the whole Stratis network (or the whole Bitcoin ecosystem, if the Bitcoin blockchain was employed). This offers the remarkable versatility of an extensive 2.0 platform, combined with the full control of a private chain - secured by the host blockchain but tailored and administrated by the owning organisation.

On a separate note, Stratis employs a proof-of-stake approach to consensus which aligns the interests of end-users (businesses) and those tasked with securing the network (full nodes). This means that a business can run a full Stratis node as well as nodes for their own blockchain without the overheads associated with specialist mining hardware.

Lastly, a series of measures will be used to combat bloat on the main chain, which ultimately serves as a means to secure child chains and can therefore be kept as lightweight as possible.

Bitcoin compatibility

Because Stratis's Private chains are based on the same code as the main blockchain, the interface for private chains is 100% compatible with that of the main Stratis chain. Stratis will provide the same RPC API as Bitcoin Core initially, which means that any applications or platforms that use Bitcoin's RPC or command line can be ported quickly to Stratis. New functionality is provided by Stratis-specific API calls.

The compatibility between main and Private chains also means that it is a simple matter to incorporate new features developed for Stratis into a private chain - and potentially vice versa, since any feature developed by a business could be released into a future update of Stratis. However, this would only take place with the express consent of the business. Although Stratis's customers de facto have full use of every feature on the Stratis blockchain, there is no onus on them to make privately-developed features available to others.

Conclusion

Stratis's private blockchains offer several significant advantages over the creation of a new chain from scratch, and for most organisations will provide all the required benefits without either being unnecessarily restrictive or entailing the significant overheads involved in creating and maintaining a cryptocurrency network.

The cloud provisioning approach to blockchain, or blockchain-as-a-Service (BaaS), makes deploying a new chain a process as simple as signing up for an account and selecting required parameters. These tailor-made solutions are accessible via web interfaces and APIs, although users can run full nodes for both their private chain and the host Stratis network if they wish. Compatibility with Bitcoin means that Bitcoin-based services can easily be ported to Stratis for additional functionality and convenience. As a result, Stratis is positioned strongly for an entry into the BaaS space.

Case Studies

Proof of Existence

The immutable and transparent nature of the blockchain lends itself to applications in which the existence of a file or document must be proved for a particular point in time.

Blockchain solutions are already informally used as a kind of digital copyright. Users take a 'hash' – a cryptographic digest of a file that serves as a unique fingerprint – and upload it to the blockchain. 2.0 blockchains that allow arbitrary messages to be recorded are convenient for this purpose, but Bitcoin and other first-generation blockchains allow short strings of characters to be embedded in transactions. Because each block is time-stamped and each hash represents a specific file (changing even a single character of a document or a pixel of an image results in a completely different hash), this proves with beyond any reasonable degree of doubt that the file existed at the time that the hash was uploaded. This is an approach that can be extended from copyright and patents to contracts of all kinds, and even to establishing the physical condition of a property or a hire car before it is used by a customer.

Clearing and settlement

Clearing and settlement is a major pain point for the banking industry, costing many tens of billions of dollars every year. Recent research by Santander suggested that a near real-time digital ledger for clearing could save over \$20 billion per year. [\[4\]](#)

Many of the cost savings centre on the clearing and settlement cycle that is a feature of most current investment markets. Counterparty balances across a wide range of markets and financial institutions around the world are matched and reconciled on a rolling three-day basis. Currently this takes place on technology that is more than 40 years old as payments are batched and sent at intervals by a system called Automated Clearing House (ACH). There are significant benefits to moving this process to a blockchain platform, as some major banks are now actively considering, thereby clearing payments almost instantly. This could also potentially reduce the capital financial institutions have to hold against trades.

For some multinational organisations where several different currencies may be in use and funds moved between countries and departments on a daily basis – and particularly for the remittance industry – such an approach could prove invaluable for cross-border financial transfers. The blockchain potentially cuts the time for reconciliation down from a day or more to just minutes. [\[5\]](#)

Creating a private blockchain

TradeCorp is a financial services business that wishes to deploy and test a trading platform that utilizes blockchain technology. As part of their Agile development, they decide to develop a proof-of-concept platform to explore the issues they will face when bringing their idea to market.

Due to the anticipated volume and speed of transactions, they require 10 MB blocks and 30-second block time, and hence Bitcoin is not fit for their purposes. Instead, they engage Stratis to deploy and host a Private Chain for them. This is achieved with the following steps:

- Create an account on the Stratis Cloud Portal
- Purchase Stratis to fuel your Private Chain. (There will be a simple process for purchasing Stratis with many different payment options)
- Visit the provisioning tab on the Cloud management portal and select 'Deploy private blockchain'. Provide the required blockchain specifications outlined below:
- Identifying Name of the blockchain
- Target block time (e.g. 30 seconds)
- Privacy level - any peer can join the network; private network; private or public transactions
- Mining rewards (private chain mining only). E.g. 100 native currency units per block, halving every 100,000 blocks.
- Ports for P2P connections and the JSON-RPC API, e.g. 6060, 5721.
- Permitted transaction types, e.g. paytoaddress, paytomultisig, paytoscripthash.
- Maximum block size, e.g. 5 MB.
- Maximum metadata per transaction (OP_RETURN), e.g. 4,096 bytes.
- Click confirm/create new blockchain
- TradeCorp's private blockchain has now been provisioned and their primary node can be accessed via SSH on the IP/port displayed in the Stratis management portal.

TradeCorp now have a Private blockchain that is secured by the Stratis parent blockchain, which also meets their exact requirements. They also have access to the all of the technology developed by the Stratis projects, which can be deployed to their blockchain with little development overhead.

The whole process can be completed in as little as 10 minutes.

Stratis is designed to make provisioning customised blockchains as easy as possible and with the needs of the financial services industry in mind. These features mean that it is a versatile solution for most businesses, from SMEs up to large financial organisations.

Fiat gateway

Financial services company RemitCo wishes to facilitate the remittance of funds by migrant workers in the Middle East back to their families at home. Although remittance is a \$600 billion market, there is little competition in many locations and low-income workers may be heavily penalised in various ways. Unofficial services run by unscrupulous operators leave them open to risk, and fees can be high – as much as 10% of monthly pay. A lack of documentation and the comparatively small amounts of money involved mean that many cannot access official banking and money transfer services. Nevertheless, a high proportion are web literate and own internet-enabled mobile phones.

RemitCo deploys a private blockchain on top of the Stratis network and creates a token representing units of the local fiat currency in which migrant workers are paid. A service in the host country collects funds from employees and acts as a gateway to the blockchain. The workers now send these fiat tokens back to their families, which takes seconds or minutes instead of days, costs almost nothing and is fully secure and transparent – there are no unwanted middlemen and no hidden costs. A separate branch of RemitCo in the receiver's country acts as a gateway for funds back out of the blockchain.

Because RemitCo's blockchain is private, there are no concerns about fraud or money laundering since only approved personnel can move funds into and out of the blockchain. Similarly, the use of fiat-equivalent tokens means that users are not exposed to exchange rate volatility, as they would be if they used Bitcoin or other open protocols. The remittance process is streamlined and cost-effective, meaning that RemitCo can charge a smaller fee than the unofficial money transfer businesses, whilst offering a better service for its customers. Thus Stratis offers advantages for RemitCo that would not be available with a fully public blockchain.

Blitz sidechain

The Blitz blockchain already has a dedicated community and a series of services built on top of it. These include the Fitalize platform, which uses fitness devices such as the Fitbit to reward users with crypto coins on a per-step basis, and The Viral Exchange (TVE), a social media project that leverages cryptocurrency payments to incentivise users to like, share and follow posts for rapid publicity and growth.

In this example, the Blitz developers and community decide to move their blockchain to the Stratis ecosystem, thereby gaining a series of benefits:

- **Accelerated development.** Blitz is now able to follow closely the code base of Stratis, rather than spend time and resources maintaining its own version of the network software. Very little development is required in order to update the code.

- **New features.** As well as its own features, Blitz can now use all of the features offered by Stratis – again saving the time, money and effort otherwise required to develop these from scratch on a separate chain.
- **New network and network effect.** Blitz will keep its own services and the businesses it has built up around it, but it can now provide those to the whole Stratis ecosystem – enabling the community to access new markets and other businesses.
- **Continued independence.** Blitz retains its own unique character, community and use-cases, new potential users notwithstanding. The developers and community can make their own decisions about the direction taken by the platform, facilitated but not restricted by being part of Stratis.

References

- [1] <https://bitcoin.org/bitcoin.pdf>
- [2] <https://www.gov.uk/government/news/distributed-ledger-technology-beyond-block-chain>
- [3] <http://money.cnn.com/2015/11/02/technology/bitcoin-1-billion-invested/>
- [4] <http://www.ft.com/cms/s/2/eb1f8256-7b4b-11e5-a1fe-567b37f80b64.html#axzz46TUQ2D8h>
- [5] <https://research.tabbgroup.com/report/v14-009-blockchain-clearing-and-settlement-crossing-chasm>
- [6] The most complete Bitcoin port (Part 1: Crypto),
<http://www.codeproject.com/Articles/768412/NBitcoin-The-most-complete-Bitcoin-port-Part-Crypt>
- NBitcoin Indexer: A scalable and fault tolerant block chain indexer,
<http://www.codeproject.com/Articles/819567/NBitcoin-Indexer-A-scalable-and-fault-tolerant-blo>
- [7] See Programming The blockchain in C#,
<https://www.gitbook.com/book/programmingblockchain/programmingblockchain/details>
- [8] Blockstream Elements <https://blockstream.com/sidechains.pdf>
- [9] <https://elementsproject.org/>